BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 38, Number 2, Pages 131–169
S 0273-0979(00)00892-2
Article electronically published on December 27, 2000

RESOLUTION OF SINGULARITIES AND MODULAR GALOIS THEORY

SHREERAM S. ABHYANKAR

Abstract. I shall sketch a brief history of the desingularization problem from Riemann thru Zariski to Hironaka, including the part I played in it and the work on Galois theory which this led me to, and how that caused me to search out many group theory gurus. I shall also formulate several conjectures and suggest numerous thesis problems.

Section 0: Preamble

I want to tell you the story of the problem of resolution of singularities in algebraic geometry and its intimate relationship with Galois theory and group theory. With a view towards making the subject more approachable to prospective students, my story will be intermingled with personalized history.

I shall start off in Section 1 by giving examples of singularities of curves and surfaces. Then in Section 2 we shall see what it means to resolve these singularities. A bit of history will trace my mathematical lineage and its links to the resolution problem in particular and algebraic geometry in general. In Section 3 we shall make the passage from characteristic zero to positive characteristic. In Section 4 I shall illustrate the traditional Indian method of learning by recounting my experiences with my father. Then I shall show how my journey from India to the United States for doing graduate work paralleled the march of algebraic discoveries from India through Arabia to Europe in ancient times. This resulted in my meeting my Guru Zariski at Harvard. Section 4 is concluded by describing how I found my Ph.D. problem in Zariski's address at the International Congress of 1950.

Section 5 gives more details of my early training under Zariski. This was marked by the reading of the fundamental work of Krull on generalized valuations and their use by Zariski to explain birational transformations. Then in Section 6 we come to the high regard held by Zariski for the works of Jung and Chevalley. Jung's work on complex surface singularities dates back to 1908. Chevalley's fundamental paper on local rings appeared in 1943. Zariski asked me to put these two together. In this an important role is played by Zariski's theory of normalization which, following Dedekind, gets rid of singularities in codimension 1. Also topological ideas come to the fore. They tell us the Galois structure of singularities. This amalgamates the ideas of Galois and Riemann.

Received by the editors December 7, 1999.

2000 *Mathematics Subject Classification.* Primary 12F10, 14H30, 20D06, 20E22.

Abhyankar's work was partly supported by NSF Grant DMS 97-32592 and NSA grant MDA 904-97-1-0010.

In Section 7, we come to Zariski's returning from an Italian trip, and my making counter-examples. These counter-examples show a fundamental difference between the Galois theories of singularities in characteristic zero and prime characteristic p. As a result, for resolving singularities, it becomes necessary to augment the abstract college algebra arsenal of local rings and valuations by the explicit manipulations of high-school algebra. It took another ten years to inject more and more high-school algebra for converting the characteristic p surface desingularization to arithmetic surfaces and characteristic p solids. But unlike the surface case, the solid case is settled only over algebraically closed ground fields. Section 8 takes up the solid case over finite fields. There a simultaneous resolution conjecture is formulated for deducing the finite field case from the algebraically closed case. Also there is an analogous birational factorization conjecture. Both of these have local and global versions. Some progress in these was done by some of my former students. Indeed, as I shall relate throughout the paper, in addition to having an illustrious line of teachers and teacher's teachers, I have been blessed with numerous brilliant students who continue pushing the frontiers of the subject. It is a fulfilling pleasure to be sandwiched in between.

In Section 9, to make matters more precise, I take recourse of the language of models. Points and curves on a surface are replaced by their local rings. Likewise irreducible subvarieties of a higher dimensional variety are replaced by their local rings. A projective model is a suitable collection of local rings. Birational transformations are converted into dominating models. Numerous problems in the area of resolution of singularities are formulated as precise Ph.D. or post-Ph.D. problems.

Expanding on the thoughts of Galois and Riemann, Section 10 relates fundamental groups from topology to Galois groups from algebra via monodromy groups from analysis. There I list the books which Zariski advised me to read concerning this matter.

This brings us to the second part of the paper emphasizing Galois theory and group theory. Section 11 explains how the nonadaptability of Jung's desingularization method to characteristic p led me to formulate some Galois theory conjectures for the affine line and more generally for affine curves. The great interest shown by Serre brought me back to this topic after a thirty-year gap. In the meantime several talented students kept me busy with singularities of special subvarieties of flag manifolds and related combinatorics of Young tableaux.

As described in Section 12, soon it became clear to me that to pursue Galois theory, a retooling in group theory was essential. So I renewed my acquaintance with Walter Feit, and made the acquaintance of numerous other group theory gurus from Bill Kantor to Ernie Shult and Michael O'Nan. Of special importance in this activity are the various recognition theorems of group theory described in Section 13. The tie up with them is provided by the method of throwing away roots as explained in Section 14. Putting all this together, in Section 15 it is shown that some explicit unramified coverings of the affine line which were divined in my 1957 paper have various interesting groups as Galois groups. These include the alternating and symmetric groups, the five Mathieu groups, and several finite classical groups. Some of this is joint work with my students and collaborators.

Section 16 continues the mathematical genealogy by recording that David Harbater, who settled the affine curve conjecture, is my nephew, since he was a student of Mike Artin, who in turn was a student of Zariski. Harbater based his proof on the work of Raynaud, who had settled the affine line conjecture. Various other

Galois theory conjectures for curves and higher dimensional varieties are formulated in Sections 16 to 19, and some of them are posed as Ph.D. and post-Ph.D. problems. In Section 17 we provide links between these conjectures and the theory of permutation polynomials. Likewise, in Section 18 we link them to Galois embedding problems and in Section 19 with generalized iterates coming out of the seminal work of Carlitz on explicit class field theory.

With this survey of the contents at hand, let us start by asking:

Section 1: What are singularities?

At a singularity a curve crosses itself or has a special beak-like shape or both. For instance the alpha curve $y^2 - x^2 - x^3 = 0$ crosses itself at the origin, where it has the two tangent lines $y = \pm x$. Such a singular point is called a node. The cuspidal cubic $y^2 = x^3$ has a beak-like shape at the origin. Such a singularity is called a cusp. Most points of a curve are simple points. Singularities are those points where the curve has some special features. The vertex of the quadratic cone $z^2 = x^2 + y^2$ is an example of a surface singularity. Thus the origin $(0, 0, 0)$ is a double point of the cone, and all other points of the cone are simple points.

Quite generally most points of a hypersurface in n-space given by a polynomial equation $f(x_1, \ldots, x_n) = 0$ are simple points. At a simple point P at least one of the partial derivatives of f is not zero. Say the partial of f with respect to x_1 is not zero at P. Then by the implicit function theorem we can solve $f = 0$ near P by expressing x_1 as a function of $x_2, \ldots, x_n$. When we cannot do this, we have a singular point. Thus the singular points of the hypersurface are where f as well as all its partials are zero. Here by partials we mean the first partials.

If all the first partials of f are zero at a point P, but some second partial is not, then P is called a double point. Similarly for triple or 3-fold, 4-fold, $\ldots$, e-fold points. Thus simple means 1-fold. If the locus in n-space we are studying is given by several equations $f_1 = 0, \ldots, f_m = 0$ in $x_1, \ldots, x_n$, then instead of taking the n first partials of the single polynomial f, we take the $m \times n$ jacobian matrix of the first partials of the polynomials $f_1, \ldots, f_m$ with respect to the variables $x_1, \ldots, x_n$. Now the singular points are defined to be those where the rank of this matrix is not maximal. Alternatively, simple points are those where its rank is maximal, and then by the multivariate implicit function theorem, near a simple point, all of the variables can be expressed as functions of some of them, say d of them. The given locus consisting of the common solutions of the simultaneous equations $f_1 = 0, \ldots, f_m = 0$ is called an algebraic variety of dimension d.

Section 2: What does it mean to resolve them?

Let us make the substitution $x = x'$ and $y = x'y'$ in the equation of the nodal cubic, i.e., the alpha curve given by $y^2 - x^2 - x^3 = 0$. This gives us $y^2 - x^2 - x^3 = x'^2y'^2 - x'^2 - x'^3 = x'^2(y'^2 - 1 - x')$. Discarding the extraneous factor x'^2 we get the proper transform $y'^2 - 1 - x' = 0$, which being a parabola has no singularities. Thus the singularity of the nodal cubic is resolved by one quadratic transformation. The inverse of the quadratic transformation is given by $x' = x$ and $y' = y/x$. The indeterminate form y/x indicates that, as x and y both approach zero, y' takes all possible values. In other words, the origin $(0, 0)$ of the (x, y)-plane blows-up into the line $x' = 0$ of the (x', y')-plane which we call the exceptional line. It is this explosion that unravels the singularity. By putting $x' = 0$ in the original equations $x = x'$ and

$y = x'y'$ we directly see that the exceptional line shrinks to the origin $(0, 0)$ of the (x, y)-plane. The total transform of the nodal cubic consists of the exceptional line together with the proper transform which is a parabola. At any rate a quadratic transformation and its inverse both involve only rational expressions, and so a quadratic transformation is birational. A birational transformation of a plane is called a Cremona transformation in honor of the originator of such transformations. As a piece of history, Cremona was my triple-parama-guru. Veronese was a pupil of Cremona. Castelnuovo was a pupil of Veronese. My own guru Zariski was a pupil of Castelnuovo. This makes Castelnuovo my parama-guru and Veronese my parama-parama-guru.

In the latter half of the nineteenth century there was close communication between the Italian algebraic geometry school led by Cremona and the German algebraic geometry school led by Felix Klein and Max Noether. Taking the cue from Cremona [Cre], in 1873 Noether [NoM] showed that the singularities of any plane curve can be resolved by a finite succession of quadratic transformations.

As Klein says in his colorful book [Kle], *Entwicklung der Mathematik im neunzehnten Jahrhundert* (*Development of Mathematics in the Nineteenth Century*), he and Noether were both disciples of Clebsch, who in turn was a follower of Riemann. Indeed it was Riemann who in his 1851 thesis [Rie] introduced the Riemann surface of y as an algebraic function of x when y is related to x by a polynomial equation $f(x, y) = 0$. This may be regarded as the first proof of resolution of singularities of plane curves. Riemann's construction of the Riemann surface is topological and function-theoretic. Noether tremendously simplified the matter by replacing topology and function theory by algebra and geometry. Indeed, sometimes Noether is called the father of algebraic geometry. However, again referring to his *Entwicklung*, Klein says that, "we, the young Germans, learned algebraic geometry from Salmon-Fiedler," which refers to Fiedler's German translation of Salmon's 1852 book [Sal] on Higher Plane Curves. In turn, Salmon, in the preface to his book, says that he was only reporting on the works of his two friends, Cayley [Cay] and Sylvester [Syl]. So there is justification in saying that algebraic geometry started in England around 1840 in the hands of the invariant trinity (Klein's words) Cayley-Sylvester-Salmon. Of course, we may even stretch back the birth of algebraic geometry to the works of Isaac Newton [New] around 1660.

I am well aware that this view of the origins of algebraic geometry may differ from some people's strong belief that the entire subject was spontaneously born in Grothendieck's mind [Gro] around 1962 and revealed to the rest of mankind by the kind agency of Hartshorne [Har] in 1977.

For the viewpoint that algebraic geometry started with Newton, or even with the Indian mathematicians Shreedharacharya and Bhaskaracharya of 500 A.D. and 1100 A.D. respectively, you may see my 1976 *American Mathematical Monthly* article [A11] entitled "Historical ramblings in algebraic geometry and related algebra", which was later expanded into my 1990 American Mathematical Society book [A15] entitled *Algebraic Geometry for Scientists and Engineers.*

Section 3: Resolution from Riemann through Zariski to Hironaka

Thus Riemann's topological and function-theoretic construction of the Riemann surface of $f(x, y) = 0$ was algebracized (or geometrized) by Noether in resolving the singularities of the curve $C : f(x, y) = 0$ by a succession of Cremona quadratic transformations. Another way of algebracizing the Riemann construction was put forward by Dedekind in the Dedekind-Weber paper [DWe] of 1882. To wit, Dedekind took the integral closure of the affine coordinate ring of C in its quotient field and, lo and behold, the singularities of C are resolved in one fell swoop. Emmy Noether [NoE], the daughter of Max, followed Dedekind in developing the college algebra of groups-rings-fields by adding to it a rich chapter of ideal theory. On the other hand, Max Noether's algebraization belonged to the high-school algebra of polynomial and power series manipulation. Thus Max Noether, in addition to being a possible father of algebraic geometry, could also be called a grandfather of modern algebra.

Amongst the three approaches to curve resolution, namely that of Riemann, Noether, and Dedekind, it was primarily Noether's method which found its flowering in resolution of singularities of surfaces and solids (= 3-dimensional objects) by Zariski [Za2], [Za4] in 1939-1944, and then in 1964 by Hironaka [Hir] for all dimensions. However, the Zariski-Hironaka work was restricted to characteristic zero, i.e., when the coefficients of the polynomials defining the variety are in a field of characteristic zero such as the field of real or complex numbers. A field is a set of elements with the operations of addition and multiplication defined on them. It is of characteristic zero means that in it $1 + 1 + \cdots + 1$ is never zero. It is of prime characteristic p if in it $1 + 1 + \cdots + 1$, taken p times, equals zero. For example we could add and multiply any two of the integers $0, 1, \ldots, 6$ and then replace the result by the remainder obtained after dividing it by 7; this gives us a field of characteristic 7; in it for instance we have $4 + 4 = 1$ and $4 \times 4 = 2$. So what about resolving singularities of surfaces, solids, and higher dimensional varieties, over a field of characteristic p? This is where I entered the picture.

Section 4: How I got interested in doing resolution

To start at the beginning, my father taught me mathematics by the ancient Indian method. Thus he would recite to me a few lines from the geometry and algebra books written by Bhaskaracharya around 1100 A.D. These books, called *Leelavati* and *Beejganit*, being the first two parts of his five-part treatise on astronomy, are in Sanskrit verse. I would then commit those lines to memory by repeating them several times. My father would follow it up by reciting a few more lines. With the implicit faith that their sound would eventually reveal their meaning, I would repeat the new lines several times, and so on. The solution of a quadratic equation by completing the square which I had memorized in this manner is reproduced in my 1982 Springer Lecture Notes on Canonical Desingularization [A12]. There I go on to say that the entire essence of Hironaka's proof lies in generalizing this completing of the square method.

This is an example of the dictum that history should be interesting and inspiring, though not necessarily completely true. What I am referring to is the fact that although I did learn from my father, when I was about ten, Bhaskaracharya's book on geometry called *Leelavati*, it was much later when I was about forty-five that at my request my father made a Marathi translation of Bhaskaracharya's book on algebra called *Beejganit*, and it was only then that I memorized the verse giving the completion of the square method of solving quadratic equations.

At any rate, armed with the high-school algebra (i.e., manipulative algebra) training from my father, in July 1951, when I was twenty, I set out for America by boat.

Embarking from the Bombay pier my boat took the same path by which algebra had traveled from India to Europe via Arabia, where it acquired its current Arabic-derived name as opposed to its original Sanskrit name Beejganit. Refueling at the Arabian Sea port of Aden, the boat proceeded to touch land next in Italy, where, in the sixteenth century, cubic and quartic equation were solved by Cardano and Ferrari. Next stop was Marseille, in France. There I said, "Aha, here is where the youthful Galois, in 1830, proved the impossibility of solving quintic equations by introducing the Galois group." Once again this is an example of making history colorful, because actually by the time the boat touched port in Marseille I had become unconscious because of typhoid fever, which I caught on the boat. Also the boat may have landed in Italy only in my imagination. From there we went on to England, where I was stranded for two months in the Seaman's Hospital. In my hospital bed I may have been (?) absorbing the sympathetic waves radiated by Caley-Sylvester-Salmon as they went about creating algebraic geometry from 1840 to 1880. Was I also imbibing the spirit of Newton, which is perennially alive in his binomial theorem with exponents integral or fractional and in his fractional power series expansions, which were rediscovered one hundred fifty years after him by Puiseux?

Thus I was a month and a half late arriving at Harvard. It happened to be a Saturday, when normally professors do not come to the department. Luckily for me on that Saturday the departmental secretary was there and pointed out to me, "Mr. Zariski is here, so you may go and talk to him." I proceeded to have a long two-hour conversation with Zariski. He asked me many questions and I reciprocated, not yet being exposed to the western etiquette of avoiding personal questions. So he found out that my father was a math professor, and I found out that he was brought up by his mother in a town where the borders changed between Russia and Poland, but he regarded himself as a Russian. He told me that his mother had a cloth shop. My teachers in Bombay had suggested I take three elementary courses and one advanced course, as was allowed to entering graduate students at Harvard, but after talking to me Zariski completely changed my plan, and so I ended up with three advanced courses and only one elementary course and that too only because Zariski was teaching it. Thus, I never took a basic course on linear algebra. I at once proceeded to take Zariski's advanced course based on notes of his forthcoming book, which eight years later metamorphed into his two-volume treatise [ZSa] with Samuel. The elementary course which I took with Zariski was Math 103 on projective geometry.

On that same eventful Saturday, at Zariski's suggestion, I walked to his house to borrow his copy of Veblen and Young's book [VYo] on projective geometry, which was being used in the course. This was the first of many trips to his house, later accompanied by meals there due to the kindness of Mrs. Yole Zariski. Especially I remember the tasty salads made with romaine lettuce.

So my relationship with Zariski started the very first day I arrived in America.

At the end of the first semester, seeing how excited I had become about the projective geometry course, Zariski said to me, "Projective geometry is a beautiful dead subject. Do not try to do research in it." Nevertheless, in my second semester, being scared out of Whitney's topology course, I took yet another semester of higher dimensional projective geometry with Zariski, in which he explained Grassman coordinates.

During the summer between my first and second years in graduate school I spent most of my time, almost twelve hours a day, in the library looking through many of Zariski's papers. I came upon Zariski's hour lecture at the International Congress of Mathematicians held two years before in Cambridge. It was the first such meeting after the sixteen-year interruption caused by the war and its aftermath. Zariski's paper [Za5] was on ideas of abstract algebraic geometry. In it he described how he resolved the singularities of surfaces and solids in characteristic zero and declared the problem in characteristic p to be intractable even for the innocent-looking surface $z^p = f(x, y)$. He continued by saying, "It is not a problem for the geometer, but it is a problem for the algebraist with a feeling for all the unpleasant things which can happen in characteristic p." On reading this, I immediately said to myself, "This is what I am going to do for my thesis."

Section 5: Zariski gives me a reading course

Towards the end of my first summer at Harvard, i.e., late August or early September of 1952, one day I met Zariski riding home on his bicycle. Seeing me he got down, and we chatted a bit. Then I asked him if I could have a reading course with him that fall. Whereupon he asked me if I was going to register for his course on algebraic curves. When I said I did not know, he responded that then he would not give me a reading course. To that I shrugged my shoulders, and he started riding away. After going a bit he returned. Getting down from his bicycle, he asked me whether I was going to work with him. Again, when I said I did not know, he repeated that he would not give me a reading course and started riding away. After riding off a short distance he again returned. Again getting down from his bicycle, he said, "All right, you may have the reading course," and he rode away. So in the end I did register for his course on algebraic curves and for the reading course. I found his very first lecture on algebraic curves, full of places and valuations, so exciting that at the end of it I went up to him and told him that yes, I did want to work with him and have chosen as my thesis topic the problem of characteristic p resolution mentioned in his International Congress Address of 1950. To that he smiled and let it pass. During the next several months he tried to indicate that this was not a thesis problem and I should be working on something easier. Then in the spring he went off to Italy for a semester.

Having taken three courses with Zariski and having gotten so interested in his work, why was I being so evasive about working with him? The problem was that Pesi Masani, my teacher in Bombay, was a student of Garrett Birkhoff. Masani had communicated with Birkhoff regarding my admission to Harvard. On the boat from Bombay I had solved one and a half unsolved problems listed in Birkhoff's book [Bir] on lattice theory. Birkhoff assumed that this would form the main part of my thesis. In later years I had many pleasant contacts with Birkhoff, and in fact my "Historical ramblings" article [A11] was written largely due to his constant encouragement. Moreover, my early training in lattice theory had gotten me interested in ordered structures. That is what immediately attracted me to the problem of resolution of singularities with its close connection to valuation theory which involves ordered abelian groups. The original construction of real valuations by Ostrowski [Ost] in 1918 was generalized by Krull in his 1932 paper [Kr1] on

"Allgemeine Bewertungstheorie", where he employed values in any ordered abelian group. These general valuations of Krull form the basis of Zariski's paper [Za3] on birational correspondences, where he uses them to algebracize the idea of limits.

Section 6: Zariski asks me to read Jung and Chevalley

In the spring of 1953, while Zariski was in Italy, we corresponded several times. Seeing that I was not giving up on characteristic p resolution, he wrote me a four-page letter suggesting possible approaches. Specifically he suggested that I should read the 1908 paper [Jun] of Jung, where he proved a local version of resolution of singularities of complex surfaces. Zariski went on to say that I should also study the 1943 local rings paper [Che] of Chevalley and use it to algebracize Jung's proof with a view of adapting it to characteristic p. Zariski continued by summarizing Jung's proof thus. Let us project the given algebraic surface $S : f(x, y, z) = 0$ of z-degree n onto the (x, y)-plane. Then above most points of the (x, y)-plane there lie n points of the surface S. Those points above which there are fewer than n points are called discriminant points. They fill up a curve D in the (x, y)-plane given by the vanishing of the z-discriminant of f, i.e., the z-resultant of f and its z-derivative f_z. Applying Noether's resolution process to D, we may suppose that D has only normal crossings, i.e., only nodes for its singularities. Now the local fundamental group at a simple point of D is cyclic, and at a node it is abelian on two generators; and hence in the former case the corresponding points of S are simple, and in the latter case they are 'nice' singularities which can be resolved without much effort. This is what I was supposed to algebracize and adapt to characteristic p if possible. In the claim that points of S, above a simple point of D, are simple for S, we are actually replacing S by its normalization. It was this process of normalization of surfaces and higher dimensional varieties by which Zariski, in his 1939 paper [Za1], had generalized Dedekind's idea of curve resolution by passing to the integral closure, the clue being the fact that a normal variety has no singularities in codimension 1. Eventually I ended up by showing that Jung's method cannot be adapted to characteristic p because, even at a simple point of the branch locus, the local fundamental group need not be abelian and actually may even be unsolvable, and points of the normal surface above it may be singular. For a normal variety, the discriminant locus coincides with the branch locus. In general, the discriminant locus is the union of the branch locus and the projection of the singular locus.

Towards the end of his stay in Italy, Zariski sent me a postcard suggesting that I go over to his house in Cambridge to meet his son, Raphael, who would let me take whatever of Zariski's reprints I could find, including the only remaining copy of his 3-dimensional resolution paper [Za4], and to get Raphael's help for getting a summer job in the Harvard University Press, where he was working. In the same postcard Zariski informed me, referring to his recent ulcer operation, that a 3-dimensional singularity was removed from his stomach. This was a picture postcard of Michaelangelo's statue of Moses. It is still in my possession. Ever since, in my mind, I have always identified Zariski with the wise Moses.

Section 7: I make counter-examples

In the fall of 1953, when Zariski returned from Italy, I presented him with my 50-page essay on the algebraization of local fundamental groups as a family of

Galois groups, which is how I paraphrased Jung's ideas by using Chevalley's local rings paper supplemented by the equally fundamental 1938 local rings paper [Kr2] of Krull and the 1946 local rings paper [Coh] of Cohen. This essay was subtitled "My attempt at understanding your four-page letter" together with the sentence "Please tell me if I am studying in the right direction." I followed this up by biweekly ten-page bulletins entitled "On uniformization i" with $i = 1, 2, \ldots, 9$. In Bulletin 1, I gave a counter-example to the local fundamental group at a normal crossing being abelian even in characteristic p. Then Zariski said that at least at a simple point of the branch locus the local fundamental group should be cyclic. In Bulletin 2, I showed that, in characteristic p, this need not even be solvable. Then Zariski suggested that at least points of the surface above a simple point of the branch locus should be simple. In Bulletin 3, I gave a counter-example to this also. After two or three further such negative bulletins, Zariski said that his ideas were exhausted. After a couple of more weeks of hard work I dialed TR(owbridge) 6-7938, which was Zariski's home phone number, still etched in my memory, and told him that I cannot do characteristic p resolution. Zariski responded that all right, after some time we could discuss a suitable thesis problem for me.

After that phone call, continuously for three days and three nights, that is seventy-two hours at a stretch, I kept working on characteristic p surface resolution and got the first positive result by uniformizing valuations whose value group consists of rational numbers with unbounded powers of p in their denominators, since, in his 1950 International Congress Address, Zariski had declared these to be the most intractable. As a beginning I dealt with the case of $p = 2$. Excitedly, late at night I telephoned Zariski with the good news. Early next morning he came to the department, and I started explaining the matter to him on the blackboard. When I fumbled, Zariski said, "What is the matter with you, Abhyankar? In spite of having a fever I have come to listen to you." Fortunately my fumble was only temporary. Then in the next three or four biweekly bulletins I finished resolving singularities of characteristic p surfaces. This positive result appeared in my 1956 paper [A02]. The various counter-examples appeared in my 1955 paper [A01]. Two years later, in my 1957 paper [A05], by taking plane sections of the surfaces involved in these counter-examples, I was led to a conjecture about fundamental groups of affine curves in characteristic p. Then, in my 1959-60 papers [A06], I used the local fundamental group results of [A01] to obtain some results on global fundamental groups of surfaces in characteristic p.

In April or May of 1954 Zariski said that I should submit my Ph.D. thesis, but I held off, saying that I wanted to do it for any dimension. By August, Zariski insisted I finish. In fact he had already applied to the newly formed National Science Foundation to grant me a post-doctoral fellowship for the academic year 1954-55, saying in the application that during that year I was well qualified to do the higher dimensional problem. When in September 1954 Zariski gave a dinner party to celebrate my thesis, he told me that he too was unhappy that I was about to give up the problem, because, although it was his duty to say that it was not a thesis problem, he had very much hoped I would be able to solve it. Another pleasant memory I have about my thesis is that John Tate joined the Harvard math department the day I defended my thesis, and I was able to answer all the questions he asked me in my oral exam. Yet another amusing memory is that when originally I had written only a two-page introduction to my thesis, Zariski wrote from his Nantucket vacation cottage that I must do a better job in my introduction, because that was the only part which Richard Brauer, who was the second reader, was expected to read. When I ended up writing a twelve-page introduction, Zariski was very happy. In spring 1953, when Zariski was in Italy, I had taken a course on noncommutative rings with Brauer, and when I proposed Cohen's paper [Coh] as a topic for the term paper for that course, Brauer said, "No, that is too much Zariski-type," and so I ended up writing about Hochschild cohomology. It took me another thirty-five years to realize what great group theory pioneering work Brauer had done. Also I have pleasant memories how, during my post-doctoral year 1954-55, Tate used to come over to my apartment to give me private lessons in algebraic number theory. During that year I also heard some inspiring MIT lectures of Iwasawa on infinite Galois theory of algebraic number fields. The influence of Brauer, Iwasawa, and Tate is evident in my work on algebraic fundamental groups.

In spite of Zariski saying to NSF that I was well equipped to do higher dimensional resolution during the academic year 1954-55, actually it took me ten more years to do characteristic p resolution for dimension 3, as reported in my 1966 Academic Press book [A08], and for dimensions higher than that the problem still remains open. In the meantime in my 1965 Purdue Conference paper [A07], I had proved resolution of singularities for arithmetical surfaces, i.e., surfaces defined by polynomials with integer coefficients, which in my 1969 Tata Institute Conference paper [A10] I extended to the still more general situation of 2-dimensional excellent schemes. Again the resolution problem remains open for three and higher dimensional arithmetical varieties or excellent schemes. Seeing that not much progress in the resolution problem was made after my 1966 book, Springer-Verlag put out a new edition [A31] of it in 1998. In this new edition, I have added an appendix giving a short proof of analytic resolution for all dimensions in characteristic zero. This proof is a consequence of a new avatar of an algorithmic trick which I had used in the original edition of the book. The same algorithmic trick was also used in my 1966 paper [A09], dedicated to the centenary of my parama-guru (= guru's guru) Castelnuovo, to prove some lemmas leading to local uniformization of valuations of maximal rational rank for all dimensions in characteristic p. This analytic proof should provide a good introduction to the great papers of Zariski and Hironaka. Hopefully it should also provide an impetus to young algebraic geometers to complete the resolution problem. In particular:

Section 8: Here is a start-up resolution problem for a thesis

Unlike the surface case, where I proved resolution of singularities over any field of characteristic p for 3-dimensional varieties, in my 1966 book [A08] I proved it only over algebraically closed fields of characteristic p; actually, in [A08] I assumed $p > 5$, and, as reported on page 253 of [A15], I dealt with $p \leq 5$ elsewhere. These restrictions were due to the fact that in [A08] I used an Auxiliary Theorem which says that any d dimensional variety over an algebraically closed ground field can be birationally transformed to a variety having no e-fold point for any $e > d!$. I proved this Auxiliary Theorem by generalizing an argument used by Albanese [Alb] in the surface case and by repeated use of the Veronese embedding invented by my parama-parama-guru Veronese. This refers to the fact that by referring to the ∞^5 conics in the projective plane as hyperplane sections in the 5-dimensional projective space we get an embedding of the projective plane in the projective 5-space, and similarly referring to all m-degree hypersurfaces in the projective n-space as hyperplanes we embed it in the projective r-space with $r = \binom{n+m}{m} - 1$. Since the Auxiliary Theorem is proved by projecting from rational e-fold points with large e, the ground field is required to be algebraically closed. Now 3-dimensional resolution over finite fields, which is in great demand for arithmetical applications, would follow from 3-dimensional resolution over algebraically closed fields if the Weak Simultaneous Resolution Conjecture, which I made in my 1956 paper [A04], can be proved in its local form in the 3-dimensional case.

In his 1951 paper [Za6] on Holomorphic Functions, which was declared "bahnbrechend" by Krull, Zariski generalized the concept of the normalization of a variety V in its function field K to the normalization of V in a finite algebraic field extension K' of K. If we can find a nonsingular variety W which birationally dominates V and whose normalization in K' is nonsingular, we may say that we have Simultaneous Resolution for V in K'. In [A04] I showed that this is not always possible even locally for surfaces. This led me to make the Weak Simultaneous Resolution Conjecture, which says that it should be possible to find a normal W birationally dominating V such that the normalization of W in K' is nonsingular, and to the corresponding Local Conjecture, which says that this can be done along any valuation. The two-dimensional case of the said Local Conjecture played an important role in my proof of characteristic p surface resolution given in [A02] and also in my arithmetic surface resolution proof given in [A07]. The thesis problem which I am suggesting, and which would complete the proof of 3-dimensional resolution over finite fields, is to settle the said Local Conjecture for dimension three. Some cases of this were done in the 1996 thesis [Fu1] of David Fu, the twenty-second of my twenty-four Ph.D. students.

To pose another related thesis problem, suppose that a nonsingular variety W birationally dominates a nonsingular variety V. We may then ask if W is necessarily an iterated monoidal transform of V, i.e., if there exists a sequence $V = V_0, V_1, \ldots, V_s = W$ of birationally equivalent nonsingular varieties which are successively obtained by blowing-up nonsingular subvarieties. In [Za4] Zariski proved this to be so for characteristic zero surfaces, and then in [A03] I generalized it for general surfaces. In his 1971 thesis [Sha] my fourth Ph.D. student, David Shannon, showed that this is not true for dimension three even locally. This led me to make the Weak Birational Factorization Conjecture saying that there always exists an iterated monoidal transform $\overline{V}$ of V such that $\overline{V}$ is also an iterated monoidal transform of W, and also the corresponding Local Conjecture along any valuation. This Local Conjecture was solved by my eighth Ph.D. student, Chris Christensen, in his 1977 thesis [Chr] for some 3-dimensional local cases. Recently, in [Cu1] and [Cu2], Dale Cutkosky settled the Local Conjecture for any dimension in characteristic zero. So I am glad to declare Dale to be my adopted post-doctoral student. As a thesis problem, I propose the Local as well as Global versions of the Weak Birational Factorization Conjecture for all dimensions and all characteristics, including arithmetical varieties.

Section 9: More precisely speaking

Since I am suggesting these as thesis problems, let me depart from the informal style which I have followed so far and state things more precisely. So here is a brief review of the relevant definitions; details can be found in my books [A08] and [A15].

Let k be either a field or the ring of ordinary integers; i.e., let us be in the algebraic or the arithmetical case respectively. Let K be a function field over k; i.e., let K be an overfield of k such that K is the quotient field of a finitely generated ring extension of k. Let d be the dimension of K over k; i.e., if k is a field, then d equals the transcendence degree of K over k, and if k is the ring of integers, then d equals one plus the said transcendence degree. The problem of resolution of singularities amounts to finding a nonsingular projective model of K/k. Before defining these terms, let us introduce local rings.

A quasilocal ring R is a (commutative) ring (with 1) having a unique maximal ideal $M(R)$. A local ring R is a noetherian quasilocal ring; the smallest number of elements which generate $M(R)$ is called the embedding dimension of R, and the maximum length l of chains of distinct prime ideals $P_0 \subset P_1 \subset \cdots \subset P_l$ in R is called the dimension of R; we always have $\operatorname{emdim}(R) \geq \dim(R)$, and R is said to be regular if equality holds. A typical example of an n-dimensional regular local ring is the (formal) power series ring in n indeterminates with coefficients in any field. For any (integral) domain A, the set of all localizations A_P of A with respect to the various prime ideals P in A is denoted by $\mathfrak{V}(A)$. Here A_P is the set of all x/y with $x \in A$ and $y \in A \setminus P$; it is a quasilocal ring with $M(A_P) = PA_P$ and $A \cap M(A_P) = P$; if A is noetherian, then so is A_P; if A is a regular local ring, then so is A_P. If B is a polynomial ring over k, then every member of $\mathfrak{V}(B)$ is regular; geometrically speaking this says that the geometric and arithmetical affine spaces are nonsingular.

A quasilocal ring R^* dominates a quasilocal ring R means R is a subring of R^* and $M(R) = R \cap M(R^*)$. A quasilocal ring R^* dominates a set Λ of quasilocal rings means R^* dominates some member of Λ. A set Λ^* of quasilocal rings dominates a set Λ of quasilocal rings means every member of Λ^* dominates Λ. A valuation of K/k is a map $v : K \to \Gamma \cup \{\infty\}$, where Γ is an ordered abelian group, such that for all $a \neq 0 \neq b$ in K we have $v(ab) = v(a) + v(b)$ and $v(a+b) \geq \min(v(a), v(b))$, for any $a \in K$ we have: $v(a) = \infty \Leftrightarrow a = 0$, and for all $0 \neq c \in k$ we have $v(c) = 0$. By omitting this last condition we get the definition of a valuation of any field K. By the valuation ring of v we mean the set R_v consisting of all $a \in K$ with $v(a) \geq 0$; note that R_v is a quasilocal ring with quotient field K, and $M(R_v)$ consists of all $a \in K$ with $v(a) > 0$. We say that a valuation v dominates a quasilocal ring R or a set of quasilocal rings Λ, meaning that R_v dominates R or Λ respectively.

By an affine subring of K/k we mean a subring A of K with quotient field K such that $A = k[\xi_1, \ldots, \xi_n]$ for a finite number of elements $\xi_1, \ldots, \xi_n$ in A; we then say that $\mathfrak{V}(A)$ is an affine model of K/k. By a projective model of K/k we mean a set of local rings which can be expressed as a union $\cup_{0 \leq i \leq n} \mathfrak{V}(A_i)$ of affine models of K/k for which there exist nonzero elements $\eta_0, \ldots, \eta_n$ in K such that $A_i = k[\eta_0/\eta_i, \ldots, \eta_n/\eta_i]$ for $0 \leq i \leq n$. To see that affine models correspond to affine varieties, let Q be the kernel of the k-epimorphism of the polynomial ring $B = k[x_1, \ldots, x_n]$ onto A which sends x_i to ξ_i. Let $\mathfrak{Z}(Q)$ be the variety in the affine n-space over k defined by Q, i.e., the zero-set of Q. Then $\mathfrak{Z}(P) \mapsto A_{P/Q}$, with P varying over all prime ideals in B with $Q \subset P$, gives a bijection of the set of all irreducible subvarieties of $\mathfrak{Z}(Q)$ onto $\mathfrak{V}(A)$. Similarly, projective models correspond to projective varieties. All this is very clear when k is an algebraically closed field; in the more general case it is somewhat make-believe.

More generally, by a model of K/k we mean a set V of local rings which can be expressed as a nonempty finite union of affine models of K/k such that any valuation v of K/k dominates at most one member of V which, if it exists, is called the center of v on V. A model of K/k is said to be nonsingular if every member of it is regular. A model of K/k is said to be complete if every valuation of K/k dominates it. A projective model of K/k is clearly a complete model of K/k. Now we are ready to state the precise versions of the Resolution Conjecture and the Uniformization Conjecture.

Resolution Conjecture. *There exists a nonsingular projective model of K/k.*

Uniformization Conjecture. *Given any valuation v of K/k there exists a projective model of K/k on which the center of v is regular.*

Clearly the Resolution Conjecture is stronger than the Uniformization Conjecture. As I have already said, these were settled affirmatively by: (1) Riemann for $d = 1$ and $k =$ the complex field, (2) Dedekind for $d = 1$ and any k, (3) Zariski for $d \leq 3$ and $k =$ a field of characteristic zero, (4) Hironaka for any d and $k =$ a field of characteristic zero, and (5) me for $d = 2$ and any k as well as for $d = 3$ and $k =$ an algebraically closed field of characteristic p. In all other cases these conjectures are wide open and are inviting attention of young algebraic geometers.

To make the Birational Factorization Conjectures precise, let us define monoidal transformations. First, for the local version, given a regular local ring R, by a nonsingular ideal in R we mean a nonzero nonunit ideal I in R such that R/I is a regular local ring, and given a valuation v of the quotient field of R dominating R, by a monoidal transform of R along v we mean a local ring R_1 of the form $R_1 = R[I/\zeta]_{M(R_v)\cap R[I/\zeta]}$ for some nonsingular ideal I in R and some nonzero element ζ of I with $R[I/\zeta] \subset R_v$, and we note that then R_1 is a regular local ring which dominates R and is dominated by v. By an iterated monoidal transform of R along v we mean a regular local ring $\overline{R}$ for which there exists a finite sequence $R = R_0, R_1, \ldots, R_e = \overline{R}$ such that R_i is a monoidal transform of R_{i-1} along v for $1 \leq i \leq e$. Next, for the global version, by an ideal I on a projective model V of K/k we mean an assignment which, to every $R \in V$, assigns an ideal $I(R)$ in R, such that for every affine subring A of K/k with $\mathfrak{V}(A) \subset V$ we have $(\cap_{R\in\mathfrak{V}(A)} I(R))R = I(R)$ for all $R \in \mathfrak{V}(A)$, and, assuming V to be nonsingular, we say that I is nonsingular if, for every $R \in V$, the ideal $I(R)$ in R is either the unit ideal or a nonsingular ideal. By a monoidal transform of a nonsingular projective model V of K/k we mean a set V_1 of local rings such that for some nonsingular ideal I on V we have $V_1 = \{R \in V : I(R) = R\} \cup_{R\in V \text{ with } I(R)\neq R} (\cup_{0\neq\zeta\in I(R)} \mathfrak{V}(R[I/\zeta]))$, and we note that then V_1 is a nonsingular projective model of K/k which dominates V. By an iterated monoidal transform of V we mean a nonsingular projective model $\overline{V}$ of K/k for which there exists a finite sequence $V = V_0, V_1, \ldots, V_e = \overline{V}$ such that V_i is a monoidal transform of V_{i-1} for $1 \leq i \leq e$. Now here are the precise versions of the Birational Factorization Conjectures.

Weak Birational Factorization Global Conjecture. *Given any nonsingular projective models V and W of K/k, there exists an iterated monoidal transform $\overline{V}$ of V such that $\overline{V}$ is also an iterated monoidal transform of W.*

Weak Birational Factorization Local Conjecture. *Given any projective models V and W of K/k, and any regular members $R \in V$ and $S \in W$ which are dominated by a common valuation v of K/k, there exists an iterated monoidal transform $\overline{R}$ of R along v such that $\overline{R}$ is also an iterated monoidal transform of S along v.*

Again, as I have said, the $d = 2$ case of both of these was done by Zariski [Za4] and I [A03], some cases of the $d = 3$ Local Conjecture were done by Christensen [Chr], and the general d case of the Local Conjecture when k is a field of characteristic zero was done by Cutkosky [Cu1], [Cu2]. All other cases are open as possible thesis problems. The weaker versions of these two Conjectures may be stated as:

Birational Domination Global Conjecture. *Given any nonsingular projective models V and W of K/k, there exists an iterated monoidal transform $\overline{V}$ of V such that $\overline{V}$ dominates W.*

Birational Domination Local Conjecture. *Given any projective models V and W of K/k, and any regular members $R \in V$ and $S \in W$ which are dominated by a common valuation v of K/k, there exists an iterated monoidal transform $\overline{R}$ of R along v such that $\overline{R}$ dominates S.*

For both of these: the $d = 2$ case was done by Zariski [Za2] and me [A03], the $d = 3$ case was done by Zariski [Za4] and me [A08] when k is a field of characteristic zero or nonzero respectively, and the general d case was done by Hironaka [Hir] when k is a field of characteristic zero. All other cases are good thesis problems.

Note that for $d = 1$ the above four as well as the next four conjectures are trivially true. Also note that for $d = 2$ the Birational Factorization Conjectures follow from the corresponding Birational Domination Conjectures in view of the above stated fact that, for $d = 2$, Zariski [Za4] and I [A03] had proved "Strong Birational Factorization", saying that a nonsingular projective model W of K/k which dominates another nonsingular projective model V of K/k must be an iterated monoidal transform of V. Again as stated above, for $d = 3$, "Strong Birational Factorization" was disproved by Shannon [Sha].

Turning to the Simultaneous Resolution Conjectures, recall that a local ring is normal means it is integrally closed in its quotient field, and a model is normal means every member of it is normal. Let K' be a finite algebraic field extension of K, let V be a normal projective model of K/k, and let $R \in V$. By a local ring in K' lying above R we mean the localization of the integral closure of R in K' at a maximal ideal in the said integral closure. By the normalization of V in K' we mean the set V' of all local rings in K' which lie above various members of V; it can be shown then that V' is a projective model of K'/k. Now we may state the Simultaneous Resolution Conjectures.

Weak Simultaneous Resolution Global Conjecture. *Given any normal projective model V of K/k, any finite algebraic field extension K' of K, and any nonsingular projective model V' of K'/k which dominates the normalization of V in K', there exists a normal projective model W of K/k dominating V such that the normalization of W in K' is an iterated monoidal transform of V'.*

Weak Simultaneous Resolution Local Conjecture. *Given any normal projective model V of K/k, and any finite algebraic field extension K' of K, let V' be any normal projective model of K'/k which dominates the normalization of V in K', and let v' be any valuation of K'/k whose center R' on V' is regular. Then there exist normal projective models W and W' of K/k and K'/k respectively such that for the center S' of v' on W' we have that S' is an iterated monoidal transform of R' along v' and for $S = K \cap S'$ we have that $S \in W$ and S' lies above S.*

For $d = 2$, the above Local Conjecture played an important role in my surface resolution proofs given in [A02], [A07], and some cases of the above Global Conjecture were done in my paper [A04]. For $d = 3$, some cases of the above Local Conjecture are in Fu's thesis [Fu1]. All other cases of the above two conjectures provide excellent thesis problems. In particular, in case of $d = 3$ and $k =$ a finite field, a positive answer to the above Local Conjecture will provide a positive answer to the Resolution Conjecture.

With the definition of monoidal transformations at hand, we may strengthen the Resolution and Uniformization Conjectures thus. Given a principal ideal I in a regular local ring R, we say that I has a normal crossing at R if $I = x_1^{u_1} \dots x_n^{u_n} R$ where $u_1, \dots, u_n$ are nonnegative integers and $(x_1, \dots, x_n)R = M(R)$ with $\dim(R) = n$; if the number of nonzero u_i is t, then we say that I has a t-fold normal crossing at R. By a nonzero principal ideal on a model V of K/k we mean an ideal I on V such that, for every $R \in V$, the ideal $I(R)$ in R is a nonzero principal ideal. A nonzero principal ideal I on a nonsingular projective model of K/k is said to have only normal crossings on V if, for every $R \in V$, the ideal $I(R)$ has a normal crossing at R. Given any nonsingular projective model W of K/k dominating a nonsingular projective model V of K/k and given any ideal I on V, we get a unique ideal IW on W such that for all $R \in V$ and $S \in W$ with S dominating R we have $(IW)(S) = I(R)S$; it is clear that if I is a nonzero principal ideal on V, then IW is a nonzero principal ideal on W. Now we are ready to state:

Embedded Total Resolution Conjecture. *Given any nonzero principal ideal I on any nonsingular projective model V of K/k, there exists an iterated monoidal transform W of V such that the ideal IW has only normal crossings on W.*

Embedded Total Uniformization Conjecture. *Given any projective model V of K/k, any regular $R \in V$, any nonzero principal ideal I in R, and any valuation v of K/k dominating R, there exists an iterated monoidal transform S of R along v such that the ideal IS has a normal crossing at S.*

Both these were done by me for $d = 2$ in [A03], [A32] and for $d = 3$ with any field k in [A08], and by Hironaka for any d with a characteristic zero field k in [Hir]. All other cases constitute top-notch thesis problems.

Section 10: Fundamental groups and Galois theory

Zariski's fall 1952 course on algebraic curves was very algebraic. In the entire course he drew a picture only once. That was to explain the relation of fundamental groups from topology to Galois groups from algebra via monodromy groups from complex function theory, which made me rather nostalgic, because while I was in college in India, I had studied plenty of complex function theory from British books, such as Forsyth's 1893 book [For], although I did not know much about algebraic geometry as such. Indeed, seeing that in the various footnotes in Forsyth's book the frequent message was "for a thorough and rigorous treatment see such and such source material in German," during my first year in college I spent eight hours a day studying German. This came in handy when, in spring 1953, the four books on algebraic geometry which Zariski advised me to study were all in German. In addition to Severi's *Vorlesungen* [Sev], they were the three old Riemann Surface books by Neumann [Neu], Stahl [Sta], and Weyl [Wey]. About Stahl's book I have an entry in my diary calling it the book I enjoyed most. Actually, although I distinctly remember Zariski talking about the fundamental group of the punctured real plane (= complex line) in terms of the standard loops around the punctures, I do not really remember his relating it to Galois groups.

In any case, to discuss this relationship let us consider a univariate monic polynomial

$$F(Y) = Y^n + \sum_{1 \le i \le n} a_i Y^{n-i} = \prod_{1 \le j \le n} (Y - \alpha_j)$$

of degree $n > 0$ with coefficients a_i in a field K, and roots α_j in an overfield of K. Assume that F is separable; i.e., the roots α_j are distinct. Let S_n be the permutation group on n letters. According to Galois' original definition, the Galois group $\mathrm{Gal}(F, K)$ is the group of all relations preserving permutations of the roots of F, i.e., the subgroup of S_n consisting of all $\sigma \in S_n$ such that $\Phi(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)}) = 0$ for all polynomial relations $\Phi(\alpha_1, \ldots, \alpha_n) = 0$ over K. According to the more modern definition, $\mathrm{Gal}(K', K)$ is the group of all K-automorphisms of the splitting field $K' = K(\alpha_1, \ldots \alpha_n)$ of F over K, and $\mathrm{Gal}(F, K)$ is the permutation representation of $\mathrm{Gal}(K', K)$ which sends each $\tau \in \mathrm{Gal}(K', K)$ to the $\sigma \in S_n$ such that $\tau(\alpha_i) = \alpha_{\sigma(i)}$. Better still, thinking of S_n as acting on $\alpha_1, \ldots, \alpha_n$, we simply have $\tau(\alpha_i) = \sigma(\alpha_i)$.

When the coefficients $a_1, \ldots, a_n$ of F are themselves polynomials in a multivariable $X = (X_1, \ldots, X_d)$, a knowledge of the Galois group of F helps us to understand the singularities of the d-dimensional hypersurface $F = 0$. In case these polynomials in X have complex coefficients, by giving various values to X and solving for Y, we get n determinations of Y as a function of X. These n determinations permute amongst themselves when X traverses various closed paths emanating from a fixed point P in the d-dimensional complex space $\mathbb{C}^d$ punctured at the discriminant points Δ of F, which are the values of X to which correspond less than n values of Y. Note that Δ is the zero-set of the Y-discriminant of F which is obtained by eliminating Y between F and its Y-derivative F_Y. The totality of these permutations of the n determinations constitute the monodromy group of F, which was introduced by Riemann [Rie] in 1851. It is easy to see that the Galois group of F is isomorphic as a permutation group to its monodromy group. Moreover, the monodromy theorem of complex analysis says that when two paths are homotopic, i.e., can be continously deformed into each other, they give rise to the same permutation of the n determinations. This sets up a homomorphism from the topological fundamental group $\pi_1(\mathbb{C}^d \setminus \Delta, P)$ of the punctured d-space $\mathbb{C}^d \setminus \Delta$ with base point P onto the monodromy group of F, and hence also onto the Galois group $\mathrm{Gal}(F, \mathbb{C}(X))$ of F over the rational function field $\mathbb{C}(X)$ which consists of quotients of polynomials in X with complex coefficients. Note that $\pi_1(\mathbb{C}^d \setminus \Delta, P)$ is the group of all homotopy equivalence classes of closed paths in $\mathbb{C}^d \setminus \Delta$ emanating from P. Thus calculations of Galois groups and fundamental groups reflect on each other.

Section 11: Unsolvable surface coverings

To show that Jung's 1908 proof of a local version of resolution of singularities of complex surfaces does not adapt to characteristic p, in my 1955 paper [A01], I considered the surface given by

$$\widehat{F}(Y) = Y^{p+1} + XY + Z$$

and projected it onto the (X, Z)-plane. To find the discriminant locus for this projection, we calculate the Y-derivative to be $\widehat{F}_Y = Y^p + X$, and eliminating Y between it and $\widehat{F}$ we get $\widehat{F} - Y\widehat{F}_Y = Z$. Thus the discriminant locus is the line $Z = 0$ which has a simple point at the origin $X = Z = 0$. Now the algebraic reflection of the local fundamental group is the local Galois group $\mathrm{Gal}(\widehat{F}, \widehat{K})$ where $\widehat{K}$ is the (formal) meromorphic series field $k((X, Z))$ over the algebraically closed field k of characteristic p. In [A01], for $p = 5$, by direct computation I showed that $\mathrm{Gal}(\widehat{F}, \widehat{K})$ is unsolvable. Thirty-five years later, in [A17], I proved that for any p we have $\mathrm{Gal}(\widehat{F}, \widehat{K}) = \mathrm{PGL}(2, p)$, where we recall that for any integer $m > 0$ and any power $q > 1$ of p, the m-dimensional general linear group $\mathrm{GL}(m, q)$ is the group of all $m \times m$ nonsingular matrices over the Galois field $\mathrm{GF}(q)$ of q elements, and the projective general linear group $\mathrm{PGL}(m, q)$ is the homomorphic image of $\mathrm{GL}(m, q)$ when we mod it out by all scalar matrices. Also note that the special linear group $\mathrm{SL}(m, q)$ consists of all members of $\mathrm{GL}(m, q)$ whose determinant equals 1, and the projective special linear group $\mathrm{PSL}(m, q)$ is the corresponding subgroup of $\mathrm{PGL}(m, q)$.

Stepping back to relate things chronologically, in my 1957 paper [A05], i.e., two years after the 1955 paper [A01], I took a plane section of the above surface covering and by generalizing it obtained several explicit equations giving unramified covering of the affine line L_k over k. These equations included the trinomials

$$\overline{F}_n(Y) = Y^n + XY^t + 1 \quad \text{where} \quad 0 < n - p = t \not\equiv 0 \bmod p,$$

and I proposed that their Galois groups $\mathrm{Gal}(\overline{F}_n, k(X))$ be computed. Without actually computing these Galois groups, but indirectly manipulating with the above coverings, I showed that by taking subquotients of the algebraic fundamental group $\pi_A(L_k)$ we get all finite groups. This led me to make the following conjecture where $Q(p)$ is the set of all quasi-p groups, that is finite groups G which are generated by their p-Sylow subgroups.

Affine Line Conjecture. $\pi_A(L_k) = Q(p)$.

Here the algebraic fundamental group $\pi_A(L_k)$ is defined to be the set of all finite Galois groups of unramified coverings of L_k, and the subquotients of $\pi_A(L_k)$ are the homomorphic images of the subgroups of the groups belonging to $\pi_A(L_k)$. As I noted in [A05], the inclusion $\pi_A(L_k) \subset Q(p)$ is an easy consequence of the Riemann-Hurwitz genus formula. In [A05] I also made the following stronger conjecture where $Q_t(p)$ is the set of all quasi-(p, t) groups, i.e., finite groups G such that $G/p(G)$ is generated by t generators, with $p(G) =$ the subgroup of G generated by all of its p-Sylow subgroups.

Affine Curve Conjecture. *For any nonnegative integer t we have $\pi_A(L_{k,t}) = Q_t(p)$ where $L_{k,t} = L_k$ minus t points, and more generally for any nonsingular projective curve C_g of genus g over k we have $\pi_A(C_{g,t}) = Q_{2g+t}(p)$ where $C_{g,t} = C_g$ minus $t + 1$ points.*

Again, the algebraic fundamental groups $\pi_A(L_{k,t})$ and $\pi_A(C_{g,t})$ are defined to be the sets of all finite Galois groups of unramified coverings of $L_{k,t}$ and $C_{g,t}$ respectively.

After another two years, in the series of papers [A06] which I wrote in 1959-60, I used the local results of the 1955 paper [A01] to prove some global results about coverings of varieties with branch loci having only normal crossings. It may be noted that in writing the papers [A05] and [A06] I was influenced by Serre, who, since 1956, has been a second guru to me.

Then for about thirty years I forgot all about coverings and fundamental groups, until fall 1988 when suddenly Serre sent me a series of four long letters, briefly saying that he had gone back to my 1957 paper [A05] and could prove that for $t = 1$ the Galois group $\mathrm{Gal}(\overline{F}_n, k(X))$ equals $\mathrm{PSL}(2, p)$ and asking me if I could now calculate it for $t > 1$. He also asked that, since my Affine Line Conjecture implies every finite simple group of order divisible by p and hence every alternating group A_n with $n > p+1 > 3$ belongs to $\pi_A(L_k)$, could I find such alternating group coverings.

Immediately upon receiving Serre's letters I did not pay full attention to them, because for the last six years, that is from 1982 onwards, I was busily working on Young Tableaux with a view of applying them to analyze the singularities of certain special subvarieties of flag manifolds. Some of this tableaux work with applications to Invariant Theory can be found in my book [A14] *Enumerative Combinatorics of Young Tableaux* with its summary in my paper [A13] dedicated to Nagata's sixtieth birthday, and in my tutorial paper [A16] for a conference on Computer Vision which has a quick introduction to flag manifolds. The combinatorial aspects of the tableaux work can also be found in my three joint papers [AK1]–[AK3] with my twelfth Ph.D. student, Devadatta Kulkarni; my four joint papers [AJ1]–[AJ4] with my fourteenth Ph.D. student, Sanjeevani Joshi; and my one joint paper [AG1] with my fifteenth Ph.D. student, Sudhir Ghorpade. Some other related tableaux work can be found in the paper [Mul] of my tenth Ph.D. student, S. B. Mulay; in the paper [Udp] of my thirteenth Ph.D. student, S. G. Udpikar; and in the paper [Mod] of my seventeenth Ph.D. student, M. R. Modak.

Section 12: I meet many group theory gurus

Fortunately in Serre's last letter of 1988 he said, "My email is...." Being a new convert to email, I was very enthusiastic about it and so our weekly "conversation" by email started. During the next two years we exchanged almost a hundred emails and smails. In the first few months of our correspondence it became clear to me that I must learn a lot of group theory, since it provides a powerful tool for computing Galois groups. During October to December, while Serre was at Harvard, emails from him were my primary source of picking up group theory knowledge. But then in the middle of December 1988 Serre returned to Paris, where he did not as yet have email.

So what to do? Looking through group theory literature and looking through the AMS directory for emails, which were not yet very common, I realized that Bill Kantor in Oregon might be a possible group theory guru. So I sent off an email to him asking some questions. Back came a reply saying, "I am a walking encyclopedia of group theory. Ask me anything." Soon I realized this was indeed very true. After several months of remaining an e-guru, eventually he visited me in Purdue, where he talked all the time. Afterwards I fell into the habit of making a bi-annual pilgrimage to Eugene, Oregon, to get my next lesson, and then the next lesson, and so on. Bill has an uncanny intuition of how group theory can be useful in my Galois theory work, so he throws out juicy information. But since things are obvious to him, he is reticent about explaining them. So in Ernie Shult of Manhattan, Kansas, I found a gentler, kinder group theorist who patiently fills in the gaps and of course provides a lot of new information too.

By and by, to my growing list of group theory gurus I have added Peter Neumann of Oxford, Peter Cameron of Queen Mary College in London, Martin Liebeck of Imperial College in London, Jan Saxl of Cambridge, John Thompson of Florida and Cambridge, Gernot Stroth of Halle, Christopher Hering of Tübingen, Bob Guralnick of USC, Michael Aschbacher of Cal Tech, Jonathan Hall and Ulrich Meierfrankenfeld of Michigan State, John Conway of Princeton, Steve Smith of Chicago, and the late Michio Suzuki of Illinois.

But before meeting this long line of group theory gurus, after Serre left for Paris, I renewed my old acquaintance with Walter Feit, dating back to 1957, and with the late Danny Gorenstein, dating back to 1953. First in February 1989 I spent a week at Yale as a houseguest of Walter and Sidnie Feit. In addition to reminiscing about how we frequently used to eat together and go to movies together at Cornell in 1957, Walter proceeded to pull me up by the bootstraps about the development of group theory in the last thirty years. Then in April 1989 I spent a few days with Danny Gorenstein at Rutgers and there met another very kind and gentle guru, Michael O'Nan. Indeed in the last seven or eight years it has become my habit that when I get stuck on some 'obvious' point in group theory, I call up either Ernie Schult or Michael O'Nan.

In realizing that group theory and Galois theory are two facets of the same fundamental entity, I was only retracing Galois' discovery. At any rate, I am very humbled by seeing how smart all these great group theory gurus are and how very profound their knowledge is.

Actually, as may be clear from the fact that in my thesis I could prove the unsolvability of certain Galois groups, my interest in group theory is long-standing and started when, as a college student in Bombay, I was reading Birkhoff-Mac Lane's book [BMa] *Survey of Modern Algebra* and found in it the easy-to-state conjecture of Burnside that every finite group of odd order is solvable. Fascinated by this conjecture, I wrote to Philip Hall in Cambridge for advice. It is he who in a way jump-started group theory in England after the pioneering days of Caley and Burnside. In his reply, Philip Hall sent me a list of group theory papers I could be reading. Following his advice I read some papers of Bernhard and Hanna Neumann and some papers of Reinhold Baer. I should point out that in Bombay I was already reading the group theory books of Carmichael [Car], Speiser [Spe], and Zassenhaus [Z02] with occasional guidance of F. W. Levi, who was a friend of my father and who had joined the newly opened Tata Institute as one of the two math professors. In 1956 Levi returned to the Free University of Berlin. The other math professor in Tata Institute, D. D. Kosambi, was also a friend of my father. When Kosambi asked me why I was majoring in physics in spite of being more interested in mathematics, I said, "Because of my intense interest in mathematics and mathematics being otherworldly, I don't know what I should do if one day I can no longer do mathematics," to which Kosambi replied, "Then you should kill yourself." In my mind that cleared the way for me to just pursue mathematics. It was in Gwalior, where my father, S. K. Abhyankar, was a professor of mathematics, that I was introduced to Burnside and Panton's *Theory of Equations* [BPa], from which I first learned group theory. This was William Snow Burnside and not the group theorist William Burnside. It is only recently that I realized that there were two Burnsides. Incidentally, both got a D.Sc. from Dublin around the same time.

Many years later I met Zassenhaus first in Notre Dame and then in Ohio State. When one day in June 1990 Garrett Birkhoff was our lunch guest, he told us that Carmichael was his father's first Ph.D. student.

After coming to Harvard, I fell under the magnetic spell of Oscar Zariski and forgot all about group theory. It was amazing that after thirty years, when I needed to update my knowledge of group theory, my new gurus were Walter Feit and John Thompson, who had solved the odd order problem; Bill Kantor, who was a student of a student (Peter Dembowski) of Reinhold Baer; Peter Neumann, who is a son of Bernhard and Hanna Neumann; and the three brilliant students of Peter Neumann, i.e., Peter Cameron, Jan Saxl, and Martin Liebeck. It was a happy coincidence when, in 1983 while lecturing in Canberra, Australia, I was telling the story of Alfred Young and a spry old gentleman from the audience started correcting me. Lo and behold it was none other than Bernhard Neumann, to whom I was happy to say, "Your and Hanna Neumann's were the very first mathematical papers I ever read." Once, on relating all this to Serre I said, "What a small world," to which he replied, "No, what a nice world."

Section 13: Recognition theorems of group theory

A more poetic title for this section could have been "Attempts to use the power of modern group theory of finite simple groups for calculating Galois groups".

At any rate, various Recognition Theorems of Group Theory provide powerful tools for computing Galois groups. They also provide suggestive guidelines for constructing explicit equations with assigned Galois groups. Examples of such Recognition Theorems are:

(1) CT = Classification Theorem of Finite Simple Groups,
(2) CPT = Classification of Projectively Transitive Permutation Groups (using CT),
(3) CDT = Classification of Doubly Transitive Permutation Groups (using CT),
(4) CR3 = Classification of Rank 3 Permutation Groups (again using CT),
(5) Jordan-Marggraff Theorems on Limits of Transitivity,
(6) Burnside's Theorem (which is a special case of the O'Nan-Scott Theorem),
(7) Zassenhaus-Feit-Suzuki Theorem,
(8) Kantor's Rank 3 Theorem (using Buekenhout-Shult's Polar Space Theorem),
(9) Cameron-Kantor's Theorems on Transitive Collineation Groups, and
(10) Liebeck's Orbit Size Theorems (which use CT).

Here CT says that, in addition to the cyclic groups of prime order and the alternating groups on at least 5 letters, the 16 infinite families of finite simple Lie-type groups, i.e., matrix groups over finite fields, together with the 26 sporadic (= one of a kind) finite simple groups, constitute a complete list of finite simple groups; for details see Gorenstein's article [Gor] or Kleidman-Liebeck's book [KLi]. As related in [Gor], CT was a team effort of several dozen group theorists carried on over the thirty-year period 1950-1980. The prototypes of the finite simple Lie-type groups are the projective special linear groups $\mathrm{PSL}(m,q)$ of dimension m over the Galois Field $\mathrm{GF}(q)$ of q elements where $q > 1$ is a power of a prime p, excluding small values of m and q. These linear groups, together with the symplectic, unitary, and orthogonal groups, are called the classical groups, which have to be supplemented by their exceptional and twisted incarnations. Note that the symplectic, unitary and orthogonal groups are the isometry groups of alternating, hermitian, and quadratic forms respectively. Thus they are the finite field analogues of the group of distance-preserving linear transformations of the real euclidean space; for details see Aschbacher's book [As2]. Recall that a finite group is simple means that it has no nonidentity normal subgroup other than itself; as usual $<$ and $\triangleleft$ denote subgroup and normal subgroup respectively, and so $H \triangleleft G$ means $H < G$ such that $gHg^{-1} = H$ for all $g \in G$; a composition series of a finite group G is a series $1 = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_l = G$ such that G_i/G_{i-1} is simple for $1 \leq i \leq l$; the factor groups G_i/G_{i-1} are called composition factors of G; and G is solvable means all of its composition factors are cyclic. The oldest amongst the sporadics are the five Mathieu groups $M_{11}, M_{12}, M_{22}, M_{23}, M_{24}$ (where the subscript indicates the degree as a permutation group, i.e., the number of letters they permute) which appeared in his 1861 paper [Mat]. Although they all turned out to be simple, they were originally discovered by Mathieu as exactly 4-transitive, 5-transitive, 3-transitive, 4-transitive, 5-transitive permutation groups respectively, where we recall that a permutation group is t-transitive means it sends any t letters of the permuted set to any other t letters of the permuted set; also transitive means 1-transitive, and exactly t-transitive means t-transitive but not $(t+1)$-transitive. For a good discussion of the Mathieu groups see Huppert-Blackburn's book [HBl]; the remaining 21 sporadics were discovered a century later as reported in [Gor].

For CT $\Rightarrow$ CPT = the classification of all subgroups of $\mathrm{GL}(m, q)$ acting transitively on nonzero vectors, see Kantor's 1985 paper [Ka2], which is partly based on Hering's papers [He1] and [He2]. The proof of CDT uses CT directly as well as CPT, and it also uses the O'Nan-Scott Theorem about primitive groups (see Cameron [Cam]), which is a sharpening of Burnside's Theorem proved in his book [Bur], which asserts that a doubly transitive permutation group has a unique minimal normal subgroup, which is either elementary abelian or nonabelian simple; note that an elementary abelian group is the direct sum of a finite number of copies of a cyclic group of prime order. For a cursory treatment of Burnside's theorem see Wieland's book [Wie], which also describes the Jordan-Marggraff theorems (Jordan [Jor] and Marggraff [Mar]) on limits of transitivity characterizing alternating and symmetric groups. An elementary self-contained treatment of Burnside's theorem may be found in my forthcoming paper [A36]. Recall that a point stabilizer G_u of a transitive permutation group G consists of those members of G which map an element u of the permuted set onto itself; G is primitive means G_u is a maximal subgroup of G, the number of orbits of G_u is called the Rank of G, and their sizes are called the subdegrees of G. The implication CT $\Rightarrow$ CR3 was achieved by Liebeck [Li1] and others; it uses the fundamental results of Aschbacher [As1] on maximal subgroups of classical groups. Yet some other consequences of CT are Liebeck's Orbit Size Theorems [Li2] characterizing certain classical groups by their nontransitive projective actions in terms of orbit sizes. In their 1979 paper [CKa], without using CT, Cameron and Kantor proved their theorems characterizing certain classical groups of dimension at least three by their transitive projective actions. For the two-dimensional situation we have the Zassenhaus-Feit-Suzuki Theorem [Z01], [Fei], [Suz] characterizing doubly transitive permutation groups in which only the identity fixes three points. In his Rank 3 Theorem, without using CT, Kantor [Ka1] proved that if the subdegrees of a Rank 3 permutation group coincide with the subdegrees of a "polar geometry" (symplectic or unitary or orthogonal), then it is a group of automorphisms of such a geometry. Kantor deduced this from the

Buekenhout-Shult characterization of polar spaces [BSh], which in turn is based on the work of Tits on spherical buildings [Tit].

Clearly for any $n > 0$ the symmetric group S_n is n-transitive, and for any $n > 2$ the alternating group A_n is $(n-2)$-transitive. It was a spectacular consequence of CDT, and hence of CT, that other than the alternating and symmetric groups, the four Mathieu groups $M_{11}, M_{12}, M_{23}, M_{24}$ are the only 4-transitive permutation groups.

Section 14: Throwing away roots

One of the basic tools which links up the RTG = the Recognition Theorems of Group theory with the calculation of Galois groups and which was initiated in my 1992 paper [A17] is the MTR = the Method of Throwing away Roots. To explain this, first note that, for any field K, the polynomial

$$F(Y) = Y^n + \sum_{1 \le i \le n} a_i Y^{n-i} \in K[Y]$$

with $a_i \in K$ is irreducible in $K[Y]$ iff its Galois group $G = \mathrm{Gal}(F, K) < S_n$ is transitive, where S_n is the symmetric group on its roots $\alpha = \alpha_1, \ldots, \alpha_n$. Now the point stabilizer G_α of G may be regarded as a subgroup of the symmetric group S_{n-1} on $\alpha_2, \ldots, \alpha_n$, and then G is 2-transitive iff G_α is transitive. This suggests that we should throw away a root, say α, of F to get its "naive" derivative

$$F'(Y) = \frac{F(Y)}{Y - \alpha} = \frac{F(Y) - F(\alpha)}{Y - \alpha} \in K(\alpha)[Y]$$

which, not to confuse it with the usual derivative, may be called the "twisted" derivative. Thus G is 2-transitive iff F and F' are both irreducible, where the irreducibility of F' is in $K(\alpha)[Y]$. Moreover, assuming F to be irreducible in $K[Y]$, the rank of G is one plus the number of irreducible factors of $F'(Y)$ in $K(\alpha)[Y]$, and their degrees are the subdegrees of G except for the subdegree 1 belonging to the linear factor we threw away. So when F' is irreducible we may use CDT, and when F' has two factors we may use CR3. In the former case we may even be able to use the Jordan-Marggraff Theorems on Limits of Transitivity, or Burnside's Theorem, or the Zassenhaus-Feit-Suzuki Theorem, or Cameron-Kantor's Theorems on Transitive Collineation Groups. For instance, as I have shown in my recent 1997 paper [A30], Burnside's Theorem is sufficient to prove the unsolvability of the surface covering $Y^{p+1} + XY + Z$ considered in my 1955 paper [A01], and this in turn settles the two-variable case of Hilbert's 13th problem [Hi1], [Hi2] by giving an example of an algebraic function of two variables which cannot be expressed as a composition of algebraic functions of one variable. In the latter case we may be able to use Kantor's Rank 3 Theorem. When in 1989 I was busily using CDT to calculate Galois groups, Kantor visited me in Purdue and said, "Why are you interested only in doubly transitive groups? Here is a remarkable theorem about Rank 3 groups," and he wrote on my blackboard his Rank 3 Theorem. It took me almost five years of meditation on his suggestion to start effectively using it.

The preamble to Kantor's theorem is the fact that the transitive action of the symplectic, unitary, and orthogonal groups on their singular projective hyperquadrics, that is where the corresponding forms vanish, is of Rank 3. Kantor's theorem says that the subdegrees of these Rank 3 actions determine the forms. This he proves by applying Sylow theory to the Buekenhout-Shult characterization of polar spaces from their paper [BSh]. Roughly speaking, the said characterization asserts that a hyperquadric is determined by knowing the points and lines on it and knowing that they satisfy the one or all axioms. According to this axiom, given any line λ on the hyperquadric and any point π not on λ, either all the lines joining π to various points of λ are on the hyperquadric or this is so for exactly one point of λ. This characterization was a tremendous simplification over the characterization contained in Tits' Springer Lecture Notes [Tit] on spherical buildings. Tits' characterization itself was a simplification of the original characterization of hyperquadrics given in Veldkamp's 1959 papers [Vel]. This brings me to what I said in my discursive Tata Institute paper [A23] pointing out that even a great man like Zariski can be wrong once. I was referring to the assertion which he made to me at the end of his projective geometry course that projective geometry was a beautiful but dead subject and that it was not worth doing research in it. As I have just pointed out, projective geometry had a robust rebirth around 1960.

Actually, there is a situation when factorization is useful for Galois group computation even when F is not irreducible. That is so when a priori we know that the Galois group of F is a subgroup of $\mathrm{PGL}(m,q)$ and we are ready to use Liebeck's Orbit Size Theorems. To explain this, assume that K contains the Galois field $\mathrm{GF}(q)$ where $q>1$ is a power of a prime p, and for some integer $m>0$ we have $n=\langle m-1\rangle$ and $a_i=0$ whenever i is not of the form $\langle m-j-1\rangle$ with $1\le j\le m$, where we are using the abbreviation

$$\langle l\rangle = 1+q+\cdots+q^l$$

with the understanding that $\langle -1\rangle=0$. We then call F a projective q-polynomial of q-degree m over K. Also assume that $a_m\neq 0$; i.e., F is separable. In [A21] and [A29] I have shown that then in a natural manner $\mathrm{Gal}(F,K)<\mathrm{PGL}(m,q)$. This is deduced by vectorizing F to get

$$E(Y)=YF(Y^{q-1})=Y^{q^n}+\sum_{1\le i\le m} b_iY^{q^{m-i}}$$

with $b_i\in K$ and $b_m\neq 0$, which we call a separable vectorial q-polynomial of q-degree m over K, and noting that then $\mathrm{Gal}(E,K)<\mathrm{GL}(m,q)$ and $\mathrm{Gal}(E,K)$ maps onto $\mathrm{Gal}(F,K)$ under the canonical epimorphism of $\mathrm{GL}(m,q)$ onto $\mathrm{PGL}(m,q)$. Note that for the projectivization F of E we have

$$F(Y)=Y^{\langle m-1\rangle}+\sum_{1\le i\le m} b_iY^{\langle m-i-1\rangle}$$

with $b_i\in K$ and $b_m\neq 0$. Again, to make history interesting, the evolution from the covering $Y^{p+1}+XY+Z$ considered in [A01] to the general projective polynomial F displayed above can be explained by saying that first I changed the exponent of Y from $p+1$ to $q+1$; then changed the "polynomial" $q+1$ to the "power series" $1+q$, which by adding more terms could be generalized to $1+q+\cdots+q^{m-1}=\langle m-1\rangle$, giving the more general surface $\widehat{F}_m(Y)=Y^{\langle m-1\rangle}+XY+Z$; and then by inserting more similar terms in Y obtained F. The thought process to go from $q+1$ to $\langle m-1\rangle$ took almost four years. At any rate, for the meromorphic series field $\widehat{K}=k(X,Z)$ over an algebraically closed field k of characteristic p, essentially in [A17], by using the Zassenhaus-Feit-Suzuki Theorem, I proved that $\mathrm{Gal}(\widehat{F}_2,\widehat{K})=\mathrm{PGL}(2,q)$; and then essentially in [A21], by using Theorem I from the Cameron-Kantor paper [CKa], I proved that $\mathrm{Gal}(\widehat{F}_m,\widehat{K})=\mathrm{PGL}(m,q)$ for all $m>2$. Moreover, as pointed out in [A28] and [A29], for the rational function field $\widetilde{K} = k(X, Z)$ we have $\mathrm{Gal}(\widehat{F}_m, \widetilde{K}) = \mathrm{PGL}(m, q)$ for all $m > 1$, and for the corresponding vectorial polynomial $\widehat{E}_m(Y) = Y^{q^m} + XY^q + ZY$ we have $\mathrm{Gal}(\widehat{E}_m, \widetilde{K}) = \mathrm{Gal}(\widehat{E}_m, \widehat{K}) = \mathrm{GL}(m, q)$ for all $m > 1$,

It is quite an interesting story how I met Martin Liebeck. On one of my pilgrimages to Manhattan, Kansas, Ernie Shult explained to me how symplectic groups have one projective orbit, unitary groups have two, and orthogonals three. On hearing this I asked whether just as Kantor's Rank 3 Theorem can recognize these three groups from the three subdegrees of their action on the singular hyperquadric, could one recognize the orthogonal groups from their three orbit sizes? To which Ernie said, "Most likely." That year Bill Kantor was in Japan and, having asked him whom I should consult while he was away, told me to talk to his friends Steve Smith of Chicago and Jonathan Hall of Michigan State. So I asked my question of Steve Smith. He proceeded to email it to Martin Liebeck in London, Jan Saxl in Cambridge, and Cheryl Praeger (another student of Peter Neumann) in Perth, Australia. A reply came from Martin that yes, he can show that the orbit sizes do determine the orthogonal groups and also the unitary groups. At my request he published his Orbit Size Theorems in his paper [Li2] as a companion to my paper [A24]. In the meantime I had also visited Michigan State, where Jonathan Hall, being busy as a new chairman, suggested I talk to the young German group theorist Ulrich Meierfrankenfeld. In Ulrich I had acquired a third friendly and kind group theory guru, like Michael O'Nan and Ernie Shult, to whom I could ask obvious (not to me) questions.

Recently, when I was spending a month in London learning group theory from Martin Liebeck, he told me how he and Gary Seitz, in their paper [LSe], used Lang's Theorem to simplify Aschbacher's 1984 paper [As2]. Although I was a junior colleague of Serge Lang in Columbia University, during the two-year period 1955-57, it has taken me forty years to become a fan of his, for as it is said, "For everything there is a season under Heaven." At any rate, Lang's Theorem, which he proved in his 1956 paper [Lan], is a versatile technique for first proving things over the algebraic closure of $\mathrm{GF}(q)$ and then bringing them down to the level of $\mathrm{GF}(q)$. In its most primitive form it says that given any $x \in \mathrm{GL}(m, \overline{q})$ = the group of all nonsingular $m \times m$ matrices over the algebraic closure of $\mathrm{GF}(q)$, we can find $y = (y_{ij}) \in \mathrm{GL}(m, \overline{q})$ such that $x = y^{(q)}y^{-1}$ where $y_{ij}^{(q)} = y_{ij}^q$. Note the resemblance of this with the $(q-1)$-cyclic equation $Y^{q-1} = X$ over $\mathrm{GF}(q)(X)$.

Section 15: Nice equations for nice groups

Returning to a chronological recounting of the story, after getting Serre's letters of 1988 and after retraining myself in group theory, in my 1992 paper [A17] I showed the answers to both of his questions to be the same by proving that for the Galois group $\overline{G}_n = \mathrm{Gal}(\overline{F}_n, k(X))$ of the trinomial $\overline{F}_n(Y) = Y^n + XY^t + 1$ over an algebraically closed field k of characteristic p where n and t are any integers with $0 < n - p = t \not\equiv 0 \bmod p$, we have $\overline{G}_n$ = the alternating group A_n provided $t > 1$ except when $(p, t) = (7, 2)$. This I proved by using MTR + CDT. I also showed that in the exceptional case $\overline{G}_n = A_9$ or $\mathrm{PSL}(2, 8)$ depending on whether a certain six-degree polynomial with coefficients in a hyperelliptic function field over $\mathrm{GF}(7)$ does or does not factor.

Then, as reported in my 1994 paper [A20], after intensively working day and night for four months, I managed to factor the said polynomial and thereby proved that for $(p,t) = (7,2)$ we have $\overline{G}_n = \mathrm{PSL}(2,8)$. As I said in [A20], the deep concentration reached during the factorization gave me the semblance of Savikalpa Samadhi, which is one step lower than Nirvikalpa Samadhi, the ultimate goal of Dhayna Yoga. After giving up this body, the devotees of Shiva go to his abode Kailasa, and similarly the devotees of Vishnu go to his abode Vaikuntha and the devotees of Krishna go to Goloka = the Cow-Heaven. So I may aspire to go to the Factor-Heaven. After all, what is Galois Theory but Group Theory plus Factorization!

Ultimately, from the above proof, in case of $t > 2$, I was able to replace CDT by the Jordan-Marggraff Theorems on limits of transitivity, but in case of $t = 2$, I have not been able to remove CDT, and hence CT, to this day. To do so is a good thesis problem.

The construction of explicit unramified coverings of the affine line for the remaining alternating groups and, in case of $p = 2$, for the symmetric groups was achieved in my papers [A17] and [A19]. In case of $p = 2$, as reported in [AOS], the assistance of my sixth Ph.D. student, Avinash Sathaye, was valuable.

Before tackling the $t > 1$ case, I first gave my own proof of the $t = 1$ case by using the Zassenhaus-Feit-Suzuki Theorem. My proof as well as Serre's original proof served to show that more generally we have $\mathrm{Gal}(Y^{q+1} + XY + 1, k(X)) = \mathrm{PSL}(2,q)$ for any power $q > 1$ of p. Serre described my proof as an ascending proof versus his descending proof. Serre's proof was included in an appendix to my 1992 paper [A17]. After the paper was published Serre found out that his proof was essentially given in Carlitz's 1956 paper [Ca2]. Let me also note that after the factorization yoga of my paper [A20], Serre found a "modular" substitute for it, as he wrote me in letter [Se3], which appeared in the Springer volume of papers presented at my 60th birthday conference, edited by Chandrajit Bajaj.

In studying Volume III of Huppert-Blackburn [HBl], I learnt enough about the Mathieu groups to prove that, as reported in my papers [A18], [A22] together with my joint paper [APS] with Popp-Seiler and my joint papers [AY1], [AY2] with my twenty-first Ph.D. student, Ikkwon Yie, and computing Galois groups over $k(X)$, for $p = 3$ the Galois group of $Y^{11} + XY^2 + 1$ is M_{11} and it is isomorphic with the Galois group of $Y^{12} + Y + X$, verifying the fact that M_{11} has a permutation representation of degree 12, and for $p = 2$ the Galois groups of $Y^{23} + XY^3 + 1$ and $Y^{24} + Y + X$ are M_{23} and M_{24} respectively, with similar explicit polynomials having Galois groups M_{22}, M_{12} and $\mathrm{Aut}(M_{12})$ in case of $p = 2$. Again all these give unramified coverings of the affine line. The M_{24} polynomial was "found" by heuristically integrating the M_{23} polynomial to get $Y^{24} + XY^4 + Y + C$ and putting in it $X = 0$ and $C = X$.

As I have indicated, by first changing the exponent of Y from $q+1$ to $1+q$ and then to $1 + q + \cdots + q^{m-1} = \langle m-1 \rangle$ for any integer $m > 1$, from the polynomial $Y^{q+1} + XY + 1$, in [A21], I obtained the unramified covering of the affine line given by

$$F^*(Y) = Y^{\langle m-1 \rangle} + XY + 1 \quad \text{with} \quad \mathrm{Gal}(F^*, k(X)) = \mathrm{PSL}(m,q),$$

and by taking X from the Y-term to the constant term, I obtained the unramified covering of the once punctured affine line given by

$$F^{**}(Y) = Y^{\langle m-1\rangle} + Y + X \quad \text{with} \quad \mathrm{Gal}(F^{**}, k(X)) = \mathrm{PGL}(m, q).$$

In my paper [A24], by using Liebeck's Orbit Size Theorems from his companion paper [Li2], I showed that if $q = q'^2$ where q' is a power of p, then by "inserting" one term in F^* we get an unramified covering of the affine line given by the quartinomial

$$F^{\dagger}(Y) = Y^{\langle 2m-2\rangle} + X^{q'} Y^{\langle m-1\rangle} + XY^{\langle m-2\rangle} + 1$$
$$\text{with} \quad \mathrm{Gal}(F^{\dagger}, k(X)) = \mathrm{PSU}(2m-1, q')$$

where PSU denotes projective special unitary group. Likewise in my papers [A25] and [A26], by using Kantor's Rank 3 Theorem from his paper [Ka1] and Theorem II from Cameron-Kantor's paper [CKa], I showed that by "inserting" two or three terms in F^* we get unramified coverings of the affine line given by a quintinomial and a sextinomial with Galois groups $\mathrm{PSp}(2m, q)$ and $\mathrm{P}\Omega^-(2m, q)$ respectively, where these denote the projective symplectic group and the projective "negative" orthogonal group, i.e., the one with Witt index $m-1$; the one with Witt index m may be called "positive."

It is amazing that all the above nice equations are special cases of the explicit equations giving unramified coverings of the affine line which, by divine guidance aided by experience with singularities, I wrote down in my 1957 paper [A05].

Section 16: Nephews and nieces

Then as a pleasant finale, in their brilliant 1994 papers [Ray] and [Ha1], Michel Raynaud and David Harbater proved the Affine Line Conjecture and Affine Curve Conjecture respectively. Since their proofs are existential, it seems worthwhile to march on with the project of finding explicit nice equations for nice groups, especially because this contributes to the following conjecture which I made in my 1995 paper [A22] and repeated in my 1999 paper [A33] and which says that for any power $q > 1$ of the prime characteristic p we have:

Affine Arithmetical Conjecture. $\pi_A(L_{GF(q)}) = Q_1(p)$.

This is based on the philosophy that going from an algebraically closed ground field to a finite field is like adding a branch point, and so $\pi_A(L_{\mathrm{GF}(q)})$ should equal $\pi_A(L_{k,1})$ where k is an algebraically closed field of characteristic p.

Here is another conjecture which I communicated to Harbater some years ago and which follows the philosophy that, in characteristic p, whatever could happen should happen (provided there is enough room).

Affine Inertia Conjecture. *Let G be a quasi-p group together with a subgroup H such that H and its conjugates generate G, and H has a normal p-Sylow subgroup P with cyclic quotient H/P. Then there exists an unramified covering of the affine line L_k with Galois group G such that H is the inertia group at some point above the point at infinity.*

Since Mike Artin and I were both students of Zariski, we are gurubandhus, where bandhu is brother in Sanskrit. Harbater, being a student of Artin, is my nephew. For the same reason Caroline Melles, who encouraged me to write this historical essay, is my niece. Again, Kate Stevenson, who has contributed to the Affine Arithmetical Conjecture in her joint paper [GSt] with Bob Guralnick, and Rachel Pries, who has contributed to the Affine Inertia Conjecture in her paper

[Pri], being students of Harbater, are my grandnieces. Once again, what a small or nice world!

Somewhat stretching the genealogy, Mike Artin's father, Emil Artin, being Zariski's friend, was supposed to have become my mathematical uncle (= post-doctoral mentor) when, as suggested by him and Zariski, I was in 1958-59 working for a year in Princeton; however, before I arrived, Artin returned to Germany. Likewise, Claude Chevalley, another friend of Zariski, was supposed to have become my mathematical uncle when, at his invitation, in 1955 I accepted a job in Columbia, but he returned to France before I arrived. Many years later, when my father passed away, I found among his correspondence a letter which Zariski wrote to him in 1954 saying, "Your son has solved a problem which both Chevalley and I had unsuccessfully worked on."

Originally I came to the Affine Arithmetical Conjecture when, influenced by Mike Fried's frequent comments, I started 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 started calculating the arithmetic monodromy groups in addition to the geometric monodromy groups. As reported in my papers [A33] and [A34], it turned out that then the linear and symplectic groups got enlarged to their semilinear incarnations. For instance $\mathrm{PGL}(m,q)$ got enlarged to $\mathrm{P\Gamma L}(m,q) = \Gamma\mathrm{L}(m,q)/(\text{scalar matrices})$ where $\Gamma\mathrm{L}(m,q)$ may be defined to be the semidirect product of $\mathrm{Aut}(\mathrm{GF}(q))$ and $\mathrm{GL}(m,q)$ with the componentwise action of the former on the latter.

In my 1996 paper [A27] I revisited the factorizations which I had developed in establishing the symplectic, unitary, and orthogonal group coverings and, at the end of that paper, codified them into a mantra.

By using this mantra, in my joint papers [AL1], [AL2] with my twenty-fourth Ph.D. student, Paul Loomis, more evidence towards the Affine Arithmetical Conjecture is provided by showing that the Galois group calculations of the symplectic polynomials remain valid if the assumption of the ground field being algebraically closed is replaced by the weaker assumption that it contains $\mathrm{GF}(q)$. Again by using the mantra, it is also shown that by deforming those polynomials their Galois groups are enlarged from the isometry groups $\mathrm{PSp}(2m,q)$ to the similitude groups $\mathrm{PGSp}(2m,q)$; note that a similitude is a linear transformation which may magnify the form instead of leaving it unchanged as in an isometry.

The evidence gathered so far supports more the following variation of the Affine Arithmetical Conjecture where, for any field κ, by $\pi_A(L_{\kappa,\infty})$, we denote the algebraic fundamental group of L_κ minus all of its points, i.e., the set of all finite Galois groups of finite Galois extensions of $\kappa(X)$ without any ramification condition.

Total Arithmetical Conjecture. $\pi_A(L_{GF(q),\infty})$ = *the set of all finite groups.*

Section 17: Permutation polynomials and genus zero coverings

The calculation of the Galois groups of the polynomials considered so far was facilitated by the fact that they are genus zero over the algebraically closed ground field k of characteristic p in the sense that they are of the form $h(Y) + X\widehat{h}(Y)$ with $0 \neq h(Y) \in k[Y]$ and $0 \neq \widehat{h}(Y) \in k[Y]$, and hence can be "solved" for X. Thus, for instance, the polynomial F^* is genus zero over k. Some of our polynomials, such as F^{**}, are actually strong genus zero over k in the sense that they are of the form $h(Y)+X$, but these tend to give unramified coverings of $L_{k,1}$ rather than L_k, which explains why most of our polynomials were genus zero but not strong genus zero. Actually the unitary polynomial $F^{\dagger}$ is not genus zero over k, but it is almost genus zero over k in the sense that some irreducible factor of it is genus zero over k and has the same splitting field over $k(X)$ as $F^{\dagger}$. Similarly, the orthogonal polynomial is also weak genus zero, whereas the symplectic polynomial is actually genus zero. Likewise some polynomials could be almost strong genus zero in an obvious sense.

Recently I was able to grow certain PPs (=Permutation Polynomials) and EPs (=Exceptional Polynomials) into odd dimensional orthogonal group coverings. To explain this, recall that, for a power $q^* > 1$ of p, a univariate polynomial $h(Y)$ with coefficients in $\mathrm{GF}(q^*)$ is said to be a PP over $\mathrm{GF}(q^*)$ if the map $\mathrm{GF}(q^*) \to \mathrm{GF}(q^*)$ given by $c \mapsto h(c)$ is bijective. Moreover, $h(Y)$ is said to be an EP over $\mathrm{GF}(q^*)$ if every irreducible factor of the bivariate polynomial $[h(Y) - h(Z)]/(Y - Z)$ in $\mathrm{GF}(q^*)[Y, Z]$ is reducible in $\mathrm{GF}(\overline{p})[Y, Z]$ where $\mathrm{GF}(\overline{p})$ is the algebraic closure of $\mathrm{GF}(p)$. Clearly $[h(Y) - h(Z)]/(Y - Z)$ is the twisted derivative of $h(Y) + X$. Now it is a basic fact (see Fried [Fri]) that a separable $h(Y)$, i.e., $h(Y) \in \mathrm{GF}(q^*)[Y] \setminus \mathrm{GF}(q^*)[Y^p]$, is an EP over $\mathrm{GF}(q^*)$ iff it is a PP over $\mathrm{GF}(q^{**})$ for infinitely many different powers q^{**} of q^*. Since the compositions of EPs are themselves EPs, it suffices to study indecomposable EPs. The search for PP's goes back at least to Dickson's thesis of 1897, which was essentially included in his 1901 book [Dic]. Spurred on by the Carlitz Conjecture of 1966, it culminated in the 1993 seminal paper [FGS] of Fried-Guralnick-Saxl, where it was settled affirmatively by invoking CT. In 1993 Wan [Wan] put forward a stronger version of the Carlitz conjecture which was settled by Lenstra [Len] in 1995 without using CT. The Carlitz Conjecture says that, assuming $p \neq 2$, the degree of any indecomposable EP over $\mathrm{GF}(q^*)$ is necessarily odd. The Wan Conjecture says that, without any assumption on p, for the degree n of any indecomposable EP over $\mathrm{GF}(q^*)$ we must have $\mathrm{GCD}(n, q^* - 1) = 1$.

Again let $q > 1$ be a power of p, let $m > 0$ be an integer, and recall that an affine group is a subgroup of the semidirect product of $\mathrm{GL}(m, q)$ acting on $\mathrm{GF}(q)^m$, and hence its degree is a power of p. In the Fried-Guralnick-Saxl paper [FGS] it was shown that except when $p = 2$ or 3 the Galois group of an indecomposable EP must be an affine group. This was rounded off by the discovery of the MCM and LZ polynomials, by which we respectively mean the $p = 2$ family of EPs of degree $q(q-1)/2$ found by Mueller-Cohen-Matthews [Mue], [CMa] in 1994 and the $p = 3$ family of EPs of degree $q(q - 1)/2$ found by Lenstra-Zieve [LZi] in 1996; both of these have $\mathrm{PSL}(2, q)$ as Galois group over $k(X)$. In the direction of pure Galois Theory the results of the FGS paper were extended by Guralnick-Saxl in their follow-up guiding-light paper [GSa] of 1995 in which they studied the Galois groups of $h(Y) + X$ for an arbitrary univariate polynomial $h(Y)$ over $k(X)$. In particular, in Theorem 3.1(B) on page 131 of the Guralnick-Saxl paper [GSa] there is a list of all the possible classical groups which may occur as Galois groups of $h(Y) + X$, i.e., of strong genus zero equations over k. Amazingly, this list is exactly complimentary to the list of classical Galois groups of nice equations which I had found and, as noted above, all of which are almost genus zero over k. Actually this is not so surprising, because I was usually looking for unramified coverings of L_k rather than $L_{k,1}$.

In greater detail, the list of classical groups I had found consisted of symplectic groups, odd dimensional unitary groups, and even dimensional "negative" orthogonal groups, whereas the Guralnick-Saxl list consists of even dimensional unitary groups, even dimensional "positive" orthogonal groups, and odd dimensional orthogonal groups.

As partly reported in [A27], I was able to grow the MCM and LZ polynomials into strong genus zero coverings with odd dimensional orthogonal groups as Galois groups. Similarly, I was able to grow some Dickson polynomials into strong genus zero coverings with even dimensional "positive" orthogonal groups as Galois groups; for the two-dimensional case of this together with an introduction to Dickson polynomials see my joint paper [ACZ] with Steve Cohen and Mike Zieve. For even dimensional unitary groups I am preparing a joint paper with Nick Inglis.

In his forthcoming paper [Gur], Bob Guralnick has put forward an exciting new conjecture, which supports my experience with genus zero coverings and which says that except for a finite number of simple groups, the composition factors of the Galois groups of (almost) genus zero coverings over k are either cyclic, alternating, or Lie-type in the same characteristic p as k.

Section 18: Higher dimensional algebraic fundamental groups

Turning to varieties of dimension $d > 1$ over an algebraically closed ground field k of characteristic p, for any integer $t \geq 0$ let $P_t(p)$ be the set of all (p,t)-groups, i.e., finite groups G such that $G/p(G)$ is an abelian group generated by t generators. Note then that for $t \leq 1$ we have $P_t(p) = Q_t(p)$, but for $t > 1$ the set $P_t(p)$ is much smaller than the set $Q_t(p)$.

The following conjectures which were implicit in my 1955 paper [A05] and my 1959-60 papers [A06] respectively were made explicit in my 1997 paper [A28].

Normal Crossings Local Conjecture. $\pi_A^L(N_{k,t}^d) = P_t(p)$ *for* $d > 1$ *and* $t > 0$.

Normal Crossings Global Conjecture. $\pi_A(L_{k,t}^d) = P_t(p)$ *for* $d > 1$ *and* $t \geq 0$.

In the Local Conjecture, $N_{k,t}^d$ represents a neighborhood of a simple point on a d-dimensional algebraic variety over k from which we have deleted a divisor having a t-fold normal crossing at the simple point, and $\pi_A^L(N_{k,t}^d)$ is the corresponding algebraic local fundamental group, by which we mean the set of all Galois groups of finite unramified local Galois coverings of $N_{k,t}^d$. Algebraically speaking, let R be the formal power series ring $k[[X_1, \dots, X_d]]$, let I be the quotient field $k((X_1, \dots, X_d))$ of R, let $\widehat{\Omega}$ be the set of all finite Galois extensions of I in a fixed algebraic closure of I, and let Ω be the set of all $J \in \widehat{\Omega}$ such that $X_1R, \dots, X_tR$ are the only height-one primes in R which are possibly ramified in J. We may now identify $\pi_A^L(N_{k,t}^d)$ with the set of all Galois groups $\mathrm{Gal}(J, I)$ with J varying in Ω. In the 1955 paper [A01] I proved the inclusion $\pi_A^L(N_{k,t}^d) \subset P_t(p)$, and by examples showed that $\pi_A^L(N_{k,t}^d)$ contains unsolvable groups. By refining these examples, in [A28] and [A29] I showed that, for any integer $m > 1$ and any power $q > 1$ of p, upon letting $\widetilde{K}_d = k(X, Z, X_3, \dots, X_d)$ and $\widehat{K}_d = k((X, Z, X_3, \dots, X_d))$ with $\langle m-1 \rangle = 1 + q + \dots + q^{m-1}$, for the projective polynomial $\widehat{F}_m(Y) = Y^{\langle m-1 \rangle} + XY + Z$ and its vectorization $\widehat{E}_m(Y) = Y^{q^m} + XY^q + ZY$, we have $\mathrm{Gal}(\widehat{F}_m, \widetilde{K}_d) = \mathrm{Gal}(\widehat{F}_m, \widehat{K}_d) = \mathrm{PGL}(m, q)$ and $\mathrm{Gal}(\widehat{E}_m, \widetilde{K}_d) = \mathrm{Gal}(\widehat{E}_m, \widehat{K}_d) = \mathrm{GL}(m, q)$. It follows that $\pi_A^L(N_{k,t}^d)$ contains $\mathrm{PGL}(m, q)$ and $\mathrm{GL}(m, q)$ for every integer $m > 1$ and every power $q > 1$ of p.

In the Global Conjecture, $L_{k,t}^d$ represents the d-dimensional affine space L_k^d over k from which we have deleted t hyperplanes $H_1, \dots, H_t$ which together with the hyperplane at infinity have only normal crossings, and $\pi_A(L^d_{k,t})$ is the set of all finite Galois groups of unramified coverings of $L^d_{k,t}$. Again, in the 1959-60 papers [A06] I proved the inclusion $\pi_A(L^d_{k,t}) \subset P_t(p)$, and the above projective and vectorial polynomials show that $\pi_A(L^d_{k,t})$ contains $\mathrm{PGL}(m,q)$ and $\mathrm{GL}(m,q)$ for every integer $m > 1$ and every power $q > 1$ of p. In [A28] the Global Conjecture is generalized by replacing hyperplanes by hypersurfaces, and also a Local-Global Conjecture is formulated.

In a recent discussion, David Harbater has raised the question whether all the members of $\pi^L_A(N^d_{k,t})$ as well as $\pi_A(L^d_{k,t})$ actually belong 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 coverings. To review the standard terminology used below, Z_n is the cyclic group of order n, and $Z(A)$ is the center of a group A; i.e., $Z(A)$ is the set of all elements of A which commute with every element of A. For any groups A and B with $Z(A) = Z(B) = Z_2 = \{1, i\}$, the central product $A * B$ of A and B is the quotient of their direct product $A \times B$ by the normal subgroup $\{(1,1), (i,i)\}$ of order 2. Finally, for any groups A and B, by an A-extension of B we mean a group C together with an exact sequence $1 \to A \to C \to B \to 1$; this extension is split means some subgroup of C maps isomorphically onto B, and central means the image of A in C is $Z(C)$.

The first set of Stroth groups G are for $p = 3$, and they are $G = A * \mathrm{GL}(2,3)$, where A 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 $G = B * \mathrm{GL}(3,4)$ where B is an extra-special group of order 27; i.e., B is a nonsplit central Z_3 extension of Z_3^2 with $Z(B) = Z_3$; note that there are two versions of B, 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 $\mathrm{GL}^\flat(3,4)$.

I would like to assign as a thesis problem determining whether $Q_8 * \mathrm{GL}(2,3)$ belongs to $\pi^L_A(N^3_{k,3})$ for $p = 3$.

As an aid to the above problem, in the paper [A35] I have obtained an Embedding Criterion. To explain this, recall that a GEP (= Galois Embedding Problem) is a (finite) Galois extension K'/K together with an epimorphism $r : G'' \to G'$ of finite groups and an isomorphism $r' : G' \to \mathrm{Gal}(K', K)$. A solution to this GEP is a Galois extension K''/K together with an isomorphism $r'' : G'' \to \mathrm{Gal}(K'', K)$ such that K'' is an overfield of K' and the diagram commutes, i.e., $r'r = sr''$ where $s : \mathrm{Gal}(K'', K) \to \mathrm{Gal}(K', K)$ is the Galois theoretic epimorphism. Then the Embedding Criterion proved in [A35] says that the GEP with the canonical epimorphism $r : \mathrm{GL}(m,q) = G'' \to G' = \mathrm{PGL}(m,q)$, where m is divisible by $q-1$ and $\mathrm{GF}(q) \subset K$, has a solution iff K'/K is the splitting field of a separable projective q-polynomial of q-degree m over K. This I deduced from the Polynomial

Theorem, which I proved in [A35] and which says that if K''/K is a Galois extension where K is an overfield of $\mathrm{GF}(q)$ having at least q^m elements, then $\mathrm{Gal}(K'', K)$ is abstractly isomorphic to a subgroup of $\mathrm{GL}(m, q)$ iff K''/K is the splitting field of a separable vectorial q-polynomial of q-degree m over K.

When, while proving the above Embedding Criterion, I did not know whether the diagram commuted, Michael Aschbacher very kindly helped out to make it commute by showing that every automorphism of PGL lifts to an automorphism of GL. The main lesson I learnt in doing this lifting is the importance of transvections, which are the basis-free incarnations of elementary row and column operations of basic matrix theory.

Section 19: Generalized iteration and modular Galois descent

Let $m > 0$ be any integer, let $q = p^u > 1$ be any power of a prime p, and let us consider the generic vectorial q-polynomial

$$E^\sharp(Y) = Y^{q^m} + \sum_{1 \le i \le m} X_i Y^{q^{m-i}}$$

of q-degree m over $K^\sharp = k_q(X_1, \dots, X_m)$ where $X_1, \dots, X_m$ are indeterminates over a field k_q of characteristic p which we assume contains $\mathrm{GF}(q)$. Now, as proved by E. H. Moore in his path-breaking 1896 paper [Moo], $\mathrm{Gal}(E^\sharp, K^\sharp) = \mathrm{GL}(m, q)$; for a very short elementary proof of this see my 1999 paper [A34]. However, as shown in [A34], if we do not assume that k_q contains $\mathrm{GF}(q)$, then the Galois group gets bloated towards $\Gamma\mathrm{L}(m, q)$; and in fact if k_q coincides with $\mathrm{GF}(p)$, then the Galois group coincides with $\Gamma\mathrm{L}(m, q)$. Thus, referring to the Total Arithmetical Conjecture, although we succeed in showing that $\Gamma\mathrm{L}(m, q)$ belongs to $\pi_A(L_{\mathrm{GF}(p),\infty})$, we lose $\mathrm{GL}(m, q)$. So we want to find a method of descending from $\mathrm{GF}(q)$ to $\mathrm{GF}(p)$. More generally, given any integer $n > 0$, we shall try to descend from $\mathrm{GF}(q^n)$ to $\mathrm{GF}(q)$, which amounts to ascending from $\mathrm{GF}(q)$ to $\mathrm{GF}(q^n)$. As we shall explain in a moment, we do this by introducing Generalized Iteration. The fact that the Total Arithmetical Conjecture deals with coefficients in the one variable polynomial ring $k_q[X]$, whereas here we are working with the many variable polynomial ring $k_q[X_1, \dots, X_m]$, can be taken care of by invoking Hilbert Irreducibility, as explained in Helmut Voelklein's new book [Vo3], to specialize to one variable.

A similar situation prevails for the Affine Arithmetical Conjecture vis-a-vis the vectorization $E^{**}(Y) = Y^{q^m} + Y^q + XY$ of the projective trinomial $F^{**}(Y) = Y^{\langle m-1 \rangle} + Y^q + XY$; namely, as I have shown in [A33], we have $\mathrm{Gal}(E^{**}, k_q(X)) = \mathrm{GL}(m, q)$ and $\mathrm{Gal}(E^{**}, \mathrm{GF}(p)(X)) = \Gamma\mathrm{L}(m, q)$. Since this gives an unramified covering of the once punctured affine line rather than the affine line itself, we should really be working with the vectorization of the projective trinomial $F^*(Y) = Y^{\langle m-1 \rangle} + XY^q + Y$, for the details of which see [A33].

The idea of Generalized Iteration came out of Carlitz's explicit class theory [Ca1] (for a modern version see Hayes [Hay]), which was revived by Drinfeld [Dri]; my Drinfeld Module Theory gurus have been Gekeler [Gek], Goss [Gos] and Thakur [Tha], and I spent several weeks visiting them in Saarbrücken, Ohio State and Arizona respectively. To explain it, let K be any overfield of $\mathrm{GF}(q)$, and let

$$E(Y) = Y^{q^n} + \sum_{1 \le i \le m} b_i Y^{q^{m-i}}$$

with $b_i \in K$ and $b_m \neq 0$ be any separable monic vectorial q-polynomial of q-degree m over K. For every nonnegative integer j we inductively define the (ordinary) j-th iterate $E^{[[j]]}$ of E by putting $E^{[[0]]} = E^{[[0]]}(Y) = Y$, $E^{[[1]]} = E^{[[1]]}(Y) = E(Y)$, and $E^{[[j]]} = E^{[[j]]}(Y) = E(E^{[[j-1]]}(Y))$ for all $j > 1$. Next we define the generalized r-th iterate $E^{[r]}$ of E for any $r = r(T) = \sum r_i T^i \in K[T]$ with $r_i \in K$ (and $r_i = 0$ for all except a finite number of i), where T is an indeterminate, by putting $E^{[r]} = E^{[r]}(Y) = \sum r_i E^{[[i]]}(Y)$. Note that for the Y-derivative $E^{[r]}_Y(Y)$ of $E^{[r]}(Y)$ we clearly have $E^{[r]}_Y(Y) = E^{[r]}_Y(0) = r(b_m)$, and hence if $r(b_m) \neq 0$, then $E^{[r]}$ is a separable vectorial q-polynomial over K whose q-degree in Y equals m times the T-degree of r. Now let us fix

$$s = s(T) \in \mathrm{GF}(q)[T] \text{ of } T\text{-degree } n \text{ with } s(X_m) \neq 0$$

and note that then $E^{[s]}$ is a separable vectorial q-polynomial of q-degree mn in Y over K. Let $\mathrm{GF}(q,s)$ be the zero dimensional local ring $\mathrm{GF}(q)[T]/s(T)\mathrm{GF}(q)[T]$, and let $\mathrm{GL}(m,q,s)$ be the group of all invertible $m \times m$ matrices over $\mathrm{GF}(q,s)$. Note that if s is irreducible in $\mathrm{GF}(q)[T]$, then $\mathrm{GL}(m,q,s)$ is isomorphic to $\mathrm{GL}(m,q^n)$. In [A34] I made the following:

Generalized Iteration Conjecture. $Gal(E^{\sharp[s]}, K^\sharp) = GL(m,q,s)$.

Carlitz [Ca1] proved this for $m = 1$, and in my joint paper [AS1] with my twenty-third Ph.D. student, Ganesh Sundaram, it was proved for $s = T^n$. Assuming s to be irreducible in $\mathrm{GF}(q)[T]$ and recalling that $q = p^u$, in my forthcoming joint paper [AS2] with Ganesh it is proved when m is square-free with $\mathrm{GCD}(m,n) = 1$ and $\mathrm{GCD}(mnu, 2p) = 1$. This proof uses CPT = Classification of Projectively Transitive Permutation Groups, whose foundation is Burnside's Theorem; it also uses the Carlitz case, as well as the Singer Cycle Lemma, which implies that the determinant of any Singer Cycle, i.e., a matrix of order $q^m - 1$ in $\mathrm{GL}(m,q)$, is an element of order $q-1$ in $\mathrm{GF}(q)$. In my forthcoming paper [A37] I have extended this proof when the last hypothesis is replaced by the weaker hypothesis that $\mathrm{GCD}(m,p) = 1$. In another forthcoming paper [A36] I have proved the case when $m = n = 2$. Likewise, in my forthcoming paper [AKe] with my twentieth Ph.D. student, Pradipkumar Keskar, I have proved the case when $n < m$ and $\mathrm{GCD}(m,n) = 1$.

When Serre told me that his proof of the Galois group of $Y^{q+1} + XY + 1$ being $\mathrm{PSL}(2,q)$ included in an appendix of my paper [A17] was essentially Carlitz's 1956 proof [Ca2], I thought that was my first encounter with Carlitz. Then I remembered that a Binomial Lemma in my resolution proof of arithmetical surfaces turned out to be related to some Binomial Identities proved by Carlitz in the thirties, as was pointed out to me by my Purdue colleague Michael Drazin. Counting the Carlitz Conjecture incidence to be the third, the present one becomes my fourth encounter with the great Carlitz, who wrote more than 700 papers and who passed away a few months ago at the ripe old age of 92.

In my various trips to Cambridge and Florida, John Thompson has been very helpful in patiently explaining to me the mysteries of Singer Cycles, Burnside's Theorem, CPT, and other group theory folklore which I needed to use. Eventually I may aspire to enter the rarefied atmosphere of his [Th1], [Th2], as well as Matzat-Malle's [MMa] and Voelklein's [Vo1], [Vo2], characteristic zero Galois theory work. I hope to do so by "lifting" some of my equations from characteristic p to characteristic zero. Indeed that is why I have called some of them E to remind us of elliptic curves and more generally of abelian varieties; in turn, $E^{[s]}$ should remind us of s-division points of abelian varieties, since in the theory of Generalized Iteration I am trying to mimic Serre's characteristic zero work [Se1] on division points of elliptic curves and his unpublished generalization of it [Se2] to abelian varieties. My joint paper [ACZ] with Cohen and Zieve may be viewed as a small beginning of the lifting project.

By now it should be abundantly clear that my own personal interest and pleasure is in finding explicit nice equations with prescribed Galois groups, which I can hold in my hand, rather than in simply saying that "there exist" such and such coverings or whatever. The trouble with that is the lack of such an abstract concept of "there" in my Indian background or, if you prefer, in my child-like high-school or grade-school mind. I want to know "where" does it (or does it not) exist? Though of course, with great respect, I bow my head to the abstract existential work of my superiors.

Section 20: Acknowledgments

My thanks are due to Chris Christensen, Caroline Melles and Ruth Michler for providing me with notes of my lectures on which this paper is based and to my dear wife, Yvonne Abhyankar, for the great help she has given me in converting them into a readable narrative.

References

[A01] S. S. Abhyankar, *On the ramification of algebraic functions*, American Journal of Mathematics **77** (1955), 572-592. MR **17:**193c

[A02] S. S. Abhyankar, *Local uniformization on algebraic surfaces over ground fields of characteristic* $p \neq 0$, Annals of Mathematics **63** (1956), 491-526. MR **17:**1134d

[A03] S. S. Abhyankar, *On the valuations centered in a local domain*, American Journal of Mathematics **78** (1956), 321-348. MR **18:**556b

[A04] S. S. Abhyankar, *Simultaneous resolution for algebraic surfaces*, American Journal of Mathematics **78** (1956), 761-790. MR **18:**600b

[A05] S. S. Abhyankar, *Coverings of algebraic curves*, American Journal of Mathematics **79** (1957), 825-856. MR **20:**872

[A06] S. S. Abhyankar, *Tame coverings and fundamental groups of algebraic varieties I - VI*, American Journal of Mathematics **81–82** (1959-1960), 46-94 of vol 81, and 120-190 and 341-338 of vol 82. MR **21:**3428; MR **22:**1574; MR **22:**1575; MR **22:**1576

[A07] S. S. Abhyankar, *Resolution of singularities of arithmetical surfaces*, Purdue Conference on Arithmetical Algebraic Geometry, Harper and Row (1965), 111-152. MR **34:**171

[A08] S. S. Abhyankar, *Resolution of Singularities of Embedded Algebraic Surfaces*, Academic Press, 1966. MR **36:**164

[A09] S. S. Abhyankar, *An algorithm on polynomials in one indeterminate with coefficients in a two dimensional regular local domain*, Annali di Mathematica Pura ed applicata **71** (1966), 25-60. MR **34:**7514

[A10] S. S. Abhyankar, *Resolution of singularities of algebraic surfaces*, Algebraic Geometry, Proceedings of the 1968 Bombay International Colloquium at the Tata Institute of Fundamental Research, Oxford University Press (1969), 1-11. MR **41:**1734

[A11] S. S. Abhyankar, *Historical ramblings in algebraic geometry and related algebra*, American Mathematical Monthly **83** (1976), 409-448. MR **53:**5581

[A12] S. S. Abhyankar, *Weighted Expansions for Canonical Desingularization*, Springer Lecture Notes in Mathematics **910** (1982). MR **84m:**14013

[A13] S. S. Abhyankar, *Determinantal loci and enumerative combinatorics of Young tableaux*, Algebraic Geometry and Commutative Algebra in Honor of Masayoshi Nagata, vol. I, Kinokuniya Company Ltd., Tokyo (1987), 1-26. MR **90b:**14063

[A14] S. S. Abhyankar, *Enumerative Combinatorics of Young Tableaux*, Marcel Dekker, 1988. MR **89e:**05011

[A15] S. S. Abhyankar, *Algebraic Geometry For Scientists And Engineers*, American Mathematical Society, 1990. MR **92a:**14001

[A16] S. S. Abhyankar, *Invariant theory and enumerative combinatorics of Young tableaux*, Geometric Invariance in Computer Vision, Edited by J. L. Mundy and A. Zisserman, MIT Press (1992), 45-76. CMP 93:06

[A17] S. S. Abhyankar, *Galois theory on the line in nonzero characteristic*, Bulletin of the American Mathematical Society **27** (1992), 68-133. MR **94a:**12004

[A18] S. S. Abhyankar, *Mathieu group coverings in characteristic two*, C. R. Acad. Sci. Paris **316** (1993), 267-271. MR **94g:**14013

[A19] S. S. Abhyankar, *Alternating group coverings of the affine line in characteristic greater than two*, Math. Annalen **296** (1993), 63-68. MR **94e:**14020

[A20] S. S. Abhyankar, *Square-root parameterization of plane curves*, Algebraic Geometry and Its Applications, Papers Presented at the 60th Birthday Conference of Shreeram S. Abhyankar, Edited by C. Bajaj, Springer-Verlag (1994), 19-84. MR **95d:**12004

[A21] S. S. Abhyankar, *Nice equations for nice groups*, Israel Journal of Mathematics **88** (1994), 1-24. MR **96f:**12003

[A22] S. S. Abhyankar, *Mathieu group coverings and linear group coverings*, Contemporary Mathematics **186** (1995), 293-319. MR **97e:**14038

[A23] S. S. Abhyankar, *Fundamental group of the affine line in positive characteristic*, Proceedings of the 1992 International Colloquium on Geometry and Analysis, Tata Institute of Fundamental Research, Bombay (1995), 1-26. MR **97b:**14034

[A24] S. S. Abhyankar, *Again nice equations for nice groups*, Proceedings of the American Mathematical Society **124** (1996), 2967-2976. MR **96m:**12004

[A25] S. S. Abhyankar, *More nice equations for nice groups*, Proceedings of the American Mathematical Society **124** (1996), 2977-2991. MR **96m:**12005

[A26] S. S. Abhyankar, *Further nice equations for nice groups*, Transactions of the American Mathematical Society **348** (1996), 1555-1577. MR **96m:**14021

[A27] S. S. Abhyankar, *Factorizations over finite fields*, Finite Fields and Applications, London Mathematical Society Lecture Notes Series **233** (1996), 1-21. MR **98c:**11130

[A28] S. S. Abhyankar, *Local fundamental groups of algebraic varieties*, Proceedings of the American Mathematical Society **125** (1997), 1635-1641. MR **97h:**14032

[A29] S. S. Abhyankar, *Projective polynomials*, Proceedings of the American Mathematical Society **125** (1997), 1643-1650. MR **98a:**12001

[A30] S. S. Abhyankar, *Hilbert's thirteenth problem*, Proceedings of the Franco-Belgian Conference in Reims, Société Mathématique de France, Séminaires et Congrès **2** (1997), 1-11. MR **98i:**12003

[A31] S. S. Abhyankar, *Resolution of Singularities of Embedded Algebraic Surfaces*, Second Enlarged Edition containing an Appendix on Analytic Desingularization in Characteristic Zero for Any Dimension, Springer-Verlag, 1998. MR **99c:**14021

[A32] S. S. Abhyankar, *Polynomial expansion*, Proceedings of the American Mathematical Society **126** (1998), 1583-1596. MR **98g:**12003

[A33] S. S. Abhyankar, *Semilinear transformations*, Proceedings of the American Mathematical Society **127** (1999), 2511-2525. MR **2000e:**12009

[A34] S. S. Abhyankar, *Galois theory of semilinear transformations*, Aspects of Galois Theory, London Mathematical Society Lecture Notes Series **256** (1999), 1-37. MR **2000j:**12008

[A35] S. S. Abhyankar, *Galois embeddings for linear groups*, Transactions of The American Mathematical Society **352** (2000), 3881-3912. CMP 2000:14

[A36] S. S. Abhyankar, *Two step descent in modular Galois theory, therorems of Burnside and Caley, and Hilbert's thirteenth problem*, To Appear.

[A37] S. S. Abhyankar, *Desingularizaton and modular Galois theory*, To Appear.

[ACZ] S. S. Abhyankar, S. D. Cohen and M. Zieve, *Bivariate factorization connecting Dickson polynomials and Galois theory*, Transactions of The American Mathematical Society **352** (2000), 2871-2887. MR **2000j:**12003

[AG1] S. S. Abhyankar and S. R. Ghorpade, *Young tableaux and linear independence of standard monomials in multiminors of a multimatrix*, Discrete Mathematics **96** (1991), 1-32. MR **93b:**15033

[AJ1] S. S. Abhyankar and S. B. Joshi, *Generalized codeletion and standard multitableaux*, Canadian Mathematical Society Conference Proceedings **10** (1989), 1-24. MR **91c:**05196

[AJ2] S. S. Abhyankar and S. B. Joshi, *Generalized roinsertive correspondence between multitableaux and multimonomials*, Discrete Mathematics **90** (1991), 111-135. MR **92m:**05202

[AJ3] S. S. Abhyankar and S. B. Joshi, *Generalized rodeletive correspondence between multitableaux and multimonomials*, Discrete Mathematics vol 93 (1991), 1-17. MR **93a:**05129

[AJ4] S. S. Abhyankar and S. B. Joshi, *Generalized coinsertion and standard multitableaux*, Journal of Statistical Planning and Inference **34** (1993), 5-18. MR **94c:**05071

[AKe] S. S. Abhyankar and P. H.Keskar, *Descent principle in modular Galois theory*, To Appear.

[AK1] S. S. Abhyankar and D. M. Kulkarni, *On hilbertian ideals*, Linear Algebra and its Applications **116** (1989), 53-79. MR **90c:**14032

[AK2] S. S. Abhyankar and D. M. Kulkarni, *Bijection between indexed monomials & standard bitableaux*, Discrete Mathematics **79** (1990), 1-48. MR **91c:**05195

[AK3] S. S. Abhyankar and D. M. Kulkarni, *Coinsertion and standard bitableaux*, Discrete Mathematics **85** (1990), 115-166. MR **92d:**05179

[AL1] S. S. Abhyankar and P. A. Loomis, *Once more nice equation for nice groups*, Proceedings of the American Mathematical Society **126** (1998), 1885-1896. MR **98k:**12003

[AL2] S. S. Abhyankar and P. A. Loomis, *Twice more nice equations for nice groups*, Contemporary Mathematics **245** (1999), 63-76. CMP 2000:09

[AOS] S. S. Abhyankar, J. Ou and A. Sathaye, *Alternating group coverings of the affine line for characteristic two*, Discrete Mathematics **133** (1994), 25-46. MR **95h:**14018

[APS] S. S. Abhyankar, H. Popp and W. K. Seiler, *Mathieu group coverings of the affine line*, Duke Math. Jour **68** (1992), 301-311. MR **93j:**14018

[AS1] S. S. Abhyankar and G. S. Sundaram, *Galois theory of Moore-Carlitz-Drinfeld modules*, C. R. Acad. Sci. Paris **325** (1997), 349-353. MR **98g:**11067

[AS2] S. S. Abhyankar and G. S. Sundaram, *Galois groups of generalized iterates of generic vectorial polynomials*, To Appear.

[AY1] S. S. Abhyankar and I. Yie, *Some more Mathieu group coverings in characteristic two*, Proceedings of the American Mathematical Society **122** (1994), 1007-1014. MR **95b:**12007

[AY2] S. S. Abhyankar and I. Yie, *Small Mathieu group coverings in characteristic two*, Proceedings of the American Mathematical Society **123** (1995), 1319-1329. MR **95f:**14050

[Alb] G. Albanese, *Transformazione birazionale di una superficie algebriche in un'altra priva di punti multipli*, Rendiconti della Circolo Matematica de Palermo **48** (1924), 321-332.

[As1] M. Aschbacher, *On the maximal subgroups of the finite classical group*, Inventiones Mathematicae **76** (1984), 469-514. MR **86a:**20054

[As2] M. Aschbacher, *Finite Group Theory*, Cambridge University Press, 1986. MR **89b:**20001; corrected reprint MR **95b:**20002

[Bir] G. Birkhoff, *Lattice Theory*, American Mathematical Society, 1948. MR **10:**673a

[BMa] G. Birkhoff and S. MacLane, *Survey of Modern Algebra*, Macmillan, 1941. MR **3:**99h

[BSh] F. Buekenhout and E. E. Shult, *On the foundations of polar geometry*, Geometriae Dedicata **3** (1974), 155-170. MR **50:**3091

[Bur] W. Burnside, *Theory of groups of finite order*, Cambridge University Press, First Edition 1897, Second Edition 1911.

[BPa] W. S. Burnside and A. W. Panton, *Theory of Equations I–II*, Dublin, Hodges, Figgis and Co., London, 1904.

[Cam] P. J. Cameron, *Finite permutation groups and finite simple groups*, Bulletin of the London Mathematical Society **13** (1981), 1-22. MR **83m:**20008

[CKa] P. J. Cameron and W. M. Kantor, *2-Transitive and antiflag transitive collineation groups of finite projective spaces*, Journal of Algebra **60** (1979), 384-422. MR **81c:**20032

[Ca1] L. Carlitz, *A class of polynomials*, Transactions of the American Mathematical Society **43** (1938), 167-182. CMP 95:18

[Ca2] L. Carlitz, *Resolvents of certain linear groups in a finite field*, Canadian Journal of Mathematics **8** (1956), 568-579. MR **18:**377f

[Car] R. D. Carmichael, *Introduction to the Theory of Groups of Finite Order*, Ginn, Boston, 1937; 1956 reprint. MR **17:**823a

[Cay] A. Cayley, *On the intersection of curves*, Mathematische Annalen **30** (1887), 85-90.

[Che] C. Chevalley, *On the theory of local rings*, Annals of Mathematics **44** (1943), 690-708. MR **5:**171d

[Chr] C. Christensen, *Strong domination/weak factorization of three-dimensional regular local rings I–II*, Journal of Indian Mathematical Society **45-47** (1981-83), 21-47 and 241-250. MR **88a:**14010a; MR **88a:**14010b

[CMa] S. D. Cohen and R. W. Matthews, *A class of exceptional polynomials*, Transactions of the American Mathematical Society **345** (1994), 897-909. MR **95d:**11164

[Coh] I. S. Cohen, *On the structure and ideal theory in complete local rings*, Transactions of the American Mathematical Society **59** (1946). MR **7:**509h

[Cre] L. Cremona, *Elementi di Geometria Projecttiva*, Rome/Turin: G. B. Paravia and Company, 1873.

[Cu1] S. D. Cutkosky, *Local factorization of birational maps*, Advances in Mathematics **132** (1997), 167-315. MR **99c:**14018

[Cu2] S. D. Cutkosky, *Local monomialization and factorization of morphisms*, Asterisque, No. 260 (1999).

[DWe] R. Dedekind and H. Weber, *Theorie der algebraischen functionen einer veränderlichen*, Crelle Journal **92** (1882), 181-290.

[Dic] L. E. Dickson, *Linear Groups*, Teubner, 1901.

[Dri] V. G. Drinfeld, *Elliptic Modules*, Math. Sbornik **94** (1974), 594-627. MR **52:**5580

[Fei] W. Feit, *On a class of doubly transitive permutation groups*, Illinois Journal of Mathematics **4** (1960), 170-186. MR **22:**4784

[For] A. R. Forsyth, *Theory of Functions of a Complex Variable*, Cambridge University Press, London, 1893.

[Fri] M. D. Fried, *On Hilbert's irreducibility theorem*, Journal of Number Theory **6** (1974), 211-231. MR **50:**2117

[FGS] M. D. Fried, R. Guralnick and J. Saxl, *Schur covers and Carlitz's conjecture*, Israel Journal of Mathematics **82** (1993), 157-225. MR **94j:**12007

[Fu1] D. E. Fu, *Local weak simultaneous resolution for high rational ranks*, Journal of Algebra **194** (1997), 614-630. MR **98m:**13005

[Gek] E.-U. Gekeler, *Moduli for Drinfeld modules*, The Arithmetic of Function Fields, eds. D. Goss et al, de Gruyter (1992), 153-170. MR **93m:**11049

[Gor] D. Gorenstein, *Classifying the finite simple groups*, Bulletin of the American Mathematical Society **14** (1986), 1-98. MR **87k:**20001

[Gos] D. Goss, *Basic Structures of Function Field Arithmetic*, Springer-Verlag, 1996. MR **97i:**11062

[Gro] A. Grothendieck, *Eléments de Géométrie Algébrique I–IV*, Publ. Math. IHES, 1960-1967. MR **30:**3885; MR **33:**7330; MR **36:**178; MR **39:**220

[Gur] R.M. Guralnick, *Monodromy groups of covers of small genus in positive characteristic*, To Appear.

[GSa] R. M. Guralnick and J. Saxl, *Monodromy groups of Polynomials*, Groups of Lie Type and Their Geometries (W. M. Kantor and L. Di Marino, eds.), Cambridge University Press (1995), 125-150. MR **96b:**20003

[GSt] R.M. Guralnick and K. F. Stevenson, *Prescribing ramification*, To Appear.

[Ha1] D. Harbater, *Abhyankar's conjecture on Galois groups over curves*, Inventiones Mathematicae **117** (1994), 1-25. MR **95i:**14029

[Har] R. Hartshorne, *Algebraic Geometry*, Springer-Verlag, 1977. MR **57:**3116

[Hay] D. R. Hayes, *Explicit class field theory for rational function fields*, Transactions of the American Mathematical Society **189** (1974), 77-91. MR **48:**8444

[He1] C. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order*, Geometrae Dedicata **2** (1974), 425-560. MR **49:**439

[He2] C. Hering, *Transitive linear groups and linear groups which contain irreducible subgroups of prime order II*, Journal of Algebra **93** (1985), 151-164. MR **86k:**20046

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

[Hi2] D. Hilbert, *Über die Gleichung neunten Grades*, Mathematische Annalen **97** (1927), 243-250.

[Hir] H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic* 0, Annals of Mathematics **79** (1964), 109-326. MR **33:**7333

[HBl] B. Huppert and N. Blackburn, *Finite Groups I, II, III*, Springer-Verlag, New York (1982). MR **84i:**20001a; MR **84i:**20001b

[Jor] C. Jordan, *Traité des Substitutions et des Équatione Algébriques*, Gauthier-Villars, 1870.
[Jun] H. W. E. Jung, *Darstellung der Funktionen eines algebraischen Körpers zweier Veränderlichen x, y in der Umgebung einer Stelle $x = a, y = b$*, Crelle Journal **133** (1908), 289-314.
[Ka1] W. M. Kantor, *Rank 3 characterizations of classical geometries*, Journal of Algebra **36** (1975), 309-313. MR **52:**8229
[Ka2] W. M. Kantor, *Homogeneous designs and geometric lattices*, Journal of Combinatorial Theory, Series A **38** (1985), 66-74. MR **87c:**51007
[KLi] P. Kleidman and M. W. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, Cambridge University Press, 1990. MR **91g:**20001
[Kle] F. Klein, *Entwicklung der Mathematik im neunzehnten Jahrhundert*, Berlin, 1926.
[Kr1] W. Krull, *Allgemeine Bewertungstheorie*, Crelle Journal **167** (1932), 160-196.
[Kr2] W. Krull, *Dimensionstheorie in Stellenringe*, Crelle Journal **179** (1938), 204-226.
[Lan] S. Lang, *Algebraic groups over finite fields*, American Journal of Mathematics **78** (1956), 555-563. MR **19:**174a
[Len] H. W. Lenstra, *On the degrees of permutation polynomials*, Abstracts of the Third International Conference on Finite Fields and Applications (1995), 40.
[LZi] H. W. Lenstra and M. Zieve, *A family of exceptional polynomials in characteristic three*, Finite Fields and Applications, London Mathematical Society Lecture Notes Series **233** (1996), 209-218. MR **98a:**11174
[Li1] M. W. Liebeck, *The affine permutation groups of rank three*, Proceedings of the London Mathematical Society **54** (1987), 477-516. MR **88m:**20004
[Li2] M. W. Liebeck, *Characterization of classical groups by orbit sizes on the natural module*, Proceedings of the American Mathematical Society **124** (1996), 2961-2966. MR **97e:**20068
[LSe] M. W. Liebeck and G. M. Seitz, *On the subgroup structure of classical groups*, Inventiones Mathematicae **134** (1998), 427-453. MR **99h:**20074
[MMa] G. Malle and B. H. Matzat, *Inverse Galois Theory*, Springer-Verlag, 1999. MR **2000k:**12004
[Mar] B. Marggraff, *Über primitive Gruppen mit transitiven Untergruppen geringeren Grades*, Giessen Dissertation (1892).
[Mat] E. Mathieu, *Mémoire sur l'étude des fonctions de plusieurs quantités sur la manière de les former, et sur les substitutions qui les laissent invariables*, J. Math Pures Appl. **6** (1861), 241-323.
[Mod] M. R. Modak, *Combinatorial meaning of the coefficients of a Hilbert polynomial*, Proceedings of the Indian Academy of Sciences **102** (1992), 93-123. MR **94e:**13022
[Moo] E. H. Moore, *A two-fold generalization of Fermat's theorem*, Bulletin of the American Mathematical Society **2** (1896), 189-199.
[Mue] P. Müller, *New examples of exceptional polynomials*, Finite Fields: Theory, Applications and Algorithms, (G. L. Mullen and J. J. Shiue, eds.), Contemporary Mathematics **168** (1994), 245-249. MR **95h:**11136
[Mul] S. B. Mulay, *Determinantal loci and the flag variety*, Advances in Mathmatics **74** (1989), 1-30. MR **90j:**14071
[Neu] C. Neumann, *Riemann's Theorie der Abel'schen Integrale*, Teubner, 1888.
[New] I. Newton, *Geometria Analitica*, 1660.
[NoE] E. Noether, *Eliminationstheorie und allgemeine Idealtheorie*, Mathematische Annalen **90** (1923), 229-261.
[NoM] M. Noether, *Über einen Satz aus der Theorie der algebraischen Funktionen*, Mathematische Annalen **6** (1873), 351-359.
[Ost] A. Ostrowski, *Über einige Lösungen der Funktionalgleichung $\phi(x)\phi(y) = \phi(xy)$*, Acta Mathematica **41** (1918), 271-284.
[Pri] R. J. Pries, *Formal patching and deformation of wildly ramified covers of curves*, University of Pennsylvania Thesis (2000).
[Ray] M. Raynaud, *Revêtment de la droit affine en charactéristic $p > 0$ et conjecture d'Abhyankar*, Inventiones Mathematicae **116** (1994), 425-462. MR **94m:**14034
[Rie] B. Riemann, *Grundlagen für eine allgemeine Theorie der Functionen einer veränderlichen complexen Grösse*, Inauguraldissertation, Göttingen (1851), 1-48.
[Sal] G. Salmon, *Higher Plane Curves*, Dublin, 1852.

[Sha] D. L. Shannon, *Monoidal transforms*, American Journal of Mathematics **95** (1973), 294-320. MR **48:**8492

[Sev] F. Severi, *Vorlesungen über algebraische Geometrie*, Teubner, 1921.

[Se1] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini courbes elliptiques*, Inventiones Mathematicae **15** (1972), 259-331. MR **52:**8126

[Se2] J.-P. Serre, *Résumé de cours et travaux*, Annuaire du Collège de France **85-86** (1985).

[Se3] J.-P. Serre, *A letter to S. S. Abhyankar*, Algebraic Geometry and Its Applications, Papers Presented at the 60th Birthday Conference of Shreeram S. Abhyankar, Edited by C. Bajaj, Springer-Verlag (1994), 85-91. MR **95d:**12005

[Spe] A. Speiser, *Die Theorie der Gruppen von endlicher Ordnung*, Berlin, 1937.

[Sta] H. Stahl, *Theorie der Abel'schen Funktionen*, Teubner, 1896.

[Suz] M. Suzuki, *On a class of doubly transitive groups*, Annals of Mathematics **75** (1962), 104-145. MR **25:**112

[Syl] J. J. Sylvester, *On a general method of determining by mere inspection the derivations from two equations of any degree*, Philosophical Magazine **16** (1840).

[Tha] D. S. Thakur, *Drinfeld modules and arithmetic in the function fields*, Math. Res. Notices, Duke Math Jour. **9** (1992), 185-197. MR **93g:**11061

[Th1] J. G. Thompson, *Some finite groups which appear as* $Gal(L|K)$ *where* $K \subset Q(\mu_n)$, Journal of Algebra **89** (1984), 437-499. MR **87f:**12012

[Th2] J. G. Thompson, $GL_n(q)$*, rigidity and the braid group*, Bull. Soc. Math. Belg **42** (1990), 723-733. MR **96d:**20018

[Tit] J. Tits, *Buildings of spherical type and finite* BN*-pairs*, Springer Lecture Notes in Mathematics **386** (1974). MR **57:**9866

[Udp] S. G. Udpikar, *On Hilbert polynomial of certain determinantal ideals*, International Journal of Mathematics and Mathematical Sciences **14** (1992), 155-162. MR **92e:**05123

[VYo] O. Veblen and J. T. Young, *Projective Geometry I–II*, Ginn and Company, 1910-1918.

[Vel] F. D. Veldkamp, *Polar geometry I–V*, Nederl. Akad. Wetensch, Proc. Ser A 62-63, Indag, Math **22** (1959), 207-212. MR **23:**A2773

[Vo1] H. Voelklein, $GL_n(q)$ *as Galois group over the rationals*, Math. Annalen **293** (1992), 163-176. MR **94a:**12007

[Vo2] H. Voelklein, *Braid group action via* $GL_n(q)$ *and* $U_n(q)$*, and Galois realizations*, Israel Journal of Mathematics **82** (1993), 405-427. MR **94j:**12009

[Vo3] H. Voelklein, *Groups as Galois Groups*, Cambridge University Press, 1996. MR **98b:**12003

[Wan] D. Wan, *A generalization of the Carlitz conjecture*, Finite Fields, Coding Theory and Advances in Communications and Computing, Lecture Notes in Pure and Applied Mathematics, Dekker **141** (1993), 431-432.

[Wie] H. Wielandt, *Finite Permutation Groups*, Academic Press, 1964. MR **32:**1252

[Wey] H. Weyl, *Die Idee der Riemannschen Fläche*, Teubner, 1923.

[Za1] O. Zariski, *Some results in the arithmetical theory of algebraic varieties*, American Journal of Mathematics **61** (1939), 224-294.

[Za2] O. Zariski, *The reduction of singularities of algebraic surfaces*, Annals of Mathematics **40** (1939), 639-689.

[Za3] O. Zariski, *Foundations of a general theory of birational correspondences*, Transactions of the American Mathematical Society **53** (1943), 490-542. MR **5:**11b

[Za4] O. Zariski, *The reduction singularities of three-dimensional algebraic varieties*, Annals of Mathematics **45** (1944), 472-542. MR **6:**102f

[Za5] O. Zariski, *The fundamental ideas of abstract algebraic geometry*, Proceedings of the International Congress of Mathematicians (1950), 77-89. MR **13:**578e

[Za6] O. Zariski, *Theory and applications of holomorphic functions on algebraic varieties over arbitrary ground fields*, Memoirs of the American Mathematical Society **1** (1951). MR **12:**853f

[ZSa] O. Zariski and P. Samuel, *Commutative Algebra I–II*, Van Nostrand, 1959-1961. MR **19:**833e; MR **22:**11006

[Z01] H. J. Zassenhaus, *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, Abh. Math. Sem, Univ of Hamburg **11** (1936), 17-44.

[Z02] H. J. Zassenhaus, *The Theory of Groups*, Chelsea, 1949. MR **11:**77d

Mathematics Department, Purdue University, West Lafayette, IN 47907
E-mail address: `ram@cs.purdue.edu`