

# Chapter 1

## Use of Resultants and Approximate Roots for Doing the Jacobian Problem

Shreeram S. Abhyankar

*Mathematics Department,  
Purdue University, West Lafayette, IN 47907, USA  
ram@cs.purdue.edu*

This is an expository article giving a modified version of my talks at ISI-Kolkata and ISI-Bangalore. After sketching the history of the jacobian problem, I shall discuss the two basic tools which are employed in attacking this problem. The first is the theory of resultants which are usually coupled with discriminants. The second is the theory of approximate roots of polynomials which are inspired by the construction of square roots of positive real numbers.

### 1.1. Introduction

Two given bivariate polynomials are said to form a jacobian pair if their jacobian equals a nonzero constant, and they are said to form an automorphic pair if the variables can be expressed as polynomials in the given polynomials. By the chain rule we see that every automorphic pair is a jacobian pair. The jacobian problem asks if conversely every jacobian pair is an automorphic pair. It turns out that a useful method for attacking this problem is to study the similarity of polynomials. Two bivariate polynomials are similar means their degree forms, i.e., highest degree terms, are powers of each other when they are multiplied by suitable nonzero constants. Geometrically this amounts to saying that the corresponding plane curves have the same points at infinity counting multiplicities. At any rate, the points at infinity correspond to the distinct irreducible factors of the degree form.

Before getting into technicalities, I shall first give a short history of the problem or rather the history of my acquaintance with the problem. For that we have to go back to 1965 when a German mathematician, Karl Stein

who created Stein Manifolds, wrote me a letter asking a question. He said that there was an interesting 1955 paper in the *Mathematische Annalen* by Engel [9]. In this paper Engel claims to prove the jacobian theorem or what is now known as the jacobian problem or the jacobian conjecture or whatever. Karl Stein said to me that it is an interesting theorem but he cannot understand the proof. Can I help him? He also reduced it, or generalized it, to a conjecture about complex spaces. I wrote back to Stein giving a counterexample to his complex space conjecture. But I did not look at the Engel paper. Then in 1968, Max Rosenlicht of Berkeley asked me the same question and still I did not look at the Engel paper. Finally in 1970, my own guru (= venerable teacher) Oscar Zariski asked me the same question. Then, following the precept that one must obey one's guru, I looked up the Engel paper and found it full of mistakes and gaps.

The primary mistake in the Engel paper, which was repeated in a large number of published and unpublished wrong proofs of the jacobian problem in the last thirty-five years, is the presumed "obvious fact" that the order of the derivative of a univariate function is exactly one less than the order of the function. Being a prime characteristic person I never made this mistake. Indeed, the "fact" is correct only if the order of the function is nondivisible by the characteristic. Of course you could say that the jacobian problem is a characteristic zero problem, and zero does not divide anybody. But zero does divide zero. So the "fact" is incorrect if the order of the function is zero, i.e., if the value of the function is nonzero. Usually this mistake is well hidden inside a long argument, because you may start with a function which has a zero or pole at a given point and your calculation may lead to a function having a nonzero value at a resulting point.

A gap is a spot where you are not sure of the argument because of imprecise definitions or what have you. The gap in the Engel paper seems to be the uncritical use of the Zeuthen-Segre invariant. For this invariant of algebraic surfaces see the precious 1935 book of Zariski [12]. Over the years I have made several attempts to understand the somewhat mysterious theory of this invariant, and I still continue to do so.

In 1970-1977 I discussed the matter in my courses at Purdue and also in India and Japan. Mostly I was suggesting to the students to fix the proof and, to get them started, I proved a few small results. Notes of my lectures were taken down by Heinzer, van der Put, Sathaye, and Singh. These appeared in [1] and [4]. Then I put the matter aside for thirty years. Seeing that the problem has remained unsolved in spite of a continuous stream of wrong proofs announced practically every six months, I decided

to write up my old results, together with some enhancements obtained recently, in the form of a series of three long papers [6], [7], [8], in the Journal of Algebra, dedicated to the fond memory of my good friend Walter Feit. The ISI Jubilee Volume has given me a welcome opportunity of introducing these papers to the young students with an invitation to further investigate the problem.

Now one of my old results says that the jacobian conjecture is equivalent to the implication that each member of a jacobian pair can have only one point at infinity. Another says that each member of any jacobian pair has at most two points at infinity. Note that the first result is a funny statement; it only says that to prove the jacobian conjecture, it suffices to show that each member of any jacobian pair has only one point at infinity. The second result is of a more definitive nature, and it remains true even when we give weights to the variables which are different from the normal weights. Very recently I noticed that, and this is one of the enhancements, the weighted two point theorem yields a very short new proof of Jung's 1942 automorphism theorem [10]. This automorphism theorem says that every automorphism of a bivariate polynomial ring is composed of a finite number of linear automorphisms and elementary automorphisms. In a linear automorphism both variables are sent to linear expressions in them. In an elementary automorphism, one variable is unchanged and a polynomial in it is added to the second variable. In his 1972 lecture notes [11], Nagata declared the automorphism theorem to be very profound and so it did come as a pleasant surprise to me that the weighted two point theorem yields a five line proof of the automorphism theorem. For other recent enhancements let me refer to my Feit memorial papers cited above.

The present paper is only meant to whet the student's appetite. At any rate the material of this paper is based on my recent talks in various places such as ISI-Kolkatta and ISI-Bangalore.

## 1.2. Basic Technique

Our basic technique in attacking the jacobian problem is the use of resultants and approximate roots. Resultants are usually coupled with discriminants; the theory of these two objects will be discussed in Section 3. Approximate roots are polynomial concepts coming out of the construction of square roots in the theory of real numbers; these two topics will be discussed in Section 4. Here, assuming resultants and approximate roots, let us very briefly see how they are used in trying to do the jacobian problem.

Given any jacobian pair  $F(X, Y)$  and  $G(X, Y)$ , by making a homogeneous linear transformation we can arrange that they are monic polynomials of positive degrees  $N$  and  $M$  in  $Y$  respectively. Adjoin  $W$  to the ground field  $k$  and consider the algebraic closure  $K$  of  $k(W)$ . Now eliminate  $Z$  by using the  $Z$ -resultant to get

$$\phi(X, Y) = (-1)^{M+N} \text{Res}_Z(F(W, Z) - X, G(W, Z) - Y).$$

Then  $\phi(X, Y)$  is a monic polynomial of degree  $N$  in  $Y$  with coefficients in  $K[X]$ . Let  $\rho_0 = N$  and  $\rho_1 = M$ . Let  $d_1 = N$  and  $d_2 = \text{GCD}(\rho_0, \rho_1)$ . Let  $\text{App}_D \Phi$  denote the  $D$ -th approximate root of a monic polynomial  $\Phi$  whose  $Y$ -degree is a multiple  $E$  of  $D$ , i.e.,  $\text{App}_D \Phi$  is the unique monic polynomial  $\Psi$  of  $Y$ -degree  $E/D$  such that  $\deg_Y(\Phi - \Psi^D) < E - (E/D)$ . Let  $\psi_1(X, Y) = Y$ . For  $2 \leq i \leq h$  let us inductively define

$$\psi_i(X, Y) = \text{App}_{d_i} \phi(X, Y)$$

with

$$\rho_i = \deg_X \text{Res}_Y(\phi(X, Y), \psi_i(X, Y))$$

and

$$d_{i+1} = \text{GCD}(\rho_0, \dots, \rho_i)$$

so that  $d_2 > d_3 > \dots > d_{h+1} = 1$ . Here  $h$  is called the number of characteristic pairs.

By manipulating with this data, we can show that the polynomials  $F$  and  $G$  are similar. We can also show that if either  $h \leq 2$  or  $h = 3$  with  $d_h$  even then the given jacobian pair  $(F, G)$  is an automorphic pair. As a consequence we can settle the jacobian conjecture when  $\min(M, N) \leq 52$ . For details see [1] to [8].

### 1.3. Resultants and Discriminants

The material of this Section is taken from pages 100-104 of my new Algebra Book [5]. Details of proof can be found on pages 172-188 of that Book.

Beginning algebra students encounter discriminants of quadratic polynomials, but resultants are less well known. They were introduced by Sylvester around 1840. Actually in some sense we need to start with Descartes who introduced coordinates around 1637. Bézout built on these ideas to introduce his version of resultants for the original proof of Bézout's Theorem.

Bézout’s Theorem, proved by him around 1770, is one of the oldest theorems of algebraic geometry. It says that a curve of degree  $m$  and a curve of degree  $n$  meet in  $mn$  points provided they have no common component and provided the intersections are counted properly.

One way of proving Bézout’s Theorem is by using resultants. Vertical tangents can be located by using discriminants which are special cases of resultants.

Assuming  $n, m$  to be nonnegative integers, the  $Y$ -Resultant of two polynomials

$$f(Y) = a_0Y^n + a_1Y^{n-1} + \dots + a_n$$

$$g(Y) = b_0Y^m + b_1Y^{m-1} + \dots + b_m$$

is the determinant

$$\text{Res}_Y(f, g) = \det(\text{Resmat}_Y(f, g))$$

of the  $n + m$  by  $n + m$  matrix

$$\text{Resmat}_Y(f, g) = \begin{pmatrix} a_0 & a_1 & \dots & a_n & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_n & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_0 & a_1 & \dots & \dots & a_n \\ b_0 & b_1 & \dots & b_m & 0 & \dots & \dots & 0 \\ 0 & b_0 & b_1 & \dots & b_m & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & b_0 & b_1 & \dots & \dots & b_m \end{pmatrix}$$

where the first  $m$  rows consist of the coefficients of  $f$  and the last  $n$  rows consist of the coefficients of  $g$ . More precisely, the first row starts with the coefficients of  $f$ , these are shifted one step to the right to get the second row, shifted two steps to the right to get the third row, and so on for the first  $m$  rows, then the  $(m + 1)$ -st row starts with the coefficients of  $g$ , these are shifted one step to the right to get the  $(m + 2)$ -nd row, and so on for the next  $n$  rows. The matrix is completed by stuffing zeroes elsewhere. The determinant  $\text{Res}_Y(f, g)$  is sometimes called the Sylvester resultant of  $f$  and  $g$  because it was introduced by Sylvester in his 1840 paper where he enunciated the following:

**BASIC FACT (T1).** If the coefficients  $a_i, b_j$  belong to a domain  $R$  then we have:  $\text{Res}_Y(f, g) = 0 \Leftrightarrow n + m \neq 0$  and either  $a_0 = 0 = b_0$  or  $f$  and  $g$  have a common root in some overfield of  $R$ .

In case  $n > 0$ , the  $Y$ -Discriminant of  $f$  is defined to be the  $Y$ -Resultant of  $f$  and  $f_Y$ , i.e.,

$$\text{Disc}_Y(f) = \text{Res}_Y(f, f_Y).$$

where we view  $f_Y$  to be the polynomial

$$f_Y(Y) = na_0Y^{n-1} + (n-1)a_1Y^{n-2} + \cdots + a_{n-1}$$

i.e., we let the discriminant to be the determinant of the appropriate  $2n-1$  by  $2n-1$  matrix without considering whether  $na_0$  equals zero or not.

From the Basic Fact (T1) we deduce the following:

**COROLLARY (T2).** If  $n > 1$  and the coefficients  $a_i$  belong to a domain  $R$  then:  $\text{Disc}_Y(f) = 0 \Leftrightarrow$  either  $a_0 = 0$  or  $f$  has a multiple root in some overfield of  $R$ .

**OBSERVATION (O1).** [**Resultant and Projection**]. If  $X_1, \dots, X_N$  are indeterminates over a field  $k$  with  $N \in \mathbb{N}_+$  and  $R$  is either the polynomial ring  $k[X_1, \dots, X_N]$  or the power series ring  $k[[X_1, \dots, X_N]]$ , then  $\text{Res}_Y(f, g)$  equals a polynomial or power series  $\Phi = \Phi(X_1, \dots, X_N)$ . If  $a_0$  and  $b_0$  are in  $k^\times$  with  $nm \neq 0$  and  $k$  is algebraically closed then, in the polynomial case, by the Basic Fact it follows that the hypersurface  $\Phi = 0$  in the  $N$ -space of  $(X_1, \dots, X_N)$  is the projection of the intersection of the hypersurfaces  $f = 0$  and  $g = 0$  in the  $(N+1)$ -space of  $(X_1, \dots, X_N, Y)$ . Moreover, without assuming  $k$  to be algebraically closed but assuming that  $a_0$  and  $b_0$  are nonzero constants, in the polynomial case as well as the power series case, by the Basic Fact it follows that:  $\Phi$  is identically zero (i.e.,  $\Phi$  is the zero element of  $R$ )  $\Leftrightarrow$   $f$  and  $g$  have a nonconstant common factor in  $R[Y]$ .

**OBSERVATION (O2).** [**Discriminant and Projection**]. Again if  $X_1, \dots, X_N$  are indeterminates over a field  $k$  with  $N \in \mathbb{N}_+$  and  $R$  is either the polynomial ring  $k[X_1, \dots, X_N]$  or the power series ring  $k[[X_1, \dots, X_N]]$ , then  $\text{Disc}_Y(f)$  equals a polynomial or power series  $\Delta = \Delta(X_1, \dots, X_N)$ . Now if  $a_0$  is in  $k^\times$  with  $n > 1$  and  $k$  is algebraically closed then, in the polynomial case, for all values  $(U_1, \dots, U_N)$  of  $(X_1, \dots, X_N)$  in  $k$ , the equation  $f = 0$  has  $n$  roots which may or may not be distinct, and by the Corollary it follows that these roots are not distinct iff  $\Delta(U_1, \dots, U_N) = 0$ . In other words, when we project the hypersurface  $f = 0$  in  $(N+1)$ -space onto the  $N$ -space, above most points there lie  $n$  points, and  $\Delta = 0$  is the

locus of those points above which there lie less than  $n$  points. Moreover, without assuming  $k$  to be algebraically closed but assuming that  $a_0$  is a nonzero constant, in the polynomial case as well as the power series case, by the Corollary it follows that:  $\Delta$  is identically zero  $\Leftrightarrow f$  has a nonconstant multiple factor in  $R[Y]$ .

**OBSERVATION (O3). [Isobaric Property].** View the coefficients  $a_i, b_j$  as indeterminates over  $\mathbb{Z}$ . Give weight  $i$  to  $a_i$ , and  $j$  to  $b_j$ . Then  $0 \neq \text{Res}_Y(f, g) \in \mathbb{Z}[a_0, \dots, a_n, b_0, \dots, b_m]$  is isobaric of weight  $mn$ , i.e., for the weight of any monomial  $a_0^{i_0} \dots a_n^{i_n} b_0^{j_0} \dots b_m^{j_m}$  occurring in  $\text{Res}_Y(f, g)$  we have  $(\sum_{0 \leq r \leq n} r i_r) + (\sum_{0 \leq s \leq m} s j_s) = mn$ . In particular, the principal diagonal  $a_0^m b_m^n$  has weight  $mn$ , and it does not cancel out because there is no other term of  $b_m$ -degree  $n$  in the resultant; the principal diagonal of an  $N \times N$  matrix  $(A_{ij})$  is the term  $A_{11}A_{22} \dots A_{NN}$ . The resultant being isobaric of weight  $mn$  is the fundamental fact behind various cases of Bézout's Theorem. The following two Observations, where we use the set-up of Observation (O1), illustrate this for plane curves and general hypersurfaces respectively.

**OBSERVATION (O4). [Plane Bézout].** Let  $N = 1$  with  $X = X_1$ , and assume that  $a_0, b_0$  are nonzero elements in  $k$ , and  $f, g$  are polynomials of total  $(X, Y)$ -degrees  $n$  and  $m$  respectively. By the isobaric property we see that then always  $\deg_X \Phi \leq mn$  and “in general”  $\deg_X \Phi = mn$ . Hence the  $n$ -degree plane curve  $f = 0$  meets the  $m$ -degree plane curve  $g = 0$  in  $mn$  points “counted properly.” The possibility of  $\deg_X \Phi < mn$  is explained by saying that some intersections have “gone to infinity.”

**OBSERVATION (O5). [Hyperspatial Bézout].** Let  $N$  be general and assume that  $a_0, b_0$  are nonzero elements in  $k$ , and  $f, g$  are polynomials of total  $(X_1, \dots, X_N, Y)$ -degrees  $n$  and  $m$  respectively. By the isobaric property we see that then always  $\deg_{(X_1, \dots, X_N)} \Phi \leq mn$  and “in general”  $\deg_{(X_1, \dots, X_N)} \Phi = mn$ . Hence, in the  $(N + 1)$ -dimensional space, the  $n$ -degree hypersurface  $f = 0$  and the  $m$ -degree hypersurface  $g = 0$  meet along a “secundum” (= a subvariety of dimension two less than dimension of the ambient space) which projects onto the  $(mn)$ -degree hypersurface  $\Phi = 0$  in  $N$ -dimensional space. Again the possibility of  $\deg_{(X_1, \dots, X_N)} \Phi < mn$  says that some intersections have “gone to infinity.”

**EXAMPLE (X1). [Resultant and Discriminant in Terms of Roots].** If the coefficients  $a_i, b_j$  belong to a domain  $R$  and  $a_0 \neq 0 \neq b_0$  then, upon

writing

$$f(Y) = a_0 \prod_{1 \leq i \leq n} (Y - \alpha_i) \quad \text{and} \quad g(Y) = b_0 \prod_{1 \leq j \leq m} (Y - \beta_j)$$

with  $\alpha_1, \dots, \alpha_n$  and  $\beta_1, \dots, \beta_m$  in an overfield of  $R$ , we have

$$\begin{aligned} \text{Res}_Y(f, g) &= a_0^m b_0^n \prod_{1 \leq i \leq n} \prod_{1 \leq j \leq m} (\alpha_i - \beta_j) \\ &= a_0^m \prod_{1 \leq i \leq n} g(\alpha_i) = (-1)^{mn} b_0^n \prod_{1 \leq j \leq m} f(\beta_j) \end{aligned}$$

and

$$\text{Disc}_Y(f) = (-1)^{n(n-1)/2} a_0^n \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

EXAMPLE (X2). [**Quadratic Resultant**]. Considering the quadratic polynomials

$$f(Y) = aY^2 + bY + c \quad \text{and} \quad g(Y) = a'Y^2 + b'Y + c'$$

and calculating the  $4 \times 4$  determinant

$$\begin{pmatrix} a & b & c & 0 \\ 0 & a & b & c \\ a' & b' & c' & 0 \\ 0 & a' & b' & c' \end{pmatrix}$$

we get  $\text{Res}_Y(f, g) = (a^2c'^2 + a'^2c^2) + (b^2a'c' + b'^2ac) - (abb'c' + a'b'bc) - 2aca'c'$ .

EXAMPLE (X3). [**Quadratic Discriminant**]. Considering the quadratic

$$f(Y) = aY^2 + bY + c$$

and calculating the  $3 \times 3$  determinant

$$\begin{pmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{pmatrix}$$

we get  $\text{Disc}_Y(f) = -a(b^2 - 4ac)$ .

EXAMPLE (X4). [**Cubic Discriminant**]. Considering the cubic

$$f(Y) = a_0Y^3 + a_1Y^2 + a_2Y + a_3$$

and calculating an appropriate  $5 \times 5$  determinant we get

$$\text{Disc}_Y(f) = -a_0(a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3 - 27a_0^2a_3^2 + 18a_0a_1a_2a_3).$$

EXAMPLE (X5). [**Special Quartic Discriminant**]. Considering the quartic

$$f(Y) = Y^4 + pY^2 + qY + r$$

and calculating an appropriate  $7 \times 7$  determinant we get

$$\text{Disc}_Y(f) = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3.$$

EXAMPLE (X6). [**General Quartic Discriminant**]. Considering the quartic

$$f(Y) = a_0Y^4 + a_1Y^3 + a_2Y^2 + a_3Y + a_4$$

and calculating an appropriate  $7 \times 7$  determinant we get

$$\left\{ \begin{array}{l} \text{Disc}_Y(f) = a_0(256a_0^3a_4^3 - 192a_0^2a_1a_3a_4^2 - 128a_0^2a_2^2a_4^2 + 144a_0^2a_2a_3^2a_4 \\ \quad - 27a_0^2a_3^4 + 144a_0a_1^2a_2a_4^2 - 6a_0a_1^2a_3^2a_4 - 80a_0a_1a_2^2a_3a_4 \\ \quad + 18a_0a_1a_2a_3^3 + 16a_0a_4^4a_4 - 4a_0a_2^3a_3^2 - 27a_1^4a_4^2 \\ \quad + 18a_1^3a_2a_3a_4 - 4a_1^3a_3^3 - 4a_1^2a_2^3a_4 + a_1^2a_2^2a_3^2). \end{array} \right.$$

## 1.4. Real Numbers and Approximate Roots

The material of this Section is taken from pages 52-59 of my new Algebra Book [5].

Historically, the process of counting gave rise to the set  $\mathbb{N}_+$  of all positive integers. Augmenting it by zero, this set was enlarged to get the set  $\mathbb{N}$  of all nonnegative integers. Inserting the negative of everybody gave the full set  $\mathbb{Z}$  of all integers. Finally the process of division gave rise to the set  $\mathbb{Q}$  of all rational numbers.

Taking this much for granted, we shall describe the limiting processes which gave rise first to the set  $\mathbb{R}$  of real numbers and then to the set  $\mathbb{C}$  of all complex numbers. The passage from  $\mathbb{Q}$  to  $\mathbb{R}$  was made precise by Cauchy by means of Cauchy Sequences around 1830, and by Dedekind by means of Dedekind Cuts around 1880. After sketching this development, we show how the construction of square roots of positive integers led us, around 1975, to the construction of approximate roots of polynomials. Briefly, this solves the problem as to how close we can come to finding the  $D$ -the root of

a one-variable polynomial whose degree is a multiple of the positive integer  $D$ .

As in the quoted Algebra Book, we shall divide the material into a series of Definitions and Exercises. For the basic definitions of terms and standard set theory symbols which we shall use, such as  $\in$  for “element of,” the reader may consult the first few pages of the said Algebra Book, or any other current text-book of college mathematics.

**DEFINITION (D1). [Real and Complex Numbers].** Real numbers may be defined as equivalence classes of Cauchy sequences of rational numbers, and the complex number field  $\mathbb{C}$  may then be defined as the splitting field of the quadratic polynomial  $Y^2 + 1$  over the real number field  $\mathbb{R}$ . By analogy with  $\mathbb{N}_+$ , by  $\mathbb{Q}_+$  we denote the set of all positive rationals; moreover, by  $\mathbb{Q}_{0+}$ ,  $\mathbb{Q}_-$ , and  $\mathbb{Q}_{0-}$  we denote the set of all nonnegative rationals, negative rationals, and nonpositive rationals respectively; as usual, the absolute value of any  $r \in \mathbb{Q}$  is denoted by  $|r|$ , i.e.,  $|r| = r$  or  $-r$  according as  $r \in \mathbb{Q}_{0+}$  or  $r \in \mathbb{Q}_-$ ; by context, this will not be confused with the size  $|S|$  of a set  $S$ . A sequence  $x = (x_i)_{1 \leq i < \infty}$  in  $\mathbb{Q}$  is Cauchy means for every  $\epsilon \in \mathbb{Q}_+$  there exists  $N_\epsilon \in \mathbb{N}_+$  such that for all  $i > N_\epsilon$  and  $j > N_\epsilon$  we have  $|x_i - x_j| < \epsilon$ . This is equivalent to the Cauchy sequence  $x' = (x'_i)_{1 \leq i < \infty}$ , in symbols  $x \sim x'$ , if for every  $\epsilon \in \mathbb{Q}_+$  there exists  $M_\epsilon \in \mathbb{N}_+$  such that for all  $i > M_\epsilon$  we have  $|x_i - x'_i| < \epsilon$ . Now  $\mathbb{R}$  may be defined to be the quotient  $C_{\mathbb{Q}} / \sim$  of the set  $C_{\mathbb{Q}}$  of all Cauchy sequences in  $\mathbb{Q}$  by the equivalence relation  $\sim$ . We “identify”  $\mathbb{Q}$  with a subset of  $\mathbb{R}$  by sending any  $q \in \mathbb{Q}$  to the equivalence class of the Cauchy sequence  $(q_i)_{1 \leq i < \infty}$  with  $q_i = q$  for all  $i$ . If  $y = (y_i)_{1 \leq i < \infty}$  is another Cauchy sequence in  $\mathbb{Q}$  then the sequences  $(x_i + y_i)_{1 \leq i < \infty}$  and  $(x_i y_i)_{1 \leq i < \infty}$  are Cauchy sequences whose equivalence classes are unchanged if  $x$  and  $y$  are replaced by equivalent Cauchy sequences; this makes  $\mathbb{R}$  into a ring and in fact an overfield of  $\mathbb{Q}$ .

**DEFINITION (D2). [Ordered Fields].** The order relation  $\leq$  can be extended from  $\mathbb{Q}$  to  $\mathbb{R}$  by declaring that the equivalence class of  $x$  is  $\leq$  the equivalence class of  $y$  if the Cauchy sequences  $x$  and  $y$  in their equivalence classes can be chosen so that  $x_i \leq y_i$  for all  $i$ ; see (E3) below. Like  $\mathbb{Z}$  and  $\mathbb{Q}$ , this makes  $\mathbb{R}$  an ordered domain, i.e., a domain whose underlying additive abelian group is an ordered abelian group and in which the product of any positive elements (i.e., elements which are greater than zero) is again positive. Out of these  $\mathbb{Q}$  and  $\mathbb{R}$  are ordered fields, i.e., fields whose underlying domains are ordered domains. We extend the notation  $\mathbb{Q}_+$ ,  $\mathbb{Q}_{0+}$ ,  $\mathbb{Q}_-$ , and  $\mathbb{Q}_{0-}$  to any ordered abelian group  $G$  (and hence to ordered domains

and ordered fields) by putting  $G_+ = \{g \in G : g > 0\}$ ,  $G_{0+} = G_+ \cup \{0\}$ ,  $G_- = \{g \in G : g < 0\}$ , and  $G_{0-} = G_- \cup \{0\}$ ; also we define the absolute value of any  $g \in G$  by putting  $|g| = g$  or  $-g$  according as  $g \in G_{0+}$  or  $g \in G_-$ . In particular this defines the sets  $R_+$ ,  $R_{0+}$ ,  $R_-$ ,  $R_{0-}$ , and defines the absolute value  $|r|$  of any  $r \in \mathbb{R}$ . Note that now  $\mathbb{Z}_+ = \mathbb{N}_+$  and  $\mathbb{Z}_{0+} = \mathbb{N}$ . An ordered abelian group  $G$  is archimedean means for all  $x, y$  in  $G_+$  we have  $nx > y$  for some  $n \in \mathbb{N}_+$ . Clearly  $\mathbb{R}$  is an archimedean ordered field, i.e., an ordered field whose underlying additive ordered abelian group is archimedean. A sequence  $x = (x_i)_{1 \leq i < \infty}$  in an ordered abelian group  $G$  is Cauchy means for every  $\epsilon \in G_+$  there exists  $N_\epsilon \in \mathbb{N}_+$  such that for all  $i > N_\epsilon$  and  $j > N_\epsilon$  we have  $|x_i - x_j| < \epsilon$ ; the sequence  $x$  is convergent means it converges to a limit  $\xi \in G$ , i.e., for every  $\epsilon \in G_+$  there exists  $M_\epsilon \in \mathbb{N}_+$  such that for all  $i > M_\epsilon$  we have  $|\xi - x_i| < \epsilon$ ; we indicate this by some standard notation such as  $x_i \rightarrow \xi$  as  $i \rightarrow \infty$  or  $\lim_{i \rightarrow \infty} x_i = \xi$ . An ordered abelian group is complete means in it every Cauchy sequence is convergent. Clearly  $\mathbb{R}$  is a complete field, i.e., an ordered field whose underlying additive group is complete as an ordered abelian group.

**DEFINITION (D3). [Torsion Subgroups and Divisible Groups].** By the subgroup of a group  $G$  generated by elements  $x_1, x_2, \dots$  in  $G$  we mean the smallest subgroup of  $G$  which contains these elements. The order of an element in a group is the order of the subgroup generated by it. The subgroup of an additive abelian group  $G$  generated by all of its elements of finite order is called the torsion subgroup of  $G$ ; if this is zero then  $G$  is said to be torsion free. An additive abelian group  $G$  is divisible means for every  $g \in G$  and  $n \in \mathbb{Z}^\times$  there is  $h \in G$  with  $nh = g$ .

**EXERCISE (E1).** Show that for any elements  $a, b$  in a torsion free additive abelian group and any nonzero integer  $n$  we have:  $na = nb \Rightarrow a = b$ . Show that any ordered abelian group is torsion free, and hence any ordered field is of characteristic zero. Show that for all  $x, y$  in an ordered field we have  $|xy| = |x||y|$ . Show that the usual order on  $\mathbb{Q}$  is the only order on it which makes it an ordered field.

**EXERCISE (E2).** Show that for all  $x, y$  in an ordered abelian group  $G$  we have  $|x + y| \leq |x| + |y|$ , and from this deduce that any convergent sequence in  $G$  is Cauchy and has a unique limit.

**DEFINITION (D4). [Rational Completions].** Given any torsion free additive abelian group  $G$ , let  $G^* = G \times \mathbb{Z}^\times / \sim$  where the equivalence relation  $\sim$  is given by:  $(g, n) \sim (g', n') \Leftrightarrow n'g = ng'$ , and embed  $G$  in  $G^*$  by

identifying every  $g \in G$  with the equivalence class containing  $(g, 1)$ . Define addition in  $G^*$  by taking equivalence classes in the proposed equation  $(g, n) + (h, m) = (mg + nh, nm)$ . Note that then  $G^*$  is a divisible additive abelian group such that for every  $\bar{g} \in G^*$  we have  $n\bar{g} \in G$  for some  $n \in \mathbb{Z}^\times$ . We call  $G^*$  the rational completion of  $G$ . Note that if  $G$  is divisible then  $G^* = G$ .

EXERCISE (E3). In (D2) show that the induced relation  $\leq$  on the equivalence classes of Cauchy sequences in  $\mathbb{Q}$  is a linear order.

EXERCISE (E4). In (D4) show that the induced relation  $\leq$  on the equivalence classes of Cauchy sequences in an ordered abelian group is a linear order.

EXERCISE (E5). Let  $G$  be any nonzero archimedean ordered abelian group. Show that given any  $g > 0$  in  $G$  and  $x > 0$  in  $\mathbb{R}$ , there exists a unique order monomorphism (i.e., a group monomorphism which is order preserving)  $\phi : G \rightarrow \mathbb{R}$  such that  $\phi(g) = x$ , and there exists a unique order isomorphism (i.e., a group isomorphism which is order preserving)  $\psi : \overline{G^*} \rightarrow \mathbb{R}$  such that  $\psi(g) = x$ . Moreover, for these maps we always have  $\phi(h) = \psi(h)$  for all  $h \in G$ .

EXERCISE (E6). Show that  $x \mapsto x^2$  gives a surjection  $\mathbb{R} \rightarrow \mathbb{R}_{0+}$ .

HINT. The usual method of finding the decimal expansion  $1.14142\dots$  of  $\sqrt{2}$  can be explained in terms of decimal expansions of integers by saying that  $1^2 < 2 < 2^2$ ,  $14^2 < 2 \times 10^2 < 15^2$ ,  $141^2 < 2 \times 10^4 < 142^2$ ,  $1414^2 < 2 \times 10^6 < 1415^2$ ,  $14142^2 < 2 \times 10^8 < 14143^2$ , and so on. More generally let  $n > 1$  and  $d > 1$  be any integers, and let  $y > 0$  and  $i > 0$  be any integers. Then clearly there is a unique integer  $x_i$  such that  $x_i^d \leq yn^{di} < (x_i + 1)^d$ ;  $x_i$  is nothing but the  $n$ -adic expansion of the largest integer  $\leq y^{1/d}n^i$ . Obviously the sequence  $(x_i/n^i)$  is Cauchy and for its limit  $x$  in  $\mathbb{R}_+$  we have  $x^d = y$ . Any positive rational can be written in the form  $y/z^d$  where  $y$  and  $z$  are positive integers, and then we get  $x/z \in \mathbb{R}_+$  with  $(x/z)^d = y/z^d$ . Finally, any  $\eta \in \mathbb{R}_+$  can be written as the limit of a sequence  $(\eta_j)$  in  $\mathbb{Q}_+$  and then taking  $\xi_j \in \mathbb{R}_+$  with  $\xi_j^d = \eta_j$  we get a Cauchy sequence  $(\xi_j)$  for whose limit  $\xi \in \mathbb{R}_+$  we have  $\xi^d = \eta$ .

DEFINITION (D5). [**Rational Ranks**]. In view of the first sentence of (E1), any torsion free divisible additive abelian group may clearly be regarded as a  $\mathbb{Q}$ -vector-space. The  $\mathbb{Q}$ -vector-space dimension of the rational completion of a torsion free additive abelian group  $G$  is called the rational

rank of  $G$  and is denoted by  $r(G)$ . Alternatively,  $r(G)$  may be characterized as the cardinal of a maximal (= nonenlargeable)  $\mathbb{Z}$ -linearly independent subset  $H$  of  $G$ , where independent means that for any finite number of distinct elements  $x_1, \dots, x_d$  in  $H$  and any integers  $n_1, \dots, n_d$  we have:  $n_1x_1 + \dots + n_dx_d = 0 \Rightarrow n_1 = \dots = n_d = 0$ .

**DEFINITION (D6). [Dedekind Cuts].** Instead of using Cauchy sequences to prove (E5), we can use Dedekind Cuts. So let  $G$  be a nonzero divisible archimedean ordered abelian group. A Dedekind cut of  $G$  is a pair  $(L, U)$  of nonempty subsets of  $G$  with  $U = G \setminus L$  such that for all  $l \in L$  and  $u \in U$  we have  $l < u$  and there is no  $u' \in U$  with  $U = \{u \in G : u' \leq u\}$ . For any  $t \in G$  we get a Dedekind cut  $(L_t, U_t)$  with  $L_t = \{l \in G : l \leq t\}$  and  $U_t = \{u \in G : t < u\}$ . Let  $D_G$  be the set of all Dedekind cuts of  $G$ . It can be shown that  $G$  is complete  $\Leftrightarrow t \mapsto (L_t, R_t)$  gives a surjection  $G \rightarrow D_G$ . Indeed,  $D_G$  may be defined to be the completion of  $G$ . At any rate, for proving (E5), given any  $h \in G$  let  $\theta(h)$  be the real number which corresponds to the Dedekind cut  $(L, U)$  of  $\mathbb{Q}$  where  $L = \{m/n \in \mathbb{Q} \text{ with } m \in \mathbb{Z} \text{ and } n \in \mathbb{N}_+ : nh \leq mg\}$  and  $U = \mathbb{Q} \setminus L$ , and take  $\phi(h) = x\theta(h)$ .

**DEFINITION (D7). [Approximate Roots].** In the Hint to (E6) we showed how to use  $n$ -adic expansions of positive integers to find successive approximations to the  $d$ -th root of a positive integer. Mixing a generalization of this with a generalization of the completing the square method of solving quadratic equations leads us to the concept of approximate roots of polynomials. So consider a monic polynomial

$$F = F(Y) = Y^N + \sum_{1 \leq i \leq N} A_i Y^{N-i}$$

of degree  $N > 0$  in  $Y$  with coefficients  $A_i$  in a ring  $R$ . If  $N$  is a unit in  $R$  then we can generalize the completing the square idea to completing the  $N$ -th power by writing

$$F(Y) = (Y + A_1/N)^N + \sum_{2 \leq i \leq N} A'_i (Y + A_1/N)^{N-i}$$

with  $A'_i \in R$ , i.e., by killing the coefficient of  $Y^{N-1}$ . [On page 58 of my Lectures on Algebra Volume I, inadvertently the two plus signs in the above display have been printed as minus signs and, three lines above that,  $N > 0$  has been printed as  $N \geq 0$ ]. To generalize this further let  $D > 0$  be an integer which divides  $N$ . Instead of assuming  $N$  to be a unit in  $R$ , assume  $D$  to be a unit in  $R$ ; note that in case of a field  $R$  this is equivalent to assuming

that the characteristic of  $R$  does not divide  $D$  and so characteristic zero is always ok. Now we look for a monic polynomial

$$G = G(Y) = Y^{N/D} + \sum_{1 \leq i \leq N/D} B_i Y^{(N/D)-i}$$

of degree  $N/D$  in  $Y$  with coefficients  $B_i$  in  $R$  such that  $G^D$  is as close to being equal to  $F$  as possible. As (E7) below shows, if we interpret this as requiring  $\deg_Y(F - G^D) < N - (N/D)$  then a unique  $G$  exists, and we call it the approximate  $D$ -th root of  $F$  (relative to  $Y$ ) and denote it by  $\text{App}_D(F)$  or  $\text{App}_{D,Y}(F)$ . Recall that for any  $m, n$  in  $\mathbb{N}$  with  $n > 1$ , the  $n$ -adic expansion of  $m$  consists of writing  $m = \sum_{i \geq 0} m_i n^i$  where integers  $0 \leq m_i < n$  are the digits of the expansion. Likewise for any  $f, g$  in  $R[Y]$  with  $g$  monic of positive  $Y$ -degree, the  $g$ -adic expansion of  $f$  consists of writing  $f = \sum_{i \geq 0} f_i g^i$  where  $f_i \in R[Y]$  with  $\deg_Y f_i < \deg_Y g$  are the digits of the expansion. By (E8) below these expansions exist and are unique. Moreover, if  $f$  is monic of  $Y$ -degree  $N > 0$  and the  $Y$ -degree of  $g$  is  $N/D \in \mathbb{N}_+$  where  $D \in \mathbb{N}_+$  is a unit in  $R$ , then  $f_D = 1$  and  $f_i = 0$  for all  $i > D$ ; we try completing the  $D$ -th power by putting  $\tau_f(g) = \tau_{f,Y}(g) = g + (f_{D-1}/D)$  and calling it the  $f$ -Tschirnhausen of  $g$  (relative to  $Y$ ). This references to the 1683 work of Tschirnhausen who was a friend of Leibnitz. By (E9) below, starting with any monic  $g$  of degree  $N/D$  and applying  $\tau_f$  to it  $N/D$  times will produce the approximate  $D$ -th root of  $f$ .

EXERCISE (E7). Let  $F$  be a monic polynomial of degree  $N > 0$  in  $Y$  over a ring  $R$ . Let  $D > 0$  be an integer such that  $D$  divides  $N$  and  $D$  is a unit in  $R$ . Show that there exists a unique monic polynomial  $G$  of degree  $N/D$  in  $Y$  over  $R$  such that  $\deg_Y(F - G^D) < N - (N/D)$ . Hint: With display as in (D7), the last condition gives the equations  $A_i = DB_i + P_i(B_1, \dots, B_{i-1})$  for  $1 \leq i \leq N/D$  where the coefficient of  $Y^{N-i}$  in  $G^D$  equals  $DB_i + P_i(B_1, \dots, B_{i-1})$  with  $P_i$  a polynomial over  $\mathbb{Z}$ ; since  $D$  is a unit in  $R$ , these can be solved successively (in a unique manner).

EXERCISE (E8). Given integers  $m \geq 0$  and  $n > 1$ , show the unique existence of the  $n$ -adic expansion of  $m$ . Given univariate polynomials  $f, g$  over a ring  $R$  with  $g$  monic of positive degree, show the unique existence of the  $g$ -adic expansion  $f = \sum_{i \geq 0} f_i g^i$  of  $f$ . Show that if  $f$  is monic of degree  $N > 0$  and the degree of  $g$  is  $N/D$  where  $D$  is a positive integer factor of  $N$ , then  $f_D = 1$  and  $f_i = 0$  for all  $i > D$ , and moreover:  $\text{App}_D(f) = g \Leftrightarrow f_{D-1} = 0$ .

EXERCISE (E9). Let  $f, g$  be univariate monic polynomials of positive degrees  $N$  and  $N/D$  over a ring  $R$  where  $D$  is a positive integer which di-

vides  $N$ , and is a unit in  $R$ . Let  $\tau_f(g) = \bar{g}$ , and let  $f = \sum_{0 \leq i \leq D} f_i g^i$  and  $f = \sum_{0 \leq i \leq D} \bar{f}_i \bar{g}^i$  be the  $g$ -adic and  $\bar{g}$ -adic expansions of  $f$  respectively. Show that if  $f_{D-1} \neq 0 \neq \bar{f}_{D-1}$  then  $\deg(\bar{f}_{D-1}) < \deg(f_{D-1})$ . From this deduce that  $\tau_f^{N/D}(g) = \text{App}_D(f)$ .

## Epilogue

MANGALACHARAN

ATA VISHVATMAKE DEVE | YENE VAGYADNYE TOSHAVE

TOSHONI MAJA DYAVE | PASAYDANA HE

GANITAVIDYECHEE JAGRUTEE | KARONIYA SARVA JAGATEE

PRADNYASURYE UJALATEE | SUKHAVAYA SAKALA JANA

Here is a free Paraphrase of the above MANGALACHARAN = INVOCATION in my mother tongue MARATHI whose founding father DHYANESHVAR composed the first two lines around 1250 A.D. to which I added the last two lines.

PARAPHRASE. May the Lord God of the Universe be pleased with my recounting of the story of algebra and geometry which are the essence of our beloved subject of mathematics. Being pleased may he shower his blessings upon us and make our endeavor pleasurable.

## References

- [1] Abhyankar, S. S. (1977). *Expansion Techniques in Algebraic Geometry*. Tata Institute of Fundamental Research, Bombay.
- [2] Abhyankar, S. S. (1977). On the semigroup of a Meromorphic Curve (Part I). *Proceedings of the International Symposium on Algebraic Geometry* (Kyoto), Kinokuniya, Tokyo, pp. 249-414.
- [3] Abhyankar, S. S. (1990). *Algebraic Geometry for Scientists and Engineers*. American Mathematical Society, 1990.
- [4] Abhyankar, S. S. (1994). Some Remarks on the Jacobian Question. *Purdue Lecture Notes*, pp. 1-20 (1971); Published in the *Proceedings of the Indian Academy of Sciences*. **104** 515-542.
- [5] Abhyankar, S. S. (2006). *Lectures on Algebra I*. World Scientific.
- [6] Abhyankar, S. S. (2008). Some Thoughts on the Jacobian Conjecture, Part I. *Journal of Algebra* **319** 493-548.
- [7] Abhyankar, S. S. (2008). Some Thoughts on the Jacobian Conjecture, Part II. *Journal of Algebra*. **319** 1154-1248.
- [8] Abhyankar, S. S. (2008). Some Thoughts on the Jacobian Conjecture, Part III. *Journal of Algebra*. To Appear.

- [9] Engel, W. (1955). Ein Satz über ganze Cremona Transformationes der Ebene. *Mathematische Annalen*. **130** 11-19.
- [10] Jung, H. W. E. (1942). Über ganze birationale Transformatione der Ebene. *Crelle Journal*. **184** 161-174.
- [11] Nagata, M. (1972). *On the automorphism group of  $k[X, Y]$* , Lecture Notes in Mathematics, Tokyo.
- [12] Zariski, O. (1935). *Algebraic Surfaces*. Springer-Verlag.