International Journal of Pure and Applied Mathematics
Volume 86 No. 1 2013, 95-131
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v86i1.9

COMPUTABLE IMPLEMENTATION OF "FUNDAMENTAL THEOREM OF ALGEBRA"

Jon A. Sjogren[1] §, Xinkai Li[2], Mu Zhao[2], Chao Lu[2]

[1]Mail Stop 715, 2308 Mt. Vernon Ave.
Alexandria VA 22301, USA

[2]Department of Computer & Information Sciences
Towson University
8000 York Rd, Towson, MD 21252, USA

Abstract: The Fundamental Theorem of Algebra (FTA) has been studied for more than 300 years: more or less satisfactory proofs of FTA emerged in the 18th and 19th centuries. Proofs denoted as 'algebraic' or 'elementary' derived from the axioms defining a Real-Closed Field (RCF). A proof is given that brings up-to-date work of Gauss (1816) and P. Gordan (1879). It does not refer explicitly to the complex numbers but instead works with auxiliary polynomials in two variables. We report that computer software has been developed to effect symbolic calculation in the context of exact arithmetic. Some examples show how these routines apply to the algebra of symmetric multinomial forms used in Laplace's proof (1795) of FTA, as well as to the theory of Sylvester forms and the Bézoutian formulation of the resultant.

AMS Subject Classification: 08-02
Key Words: Fundamental Theorem Algebra (FTA), Real Closed Field (RCF), symmetric polynomial, symbolic calculation, error-free computing

1. Introduction

The historically important result known as the Fundamental Theorem of Alge-

Received: April 4, 2013

§Correspondence author

bra (FTA), which can also be named the Main Theorem on Complex Polynomials, has been studied for more than 300 years. This proposition states that given a degree $n>0$ and complex numbers $a_0, ..., a_{n-1} \in \mathbb{C}$, if we form the polynomial $P(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_0$, there exists a complex value z_0 which serves as a *zero* for the polynomial considered as a *function*, namely $P(z_0) = 0$.

Until about 1840 it was usual to consider only polynomial functions of the form

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0,$$
$$\text{where all the } a_j \text{ are } \textit{real},\ j = 0, \ldots, n-1.$$

In fact the title of Gausss 1815 monograph was "... every integral rational algebraic function of one variable can be resolved into real factors of the first or second degree." It gradually became understood [27] that effecting this factorization (or solving for a complex root) for $f(X)$ would immediately solve the apparently more general case of (complex coefficients) $P(z)$ referred above.

The more or less satisfactory proofs of FTA that emerged over the 18^{th} and 19^{th} centuries provide a narrative on the state of mathematical technique, and philosophy of rigor. The developing proofs were critical to the history of algebra and complex analysis especially, but also involve logic/model theory, topology and algebraic geometry. An entire book [13] is devoted to an exposition and comparison of the various known classes of proof.

In this article we concentrate on a collection of proofs commonly denoted as algebraic, with a view toward visualizing their steps computationally. The idea is to minimize the need for concepts extraneous to Algebra. It is known that the Theorem when applied to the "standard real numbers" $\mathbb{R}$ requires attention to the transcendental properties of $\mathbb{R}$. These properties, sufficient for FTA, are encapsulated in the axioms for a Real-Closed Field (RCF). Other real-closed fields include the hyper-reals $\mathbb{R}^*$, the "constructive real numbers" and the real algebraic numbers $\mathbb{R}_A$.

An algebraic proof of FTA will apply to $\mathbb{R}$, but equally well to any RCF. In fact a few axioms characterize a real-closed field and the proofs of interest employ these axioms and the rules of first-order predicate calculus. It is discussed in classic papers, owing to [34] and back to [3], that such derivations/theorems embody everything one could say about the real numbers in first-order sentences. Thus any two real-closed fields are *elementarily equivalent*.

We sum up the axioms of RCF somewhat informally. Such a field $\mathbb{F}$ has an ordering compatible with the algebraic field operations, and the non-negative elements are precisely the perfect squares. Besides this (we have so far a "formally real field"), another axiom is needed that takes various forms. For our

purposes, this "Final Axiom" states that any *odd-degree* polynomial $f(X)$ over the field has a root $y \in \mathbb{F}$ with $f(y) = 0$ (functional evaluation). If the axiom holds always for polynomials over $\mathbb{F}$, this field is an RCF.

The formulation of FTA that we take is that for an RCF $\mathbb{F}$, any polynomial $f(X)$ factors into a number of polynomials of degree 1 (linear) and a number of irreducible polynomials of degree 2 (quadratic). Calling factors of the first kind 1-$factors$ and of the second kind 2-$factors$, we are concluding that any polynomial of degree >0 has a complete factorization (and unique up to scalar multiples of the factors), that is, a *complete* $1,2$-$factorization$. In fact since $f(X)$ is taken as *monic*, with leading coefficient equal to 1, all the 1-*and* 2-$factors$ can be taken as *monic* as well (compare "Gauss's Lemma" [20]).

To get Gauss's formulation from 1815, referred to as [16], it is only necessary to show that the standard $\mathbb{R}$ satisfies the last axiom of RCF. This is where the transcendent definition of $\mathbb{R}$ (Bolzano-Weierstrass property) is indispensable. We give sketches of two approaches to this verification, one better known than the other, in the following Section.

A discussion is pursued in the two Eureka articles [22], which shows why, knowing that FTA actually holds (for the standard reals), there *must be* such an 'elementary' or first-order proof. Thus we have miraculously proven, by means of meta-mathematics, that FTA in Gauss's form is immediately valid for other RCF such as the hyper-reals or "constructive real numbers". The Eureka authors suggest that the proof we refer to as Gauss II (1815) is indeed such a proof. Much of the treatment in Gauss II does not appear 'elementary', but it is argued that everything there can be reduced to first-order clauses and derivations. This should not be possible when carrying through less 'algebraic' proofs of FTA, such as one that relies on Brouwer's fixed-point theorem for a Euclidean ball [2], or on a maximum principle for functions on a compact planar domain [2] (see also texts in complex variables such as [21]).

The approach of Gauss II borrows from earlier attempts. The idea is to reduce the "evenness index" μ of the degree of $f(X)$, $deg(f) = n$, where $n = 2^{\mu}(2m+1)$. This insight is associated with de Foncenex, Euler, Lagrange and the 1795 proof of P. S. Laplace. This latter proof, which pointedly exploits a descent on the evenness index using the main theorem of (multivariate) symmetric polynomials, is discussed later in this article from the standpoint of symbolic computation. This proof makes effective use of the field $\mathbb{C}$ of complex numbers and it fact it would be technically intricate to adapt the Laplace proof to the real case $f(X)$ as stated in the title phrase of Gauss II.

The remark attributed to Lagrange in [11] was that finally a proof of FTA fulfilling all expectations had been found, the only flaw being that Laplace's

proof is not amenable to concrete calculation. Software for symbolic calculation developed at Towson University points a way to dealing with the Laplace methods computationally.

Gauss's criticism of the Laplace 1795 proof was based on the latter's assumption of the existence of roots in some domain, then showing these roots must in fact be complex numbers. Gauss carried through another derivation, similar in reducing the evenness index step by step. Historical research revealed that J. Wood 1798 had found a similar method, and a completion of this 'algebraic' proof was sketched out in [30]. Within a broad sweep, the related 'elementary' approaches of Gauss II, Wood and Smithies, [18], [19], [12] and [27], instead of symmetric polynomials, make use of generalized resolvants or resultants. Elliott's critique revealed that in particular J. C. Malet's short paper was over-optimistic and had implicitly assumed the conclusion to be proved. Of all these methods, Gauss II received scholarly attention, Gordan I has been referenced, but the others are hardly referred to subsequently.

In fact the second treatment by Gordan II, 1885, in his compendium on Invariant Theory, is close to the Wood-Smithies proof, certainly giving more detail on the application of the Resultant. Nonetheless there is something to be gained by taking advantage of progress made in the 130 years since Gordan's tome appeared. For instance, it can be useful to work with polynomials and resultants defined over a commutative ring more general than a field, which was not worked out in Gordan's book. The approach of Gauss II and others starts with the definition of the given polynomial over the real field, and we proceed with the construction of 1- and 2-factors without requiring the preconception of a general algebraic closure $\mathbb{C} = \mathbb{R}[\sqrt{-1}]$. Thus we are taking a point of view similar to when imaginary numbers were used, but on an *ad hoc* basis (say before Argand, Cauchy et al).

2. Transcendental Component of FTA

To do an induction on "evenness index" requires a base case which is the "Final Axiom" concerned with odd-degree polynomials. In the case of the standard reals $\mathbb{R}$, this principle is proved with the basic Bolzano-Weierstrass defining property of $\mathbb{R}$, which amounts to the fact that an open interval (a, b) is topologically connected, with topology induced from the usual metric on $\mathbb{Q} \subset \mathbb{R}$.

Let us take $c = \Sigma_{j=0}^{(n-1)} |a_j|$, then we will have

$$f(x) \begin{cases} > c & \text{for } x > 2c + 1 \\ < -c & \text{for } x < -2c - 1, \end{cases}$$

where n is odd, see [21]. Since $c \geq 0$, and $f(x)$ is a continuous function on this interval $(-2c-1, 2c+1)$, it must attain the value 0 at some x_0 in the open interval [10], and hence $f(X)$ has a linear factor $(X - x_0)$.

From examining a large sample of the articles proving FTA, one concludes that all available proofs of FTA, those employing complex variables, Fubini's theorem, or algebraic curves [15], not only the "elementary, algebraic" proofs, use some similar limiting argument. That is, we need a characterization of $f(X)$ when x attains large values, or $x \to \pm\infty$, or a characterization of $P(z)$ as $|z| \to \infty$ is needed. The argument above from Intermediate Value Theorem above is typical.

Attempting a second kind of proof, that the reals $\mathbb{R}$ satisfy the Final real-closed axiom, one can try to keep the argumentation within a "compact" framework. The result we want would follow if we knew that every linear transformation A (endomorphism) of $\mathbb{R}^n$ (for n odd) has a real eigenvalue λ. The reason is that $f(X)$ may be encoded into a *companion matrix*,

$$A = \begin{pmatrix} 0 & \cdots & & -a_0 \\ 1 & 0 & & -a_1 \\ & 1 & 0 & \cdots \\ & & 1 & -a_{n-1} \end{pmatrix}.$$

If there is a vector $\vec{v} \in \mathbb{R}^n$ with $A\vec{v} = \lambda\vec{v}$, $\lambda \in \mathbb{R}$, then $f(\lambda) = 0$, using $f(X) = \chi_A(X) = |(X \cdot I - A)|$. As a transformation, either A is singular (so has $\lambda = 0$ as eigenvalue), or else A restricted to $\mathbb{S}^{n-1} \subset \mathbb{R}^n$ can be normalized to give a continuous mapping $T : \mathbb{S}^{n-1} \to \mathbb{S}^{n-1}$. Supposing that non-singular A has no eigenvector $\vec{v}$, then T never maps any vector $\vec{y} \in \mathbb{S}^{n-1}$ to $\vec{y}$ (itself) nor to its opposite (antipode) $-\vec{y}$. Hence by construction of a homotopy [10], T is freely homotopic amongst mappings $\phi : \mathbb{S}^{n-1} \to \mathbb{S}^{n-1}$ both to the identity mapping of $\mathbb{S}^{n-1}$ and also to the antipodal mapping $\vec{y} \to -\vec{y}$. But when $n-1$ is even, these two mappings are not homotopic to each other: the one has Brouwer degree =1, the other has degree equal to $(-1)^n = -1$. Thus an eigenvector $\vec{v}$ for A, hence an eigenvalue λ, and a real root of $f(X)$ must exist.

We have introduced distinctly non-elementary concepts with "degree" and "homotopy" of mappings. One can reach the same conclusion with more primitive tools by resorting to the "cueball" theorem as proved in [29] using ideas from foliation theory due to D. Asimov. Only the calculus of volumes is used, together with the contraction mapping principle. Suppose as before, that when computing $T(\vec{y})$, neither $\vec{y}$ nor $-\vec{y}$ ever comes up. Then the projection of $T(\vec{y})$ onto the tangent plane of $\mathbb{S}^{n-1)}$ (just the set of vectors $\vec{u}$ orthogonal to $\vec{y}$, $\vec{u} \cdot \vec{y} = 0$) always gives a non-zero vector, in fact one bounded away from zero

by compactness. Normalizing this vector yields a *unit* vector field on $\mathbb{S}^{n-1}$, which is impossible by the "combing flat the cueball" theorem when $n > 0$ is an odd integer.

Appealing to one of these two transcendental arguments, we see that the field of standard real numbers as defined by Dedekind, or through Cauchy sequences, satisfies the Final Axiom of RCF, that odd-degree polynomials possess a root (zero).

3. Basic Determinantal Forms

As far as it is useful in the Theory of Equations, the "Resultant", or Sylvester's determinant, can be approached from distinct directions. The origins of the construction must lie in the ancient algorithm for finding a common factor of counting numbers, attributed to Euclid. Given polynomials $f(X), g(X)$ in one variable, of various degrees, one may carry out the well-known procedure of successive remainders, until arriving at a non-zero scalar, indicating that f and g are relatively prime in $\mathbb{F}[X]$. This actually happens only when a determinant, namely the specialization of the appropriate Sylvester (or Bézout) form, does not compute to 0.

We will have to use the Resultant not only over the real numbers, but also when the scalars can take values in an arbitrary (commutative with 1) integral domain. This is the small price to pay for giving up a reliance on everything being embedded in the complex field $\mathbb{C}$. The conclusion that FTA (first- and second-order complete factorization) holds for a general real-closed field will follow as well as for the "standard reals".

In other words, if the special determinant whose entries come from f, g vanishes, the Euclid algorithm cannot be carried through to a scalar residue, it terminates 'prematurely' at 0. This means precisely that over $\mathbb{H}[X]$, the two polynomials possess a common factor of degree 1 (linear, '$x + b$') or higher, where $\mathbb{H}$ is the coefficient domain.

P. Gordan several times declares, "Vanishing of the resultant means the existence of a common linear factor". This statement is true if $\mathbb{H}$ is the complex numbers $\mathbb{C}$ and if we accept the truth of FTA as given. Otherwise such a statement may have caused a misunderstanding in the paper of [27], see comments by [12], and elsewhere. In fact there are similar resultant-like forms that detect for the presence of common factors of degree 2 and higher. Thus if 1-Res, the ordinary resultant, vanishes and the 2-Res does not vanish, there must exist what is called a common linear factor of $f(X)$ and $g(X)$ over $\mathbb{H}$. Exploitation

in Algebra of these "higher" resultants has apparently been rather limited.

A more direct approach to the resultant of two polynomials is followed in texts such as [36] or [24]. The Sylvester form is defined, and an identity $Af + Bg = R(f, g)$ is derived. The polynomial $A(X)$ is of *degree* $\leq m-1$, and $degB \leq n-1$ where $deg(f) = n,\ deg(g) = m$. The identity shows that f and g do have a common factor of at least degree 1. In completing the argument, we defer to the treatment given in the classic texts.

Now we sketch out the construction of the multi-variate forms we need. Given commuting indeterminates $u_0, \ldots, u_n, v_0, \ldots, v_m$, we define

$$\mathcal{S}_{ij} = \begin{cases} u_{(j-i)} & \text{for } i = 1, \ldots, m \\ v_{(m+j-1)} & \text{for } i = m+1, \ldots, m+n, \end{cases} \qquad (A)$$

which gives an $(m+n) \times (m+n)$ matrix called the *Sylvester* matrix. The *Sylvester* form $\mathcal{R} = |[\mathcal{S}]|$ will be an element in the multivariate polynomial ring $\mathbb{H}[u_0, \ldots, u_n, v_0, \ldots, v_m]$.

Example 1. $\mathcal{S}(u_0, u_1, v_0, v_1) = [u_0, u_1; v_0, v_1]$,

$$\mathcal{S}(u_0, u_1, u_2, v_0, v_1, v_2, v_3) = \begin{bmatrix} u_0 & u_1 & u_2 & 0 & 0 \\ & u_0 & u_1 & u_2 & 0 \\ & & u_0 & u_1 & u_2 \\ v_0 & v_1 & v_2 & v_3 & 0 \\ & v_0 & v_1 & v_2 & v_3 \end{bmatrix}.$$

Notice how the main diagonal consists of m copies of u_0 and n copies of v_m.The following results from the literature sum up the issue of factorization.

Letting $f, g \in \mathbb{H}[X]$ be given by

$$f(X) = a_0 X^n + a_1 X^{n-1} + \cdots + a_n,$$

$$g(X) = b_0 X^m + b_1 X^{m-1} + \cdots + b_m.$$

We define the *resultant* $\mathcal{R}(f, g)$ to be the specialization of $\mathcal{S}_{\{n,m\}}$ to the sectors of coefficients of f, respectively g. In other words, we substitute a_j for u_j and b_j for v_j in the Sylvester form of the appropriate size. In our proof of FTA the coefficient ring $\mathbb{H}$ will either be a field, a polynomial ring over some field, in any case a U.F.D. (unique factorization domain).

In fact we have a version of the Main Theorem of Resultant Theory [6].

Theorem 1. *If* $\mathbb{H}$ *is a UFD then* $(f, g) \equiv$ *greatest common divisor over* $\mathbb{H}[X]$ *has degree* ≥ 1*, if and only if* $\mathcal{R}(f, g) = 0$.

Example 2. Consider $\mathbb{H} = \mathbb{R}[u]$ a polynomial ring with real coefficients. Let $f(X) = X^3 + u, g(X) = X^2 - u$, then

$$\mathcal{R}_{f,g} = |\mathcal{S}| = \begin{vmatrix} 1 & 0 & 0 & u & 0 \\ 0 & 1 & 0 & 0 & u \\ 1 & 0 & -u & 0 & 0 \\ 0 & 1 & 0 & -u & 0 \\ 0 & 0 & 1 & 0 & -u \end{vmatrix}.$$

We obtain $\mathcal{R}(u) = u^2 - u^3$ whose roots are $u = 0$ (doubled) and $u = +1$. These show at which parameters u, that f and g have a common factor. In fact for $u_1 = 1$, we have $f(X, u_1) = X^3 + 1, g(X, u_1) = X^2 - 1$ with the common factor $h(X) = X + 1$.

We may say that projecting to the quotient field $\mathbb{E}$,

$$\phi : \mathbb{H} \to \mathbb{H}/(u - 1) \simeq \mathbb{E}.$$

We have a common factor for $\phi(f)$ and $\phi(g)$ in $\mathbb{E}$. Thus we have "found" a common factor of f, g in a quotient ring of $\mathbb{H}$, namely the field $\mathbb{E} \simeq \mathbb{R}$, the standard real numbers.

Example 3. Taking $\mathbb{H} = \mathbb{R}[u]$ consider

$$f_1(X, u) = u^2 - X^2,$$

$$f_2(X, u) = u^3 - X^3.$$

We form the resultant over the "indeterminate" X,

$$\mathcal{R}_{f_1,f_2}(u) = \begin{vmatrix} -1 & 0 & u^2 & 0 & 0 \\ 0 & -1 & 0 & u^2 & 0 \\ 0 & 0 & -1 & 0 & u^2 \\ -1 & 0 & 0 & u^3 & 0 \\ 0 & -1 & 0 & 0 & u^3 \end{vmatrix}.$$

This determinant evaluates identically to 0, so we conclude that for *all* values of u chosen in $\mathbb{R}$, there is a common factor of f_1, f_2 of *degree* ≥ 1. As we know,

$$f_1(X, u) = (u - X)(u + X),$$

$$f_2(X, u) = (u - X)(u^2 + uX + X^2).$$

So this result was expected.

4. Properties of the Resultant

The classic text of P. Gordan, *Invariantentheorie* (1885) demonstrates many properties within the context of the theory of determinants and other invariants. Only a few of these bear directly on our modified proof of FTA for real polynomials. With full appreciation for Gordan's lively style, in some cases the treatment can be made more understandable to the modern reader.

Recall that a multi-variant polynomial $G(y_0, \ldots, y_n)$ is called *homogeneous* of degree d if all the terms of G, typically

$$c_{\alpha(0),\alpha(1),\ldots,\alpha(n)} y_0^{\alpha(0)} \ldots y_n^{\alpha(n)}$$

possess the same total degree $= \sum_{j=0}^{n} \alpha(j)$, recorded as long as

$$c_{\alpha(0),\alpha(1),\ldots,\alpha(n)} y_0^{\alpha(0)} \ldots y_n^{\alpha(n)} \neq 0.$$

It is well-known [6] that

Proposition 1. The polynomial $G \in \mathbb{H}[y_0, \ldots, y_n]$ is homogeneous of degree d if and only if for any scalar $\lambda \in \mathbb{H}$ we calculate

$$G(\lambda y_0, \ldots, \lambda y_n) = \lambda^d G(y_0, \ldots, y_n).$$

Proposition 2. The Sylvester form $\mathcal{R} = |\mathcal{S}(u_0, \ldots, u_n, v_0, \ldots, v_m)|$ is homogeneous of degree $m + n$.

Proof. The Sylvester matrix has size $(m+n)\times(m+n)$. Substituting λu_0 for u_0, λv_j for v_j etc, everywhere in this matrix has the effect of multiplying each row of S the scalar $\lambda \in \mathbb{H}$. Now by fundamental property of the determinant "form", we have

$$\mathcal{R}(\lambda u_0, \ldots, \lambda v_m) = \lambda^{m+n} \mathcal{R}(u_0, \ldots, v_m).$$

Hence by Proposition 1, $\mathcal{R}$ is homogeneous of degree $m + n$.

Definition 1. The *weight* of a multi-variable term

$$M = c_{\alpha(0),\alpha(1),\ldots,\alpha(n),\beta(0),\beta(1),\ldots,\beta(m)} u_0^{\alpha(0)} \ldots u_n^{\alpha(n)} v_0^{\beta(0)} \ldots v_m^{\beta(m)}$$

is defined as $w(M) = \Sigma_{i=0}^{n} i\cdot\alpha(i) + \Sigma_{j=0}^{m} j\cdot\beta(j)$. Thus for example, $(u_0^2 u_1^3 u_2^2 v_0^5 v_1^2 v_3^2) = 7 + 8 = 15$.

Definition 2. A form consisting of terms $f = r_1 M_1 + \cdots + r_t M_t$ is said to be *isobaric* of weight p if $r_j \neq 0$ implies $w(M_j) = p$ for $j = 1, \ldots, t$.

Proposition 3. The Sylvester form $R = |S(u_0, \ldots, u_n, v_0, \ldots, v_m)|$ is isobaric of weight mn.

Proof. Every term in $\mathcal{R}$ can be expressed according to the defining expansion of a determinant. Let $M = \pm\Pi_{i=1}^{m+n}[\mathcal{S}]_{i\sigma(i)}$ be a typical term arising from a permutation $\sigma \in S_{m+n}$. Formula (A) above allows these factors to be rewritten as

$$M = \Pi_{i=1}^{m} u_{\sigma(i)-i} \cdot \Pi_{i=m+1}^{m+n} v_{m+\sigma(i)-i}.$$

Note that for example $w(u_j^3) = 3w(u_j)$, so we obtain

$$w(M) = \Sigma_{i=1}^{m}\sigma(i) - i + \Sigma_{i=m+1}^{m+n}(m + \sigma(i) - i) = \Sigma_{i=m+1}^{m+n} m = mn.$$

Example 4.

$$\mathcal{S}(u_0, u_1, u_2, v_0, v_1, v_2) = \begin{vmatrix} u_0 & u_1 & u_2 & 0 \\ & u_0 & u_1 & u_2 \\ v_0 & v_1 & v_2 & 0 \\ & v_0 & v_1 & v_2 \end{vmatrix}$$

$= u_0^2v_2^2 - u_0u_1v_1v_2 + u_0u_2v_1^2 - u_0u_2v_0v_2 + u_1^2v_0v_2 - u_0u_2v_0v_2 - u_1u_2v_0v_1 + u_2^2v_0^2$, which is indeed homogeneous of degree $m+n = 4$ and isobaric of weight $mn = 4$.

We move on to a discussion of how the resultant applies to a polynomial in two variables. A useful result is:

Proposition 4. "Gordan's Lemma" Let $\lambda \in \mathbb{H}$ be a coefficient ring and f, g polynomials in x as above. Then $\mathcal{R}(f + \lambda g, g) = \mathcal{R}(f, g)$. Thus a scalar multiple of the second argument can always be added to the first argument of the resultant, without changing its value. Take first the case $m \leq n$.

Proof. As a typical instance we deal with

$$\mathcal{R}(f + \lambda g, g) =$$

$$\begin{vmatrix} a_0 & a_1 & \dots & \lambda b_0 + a_j & \lambda b_1 + a_{j+1} & \dots \\ & a_0 & & & \lambda b_0 + a_j & \dots \\ & & \dots & \dots & \dots & \\ b_0 & b_1 & \dots & b_{j+1} & b_m & \dots \\ & b_0 & & & & \\ & & b_0 & & & \\ & & & \dots & & \\ & & & & b_0 & b_m \end{vmatrix}.$$

As the array suggests, the $m + j + 1$ -st row when multiplied by $-\lambda$ and added to the first row, $m + j + i$ row multiplied by $-\lambda$ and added to the i-th row, $i = 2, \dots, n$. This results in the usual expression for $\mathcal{R}(f, g)$. The case of n<m can be treated similarly.

Consideration of homogeneous polynomials can help determine whether a resultant may be equal to 0. In fact the generator u in $\mathbb{H} = \mathbb{R}[u]$ can be

considered an indeterminate, a factor for a multi-variate polynomial over $\mathbb{R}$. We can make use of the natural isomorphism $\mathbb{F}[Y][X] \simeq \mathbb{F}[X,Y]$, where $\mathbb{F}$ is some ordered field. Given $f(X,Y)$ and $g(X,Y)$, define $\mathcal{R}_X(f,g)$ as if the polynomials are in the one variable X, but defined over the polynomial ring $\mathbb{F}[Y]$.

In the case that f and g are homogeneous in X and Y, we have a useful result. Similar statements also apply when the indeterminates are more numerous, see [6]. Write

$$f(X,Y) = a_0(Y)X^n + a_1(Y)X^{n-1} + \cdots + a_n(Y), \qquad (I)$$

$$g(X,Y) = b_0(Y)X^n + b_1(Y)X^{n-1} + \cdots + b_n(Y),$$

where $a_j(Y)$, $b_j(Y)$ have degree equal to j in Y. Then $f(X,Y)$, $g(X,Y)$ are homogeneous of degrees n and m respectively.

Proposition 5. In this (homogeneous) case, we have $\mathcal{R}_X(f,g)$ equal to a homogeneous polynomial in the "remaining variable" Y, hence a monomial cY^{mn} where $c \in \mathbb{F}$. It is possible that $c = 0$.

Example 5. Take $f(X,Y) = X + Y, g(X,Y) = X^3 + Y^3$, then we compute $\mathcal{R}_X(f,g) \equiv 0$.

Proof. Each term of $\mathcal{R}_X(f,g)$ is of the form $M = a_{s_\mathbf{1}} a_{s_\mathbf{2}} \ldots$ $a_{s_m} b_{t_\mathbf{1}} b_{t_\mathbf{2}} \ldots b_{t_n}$ where $0 \leq s_\rho \leq n$, $0 \leq t_\varepsilon \leq m$, some of the indices possibly being repeated. By Proposition 3, the corresponding term of the determinant, that is in $\mathcal{S}_X(f,g)$ is *isobaric* of weight mn, hence

$$\Sigma_{\rho=1}^{ms_\rho} + \Sigma_{\epsilon=1}^{nt_\epsilon} = mn.$$

But the degree of a_{s_l} is just s_l, that is $a_{s_l} = c_{s_l} Y^{s_l}$ with $c_{s_l} \in \mathbb{F}$, so the degree of the factor M is just mn as well.

Taking the resultant of two homogeneous polynomials in several variables is important in algebraic geometry as it provides a method for describing the locus of the intersection of two projective curves in the plane (or more generally, two hyper-surfaces). Returning to consideration of $f(X,Y)$, this polynomial might not turn out to be homogeneous. But in any case f does have a non-zero homogeneous summand consisting of all terms of highest total degree. We can name this the *principal* part $f_P(X,Y)$. In particular,

$f(X,Y) = a_0(Y)X^d + a_1(Y)X^{d-1} + \cdots + a_d(Y) + f\_(X,Y)$, where $a_j(Y)$ has degree j in Y, and $f\_(X,Y)$ consists of terms having total degree less than d. Thus we have $f(X,Y) = f_P(X,Y) + f\_(X,Y)$.

Example 6. Consider $f(X,Y) = X^2 + 2XY - X + 3Y$, then $f_P = X^2 + 2XY$ and $f\_ = -X + 3Y$.

Proposition 6. If $\mathcal{R}_X(f,g)$ vanishes identically in Y, so does $\mathcal{R}_X(f_P,g_P)$, the resultant of the principal parts.

Proof. Start with the assumption that the terms of the Sylvester form specialized for f_P, g_P add up to αY^{mn} where α is non-zero. A typical unspecialized term is

$$\tilde{M} = u_{s_1}u_{s_2}\dots u_{s_m}v_{t_1}v_{t_2}\dots v_{t_n}, 0 \le s_\rho \le n, 0 \le t_\epsilon \le m,$$

and $\Sigma_1^m s_\rho + \Sigma_1^n t_\epsilon = mn$ by Proposition 3. To get the corresponding term of $\mathcal{R}_X(f,g)$ or $\mathcal{R}_X(f_P,g_P)$, one must substitute the coefficients $a_j(Y)$, $b_j(Y)$ as in formula (I), for the vectors $\vec{u}$ and $\vec{v}$ respectively. In the case of the homogeneous terms of highest degree n and m, we know that

$$\begin{aligned} &deg\ a_j(Y) = j \text{ since } a_j(Y) = c_jY^j, \\ &deg\ b_j(Y) = j \text{ since } a_j(Y) = e_jY^j. \end{aligned}$$

These terms of *degree* (n,m) from (f_P,g_P) contribute a term to the resultant namely $M_P = a_{s_1}a_{s_2}\dots a_{s_m}b_{t_1}b_{t_2}\dots b_{t_n} = \theta Y^{mn}$, $\theta \in \mathbb{F}$. Now in replacing f_P by $f_P + f_- = f(X,Y)$, g_P by $g(X,Y)$, we examine what effect the additional lower-degree terms will have on $M_P \mapsto M$. It is elementary, observing the product in the expression for M_P, that each such resulting term will have degree strictly less than mn. For instance we have $b_{t_k} = e_{t_k}Y^{t_k}$ in g_P. In the original $g(X,Y)$, the corresponding coefficient of X^{m-t_k} will be $\tilde{b}_{t_k} = e_{t_k}Y^{t_k} + \gamma_1 Y^{\tau_1} + \gamma_2 Y^{\tau_2} + \dots$, where all $\tau_i < t_k$. Hence the terms in Y^s of lower degree than called for in $a_j(resp.\ b_j)$ have no effect on the homogeneous part of $\mathcal{R}_X(f_P,g_P)$.

A sharper way of phrasing this result in two variables would be given next.

Proposition 6'. If $\mathcal{R}_X(f_P,g_P) = cY^{mn}$ then $\mathcal{R}_X(f,g) = cY^{mn} + \Sigma_{k=0}^{mn-1}\delta_k Y^k$; in other words, the highest degree term of a resultant, and the resultant of the homogeneous parts, are equal.

This Proposition has an analog for any number of variables $X_1,\dots,X_r$, where we examine $\mathcal{R}_{X_1}(f,g)$ as a polynomial in $X_2,\dots,X_r$. As indicated above, the proof of this analog, with its applications to higher algebraic geometry, is certainly more involved than our proof of Proposition 6.

We can now state the Fundamental Theorem of Elimination Theory over a commutative (unique factorization) domain $\mathbb{H}$.

Theorem 2. *Let*

$$f(X) = a_0X^n + a_1X^{n-1} + \dots + a_n,$$

$$g(X) = b_0X^m + b_1X^{m-1} + \dots + b_m, \tag{1}$$

$$a_i, b_j \in \mathbb{H},\ a_0 \neq 0, b_0 \neq 0.$$

Then f and g have a common polynomial factor, which has degree one or greater, if and only if $\mathcal{R}_X(f,g) = 0$.

Proof. This can be derived from the relation

$$A(X)f(X) + B(X)g(X) = \mathcal{R}_X(f,g), \tag{2}$$

holding for certain polynomials with $degA \leq m-1, degB \leq n-1$. For full details see the discussion in [36], [24], and [6].

A proof-sketch of the above result (2) is as follows,

$$\mathcal{R}(f,g) = \begin{vmatrix} a_0 & a_1 & \dots & a_j & a_{j+1} & \dots \\ & a_0 & a_1 & \dots & a_j & \dots \\ & & & & \dots & \dots \\ & & & & \dots & a_n \\ b_0 & b_1 & \dots & b_j & b_{j+1} & \dots \\ & b_0 & b_1 & \dots & b_j & \dots \\ & & & & \dots & \dots \\ & & & & \dots & b_m \end{vmatrix} \begin{matrix} \\ \\ m \\ \\ \\ \\ n \\ \\ \\ \\ \end{matrix}.$$

This was just the canonical Sylvester manner of writing the resultant found in most of the classic texts. Now we change the appearance of this determinant without altering its value. We multiply the first column by $X^{(n+m-1)}$ and add the result to the last column of $\mathcal{R}(f,g)$; next we multiply the second column by X^{n+m-2} and add the result to the (new) final, $(n+m)$-*th* column, and so forth, the $n+m-1$ column being multiplied by X^1 and added to the (revised!) final column. This process now results in the matrix of $\mathcal{R}(f,g)$ being unchanged, except for the final column which appears as follows. We may express the column as a (transposed) row vector:

$$[X^{m-1}f(X), X^{m-2}f(X), \dots, f(x), X^{n-1}g(X), X^{n-2}g(X), \dots, g(X)]^T.$$

Expanding the new picture of $\mathcal{R}$, a determinant, by its final column gives a linear combination over $\mathbb{H}$ of the expressions $X^j f(X)$, $X^k g(X)$ above so as to equal $\mathcal{R}_X(f,g)$, which is formula (2).

Remark: Now we are prepared to show that any polynomial of degree $n \geq 1$ over a real-closed field $\mathbb{F}$, breaks into irreducible factors of degree 1 and degree 2. No specific reference is made to a *field* extension such as $\mathbb{F}[\sqrt{-1}]$, although *a field properly containing* $\mathbb{F}$ is usually constructed as part of the proof. Again, the proof of this factorization theorem is **valid** for $\mathbb{F}$ = real algebraic numbers,

hyper-reals, "definable numbers", the field of Puiseux series, etc., that is, to any real-closed field (RCF).

Contemporary work on an "elementary proof" of FTA should be based on something more than a desire further to simplify Gauss II. The steps of the present article should be constructible according to the first-order predicate calculus, at least in principle. The major results of resultant theory and homogeneous forms should be seen to be expressible in terms of 1^{st} order real-field theory, with plenty of new variables, constants and predicates available to define. It was claimed by [35] that the Sturmian theory [33] of zero sequences could be so formalized. Either of these two projects would be a daunting undertaking in practice.

5. Quadratic Fields over $\mathbb{R}$

We collect some results pertaining to a domain designated

$$\mathbb{D}_u = \mathbb{R}[u]/(u^2 + su + t),\ s, t \in \mathbb{R},$$

where $\mathbb{R}$ constitutes the standard reals, or without loss of generality, some other real-closed field $\mathbb{F}$. Also, u is an indeterminate and we take it that $s^2 < 4t$ so the discriminant of $\lambda(u) = u^2 + su + t$ is negative, and hence $\lambda(u)$ is irreducible over $\mathbb{F}$.

The point of view taken is that the concept of "the complex numbers $\mathbb{C}$" has not been fully developed, at least for certain RCF, and thus we treat specific field extensions such as $\mathbb{D}_u$. Working in a polynomial ring modulo $\lambda(u)$, we use only the simplest "field" constructions. Later one could prove that all these fields are isomorphic to $\mathbb{F}(\sqrt{-1})$, but "field isomorphism" is not really relevant to our approach toward FTA as this concept cannot be formulated within the predicates of the theory of RCF.

Now it is easy to show that $w \in \mathbb{D}_u$ can be written uniquely as $\gamma + \delta u$, with $\gamma, \delta \in \mathbb{F}$, by reducing a given polynomial in u modulo $\lambda(u)$ a number of times. Furthermore there is a *conjugation operator*

$$\chi : \mathbb{D}_u \to \mathbb{D}_u$$

defined by $\chi(t) = t, t \in \mathbb{F}$, and $\chi(u) = \bar{u} = -u - s$, extended by linearity. Note that $\chi(-u - s) = -(-u - s) - s = u$, so $\chi^2 = \mathbf{id}$, and we have an involution on $\mathbb{D}_u$.

χ-**Property 1.** Summing up, we have $\gamma + \delta u \xrightarrow{\chi} \gamma - \delta u - \delta s$.

χ-**Property 2.** $\overline{(w_1 + w_2)} = \chi(w_1 + w_2) = \chi(w_1) + \chi(w_2) = \overline{w_1} + \overline{w_2}$.

χ-**Property 3.** $\overline{w_1 w_2} = \bar{w_1}\bar{w_2}$.

Proof. We have $w_1 w_2 = \gamma_1\gamma_2 - \delta_1\delta_2 t + (\gamma_1\delta_2 + \gamma_2\delta_1 - \delta_1\delta_2 s)u$, hence $\chi(w_1 w_2) = \overline{w_1 w_2} = \gamma_1\gamma_2 - \delta_1\delta_2 t + (\gamma_1\delta_2 + \gamma_2\delta_1 - \delta_1\delta_2 s)u - (\gamma_1\delta_2 - \delta_1\delta_2 s)s$.

On the other hand $\overline{w}_1\overline{w}_2 = (\gamma_1 - \delta_1 u - \delta_1 s)\cdot(\gamma_2 - \delta_2 u - \delta_2 s) = \gamma_1\gamma_2 - \gamma_1\delta_2 s - \gamma_2\delta_1 s + (-\delta_1\gamma_2 + \delta_1\delta_2 s - \delta_2\gamma_1 + \delta_2\delta_1 s)u + \delta_1\delta_2(-su - t) + \delta_1\delta_2 s^2$.

By comparing terms we observe that

$$\chi(w_1 w_2) = \chi(w_1)\chi(w_2).$$

Definition 3. An element $w \in \mathbb{D}_u$ is *real* if $w = \gamma + \delta u$ with $\delta = 0$.

χ-**Property 4.** The element w is real if and only if $\bar{w} = w$.

Proof. If w is real, $\delta = 0$ so $\overline{w} = \gamma = w$. conversely if $\bar{w} = w$, we have $-\delta u - \delta s = \delta u$ which by uniqueness of the representation gives $2\delta = 0$. Since an ordered field has no torsion elements we conclude that $\delta = 0$.

Next, we need to define conjugation applied to a polynomial $f(X) \in \mathbb{D}_u[X]$. Letting $f(X) = c_0 X^n + c_1 X^{n-1} + \cdots + c_n$ with $c_j \in \mathbb{D}_u, j = 0, \ldots, n$, we define

$$\chi(f) = \bar{f}(X) = \bar{c}_0 X^n + \bar{c}_1 X^{n-1} + \cdots + \bar{c}_n,$$

and say that $f \in \mathbb{D}_u[X]$ is real if the coefficients $c_j \in \mathbb{D}_u$ are real, that is $c_j = \bar{c}_j$ for all j. From the definitions we have:

χ-**Property 5.** The polynomial $f(X)$ is real if and only if $f = \bar{f}$. Next we treat the polynomial operations.

χ-**Property 6.** If $g(X) = f_1(X) + f_2(X), k(X) = f_1(X) f_2(X)$, then $\overline{g}(X) = \overline{f}_1(X) + \overline{f}_2(X), \overline{k}(X) = \overline{f}_1(X)\overline{f}_2(X)$.

Proof. The coefficient in the sum for X^j is the sum of the corresponding coefficients and its conjugate equals the sum of their conjugates, so we have the first result by χ-**Property 2**. For the product of two polynomials, its coefficients arise as entries in the convolution of two sequences indexed by $\mathbb{N}$, each with finitely many (bounded in number by the degree) non-zero entries. The convolution is computed as the sum of the products each of two factors, and conjugation is respected, according to χ-**Property 2** and χ-**Property 3**, by both sum and product operations.

χ-**Property 7.** If $f(X)$ divides real $h(X) \in \mathbb{R}[X]$ so does $\overline{f}(X)$.

Proof. If $h(X) = f(X)g(X)$, conjugating both sides leads by χ-**Property 6** to the co-factor $\overline{g}(X)$ for $\bar{f}(X)$ in $h(X)$, where we may use χ-**Property 5** since h is real as a polynomial.

Note. There is no harm in writing $\overline{\phi(X)}$ instead of $\overline{\phi}(X)$ since X is unaffected by conjugation. However, if X is replaced by another expression in $\mathbb{D}_u[X]$ it is best to apply the following.

χ-**Property 8.** If $h(X) = f(g(X))$, then $\overline{h}(X) = \overline{f}(\overline{g}(X))$.

Proof. As a polynomial, $f(X)$ is a linear combination of powers of X , so $\bar{h}(X)$ will be a sum of terms typically $\bar{c}_j\overline{g(X)^j}$ so the problem reduces to "the conjugate of the power of a polynomial is equal to the same power taken of the conjugate" which is proved by induction on the power j, using χ-**Property** 6.

6. FTA by the Method of Laplace

In 1795, Laplace offered a convincing algebraic proof of FTA. In his proof, he used the theorem on symmetric functions which was proved by Newton in 1673, it has also been known as fundamental theorem of symmetric polynomials. Before introducing the fundamental theorem of symmetric polynomials, several definitions need to be given.

Definition 4. A symmetric polynomial is a polynomial $P(X_1, X_2, \ldots, X_n)$ in n variables, such that if any two of the variables are interchanged, one obtains the same polynomial.

Formally, $P(X_1, X_2, \ldots, X_n)$ is a symmetric polynomial, if for any permutation of the subscripts $1, 2, \ldots, n$, one has the same polynomial $P(X_1, X_2, \ldots, X_n)$. For example, in two variables X_1, X_2, a symmetric polynomial could appear as:

$$5X_1^2X_2^2 + X_1^2X_2 + X_2^2X_1 + (X_1 + X_2)^2.$$

There are many ways to make specific symmetric polynomials in any number of variables such as $\prod_{1\le i\le j\le n}(X_i - X_j)^2$.

Definition 5. The elementary symmetric polynomials in n variables $X_1 \ldots X_n$, written as $e_i(X_1, \ldots, X_n)$ for $i = 0, 1, \ldots, n$, can be defined as

$$e_0(X_1, X_2, \ldots, X_n) = 1, \quad e_1(X_1, X_2, \ldots, X_n) = \sum_{1\le j\le n} X_j,$$

$$e_2(X_1, X_2, \ldots, X_n) = \sum_{1\le j\le k\le n} X_jX_k.$$

And so forth, down to: $e_n(X_1, X_2, \ldots, X_n) = X_1X_2 \ldots X_n$

In general, for $k \ge 0$ we define

$$e_k(X_1, \ldots, X_n) = \sum_{1\le j_{\mathbf{1}}<j_{\mathbf{2}}<\cdots<j_k\le n} X_{j_{\mathbf{1}}}, \ldots, X_{j_k}.$$

The elementary symmetric polynomials, power sum symmetric polynomials and complete homogeneous symmetric polynomials are three basic blocks of symmetric polynomials used to generate the ring of symmetric polynomials in n variables.

The fundamental theorem of symmetric polynomials

Theorem 3. *Any symmetric polynomial can be expressed as a polynomial in the elementary symmetric polynomials on those variables.*

Proof. First, we review the definition of lexicographic order. The symmetric polynomial $P(x_1 \ldots, x_n)$can be expressed as the sum of monomials of the form as $cx_1^{i_\mathbf{1}} \ldots x_n^{i_n}$, where i_k is a nonnegative integer. Then, the order on the monomials can be defined by specifying that $c_1 x_1^{i_\mathbf{1}} \ldots x_n^{i_n} < c_2 x_1^{j_\mathbf{1}} \ldots x_n^{j_n}$, when $c_2 \neq 0$ and there is some $0 \leq k \leq n-1$ such that $i_{n-l} = j_{n-l}$ for $l = 0, 1, \ldots, k-1$ but $i_{n-k} < j_{n-k}$. For instance, $5x_1^2 x_2^3 x_3^6 < 8x_1 x_2^4 x_3^6$. In other words, starting in the nth position in both monomials, go back until the two exponents are not equal. The monomial with the larger exponent in that position has higher order. This is called a lexicographic order on the monomials.

Suppose that $cx_1^{i_\mathbf{1}} \ldots x_n^{i_n}$ is the largest monomial in P. Then we must have $i_1 \leq i_2 \leq \cdots \leq i_n$, otherwise this monomial is not the largest one of P, because when P is symmetric, the polynomial P must also have the monomial $cx_1^{j_\mathbf{1}} \ldots x_n^{j_n}$, where $(j_1, j_2, \ldots, j_n)$ is the sequence $(i_1, i_2, \ldots, i_n)$ sorted in increasing order. But this monomial is larger than the monomial $cx_1^{i_\mathbf{1}} \ldots x_n^{i_n}$ unless we have $i_1 \leq i_2 \leq \cdots \leq i_n$. Thus, we can define a symmetric polynomial R by $R = ce_1^{i_n - i_{n-\mathbf{1}}} e_2^{i_{n-\mathbf{1}} - i_{n-\mathbf{2}}} \ldots e_{n-1}^{i_\mathbf{2} - i_\mathbf{1}} e_n^{i_\mathbf{1}}$, where e_k is the k^{th} elementary symmetric polynomial in the n variables $x_1, \ldots, x_n$. So that R is a polynomial in the elementary symmetric polynomials. Also we can prove that the largest monomial of R equals to $cx_1^{i_\mathbf{1}} \ldots x_n^{i_n}$. Because the largest monomial of $R = ce_1^{i_n - i_{n-\mathbf{1}}} e_2^{i_{n-\mathbf{1}} - i_{n-\mathbf{2}}} \ldots e_{n-1}^{i_\mathbf{2} - i_\mathbf{1}} e_n^{i_\mathbf{1}}$ equals to:

$$
\begin{aligned}
&c \cdot (\textit{largest monomial of } e_1)^{i_n - i_{n-\mathbf{1}}} \cdot (\textit{largest monomial of } e_2)^{i_{n-\mathbf{1}} - i_{n-\mathbf{2}}} \\
&\quad \ldots (\textit{largest monomial of } e_{n-1})^{i_\mathbf{2} - i_\mathbf{1}} \cdot (\textit{largest monomial of } e_n)^{i_\mathbf{1}} \\
&\quad = c(x_n)^{i_n - i_{n-\mathbf{1}}} (x_{n-1} x_n)^{i_{n-\mathbf{1}} - i_{n-\mathbf{2}}} \ldots (x_2 x_3 \ldots x_n)^{i_\mathbf{2} - i_\mathbf{1}} (x_1 x_2 x_3 \ldots x_n)^{i_\mathbf{1}} \\
&\quad = cx_1^{j_\mathbf{1}} \ldots x_n^{j_n}, \text{ since } e_k(X_1, \ldots, X_n) = \textstyle\sum_{1 \leq i_\mathbf{1} \leq i_\mathbf{2} \leq \cdots \leq i_k \leq n} X_{i_\mathbf{1}} \ldots X_{i_k} \text{ is the}
\end{aligned}
$$

k^{th} elementary symmetric polynomial.

Therefore, we reduce $P(x_1, \ldots, x_n)$ by successively subtracting a product of elementary symmetric polynomials to eliminate the largest monomial without introducing any larger monomials. This way, in each step, the largest monomial is reduced until it becomes zero, and we get the sum of the subtracted-off polynomials, which is the desired expression of P as a polynomial function of elementary polynomials.

Example 7. Suppose we have a symmetric polynomial as the following and we have written it in an increasing order:

$$P = x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + 6x_1 x_2 x_3 + x_2^2 x_3 + x_1 x_3^2 + x_2 x_3^2.$$

The largest monomial is $x_2x_3^2$, so we subtract off $e_1^{2-1}e_2^{1-0}e_3^0$, which is e_1e_2, then we get:

$$P - e_1e_2 = x_1^2x_2 + x_1x_2^2 + x_1^2x_3 + 6x_1x_2x_3 + x_2^2x_3 + x_1x_3^2 + x_2x_3^2 - (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) = 3x_1x_2x_3.$$

Now the largest monomial is $3x_1x_2x_3$, so we subtract off $3e_1^{1-1}e_2^{1-1}e_3^1$, which is $3e_3$, getting $P - e_1e_2 - e_3 = 3x_1x_2x_3 - 3x_1x_2x_3 = 0$. This gives $P = e_1e_2 + e_3$.

7. FTA by the Method of Resultants

On the face of it, the Fundamental Theorem of Algebra deals with just one polynomial or 'equation',

$$f(X) = X^n + a_1X^{n-1} + \ + a_n = 0,$$

where $a_j \in \mathbb{F}$, the ground field, for $j = 1, \ldots, n$. We may as well write for our real-closed field of interest $\mathbb{F}$ the standard real numbers $\mathbb{R}$, since we know that the same first-order results, and essentially the proofs too, will hold for both. The coefficient a_0 can be omitted partly to ensure that $f(X)$ is legitimately of degree n. In the Introduction several analytic methods were given to verify that $\mathbb{R}$ is indeed 'real-closed', that is, in case $n = 2m + 1$ is odd, a solution $x_0 \in \mathbb{R}, f(x_0) = 0$ always exists.

The rest of the proof of FTA utilizes only algebraic means, measures and methods. Some bookkeeping on the degree is necessary, if $n = 2^\mu(2m + 1)$, we call μ the "index of evenness" of n or simply "index". The equation $g(X) = 0$ is said to be "easier to solve" than $f(X) = 0$ when $n' = deg\ g(X) = 2^{\mu'}(2m' + 1)$ and

$$\mu < \mu,\ or\ \mu' = \mu\ and\ m' < m\ (in\ other\ words\ n' < n). \qquad (L)$$

Thus "easier to solve" or "easier to factor" is really a relation between the degrees of two polynomials, and has nothing to do with the values of the coefficients. The relation on degrees can be written $n' <_L n$. The relation (L) then leads to a ready-made induction, reducing the problem of factorization of an n-polynomial to that of one or more n'-polynomials. When $\mu = 0$ there is always a linear factor, as seen in the Introduction, which arises from a root x_0 so that $f(X) = (X - x_0)h(X),\ \ deg\ h(X) = n - 1$.

The ordering defined by (L) above is a total (or linear) order on the natural numbers $\mathbb{N}$. This ordering also arises from the lexicographical ordering induced on the Cartesian product $\{\zeta : \mathbb{N}\}$ with $\{2m + 1$, odd natural numbers$\}$ by the canonical ordering on $\mathbb{N}$.

Let $\mathcal{J}$ be a property of polynomials in $\mathbb{R}[X]$. We may introduce the concept, "the polynomial f satisfies the reduction criterion with respect to $\mathcal{J}$ ", as meaning that whenever $g(X)$ is "easier to factor" than f, it satisfies $\mathcal{J}(g)$. We will set up the specific instance of the reduction criterion that we need further along. Next we summarize the logic of the proof, which is based on [19], [30] and [37].

Definition 6. A 1-factor is a linear (degree one) factor of a polynomial $g(X) \in \mathbb{R}[X]$, a 2-factor is an *irreducible* degree-two factor, so that $g(X) = (X^2 + sX + t)h(X)$, with the discriminant $s^2 - 4t$ *negative*.

Definition 7. Given $\mathbb{H}$ a field or a UFD, a complete factorization into irreducibles is a sequence $\{h_i(X_1, \ldots, X_r)\}$, $i = 1, \ldots, k$ of irreducible multivariable polynomials, whose product gives the polynomial $g(X_1, \ldots, X_r)$, which is to be so decomposed or *factorized*.

Gauss's Factorization Theorem. Under the conditions of definition 7, any polynomial $g(X_1, \ldots, X_r)$ has a complete factorization into irreducibles $\{h_i\}$ whose entries are unique except for a rearrangement of the indices and scalar multiples [20].

Note that if a variable $Y = X_i$ is singled out as distinguished and $g()$ has leading coefficient equal to 1 ("monic") with respect to Y, then all the irreducible factors can be chosen monic as well.

Definition 8. A complete 1,2-factorization of $g(X) \in \mathbb{F}(X)$ is just a factorization into irreducibles such that each factor is either a 1-factor or a 2-factor.

Lemma A. If deg $f(X) = n = 2m+1$ is odd, then $f(X)$ has a linear factor arising from some "zero" $x_0 \in \mathbb{R}$, so that $f(X) = (X - x_0)h(X)$. Thus $f(X)$ has a 1-factor.

Proof. This was established in Section 2, "Transcendental Component" for the standard real numbers and in general by the Final Axiom of the theory of RCF.

Lemma B. Suppose that for all $0 < q \leq n, deg(g) = q$ implies that $g(X)$ has a 1-factor or a 2-factor. Then if deg $f(X) = n, f$ has a complete 1,2-factorization.

Proof. By hypothesis, $f(X)$ has either a linear or irreducible quadratic factor so

$$f(x) = (X - x_0)g(X) \; or \; f(X) = (X^2 + sX + t)h(X). \tag{3}$$

If $deg\ g(X) = 0$ or $deg\ h(X) = 0$, we are done. Otherwise $1 \leq deg\ g < n$ or $1 \leq deg\ h < n$ as the case may be, an induction hypothesis supplies a complete 1,2-factorization for g or h. Finally, the formulas are used to yield a complete 1, 2-factorization for $f(X)$ as well.

Our main result is:

Proposition 7. Any polynomial $f(X) \in \mathbb{R}[X]$ of degree $n \geq 1$ has a 1-factor (linear) or a 2-factor (quadratic irreducible).

Together with Lemma B, this Proposition yields, collecting scalar factors:

Theorem 4. ***Fundamental Theorem of Algebra*** *(for any RCF $\mathbb{F}$). Any monic polynomial $f(X) \in \mathbb{F}[X]$ has a complete 1,2-factorizaiton into monic factors that are unique up to a choice of ordering.*

Before stating and proving the final lemmas that give Proposition 7 and Theorem 4, we make explicit the Reduction Hypothesis we wish to use. We repeat the wordage of Reduction Hypothesis a few times so that its significance is clearer.

Reduction Hypothesis for $f(X)$. The polynomial $f(X)$ in $\mathbb{R}[X]$ or $\mathbb{F}[X]$ satisfies the Reduction Hypothesis for "factorization" if every polynomial $g(X)$ "easier to factor" than $f(X)$, has a 1-factor or a 2-factor. Thus if $deg\ g <_L deg\ f$, then $g(X)$ satisfies the *conclusion* of Proposition 7.

Example 8. A polynomial $f(X)$ of degree 12 that factors into a factor of degree 8 and one of degree 4 will gain a 1- or 2-factor from the factor of degree 4, since $4 <_L 12$ and assuming that f satisfies the Reduction Hypothesis. On the other hand, for a polynomial $h(X)$ of degree 8 to satisfy RH would mean that every polynomial of degree 12, 20, 24, ..., plus 2, 6, 10, ..., would already be known to possess a 1- or 2-factor.

Lemma C. Let $f(X) \in \mathbb{R}[X]$ be a reducible polynomial, with every $g(X)$ satisfying $deg\ g(X) <_L deg\ f(X)$ having a 1-factor or 2-factor. [Simply, $f(X)$ satisfies the Reduction Hypothesis with respect to factorization.] Then $f(X)$ has a 1-factor or a 2-factor.

Proof. Since $f(X)$ is reducible, $f(X) = g_1(X)g_2(X)$ where $deg\ g_1$, $deg\ g_2 \geq 1$. We observe that both $deg\ g_1$, $deg\ g_2 < deg\ f = n$, and the index μ where $deg\ g = 2^{\mu}(2m+1)$ is less than or equal to that of f for at least one of $g_1,\ g_2$. Putting these facts together, we find $deg\ g_1 <_L deg\ f$ OR $deg\ g_2 <_L deg\ f$. By the Reduction Hypothesis, the factor g_1 or g_2 satisfying this inequality has a 1-factor or a 2-factor, and this factor can be used as the required 1- or 2-factor for $f(X)$. We give another version of Proposition 7.

Proposition 7'. Suppose that $deg\ f(X) \geq 3$. Then $f(X)$ is reducible in $\mathbb{R}[X]$. Combined with Lemma C, this result would immediately imply Proposition 7 and Theorem 4 (FTA).

Theorem 4' (Alternate FTA) If $f(X)$ is irreducible in $\mathbb{R}[X]$, then $deg\ f \leq 2$.

Proof of Equivalence with **Theorem 4.** We have just seen how Proposition

7' or Theorem 4' implies Theorem 4 (FTA). Conversely, suppose that FTA holds and $f(X)$ is irreducible. But by FTA, $f(X)$ has a 1-factor or 2-factor and hence must be equal to that factor up to a scalar multiple, thus has degree ≤ 2.

Remark about **Proposition 7'**: Of course if $deg\ f = 3$, we already know by Lemma A that f has a 1-factor so is reducible. Also when $deg\ f = 4$, one can obtain a factorization of $f(X)$ using the classical "Cardano resolvent" [32]. Hence the unknown degree values are even, $n = deg\ f$, starting with $n = 6$.

To finish the proof of Proposition 7, we need two technical results.

Lemma D. Let $f(X) \in \mathbb{R}[X]$, with $degf \geq 3$, be irreducible and satisfy the Reduction Hypothesis for $<_L$ together with the property of 1,2-factorization. [Again, this means that any $g(X)$ easier to factor than $f(X)$ is known already to possess a 1- or 2-factor.] Then there exist $s, t \in \mathbb{R}$ with $s^2 < 4t$ such that over the quadratic field $\mathbb{D}_u$ defined by s,t, we have that $f(X)$ considered as an element of $\mathbb{D}_u[X]$ factors non-trivially, and also $f(X+u)$ and $f(X-u)$ have a non-trivial common factor $y(X,u) \in \mathbb{D}_u[X]$.

Lemma E. Suppose that $f(X) \in \mathbb{R}[X]$ with $degf \geq 2$ is irreducible and satisfies the Reduction Hypothesis, furthermore that over some quadratic field $\mathbb{D}_u$, there is a common factor $y(X,u)$ of $f(X+u)$ and $f(X-u)$. Then $deg\ f(X) = 2$.

These two results could be merged into one, but we separate two threads of the unified proof. Combining them enables us to prove Proposition 7' and by the logic declaimed above, also Proposition 7, Theorem 4 and Theorem 4'.

Proof of **Proposition 7**. The sequence of natural numbers $1 <_L 3 <_L 5 <_L \cdots <_L 2 <_L 6 \ldots$ is a total order and well-founded (there are no infinite decreasing sequences). Thus a complete induction can be applied to all of $\mathbb{N}_L$. Alternatively, given at the outset a polynomial $f(X)$ with $deg\ f = n = 2^{\mu}(2m+1)$, one can modify the proof to deal only with the finite set $\mathbb{N}_{-} = \{r \in \mathbb{N} : r < n^{\mu}\}$. In this manner we could avoid dealing with infinite sequences of integers, limit elements (similar to limit ordinals under "set membership" relation), and deal only with finite collections. Now we start the induction. We choose n as minimal under $<_L$ to be the degree of some polynomial $f(X) \in \mathbb{R}[X]$ that has no 1-factor or 2-factor. By Lemma C, $f(X)$ is irreducible, and we may take $n \geq 3$, otherwise the conclusion of Proposition 7 holds immediately. Hence all the antecedent conditions in Lemma D hold for $f(X)$. The consequent of Lemma D , together with the same antecedent conditions (RH and irreducibility) show also that the hypotheses of Lemma E are satisfied. Therefore we arrive at the conclusion $deg\ f = 2$ as the only remaining possibility, a blatant contradiction. Hence there is no such "least degree" n (with respect to $<_L$), and no counter-example $f(X)$ to **Proposition 7**.

There remains only to verify Lemmas D and E to complete the proof of FTA over a real-closed field. We highlight the principal technique used for Lemma D, and expand on the idea due to James Wood of using a Resultant that arises from the original polynomial.

8. Factors over the Ring $\mathbb{R}[X]$

In keeping with the notation of [19] we write,

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_n(= 0),$$

with $degf = n = 2^\mu(2m + 1)$. Now choose an indeterminate algebraically independent of X, called u. When $n \geq 2$ we define polynomials in $\mathbb{R}[X, u]$, $F(X, u) = \frac{1}{2}\{f(X+u)+f(X-u)\}$, the "even part", and $G(X, u) = \frac{1}{2u}\{f(X+u) - f(X-u)\}$, the "reduced odd part".

Of interest is the resultant $L(u) \equiv \mathcal{R}_X(F, G)$. But note that

$$f(X + u) = F(X, u) + uG(X, u).$$

By Gordan's Lemma on resultants, the resultant $\mathcal{R}_X(f(X + u), G(X, u))$ must be the same polynomial in u as $L(u)$. Therefore $L(u)$ determines whether $f(X + u)$ can be factored in common with $G(X, u)$. We note some properties of this resultant, valid when ≥ 2

Property 1. Let $F_P(X, u), G_P(X, u)$ be the respective "principal" homogeneous parts, which have total degrees n and $(n - 1)$. Then $\mathcal{R}_X(F_P, G_P)$ is not identically 0 as a polynomial in u.

Proof. If this resultant were identically zero, it would mean that $(X+u)^n + (X-u)^n$ and $(X+u)^n-(X-u)^n$ would have a common factor in $\mathbb{R}[X, u]$, hence so would $(X + u)^n$ and $(X - u)^n$, but this would violate the Gauss (unique) factorization theorem over this ring.

Property 2. We have $deg_uL(u) = n(n - 1)$ unless the principal homogeneous part $L_P(u) = R_X(F_P, G_P)$ is zero.

Proof. The polynomials $F(X, u)$ and $G(X, u)$ have degree n and $(n - 1)$ respectively, thus so do their principal homogeneous parts. By Proposition 5, their resultant has degree $n(n - 1)$ unless in fact $R_X(F_P, G_P) = 0$ identically. Thus according to Property 1, $deg_uL(u) = n(n-1)$ and we obtain the following.

Property 3. In fact $L(u) = M(w)$ where $u^2 = w$ and $(M) = \frac{1}{2}n(n - 1)$.

Proof. By substituting values it can easily be seen that F and G are even functions of u, hence *even polynomials* in u, over $\mathbb{R}[X]$. Thus whenever u

appears in the specialized Sylvester form $\mathcal{S}_X(F,G)$, only entries depending on $u^2 = w$ appear. Hence $\mathcal{R}_X(F,G)=$ determinant of the specialized Sylvester matrix, has only terms in powers of w occurring, and we determine its degree from Properties 1 and 2.

Property 4. $M(w)$ is a polynomial "easier to factor" than $f(X)$.

Proof. It is only necessary to confirm that $deg(M) <_L deg(f) = n$, which comes from Property 3.

Proof of **Lemma D**. We apply the construction above to $f(X)$ which is assumed to satisfy the hypotheses of Lemma D. In view of Property 4, one concludes that $M(w)$ has a 1- or 2-factor in $\mathbb{R}[w]$.

Now Case 1 occurs when the purported 1-factor is of the form $k(w) = w-a$. Take first the possibility that $a \geq 0$, but then $u^2 = a$ with its solution $\sqrt{a}$, which exists by the Axioms of a real-closed field, would mean that $f(X + \sqrt{a})$ is reducible over $\mathbb{R}[X]$, hence so is $f(X)$, contradicting the hypothesis.

Next we consider $a < 0$ when we set $s = 0$ and $t = -a > 0$, so that by the Main Theorem of Resultants we deduce that $f(X + u)$ has a factor $\beta(X)$ whenever $u^2 = a$, or expressed otherwise $f(X)$ is reducible in $\mathbb{D}_u[X]$ where $\mathbb{D}_u$ is defined by the parameters $s = 0, t = -a$.

Case 2. If there is no 1-factor of $M(w)$, there must be a 2-factor $w^2 + \sigma w + \tau, \sigma^2 < 4\tau$.

Writing $\gamma(u) = u^4 + \sigma u^2 + \tau$, we arrive at a factor of γ, $\lambda(u) = u^2 + su + t$ where $s = \{2\sqrt{\tau} - \sigma\}^{1/2}, t = \sqrt{\tau}$ which are defined in $\mathbb{R}$ and satisfy $s^2 = 2\sqrt{\tau} - \sigma < 4t = 4\sqrt{\tau}$, since $-\sigma < 2\sqrt{\tau}$ whatever be the sign of σ.

The complementary factor of $\gamma(u)$ will be $\kappa(u) = u^2 - su + t$. Similar to what was done in Case 1, we may define the field $\mathbb{D}_u$ based on parameters (s,t), the polynomial $\lambda(u) \in R[u]$, or the parameters $(-s,t)$, the polynomial $\kappa(u)$. When Case 1 leads to an irreducible $u^2 + t$, or when in Case 2 we have irreducible $\lambda(u)$ as above, we observe that the resultant $\mathcal{R}_X(F,G)$ vanishes in $\mathbb{D}_u$.

Hence by the Main Theorem of Resultants, $F(X,u)$ and $G(X,u)$ have a common factor in $\mathbb{D}_u$, and by Gordan's Lemma, so do $f(X+u)$ and $G(X,u)$ have a common factor that we designate $\beta(X,u)$. Noting that $\frac{1}{u} = u^{-1} = -\frac{1}{t}(s+u)$ in $\mathbb{D}_u$, we must have $\beta(X,u)$ also dividing $f(X-u)$. Certainly then $\beta(X-u,u)$ is a factor of $f(X)$ in $\mathbb{D}_u[X]$ whose X-degree is greater than or equal to 1. Thus Lemma D is established.

Proof of **Lemma E.** Since $\epsilon(X,u)$ divides $f(X+u)$ over $\mathbb{D}_u$, the polynomial $\epsilon(X-u,u)$ will divide $f(X)$. For the moment write $\phi(X) = \phi_u(X) = \epsilon(X-u,u)$. Thus $\phi(X)\psi(X) = f(X)$ for some $\psi(X) \in \mathbb{D}_u[X]$. By Lemma A, we have that $n = deg\ f(X)$ is an even natural number. First we show that the

factor $\phi(X)$ in $\mathbb{D}_u(X)$ must have X-degree $= n/2$. Otherwise if $deg\ \phi < n/2$, we can choose an irreducible factor $\phi_1(X)$ dividing $\phi(X)$ in $\mathbb{D}_u(X)$. Since $f(X)$ is real (has real coefficients), also $\overline{\phi_1(X)}$, the u-conjugate, divides $f(X)$ by χ**-Property 7.** But $\phi_1(X)$ is not real so by χ**-Property 5** does not equal $\overline{\phi_1}(X)$, and both are irreducible with only scalar factors in common. Also by χ**-Property 5**, $\phi_1(X)\overline{\phi_1}(X)$ is real, hence, $f(X) = \phi_1(X)\overline{\phi_1}(X)h(X)$ for a residual real factor $h(X)$. Since $deg\ \phi_1(X) = deg\ \overline{\phi_1}(X)$, the irreducibility of $f(X)$ in $\mathbb{R}[X]$ shows that the the only possibility is $deg\ \phi_1 = deg\ \phi = n/2$. We have at the same time proved that $\phi_u(X)$ must be irreducible in $\mathbb{D}_u$ (X). The complementary factor $\psi(X)$ must equal $\overline{\phi}(X)$ and be irreducible as well. This fact comes up again later in the proof.

Recall the hypotheses of Lemma E. We have just shown that

$$f(X+u) = \phi(X+u)\psi(X+u),$$

$$f(X-u) = \phi(X-u)\psi(X-u)$$

with the factors displayed on the right-hand side being *irreducible* in $\mathbb{D}_u[X]$. According to hypothesis, $f(X+u)$ and $f(X-u)$ have a common factor. Up to a reflection symmetry, there are essentially only two possibilities: $\phi(X+u) = \phi(X-u)$ and $\phi(X+u) = \psi(X-u)$. Addressing the first choice, suppose that $\phi(X+u) - \phi(X-u)$ equals the zero polynomial in X. Letting $q = n/2 - 1$, the only terms of this expression involving X^q come from the leading (monic) terms $(X+u)^{q+1}$ and $(X-u)^{q+1}$, so in the *difference*, these coefficients are respectively $(q+1)u$ and $-(q+1)(-u)$, hence do not add to zero. Therefore $\phi_u(X+u) = \phi_u(X-u)$ is impossible.

The second choice was that $\phi(X+u) = \psi(X-u) = \overline{\phi}(X-u)$ as polynomials over $\mathbb{D}_u$. Again if $q+1 = n/2$, we write

$$\phi(X+u) = (X+u)^{q+1} + c_1(X+u)^q + c_2(X+u)^{q-1} + \ldots,$$

$$\psi(X-u) = (X-u)^{q+1} + \overline{c_1}(X-u)^q + \overline{c_2}(X-u)^{q-1} + \ldots,$$

so the $n/2$ degree terms match up as before, but enumerating the terms in X^q give respectively $(q+1)u + c_1$ from the first row, and $-(q+1)u + \overline{c_1}$ from the second row. Writing $c_1 = a_1 + b_1 u$, we obtain $\overline{c_1} = (a_1 - b_1 s) - b_1 u$, and relying on unique representation of elements of $\mathbb{D}_u$, $(q+1+b_1)u = (-q-1-b_1)u$, $a_1 = a_1 - b_1 s$. Since $\mathbb{D}_u$ is an integral domain, if b_1 were equal to 0 we would have $2(q+1) = 0$ as integers, thus $q+1 = 0$ which is absurd. The only remaining possibility is $s = 0$, and in that case the characterizing polynomial of $\mathbb{D}_u$ must be of the form $u^2 + t = 0$ with $t > 0$.

Since $s = 0$, we observe that $\chi(X - u) = X + u$, hence in fact

$$\phi(X + u) = \psi(X - u) = \overline{\phi}(X - u) = \overline{\phi}(\overline{X + u}) = \overline{\phi(X + u)},$$

so by $\chi -$ **Property 5** of u-conjugation, we deduce that $\phi(X + u)$ is actually real. In this last calculation, we also appealed to $\chi -$ **Property 8** where the argument is $X - u$. Since its degree $n/2 <_L n$, the polynomial $\phi(X + u)$ is "easier to factor" than $f(X)$ and hence by the standard hypothesis (RH) built into Lemma E, we obtain that $\phi(X + u)$ has a 1-factor or a 2-factor in $\mathbb{R}[X]$. That means that in case $deg\ \phi > 2$, it follows that $\phi(X + u)$ is reducible in $\mathbb{R}[X]$, hence $\phi(X)$ is reducible in $\mathbb{D}_u$ which contradicts what we already have established. If $deg(\phi) = 1$, we have $deg\ f(X) = 2$ and the conclusion of Lemma E holds. The only remaining case occurs when $deg\ \phi(X) = 2$. This means that $deg\ f(X) = 4$, so Cardano's formulas can be applied to obtain a factorization of $f(X)$. Another way is to reason that since the parameter s equals zero, $\phi(X)$ is automatically reducible over $\mathbb{D}_u[X]$. More explicitly, a quadratic $\phi(X) = X^2 + c_1X + c_2$ can be factored by "completing the square" as long as every element $a + bu$ in $\mathbb{D}_u$ has a square root. Recalling that the parameters $(s, t) = (0, t)$ for $\mathbb{D}_u$ in our present situation, we have the explicit formula, similar to one we have seen earlier, for solving $y^2 = a + bu$, namely

$$\pm y = \frac{1}{\sqrt{2}}\{\sqrt{a + \sqrt{a^2 + b^2t}} + sgn(b)u\sqrt{-a/t + \sqrt{(a/t)^2 + b^2/t}}\},$$

where $sgn(b) = b/|b|$.

This formula and the factorization of $\phi(X)$ can be verified by explicit arithmetic. But ϕ was determined to be irreducible in $\mathbb{D}_u[X]$, so this case of $deg\ \phi = 2$ is moot.

We completed an examination of the "second choice", namely $\phi(X + u) = \psi(X-u)$, which was refuted, leading inevitably to $deg\ f(X) \leq 2$, the conclusion of Lemma E. We indicated earlier how induction based on the $<_L$ ordering, and application of Lemmas D and E, yields Propositions 7 and 7', Theorem 4 and the Fundamental Theorem of Algebra.

9. Computer Implementation

In this section, we report the computer implementation, which has been developed to affect symbolic calculation in the context of exact arithmetic. Some examples show how these routines apply to the algebra of symmetric multinomial forms used in Laplaces proof (1795) of FTA, as well as to the theory of Sylvester forms and the Bézoutian formulation of the resultant.

Laplace's Method

Once the symmetric polynomials are represented by elementary polynomials, we could see a more complex polynomial, which has important form in Laplaces proof. Suppose e_k is the k^{th} elementary symmetric polynomial in the n variables $x_1, \ldots, x_n$. Then, if we have $(x) = \prod\{x - T_i(h, x_1, \ldots, x_n)\}$, where T_i is polynomial of $h, x_1, \ldots, x_n$, and h is constant, we could express F in terms of elementary polynomials through several steps. Here we give a simple example to explain the process.

Example 9. Consider $e_i(x_1, x_2, x_3, x_4)$ to be the elementary symmetric polynomial of x_1, x_2, x_3, x_4, which is also a monic-univariate polynomials. So that,

$$\begin{cases} e_1(x_1, \ldots, x_4) = x_1 + x_2 + x_3 + x_4 \\ e_2(x_1, \ldots, x_4) = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ e_3(x_1, \ldots, x_4) = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\ e_4(x_1, \ldots, x_4) = x_1x_2x_3x_4. \end{cases}$$

Write $F(x) = \prod\{x - (x_1 + x_2 + x_1x_2)\} \cdot \{x - (x_1 + x_3 + x_1x_3)\} \ldots \{x - (x_3 + x_4 + x_3x_4)\}$ in terms of $e_i(x_1, x_2, x_3, x_4)$.

Solution: We could write $F(x) = \prod\{x - T_1\} \cdot \{x - T_2\} \ldots \{x - T_6\}$ at first, where $T_1 = x_1 + x_2 + x_1x_2$ and so on. After expansion of $F(x)$, the coefficient of $F(x)$ should be elementary symmetric polynomial $e_k(T_1, T_2, \ldots, T_6), k = 1, 2, \ldots, 6$. $F(x)$ can be expressed as:

$$\begin{aligned} F(x) = x^6 - e_1(T_1, T_2, \ldots, T_6) \cdot x^5 + e_2(T_1, T_2, \ldots, T_6) \cdot x^4 - e_3(T_1, T_2, \ldots, T_6) \cdot x^3 \\ + e_4(T_1, T_2, \ldots, T_6) \cdot x^2 - e_5(T_1, T_2, \ldots, T_6) \cdot x + e_2(T_1, T_2, \ldots, T_6). \end{aligned}$$

Now, we rewrite $e_k(T_1, T_2, \ldots, T_6)$ in terms of $e_i(x_1, x_2, x_3, x_4)$. First, it is obvious that $e_k(T_1, T_2, \ldots, T_6)$ is also a function of x. For example, $e_1(T_1, T_2, \ldots, T_6)$ equals to: $T_1 + T_2 + T_3 + T_4 + T_5 + T_6$. And this equals to: $3(x_1 + x_2 + x_3 + x_4) + x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4$, which can also be rewritten in terms of $e_i(x_1, x_2, x_3, x_4)$ as $3e_1(x_1, x_2, x_3, x_4) + e_2(x_1, x_2, x_3, x_4)$.

Follow the same process, we could get all $e_k(T_1, T_2, \ldots, T_6)$ in terms of $e_i(x_1, x_2, x_3, x_4)$ and we substitute them back into $F(x)$.

Once we have the mathematical proof and structure, we can hand over the tedious work to a computer and let it generate the detail formulas for us. Here we provide the core loop to implement the process as follows:

Step 1: Input number of variables n and generate $e_i(x_1, \ldots, x_6), i = 1, \ldots, n$, which are the elementary polynomials of x_i.

Step 2: $F(x) = \prod_{i=1}^{k}\{x - T_i(h, x_1, x_2, \ldots, x_n)\} = \prod_{i=1}^{k}(-1)^{i-1} \cdot e_{k+1-i}(T_1, \ldots, T_k) \cdot x^{i-1}$, where $Ti(.)$ can be any function of h and x_i. And k must be a number

to ensure that the product of $Ti(.)$ is symmetric function, where k depends on the form of $Ti(.)$ and n.

Step 3: Express $e_k(T_1, T_2, \ldots, T_k)$in terms of $e_i(x_1, \ldots, x_n)$;

Write $e_k(T_1, T_2, \ldots, T_k)$ in terms of $x_1, x_2, \ldots, x_n$ as increasing order so that the largest monomial equals to $x^{i_1}{}_1 \ldots x^{i_n}{}_n$;

Follow the method introduced in the proof of FTA and translate $e_k(T_1, T_2, \ldots, T_k)$ to $e_i(x_1, \ldots, x_n)$.

Step 4: Write $F(X)$ in terms of $e_i(x_1, \ldots, x_n)$

We have programmed a software package in C++ to solve the problem as what is showed in the above example. We first input the three parameters n, k and h into computer. Here n denotes the degree of $x_1, x_2, \ldots, x_n, k$ is the number of x variables in each T_i, and h is constant, which is shown in Figure 1.

```
ESCL<PadicInt32>: elementaryPoly[4,2,1]
The variable [Si] is following:
        [S0] = 1
        [S1] = [X4]+[X3]+[X2]+[X1]
        [S2] = [X4][X3]+[X4][X2]+[X4][X1]+[X3][X2]+[X3][X1]+[X2][X1]
        [S3] = [X4][X3][X2]+[X4][X3][X1]+[X4][X2][X1]+[X3][X2][X1]
        [S4] = [X4][X3][X2][X1]
```

Figure 1: Program Segment

```
The middle variable [Ti] is following:
        [T1] = [X2][X1]+[X2]+[X1]
        [T2] = [X3][X1]+[X3]+[X1]
        [T3] = [X4][X1]+[X4]+[X1]
        [T4] = [X3][X2]+[X3]+[X2]
        [T5] = [X4][X2]+[X4]+[X2]
        [T6] = [X4][X3]+[X4]+[X3]
```

Figure 2: Program Segment

```
        [E1] = [X4][X3]+[X4][X2]+[X4][X1]+3[X4]+[X3][X2]+[X3][X1]+3[X3
]+[X2][X1]+3[X2]+3[X1]

        [E2] = [X4]^2[X3][X2]+[X4]^2[X3][X1]+2[X4]^2[X3]+[X4]^2[X2][X1
]+2[X4]^2[X2]+2[X4]^2[X1]+3[X4]^2+[X4][X3]^2[X2]+[X4][X3]^2[X1]+2[X4][
X3]^2+[X4][X3][X2]^2+3[X4][X3][X2][X1]+9[X4][X3][X2]+[X4][X3][X1]^2+9[
X4][X3][X1]+8[X4][X3]+[X4][X2]^2[X1]+2[X4][X2]^2+[X4][X2][X1]^2+9[X4][
X2][X1]+8[X4][X2]+2[X4][X1]^2+8[X4][X1]+[X3]^2[X2][X1]+2[X3]^2[X2]+2[X
3]^2[X1]+3[X3]^2+[X3][X2]^2[X1]+2[X3][X2]^2+[X3][X2][X1]^2+9[X3][X2][X
1]+8[X3][X2]+2[X3][X1]^2+8[X3][X1]+2[X2]^2[X1]+3[X2]^2+2[X2][X1]^2+8[X
2][X1]+3[X1]^2
```

Figure 3: Program Segment

We could see that the program can run automatically, and gives the elementary polynomials s_i, as shown in Figure 2. And because T_i has been defined in the above formulas, we could generate $e_i(T_1, \ldots, T_6)$. For example, $e_1(T_1, \ldots, T_6)$ and $e_2(T_1, \ldots, T_6)$ are shown in Figure 3. Finally, the computer will translate $e_i(T_1, \ldots, T_6)$ in terms of e_i, shown in Figure 4. Therefore, the

```
After the replace the [Ei] is following:
        [E0] = 1
        [E1] = [S2]+3[S1]

        [E2] = -[S4]+[S3][S1]+3[S3]+2[S2][S1]+2[S2]+3[S1]^2

        [E3] = -2[S4][S2]+[S4][S1]^2+2[S4][S1]+8[S4]+[S3]^2+2[S3][S2]+
[S3][S1]^2+4[S3][S1]+2[S2]^2+[S2][S1]^2+4[S2][S1]+[S1]^3

        [E4] = -[S4]^2+[S4][S3][S1]+2[S4][S3]+2[S4][S2][S1]+12[S4][S2]
+8[S4][S1]-4[S4]+[S3]^2[S1]+3[S3][S2][S1]+4[S3][S2]+[S3][S1]^2+[S3][S1
]+2[S2]^2[S1]+[S2]^2+2[S2][S1]^2

        [E5] = [S4]^2[S2]+3[S4]^2[S1]+8[S4]^2+2[S4][S3][S2]+4[S4][S3][
S1]+8[S4][S3]+2[S4][S2]^2+4[S4][S2][S1]-4[S4][S2]+3[S4][S1]^2-4[S4][S1
]+[S3]^2[S2]+[S3]^2[S1]+3[S3]^2+2[S3][S2]^2+2[S3][S2][S1]+[S3][S1]^2+[
S2]^3+[S2]^2[S1]

        [E6] = [S4]^3+3[S4]^2[S3]+2[S4]^2[S2]-4[S4]^2+3[S4][S3]^2+4[S4
][S3][S2]+[S4][S3][S1]-4[S4][S3]+[S4][S2]^2-[S4][S1]^2+[S3]^3+2[S3]^2[
S2]+[S3]^2[S1]-[S3]^2+[S3][S2]^2+[S3][S2][S1]
```

Figure 4: Program Segment

```
THE F(x,u) G(x,u) WILL BE FOLLOWING:
        F(x,u) = [x]^3+3[x][u]^2+[x]-1
        G(x,u) = 3[x]^2+[u]^2+1

THE BEZOUT MATRIX WILL BE FOLLOWING:
        3[u]^4+4[u]^2+1   3   [u]^2+1

        3   -8[u]^2-2   0

        [u]^2+1   0   3


THE DETERMINATE FOR [b i,j] IS FOLLOWING:
        det = -64[u]^6-96[u]^4-36[u]^2-31
```

Figure 5: Program Segment

computer makes it possible to give the specific form of polynomial fundamental theorem of algebra.

Bézoutian Formulation of the Resultant

In algebra, the resultant of two monic polynomials $P(x)$ and $Q(y)$ over a field k is defined as the product:

$$res(P,Q) = \prod_{(x,y):P(x)=0,Q(y)=0}(x-y).$$

It is generally easier to compute the determinant of the Bézout matrix of $P(x)$ and $Q(y)$ rather than to work with the larger Sylvester matrix.

Bézout matrix

The Bézout matrix is a special square matrix associated with two polynomials. Let $f(x)$ and $g(x)$ be two complex polynomials of degree no greater than n with coefficients, which could be zero:

```
THE F(x,u) G(x,u) WILL BE FOLLOWING:
        F(x,u) = [x]^4+[x]^3[a3]+6[x]^2[u]^2+[x]^2[a2]+3[x][u]^2[a3]+[
x][a1]+[u]^4+[u]^2[a2]
        G(x,u) = 4[x]^3+3[x]^2[a3]+4[x][u]^2+2[x][a2]+[u]^2[a3]+[a1]

THE BEZOUT MATRIX WILL BE FOLLOWING:
        [b 0, 0] = -4[u]^6+3[u]^4[a3]^2-6[u]^4[a2]+4[u]^2[a3][a1]-2[u]
^2[a2]^2+[a1]^2
        [b 0, 1] = 3[u]^4[a3]-2[u]^2[a3][a2]+6[u]^2[a1]+[a2][a1]
        [b 0, 2] = -4[u]^4+[u]^2[a3]^2-4[u]^2[a2]+[a3][a1]
        [b 0, 3] = [u]^2[a3]+[a1]
        [b 1, 0] = 3[u]^4[a3]-2[u]^2[a3][a2]+6[u]^2[a1]+[a2][a1]
        [b 1, 1] = 20[u]^4-8[u]^2[a3]^2+12[u]^2[a2]-2[a3][a1]+2[a2]^2
        [b 1, 2] = -7[u]^2[a3]+2[a3][a2]-3[a1]
        [b 1, 3] = 4[u]^2+2[a2]
        [b 2, 0] = -4[u]^4+[u]^2[a3]^2-4[u]^2[a2]+[a3][a1]
        [b 2, 1] = -7[u]^2[a3]+2[a3][a2]-3[a1]
        [b 2, 2] = -20[u]^2+3[a3]^2-2[a2]
        [b 2, 3] = 3[a3]
        [b 3, 0] = [u]^2[a3]+[a1]
        [b 3, 1] = 4[u]^2+2[a2]
        [b 3, 2] = 3[a3]
        [b 3, 3] = 4
THE DETERMINATE FOR [b i,j] IS FOLLOWING:
        det = 4096[u]^12-3072[u]^10[a3]^2+8192[u]^10[a2]+768[u]^8[a3]^
4-4096[u]^8[a3]^2[a2]-512[u]^8[a3][a1]+5632[u]^8[a2]^2-64[u]^6[a3]^6+5
12[u]^6[a3]^4[a2]+512[u]^6[a3]^3[a1]-1536[u]^6[a3]^2[a2]^2-1920[u]^6[a
3][a2][a1]+1792[u]^6[a2]^3+1664[u]^6[a1]^2-96[u]^4[a3]^5[a1]+32[u]^4[a
3]^4[a2]^2+608[u]^4[a3]^3[a2][a1]-192[u]^4[a3]^2[a2]^3-400[u]^4[a3]^2[
a1]^2-864[u]^4[a3][a2]^2[a1]+272[u]^4[a2]^4+768[u]^4[a2][a1]^2-36[u]^2
[a3]^4[a1]^2+24[u]^2[a3]^3[a2]^2[a1]-4[u]^2[a3]^2[a2]^4+168[u]^2[a3]^2
[a2][a1]^2-104[u]^2[a3][a2]^3[a1]-216[u]^2[a3][a1]^3+16[u]^2[a2]^5+72[
u]^2[a2]^2[a1]^2-4[a3]^3[a1]^3+[a3]^2[a2]^2[a1]^2+18[a3][a2][a1]^3-4[a
2]^3[a1]^2-27[a1]^4
```

Figure 6: Program Segment

$$f(x) = \sum_{i=0}^{n} \mu_i x^i, \quad g(x) = \sum_{i=0}^{n} v_i x^i.$$

Then, the entries of the Bézout matrix of order n associated with the polynomials f and g are: $B_n(f,g) = (b_{ij})_{i,j=1,\ldots,n}$, where

$$b_{ij} = \sum_{k=1}^{m_{ij}} \mu_{j+k-1} v_{i-k} - v_{j+k-1} \mu_{i-k} (m_{ij} = min(i, n+i-j)).$$

For example, $n = 4$, we have two polynomials $f(x)$ and $g(x)$ of degree 4, $B_4(f,g) =$

$$\begin{pmatrix} \mu_1 v_0 - \mu_0 v_1 & \mu_2 v_0 - \mu_0 v_2 & \mu_3 v_0 - \mu_0 v_3 & \mu_4 v_0 - \mu_0 v_4 \\ \mu_2 v_0 - \mu_0 v_2 & \mu_2 v_1 - \mu_1 v_2 + \mu_3 v_0 - \mu_0 v_3 & \mu_4 v_0 + \mu_3 v_1 - \mu_1 v_3 - \mu_0 v_4 & \mu_4 v_1 - u_1 v_4 \\ \mu_3 v_0 - \mu_0 v_3 & \mu_4 v_0 + \mu_3 v_1 - \mu_1 v_3 - \mu_0 v_4 & \mu_4 v_1 + \mu_3 v_2 - \mu_2 v_3 - \mu_1 v_4 & \mu_4 v_2 - \mu_2 v_4 \\ \mu_4 v_0 - \mu_0 v_4 & \mu_4 v_1 - \mu_1 v_4 & \mu_4 v_2 - \mu_2 v_4 & \mu_4 v_3 - \mu_3 v_4. \end{pmatrix}$$

If $f(x) = 2x^3 - 3$ and $g(x) = x^2 + x$, then calculate b_{ij} and we get,

$$B_3(f,g) = \begin{pmatrix} 3 & 3 & 0 \\ 3 & 0 & 2 \\ 0 & 2 & 2 \end{pmatrix}.$$

Also, we can see that the Bézout matrix is symmetric.

Computing process

We apply the resultant computation method in our modified Wood-Gordan proof. Then the $Q(v)$ can be obtained through the following steps:

Step 1: $f(x)$ has a degree $n = 2^q P$, where P is odd and $q \geq 1$. We assume $q = 1, P = 3$ and

$$f(x) = x^6 - e_1x^5 + e_2x^4 - e_3x^3 + e_4x^2 - e_5x + e_6.$$

Step 2: Construct the polynomials $F(x, u)$ and $G(x, u)$ according to the following rules:

$$\begin{cases} F(x,u) = \frac{1}{2}[f(x+u) + f(x-u)] \\ G(x,u) = \frac{u^{-1}}{2}[f(x+u) - f(x-u)] \end{cases}$$

$F(x,u) = x^6 - e_1x^5 + (e_2 + 15u^2)x^4 + (-e_3 - 10e_1u^2)x^3 + (e_4 + 6e_2u^2 + 15u^4)x^2 + (-e^5 - 3e_3u^2 - 5e_1u^4)x + (e_6 + e_4u^2 + e_2u^4 + u^6)$

$G(x,u) = 6x^6 - 5e_1x^4 + (4e_2 + 20u^2)x^3 + (-3e_3 - 10e_1u^2)x^2 + (2e_4 + 4e_2u^2 + 6u^4)x + (-e_5 - e_3u^2 - e_1u^4)$

Step 3: Construct Bézout matrix of $F(x, u)$ and $G(x, u)$ in regard of x, $B_6(F, E) = (b_{ij})_{i,j=1,\ldots,6}$, where

$b_{ij} = \sum_{k=1}^{m_{ij}} \mu_{j+k-1}v_{i-k} - v_{j+k-1}\mu_{i-k} \quad (m_{ij} = min(i, 6 + i - j))$.

Since the entries of the matrix b_{ij} are quite complicated, we will not provide full details here. However, they are all polynomials as $b_{ij}(u, e_1, \ldots, e_6)$.

Step 4: Since the resultant $R(u)$ of F and G is exactly the determinant of Bézout matrix of F and G. We will compute the determinant of the matrix $B_6(F, G)$. Then we can get $R(u)$, which is of degree 30, and consists only of terms in $u^2, u^4, \ldots, u^{30}$.

Step 5: Let $v = u^2$, we get the $Q(v)$, which is of degree 15.

Following this process, we get the exact form of $Q(v)$ when $q = 1$ and $P = 3$, and we can get other $Q(v)$ when P is odd and $q \geq 1$ analogously.

Implementation on a computer

Example 9. Examining for practice the case of polynomial $f(x) = x^3 + x - 1$, which does not need a reduction in index, the implementation is shown in Figure 5.

Example 10. Given $f(x) = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$, then the implementation is shown in Figure 6.

10. Software Design Considerations

10.1. The general structure of C^{++} package

In the past few years our group at Towson University has been developing a symbolic C^{++} mathematical software package. The package is designed for error free calculation. Our goal is to realize large matrix calculation efficiently without truncation error. In the software package, we also added some specific functions for mathematical calculation. The structure chart of our software is shown in Figure 7.

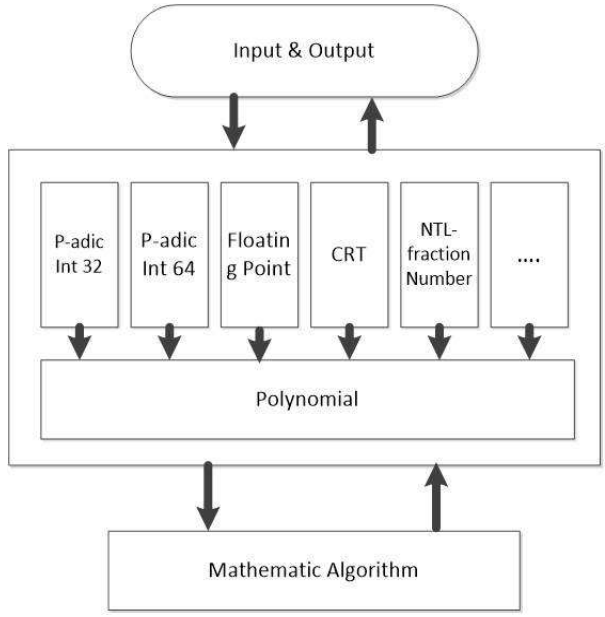

Figure 7: C++ package general structure chart

There are three modules: the I/O, data structures, and mathematical algorithm. These are independent layers. One specific data structure can be directly used on all mathematical algorithms after it has been built. Here we can take the calculation of matrix determinant as an example. If we choose P-adic Int32 data structure, and the prime is chosen as 46337. A program segment is shown in Figure 8.

With the same matrix determinant function template, we can directly use the Polynomial data structure to realize it as shown in Figure 9.

```
Matrix Input is:
        1  1/2  1/3

        1/2  1/3  1/4

        1/3  1/4  1/5

The input will be transformed to P-adic sequence entry:
a[0, 0]: .1 0 0 0 0 0 0 0 0 0
a[0, 1]: .1 0 0 0 0 0 0 0 0 0
a[0, 2]: .1 0 0 0 0 0 0 0 0 0
a[1, 0]: .23169 23168 23168 23168 23168 23168 23168 23168 23168 23168

a[1, 1]: .23169 23168 23168 23168 23168 23168 23168 23168 23168 23168

a[1, 2]: .23169 23168 23168 23168 23168 23168 23168 23168 23168 23168

a[2, 0]: .15446 30891 15445 30891 15445 30891 15445 30891 15445 30891

a[2, 1]: .15446 30891 15445 30891 15445 30891 15445 30891 15445 30891

a[2, 2]: .15446 30891 15445 30891 15445 30891 15445 30891 15445 30891


A matrix determinant calculation process is implemented

The P-adic result for matrix determinant is following:
.7873 29840 30526 10275 28467 24691 20229 36018 33615 34988

P-adic sequence decoding to rational number:
1/2160
```

Figure 8: Program Segment

10.2. Polynomial data structure

There are three classes used on polynomial data structure: symbols, symbol terms and polynomial.

Symbols. Symbol class is used to record the basic symbol definition. For example of (a, b, x) in Figure 10, you can define x, y, z or $a_1, b_2, \cdots, b_n$ as elementary symbols. You also can record more than one character as elementary.

Symbol terms. The symbol terms class is used to record the symbol parts in polynomials. An example of $(ab^2x^3y^4)$ is given in Figure 11. Each symbol term is stored as a linked list, and the different symbol elements are the nodes of the linked list. Each node contains the address of next node and each node also contains the symbol element values and power values.

```
The input Polynomial matrix is following
2[x]+1   [x]^2   1/2

3        [x]^3   [x]

0        [x]+1   1

The determinant for the polynomial is following:
2[x]^4-[x]^3-6[x]^2+1/2[x]+3/2
```

Figure 9: Program Segment

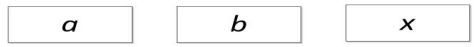

Figure 10: Data structure for symbols

Polynomial. In polynomial class, the linked list structure is used. Each term is represented by a node. Each node contains the next node address, coefficient and a symbol term. Coefficients can be any rational number data structure, such as P-adic Int32 or integer.

A set of polynomial operators have been defined: Operator Addition +, Operator Subtraction -, Operator Multiplication *, Operator Division /, Operator Equal == and so on. These operators serve as the basic functions of the implementation of the polynomial arithmetic. During the calculation process all rational numbers in the polynomial entries will use the rounding error free data structure, the rational number error-free result will be generated. An example is shown in Figure 12 $(2y + 3xy + 4ab + b)$.

10.3. Function structure for Implementation

Laplace's Method. For Laplace's method, the entry variables are xNum, eleNum and coef. This routine will accept the polynomial with structure according to $x_1 + x_2 + \cdots x_n + hx_1x_2 \cdots x_m$. Here, xNum, eleNum and coef means

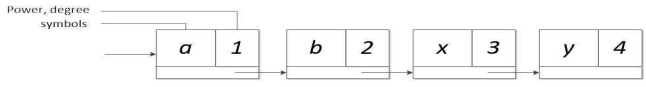

Figure 11: Data structure for symbol terms

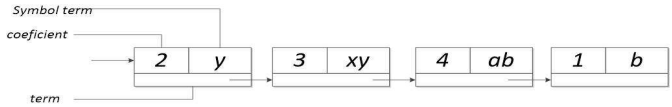

Figure 12: Data structure for polynomial

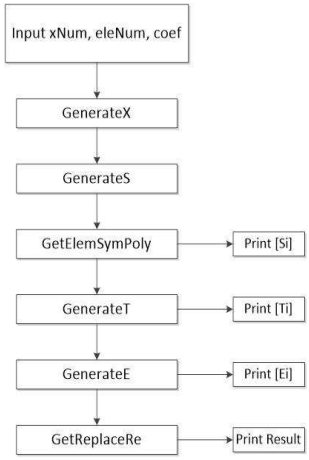

Figure 13: Flow chart for Laplaces method

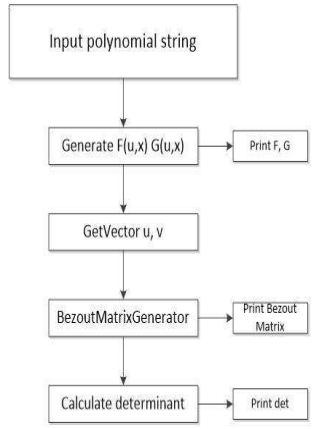

Figure 14: Flow chart for resultant of polynomial

n, h and m. The flow chart of this C^{++} function can be given as shown in Figure 13.

Resultant of Polynomials. The entries for resultant of polynomial function are the string of polynomial and the variables of the polynomial. For example, as shown in Figure 14, the polynomial $f(y) = y^3 + y^2 + y + 3$, the entries are $y^3 + y^2 + y + 3$ and y.

11. Conclusions

In this article, we briefly reviewed the development and proofs of the Fundamental Theorem of Algebra (FTA) with a time-line of 300 years, and concentrated on a collection of proofs commonly denoted as "algebraic". It is known that FTA, when applied to the "standard real numbers" $\mathbb{R}$, requires attention to the transcendental properties of this "metrically complete Archimedean ordered

field". These properties, sufficient for FTA, are encapsulated in the axioms for a Real-Closed Field (RCF).

Computer software has been developed to effect symbolic calculation in the context of exact arithmetic. Examples are given to show how these routines apply to the algebra of symmetric multinomial forms used in Laplace's proof (1795) of FTA, as well as to the theory of Sylvester forms and the Bzoutian formulation of the Resultant. Detailed computer implementation consideration and data structures are discussed at the end of the paper. We will explore additional applications in the future using the software that we have developed, especially on how to use the symmetric polynomial generation, symbolic and error-free computing in coding theory.

Acknowledgments

This research project has been supported by the Air Force Office of Scientific Research, FA9550-11-1-0315.

References

[1] Alperin, J.L., *Local Representation Theory: Modular Representations as an Introduction to the Local Representation Theory of Finite Groups*, Cambridge University Press(1986)

[2] Arnold, B.H., A Topological Proof of the Fundamental Theorem of Algebra, *Amer. Math. Monthly*, **56**, no.7(1949) 465-466

[3] Artin, E. & Schreier, O., Algebraische Konstruktion reeller Körper; Über die Zerlegung definiter Funktionen in Quadrate; Eine Kennzeichnung der reell abgeschlossenen Körper, *Abh. Math. Sem. Univ. Hamburg*, **5**(1927) 8599

[4] Bourbaki, N., *Algebre*, Chap. VI(1952), 40-41

[5] Branco de Oliveira, O.R., The Fundamental Theorem of Algebra: From the Four Basic Operations, *arXiv*: 1110.0165v1(2011)

[6] Brown, W.C., *Matrices Over Commutative Rings*(1993), Marcel Dekker, New York

[7] Burkel, R.B., Fubinito Immediately implies FTA, *Amer. Math Monthly* **113**(2006), 344-347

[8] Cauchy, A.-L., *Cours d'analyse vol VII*, Bologna(1990)

[9] Cayley, A., Note sur la methode d'elimination de Bézout, *J. Reine Angew. Math* **53**(1857), 366367

[10] Dugundji, J., *Topology*, Allyn and Bacon(1966), New York

[11] Ebbinghaus et al, H.-D., *Numbers*, Graduate Texts in Mathematics vol. **123**(1993), Springer-Verlag, New York

[12] Elliott, E.B., On the Existence of a Root of a Rational Integral Equation, *Proc. London Math. Soc.*(1893) Series 1 **25** 173-184

[13] Fine, B. and Rosenberger, G., *The Fundamental Theorem of Algebra*, Undergraduate Texts in Mathematics, Springer-Verlag(1997), New York

[14] Foncenex, D. de, *Réflexions sur les quantités imaginaires*, Misc. Taurinensia **1**(1759), 113-146

[15] Gauss, C.-F., *Demonstratio nova theorematis functionem algebraicam rationale ...*, Universität Helmstedt(1799)

[16] Gauss, C.-F., *Demonstratio nova alter theorematis onmen functionem algebraicam rationale integram ...*, Comm. Soc. Reg. Sci. Göttingen **3**(1815), 107-142

[17] Gersten, S.M. and Stallings, J.R., On Gausss First Proof of the Fundamental Theorem of Algebra, Proc. *Amer. Math. Soc*(1988), **103** no. 1, 231-232

[18] Gordan, P., *Ueber den Fundamentalsatz der Algebra*, Math. Ann. **10**(1876), 572-575

[19] Gordan, P., *Vorlesungen ueber Invariantentheorie*, vol **1**(1885), B.G. Teubner, Leipzig

[20] Herstein, I.N., *Topics in Algebra*, second ed., J. Wiley(1975), New York

[21] Hille, E., *Analytic Function Theory*, Chelsea. 2 Vols(1973), New York

[22] Hyland, J.M.E., Why is there an Elementary Proof of the Fundamental Theorem of Algebra?, *Eureka* **45**(1985), 40-41

[23] Kerber, M., Division-free computation of subresultants using Bézout matrices. *Tech. Report*(2006) MPI-I-2006-1-006

[24] Lang, S., *Algebra*, 3rd revised ed. Springer-Verlag(2002), New York

[25] Littlewood, J.E., Mathematical notes (14): Every Polynomial has a Root, *J. London Mathematical Society* **16**(1941), 95-98

[26] Macdonald, I.G., *Symmetric Functions and Hall Polynomials*, 2nd ed. Clarendon Press, Oxford(1998)

[27] Malet, J.C., Proof that every algebraic equation has a root, *Trans. R. Irish Acad* **26**(1878), 453-455

[28] Mead, D.G., Newton's Identities, *The American Mathematical Monthly* **99**(1992), 749751

[29] Milnor, J., Analytic proofs of the "hairy ball theorem" and the Brouwer fixed-point theorem, *Amer. Math. Monthly* **85**(1978), no. 7, 521-524

[30] Smithies, F., A Forgotten Paper on the Fundamental Theorem of Algebra, *Notes and Records of the Royal Society of London*, **54**(2000) 333-341

[31] Stanley, R.P., *Enumerative Combinatorics*, Vol. 2. Camridge: Cambridge University Press, Cambridge(1999), U.K

[32] Stewart, I., *Galois Theory*, 3rd ed., Chapman and Hall/CRC(2004), Boca Raton

[33] Sturm, C.-F., Mémoire sur les résolutions des équations numériques, *Acad. Royale des Science* **6**(1835), 271-318

[34] Tarski, A., *A Decision Method for Elementary Algebra and Geometry*, Univ. of California Press(1951), Berkeley

[35] Taylor, P., Gauss's Second Proof, *Eureka* **45**(1985), 42-47

[36] Van der Waerden, B.L., *Modern Algebra vol. 1*, Ungar(1948), New York

[37] Wood, J. and Maskelyne, N., On the Roots of Equations, *Philosophical Transactions of the Royal Society of London*, **88**(1798), 369-377