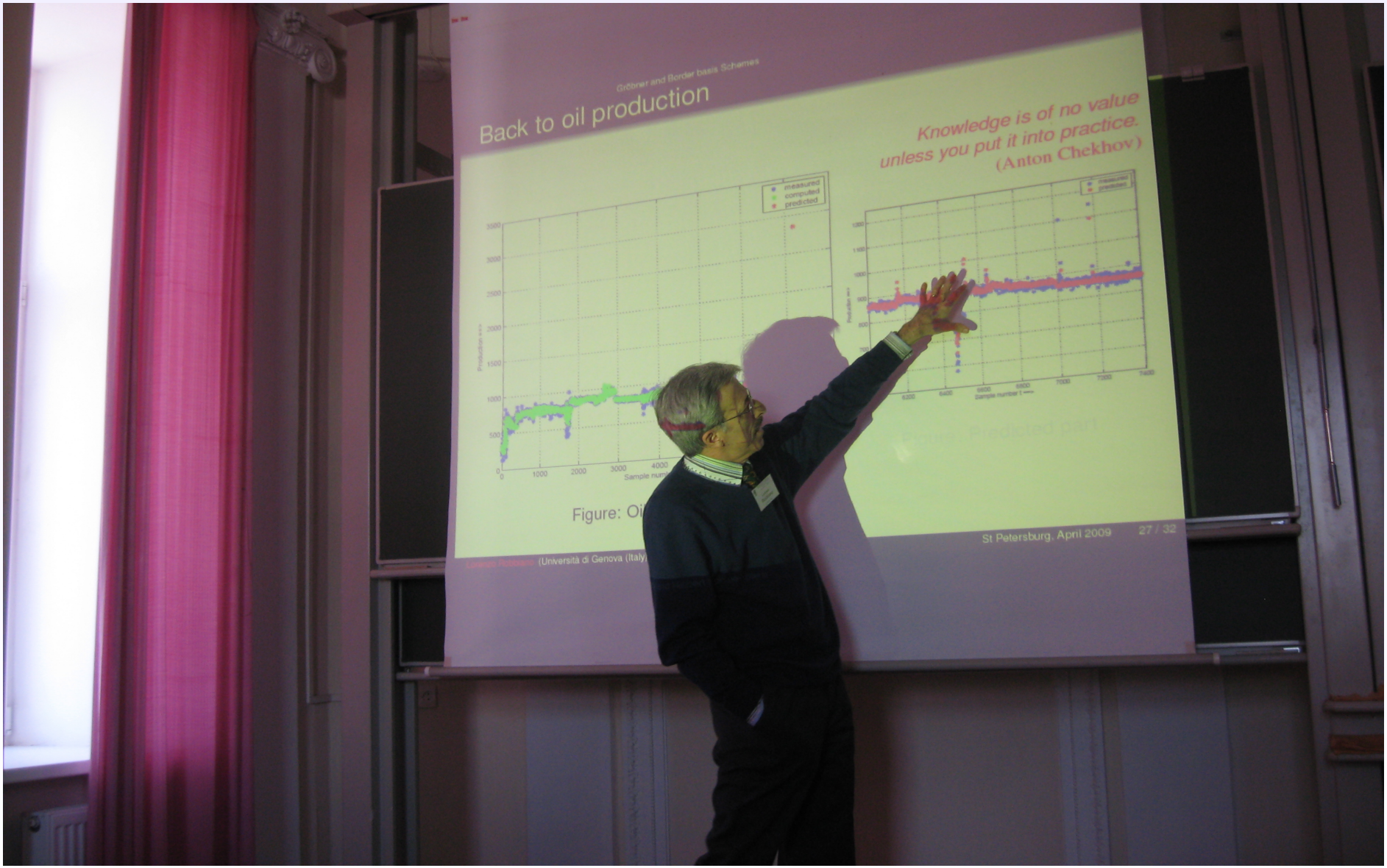
Computational Linear and Commutative Algebra

Lorenzo Robbiano

University of Genoa, Italy
Department of Mathematics

2009


Gröbner and Border basis Schemes
Back to oil production
Knowledge is of no value
unless you put it into practice.
(Anton Chekhov)
measured
computed
predicted
Sample number
St Petersburg, April 2009
27 / 32
(Università di Genova (Italy)

The Cover

Martin Kreuzer · Lorenzo Robbiano

Computational Linear and Commutative Algebra

This book combines, in a novel and general way, an extensive development of the theory of families of commuting matrices with applications to zerodimensional commutative rings, primary decompositions and polynomial system solving. It integrates the *Linear Algebra of the Third Millennium*, developed exclusively here, with classical algorithmic and algebraic techniques. Even the experienced reader will be pleasantly surprised to discover new and unexpected aspects in a variety of subjects including eigenvalues and eigenspaces of linear maps, joint eigenspaces of commuting families of endomorphisms, multiplication maps of zerodimensional affine algebras, computation of primary decompositions and maximal ideals, and solution of polynomial systems.

This book completes a trilogy initiated by the uncharacteristically witty books *Computational Commutative Algebra 1* and *2* by the same authors. The material treated here is not available in book form, and much of it is not available at all. The authors continue to present it in their lively and humorous style, interspersing core content with funny quotations and tongue-in-cheek explanations.

Mathematics

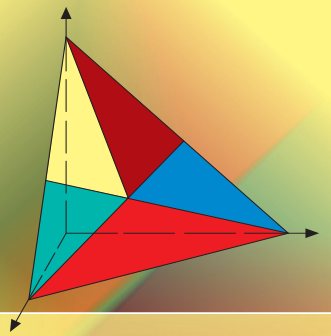
ISBN 978-3-319-43599-2

▸ springer.com

Kreuzer · Robbiano

Computational Linear and Commutative Algebra

Martin Kreuzer
Lorenzo Robbiano



Computational Linear and Commutative Algebra

Springer

1 Endomorphisms

- Generalized Eigenspaces
  - Big Kernels and Small Images
  - Minimal Polynomials and Eigenspaces
- Minimal and Charachteristic Polynomials
- Nilpotent Endomorphisms and Multiplicities
- Commendable Endomorphisms
- Other Special Endomorphisms

2 Families of Commuting Endomorphisms

- Commuting Families
- Kernels and Big Kernels of Ideals
  - Properties of Zero-Dimensional Rings
  - Properties of Kernels and Big Kernels of Ideals
- Eigenfactors
- Joint Eigenspaces
- Cyclic Vector Spaces
- Splitting Endomorphisms
- Commendable Families
- Simultaneous Diagonalization and Triangularization

3 Special Families of Endomorphisms

- $\mathcal{F}$-Cyclic Vector Spaces
- Unigenerated Families
- Commendable Families
- Local Families
- Dual Families
- Extended Families

4 Zero-Dimensional Affine Algebras

- Multiplication Endomorphisms
- Primary Decomposition and Separators
- Commendable and Splitting Multiplication Endomorphisms
- Local Multiplication Families
- Dual Multiplication Families
- Hilbert Functions and the Cayley-Bacharach Property

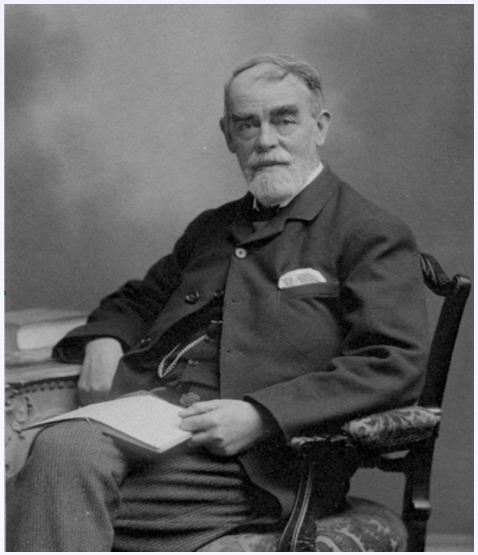
5 Computing Primary and Maximal Components

- Computing Primary Decompositions
  - Using the Generically Extended Linear Form
  - Using Linear Forms and Idempotents
  - Computing Joint Eigenspaces
- Primary Decomposition over Finite Fields
- Computing Maximal Components via Factorization
  - Minimal Polynomials and Finite Field Extensions
  - Factorizing over Extension Fields
  - Using Factorizations to Compute Maximal Components
- Primary Decompositions Using Radical Ideals
  - Maximal Components via Radical Ideals
  - Primary Components from Maximal Components
- The Separable Subalgebra

6 Solving Zero-Dimensional Polynomial Systems

- Rational Zeros via Commuting Families
  - Computing One-Dimensional Joint Eigenspaces
  - Computing Linear Maximal Ideals
- Rational Zeros via Eigenvalues and Eigenvectors
  - The Eigenvalue Method
  - The Eigenvector Method
- Solving Polynomial Systems over Finite Fields
  - Computing Isomorphisms of Finite Fields
  - Solving over Finite Fields via Cloning
  - Solving over Finite Fields via Univariate Representation
  - Solving over Finite Fields via Recursion
- Solving Polynomial Systems over the Rationals
  - Splitting Fields in Characteristic Zero
  - Solving over the Rational via Cloning

Standard References



Books are like imprisoned souls
till someone takes them
down from a shelf and frees them.

(Samuel Butler, 1875–1941)

M. Kreuzer – L. Robbiano: Computational Commutative Algebra 1, Springer (2000)

M. Kreuzer – L. Robbiano: Computational Commutative Algebra 2, Springer (2005)

The new book took six years to be completed.

M. Kreuzer – L. Robbiano: Computational Linear and Commutative Algebra, Springer (2016)

It is dedicated to the memory of our friend Tony Geramita who passed away on June 22, 2016.

Sources and Motivation 1

Figure: Daniel Lazard

Stickelberger's Eigenvalue Theorem (1920) in Number Theory, rediscovered in the context of commutative algebra by Lazard (1981).

Let P/I be a zero-dimensional affine K-algebra, let $f \in P$ and ϑ_f the corresponding multiplication map of P/I.

- If there exists a point $p \in \mathcal{Z}_K(I)$ then $f(p) \in K$ is an eigenvalue of ϑ_f.
- If $\lambda \in K$ is an eigenvalue of ϑ_f then there is $p \in \mathcal{Z}_{\overline{K}}(I)$ with $\lambda = f(p)$.

Sources and Motivation 2

Figure: Auzinger Stetter Möller

Auzinger-Stetter-Möller (1988,...)

Rediscovered this connection and obtained several results, mostly related to non-exact solutions of systems of polynomial equations.

Sources and Motivation 3

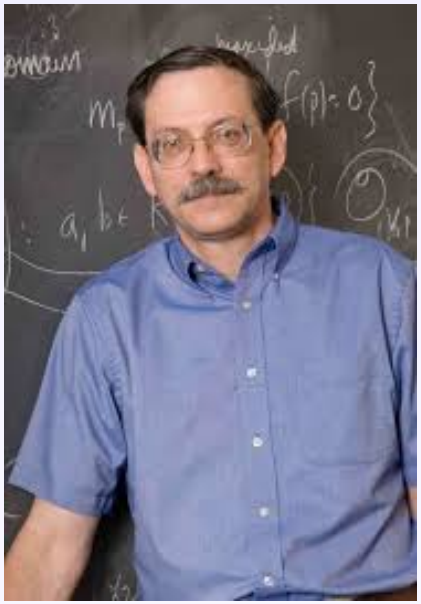


Figure: David Cox

Cox (2005)

Solving equations via algebras, in: A. Dickenstein and I. Emiris (eds.), Solving Polynomial Equations, Algorithms and Comp. in Math. **14**, Springer, Berlin 2005, pp. 63–124.

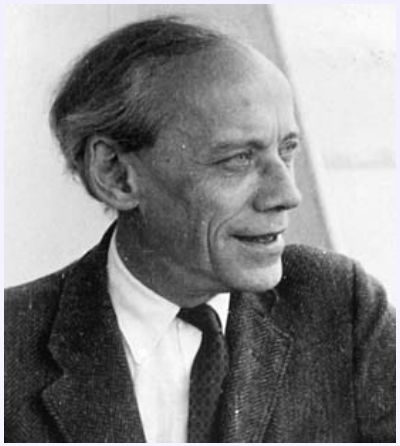
Mainly in the case of an algebraically closed field.

One Endomorphism

I would like to understand things better,
but I dont want to understand them perfectly.

(Douglas R. Hofstadter 1945–)

Characteristic and Minimal Polynomials



It is my experience that proofs involving matrices can be shortened by 50% if one throws the matrices out.

(Emil Artin 1898–1962)

Let K be a field, let V be a finite-dimensional K-vector space, and let $\varphi \in \mathrm{End}_K(V)$ be a K-endomorphism of V.

Definition

The polynomial $\chi_\varphi(z) = \det(z\ \mathrm{id}_V - \varphi)$ is called the characteristic polynomial of φ.

Since $\mathrm{End}_K(V)$ is a finite-dimensional K-vector space, the kernel of the substitution homomorphism $\varepsilon : K[z] \longrightarrow K[\varphi]$ given by $f(z) \mapsto f(\varphi)$ is a non-zero ideal.

Definition

The monic generator of the ideal $\mathrm{Ker}(\varepsilon)$, i.e. the monic polynomial of smallest degree in this ideal is called the minimal polynomial of φ, and is denoted by $\mu_\varphi(z)$.

Fitting's Lemma

I'd like to buy a new boomerang,
but I don't know how to throw the old one away.

Proposition (Fitting's Lemma)

Consider the chains of K-vector subspaces of V

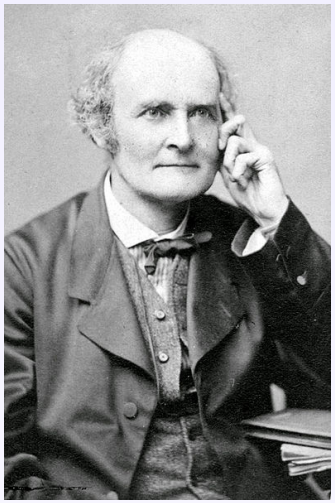
$$\mathrm{Ker}(\varphi) \subseteq \mathrm{Ker}(\varphi^2) \subseteq \cdots \qquad \textit{and} \qquad \mathrm{Im}(\varphi) \supseteq \mathrm{Im}(\varphi^2) \supseteq \cdots$$

(a) *There exists a smallest number $m \geq 1$ such that $\mathrm{Ker}(\varphi^m) = \mathrm{Ker}(\varphi^t)$ for all $t \geq m$. It is equal to the smallest number $m \geq 1$ such that $\mathrm{Im}(\varphi^m) = \mathrm{Im}(\varphi^t)$ for all $t \geq m$.*

(b) *The number m satisfies $\mathrm{BigKer}(\varphi) = \mathrm{Ker}(\varphi^m)$ and $\mathrm{SmIm}(\varphi) = \mathrm{Im}(\varphi^m)$.*

(c) *We have $V = \mathrm{BigKer}(\varphi) \oplus \mathrm{SmIm}(\varphi)$.*

Cayley-Hamilton



Cayley (1821–1895)

Hamilton (1805–1865)

Theorem (Cayley-Hamilton)

Let $\varphi : V \longrightarrow V$ be a K-endomorphism of V.

(a) *The minimal polynomial $\mu_\varphi(z)$ is a divisor of the characteristic polynomial $\chi_\varphi(z)$.*

(b) *The polynomials $\mu_\varphi(z)$ and $\chi_\varphi(z)$ have the same irreducible factors, and hence the same squarefree part.*

Generalized Eigenspaces

Let $\varphi \in \mathrm{End}_K(V)$. We decompose its minimal polynomial and get

$$\mu_\varphi(z) \;=\; p_1(z)^{m_1} \cdots p_s(z)^{m_s}$$

Then the characteristic polynomial of φ factors in this way

$$\chi_\varphi(z) = p_1(z)^{a_1} \cdots p_s(z)^{a_s} \text{ with } a_i \geq m_i$$

Definition

(a) The polynomials $p_1(z), \ldots, p_s(z)$ are called the eigenfactors of φ.

(b) If an eigenfactor $p_i(z)$ of φ is of the form $p_i(z) = z - \lambda$ with $\lambda \in K$ then λ is called an eigenvalue of φ.

(c) For $i = 1, \ldots, s$, the K-vector subspace $\mathrm{Eig}(\varphi, p_i(z)) = \mathrm{Ker}(p_i(\varphi))$ is called the eigenspace of φ associated to $p_i(z)$. Its non-zero elements are called $p_i(z)$-eigenvectors, or simply eigenvectors of φ.

(d) For $i = 1, \ldots, s$, the K-vector subspace $\mathrm{Gen}(\varphi, p_i(z)) = \mathrm{BigKer}(p_i(\varphi))$ is called the generalized eigenspace of φ associated to $p_i(z)$.

Generalized Eigenspaces Decomposition

Main Theorem (Generalized Eigenspace Decomposition)

Let $\varphi \in \mathrm{End}_K(V)$ *and let* $\mu_\varphi(z) = p_1(z)^{m_1} \cdots p_s(z)^{m_s}$.
The vector space V *is the direct sum of the generalized eigenspaces of* φ, *i.e. we have*

$$V = \mathrm{Gen}(\varphi, p_1(z)) \oplus \cdots \oplus \mathrm{Gen}(\varphi, p_s(z))$$

Commendable Endomorphisms

When you transport something by car,
it is called a shipment.
But when you transport something by ship,
it is called cargo.

Definition

The K-linear map $\varphi : V \longrightarrow V$ is called commendable (or non-derogatory) if, for every $i \in \{1, \ldots, s\}$, the eigenfactor $p_i(z)$ of φ satisfies

$$\dim_K(\mathrm{Eig}(\varphi, p_i(z))) = \deg(p_i(z))$$

Equivalently, we require that $\dim_{K[z]/\langle p_i(z)\rangle}(\mathrm{Eig}(\varphi, p_i(z))) = 1$ for $i = 1, \ldots, s$.

Main Theorem (Characterization of Commendable Endomorphisms)

Let $\varphi : V \longrightarrow V$ be a K-linear map. Then the following conditions are equivalent.

(a) *The endomorphism φ is commendable.*

(b) *We have $\mu_\varphi(z) = \chi_\varphi(z)$.*

(c) *The vector space V is a cyclic $K[z]$-module via φ.*

Families of Commuting Endomorphisms

They are strange types of families,
with no fathers, no mothers, no children.
Their only concern is to be commutative.

Commuting Families of Endomorphisms

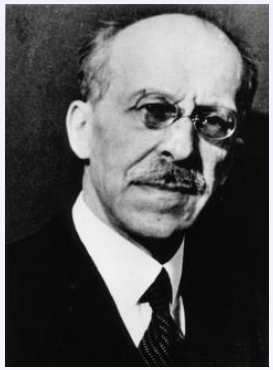
Morally speaking,
matrices should not commute.

Definition

Given a set of commuting endomorphisms S of V, we let $\mathcal{F} = K[S]$ be the commutative K-subalgebra of $\mathrm{End}_K(V)$ generated by S and call it the family of commuting endomorphisms, or simply the commuting family, generated by S.

Since $\mathrm{End}_K(V)$ is a finite-dimensional K-vector space, also $\mathcal{F}$ is a finite-dimensional vector space hence a zero-dimensional K-algebra.

Dimension



Schur (1875–1941)

Jacobson (1910–1999)

Definition

Let $\mathcal{F}$ be a family of commuting endomorphisms of V. The dimension of $\mathcal{F}$ as a ring is zero while $\dim_K(\mathcal{F})$ is the dimension of the family $\mathcal{F}$ as a K-vector space.

Example

If $\varphi \in \mathrm{End}_K(V)$ and $\mathcal{F} = K[\varphi]$, we have $\dim_K(\mathcal{F}) = \deg(\mu_\varphi(z))$.
Therefore, it is $\leq \dim(V)$, with equality if and only if φ is commendable.

- The maximal dimension of a commuting family was determined by J. Schur and N. Jacobson a long time ago: it coincides with $\lfloor d^2/4 \rfloor + 1$ for $d = \dim_K(V)$.

Dimension II

Example

Let $V = K^6$, and let $\mathcal{F}$ be the K-algebra generated by $\{\mathrm{id}_V\}$ and the set of all endomorphisms of V whose matrix with respect to the canonical basis of V is of the form $\left(\begin{smallmatrix} 0 & A \\ 0 & 0 \end{smallmatrix}\right)$ with a matrix A of size 3×3. Then the family $\mathcal{F}$ is commuting, since we have $\left(\begin{smallmatrix} 0 & A \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & B \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & B \\ 0 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & A \\ 0 & 0 \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ for all matrices A, B of size 3×3. Here we have $\dim_K(V) = 6$ and $\dim_K(\mathcal{F}) = 10 = 6^2/4 + 1$, the maximal possible dimension.

In 1961 Murray Gerstenhaber proved that if the family $\mathcal{F}$ is generated by two commuting matrices, the sharp upper bound for the dimension of $\mathcal{F}$ is $\dim_K(V)$.

◇ A sharp upper bound for the dimension of a family generated by three commuting matrices is apparently not known.

Ideal of Relations

WiFi *went down for five minutes,*
so I had to talk to my family.
They seem like nice people.

Definition

Let $\Phi = (\varphi_1, \ldots, \varphi_n)$ be a system of K-algebra generators of $\mathcal{F}$, and let the K-algebra homomorphism $\pi : P \longrightarrow \mathcal{F}$ be defined by letting $\pi(1) = \mathrm{id}_V$ and $\pi(x_i) = \varphi_i$ for $i = 1, \ldots, n$. Then the kernel of π is called the ideal of algebraic relations of Φ and denoted by $\mathrm{Rel}_P(\Phi)$.

$\mathrm{Rel}_P(\Phi)$ can be computed using a nice algorithm called

Buchberger-Möller Algorithm for Matrices

ALGORITHM **(The Buchberger-Möller Algorithm for Matrices)**
Let $\Phi = (\varphi_1, \ldots, \varphi_n)$ be a system of K-algebra generators of $\mathcal{F}$. For every $i \in \{1, \ldots, n\}$, let $M_i \in \mathrm{Mat}_d(K)$ be a matrix representing φ_i with respect to a fixed K-basis of V, and let σ be a term ordering on $\mathbb{T}^n$. Consider the following sequence of instructions.

(1) Let $G = \emptyset, \mathcal{O} = \emptyset, S = \emptyset, \mathcal{N} = \emptyset$, and $L = \{1\}$.

(2) If $L = \emptyset$, return the pair $(G, \mathcal{O})$ and stop.
Otherwise let $t = \min_\sigma(L)$ and delete it from L.

(3) Compute $t(M_1, \ldots, M_n)$ and reduce it against $\mathcal{N} = (N_1, \ldots, N_k)$ to obtain

$$R = t(M_1, \ldots, M_n) - \sum_{i=1}^{k} c_i N_i \qquad \text{with } c_i \in K$$

(4) If $R = 0$, append the polynomial $t - \sum_{i=1}^{k} c_i s_i$ to G, where s_i denotes the i-th element of S. Remove from L all multiples of t. Continue with Step (2).

(5) Otherwise, we have $R \neq 0$. Append R to $\mathcal{N}$ and $t - \sum_{i=1}^{k} c_i s_i$ to S. Append the term t to $\mathcal{O}$, and append to L those elements of $\{x_1 t, \ldots, x_n t\}$ which are neither multiples of a term in L nor in $\mathsf{LT}_\sigma(G)$. Continue with Step (2).

This is an algorithm which computes the reduced σ-Gröbner basis of $\mathrm{Rel}_P(\Phi)$ and a list of terms $\mathcal{O}$ whose residue classes form a vector space basis of $P/\mathrm{Rel}_P(\Phi)$.

Kernels of Ideals

Definition

Let I be an ideal in the commuting family $\mathcal{F}$.

(a) The K-vector subspace $\mathrm{Ker}(I) = \bigcap_{\varphi \in I} \mathrm{Ker}(\varphi)$ of V is called the kernel of I.

(b) The K-vector subspace $\mathrm{BigKer}(I) = \bigcap_{\varphi \in I} \mathrm{BigKer}(\varphi)$ of V is called the big kernel of I.

Theorem (Kernels and Big Kernels of Comaximal Ideals)

Let $I_1, \ldots, I_s$ be pairwise comaximal ideals in the family $\mathcal{F}$, and let $I = I_1 \cap \cdots \cap I_s$.

- *We have* $\mathrm{Ker}(I) = \mathrm{Ker}(I_1) \oplus \cdots \oplus \mathrm{Ker}(I_s)$.
- *We have* $\mathrm{BigKer}(I) = \mathrm{BigKer}(I_1) \oplus \cdots \oplus \mathrm{BigKer}(I_s)$.

Joint Eigenspaces

I read that you can make chocolate fondue from chocolate leftovers.
I am confused. What are chocolate leftovers?

Main Theorem (Joint Generalized Eigenspace Decomposition)

Let $\mathcal{F}$ be a family of commuting endomorphisms of V, and let $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ be the maximal ideals of $\mathcal{F}$.

(a) *We have* $V = \bigoplus_{i=1}^{s} \mathrm{BigKer}(\mathfrak{m}_i)$.

(b) *The joint eigenspaces of $\mathcal{F}$ are* $\mathrm{Ker}(\mathfrak{m}_1), \ldots, \mathrm{Ker}(\mathfrak{m}_s)$.

(c) *The joint generalized eigenspaces of $\mathcal{F}$ are* $\mathrm{BigKer}(\mathfrak{m}_1), \ldots, \mathrm{BigKer}(\mathfrak{m}_s)$.

Splitting Endomorphisms

Can we find a single endomorphism such that its generalized eigenspaces are the joint generalized eigenspaces of the family?

Definition

Let $\mathfrak{m}_1, \ldots, \mathfrak{m}_s$ be the maximal ideals of $\mathcal{F}$, and let $\varphi \in \mathcal{F}$. If we have the equalities $\mathrm{Gen}(\varphi, p_{\mathfrak{m}_i,\varphi}(z)) = \mathrm{BigKer}(\mathfrak{m}_i)$ for $i = 1, \ldots, s$ then φ is called a splitting endomorphism for $\mathcal{F}$.

Proposition

Let $\mathcal{F}$ be a commuting family, and let s be the number of maximal ideals in $\mathcal{F}$. An endomorphism $\varphi \in \mathcal{F}$ is a splitting endomorphism if and only if it has s eigenfactors.

Proposition

If we have $\mathrm{card}(K) \geq \dim_K(\mathcal{F})$ *then there exists a splitting endomorphism for $\mathcal{F}$.*

Brain, n. *An apparatus with which we think that we think.*
(Ambrose Bierce)

Special Families of Endomorphisms

$\mathcal{F}$- cyclic Vector Spaces

Let $S \subseteq \mathrm{End}_K(V)$ be a set of commuting matrices, and let $\mathcal{F} = K[S]$. Then V has a natural structure as an $\mathcal{F}$-module given by $\varphi \cdot v = \varphi(v)$ for all $\varphi \in \mathcal{F}$ and $v \in V$.

ALGORITHM **(Cyclicity Test)**

Let $S = \{\varphi_1, \ldots, \varphi_r\} \subseteq \mathrm{End}_K(V)$ be a set of commuting endomorphisms, let $\mathcal{F}$ be the family generated by the set S, and let $\Phi = (\varphi_1, \ldots, \varphi_r)$. Then let $B = \{v_1, \ldots, v_d\}$ be a basis of V, and, for $i = 1, \ldots, r$, let $A_i \in \mathrm{Mat}_d(K)$ be the matrix representing φ_i in the basis B. Consider the following instructions.

(1) *Using the BM-Algorithm for Matrices compute a tuple of terms $\mathcal{O} = (t_1, \ldots, t_s)$ whose residue classes form a K-basis of $K[x_1, \ldots, x_r]/\mathrm{Rel}_P(\Phi)$.*

(2) *If $s \neq d$ then return* `"Not cyclic"` *and stop.*

(3) *Let $z_1, \ldots, z_d$ be indeterminates. Form the matrix $C \in \mathrm{Mat}_d(K[z_1, \ldots, z_d])$ whose columns are $t_i(A_1, \ldots, A_d) \cdot (z_1, \ldots, z_d)^{\mathrm{tr}}$ for $i = 1, \ldots, d$.*

(4) *Compute the determinant $\Delta = \det(C)$. If $\Delta \neq 0$, find a tuple $(c_1, \ldots, c_d) \in K^d$ such that $\Delta(c_1, \ldots, c_d) \neq 0$, return the vector $v = c_1 v_1 + \cdots + c_d v_d$, and stop.*

(5) *Return* `"Not Cyclic"` *and stop.*

This is an algorithm which checks whether V is a cyclic $\mathcal{F}$-module and, in the affirmative case, computes a generator.

Unigenerated Families

Example

Let φ_1, φ_2 be two $\mathbb{Q}$-endomorphisms of $V = \mathbb{Q}^7$ which are given by the matrices

$$A_1 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -12 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -12 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 7 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 3 & 0 \end{pmatrix} \quad A_2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

We check that $A_1A_2 = A_2A_1$. Hence $\{\varphi_1, \varphi_2\}$ generates a commuting family $\mathcal{F} = \mathbb{Q}[\varphi_1, \varphi_2]$. We have $\chi_{\varphi_1}(z) = \mu_{\varphi_1}(z) = z^7$, while $\mu_{\varphi_2}(z) = z^3$, hence φ_1 is commendable and φ_2 is not.

A theorem shows that $\mathcal{F}$ is unigenerated by φ_1, and that φ_2 is polynomial in φ_1.

Using Buchberger-Möller for Matrices we find

$$A_2 = -\frac{847}{20736} A_1^6 - \frac{85}{1728} A_1^5 - \frac{7}{144} A_1^4 - \frac{1}{12} A_1^3$$

Please do not try by hand!

Commendable Families

"Have you lived in this village all your life?"
"No, not yet"
(Ambrose Bierce)

Definition

Let $\mathcal{F}$ be a family of commuting endomorphisms of the K-vector space V.
The family $\mathcal{F}$ is called commendable if we have the equality

$$\dim_K(\mathrm{Ker}(\mathfrak{m})) = \dim_K(\mathcal{F}/\mathfrak{m}), \text{ equivalently } \dim_{\mathcal{F}/\mathfrak{m}}(\mathrm{Ker}(\mathfrak{m})) = 1$$

for every maximal ideal $\mathfrak{m}$ of $\mathcal{F}$.
If the family $\mathcal{F}$ is not commendable, we also say that it is derogatory.

Dual Families

As usual, let K be a field and V a finite dimensional K-vector space of dimension d. Recall that the dual vector space of V is $V^* = \mathrm{Hom}_K(V, K)$, i.e. the set of all K-linear maps $\ell : V \longrightarrow K$. For a map $\varphi \in \mathrm{End}_K(V)$, the dual endomorphism of φ is the K-linear map $\varphi^\vee : V^* \longrightarrow V^*$ given by $\varphi^\vee(\ell) = \ell \circ \varphi$.

Definition

Let $\mathcal{F}$ be a family of commuting endomorphisms in $\mathrm{End}_K(V)$.

(a) We call $\mathcal{F}^\vee = K[\varphi^\vee \mid \varphi \in \mathcal{F}]$ the dual family of $\mathcal{F}$.

(b) Given an ideal I of $\mathcal{F}$, we call $I^\vee = \langle \varphi^\vee \mid \varphi \in I \rangle$ the dual ideal of I.

Proposition

Let $B = (v_1, \ldots, v_d)$ be a basis of V, let $\varphi \in \mathrm{End}_K(V)$, and let $M_B(\varphi)$ be the matrix which represents φ with respect to B. Then the dual map $\varphi^\vee$ is represented by $M_{B^*}(\varphi^\vee) = (M_B(\varphi))^{\mathrm{tr}}$ with respect to the dual basis B^*.

Fundamental Results

Theorem

Let $\mathcal{F}$ be a family of commuting endomorphisms of V.

(a) *The vector space V is a cyclic $\mathcal{F}$-module if and only if $\mathcal{F}^{\check{}}$ is commendable.*

(b) *The vector space V^* is a cyclic $\mathcal{F}^{\check{}}$-module if and only if $\mathcal{F}$ is commendable.*

Theorem

Let $K \subseteq L$ be a field extension. Then we have the following equivalences.

(a) *The $\mathcal{F}$-module V is cyclic if and only if V_L is a cyclic $\mathcal{F}_L$-module.*

(b) *The family $\mathcal{F}$ is commendable if and only if $\mathcal{F}_L$ is commendable.*

"Look! I solved this puzzle in two days!"
"So what?"
"On the box it says 3–6 years"

Zero-Dimensional Affine Algebras

Multiplication Endomorphisms

In the following we let K be a field and R a zero-dimensional affine K-algebra i.e a zero-dimensional K algebra of type $R = P/I$ where $P = K[x_1, \ldots, x_n]$.
Thus R is a finite dimensional K-vector space, and we let $d = \dim_K(R)$.

Definition

(a) For every element $f \in R$, the multiplication by f yields a K-linear map $\vartheta_f : R \longrightarrow R$ such that $\vartheta_f(g) = f \cdot g$ for all $g \in R$. It is called the multiplication endomorphism by f on R.

(b) The family $\mathcal{F} = K[\vartheta_{x_1}, \ldots, \vartheta_{x_n}]$ is called the multiplication family of R.

(c) Let $B = (t_1, \ldots, t_d)$ be a K-basis of R, and let $f \in R$. Then the matrix $M_B(\vartheta_f) \in \mathrm{Mat}_d(K)$ which represents ϑ_f with respect to the basis B is called the multiplication matrix of f with respect to B.

Proposition

Let $\mathcal{F} = K[\vartheta_{x_1}, \ldots, \vartheta_{x_n}]$ be the multiplication family of R.

(a) *We have $\mathcal{F} = \{\vartheta_f \mid f \in R\}$.*

(b) *The map $\iota : R \longrightarrow \mathcal{F}$ given by $f \mapsto \vartheta_f$ is an isomorphism of K-algebras. Its inverse is the map $\eta : \mathcal{F} \longrightarrow R$ given by $\varphi \mapsto \varphi(1)$, i.e. $\vartheta_f \mapsto f$.*

A Dictionary

At this point we can build a translation table, a dictionary which translates notions from the previous chapters into notions of commutative algebra.

For instance, we can

1. interpret separators as joint eigenvectors,
2. interpret primary decomposition,
3. view commendable and splitting endomorphisms in terms of weakly curvilinear and curvilinear rings,
4. discuss socle elements and maximal nilpotency,
5. checking the Gorenstein and the Cayley-Bacharach property.

The way to get good ideas is
to get lots of ideas
and throw the bad ones away.

(Linus Pauling 1901–1994)

Computing Primary and Maximal Components

Computing the Minimal Polynomial

A key tool for the computation of primary decompositions is the computation of minimal polynomials (of elements or of endomorphisms).

ALGORITHM **(The Minimal Polynomial of an Element, I)**
Let $R = P/I$ be a zero-dimensional affine K-algebra, let $f \in P$, and let $\bar{f}$ be its image in P/I. The following instructions compute the minimal polynomial of $\bar{f}$.

(1) In $P[z]$ form the ideal $J = \langle z - f \rangle + I \cdot P[z]$ and compute $J \cap K[z]$.

(2) Return the monic generator of $J \cap K[z]$.

If a K-basis B of $R = P/I$ is known we can do better.

ALGORITHM **(The Minimal Polynomial of an Element, II)** Let $R = P/I$ be a zero-dimensional affine K-algebra, let $f \in P$, and let $\bar{f}$ be its image in P/I. Suppose that we know a K-basis B of R and an effective method $\mathrm{NF}_B : P \longrightarrow K^d$ which maps an element of P to the coefficient tuple of its residue class in R with respect to the basis B. Then the following instructions compute the minimal polynomial of $\bar{f}$.

(1) Let $L = (1)$.

(2) For $i = 1, 2, \ldots,$ compute $\mathrm{NF}_B(f^i)$ and check whether it is K-linearly dependent on the elements in L. If this is not the case, append $\mathrm{NF}_B(f^i)$ to the tuple L and continue with the next number i.

(3) If there exist $c_0, \ldots, c_{i-1} \in K$ such that $\mathrm{NF}_B(f^i) = \sum_{k=0}^{i-1} c_k \, \mathrm{NF}_B(f^k)$ then return the polynomial $\mu_{\bar{f}}(z) = z^i - \sum_{k=0}^{i-1} c_k z^k$ and stop.

Primary Decomposition over Finite Fields

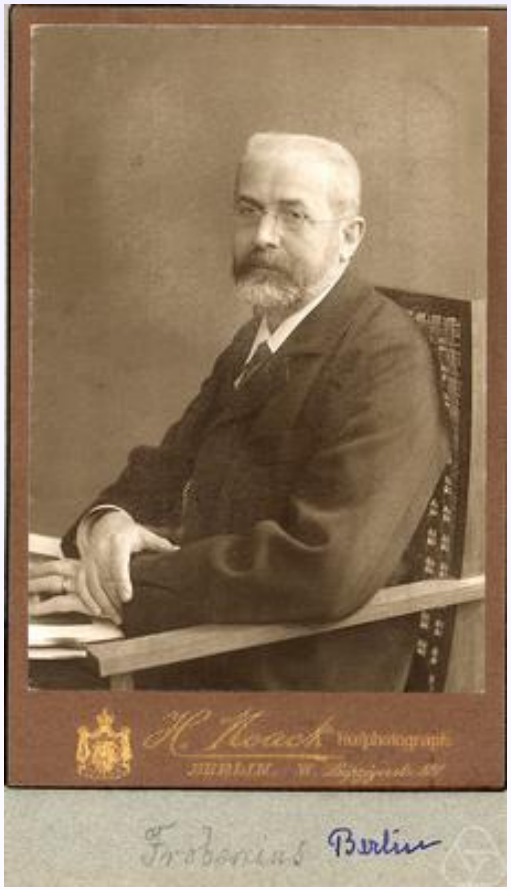


Figure: Ferdinand Georg Frobenius (1849 – 1917)

The Frobenius Endomorphism

In the following we let K be a finite field. Then the characteristic of K is a prime number p and the number of its elements is of the form $q = p^e$ with $e > 0$.

Furthermore, it is known that all fields having q elements are isomorphic. In the following we say that a field K with p^e elements represents $\mathbb{F}_q$.

Definition

Let p be a prime number, and let R be a ring of characteristic p.

(a) The map $\phi_p : R \longrightarrow R$ defined by $a \mapsto a^p$ is a ring endomorphism of R. It is called the Frobenius endomorphism of R.

(b) Suppose that R is an algebra over the field $\mathbb{F}_q$. Then the map $\phi_q : R \longrightarrow R$ defined by $a \mapsto a^q$ is $\mathbb{F}_q$-linear. It is called the q-Frobenius endomorphism of R.

The Frobenius Space

I used to be indecisive. Now I'm not so sure.

Definition

The set

$$\mathrm{Frob}_q(R) \;=\; \mathrm{Eig}(\phi_q, z-1) \;=\; \{f \in R \mid f^q - f = 0\}$$

i.e., the fixpoint space of R with respect to ϕ_q, is called the q-Frobenius space of R.

Main Theorem (Properties of the q-Frobenius Space)

Let R be a zero-dimensional affine $\mathbb{F}_q$-algebra, and let s be the number of primary components of the zero ideal of R.

(a) *We have* $\mathrm{Frob}_q(R) = \{\sum_{i=1}^{s} c_i e_i \mid c_1, \ldots c_s \in \mathbb{F}_q\}$ *where* $e_1, \ldots, e_s$ *are the primitive idempotents of* R.

(b) *We have* $\dim_{\mathbb{F}_q}(\mathrm{Frob}_q(R)) = s$.

To steal ideas from one person is plagiarism;
to steal from many is research
(Steven Wright)

Solving Zero-Dimensional Polynomial Systems

Computing Rational Zeros

In this part of the book we revisit two classical methods used by numerical analysts, the Eigenvalue Method and the Eigenvector Method.

The result of Lazard is now inserted in our general perspective, so that we show how to compute 1-dimensional joint eigenspaces and linear maximal ideals.

An easy corollary is the following

Corollary

For $i = 1, \ldots, n$, the i-th coordinate of the rational zeros of a zero-dimensional polynomial system are the eigenvalues of the multiplication mat ϑ_{x_i}.

The we prove the good Eigenvalue Method and we show an algorithm to compute all the rational zeros more directly.

Using the dual families of multiplication endomorphisms we put the Eigenvector Method in the correct perspective.

Soving Polynomial Systems over Finite Fields

This is a huge section which uses Frobenius Spaces.

In particular it is shown how to explicitly calculate the automorphisms of a finite field. They are easy to describe formally since the Galois group is easy, but we describe several algorithms to explicitly compute them.

Example

Let $K = \mathbb{F}_{101}$, and let $L = K[x]/\langle f(x)\rangle$ be the field with $q = 101^4$ elements defined by $f(x) = x^4 + 41\,x^3 - 36\,x^2 + 39\,x - 12$.
The four K-automorphisms of L are
Identity
$\bar{x} \mapsto 34\,\bar{x}^3 + 20\,\bar{x}^2 - 3\,\bar{x} - 41$
$\bar{x} \mapsto 4\,\bar{x}^3 + 47\,\bar{x}^2 - 29\,\bar{x} - 35$,
$\bar{x} \mapsto 34\,\bar{x}^3 + 34\,\bar{x}^2 + 31\,\bar{x} + 35$

Soving Polynomial Systems over the Rationals

This algorithm has been proved to work,
but has never been observed to do so.

(Alexander Barvinok, University of Michigan)

If we want exact solution, our power is very limited. For instance suppose we want to find the smallest field which contains all the solutions to $x^5 - x - 2 = 0$.
We let $f(x) = x^5 - x - 2$ and use a nice tool called the Splitting Algebra.

Let $y_1, \ldots, y_5$ be new indeterminates, let $s_1, \ldots, s_5$ be the elementary symmetric polynomials in $y_1, \ldots, y_5$, and let $P = K[y_1, \ldots, y_5]$. Then the splitting algebra of $f(x)$ is $S_f = P/\langle s_1,\ s_2,\ s_3,\ s_4 + 1,\ s_5 - 2\rangle$ and its dimension is $5! = 120$.

The key is to show that S_f is a field. This is done if we find an element in S_f whose minimal polynomial is irreducible and has degree 120.
We choose $\ell = y_1 + 2\,y_2 + 3\,y_3 + 4\,y_4 + 5\,y_5$ in P and compute the minimal polynomial $\mu_{\bar{\ell}}(z)$ of its residue class $\bar{\ell}$ in S_f.
We get the world's first seven star polynomial who had degree 120 and is irreducible.

The Burj al Arab Polynomial

$$
\begin{aligned}
& z^{120} \\
& + 900\, z^{116} \\
& + 508450\, z^{112} \\
& + 12375000\, z^{110} \\
& + 233445700\, z^{108} \\
& + 24978500000\, z^{106} \\
& + 86356219375\, z^{104} \\
& + 24591849375000\, z^{102} \\
& - 643754458910680\, z^{100} \\
& + 13397352506250000\, z^{98} \\
& - 193920628655076100\, z^{96} \\
& + 5239487723543750000\, z^{94} \\
& + 151978050797489672200\, z^{92} \\
& + 16019140173955088000000\, z^{90} \\
& + 1639052718724913338225 75\, z^{88} \\
& + 185711515314110942497500 00\, z^{86} \\
& + 89120445389616729179232500\, z^{84} \\
& + 10283912347310917452507500000\, z^{82} \\
& + 19866996525484310004765605821 0\, z^{80} \\
& + 4070169309233973479213196875000\, z^{78} \\
& + 13221410515800598227911779540290 0\, z^{76} \\
& + 10875160527804493825834956375000 00\, z^{74} \\
& + 60508849602393530392200938144445825\, z^{72} \\
& + 34766091141322443199093714056487500 0\, z^{70} \\
& + 16588200299196393742971771206570751200\, z^{68} \\
& + 33981578691557116589668851748579225000 0\, z^{66} \\
& + 17912716377537485011344833574489313000 00\, z^{64} \\
& + 10339989209288556172827143758102707500000 0\, z^{62} \\
& + 42781400263648014224518386947751638108944 0\, z^{60} \\
& + 79150070450087244766506809693886396500000 00\, z^{58} \\
& + 81063308246656004478011855097587950132006400\, z^{56} \\
& - 58166475752540506274387604979739567990000000 0\, z^{54} \\
& + 25602517447858531609031664885636569764001139200\, z^{52} \\
& - 33633709822020820727901080972825109836891200000 0\, z^{50} \\
& + 18777015324849883497072748537676712863638811875200\, z^{48} \\
& + 73307905946928174406128646864582738317564096000000\, z^{46} \\
& - 26982108991099369935732234474903468304652774400000 0\, z^{44} \\
& + 38479638527556330568997409673280988610752236800000 00\, z^{42} \\
& + 29901468960195230389988192738702179827930958042308 6080\, z^{40} \\
& + 42558998888103731720782157592320186942179161600000000\, z^{38} \\
& - 34721407124436627734704650884378604156563297405428121600\, z^{36} \\
& - 28501353116590344979210699634202748421752041241600000000\, z^{34} \\
& - 50490001735908587203119862921024550428531818527437946880 0\, z^{32} \\
& + 20153310691018337975446390185898297311743029640726528000000\, z^{30} \\
& + 21088321914096711690237205513699115109847237886097503027200\, z^{28} \\
& + 91973334995806935195413729241109562880392423979305369600000 0\, z^{26} \\
& + 20811017573464598985212561659428623245292245157485824819200 00\, z^{24} \\
& + 24920911291118865150451589694329489416904590835806658560000000\, z^{22} \\
& + 10789634922927202729701784573208260334862050602933605392973824\, z^{20} \\
& + 10717989001030340676381749813627759760756951327667200000000000\, z^{18} \\
& - 44382053095550524848343631937377293229538844407267104522240000 0\, z^{16} \\
& + 61783751232531585264871826115160196817555598688937410560000000\, z^{14} \\
& - 19651173503497822355767558381299175535603107419910266880000000 0\, z^{12} \\
& + 17057058181130156999312934476928723862270895272267776000000000000\, z^{10} \\
& + 24365639973684917858679310359271336781135285690368000000000000\, z^{8} \\
& + 40615589227675119914100324987801198834835087820800000000000000000\, z^{6} \\
& + 21508468021796121727365079945754432878804887808000000000000000000\, z^{4} \\
& + 12368003557410966199224287239940288183979630080000000000000000000\, z^{2} \\
& + 53899832988697131573013337804587950520590400000000000000000000
\end{aligned}
$$

In the Last Page of the Book

One way to continue would be to find good approximations to the zeros of...

This brings us to the topics of floating point calculations and error estimates which are well outside the scope of this volume.

A man only becomes wise when he begins to calculate
the approximate depth of his ignorance.
(Gian Carlo Menotti)

The book ends with the following sentences.

Thus we have reached the end of this book.
Or should we say that we have approximately reached the end of the book?

For sure we have reached the

end of my presentation