Introduction

There has been no exhaustive book on this subject in this country, and [this book] fills a much-needed gap.
(from an 1895 book review)

Why Was This Book Written?

Six years ago the authors were invited to give a short series of lectures on applications of Linear Algebra to Polynomial System Solving at the Indian Institute of Science in Bangalore. After being asked to produce lecture notes, we discovered a "much-needed gap" and decided to fill it by writing a short overview article. While working on this endeavour, we experienced numerous eureka moments and discovered traumatic gaps in our presumed knowledge of Linear Algebra. What is the big kernel of an endomorphism? How do you define its eigenspaces if its characteristic polynomial has no zeros, i.e., if there are no eigenvalues? What is the kernel of an ideal?

In the process of answering these natural questions, our manuscript soon exceeded the size acceptable to a journal. So, we planned to go for a new publication form, the *SpringerBriefs* instead. The first tentative title was "**Co**mputational **C**ommutative **A**lgebra and **Co**mputational **L**inear **A**lgebra," until we realized that its natural acronym had already been trademarked. And while we were worrying for two years about important questions such as whether a vector space is a cyclic module over a commuting family if and only the dual family is commendable, the *Brief* continued to grow. After breaching the 150-page-mark, we had to abandon all pretence, and admit that we were really working on the third volume of the trilogy.

Fortunately, our troubles with Linear Algebra were soon over, and we considered putting all applications into a last, final chapter. But even the best-laid plans of mice and men go oft awry, which in our case meant that both the discoveries of disconcerting knowledge gaps and the subsequent eureka moments continued unabated. Linear Algebra turned out to have numerous, deep and wonderful applications to

the algebra and geometry of zero-dimensional commutative rings, to computing primary and maximal components of polynomial ideals, and finally to solving polynomial systems. Once again, instead of ending in a few short last sections, the book doubled in size.

All told, what have we done? We tried to understand the interconnections between two topics that now make up the title: Computational Linear and Commutative Algebra. We extended a part of Linear Algebra, which had hitherto been primarily used by numerical analysts, to a theory which works for finite dimensional vector spaces over an arbitrary base field. We put many known and unknown algorithms into a general framework for computing with zero-dimensional polynomial ideals and zero-dimensional affine algebras. Did we succeed? Will that much-needed 3 cm gap on your bookshelf be filled forever? You be the Judge!

What Is This Book About?

The secret of good writing
is to say an old thing in a new way,
or to say a new thing in an old way.
(Richard H. Davis)

Our previous two volumes contained 43 sections in 6 chapters, supported by 349 exercises, 99 tutorials, and 9 appendices. This book contains 45 sections in 6 chapters, supported by 0 exercises, 0 tutorials, and 0 appendices. *What happened?*

As the above brief history of this book indicates already, it has a very different flavour: rather than being the outgrowth of numerous lecture courses, it is an account of our quest to understand some connections between Linear Algebra and Commutative Algebra, a quest which outgrew our original intentions.

Let us have a quick low-voltage ride through the contents, following the current of ideas without being shorted by the surplus of their power. The first three chapters of this book develop what we sometimes, modestly, call "Linear Algebra 1.5" to emphasize its natural connection to the material taught in first year courses, and sometimes, less modestly, the "Linear Algebra of the Third Millennium" to point out its ubiquity, wide applicability, and novel point of view. The initial insight is that one does not need eigenvalues to define the theory of eigenspaces and generalized eigenspaces. In fact, over an arbitrary base field, an endomorphism of a finite dimensional vector space does in general not have eigenvalues. But the role of these numbers can be played by the irreducible factors of the minimal polynomial, for which we therefore coined the new term *eigenfactors*.

Another key concept is the property of an endomorphism to be *commendable*. In spite of this notion having been useful previously for numerical analysts under the derogatory name "non-derogatory endomorphism", its power and beauty seem hitherto to have gone largely unnoticed in algebraic communities. In the last part of the first chapter we aim to change this.

Then, in Chaps. 2 and 3, we extend this theory to commuting families, i.e., to families of endomorphisms which commute pairwise. A commuting family is a finitely generated, commutative algebra over the base field. As such, it has ideals, and one of the main ideas is to form the kernel of an ideal, i.e., the intersection of the kernels of all endomorphisms in the ideal. Then, as a generalization of the well-known result for two commuting matrices, a commuting family has joint eigenspaces, which are the kernels of its maximal ideals, and joint generalized eigenspaces, which are the kernels of the primary components of its zero ideal. Thus we arrive at a deep and intricate connection between the decomposition of a vector space into the direct sum of the joint generalized eigenspaces of a commuting family and the primary decomposition of the zero ideal of the family.

In the third chapter, the central topic is to transfer the concept of commendability to a family. It turns out that this does not imply that any of the endomorphisms in the family has to be commendable, but is strong enough for the main theorem of the chapter: a family is commendable if and only if the vector space is a cyclic module with respect to the dual family. As abstract and ivory-towerly this may seem, it is the heart of some of the most powerful algorithms later on.

Chapters 4, 5, and 6 comprise the Computational Commutative Algebra side of the coin. In the fourth chapter a zero-dimensional affine algebra R over a field K is identified with a commuting family via its multiplication family $\mathscr{F}$. This identification brings the extensive linear algebra preparations to fruition, and surprising connections between the two fields appear: the generalized eigenspaces of $\mathscr{F}$ are the local factors of R, the joint eigenvectors of $\mathscr{F}$ are the separators of R, there is a commendable endomorphism in $\mathscr{F}$ if and only if R is curvilinear, and the family $\mathscr{F}$ is commendable if and only if R is a Gorenstein ring.

In the fifth chapter we commence the algorithmic applications by gathering together methods for computing the primary and maximal components of a zero-dimensional polynomial ideal. We offer a wide variety of tools, ranging from generically extended linear forms, idempotents, factorization over extension fields, and radical ideal computation to highly specialized instruments for harnessing the power of the Frobenius homomorphism in finite characteristic.

The final chapter is no less ambitious. In our toolbox for solving polynomial systems, we use one-dimensional joint eigenspaces, eigenvalues and eigenvectors, and we even resort to cloning ideals and fields! As long as we are content to determine the K-rational solutions of the system, or to deal with systems defined over a finite field K, we find reasonably efficient algorithms. But when we try to solve polynomial systems over the rationals, i.e., to describe the solutions in suitable number fields, even the most ingenious exact methods quickly reach their limits.

Altogether, writing this book allowed us to delve into a labyrinth of ideas and techniques combining linear algebra, commutative algebra and computer algebra.

Successfully mastering this material is a *tour de force*, and when you emerge you will be blessed with a quantum leap of knowledge. For us, it also meant achieving full awareness and understanding of our limited ability to comprehend mathematics, life, the universe, and everything. The contents of this book, and a substantial loss of free time, are mainly due to the fact the we did *not* heed the following advice.

Write what you know.
That should leave you with a lot of free time.
(Howard Nemerov)

Who Invented This Theory?

There is an old saying about those who forget history.
I don't remember it, but it's good.

Let us not forget the history of this book. A large dose of inspiration came from a few good sources. In spite of us checking dozens of more recent books on Linear Algebra, the single most useful foundation for much of the material in the first chapters was the book by K. Hoffman and R. Kunze which appeared in 1971 (see [9]). The applications of these linear algebra methods to commutative algebra and computer algebra benefited greatly from the wonderful overview article [3] by D. Cox. The original impetus for this book, now underlying some parts of Chap. 6, came from our attempts to transfer the numerical methods in H. Stetter's book [28] to the language of Computational Commutative Algebra.

Besides these main sources, we scoured an immense number of research papers before coming to the generalizations and the new ideas presented here. They are too numerous to be mentioned individually in this introduction, but at the beginning of the relevant sections we cite the most important previous works.

What is the history of studying connections between Linear Algebra and Computational Commutative Algebra? Are there any lessons to be learned from it? After D. Lazard pointed out a relation between eigenvalues and solutions of polynomial systems in [18], not much happened until 1988 when numerical analysts W. Auzinger and H. Stetter constructed a working algorithm to solve polynomial systems via Linear Algebra techniques (see [1]). A few years later H.M. Möller and R. Tenberg contributed some important algorithmic improvements (see [22]).

How did algebraists react to these exciting developments? Very mildly indeed. Besides a useful characterization of commuting matrices by B. Mourrain (see [24]) and the aforementioned overview article by D. Cox, we found little evidence of efforts to bridge the gap between the subjects and to develop a solid algebraic theory. For instance, few authors tried to forego the convenience of an algebraically closed ground field and to work over an arbitrary base field, although this is indispensable for performing symbolic computations.

What Is This Book *Not* About?

Judicious omissions create a great _____.

Just like the previous two volumes, this book is *not* about soccer, chess, gardening, photography, twisty puzzles, and our other favourite pastimes. Even within mathematics, it has gaping holes. For instance, although Linear Algebra is part of its title, you will search in vain for the fields of real and complex numbers. There is a twofold reason for this. Firstly, the Linear Algebra treated here is the theory of finite dimensional vector spaces over an arbitrary field, with the real and complex numbers just being special examples. Secondly, the title of the book also contains the word "computational", and the fields of real or complex numbers are not computable. In our exact world, the real numbers are surreal, and the complex numbers are too complex. For similar reasons you will not find anything about Numerical Linear Algebra here. Such numerical computations involve the set of floating point numbers, and this set is not a field. However, we note that this was the context in which many of the results about commendable matrices and commuting families were first discovered.

Another omission is complexity theory. Since we are in finite dimensional vector spaces, all algorithms have polynomial complexity. But for us what really counts is their *practical complexity*: how long do I have to wait for the output? Unfortunately, for this, even a constant time algorithm can take a lifetime if the constant is too big. The actual running time of the algorithms depends to a large degree on the skill of the implementators which we praise highly, but cannot explain mathematically.

The final gap appears at the end of the last chapter. Our quest to solve polynomial systems using the Computational Linear and Commutative Algebra methods presented here grinds to a halt for *big* polynomial systems over the field of rational numbers. To continue further, we would have to leave the world of exact computation and enter the *world of approximation*; but this world is beyond the reach of the rockets fuelled by the material in this book. The reader who is interested in the approximate realm is invited to look at the books [4, 25], and [28], where many bridges between symbolic and numeric methods are built. Our obsession in this book is to be exact, even if this means that we have to cope with a limited world.

You're on Earth.
There's no cure for that.
(Samuel Beckett)

How Was This Book Written?

I'm writing a book.
I've got the page numbers done.
(Steven Wright)

This book was written in our favourite style, a blend of Italian imagination and German rigour. We filled it with many jokes and quotations to keep you entertained even when the going gets tough. In our opinion, with which we fully agree, an ideal section should contain at least one theorem and one joke. And they should not be the same.

One of the highlights of this book is the inclusion of very many examples. We are convinced that a good grasp of the mathematical ideas we present has to be underpinned by meaningful, non-trivial examples. Almost all of them were computed with CoCoA (see [2]), our favourite computer algebra system. The source files of these examples are freely available on *SpringerLink* as Electronic Supplementary Material (ESM) linked to the corresponding chapters. Even some developments of the theory were only possible because of the inspiration derived from computing appropriate examples with CoCoA. *Thank you, CoCoA!*

One of the main challenges every author faces, besides getting the page numbers done, is to choose the best terminology and notation. Fortunately, many of these difficulties have already been resolved, for better or for worse, in our previous volumes [15] and [16]. So, unless explicitly stated otherwise, we follow the notation and definitions introduced there. There is one minor difference: the ideal generated by a set of elements $\{f_1, \ldots, f_s\}$ is now denoted by $\langle f_1, \ldots, f_s \rangle$, i.e., the parentheses have evolved into angle brackets. Every now and then, we take the liberty to use slightly imprecise notation such as $\mathrm{Ker}(A)$ for the null space of a matrix, or to denote the residue class of an indeterminate x_i in a ring $K[x_1, \ldots, x_n]/I$ by x_i rather than $\bar{x}_i$. We hope that no confusion arises by this occasional lack of German rigour.

Besides the substantial gaps in nomenclature, which we filled generously with our own creations, there is one important point where we decided to ignore the majority and break with tradition. In the literature, an endomorphism of a finite dimensional vector space is called *non-derogatory* if its characteristic and minimal polynomials coincide. This property can be defined using several equivalent conditions, and plays an important role throughout this book.

Frequently, when we lectured about this topic, our listeners would get confused by calling such a good property "non-bad". Would you call a rich person "non-poor"? Would you call an exciting game "non-boring"? Would you call a beautiful picture "non-ugly"? We wouldn't, and hence we introduced the notion of a *commendable* endomorphism. Of course, if an endomorphism is not commendable, it is still derogatory.

Furthermore, we have tried to keep this book as self-contained as possible. Clearly, we require that the reader has purchased and read the previous two volumes, as we do not hesitate to cite from them. Apart from that, we quote a few results from other theories not covered here if their inclusion would have led us too

far astray, but in general we believe that the book can be read from cover to cover without missing anything important if the only outside sources are [15] and [16].

Although we tried to write and proofread this book as carefully as we could, we suspect that we overlocked many errors and typos. This suspicion is fuelled by the fact that, whenever we entered a period of intense work on the book, we had to start by changing Sect. 1.1 substantially. Even though one of the early readers of the first volume noted that the book was remarkably error-free and that he found the first misprint after more than 100 pages, we later discovered that in truth Definition 1.1.1, the definition of a ring, contained an error. This proved to us that, no matter how many corrections you do, there are still infinitely many errors left.

One man is as good as another
until he has written a book.
(Benjamin Jowett)

And What Is This Book Good for?

It is impossible for a man to learn
what he thinks he already knows.
(Epictetus, 55–135 A.D.)

Like its two siblings, this book is good for learning, teaching, reading, and most of all, enjoying the topic at hand. Since much of the material presented here is not available elsewhere, the main application of this book is to learn something new. When you want to learn something, it is better not to know everything already. Certainly, we are not young enough to know everything. It is our continuing mission to boldly go where few men have gone before. Come on, join the joyride!

The second application is teaching. We tried to write this book in a way that a curious undergraduate student should not have any serious difficulties understanding it. Thus it can be used as a textbook for advanced undergraduate and for graduate courses in Computational Linear and Commutative Algebra.

The third application is as a research monograph. A couple of months in the laboratory can frequently save a couple of hours in the library. But reading this book for a couple of hours may provide you with research ideas for a couple of years. And if not, there is much pleasure to be gained from useless knowledge.

But are there any *true* applications of this theory? These days, even the purest and most abstract mathematics is in danger of being applied. The technique of solving real world problems by modelling them using polynomial equations has led to unexpected successes and crushing defeats alike. Can the contents of this book be applied to the real world? Even if all is well and good in practice, how does it work in theory?

The polynomial systems considered in this book are all of very modest size. Most algorithms have a running time which is polynomial in the dimension of the

underlying vector spaces. In typical real world applications, this dimension will be forbiddingly large. These are the conclusions on which we base our facts, and the upshot is that the road to successful applications is always under construction. On the other hand, how would you classify an algorithm for checking whether a zero-dimensional affine algebra is a Gorenstein ring? Is this *pure* mathematics?

Any mathematics is applied mathematics
when it is being applied to something;
when it is not, it is pure mathematics.
(Robert D. Richtmyer)

Some Final Words of Wisdom

Mellonta Tauta
[Those things that are to be]
(Sophocles (441 B.C.), Edgar A. Poe (1849), Pundita (2848))

What lies ahead of us? In particular, what comes after a trilogy? A tetralogy? According to Wikipedia, in the Greek theater a tetralogy was a group of three tragedies followed by a satyr play. Including the present book, we have already written three pieces of drama filled with satirical jokes, so we can definitely declare that our job is over. Or is it?

There are always so many urgent things,
there's never time for the important ones.
(Massimo Caboara)

http://www.springer.com/978-3-319-43599-2

Computational Linear and Commutative Algebra

Kreuzer, M.; Robbiano, L.

2016, XVIII, 321 p. 1 illus., Hardcover
ISBN: 978-3-319-43599-2