国外数学名著系列(续一)

(影印版)49

Harm Derksen Gregor Kemper

Computational Invariant Theory

计算不变量理论

科学出版社
www.sciencep.com

图字：01-2008-5399

图书在版编目(CIP)数据

计算不变量理论=Computational Invariant Theory / (美)德克森(Derksen, H.)等著. —影印版. —北京：科学出版社, 2009
(国外数学名著系列; 49)
ISBN 978-7-03-023492-6
I. 计… II. 德… III. 不变量-理论-英文 IV. O174
中国版本图书馆 CIP 数据核字(2008) 第 186186 号

责任编辑：范庆奎/责任印刷：钱玉芬/封面设计：黄华斌

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com
双青印刷厂印刷
科学出版社发行　各地新华书店经销
*
2009 年 1 月第　一　版　开本：B5(720 × 1000)
2009 年 1 月第一次印刷　印张：17 3/4
印数：1—2 500　字数：338 000
定价：66.00 元
(如有印装质量问题，我社负责调换〈双青〉)

《国外数学名著系列》(影印版)序

要使我国的数学事业更好地发展起来，需要数学家淡泊名利并付出更艰苦地努力。另一方面，我们也要从客观上为数学家创造更有利的发展数学事业的外部环境，这主要是加强对数学事业的支持与投资力度，使数学家有较好的工作与生活条件，其中也包括改善与加强数学的出版工作。

从出版方面来讲，除了较好较快地出版我们自己的成果外，引进国外的先进出版物无疑也是十分重要与必不可少的。从数学来说，施普林格(Springer)出版社至今仍然是世界上最具权威的出版社。科学出版社影印一批他们出版的好的新书，使我国广大数学家能以较低的价格购买，特别是在边远地区工作的数学家能普遍见到这些书，无疑是对推动我国数学的科研与教学十分有益的事。

这次科学出版社购买了版权，一次影印了 23 本施普林格出版社出版的数学书，就是一件好事，也是值得继续做下去的事情。大体上分一下，这 23 本书中，包括基础数学书 5 本，应用数学书 6 本与计算数学书 12 本，其中有些书也具有交叉性质。 这些书都是很新的，2000 年以后出版的占绝大部分，共计 16 本，其余的也是 1990 年以后出版的。这些书可以使读者较快地了解数学某方面的前沿，例如基础数学中的数论、代数与拓扑三本，都是由该领域大数学家编著的“数学百科全书”的分册。对从事这方面研究的数学家了解该领域的前沿与全貌很有帮助。按照学科的特点，基础数学类的书以“经典”为主，应用和计算数学类的书以“前沿”为主。这些书的作者多数是国际知名的大数学家，例如《拓扑学》一书的作者诺维科夫是俄罗斯科学院的院士，曾获“菲尔兹奖”和“沃尔夫数学奖”。这些大数学家的著作无疑将会对我国的科研人员起到非常好的指导作用。

当然，23 本书只能涵盖数学的一部分，所以，这项工作还应该继续做下去。更进一步，有些读者面较广的好书还应该翻译成中文出版，使之有更大的读者群。

总之，我对科学出版社影印施普林格出版社的部分数学著作这一举措表示热烈的支持，并盼望这一工作取得更大的成绩。

王 元

2005 年 12 月 3 日

To Maureen, William, Claire

To Elisabeth, Martin, Stefan

Preface

Invariant theory is a subject with a long tradition and an astounding ability to rejuvenate itself whenever it reappears on the mathematical stage. Throughout the history of invariant theory, two features of it have always been at the center of attention: computation and applications. This book is about the computational aspects of invariant theory. We present algorithms for calculating the invariant ring of a group that is linearly reductive or finite, including the modular case. These algorithms form the central pillars around which the book is built. To prepare the ground for the algorithms, we present Gröbner basis methods and some general theory of invariants. Moreover, the algorithms and their behavior depend heavily on structural properties of the invariant ring to be computed. Large parts of the book are devoted to studying such properties. Finally, most of the applications of invariant theory depend on the ability to calculate invariant rings. The last chapter of this book provides a sample of applications inside and outside of mathematics.

Acknowledgments. Vladimir Popov and Bernd Sturmfels brought us together as a team of authors. In early 1999 Vladimir Popov asked us to write a contribution on algorithmic invariant theory for Springer's Encyclopaedia series. After we agreed to do that, it was an invitation by Bernd Sturmfels to spend two weeks together in Berkeley that really got us started on this book project. We thank Bernd for his strong encouragement and very helpful advice. During the stay at Berkeley, we started outlining the book, making decisions about notation, etc. After that, we worked separately and communicated by e-mail. Most of the work was done at MIT, Queen's University at Kingston, Ontario, Canada, the University of Heidelberg, and the University of Michigan at Ann Arbor. In early 2001 we spent another week together at Queen's University, where we finalized most of the book. Our thanks go to Eddy Campbell, Ian Hughes, and David Wehlau for inviting us to Queen's.

The book benefited greatly from numerous comments, suggestions, and corrections we received from a number of people who read a pre-circulated version. Among these people are Karin Gatermann, Steven Gilbert, Julia Hartmann, Gerhard Hiß, Jürgen Klüners, Hanspeter Kraft, Martin Lorenz, Kay Magaard, Gunter Malle, B. Heinrich Matzat, Vladimir Popov, Jim Shank, Bernd Sturmfels, Nicolas Thiéry, David Wehlau, and Jerzy Weyman.

We owe them many thanks for working through the manuscript and offering their expertise. The first author likes to thank the National Science Foundation for partial support under the grant 0102193. Last but not least, we are grateful to the anonymous referees for further valuable comments and to Ms. Ruth Allewelt and Dr. Martin Peters at Springer-Verlag for the swift and efficient handling of the manuscript.

Ann Arbor and Heidelberg,
March 2002

Harm Derksen
Gregor Kemper

Table of Contents

Introduction

> "Like the Arabian phoenix rising out of the ashes, the theory of invariants, pronounced dead at the turn of the century, is once again at the forefront of mathematics. During its long eclipse, the language of modern algebra was developed, a sharp tool now at last being applied to the very purpose for which is was invented." (Kung and Rota [157])

A brief history. Invariant theory is a mathematical discipline with a long tradition, going back at least one hundred and fifty years. Sometimes its has blossomed, sometimes it has lain dormant. But through all phases of its existence, invariant theory has had a significant computational component. Indeed, the period of "Classical Invariant Theory", in the late 1800s, was championed by true masters of computation like Aronhold, Clebsch, Gordan, Cayley, Sylvester, and Cremona. This classical period culminated with two landmark papers by Hilbert. In the first [107], he showed that invariant rings of the classical groups are finitely generated. His non-constructive proof was harshly criticized by Gordan (see page 49 in this book). Hilbert replied in the second paper [108] by giving constructive methods for finding all invariants under the special and general linear group. Hilbert's papers closed the chapter of Classical Invariant Theory and sent this line of research into a nearly dormant state for some decades, but they also sparked the development of commutative algebra and algebraic geometry. Indeed, Hilbert's papers on invariant theory [107, 108] contain such fundamental results as the Nullstellensatz, the Basis Theorem, the rationality of what is now called the Hilbert series, and the Syzygy Theorem. The rise of algebraic geometry and commutative algebra had a strong influence on invariant theory—which never really went to sleep—as might be best documented by the books by Mumford et al. [169] (whose first edition was published in 1965) and Kraft [152].

The advent in the 1960s and 1970s of computational methods based on Gröbner bases[1] brought a decisive turn. These methods initiated the development of computational commutative algebra as a new field of research, and consequently they revived invariant theory. In fact, new algorithms and fast computers make many calculations now feasible that in the classical period

[1] It may be surprising that Gröbner bases themselves came much earlier. They appeared in an 1899 paper of Gordan [95], where he re-proved Hilbert's finiteness theorem for invariant rings.

were either simply impossible or carried a prohibitive cost. Furthermore, a heightened interest in modulo p questions led to a strong activity in modular invariant theory. An important role in boosting interest in computational invariant theory was also played by Sturmfels's book "Algorithms in Invariant Theory" [239]. Two other books (Benson [18] and Smith [225]) and numerous research articles on invariant theory have appeared recently, all evidence of a field in ferment.

Aims of this book. This book focuses on algorithmic methods in invariant theory. A central topic is the question how to find a generating set for the invariant ring. We deal with this question in the case of finite groups and linearly reductive groups. In the case of finite groups, we emphasize the modular case, in which the characteristic of the ground field divides the group order. In this case, many interesting theoretical questions in invariant theory of finite groups are still open, and new phenomena tend to occur. The scope of this book is not limited to the discussion of algorithms. A recurrent theme in invariant theory is the investigation of structural properties of invariant rings and their links with properties of the corresponding linear groups. In this book, we consider primarily the properties of invariant rings that are susceptible to algorithmic computation (such as the depth) or are of high relevance to the behavior and feasibility of algorithms (such as degree bounds). We often consider the geometric "incarnation" of invariants and examine, for example, the question of separating orbits by invariants. In addition, this book has a chapter on applications of invariant theory to several mathematical and non-mathematical fields. Although we are non-experts in most of the fields of application, we feel that it is important and hope it is worthwhile to include as much as we can from the applications side, since invariant theory, as much as it is a discipline of its own, has always been driven by what it was used for. Moreover, it is specifically the computational aspect of invariant theory that lends itself to applications particularly well.

Other books. Several books on invariant theory have appeared in the past twenty-five years, such as Springer [231], Kraft [152], Kraft et al. [153], Popov [193], Sturmfels [239], Benson [18], Popov and Vinberg [194], Smith [225], and Goodman and Wallach [93]. A new book by Neusel and Smith [181] has just arrived straight off the press. We hope that our book will serve as a useful addition to its predecessors. Our choice of material differs in several ways from that for previous books. In particular, of the books mentioned, Sturmfels's is the only one that strongly emphasizes algorithms and computation. Several points distinguish our book from Sturmfels [239]. First of all, this book is appearing nine years later, enabling us to include many new developments such as the first author's algorithm for computing invariant rings of linearly reductive groups and new results on degree bounds. Moreover, the modular case of invariant theory receives a fair amount of our attention in this book. Of the other books mentioned, only Benson [18], Smith [225], and

Neusel and Smith [181] have given this case a systematic treatment. On the other hand, Sturmfels's book [239] covers many aspects of Classical Invariant Theory and brings them together with modern algorithms. In contrast, our book touches only occasionally on Classical Invariant Theory. It is probably fair to say that most of the material covered in Chapters 3 and 4 (the core chapters of this book) has never appeared in a book before.

Readership. The intended readership of this book includes postgraduate students as well as researchers in geometry, computer algebra, and, of course, invariant theory. The methods used in this book come from different areas of algebra, such as algebraic geometry, (computational) commutative algebra, group and representation theory, Lie theory, and homological algebra. This diversity entails some unevenness in the knowledge that we assume on the readers' part. We have nevertheless tried to smooth out the bumps, so a good general knowledge of algebra should suffice to understand almost all of the text. The book contains many examples and explicit calculations that we hope are instructive. Generally, we aim to maximize the benefits of this book to readers. We hope that it, or at least parts of it, can also be used as a basis for seminars.

Proofs. When writing this book, we had to decide which proofs of particular statements to include or omit. Our primary consideration was whether a proof is, in our view, instructive. Of course, other factors also had some weight, such as the length of a proof, its novelty, its availability elsewhere in the literature, the importance of the result, and its relevance to computational matters. Some degree of arbitrariness is probably unavoidable in such decisions, but we do hope that our choices contribute to the readability of the book. When proofs are omitted, we give references.

Organization of the book. Most of the algorithms presented in this book rely in one way or another on Gröbner basis methods. Therefore we decided to devote the first chapter of this book to introducing Gröbner bases and methods in constructive ideal theory that are built on them. Since most of the material is also covered in several other books (see the references at the beginning of Chapter 1), we considered it justifiable and appropriate to give a concise presentation almost completely "unburdened" by proofs. The aim is to give the reader a quick overview of the relevant techniques. We cover most of the standard applications of Gröbner bases to ideal theory, such as the computation of elimination ideals, intersections, ideal quotients, dimension, syzygy modules and resolutions, radical ideals, and Hilbert series. In the section on radical calculation, we present a new algorithm that works in positive characteristic. Our treatment in Section 1.6 of de Jong's normalization algorithm goes beyond the material found in the standard texts. We believe that this algorithm has not previously appeared in a monograph. For this reason, we have decided to give full proofs in Section 1.6.

The second chapter gives a general introduction into invariant theory. The goal is to acquaint the reader with the basic objects and problems and, perhaps most important, to specify the notation. The presentation is enriched with many examples. In this chapter we aim to set the stage for later developments. In particular, Sections 2.4 through 2.6 are written with applications to Chapters 3 and 4 in mind. In Section 2.5.2, we present a proof of the Hochster-Roberts Theorem that is based on the concept of tight closure. Section 2.3.2 is devoted to separating invariants, a subject rarely or never mentioned in books on invariant theory. Here we go back to one of the original purposes for which invariant theory was invented and ask whether a subset of the invariant ring might have the same properties of separating group orbits as the full invariant ring, even if the subset may not generate the invariant ring. As it turns out, it is always possible to find a finite set with this property, even though the invariant ring itself may not be finitely generated (see Theorem 2.3.15). This result seems to be new.

Chapters 3 and 4 form the core of the book. In Chapter 3 we look at invariants of finite groups. Here the modular case, in which the characteristic of the ground field divides the group order, is included and indeed emphasized. The main goal of the chapter is to present algorithms for finding a finite set of generators of the invariant ring. As the reader will discover, these algorithms are much more cumbersome in the modular case. The importance of having algorithms for this case lies mainly in the fact that modular invariant theory is a field with many interesting problems that remain unsolved. Therefore it is crucial to be able explore the terrain by using computation. The main algorithms for computing generators and determining properties of invariant rings are presented in Sections 3.1 through 3.7. Many of the algorithms were developed by the second author. In Sections 3.10 and 3.11, we discuss methods applicable to special situations and ad hoc methods. A number of not strictly computational issues are addressed in Chapter 3, notably degree bounds. We present a recent proof found by Benson, Fleischmann, and Fogarty for the Noether bound that extends to the case of positive characteristic not dividing the group order, which was left open by Noether's original argument. In Section 3.9.3 we give a (very large) general degree bound for the modular case that depends only on the group order and the dimension of the representation. Such a bound has not appeared in the literature before. In Section 3.9.4 we revisit the topic of separating subalgebras and show that the Noether bound always holds for separating invariants even when it fails for generating invariants.

The fourth chapter is devoted to invariants of linearly reductive groups. We present a general algorithm for computing a finite set of generating invariants, which was found by the first author. This algorithm makes use of the Reynolds operator, which is studied systematically in Section 4.5. In Section 4.6 we discuss how the Hilbert series of the invariant ring can be calculated by using an integral similar to Molien's formula. As for finite groups,

degree bounds are also an important issue in the case of reductive groups. In Section 4.7 we discuss an improvement of a degree bound given by Popov. An important special case of reductive groups are tori. In Section 4.3 we present a new algorithm for computing generating invariants of tori.

In Chapter 5 we embark on a tour of several applications of invariant theory. We start with applications to different areas in algebra. Here we discuss the computation of cohomology rings of finite groups, solving systems of algebraic equations with symmetries, the determination of Galois groups, and the construction of generic polynomials via a positive solution of Noether's problem. Then we move on to other mathematical disciplines. We address applications to graph theory, combinatorics, coding theory, and dynamical systems. Finally, we look at examples from computer vision and material science in which invariant theory can be a useful tool. This chapter is incomplete in (at least) three ways. First, the scope of fields where invariant theory is applied is much bigger than the selection that we present here. We aim to present applications that we consider to be typical and that represent a certain bandwidth. Second, we are non-experts in most of the fields addressed in this chapter. Therefore certain inaccuracies are unavoidable in our presentation, and many experts will probably find that we missed their favorite article on the subject. We apologize in advance and ask readers to bring such shortcomings to our attention. Third, we very intentionally limit ourselves to giving a short presentation of a few selected topics and examples for each field of application. We want to convey to the reader more a taste of the subject matter than a comprehensive treatment. So Chapter 5 is meant to operate a bit like a space probe originating from our home planet (algebra) and traveling outward through the solar system, visiting some planets and skipping others, and taking snapshots along the way.

Finally, the book has an appendix where we have compiled some standard facts about algebraic groups. The material of the appendix is not a prerequisite for every part of the book. In fact, the appendix is needed primarily for the second half of Chapter 4.

1 Constructive Ideal Theory

In this chapter we will provide the basic algorithmic tools which will be used in later chapters. More precisely, we introduce some algorithms of constructive ideal theory, almost all of which are based on Gröbner bases. As the reader will find out, these algorithms and thus Gröbner bases literally permeate this book. When Sturmfels' book [239] was published, not much introductory literature on Gröbner bases and their applications was available. In contrast, we now have the books by Becker and Weispfenning [15], Adams and Loustaunau [6], Cox et al. [48], Vasconcelos [250], Cox et al. [49], Kreuzer and Robbiano [155], and a chapter from Eisenbud [59]. This list of references could be continued further. We will draw heavily on these sources and restrict ourselves to giving a rather short overview of the part of the theory that we require. The algorithms introduced in Sections 1.1–1.3 of this chapter have efficient implementations in various computer algebra systems, such as CoCoA [40], MACAULAY (2) [97], MAGMA [24], or SINGULAR [99], to name just a few, rather specialized ones. The normalization algorithm explained in Section 1.6 is implemented in MACAULAY and SINGULAR.

We will be looking at ideals $I \subseteq K[x_1, \ldots, x_n]$ in a polynomial ring over a field K. For polynomials $f_1, \ldots, f_k \in K[x_1, \ldots, x_n]$, the ideal generated by the f_i will be denoted by $(f_1, \ldots, f_k)K[x_1, \ldots, x_n]$ or by $(f_1, \ldots, f_k)$ if no misunderstanding can arise. The algorithms in this chapter will be mostly about questions in algebraic geometry, so let us introduce some basic notation. An **affine variety** is a subset X of the n-dimensional affine space $\mathbb{A}^n = \mathbb{A}^n(K) := K^n$ defined by a set $S \subseteq K[x_1, \ldots, x_n]$ of polynomials as

$$X = \mathcal{V}(S) := \{(\xi_1, \ldots, \xi_n) \in K^n \mid f(\xi_1, \ldots, \xi_n) = 0 \text{ for all } f \in S\}.$$

When we talk about varieties, we usually assume that K is algebraically closed. (Otherwise, we could work in the language of schemes.) The **Zariski topology** on $\mathbb{A}^n$ is defined by taking the affine varieties as closed sets. An affine variety (or any other subset of $\mathbb{A}^n$) inherits the Zariski topology from $\mathbb{A}^n$. A non-empty affine variety X is called **irreducible** if it is not the union of two non-empty, closed proper subsets. (In the literature varieties are often defined to be irreducible, but we do not make this assumption here.) The (Krull-) **dimension** of X is the maximal length k of a strictly increasing chain

$$X_0 \subsetneqq X_1 \subsetneqq \cdots \subsetneqq X_k \subseteq X$$

of irreducible closed subsets.

For an affine variety $X = \mathcal{V}(S)$, let I be the radical ideal of the ideal in $K[x_1, \ldots, x_n]$ generated by S. Then $X = \mathcal{V}(I)$, and the quotient ring $K[X] := K[x_1, \ldots, x_n]/I$ is called the **coordinate ring**. X is irreducible if and only if $K[X]$ is an integral domain, and the dimension of X equals the Krull dimension of $K[X]$, i.e., the maximal length of a strictly increasing chain of prime ideals in $K[X]$. By Hilbert's Nullstellensatz, we can identify $K[X]$ with a subset of the ring K^X of functions from X into K. Elements from $K[X]$ are called **regular functions** on X. If X and Y are affine varieties, a **morphism** $\varphi\colon X \to Y$ is a mapping from X into Y such that the image of the induced mapping

$$\varphi^*\colon K[Y] \to K^X,\ f \mapsto f \circ \varphi,$$

lies in $K[X]$.

1.1 Ideals and Gröbner Bases

In this section we introduce the basic machinery of monomial orderings and Gröbner bases.

1.1.1 Monomial Orderings

By a **monomial** in $K[x_1, \ldots, x_n]$ we understand an element of the form $x_1^{e_1} \cdots x_n^{e_n}$ with e_i non-negative integers. Let M be the set of all monomials. A **term** is an expression $c \cdot t$ with $0 \neq c \in K$ and $t \in M$. Thus every polynomial is a sum of terms.

Definition 1.1.1. *A* **monomial ordering** *is a total order ">" on M satisfying the following conditions:*

(i) $t > 1$ *for all* $t \in M \setminus \{1\}$,
(ii) $t_1 > t_2$ *implies* $st_1 > st_2$ *for all* $s, t_1, t_2 \in M$.

We also use a monomial ordering to compare terms. A non-zero polynomial $f \in K[x_1, \ldots, x_n]$ can be written uniquely as $f = ct + g$ such that $t \in M$, $c \in K \setminus \{0\}$, and every term of g is smaller (with respect to the order ">") than t. Then we write

$$\mathrm{LT}(f) = ct, \quad \mathrm{LM}(f) = t, \quad \textit{and} \quad \mathrm{LC}(f) = c$$

for the **leading term**, **leading monomial**, *and* **leading coefficient** *of f. For $f = 0$, all three values are defined to be zero.*