

Encyclopaedia of Mathematical Sciences 130

Invariant Theory and Algebraic Transformation Groups VIII

Revaz V. Gamkrelidze · Vladimir I. Popov *Subseries Editors*

Harm Derksen
Gregor Kemper

Computational Invariant Theory

Second Edition



Springer

Encyclopaedia of Mathematical Sciences

Encyclopaedia of Mathematical Sciences

Volume 130

Invariant Theory and Algebraic Transformation Groups VIII

Subseries Editors:

Revaz V. Gamkrelidze Vladimir I. Popov

More information about this series at <http://www.springer.com/series/855>

Harm Derksen • Gregor Kemper

Computational Invariant Theory

Second Enlarged Edition with two Appendices by
Vladimir L. Popov, and an Addendum by
Norbert A. Campo and Vladimir L. Popov



Springer

Harm Derksen
Department of Mathematics
University of Michigan
Ann Arbor, MI
USA

Gregor Kemper
Zentrum Mathematik - M11
Technische Universität München
Garching, Germany

ISSN 0938-0396
Encyclopaedia of Mathematical Sciences
ISBN 978-3-662-48420-3 ISBN 978-3-662-48422-7 (eBook)
DOI 10.1007/978-3-662-48422-7

Library of Congress Control Number: 2015955260

Mathematics Subject Classification (2010): 13H10, 13P10

Springer Heidelberg New York Dordrecht London
© Springer-Verlag Berlin Heidelberg 2002, 2015

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer-Verlag GmbH Berlin Heidelberg is part of Springer Science+Business Media
(www.springer.com)

To Maureen, William, Claire

To Elisabeth, Martin, Stefan

Preface to the Second Edition

It is more than 10 years ago that the first edition of this book has appeared. Since then, the field of computational invariant theory has been enjoying a lot of attention and activity, resulting in some important and, to us, exciting developments. This is why we think that it is time for a second enlarged and revised edition. Apart from correcting some mistakes and reorganizing the presentation here and there, we have added the following material: further results about separating invariants and their computation (Sects. 2.4 and 4.9.1), Symonds' degree bound (Sect. 3.3.2), Hughes' and Kemper's extension of Molien's formula (Sect. 3.4.2), King's algorithm for computing fundamental invariants (Sect. 3.8.2), Broer's criterion for the quasi-Gorenstein property (Sect. 3.9.11), Dufresne's generalization of Serre's result on polynomial invariant rings and her result with Jeffries (Sect. 3.12.2), Kamke's algorithm for computing invariants of finite groups acting on algebras (Sect. 3.13), Kemper's and Derksen's algorithm for computing invariants of reductive groups in positive characteristic (Sect. 3.13), algorithms by Müller-Quade and Beth, Hubert and Kogan, and Kamke and Kemper for computing invariant fields and localizations of invariant rings (Sect. 4.10.1), and work by van den Essen, Freudenburg, Greuel and Pfister, Kemper, Sancho de Salas, and Tanimoto on invariants of the additive group and of connected solvable groups (Sect. 4.10.5).

Last but not least, this edition contains two new appendices, written by Vladimir Popov, on algorithms for deciding the containment of orbit closures and on a stratification of Hilbert's nullcone. The second appendix has an addendum, authored by Norbert A'Campo and Vladimir Popov, containing the source code of a program for computing this stratification.

We would like to thank Bram Broer, Emilie Dufresne, Vladimir Popov, Jim Shank, and Peter Symonds for valuable comments on a pre-circulated version of this edition, Vladimir Popov and Norbert A'Campo for their contributions to the

book, and Ruth Allewelt at Springer-Verlag for managing the production process and for gently pushing us to finally finish our work and hand over the files.

Ann Arbor, MI, USA
Munich, Germany
July 2015

Harm Derksen
Gregor Kemper

Preface to the First Edition

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, and, of course, contents. 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, MI, USA
Heidelberg, Germany
March 2002

Harm Derksen
Gregor Kemper

Contents

1	Constructive Ideal Theory	1
1.1	Ideals and Gröbner Bases	2
1.1.1	Monomial Orderings	2
1.1.2	Gröbner Bases	4
1.1.3	Normal Forms	5
1.1.4	The Buchberger Algorithm	6
1.2	Elimination Ideals	8
1.2.1	Image Closure of Morphisms	9
1.2.2	Relations Between Polynomials	9
1.2.3	The Intersection of Ideals	10
1.2.4	The Colon Ideal	10
1.2.5	The Krull Dimension	11
1.3	Syzygy Modules	13
1.3.1	Computing Syzygies	13
1.3.2	Free Resolutions	16
1.4	Hilbert Series	17
1.4.1	Computation of Hilbert Series	20
1.5	The Radical Ideal	22
1.5.1	Reduction to Dimension Zero	22
1.5.2	Positive Characteristic	23
1.6	Normalization	24
	References	28
2	Invariant Theory	31
2.1	Invariant Rings	31
2.2	Reductive Groups	37
2.2.1	Linearly Reductive Groups	38
2.2.2	Other Notions of Reductivity	43
2.3	Categorical Quotients	45
2.4	Separating Invariants	48

2.5	Homogeneous Systems of Parameters	54
2.5.1	Hilbert's Nullcone	54
2.5.2	Existence of Homogeneous Systems of Parameters	56
2.6	The Cohen-Macaulay Property of Invariant Rings	57
2.6.1	The Cohen-Macaulay Property	57
2.6.2	The Hochster-Roberts Theorem	59
2.7	Hilbert Series of Invariant Rings	65
	References	67
3	Invariant Theory of Finite Groups	71
3.1	Homogeneous Components	72
3.1.1	The Linear Algebra Method	73
3.1.2	The Reynolds Operator	73
3.2	Noether's Degree Bound	74
3.3	Degree Bounds in the Modular Case	78
3.3.1	Richman's Lower Degree Bound	79
3.3.2	Symonds' Degree Bound	82
3.4	Molien's Formula	83
3.4.1	Characters and Molien's Formula	84
3.4.2	Extensions to the Modular Case	86
3.4.3	Extended Hilbert Series	89
3.5	Primary Invariants	91
3.5.1	Dade's Algorithm	92
3.5.2	An Algorithm for Optimal Homogeneous Systems Parameters	93
3.5.3	Constraints on the Degrees of Primary Invariants	94
3.6	Cohen-Macaulayness	97
3.7	Secondary Invariants	100
3.7.1	The Nonmodular Case	101
3.7.2	The Modular Case	104
3.8	Minimal Algebra Generators and Syzygies	106
3.8.1	Algebra Generators from Primary and Secondary Invariants	106
3.8.2	Direct Computation of Algebra Generators: King's Algorithm	107
3.8.3	Computing Syzygies	109
3.9	Properties of Invariant Rings	111
3.9.1	The Cohen-Macaulay Property	111
3.9.2	Free Resolutions and Depth	112
3.9.3	The Hilbert Series	115
3.9.4	Polynomial Invariant Rings and Reflection Groups	115
3.9.5	The Gorenstein Property	120

3.10	Permutation Groups	123
3.10.1	Direct Products of Symmetric Groups	123
3.10.2	Göbel's Algorithm	125
3.10.3	SAGBI Bases	130
3.11	Ad Hoc Methods	131
3.11.1	Finding Primary Invariants	132
3.11.2	Finding Secondary Invariants	134
3.11.3	The Other Exceptional Reflection Groups	138
3.12	Separating Invariants	139
3.12.1	Degree Bounds	139
3.12.2	Polynomial Separating Subalgebras and Reflection Groups	140
3.13	Actions on Finitely Generated Algebras	142
	References	147
4	Invariant Theory of Infinite Groups	153
4.1	Computing Invariants of Linearly Reductive Groups	153
4.1.1	The Heart of the Algorithm	153
4.1.2	The Input: The Group and the Representation	156
4.1.3	The Algorithm	159
4.2	Improvements and Generalizations	164
4.2.1	Localization of the Invariant Ring	165
4.2.2	Generalization to Arbitrary Graded Rings	169
4.2.3	Covariants	172
4.3	Invariants of Tori	174
4.4	Invariants of SL_n and GL_n	178
4.4.1	Binary Forms	180
4.5	The Reynolds Operator	182
4.5.1	The Dual Space $K[G]^*$	184
4.5.2	The Reynolds Operator for Semi-simple Groups	186
4.5.3	Cayley's Omega Process	193
4.6	Computing Hilbert Series	198
4.6.1	A Generalization of Molien's Formula	198
4.6.2	Hilbert Series of Invariant Rings of Tori	202
4.6.3	Hilbert Series of Invariant Rings of Connected Reductive Groups	204
4.6.4	Hilbert Series and the Residue Theorem	206
4.7	Degree Bounds for Invariants	216
4.7.1	Degree Bounds for Orbits	219
4.7.2	Degree Bounds for Tori	224
4.8	Properties of Invariant Rings	226
4.9	Computing Invariants of Reductive Groups	227
4.9.1	Computing Separating Invariants	228
4.9.2	Computing the Purely Inseparable Closure	232
4.9.3	Actions on Varieties	236

4.10 Invariant Fields and Localizations of Invariant Rings	240
4.10.1 Extendend Derksen Ideals and CAGEs	241
4.10.2 The Italian Problem	245
4.10.3 Geometric Aspects of Extended Derksen Ideals	246
4.10.4 Computational Aspects of Extended Derksen Ideals	248
4.10.5 The Additive Group	254
4.10.6 Invariant Rings and Quasi-affine Varieties	258
References	261
5 Applications of Invariant Theory	265
5.1 Cohomology of Finite Groups	265
5.2 Galois Group Computation	266
5.2.1 Approximating Zeros	269
5.2.2 The Symbolic Approach	270
5.3 Noether's Problem and Generic Polynomials	272
5.4 Systems of Algebraic Equations with Symmetries	275
5.5 Graph Theory	276
5.6 Combinatorics	278
5.7 Coding Theory	281
5.8 Equivariant Dynamical Systems	283
5.9 Material Science	285
5.10 Computer Vision	288
5.10.1 View Invariants of 3D Objects	288
5.10.2 Invariants of n Points on a Plane	289
5.10.3 Moment Invariants	291
References	293
A Linear Algebraic Groups	297
A.1 Linear Algebraic Groups	297
A.2 The Lie Algebra of a Linear Algebraic Group	299
A.3 Reductive and Semi-simple Groups	303
A.4 Roots	304
A.5 Representation Theory	306
References	307
B Is One of the Two Orbits in the Closure of the Other?	309
B.1 Introduction	309
B.2 Examples	310
B.3 Algorithm	312
B.4 Defining the Set $\overline{G \cdot L}$ by Equations	317
References	321
C Stratification of the Nullcone	323
C.1 Introduction	323
C.2 The Stratification	325

Contents	xv
C.3 The Algorithm	330
C.4 Examples	336
References	343
Addendum to Appendix C: The Source Code of HNC	345
References	358
Notation	359
Index	361

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 it was invented. (Kung and Rota [1])

A brief history Invariant theory is a mathematical discipline with a long tradition, going back at least one hundred and fifty years. Sometimes it 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 [2], he showed that invariant rings of the classical groups are finitely generated. His nonconstructive proof was harshly criticized by Gordan (see p. 42 in this book). Hilbert replied in the second paper [3] 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 [2, 3] 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. [4] (whose first edition was published in 1965) and Kraft [5].

The advent in the 1960s and 1970s of computational methods based on Gröbner bases¹ brought a decisive turn. These methods initiated the development of

¹It may be surprising that Gröbner bases themselves came much earlier. They appeared in an 1899 paper of Gordan [6], where he re-proved Hilbert’s finiteness theorem for invariant rings.

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 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 [7]. Various other monographs (such as Benson [8], Smith [9], Neusel and Smith [10], Dolgachev [11], Lorenz [12], Neusel [13], and Campbell and Wehlau [14]) and numerous research articles on invariant theory have appeared quite 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 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 nonmathematical fields. Although we are nonexperts 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 The list of monographs on invariant theory is quite long and includes the books of Dieudonné and Carrell [15], Springer [16], Kraft and Procesi [17], Kraft [5], Popov [18], Sturmfels [7], Benson [8], Popov and Vinberg [19], Dolgachev [20], Smith [9], Goodman and Wallach [21], Olver [22], Neusel and Smith [10], Dolgachev [11], Lorenz [12], Neusel [13], and Campbell and Wehlau [14]. We hope that our book will serve as a useful addition to these. Our choice of material differs in several ways from that of previous books. In particular, of the books mentioned, Sturmfels' [7] is the only one that strongly emphasizes algorithms and computation. Several points distinguish our book from [7]. First of all, the first edition of this book appeared 9 years later than [7], enabling it to include many new developments such as the first author's algorithm for computing invariant rings of linearly reductive groups, new results on degree bounds, and the concept of separating invariants. Moreover, the modular case of invariant theory receives a fair

amount of our attention in this book. On the other hand, [7] 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. In its emphasis on modular invariant theory, our book has something in common with Benson [8], Smith [9], Neusel and Smith [10], and Campbell and Wehlau [14]. It is probably fair to say that most of the material covered in Chaps. 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 to an introduction of Gröbner bases and methods in computational commutative algebra that are built on them. Since most of the material is also covered in several other books (see the references at the beginning of Chap. 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. Our treatment in Sect. 1.6 of de Jong's normalization algorithm goes beyond the material found in the standard texts. For this reason, we have decided to give full proofs in Sect. 1.6.

The second chapter gives a general introduction to 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, Sects. 2.4 through 2.7 are written with applications to Chaps. 3 and 4 in mind. In Sect. 2.6.2, we present a proof of the Hochster-Roberts theorem that is based on the concept of tight closure. Section 2.4 is devoted to separating invariants, a subject that attracted a lot of activity recently. 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 2.4.8).

Chapters 3 and 4 form the core of the book. In Chap. 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 useful to be able explore the terrain by computation. The main algorithms for computing generators and determining properties of invariant rings are presented in Sects. 3.1 through 3.9. Many of the algorithms were developed by the second author. In Sects. 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 Chap. 3, notably degree bounds. We present a 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 Sect. 3.3.2, we present a new degree bound, proved by Symonds, which holds in all characteristics and only depends on the group order and the dimension of the representation. Such a bound has not appeared in the literature before. In Sect. 3.12, 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. Section 3.13 deals with the computation of the invariant ring of a finite group acting on a finitely generated algebra which need not be a polynomial ring over a field.

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 Sect. 4.5. In Sect. 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 Sect. 4.7, we discuss an improvement of a degree bound given by Popov. An important special case of reductive groups is tori. In Sect. 4.3, we present a new algorithm for computing generating invariants of tori. Section 4.9 deals with computing invariant rings of reductive groups that need not be linearly reductive. Since invariant rings of such groups are guaranteed to be finitely generated by a celebrated result of Nagata, this constitutes (up to

the question of actions on nonreduced algebras) the final step in making Nagata's result constructive. In Sect. 4.10, we go beyond reductive groups and discuss recent techniques for computing invariant fields and localizations of invariant rings, from which the invariant ring itself can be extracted if it happens to be finitely generated.

In Chap. 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 materials 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 nonexperts 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 Chap. 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 but 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, it is required primarily for Sects. 4.5 through 4.8.

References

1. Joseph P. S. Kung, Gian-Carlo Rota, *The invariant theory of binary forms*, Bull. Am. Math. Soc., New Ser. **10** (1984), 27–85.
2. David Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. **36** (1890), 473–534.
3. David Hilbert, *Über die vollen Invariantensysteme*, Math. Ann. **42** (1893), 313–370.
4. David Mumford, John Fogarty, Frances Kirwan, *Geometric Invariant Theory*, Ergebnisse der Math. und ihrer Grenzgebiete **34**, third edn., Springer-Verlag, Berlin, Heidelberg, New York 1994.
5. Hanspeter Kraft, *Geometrische Methoden in der Invariantentheorie*, Aspects of Mathematics **D1**, Vieweg, Braunschweig/Wiesbaden 1985.
6. Paul Gordan, *Neuer Beweis des Hilbertschen Satzes über homogene Funktionen*, Nachrichten König. Ges. der Wiss. zu Gött. (1899), 240–242.
7. Bernd Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, Wien, New York 1993.
8. David J. Benson, *Polynomial Invariants of Finite Groups*, Lond. Math. Soc. Lecture Note Ser. **190**, Cambridge Univ. Press, Cambridge 1993.

9. Larry Smith, *Polynomial Invariants of Finite Groups*, A. K. Peters, Wellesley, Mass. 1995.
10. Mara D. Neusel, Larry Smith, *Invariant Theory of Finite Groups*, Mathematical Surveys and Monographs **94**, American Mathematical Society, Providence, RI 2002.
11. Igor Dolgachev, *Lectures on Invariant Theory*, London Mathematical Society Lecture Note Series **296**, Cambridge University Press, Cambridge 2003.
12. Martin Lorenz, *Multiplicative Invariant Theory*, Encyclopaedia of Mathematical Sciences **135**, Springer-Verlag, Berlin 2005.
13. Mara D. Neusel, *Invariant Theory*, Student Mathematical Library **36**, American Mathematical Society, Providence, RI 2007.
14. H. E. A. Eddy Campbell, David L. Wehlau, *Modular Invariant Theory*, Encyclopaedia of Mathematical Sciences **139**, Springer-Verlag, Berlin 2011.
15. Jean A. Dieudonné, James B. Carrell, *Invariant Theory, Old and New*, Academic Press, New York 1971.
16. Tonny A. Springer, *Invariant Theory*, Lecture Notes in Math. **585**, Springer-Verlag, Berlin, Heidelberg, New York 1977.
17. Hanspeter Kraft, Claudio Procesi, *A primer of invariant theory*, Notes by G. Boffi, Brandeis Lecture Notes 1. Updated version (2000) available at <http://www.math.unibas.ch/~kraft/Papers/KP-Primer.pdf>, 1982.
18. Vladimir L. Popov, *Groups, Generators, Syzygies and Orbits in Invariant Theory*, Translations of Mathematical Monographs **100**, American Mathematical Society, Providence, RI 1992.
19. Vladimir L. Popov, Ernest B. Vinberg, *Invariant theory*, in: N. N. Parshin, I. R. Shafarevich, eds., *Algebraic Geometry IV*, Encyclopaedia of Mathematical Sciences **55**, Springer-Verlag, Berlin, Heidelberg 1994.
20. Igor V. Dolgachev, *Introduction to Geometric Invariant Theory*, Lecture Notes Series **25**, Seoul National University Research Institute of Mathematics Global Analysis Research Center, Seoul 1994.
21. Roe Goodman, Nolan R. Wallach, *Representations and Invariants of the Classical Groups*, Encyclopedia of Mathematics and its Applications **68**, Cambridge University Press, Cambridge 1998.
22. Peter J. Olver, *Classical Invariant Theory*, London Mathematical Society Student Texts **44**, Cambridge University Press, Cambridge 1999.

Chapter 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 (or, almost synonymously, of computational commutative algebra), 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 [1] 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 [2], Adams and Loustaunau [3], Cox et al. [4], Vasconcelos [5], Cox et al. [23], Kreuzer and Robbiano [6, 7], Greuel and Pfister [8], Ene and Herzog [9], and chapters from Eisenbud [10] and Kemper [11]. This list of references could be continued further, particularly by adding books dealing with variants or special purposes of Gröbner bases. 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 Sects. 1.1, 1.2 and 1.3 of this chapter have efficient implementations in various computer algebra systems, such as CoCoA [12], MACAULAY2 [13], MAGMA [14], or SINGULAR [15], to name just a few, rather specialized ones. The normalization algorithm explained in Sect. 1.6 is implemented in MACAULAY2 and SINGULAR.

We will be looking at ideals $I \subseteq K[x_1, \dots, x_n]$ in a polynomial ring over a field K . For polynomials $f_1, \dots, f_k \in K[x_1, \dots, x_n]$, the ideal generated by the f_i will be denoted by $(f_1, \dots, f_k)K[x_1, \dots, x_n]$ or by (f_1, \dots, 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 $S \subseteq K[x_1, \dots, x_n]$ of polynomials as

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

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 nonempty affine variety X is called **irreducible** if it is not the union of two nonempty, 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

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

of irreducible closed subsets.

For an affine variety $X = \mathcal{V}(S)$, let I be the radical ideal of the ideal in $K[x_1, \dots, x_n]$ generated by S . Then $X = \mathcal{V}(I)$, and the quotient ring $K[X] := K[x_1, \dots, x_n]/I$ 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** $\varphi: X \rightarrow Y$ is a mapping from X into Y such that the image of the induced mapping

$$\varphi^*: K[Y] \rightarrow K^X, f \mapsto f \circ \varphi,$$

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 $K[x_1, \dots, x_n]$ we understand an element of the form $x_1^{e_1} \cdots x_n^{e_n}$ with e_i nonnegative 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 nonzero polynomial $f \in K[x_1, \dots, x_n]$ 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

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

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

A monomial ordering is always a well-ordering. This follows from the fact that ideals in $K[x_1, \dots, x_n]$ are finitely generated. We note that the usage of terminology is not uniform in the literature. Some authors (e.g. Becker and Weispfenning [2]) have monomials and terms interchanged, and some speak of initial or head terms, monomials and coefficients. Monomial orderings are often called term orders. When browsing through the literature one can find almost any combination of these pieces of terminology.

Example 1.1.2 We give a few examples of monomial orderings. Let $t = x_1^{e_1} \cdots x_n^{e_n}$ and $t' = x_1^{e'_1} \cdots x_n^{e'_n}$ be two distinct monomials.

- (a) The lexicographic monomial ordering (with $x_1 > x_2 > \cdots > x_n$): t is considered greater than t' if $e_i > e'_i$ for the smallest i with $e_i \neq e'_i$. We sometimes write $t >_{\text{lex}} t'$ in this case. As an example, we have

$$\text{LM}_{\text{lex}}(x_1 + x_2x_4 + x_3^2) = x_1.$$

The lexicographic monomial ordering is useful for solving systems of algebraic equations.

- (b) The graded lexicographic monomial ordering: $t >_{\text{plex}} t'$ if $\deg(t) > \deg(t')$, or if $\deg(t) = \deg(t')$ and $t >_{\text{lex}} t'$. Here $\deg(t)$ is the total degree $e_1 + \cdots + e_n$. For example,

$$\text{LM}_{\text{plex}}(x_1 + x_2x_4 + x_3^2) = x_2x_4.$$

The graded lexicographic monomial ordering can be generalized by using a weighted degree $\deg(t) := w_1e_1 + \cdots + w_ne_n$ with w_i fixed positive real numbers.

- (c) The graded reverse lexicographic monomial ordering (grevlex-ordering for short): $t >_{\text{grevlex}} t'$ if $\deg(t) > \deg(t')$, or if $\deg(t) = \deg(t')$ and $e_i < e'_i$ for the largest i with $e_i \neq e'_i$. For example,

$$\text{LM}_{\text{grevlex}}(x_1 + x_2x_4 + x_3^2) = x_3^2.$$

The grevlex ordering is often very efficient for computations. It can also be generalized by using a weighted degree.

- (d) Block orderings: Let $>_1$ be a monomial ordering on the monomials in x_1, \dots, x_r , and $>_2$ a monomial ordering on the monomials in x_{r+1}, \dots, x_n . Then the block ordering formed from $>_1$ and $>_2$ is defined as follows: $t > t'$ if $x_1^{e_1} \cdots x_r^{e_r} >_1 x_1^{e'_1} \cdots x_r^{e'_r}$, or if $x_1^{e_1} \cdots x_r^{e_r} = x_1^{e'_1} \cdots x_r^{e'_r}$ and $x_{r+1}^{e_{r+1}} \cdots x_n^{e_n} >_2 x_{r+1}^{e'_{r+1}} \cdots x_n^{e'_n}$. For example, the lexicographic monomial ordering is a block ordering. Block orderings are useful for the computation of elimination ideals (see Sect. 1.2). \triangleleft

We say that a monomial ordering is **graded** if $\deg(t) > \deg(t')$ implies $t > t'$. So the orderings in (b) and (c) of the previous example are graded.

Given a monomial ordering, we write $x_i \gg x_j$ if $x_i > x_j^e$ for all nonnegative integers e . For example, in the lexicographic monomial ordering we have $x_1 \gg x_2 \gg \cdots \gg x_n$. Moreover, if “ $>$ ” is a block ordering with blocks x_1, \dots, x_r and x_{r+1}, \dots, x_n , then $x_i \gg x_j$ for $i \leq r$ and $j > r$. If $x_i \gg x_j$ for all $j \in J$ for some $J \subset \{1, \dots, n\}$, then x_i is greater than any monomial in the indeterminates $x_j, j \in J$. This follows directly from Definition 1.1.1.

1.1.2 Gröbner Bases

We fix a monomial ordering on $K[x_1, \dots, x_n]$.

Definition 1.1.3 Let $S \subseteq K[x_1, \dots, x_n]$ be a set of polynomials. We write

$$L(S) = (\text{LM}(g) \mid g \in S)$$

for the ideal generated by the leading monomials from S . $L(S)$ is called the **leading ideal** of S (by some authors also called the initial ideal).

Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal. Then a finite subset $\mathcal{G} \subseteq I$ is called a **Gröbner basis** of I (with respect to the chosen monomial ordering) if

$$L(I) = L(\mathcal{G}).$$

It is clear that a Gröbner basis of I generates I as an ideal. Indeed, a (hypothetical) element $f \in I \setminus (\mathcal{G})$ with minimal leading monomial could be transformed into $g \in I \setminus (\mathcal{G})$ with smaller leading monomial by subtracting a multiple of an element from \mathcal{G} , which yields a contradiction. It is also clear that Gröbner bases always exist. Indeed, $\{\text{LM}(f) \mid f \in I\}$ generates $L(I)$ by definition, hence by the Noether property a finite subset $\{\text{LM}(f_1), \dots, \text{LM}(f_m)\}$ also generates $L(I)$, and so $\{f_1, \dots, f_m\}$ is a Gröbner basis. This argument, however, is nonconstructive. But we will see in Sect. 1.1.4 that there is in fact an algorithm for computing Gröbner bases.

The most obvious question about an ideal $I \subseteq K[x_1, \dots, x_n]$ that can be decided with Gröbner bases is whether $I = K[x_1, \dots, x_n]$. Indeed, this is the case if and only if \mathcal{G} contains a (nonzero) constant polynomial.

1.1.3 Normal Forms

A central element in the construction and usage of Gröbner bases is the computation of so-called normal forms.

Definition 1.1.4 Let $S = \{g_1, \dots, g_s\} \subseteq K[x_1, \dots, x_n]$ be a finite set of polynomials.

- (a) A polynomial $f \in K[x_1, \dots, x_n]$ is said to be in **normal form** with respect to S if no term of f is divisible by the leading monomial of any $g \in S$.
- (b) If f and \tilde{f} are polynomials in $K[x_1, \dots, x_n]$, then \tilde{f} is said to be a **normal form** of f with respect to S if the following conditions hold:
 - (1) \tilde{f} is in normal form with respect to S .
 - (2) There exist $h_1, \dots, h_s \in K[x_1, \dots, x_n]$ with

$$f - \tilde{f} = \sum_{i=1}^s h_i g_i \quad \text{and} \quad \text{LM}(h_i g_i) \leq \text{LM}(f) \quad \text{for all } i \quad (1.1.1)$$

(in particular, $f - \tilde{f}$ lies in the ideal generated by S);

Example 1.1.5 Let $S = \{x_1, x_1 + 1\}$. Then 1 is congruent to 0 modulo (S), but 0 is not a normal form of 1. Moreover, $f = x_1$ has two normal forms: 0 and -1 . So in general, normal forms are not uniquely determined.

Notice that S is not a Gröbner basis. \triangleleft

The following algorithm, which mimics division with remainder in the univariate case, calculates a normal form with respect to a finite set S of polynomials.

Algorithm 1.1.6 (Normal form) Given a polynomial $f \in K[x_1, \dots, x_n]$ and a finite subset $S = \{g_1, \dots, g_s\} \subset K[x_1, \dots, x_n]$, perform the following steps to obtain a normal form \tilde{f} of f with respect to S , together with polynomials $h_1, \dots, h_s \in K[x_1, \dots, x_n]$ satisfying (1.1.1).

- (1) Set $\tilde{f} := f$ and $h_i := 0$ for all i , and repeat the steps (2)–(4).
- (2) If no term of \tilde{f} is divisible by the leading monomial of any $g_i \in S$, return \tilde{f} as a normal form of f , and return the h_i .
- (3) Let ct be the maximal term of \tilde{f} such that there exists $g_i \in S$ with $\text{LM}(g_i)$ dividing t .

(4) Set

$$\tilde{f} := \tilde{f} - \frac{ct}{\text{LT}(g_i)} g_i \quad \text{and} \quad h_i := h_i + \frac{ct}{\text{LT}(g_i)}.$$

Of course the computation of the h_i can be omitted if only a normal form is desired. The termination of Algorithm 1.1.6 is guaranteed by the fact that the maximal monomials t of \tilde{f} divisible by some $\text{LM}(g_i)$ form a strictly decreasing sequence, but such a sequence is finite by the well-ordering property. The result of Algorithm 1.1.6 is in general not unique, since it depends on the choice of the g_i in step (3). However, if \mathcal{G} is a Gröbner basis of an ideal I , then normal forms with respect to \mathcal{G} are unique. In fact, if \tilde{f} and \hat{f} are two normal forms of f with respect to \mathcal{G} , then $\tilde{f} - \hat{f} \in I$, so $\text{LM}(\tilde{f} - \hat{f})$ is divisible by some $\text{LM}(g)$ with $g \in \mathcal{G}$. But if $\tilde{f} \neq \hat{f}$, then $\text{LM}(\tilde{f} - \hat{f})$ must appear as a monomial in \tilde{f} or \hat{f} , contradicting the fact that \tilde{f} and \hat{f} are in normal form. In the case of a Gröbner basis \mathcal{G} we write $\tilde{f} =: \text{NF}_\mathcal{G}(f) = \text{NF}_\mathcal{G}(f)$ for the normal form. An important property of the map $\text{NF}_\mathcal{G} : K[x_1, \dots, x_n] \rightarrow K[x_1, \dots, x_n]$ is that it is linear.

It should be mentioned that there is a variant of the normal form algorithm which stops when the leading term of \tilde{f} is zero or not divisible by any $\text{LM}(g)$, $g \in S$ (“top-reduction”).

Using Algorithm 1.1.6, we obtain a membership test for ideals.

Algorithm 1.1.7 (Membership test in ideals) Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal, \mathcal{G} a Gröbner basis of I , and $f \in K[x_1, \dots, x_n]$ a polynomial. Then

$$f \in I \iff \text{NF}_\mathcal{G}(f) = 0.$$

One can also substitute $\text{NF}_\mathcal{G}(f)$ by the result of top-reducing f .

It is easy to see that the map $\text{NF}_\mathcal{G} : K[x_1, \dots, x_n] \rightarrow K[x_1, \dots, x_n]$ is K -linear, and by Algorithm 1.1.7, its kernel is I . So the normal form provides a way to perform explicit calculations in the quotient ring $K[x_1, \dots, x_n]/I$. In fact, this was the main objective for which Gröbner bases were invented.

A Gröbner basis \mathcal{G} of an ideal I can be transformed into a **reduced Gröbner basis** by iteratively substituting an element from \mathcal{G} by a normal form with respect to the other elements, until every element is in normal form. After deleting zero from the resulting set and making all leading coefficients equal to 1, the resulting monic reduced Gröbner basis is unique (i.e., it only depends on I and the chosen monomial ordering, see Becker and Weispfenning [2, Theorem 5.43]).

1.1.4 The Buchberger Algorithm

In order to present Buchberger’s algorithm for the construction of Gröbner bases, we need to introduce s-polynomials. Let $f, g \in K[x_1, \dots, x_n]$ be two nonzero

polynomials, and set $t := \text{lcm}(\text{LM}(f), \text{LM}(g))$ (the least common multiple). Then the **s-polynomial** of f and g is defined as

$$\text{spol}(f, g) := \frac{\text{LC}(g) \cdot t}{\text{LM}(f)} f - \frac{\text{LC}(f) \cdot t}{\text{LM}(g)} g.$$

Note that the coefficients of t cancel in $\text{spol}(f, g)$, and that $\text{spol}(f, g) \in (f, g)$. The following lemma is the key step toward finding an algorithm for the construction of a Gröbner basis.

Lemma 1.1.8 (Buchberger [16]) *Let \mathcal{G} be a basis (=generating set) of an ideal $I \subseteq K[x_1, \dots, x_n]$. Then the following statements are equivalent.*

- (a) \mathcal{G} is a Gröbner basis of I .
- (b) If $f, g \in \mathcal{G}$, then $\text{spol}(f, g)$ has 0 as a normal form with respect to \mathcal{G} .

See Becker and Weispfenning [2, Theorem 5.48] or Kemper [11, Theorem 9.12] for a proof. We can give Buchberger's algorithm in a rather coarse form now.

Algorithm 1.1.9 (Buchberger's algorithm) Given a finite basis S for an ideal $I \subseteq K[x_1, \dots, x_n]$, construct a Gröbner basis (with respect to a given monomial ordering) of I by performing the following steps:

- (1) Set $\mathcal{G} := S$ and repeat steps (2)–(4).
- (2) For $f, g \in \mathcal{G}$ compute a normal form h of $\text{spol}(f, g)$ with respect to \mathcal{G} .
- (3) If $h \neq 0$, include h into \mathcal{G} .
- (4) If h was found to be zero for all $f, g \in \mathcal{G}$, then \mathcal{G} is the desired Gröbner basis.

This algorithm terminates after a finite number of steps since $L(S)$ strictly increases with every performance of steps (2)–(4).

Remark 1.1.10 The theoretical cost of Buchberger's algorithm is extremely high. In fact, no general upper bound for the running time is known. But Möller and Mora [17] proved an upper bound for the maximal degree of the Gröbner basis elements which depends doubly exponentially on the number of variables. They also proved that this doubly exponential behavior cannot be improved. What makes things even worse is the phenomenon of “intermediate expression swell,” meaning that during the computation the number and size of polynomials can become much bigger than in the final result. It is known that the memory space required for the computation of Gröbner bases increases at most exponentially with the size of the input, and all problems with this behavior can be reduced to the problem of testing ideal membership; so the problem of computing Gröbner bases is “EXPSPACE-complete.” We refer to von zur Gathen and Gerhard [18, Section 21.7] for a more detailed account of what is known about the complexity of Gröbner bases.

In spite of all this bad news, practical experience shows that the algorithm often terminates after a reasonable time (although this is usually not predictable in advance). Much depends on improvements of the algorithm given above, such as omitting some pairs f, g (by Buchberger's first and second criterion, see Becker

and Weispfenning [2, Section 5.5]), by having a good strategy which pairs to treat first, and by choosing a suitable monomial ordering (if there is any freedom of choice). There are also algorithms which transform a Gröbner basis with respect to one monomial ordering into one with respect to another ordering (see Faugère et al. [19], Collart et al. [20]). \triangleleft

There is a variant of Buchberger's algorithm which keeps track of how the polynomials in the Gröbner basis \mathcal{G} arise as linear combinations of the polynomials in the original ideal basis S . This variant is called the extended Buchberger algorithm, and its output is an (ordered) Gröbner basis $\mathcal{G} = \{g_1, \dots, g_r\}$ and an $r \times s$ -matrix A with coefficients in $K[x_1, \dots, x_n]$ such that

$$\begin{pmatrix} g_1 \\ \vdots \\ g_r \end{pmatrix} = A \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_s \end{pmatrix},$$

where $S = \{f_1, \dots, f_s\}$. On the other hand, it is straightforward to obtain an $s \times r$ -matrix B such that $(f_1, \dots, f_s)^{\text{tr}} = B(g_1, \dots, g_r)^{\text{tr}}$ by applying the Normal Form Algorithm 1.1.6 to the f_i .

1.2 Elimination Ideals

Given an ideal $I \subseteq K[x_1, \dots, x_n]$ and an integer $k \in \{1, \dots, n\}$, the **elimination ideal** of I with respect to x_k, \dots, x_n is defined as the intersection $I \cap K[x_k, \dots, x_n]$. It has the following geometric interpretation: If

$$\pi: \mathbb{A}^n \rightarrow \mathbb{A}^{n-k+1}, (\xi_1, \dots, \xi_n) \mapsto (\xi_k, \dots, \xi_n)$$

is the canonical projection, then for K algebraically closed we have

$$\overline{\pi(\mathcal{V}(I))} = \mathcal{V}(I \cap K[x_k, \dots, x_n]), \quad (1.2.1)$$

where the left hand side is the Zariski-closure. (In scheme-theoretic language, π maps a prime ideal in $K[x_1, \dots, x_n]$ to its intersection with $K[x_k, \dots, x_n]$, and we do not need the hypothesis that K is algebraically closed.) An important feature of Gröbner bases is that they can be used to compute elimination ideals.

Algorithm 1.2.1 (Computing elimination ideals) Given an ideal $I \subseteq K[x_1, \dots, x_n]$ and an integer $k \in \{1, \dots, n\}$, compute the elimination ideal $I \cap K[x_k, \dots, x_n]$ as follows:

- (1) Choose a monomial ordering such that $x_i \gg x_j$ for $i < k$ and $j \geq k$ (e.g., the lexicographic monomial ordering or a block ordering).

- (2) Compute a Gröbner basis \mathcal{G} of I with respect to this monomial ordering.
(3) $\mathcal{G} \cap K[x_k, \dots, x_n]$ is a Gröbner basis of $I \cap K[x_1, \dots, x_n]$.

It is elementary to see that this algorithm is correct (see Becker and Weispfenning [2, Proposition 6.15]). Equation (1.2.1) shows how elimination ideals can be used to solve a system of algebraic equations with a finite set of solutions.

We continue by presenting some applications of elimination ideals (and thus of Gröbner bases) which will be needed in the following chapters of this book.

1.2.1 Image Closure of Morphisms

Let X and Y be affine varieties and $f: X \rightarrow Y$ a morphism. (Again we assume that K is algebraically closed or use the language of schemes.) We want to compute the Zariski-closure of the image $f(X)$. Assume that X is embedded into \mathbb{A}^n and Y into \mathbb{A}^m for some n and m . Without loss of generality we can assume that $Y = \mathbb{A}^m$. If f is given by polynomials (f_1, \dots, f_m) with $f_i \in K[x_1, \dots, x_n]$, and X is given by an ideal $I \subseteq K[x_1, \dots, x_n]$, then the graph of f is given by the ideal

$$J := I \cdot K[x_1, \dots, x_n, y_1, \dots, y_m] + (f_1 - y_1, \dots, f_m - y_m) \quad (1.2.2)$$

in $K[x_1, \dots, x_n, y_1, \dots, y_m]$. Thus by Eq. (1.2.1), the closure of the image is

$$\overline{f(X)} = \mathcal{V}(J \cap K[y_1, \dots, y_m])$$

(see Vasconcelos [5, Proposition 2.1.3]), and can therefore be calculated by Algorithm 1.2.1.

1.2.2 Relations Between Polynomials

A further application of elimination ideals is the computation of relations between polynomials. More precisely, let $f_1, \dots, f_m \in K[x_1, \dots, x_n]$ be polynomials. We are interested in the kernel of the homomorphism

$$\Phi: K[t_1, \dots, t_m] \rightarrow K[x_1, \dots, x_n], \quad t_i \mapsto f_i,$$

of K -algebras (where t_1, \dots, t_m are further indeterminates). The answer is as follows: Define the ideal

$$J := (f_1 - t_1, \dots, f_m - t_m)$$

in $K[x_1, \dots, x_n, t_1, \dots, t_m]$. Then it is easy to show that

$$\ker(\Phi) = J \cap K[t_1, \dots, t_m], \quad (1.2.3)$$

so the desired kernel is again an elimination ideal (see Eisenbud [10, Proposition 15.30]). More generally, taking J as in (1.2.2) and forming the elimination ideal as above yields the preimage $\Phi^{-1}(I)$. Notice that generators for $\ker(\Phi)$ together with the f_i provide a presentation of the algebra generated by the f_i .

1.2.3 The Intersection of Ideals

The intersection of two ideals $I, J \subseteq K[x_1, \dots, x_n]$ (which geometrically corresponds to the union of varieties) can be computed as follows: With a new indeterminate t , form the ideal L in $K[x_1, \dots, x_n, t]$ generated by

$$I \cdot t + J \cdot (1 - t),$$

where the products are formed by multiplying each generator of I and J by t and $1 - t$, respectively. Then

$$I \cap J = L \cap K[x_1, \dots, x_n] \quad (1.2.4)$$

(see Vasconcelos [5, Corollary 2.1.1]). A different method for computing the intersection of I and J involves the calculation of a syzygy module (see Vasconcelos [5, p. 29]). We can apply any of these methods iteratively to obtain the intersection of a finite number of ideals, but there is also a direct method (involving further auxiliary indeterminates) given by Becker and Weispfenning [2, Corollary 6.20].

1.2.4 The Colon Ideal

Given two ideals $I, J \subseteq K[x_1, \dots, x_n]$, it is often important to be able to calculate the **colon ideal**

$$I : J := \{g \in K[x_1, \dots, x_n] \mid gf \in I \ \forall f \in J\}.$$

Sometimes $I : J$ is also referred to as the quotient ideal. The colon ideal has the following geometric interpretation: If I is a radical ideal and K is algebraically closed, then $I : J$ is precisely the ideal of all polynomials vanishing on $\mathcal{V}(I) \setminus \mathcal{V}(J)$. The colon ideal is also of crucial importance for the computation of radical ideals and primary decomposition.

If $J = (f)$ is a principal ideal, we sometimes write $I : f$ for the colon ideal $I : (f)$. If $J = (f_1, \dots, f_k)$, then clearly

$$I : J = \bigcap_{i=1}^k I : f_i,$$

which reduces the computation to the case that J is a principal ideal. But clearly

$$I : f = (I \cap (f)) \cdot f^{-1} \quad (1.2.5)$$

(see Vasconcelos [5, Proposition 2.1.4(a)]), which can be computed by Eq. (1.2.4). Thus colon ideals can be obtained by using any algorithm for the intersection of ideals.

For an ideal $I \subseteq K[x_1, \dots, x_n]$ and a polynomial $f \in K[x_1, \dots, x_n]$ we can also consider the ideal

$$I : f^\infty := \bigcup_{i \in \mathbb{N}} I : f^i,$$

which is sometimes referred to as the saturation ideal of I with respect to f . The saturation ideal can be calculated by successively computing the colon ideals $J_i := I : f^i = J_{i-1} : f$. This gives an ascending chain of ideals, thus eventually we get $J_{k+1} = J_k$, so $I : f^\infty = J_k$. But there is a more efficient algorithm, based on the following proposition.

Proposition 1.2.2 *Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal and $f \in K[x_1, \dots, x_n]$ a polynomial. Introduce an additional indeterminate t and form the ideal J in $K[x_1, \dots, x_n, t]$ generated by I and $tf - 1$. Then*

$$I : f^\infty = J \cap K[x_1, \dots, x_n].$$

A proof can be found in Becker and Weispfenning [2, Proposition 6.37].

1.2.5 The Krull Dimension

We define the dimension of an ideal $I \subseteq K[x_1, \dots, x_n]$ to be the Krull dimension of the quotient $K[x_1, \dots, x_n]/I$. There is a method which computes the dimension by using elimination ideals (Becker and Weispfenning [2, Section 6.3]). However, this technique involves a large number of Gröbner basis computations and is therefore not very efficient. A better algorithm is based on the following lemma.

Lemma 1.2.3 *If “ $>$ ” is any monomial ordering, then the dimensions of I and of the leading ideal $L(I)$ with respect to “ $>$ ” coincide.*

A proof can be found in Kemper [11, Exercise 9.7] (solution given). The first step is to establish the special case that “ $>$ ” is graded (or, more generally, weight-graded) by using the (vector space) isomorphism $K[x_1, \dots, x_n]/I \rightarrow K[x_1, \dots, x_n]/L(I)$ given by the normal form mapping, and the second step reduces the general case to the graded one by using the so-called convex cone of the given monomial ordering. Lemma 1.2.3 reduces our problem to the computation of the dimension of $L(I)$, which is a monomial ideal. But the variety defined by a monomial ideal is a finite union of so-called coordinate subspaces, i.e., varieties of the form $\mathcal{V}(\mathcal{M})$ with $\mathcal{M} \subseteq \{x_1, \dots, x_n\}$. Clearly such a variety is contained in the zero set of the monomial ideal J if and only if every generator of J involves at least one variable x_i lying in \mathcal{M} . We obtain the following algorithm (see Cox et al. [4, Proposition 3 of Chap. 9, §1]).

Algorithm 1.2.4 (Dimension of an ideal) Given an ideal $I \subseteq K[x_1, \dots, x_n]$, calculate the dimension of I by performing the following steps:

- (1) Compute a Gröbner basis \mathcal{G} of I with respect to any monomial ordering.
- (2) If \mathcal{G} contains a nonzero constant, then $I = K[x_1, \dots, x_n]$, and the dimension is (by convention) -1 .
- (3) Otherwise, find a subset $\mathcal{M} \subseteq \{x_1, \dots, x_n\}$ of minimal cardinality such that for every nonzero $g \in \mathcal{G}$ the leading monomial $\text{LM}(g)$ involves at least one variable from \mathcal{M} .
- (4) The dimension of I is $n - |\mathcal{M}|$.

Step (3) of the above algorithm is purely combinatorial and therefore usually much faster than the Gröbner basis computation. An optimized version of this step can be found in Becker and Weispfenning [2, Algorithm 9.6].

The set $\mathcal{M} \subseteq \{x_1, \dots, x_n\}$ occurring in Algorithm 1.2.4 has an interesting interpretation. In fact, let $\mathcal{M}' := \{x_1, \dots, x_n\} \setminus \mathcal{M}$ be the complement of \mathcal{M} . Then for every nonzero $g \in \mathcal{G}$ the leading monomial $\text{LM}(g)$ involves at least one variable *not* in \mathcal{M}' . This implies that every nonzero polynomial in $L(I)$ involves a variable not in \mathcal{M}' , so $L(I) \cap K[\mathcal{M}'] = \{0\}$. From this it follows that

$$I \cap K[\mathcal{M}'] = \{0\}. \quad (1.2.6)$$

Indeed, if $f \in I \cap K[\mathcal{M}']$ were nonzero, then $\text{LM}(f)$ would lie in $L(I) \cap K[\mathcal{M}']$. Subsets $\mathcal{M}' \subseteq \{x_1, \dots, x_n\}$ which satisfy (1.2.6) are called independent modulo I (see Becker and Weispfenning [2, Definition 6.46]). Consider the rational function field $L := K(\mathcal{M}')$ in the variables lying in \mathcal{M}' , and let $L[\mathcal{M}]$ be the polynomial ring over L in the variables from \mathcal{M} . Then (1.2.6) is equivalent to the condition that the ideal $IL[\mathcal{M}]$ generated by I in $L[\mathcal{M}]$ is not equal to $L[\mathcal{M}]$. Since we have $|\mathcal{M}'| = \dim(I)$, it follows that \mathcal{M}' is *maximally* independent modulo I . (Indeed, if there existed a strict superset of \mathcal{M}' which is independent modulo I , then $\dim(I) > |\mathcal{M}'|$, see Kemper [11, Theorem 5.9].) The maximality of \mathcal{M}' means that no nonempty subset of \mathcal{M} is independent modulo $IL[\mathcal{M}]$. By Algorithm 1.2.4, the dimension of $IL[\mathcal{M}]$ must therefore be zero. Thus we have shown:

Proposition 1.2.5 Let $I \subsetneq K[x_1, \dots, x_n]$ be an ideal and $\mathcal{M} \subseteq \{x_1, \dots, x_n\}$ as in Algorithm 1.2.4. Set $\mathcal{M}' := \{x_1, \dots, x_n\} \setminus \mathcal{M}$, and take the rational function field $L := K(\mathcal{M}')$ in the variables lying in \mathcal{M}' , and the polynomial ring $L[\mathcal{M}]$. Then the ideal $J := IL[\mathcal{M}]$ generated by I in $L[\mathcal{M}]$ is not equal to $L[\mathcal{M}]$, and $\dim(J) = 0$.

1.3 Syzygy Modules

In this section we write $R := K[x_1, \dots, x_n]$ for the polynomial ring and R^k for a free R -module of rank k . The standard basis vectors of R^k are denoted by e_1, \dots, e_k . Given polynomials $f_1, \dots, f_k \in R$, we ask for the set of all $(h_1, \dots, h_k) \in R^k$ such that $h_1f_1 + \dots + h_kf_k = 0$. This set is a submodule of R^k , called the **syzygy module** of f_1, \dots, f_k and denoted by $\text{Syz}(f_1, \dots, f_k)$. More generally, we ask for the kernel of an R -homomorphism $\varphi: R^k \rightarrow R^l$ between two free R -modules. If $f_i := \varphi(e_i) \in R^l$, then the kernel of φ consists of all $(h_1, \dots, h_k) \in R^k$ with $h_1f_1 + \dots + h_kf_k = 0$. Again $\text{Syz}(f_1, \dots, f_k) := \ker(\varphi)$ is called the syzygy module of the f_i .

1.3.1 Computing Syzygies

In order to explain an algorithm which computes syzygy modules, we have to give a brief introduction into Gröbner bases of submodules of R^k . A **monomial** in R^k is an expression of the form te_i with t a monomial in R . The notion of a monomial ordering is given as in Definition 1.1.1, with condition (i) replaced by $te_i > e_i$ for all i and $1 \neq t$ a monomial in R , and demanding (ii) for monomials $t_1, t_2 \in R^k$ and $s \in R$. Given a monomial ordering, we can now define the leading submodule $L(M)$ of a submodule $M \subseteq R^k$ and the concept of a Gröbner basis of M as in Definition 1.1.3. Normal forms are calculated by Algorithm 1.1.6, with the extra specification that te_i is said to be divisible by $t'e_j$ if $i = j$ and t divides t' , so the quotients are always elements in R . Moreover, the s-polynomial of f and $g \in R^k$ with $\text{LM}(f) = te_i$ and $\text{LM}(g) = t'e_j$ is defined to be zero if $i \neq j$. With these provisions, Buchberger's algorithm can be formulated as in Algorithm 1.1.9.

Suppose that $\mathcal{G} = \{g_1, \dots, g_k\}$ is a Gröbner basis of a submodule $M \subseteq R^l$. Then for $g_i, g_j \in \mathcal{G}$ we have that $\text{NF}_{\mathcal{G}}(\text{spol}(g_i, g_j)) = 0$, so there exist $h_1, \dots, h_k \in R$ with

$$\text{spol}(g_i, g_j) = h_1g_1 + \dots + h_kg_k, \quad (1.3.1)$$

and the h_i can be computed by the Normal Form Algorithm 1.1.6. Since $\text{spol}(g_i, g_j)$ is an R -linear combination of g_i and g_j , Eq.(1.3.1) yields a syzygy $r_{i,j} \in \text{Syz}(g_1, \dots, g_k)$. Of course $r_{i,j} = 0$ if the leading monomials of g_i and of g_j lie in different components of R^l .

The following monomial ordering “ $>_{\mathcal{G}}$ ” on R^k , which depends on \mathcal{G} , was introduced by Schreyer [21]: te_i is considered bigger than $t'e_j$ if $t\text{LM}(g_i) >$

$t' \text{LM}(g_j)$ (with “ $>$ ” the given ordering on R^l), or if $t \text{LM}(g_i) = t' \text{LM}(g_j)$ and $i < j$. It is easy to see that “ $>_{\mathcal{G}}$ ” satisfies the properties of a monomial ordering.

Theorem 1.3.1 (Schreyer [21]) *Let $\mathcal{G} = \{g_1, \dots, g_k\}$ be a Gröbner basis with respect to an arbitrary monomial ordering “ $>$ ” of a submodule $M \subseteq R^l$. Then, with the above notation, the $r_{i,j}$ ($1 \leq i < j \leq k$) form a Gröbner basis of $\text{Syz}(g_1, \dots, g_k)$ with respect to the monomial ordering “ $>_{\mathcal{G}}$ ”.*

This settles the case of syzygies for Gröbner bases. Now assume that $f_1, \dots, f_k \in R^l$ are arbitrary. Using the extended Buchberger algorithm (see at the end of Sect. 1.1), we can calculate a Gröbner basis $\{g_1, \dots, g_{k'}\}$ of the submodule generated by f_1, \dots, f_k , along with representations of the g_i as R -linear combinations of the f_j . Using the Normal Form Algorithm 1.1.6, we can also express the f_j in terms of the g_i . The choice of the f_j and g_i is equivalent to giving homomorphisms $R^k \rightarrow R^l$ and $R^{k'} \rightarrow R^l$, and expressing the f_j in terms of the g_i and vice versa is equivalent to giving homomorphisms φ and ψ such that the diagram

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \longrightarrow & R^{k'} & \longrightarrow & R^l \\ & & & & \downarrow \varphi & \nearrow \psi & \\ & & & & R^k & & \end{array}$$

commutes (both along φ and ψ), where $N := \text{Syz}(g_1, \dots, g_{k'})$ can be computed by Theorem 1.3.1. The following lemma tells us how to compute $\text{Syz}(f_1, \dots, f_k) = \ker(R^k \rightarrow R^l)$.

Lemma 1.3.2 *Let A be a commutative ring and*

$$\begin{array}{ccccccc} 0 & \longrightarrow & N & \longrightarrow & M_1 & \longrightarrow & M \\ & & & & \downarrow \varphi & \nearrow \psi & \\ & & & & M_2 & & \end{array}$$

a commutative diagram (both along φ and ψ) of A -modules, with the upper row exact. Then we have an exact sequence

$$0 \longrightarrow (\text{id} - \psi \circ \varphi)(M_1) \longrightarrow N \oplus (\text{id} - \varphi \circ \psi)(M_2) \longrightarrow M_2 \xrightarrow{\theta} M$$

with maps

$$\begin{aligned} (\text{id} - \psi \circ \varphi)(M_1) &\rightarrow N \oplus (\text{id} - \varphi \circ \psi)(M_2), \quad m \mapsto (m, -\varphi(m)), \quad \text{and} \\ N \oplus (\text{id} - \varphi \circ \psi)(M_2) &\rightarrow M_2, \quad (n, m) \mapsto \varphi(n) + m. \end{aligned}$$

In particular,

$$\ker(\theta) = \varphi(N) + (\text{id} - \varphi \circ \psi)(M_2).$$

Proof It follows by a simple diagram chase that $(\text{id} - \varphi \circ \psi)(M_1) \subseteq N$, so the first map is indeed into $N \oplus (\text{id} - \varphi \circ \psi)(M_2)$. We show the exactness at M_2 . Again by a diagram chase $\theta(\varphi(n) + m) = 0$ for $n \in N$ and $m \in (\text{id} - \varphi \circ \psi)(M_2)$. Conversely, for $m \in \ker(\theta)$ we have

$$m = \varphi(\psi(m)) + (\text{id} - \varphi \circ \psi)(m)$$

with $\psi(m) \in N$. To show the exactness at $N \oplus (\text{id} - \varphi \circ \psi)(M_2)$, take $(n, m_2 - \varphi(\psi(m_2))) \in N \oplus (\text{id} - \varphi \circ \psi)(M_2)$ with $\varphi(n) + m_2 - \varphi(\psi(m_2)) = 0$. Then

$$n = (\text{id} - \varphi \circ \psi)(n - \psi(m_2)) \in (\text{id} - \varphi \circ \psi)(M_1),$$

and $(n, m_2 - \varphi(\psi(m_2))) = (n, -\varphi(n))$. This completes the proof. \square

In summary, we obtain the following algorithm.

Algorithm 1.3.3 (Calculation of a syzygy module) Given elements $f_1, \dots, f_k \in R^l$, perform the following steps to find the syzygy module $\text{Syz}(f_1, \dots, f_k)$:

- (1) Using the extended Buchberger algorithm, calculate a Gröbner basis $\{g_1, \dots, g_{k'}\}$ of the submodule of R^l generated by the f_i together with a matrix $A \in R^{k' \times k}$ such that

$$\begin{pmatrix} g_1 \\ \vdots \\ g_{k'} \end{pmatrix} = A \cdot \begin{pmatrix} f_1 \\ \vdots \\ f_k \end{pmatrix}.$$

- (2) Using the Normal Form Algorithm 1.1.6, compute a matrix $B \in R^{k' \times k'}$ with

$$\begin{pmatrix} f_1 \\ \vdots \\ f_k \end{pmatrix} = B \cdot \begin{pmatrix} g_1 \\ \vdots \\ g_{k'} \end{pmatrix}.$$

- (3) For $1 \leq i < j \leq k'$, compute the syzygies $r_{i,j} \in \text{Syz}(g_1, \dots, g_{k'})$ given by Eq. (1.3.1).
- (4) $\text{Syz}(f_1, \dots, f_k)$ is generated by the $r_{i,j} \cdot A$ and the rows of $I_k - BA$.

1.3.2 Free Resolutions

For a submodule $M \subseteq R^l$ (with $R = K[x_1, \dots, x_n]$ as before) with generating set f_1, \dots, f_k , we can compute generators for $N := \text{Syz}(f_1, \dots, f_k) \subseteq R^k$ by using Algorithm 1.3.3. Continuing by computing the syzygies of these generators and so on, we obtain a free resolution of M , i.e., an exact sequence

$$0 \longrightarrow F_r \longrightarrow F_{r-1} \longrightarrow \cdots \longrightarrow F_2 \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0 \quad (1.3.2)$$

with the F_i free R -modules. Hilbert's syzygy theorem (see Eisenbud [10, Corollary 19.8] or the “original” reference Hilbert [22]) guarantees that there exists a free resolution of finite length (bounded by n , in fact), as given above. Free resolutions are of great interest because they contain a lot of information about the structure of M . Theorem 1.3.1 provides the following method for calculating a free resolution with only a single Gröbner basis computation.

Algorithm 1.3.4 (Schreyer's algorithm) Let $M \subseteq R^l$ be a submodule given by a generating set. Obtain a free resolution of M as follows:

- (1) Compute a Gröbner basis $\mathcal{G} = \{g_1, \dots, g_k\}$ of M with respect to an arbitrary monomial ordering “ $>$ ”. Set $i := 0$ and repeat steps (2)–(4).
- (2) Set $F_i := R^k$ and obtain the map $F_i \rightarrow F_{i-1}$ (with $F_{-1} := M$) from (1.3.2) by $(h_1, \dots, h_k) \mapsto h_1 g_1 + \cdots + h_k g_k$.
- (3) Compute the relations $r_{i,j}$ from Eq. (1.3.1). By Theorem 1.3.1, the $r_{i,j}$ form a Gröbner basis with respect to “ $>_{\mathcal{G}}$ ” of the kernel of the map defined in (2).
- (4) If all $r_{i,j}$ are zero, the resolution is complete. Otherwise, let $\mathcal{G} \subseteq R^k$ be the set of the nonzero $r_{i,j}$ and set $i := i + 1$.

The termination of Algorithm 1.3.4 after at most n iterations is guaranteed by (the proof of) Theorem 2.1 in Chap. 6 of Cox et al. [23] (which provides a new, constructive proof of Hilbert's syzygy theorem).

Now suppose that the polynomial ring R is made into a graded algebra by defining the degrees $\deg(x_i)$ of the indeterminates to be positive integers. Then the free module R^l can be made into a graded R -module by defining the $\deg(e_i)$ to be integers. Moreover, suppose that M is a graded submodule, i.e., generated by homogeneous elements. Then we want to find a graded free resolution, i.e., one that consists of graded free modules F_i with all mappings degree-preserving. Applying Buchberger's algorithm to a homogeneous generating set of M yields a homogeneous Gröbner basis, too, and by inspection of the way in which the syzygies $r_{i,j}$ are formed from Eq. (1.3.1), we see that the resolution obtained by Algorithm 1.3.4 is indeed graded (with the proper choice of the degrees of the free generators, i.e., each generator gets the same degree as the relation to which it is mapped).

In the case that R^l is graded and M is a graded submodule, we are also interested in obtaining a **minimal free resolution** of M , i.e., a free resolution such that the free generators of each F_i are mapped to a minimal generating set of the image of

F_i . Such a resolution is unique up to isomorphism of complexes (see Eisenbud [10, Theorem 20.2]), and in particular its length is unique. This length is called the **homological dimension** of M , written as $\text{hdim}(M)$, and is an important structural invariant of M . A graded resolution (1.3.2) calculated by Algorithm 1.3.4 is usually not minimal, so how can it be transformed into a minimal resolution, preferably without computing any further Gröbner bases? As a first step, we can use linear algebra to select a minimal subset of the free generators of F_0 whose image in M generates M . Thus we obtain a free submodule $F'_0 \subseteq F_0$ and a commutative diagram

$$\begin{array}{ccccccc} \cdots & \longrightarrow & F_1 & \xrightarrow{\rho} & F_0 & \longrightarrow & M \\ & & \downarrow \varphi & & \downarrow \psi & & \parallel \\ & & & & F'_0 & \longrightarrow & M, \end{array}$$

where $\varphi \circ \psi = \text{id}$. Lemma 1.3.2 yields an exact sequence

$$0 \longrightarrow (\text{id} - \psi \circ \varphi)(F_0) \longrightarrow \text{im}(\rho) \xrightarrow{\varphi} F'_0 \longrightarrow M. \quad (1.3.3)$$

Observe that $(\text{id} - \psi \circ \varphi)$ maps a free generator e_i from F_0 either to zero (if it is also a generator of F'_0) or to a nonzero element of $(\text{id} - \psi \circ \varphi)(F_0)$ corresponding to the representation of the image of e_i in M in terms of the images of those e_j contained in F'_0 . These nonzero elements are linearly independent, hence $(\text{id} - \psi \circ \varphi)(F_0)$ is a free module. We can use linear algebra to compute preimages under ρ of the free generators of $(\text{id} - \psi \circ \varphi)(F_0)$ in F_1 . This yields a free submodule $\widehat{F}_1 \subseteq F_1$ such that $\rho(\widehat{F}_1) = (\text{id} - \psi \circ \varphi)(F_0)$ and the restriction of ρ to \widehat{F}_1 is injective. Now it is easy to see that (1.3.3) and (1.3.2) lead to the exact sequence

$$0 \longrightarrow F_r \longrightarrow F_{r-1} \longrightarrow \cdots \longrightarrow F_3 \longrightarrow F_2 \oplus \widehat{F}_1 \longrightarrow F_1 \xrightarrow{\varphi \circ \rho} F'_0 \longrightarrow M \longrightarrow 0.$$

Thus we have managed to replace (1.3.2) by a free resolution with the first free module minimal. Iterating this process, we obtain the desired minimal free resolution of M . Notice that the only computationally significant steps are the selection of minimal generators for M and the computation of preimages of $e_i - \psi(\varphi(e_i))$ for some free generators e_i of F_0 . Both of these are accomplished by linear algebra. Thus a minimal resolution of M can be computed by just one Gröbner basis computation and linear algebra.

1.4 Hilbert Series

In this section, we prove some results about Hilbert series of rings, and how we can use Gröbner bases to compute them.

Definition 1.4.1 For a graded vector space $V = \bigoplus_{d=k}^{\infty} V_d$ with k an integer and V_d finite dimensional for all d we define the **Hilbert series** of V as the formal Laurent series

$$H(V, t) := \sum_{d=k}^{\infty} \dim(V_d) t^d.$$

In the literature, Hilbert series are sometimes called Poincaré series. In our applications, V will always be a graded algebra or a graded module.

Example 1.4.2 Let us compute the Hilbert series of $K[x_1, \dots, x_n]$. There are $\binom{n+d-1}{n-1}$ monomials of degree d , therefore the Hilbert series is

$$H(K[x_1, \dots, x_n], t) = \sum_{d=0}^{\infty} \binom{n+d-1}{n-1} t^d.$$

This is exactly the power series expansion of $(1-t)^{-n}$. \triangleleft

Remark 1.4.3 If V and W are two graded vector spaces, then the tensor product $V \otimes W$ also has a natural grading, namely

$$(V \otimes W)_d = \bigoplus_{d_1+d_2=d} V_{d_1} \otimes W_{d_2}.$$

It is obvious from this formula that $H(V \otimes W, t) = H(V, t)H(W, t)$. Suppose that $R = K[x_1, \dots, x_n]$ and x_i has degree $d_i > 0$. Then we have $R = K[x_1] \otimes K[x_2] \otimes \dots \otimes K[x_n]$ as graded algebras and $H(K[x_i], t) = (1-t^{d_i})^{-1}$. It follows that

$$H(R, t) = \frac{1}{(1-t^{d_1}) \cdots (1-t^{d_n})} \tag{1.4.1}$$

\triangleleft

Remark 1.4.4 If

$$0 \rightarrow V^{(1)} \rightarrow V^{(2)} \rightarrow \dots \rightarrow V^{(r)} \rightarrow 0 \tag{1.4.2}$$

is an exact sequence of graded vector spaces (all maps respect degree) with $V_d^{(i)}$ finite dimensional for all i and d , then

$$\sum_{i=1}^r (-1)^i H(V^{(i)}, t) = 0.$$

This is clear because the degree d part of (1.4.2) is exact for all d . \triangleleft

Proposition 1.4.5 (Hilbert) *If $R = \bigoplus_{d=0}^{\infty} R_d$ is a finitely generated graded algebra over a field $K = R_0$, then $H(R, t)$ is the power series of a rational function. The radius of convergence of this power series is at least 1. Moreover, if $M = \bigoplus_{d=k}^{\infty} M_d$ is a finitely generated graded R -module, then $H(M, t)$ is the Laurent series of a rational function (which may have a pole at 0).*

Proof Let $A = K[x_1, x_2, \dots, x_n]$ be the polynomial ring, graded in such a way that $\deg(x_i) = d_i > 0$. Then $H(A, t)$ is a rational function by (1.4.1), and the radius of convergence of the power series is 1 if $n > 0$, and ∞ if $n = 0$. For any integer e , we define the A -module $A(e)$ by $A(e) = \bigoplus_{d=-e}^{\infty} A(e)_d$ with $A(e)_d := A_{e+d}$. It is clear that $H(A(e), t) = t^{-e} H(A, t)$ is again a rational function. A module is free if it is isomorphic to a direct sum $\bigoplus_i A(e_i)$. The Hilbert series of a finitely generated free module M is a rational function. If M is a finitely generated A -module, then by Hilbert's syzygy theorem (see Eisenbud [10, Theorem 1.13]), there exists a resolution

$$0 \rightarrow F^{(r)} \rightarrow F^{(r-1)} \rightarrow \cdots \rightarrow F^{(1)} \rightarrow F^{(0)} \rightarrow M \rightarrow 0, \quad (1.4.3)$$

where $F^{(i)}$ is a finitely generated free A -module for all i , and the sequence is exact. It follows from Remark 1.4.4 that

$$H(M, t) = \sum_{i=0}^r (-1)^i H(F^{(i)}, t), \quad (1.4.4)$$

so $H(M, t)$ is a rational function. If M is nonnegatively graded, then the same is true for all F_i , so the radius of convergence of $H(M, t)$ is at least 1.

Let R be an arbitrary finitely generated graded algebra over $K = R_0$. Then for some n and some $d_1, \dots, d_n > 0$, there exists a homogeneous ideal $I \subseteq A$ such that $A/I \cong R$. Hence R is a finitely generated, nonnegatively graded A -module, and the claim follows. Moreover, any finitely generated graded R -module M is also a finitely generated graded A -module. \square

The above proof gives an easy way to compute the Hilbert series of a graded module M over a graded polynomial ring $R = K[x_1, \dots, x_n]$, if we have a graded free resolution (1.4.3) of M . Indeed, we only have to combine (1.4.4) and (1.4.1). A graded free resolution can be calculated by Algorithm 1.3.4, which involves the computation of a Gröbner basis of M . Given a Gröbner basis of M , there is also a more direct way to find the Hilbert series, which will be discussed in Sect. 1.4.1.

The Hilbert series encodes geometric information as the following lemma shows.

Lemma 1.4.6 *Let $R = \bigoplus_{d \geq 0} R_d$ be a graded algebra, finitely generated over the field $R_0 = K$. Then $r := \dim(R)$ is equal to the pole order of $H(R, t)$ at $t = 1$.*

Proof The proof requires the concept of homogeneous systems of parameters. For the definition and the proof of existence, we refer forward to Sect. 2.5.2. Let f_1, \dots, f_r be a homogeneous system of parameters for R , and set $A := K[f_1, \dots, f_r]$.

It follows from (1.4.1) that $H(A, t)$ has pole order r . In fact, $\lim_{t \nearrow 1} (1-t)^r H(A, t) = \prod_{i=1}^r d_i^{-1}$, where $\lim_{t \nearrow 1}$ denotes the limit from below (see Example 1.4.8 below). There exists an A -free resolution

$$0 \rightarrow F^{(r)} \rightarrow F^{(r-1)} \rightarrow \cdots \rightarrow F^{(0)} \rightarrow R \rightarrow 0.$$

Using (1.4.4) we conclude that $H(R, t)$ has pole order $\leq r$ because the same holds for all $H(F^{(i)}, t)$. Note that $H(R, t) \geq H(A, t)$ for $0 < t < 1$ since $A \subseteq R$. If the pole order of $H(R, t)$ were strictly smaller than r , then

$$0 = \lim_{t \nearrow 1} (1-t)^r H(R, t) \geq \lim_{t \nearrow 1} (1-t)^r H(A, t) = \prod_{i=1}^r d_i^{-1} > 0.$$

This contradiction shows that $H(R, t)$ has in fact pole order r . \square

Definition 1.4.7 Let $R = \bigoplus_{d \geq 0} R_d$ be a graded algebra, finitely generated over $R_0 = K$. Then the **degree** of R is defined as

$$\deg(R) = \lim_{t \nearrow 1} (1-t)^r H(R, t)$$

where $r := \dim(R)$ is the Krull dimension of R and $\lim_{t \nearrow 1}$ means the limit from below.

Up to a sign, the degree of R is the first coefficient of the Laurent series expansion of $H(R, t)$ at $t = 1$.

Example 1.4.8 If $A = K[x_1, \dots, x_n]$ with $\deg(x_i) = d_i$, then

$$\deg(A) = \lim_{t \nearrow 1} \frac{(1-t)^n}{\prod_{i=1}^n (1-t^{d_i})} = \lim_{t \nearrow 1} \frac{1}{\prod_{i=1}^n (1+t+\dots+t^{d_i-1})} = \frac{1}{\prod_{i=1}^n d_i},$$

so we have $\deg(A) = (\prod_{i=1}^n d_i)^{-1}$. \triangleleft

If $A = K[x_1, \dots, x_n]$ (all x_i of degree 1) and $I \subset A$ is a homogeneous ideal, then I corresponds to a projective variety $Y \subset \mathbb{P}^{n-1}$. Then the degree of A/I is the same as the degree of Y as a projective variety (see Hartshorne [24, p. 52]).

1.4.1 Computation of Hilbert Series

Again, let $R = K[x_1, \dots, x_n]$ be a polynomial ring, graded by $\deg(x_i) = d_i$, and suppose that $I \subseteq R$ is a homogeneous ideal. We want to compute $H(R/I, t)$, or equivalently $H(I, t) = H(R, t) - H(R/I, t)$. We choose a monomial ordering “ $>$ ” on R and use the Buchberger Algorithm 1.1.9 to compute a Gröbner basis $\mathcal{G} = \{g_1, \dots, g_r\}$ of I with respect to “ $>$ ”. The leading monomials $\text{LM}(g_1), \dots, \text{LM}(g_r)$

generate the leading ideal $L(I)$. If $m_1, \dots, m_l \in L(I)$ are distinct monomials which span $L(I)_d$, then we can find homogeneous $f_1, \dots, f_l \in I_d$ such that $\text{LM}(f_i) = m_i$. It is clear that f_1, \dots, f_l is a basis of I_d . It follows that

$$\dim(L(I)_d) = \dim(I_d).$$

We conclude $H(L(I), t) = H(I, t)$, so we have reduced the problem to computing the Hilbert series of a monomial ideal.

So suppose that $I = (m_1, \dots, m_l) \subseteq R$ is a monomial ideal. We will show how to compute $H(I, t)$ using recursion with respect to l . Let $J = (m_1, \dots, m_{l-1})$, then we have an isomorphism

$$J/(J \cap (m_l)) \cong I/(m_l)$$

of graded R -modules. Notice that

$$J \cap (m_l) = (\text{lcm}(m_1, m_l), \text{lcm}(m_2, m_l), \dots, \text{lcm}(m_{l-1}, m_l)),$$

where lcm means least common multiple. By recursion we can compute $H(J, t)$ and $H(J \cap (m_l), t)$, and $H((m_l), t) = t^{\deg(m_l)} \prod_{i=1}^n (1 - t^{d_i})^{-1}$. So we can compute $H(I, t)$ as

$$H(I, t) = H((m_l), t) + H(J, t) - H(J \cap (m_l), t). \quad (1.4.5)$$

See Bayer and Stillman [25] for more details. A slightly different approach was taken in Bigatti et al. [26].

Example 1.4.9 Let us compute the Hilbert series of the ideal $I = (xz - y^2, xw - yz, yw - z^2) \subset A := K[x, y, z, w]$, where all indeterminates have degree 1. Note that $H(A, t) = (1-t)^{-4}$ and $H((f), t) = t^d(1-t)^{-4}$ if f is a homogeneous polynomial of degree d . We choose the lexicographic ordering “ $>$ ” with $x > y > z > w$. Then $\mathcal{G} = \{xz - y^2, xw - yz, yw - z^2\}$ is a Gröbner basis of I . It follows that the initial ideal $L(I)$ is generated by xz, xw, yw . Observe that $(xz, xw) \cap (yw) = (xyzw, xyw) = (xyw)$. By (1.4.5) we get

$$H(L(I), t) = H((xz, xw, yw), t) = H((yw), t) + H((xz, xw), t) - H((xyw), t). \quad (1.4.6)$$

We know that $H((yw), t) = t^2/(1-t)^4$ and $H((xyw), t) = t^3/(1-t)^4$. We only need to find $H((xz, xw), t)$. Repeating the above process and making use of $(xz) \cap (xw) = (xzw)$, we obtain (again by (1.4.5))

$$H((xz, xw), t) = H((xw), t) + H((xz), t) - H((xzw), t) = \frac{2t^2 - t^3}{(1-t)^4}. \quad (1.4.7)$$

Substituting (1.4.7) in (1.4.6) gives

$$H(I, t) = H(L(I), t) = \frac{t^2}{(1-t)^4} + \frac{2t^2 - t^3}{(1-t)^4} - \frac{t^3}{(1-t)^4} = \frac{3t^2 - 2t^3}{(1-t)^4},$$

and finally

$$H(A/I, t) = H(A, t) - H(I, t) = \frac{1}{(1-t)^4} - \frac{3t^2 - 2t^3}{(1-t)^4} = \frac{1 + 2t}{(1-t)^2}.$$

The pole order of $H(A/I, t)$ at $t = 1$ is 2, so $\dim(A/I) = 2$. If we take $\lim_{t \nearrow 1} (1-t)^2 H(A/I, t)$, we get $\deg(A/I) = 3$. The ideal I defines a curve of degree 3 in \mathbb{P}^3 (the twisted cubic curve). \triangleleft

1.5 The Radical Ideal

The computation of the radical ideal \sqrt{I} of an ideal $I \subseteq K[x_1, \dots, x_n]$ is one of the basic tasks of constructive ideal theory. For the purposes of this book, radical computation is important since it is used in de Jong's normalization algorithm, which we present in Sect. 1.6. Unfortunately, radical computation is a rather cumbersome task, which may be a reason why quite a few papers, such as Gianni et al. [27], Krick and Logar [28], Alonso et al. [29], Eisenbud et al. [30], Matsumoto [31], Fortuna et al. [32], Kemper [33], and Laplagne [34], are devoted to it. (The situation is similar, but worse, for the task of primary decomposition.) The majority of the algorithms proposed in the literature work by reduction to the zero-dimensional case and are restricted to the case of characteristic 0. We will only sketch this case and refer to Becker and Weispfenning [2, Section 8.7] for more details. However, we will spend more time on the less well-known case of positive characteristic and present the algorithm of Matsumoto [31], which does not require the reduction to dimension 0.

1.5.1 Reduction to Dimension Zero

Given a proper ideal $I \subsetneq K[x_1, \dots, x_n]$, we can use Algorithm 1.2.4 to compute a set $\mathcal{M} \subseteq \{x_1, \dots, x_n\}$ and its complement \mathcal{M}' such that $\dim(I) = |\mathcal{M}'|$. We consider the rational function field $L := K(\mathcal{M}')$ and the ideal $J := IL[\mathcal{M}]$ generated by I in the polynomial ring $L[\mathcal{M}]$ over L . Then Proposition 1.2.5 tells us that $\dim(J) = 0$. Assume that we are able to compute the radical ideal \sqrt{J} . There is an algorithm which computes \sqrt{I} from the knowledge of \sqrt{J} and $\sqrt{I + (f)}$ for a certain $f \in$

$K[x_1, \dots, x_n] \setminus I$. The latter radical ideal can be computed by a recursive call. As stated above, we refer to Becker and Weispfenning [2, Section 8.7] for details.

Now if $\text{char}(K) = 0$, there are quite simple algorithms for computing the radical of a zero-dimensional ideal. They are based on the fact that the squarefree part of a univariate polynomial f is $f / \gcd(f, f')$. This is no longer true in positive characteristic. The paper [33] presents an algorithm for computing radicals of zero-dimensional ideals in positive characteristic. Since this algorithm is a bit messy, too, we prefer to explain Matsumoto's algorithm for computing radicals of ideals in positive characteristic. This algorithm is much simpler and does not require the reduction step to dimension 0.

1.5.2 Positive Characteristic

Matsumoto's algorithm [31] is based on the following observation: If $p := \text{char}(K) > 0$, we have the Frobenius homomorphism

$$F: K[x_1, \dots, x_n] \rightarrow K[x_1, \dots, x_n], f \mapsto f^p.$$

If $I \subseteq K[x_1, \dots, x_n]$ is an ideal, then so is the preimage $F^{-1}(I)$, and the iterated preimages $F^{-i}(I)$ form an ascending chain of ideals. By the Noether property, this becomes stable at some $F^{-k}(I)$. Since all $F^{-i}(I)$ are contained in \sqrt{I} since every element of \sqrt{I} lies in some $F^{-i}(I)$ and therefore in $F^{-k}(I)$, we obtain

$$\sqrt{I} = F^{-k}(I).$$

To turn this into an algorithm, we need to be able to compute the preimage $F^{-1}(I)$ for an ideal I . To this end, we split F into two homomorphisms. In fact, $F = \varphi \circ \psi$ with

$$\psi: K[x_1, \dots, x_n] \rightarrow K[y_1, \dots, y_n], \sum_{\underline{i} \in \mathbb{N}_0^n} a_{\underline{i}} \underline{x}^{\underline{i}} \mapsto \sum_{\underline{i} \in \mathbb{N}_0^n} F(a_{\underline{i}}) \underline{y}^{\underline{i}}$$

with y_1, \dots, y_n additional indeterminates, and

$$\varphi: K[y_1, \dots, y_n] \rightarrow K[x_1, \dots, x_n], \sum_{\underline{i} \in \mathbb{N}_0^n} a_{\underline{i}} \underline{y}^{\underline{i}} \mapsto \sum_{\underline{i} \in \mathbb{N}_0^n} a_{\underline{i}} F(\underline{x}^{\underline{i}}).$$

If we assume that K is perfect (and it is under this assumption that the algorithm works), then ψ is an isomorphism of rings, so the preimage of an ideal under ψ can be computed by applying ψ^{-1} to the generators. Moreover, φ is a homomorphism of K -algebras between two polynomial rings, and we have explained at the end of Sect. 1.2.2 how preimages of ideals under such homomorphisms can be computed.

In summary, we obtain the following algorithm:

Algorithm 1.5.1 (Matsumoto's algorithm) Given an ideal $I \subseteq K[x_1, \dots, x_n]$ in a polynomial ring over a perfect field of characteristic $p > 0$, perform the following steps to find the radical ideal \sqrt{I} :

- (1) With additional indeterminates y_1, \dots, y_n , form the ideal

$$J := I \cdot K[x_1, \dots, x_n, y_1, \dots, y_m] + (x_1^p - y_1, \dots, x_n^p - y_n)$$

in $K[x_1, \dots, x_n, y_1, \dots, y_n]$.

- (2) Compute the elimination ideal $L := K[y_1, \dots, y_n] \cap J$, so $L = \varphi^{-1}(I)$.
- (3) If $L = (f_1, \dots, f_m)$, substitute the coefficients of each f_j by p th roots and the variables y_i by x_i . This yields the polynomial $g_j := \psi^{-1}(f_j) \in K[x_1, \dots, x_n]$. Then

$$I' := (g_1, \dots, g_m) = F^{-1}(I).$$

- (4) If $I' \subseteq I$, then I is the desired radical ideal. Otherwise, set $I := I'$ and go to step (1).

We conclude this section by a remark about testing radical membership. While the computation of a radical ideal is hard, there is a simple method for testing whether a given polynomial lies in the radical of an ideal I , based on the following proposition:

Proposition 1.5.2 *Let $I \subseteq K[x_1, \dots, x_n]$ be an ideal and $f \in K[x_1, \dots, x_n]$. Then $f \in \sqrt{I}$ if and only if*

$$1 \in I \cdot K[x_1, \dots, x_n, t] + (tf - 1),$$

where t is a new indeterminate.

A proof can be found in Cox et al. [4, Proposition 8 of Chapter 4, §2]. See Lemma 4.9.3 for a simplification of the test that applies when I and f are homogeneous.

1.6 Normalization

Let R be an integral domain and \tilde{R} the integral closure of R in its field of fractions. We call \tilde{R} the **normalization** of R . If $\tilde{R} = R$, we say that R is **normal**. One reason why normalization is interesting in invariant theory, is that every invariant ring $K[x_1, \dots, x_n]^G$ is normal (see Proposition 2.4.4). The usefulness of normalization is further underlined by Corollary 3.12.5. The problem of computing the normalization of an affine domain (i.e., the quotient ring of a polynomial ring over a field by a

prime ideal) has led to various papers, among them Vasconcelos [35], de Jong [36], Decker et al. [37], Singh and Swanson [38], and Greuel et al. [39].

In this section we will describe the algorithm by de Jong [36]. The algorithm is based on a theorem by Grauert and Remmert (see the references in [36]). We start by assuming that R is a Noetherian integral domain. For $I \subseteq R$ a nonzero ideal, choose $0 \neq c \in I$ and consider the colon ideal $(c \cdot I) : I \subseteq R$. Inside $\text{Quot}(R)$, the field of fractions of R , we form

$$E(I) := c^{-1} \cdot (c \cdot I) : I.$$

(It is easy to show that $E(I)$ does not depend on the choice of c . This is not used in the sequel, but justifies the notation. It is also easy to show that $E(I)$ is isomorphic to $\text{End}_R(I)$.)

Lemma 1.6.1 *$E(I)$ is a ring and $R \subseteq E(I) \subseteq \tilde{R}$.*

Proof It is clear that R is contained in $E(I)$ and that $E(I)$ is closed under addition. If $a, b \in E(I)$, then

$$abcI \subseteq acI \subseteq cI,$$

so $abc \in R$ and $ab \in E(I)$. Since $E(I)$ is finitely generated as an R -module, it is contained in \tilde{R} . \square

If R is normal, the lemma implies $E(I) = R$. But when does the converse hold? To state our result, we set $X := \text{Spec}(R)$,

$$X_{\text{nn}} := \{P \in X \mid R_P \text{ is not normal}\}$$

(the *nonnormal locus*), and

$$\mathcal{V}_X(I) := \{P \in X \mid I \subseteq P\}.$$

Theorem 1.6.2 *With the notation introduced above, let $I \subseteq R$ be a nonzero radical ideal such that $X_{\text{nn}} \subseteq \mathcal{V}_X(I)$. Then the equivalence*

$$R \text{ is normal} \iff E(I) = R$$

holds.

Proof The implication “ \Rightarrow ” follows directly from Lemma 1.6.1, so we only need to show the converse. So assume $E(I) = R$ and let $a \in \tilde{R}$. With $J := \{b \in R \mid ab \in R\}$ we have

$$\mathcal{V}_X(J) = \{P \in X \mid a \notin R_P\},$$

so

$$\mathcal{V}_X(J) \subseteq X_{\text{nn}} \subseteq \mathcal{V}_X(I).$$

This implies $\sqrt{J} \supseteq \sqrt{I} = I$, so $I^k \subseteq J$ for some k . By way of contradiction, assume that the minimal such k is positive. Then there exists $b \in I^{k-1}$ with $b \notin J$, so $ab \notin R$. But

$$abI \subseteq aI^k \subseteq aJ \subseteq R. \quad (1.6.1)$$

Moreover, $ab \in \tilde{R}$, so we have a relation

$$(ab)^m = r_0 + r_1 ab + \cdots + r_{m-1} (ab)^{m-1}$$

with $r_i \in R$. For $u \in I$, this yields

$$(abu)^m = r_0 u^m + r_1 (abu) u^{m-1} + \cdots + r_{m-1} (abu)^{m-1} u \in I,$$

where we have used (1.6.1). This implies $abu \in I$, so $abI \subseteq I$ and $cabI \subseteq cI$. Since $cab \in R$ by (1.6.1), this means $cab \in (c \cdot I) : I$, so $ab \in E(I)$. But now our hypothesis $E(I) = R$ yields the contradiction $ab \notin R$. We conclude $k = 0$, so $J = R$ and $a \in R$. Since this holds for all $a \in \tilde{R}$, the proof is complete. \square

These results can be turned into an algorithm in the case that R is an affine domain over a perfect field K . Since the nonnormal locus X_{nn} is contained in the singular locus X_{sing} (see Kemper [11, Corollary 13.6(b)]), the Jacobian criterion (see [11, Theorem 13.10]) yields an ideal $I \subseteq R$ with $X_{\text{nn}} \subseteq X_{\text{sing}} \subseteq \mathcal{V}_X(I)$. Since X_{sing} is proper in X (see [11, Corollary 13.13(b)]), I can be chosen to be nonzero. Now $E(I)$ can be computed and the criterion form Theorem 1.6.2 can be tested. If it shows $R \not\subseteq \tilde{R}$, new elements from \tilde{R} will be produced. Since \tilde{R} is finitely generated as an R -module (see [11, Theorem 8.26]), iterating this process will eventually terminate. The most reasonable setup for the algorithm is that R is given by a presentation: $R \cong K[x_1, \dots, x_n]/J$. Then with each iteration, new generators $(g + J)/(f + J) \in \text{Quot}(R)$ will be added to R , so we need to compute a presentation for the extended algebra to carry on. The following lemma reduces this task to the computation of an elimination ideal.

Lemma 1.6.3 *Let $K \subseteq L$ be a field extension and $\varphi: K[x_1, \dots, x_n] \rightarrow L$ a homomorphism of K -algebras with kernel J . Furthermore, let $a = \varphi(g)/\varphi(f) \in L$ and consider the homomorphism*

$$\Phi: K[x_1, \dots, x_n, y] \rightarrow L, \quad x_i \mapsto \varphi(x_i), \quad y \mapsto a,$$

where y is an indeterminate. With an additional indeterminate t , set

$$\hat{J} := J \cdot K[x_1, \dots, x_n, y, t] + (fy - g, ft - 1).$$

Then

$$\ker(\Phi) = \hat{J} \cap K[x_1, \dots, x_n, y].$$

Proof Clearly \hat{J} lies in the kernel of the homomorphism $K[x_1, \dots, x_n, y, t] \rightarrow L$ with $x_i \mapsto \varphi(x_i)$, $y \mapsto a$, $t \mapsto 1/\varphi(f)$. Hence $\hat{J} \cap K[x_1, \dots, x_n, y] \subseteq \ker(\Phi)$. To prove the converse, we first remark that $fh \in \hat{J}$ for $h \in K[x_1, \dots, x_n, y, t]$ implies $h \in \hat{J}$ since f is invertible modulo \hat{J} . Furthermore, $f^i y^i - g^i \in \hat{J}$ for any nonnegative integer i , since

$$f^{i+1} y^{i+1} - g^{i+1} = (f^i y^i - g^i)fy + g^i(fy - g).$$

It follows that $f^d (y^i - (g/f)^i) \in \hat{J}$ for $d \geq i$. Let $h \in \ker(\Phi)$ and set $d := \deg_y(h)$. Write $h(g/f)$ for the result of substituting y by g/f in h . Then $\varphi(f^d h(g/f)) = 0$, so $f^d h(g/f) \in J$. By the preceding argument we also have $f^d (h - h(g/f)) \in \hat{J}$, hence $f^d h \in \hat{J}$. But this implies $h \in \hat{J}$, completing the proof. \square

We can now give the ensuing algorithm.

Algorithm 1.6.4 (de Jong's algorithm) Given a prime ideal $J \subseteq K[x_1, \dots, x_n]$ with K a perfect field, perform the following steps to obtain the normalization \tilde{R} of $R := K[x_1, \dots, x_n]/J$, given by a presentation $\tilde{R} \cong K[x_1, \dots, x_{n+m}]/\tilde{J}$ (and the embedding $R \subseteq \tilde{R}$ given by $x_i + J \mapsto x_i + \tilde{J}$):

- (1) Set $m := 0$ and $\tilde{J} := J$.
- (2) Compute the Jacobian matrix $\mathfrak{J} := (\partial f_i / \partial x_j)_{i,j}$, where $\tilde{J} = (f_1, \dots, f_k)$.
- (3) With $l := n + m - \dim(R)$, compute the ideal generated by \tilde{J} and the $(l \times l)$ -minors of \mathfrak{J} . Call this ideal I_{sing} . Choose an ideal I_0 such that $\tilde{J} \subsetneq I_0 \subseteq I_{\text{sing}}$ and an element $f \in I_0 \setminus \tilde{J}$.
- (4) Compute $I := \sqrt{I_0}$ and the colon ideal $(f \cdot I + \tilde{J}) : I$.
- (5) If $(f \cdot I + \tilde{J}) : I \subseteq \tilde{J} + (f)$ (test this by computing normal forms of the generators of the left hand side with respect to a Gröbner basis of the right hand side), we are done.
- (6) Otherwise, choose $g \in ((f \cdot I + \tilde{J}) : I) \setminus (\tilde{J} + (f))$.
- (7) Set $m := m + 1$ and form the ideal

$$\hat{J} := \tilde{I} \cdot K[x_1, \dots, x_{n+m}, t] + (fx_{n+m} - g, ft - 1)$$

in $K[x_1, \dots, x_{n+m}, t]$ with x_{n+m} and t new indeterminates.

- (8) Compute $\tilde{J} := \hat{J} \cap K[x_1, \dots, x_{n+m}]$ and go to step (2).

We conclude the section with an example.

Example 1.6.5 We can use Algorithm 1.6.4 to de-singularize curves. As an example, consider the curve \mathcal{C} in \mathbb{C}^2 given by the ideal

$$J = (x^6 + y^6 - xy),$$

which has genus 9 and a double point at the origin. A Gröbner basis of $I_{\text{sing}} = (x^6 + y^6 - xy, 6x^5 - y, 6y^5 - x)$ is $\{x, y\}$. Therefore we can choose $f = x$ and $I = I_0 = I_{\text{sing}}$. We obtain

$$(f \cdot I + \tilde{J}) : I = (x, y^5) \quad \text{and} \quad \tilde{J} + (f) = (x, y^6).$$

Thus we can choose $g := y^5$ to obtain a new element $a := (g + I)/(f + I)$ in \tilde{R} . By step (8) of Algorithm 1.6.4 we calculate the kernel \tilde{J} of the map

$$\mathbb{C}[x, y, z] \rightarrow \tilde{R}, \quad x \mapsto x + J, \quad y \mapsto y + J, \quad z \mapsto a$$

and obtain

$$\tilde{J} = (y^5 - xz, x^5 + yz - y, x^4y^4 + z^2 - z).$$

The last equation confirms the integrality of a over R . Going into the next iteration of Algorithm 1.6.4 yields no new elements in \tilde{R} , hence $\tilde{R} = \mathbb{C}[x, y, z]/\tilde{J}$. \tilde{J} defines a curve $\tilde{\mathcal{C}}$ in \mathbb{C}^3 which maps onto \mathcal{C} by projecting on the first two coordinates. With the exception of the origin, every point of \mathcal{C} has a fiber consisting of a single point, and the fiber of the origin consists of the points $(0, 0, 0)$ and $(0, 0, 1)$. \triangleleft

References

1. Bernd Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, Wien, New York 1993.
2. Thomas Becker, Volker Weispfenning, *Gröbner Bases*, Springer-Verlag, Berlin, Heidelberg, New York 1993.
3. William W. Adams, Phillippe Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics 3, American Mathematical Society, Providence, RI 1994.
4. David Cox, John Little, Donal O’Shea, *Ideals, Varieties, and Algorithms*, Springer-Verlag, New York, Berlin, Heidelberg 1992.
5. Wolmer V. Vasconcelos, *Computational Methods in Commutative Algebra and Algebraic Geometry*, Algorithms and Computation in Mathematics 2, Springer-Verlag, Berlin, Heidelberg, New York 1998.
6. Martin Kreuzer, Lorenzo Robbiano, *Computational Commutative Algebra 1*, Springer-Verlag, Berlin 2000.
7. Martin Kreuzer, Lorenzo Robbiano, *Computational Commutative Algebra 2*, Springer-Verlag, Berlin 2005.
8. Gert-Martin Greuel, Gerhard Pfister, *A Singular Introduction to Commutative Algebra*, Springer-Verlag, Berlin 2002.
9. Viviana Ene, Jürgen Herzog, *Gröbner bases in Commutative Algebra*, Graduate Studies in Mathematics 130, American Mathematical Society, Providence, RI 2012.
10. David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York 1995.
11. Gregor Kemper, *A Course in Commutative Algebra*, Graduate Texts in Mathematics 256, Springer-Verlag, Berlin, Heidelberg 2011.

12. CoCoATeam, *CoCoA: a system for doing Computations in Commutative Algebra*, available at <http://cocoa.dima.unige.it>, 2000.
13. Daniel R. Grayson, Michael E. Stillman, *Macaulay2, a software system for research in algebraic geometry*, available at <http://www.math.uiuc.edu/Macaulay2/>, 1996.
14. Wieb Bosma, John J. Cannon, Catherine Playoust, *The Magma algebra system I: The user language*, J. Symb. Comput. **24** (1997), 235–265.
15. Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, Hans Schönemann, *SINGULAR 4-0-2 — A computer algebra system for polynomial computations*, <http://www.singular.uni-kl.de>, 2015.
16. Bruno Buchberger, *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal* (German), Dissertation, Institute for Mathematics, University of Innsbruck 1965.
17. H. Michael Möller, Ferdinando Mora, *Upper and lower bounds for the degree of Gröbner bases*, in: John Fitch, ed., *EUROSAM 84, Proc. Int. Symp. on Symbolic and Algebraic Computation*, Lect. Notes Comput. Sci. **174**, pp. 172–183, Springer-Verlag, Berlin, Heidelberg, New York 1984.
18. Joachim von zur Gathen, Jürgen Gerhard, *Modern Computer Algebra*, Cambridge University Press, Cambridge 1999.
19. J. C. Faugère, P. Gianni, D. Lazard, T. Mora, *Efficient computation of zero-dimensional Gröbner bases by change of ordering*, J. Symb. Comput. **16** (1993), 329–344.
20. Stéphane Collart, Michael Kalkbrenner, Daniel Mall, *Converting bases with the Gröbner walk*, J. Symb. Comput. **24** (1997), 465–469.
21. Frank-Olaf Schreyer, *Die Berechnung von Syzygien mit dem verallgemeinerten Weierstrass'schen Divisionssatz*, Diplomarbeit, Universität Hamburg, 1980.
22. David Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. **36** (1890), 473–534.
23. David Cox, John Little, Donal O'Shea, *Using Algebraic Geometry*, Springer-Verlag, New York 1998.
24. Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, Heidelberg, Berlin 1977.
25. Dave Bayer, Mike Stillman, *Computation of Hilbert functions*, J. Symbolic Computation **14** (1992), 31–50.
26. Anna Maria Bigatti, Massimo Caboara, Lorenzo Robbiano, *Computation of Hilbert-Poincaré series*, Applicable Algebra in Engineering, Communication and Computing **2** (1993), 21–33.
27. Patrizia Gianni, Barry Trager, Gail Zacharias, *Gröbner bases and primary decomposition of polynomial ideals*, J. Symb. Comput. **6** (1988), 149–267.
28. Teresa Krick, Alessandro Logar, *An algorithm for the computation of the radical of an ideal in the ring of polynomials*, in: Harold F. Mattson, Teo Mora, T. R. N. Rao, eds., *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-9)*, Lect. Notes Comput. Sci. **539**, pp. 195–205, Springer-Verlag, Berlin, Heidelberg, New York 1991.
29. María Emilia Alonso, Teo Mora, Mario Raimondo, *Local decomposition algorithms*, in: Shojiro Sakata, ed., *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-8)*, Lect. Notes Comput. Sci. **508**, pp. 208–221, Springer-Verlag, Berlin, Heidelberg, New York 1991.
30. David Eisenbud, Craig Huneke, Wolmer V. Vasconcelos, *Direct methods for primary decomposition*, Invent. Math. **110** (1992), 207–235.
31. Ryutaroh Matsumoto, *Computing the radical of an ideal in positive characteristic*, J. Symb. Comput. **32** (2001), 263–271.
32. Elisabetta Fortuna, Patrizia Gianni, Barry Trager, *Computation of the radical of polynomial ideals over fields of arbitrary characteristic*, in: *Proceedings of the 2001 International Symposium on Symbolic and Algebraic Computation*, pp. 116–120, ACM, New York 2001.
33. Gregor Kemper, *The calculation of radical ideals in positive characteristic*, J. Symb. Comput. **34** (2002), 229–238.
34. Santiago Laplagne, *An algorithm for the computation of the radical of an ideal*, in: *ISSAC 2006*, pp. 191–195, ACM, New York 2006.

35. Wolmer V. Vasconcelos, *Computing the integral closure of an affine domain*, Proc. Amer. Math. Soc. **113** (1991), 633–638.
36. Theo de Jong, *An algorithm for computing the integral closure*, J. Symb. Comput. **26** (1998), 273–277.
37. Wolfram Decker, Theo de Jong, Gert-Martin Greuel, Gerhard Pfister, *The normalization: a new algorithm, implementation and comparisons*, in: *Computational methods for representations of groups and algebras (Essen, 1997)*, Progr. Math. **173**, pp. 177–185, Birkhäuser, Basel 1999.
38. Anurag K. Singh, Irena Swanson, *An algorithm for computing the integral closure*, Algebra Number Theory **3** (2009), 587–595.
39. Gert-Martin Greuel, Santiago Laplagne, Frank Seelisch, *Normalization of rings*, J. Symbolic Comput. **45** (2010), 887–901.

Chapter 2

Invariant Theory

For convenience, we will assume throughout this chapter that our base field K is algebraically closed, unless stated otherwise. Many results in this chapter remain true for arbitrary fields K as long as all relevant morphisms and varieties are defined over K .

We need to introduce some basic notation concerning algebraic groups. A **linear algebraic group** is an affine variety G which has a structure as a group such that the multiplication $\mu: G \times G \rightarrow G$ and the inversion $\eta: G \rightarrow G$ are morphisms of affine varieties. Examples of linear algebraic groups will be given below. We say that a linear algebraic group G **acts regularly** on an affine variety X if an action of G on X is given by a morphism $G \times X \rightarrow X$. Then we also call X a **G -variety**. A representation of G is a finite dimensional K -vector space V together with a group homomorphism $G \rightarrow \mathrm{GL}(V)$. A representation V is called **rational** if G acts regularly on V (considered as an affine n -space). In this case we will sometimes call V a **G -module**. A basic result is that every linear algebraic group has a faithful rational representation. For more information on linear algebraic groups we refer the reader to the Appendix of this book or to the books of Borel [1], Humphreys [2], and Springer [3].

2.1 Invariant Rings

Suppose that G is a linear algebraic group acting regularly on an affine variety X . If $f \in K[X]$ and $\sigma \in G$, then we define $\sigma \cdot f \in K[X]$ by

$$(\sigma \cdot f)(x) := f(\sigma^{-1} \cdot x) \quad \text{for all } x \in X.$$

This defines an action of G on the coordinate ring of X . If $f \in K[X]$ and $\sigma \cdot f = f$ for all $\sigma \in G$, then f is called an **invariant**. In general, we are interested in the set

$$K[X]^G := \{f \in K[X] \mid \sigma \cdot f = f \text{ for all } \sigma \in G\}$$

of all G -invariants. The set $K[X]^G$ is a subalgebra of $K[X]$ and we call it the **invariant ring** of G . In this book we will put a special focus on the case where $X = V$ is a representation of G . Then $K[V]$ is isomorphic to the polynomial ring $K[x_1, \dots, x_n]$, where n is the dimension of V as a K -vector space. The polynomial ring $K[V] = \bigoplus_{d=0}^{\infty} K[V]_d$ is graded with respect to the total degree. The G -action on $K[V]$ preserves degree and $K[V]^G \subseteq K[V]$ inherits the grading. This grading of $K[V]$ and $K[V]^G$ is very useful and it makes polynomial invariants of representations easier to deal with than regular invariant functions of affine varieties.

A fundamental problem in invariant theory is to find generators of the invariant ring $K[V]^G$ as a K -algebra. So a basic question is:

Can one always find finitely many generators f_1, \dots, f_r such that $K[V]^G = K[f_1, \dots, f_r]$?

It is clear that the invariant ring $K[V]^G$ is in fact the intersection of the invariant field $K(x_1, \dots, x_n)^G$ with the polynomial ring $K[x_1, \dots, x_n]$. Hilbert asked in his fourteenth problem (see Hilbert [4]) the more general question whether the intersection of any subfield L of $K(x_1, \dots, x_n)$ with $K[x_1, \dots, x_n]$ gives a finitely generated ring. Both questions have a negative answer, since there exists a counterexample due to Nagata [5]. In many cases however, the invariant ring is finitely generated.

Related to finding generators of the invariant ring is the problem of finding degree bounds. For a graded ring $R = \bigoplus_{d=0}^{\infty} R_d$ we define

$$\beta(R) := \inf\{k \mid R \text{ is generated by } \bigoplus_{d=0}^k R_d\} \in \mathbb{N}_0 \cup \{\infty\}. \quad (2.1.1)$$

The problem is to find a good upper bound D such that $\beta(K[V]^G) \leq D$ (see Derksen and Kraft [6] for an overview). Once such an upper bound is known, there is an easy but inefficient method for finding generators of the invariant ring: Using linear algebra, we can find $K[V]_d^G$ using for all $d \leq D$ as follows. If $\sigma_1, \dots, \sigma_r \in G$ generate a subgroup which is Zariski dense in G , then $K[V]_d^G$ is the kernel of the linear map $K[V]_d \rightarrow K[V]^r$ defined by

$$f \mapsto (\sigma_1 \cdot f - f, \sigma_2 \cdot f - f, \dots, \sigma_r \cdot f - f).$$

Alternatively, if G is connected, $K[V]_d^G$ can be computed using the Lie algebra action.

There are also more sophisticated algorithms for computing invariants as we will see later on. Gröbner bases are used for most algorithms related to invariant rings. Most importantly, they will be used to compute generators of invariant rings in the next chapters. Moreover, Gröbner bases can be employed to find the relations between the generators f_1, \dots, f_r of an invariant ring $K[V]^G = K[f_1, \dots, f_r]$ (see Sect. 1.2.2) and to express an arbitrary invariant as a polynomial in the generators.

Example 2.1.1 Suppose the symmetric group S_n act on $V = K^n$ by

$$\sigma \cdot (x_1, x_2, \dots, x_n) = (x_{\sigma(1)}, x_{\sigma(2)}, \dots, x_{\sigma(n)}), \quad \sigma \in S_n.$$

Let us write

$$\varphi(t) := (t + x_1)(t + x_2) \cdots (t + x_n) = t^n + f_1 t^{n-1} + f_2 t^{n-2} + \cdots + f_n$$

with $f_1, \dots, f_n \in K[x_1, \dots, x_n]$ the so-called **elementary symmetric polynomials**. Formulas for f_1, \dots, f_n are given by:

$$\begin{aligned} f_1 &= x_1 + x_2 + \cdots + x_n \\ f_2 &= x_1 x_2 + x_1 x_3 + \cdots + x_1 x_n + x_2 x_3 + \cdots + x_{n-1} x_n \\ &\vdots \quad \vdots \quad \vdots \\ f_r &= \sum_{i_1 < i_2 < \cdots < i_r} x_{i_1} x_{i_2} \cdots x_{i_r} \\ &\vdots \quad \vdots \quad \vdots \\ f_n &= x_1 x_2 \cdots x_n. \end{aligned}$$

The invariant ring of S_n in this representation is generated by the algebraically independent invariants f_1, \dots, f_n (see Theorem 3.10.1). \triangleleft

Example 2.1.2 Suppose that $\text{char}(K) = 0$. The invariant rings of the 2-dimensional special linear group SL_2 over K were studied intensively in the nineteenth century. Gordan proved that invariant rings for SL_2 are always finitely generated (cf. Gordan [7]). Let V_d be the vector space

$$\{a_0 x^d + a_1 x^{d-1} y + \cdots + a_d y^d \mid a_0, a_1, \dots, a_d \in K\}$$

of homogeneous polynomials of degree d in x and y . Such polynomials are often referred to as **binary forms**. The coordinate ring $K[V_d]$ can be identified with $K[a_0, a_1, \dots, a_d]$. We can define an action of SL_2 on V_d by

$$\sigma \cdot g(x, y) := g(\alpha x + \gamma y, \beta x + \delta y), \quad \sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \text{SL}_2.$$

There are many ways of constructing invariants for binary forms. One important invariant of a binary form is the discriminant. Suppose that $g = a_0x^d + a_1x^{d-1}y + \cdots + a_dx^d$ and $h = b_0x^e + b_1x^{e-1}y + \cdots + b_ex^e$ are binary forms of degree d and e respectively. We define the **resultant** of g and h as the $(d+e) \times (d+e)$ -determinant

$$\text{Res}(g, h) = \begin{vmatrix} a_0 & a_1 & \dots & a_d \\ a_0 & a_1 & \dots & a_d \\ \ddots & & \ddots & \\ & a_0 & a_1 & \dots & a_d \\ b_0 & b_1 & \dots & b_e \\ b_0 & b_1 & \dots & b_e \\ \ddots & & \ddots & \\ b_0 & b_1 & \dots & b_e \end{vmatrix}.$$

Since K is algebraically closed, we can write g and h as a product of linear functions

$$g = \prod_{i=1}^d (p_i x + q_i y), \quad h = \prod_{i=1}^e (r_i x + s_i y).$$

Then we find

$$\text{Res}(g, h) = \prod_{i=1}^d \prod_{j=1}^e (p_i s_j - q_i r_j). \quad (2.1.2)$$

From (2.1.2), it is easy to check that $\text{Res}(g, h)$ is an invariant function in $K[V_d \oplus V_e]$ which vanishes if and only if g and h have a common zero in \mathbb{P}^1 . The **discriminant** of g is defined as

$$\Delta(g) = \frac{(-1)^{d(d-1)/2}}{a_0} \text{Res}\left(g, \frac{\partial}{\partial x} g\right).$$

Another formula for $\Delta(g)$ is given by

$$\prod_{i < j} (p_i q_j - q_i p_j)^2. \quad (2.1.3)$$

It is clear from (2.1.3) that the discriminant is an invariant in $K[V_d]$ and it vanishes exactly when g has a multiple zero.

In the literature, discriminants and resultants are usually defined for polynomials in one variable x (see Lang [8, §10]). If g and h are inhomogeneous polynomials, then we just define $\text{Res}(g, h) = \text{Res}(\hat{g}, \hat{h})$ and $\Delta(g) = \Delta(\hat{g})$ where \hat{g} and \hat{h} are

the homogenized polynomials. For the proofs of all formulas (for inhomogeneous polynomials) we refer to Lang [8, Chap. V, § 10].

For any d , let $g_d = a_0x^d + a_1x^{d-1}y + \cdots + a_dy^d$ be the general binary form of degree d . For $d = 2$ it turns out that $K[V_2]^{\text{SL}_2} = K[\Delta(g_2)]$, where $\Delta(g_2) = a_1^2 - 4a_0a_2$ is the well-known discriminant of a quadratic polynomial $g_2 = a_0x^2 + a_1xy + a_2y^2$. Similarly, for $d = 3$ we get $K[V_3]^{\text{SL}_2} = K[\Delta(g_3)]$, where now

$$\Delta(g_3) = a_1^2a_2^2 - 4a_0a_2^3 - 4a_1^3a_3 - 27a_0^2a_3^2 + 18a_0a_1a_2a_3.$$

For binary forms of degree 4, one finds $K[V_4]^{\text{SL}_2} = K[f_2, f_3]$, where

$$f_2 = a_0a_4 - \frac{1}{4}a_1a_3 + \frac{1}{12}a_2^2 \quad \text{and} \quad f_3 = \det \begin{pmatrix} a_0 & a_1/4 & a_2/6 \\ a_1/4 & a_2/6 & a_3/4 \\ a_2/6 & a_3/4 & a_4 \end{pmatrix}.$$

The discriminant $\Delta(g_4)$ can be expressed in f_2 and f_3 , namely $\Delta(g_4) = 2^8(f_2^3 - 27f_3^2)$. For d up to 10, the invariant rings are also explicitly known (see Springer [9], Shioda [10], Dixmier and Lazard [11], and Brouwer and Popoviciu [12, 13]). But they become increasingly complicated. For example, for $d = 10$, the invariant ring requires 106 generators. \triangleleft

Example 2.1.3 Let $V = K^n$. The group $\text{GL}(V)$ acts on $\text{End}(V)$ by conjugation:

$$\sigma \cdot A := \sigma A \sigma^{-1}, \quad \sigma \in \text{GL}(V), A \in \text{End}(V).$$

(A slight variation of) the characteristic polynomial of $A \in \text{End}(V)$ is given by

$$\chi(t) := \det(tI + A) = t^n + g_1t^{n-1} + g_2t^{n-2} + \cdots + g_n.$$

We view g_1, \dots, g_n as functions of A . The coefficients $g_1, g_2, \dots, g_n \in K[\text{End}(V)]$ are clearly invariant under the action of $\text{GL}(V)$. Let us show that $K[\text{End}(V)]^G = K[g_1, \dots, g_n]$. Consider the set of diagonal matrices

$$\mathfrak{t} := \left\{ \begin{pmatrix} x_1 & & & \\ & x_2 & & \\ & & \ddots & \\ & & & x_n \end{pmatrix} \mid x_1, x_2, \dots, x_n \in K \right\}.$$

The group S_n can be viewed as the subgroup of GL_n of permutation matrices. The set \mathfrak{t} is stable under the action of S_n . The restriction of $\chi(t)$ to \mathfrak{t} is S_n -invariant, in fact, it is equal to $\varphi(t)$ as defined in Example 2.1.1. Restricting g_i to \mathfrak{t} yields the elementary symmetric polynomial f_i . It follows that g_1, \dots, g_n are algebraically independent.

If $h \in K[\text{End}(V)]^{\text{GL}(V)}$, then the restriction of h to \mathfrak{t} is S_n -invariant. We can find a polynomial ψ such that the restriction of h to \mathfrak{t} is equal to $\psi(f_1, \dots, f_n)$. Let U be the set of matrices which have distinct eigenvalues. Every matrix with distinct eigenvalues can be conjugated into \mathfrak{t} , so $U \subseteq G \cdot \mathfrak{t}$. The set U is Zariski dense, because it is the complement of the Zariski closed set defined by $\Delta(\chi) = 0$. It follows that $h = \psi(g_1, \dots, g_n)$ because $h - \psi(g_1, \dots, g_n)$ vanishes on $G \cdot \mathfrak{t} \supset U$. The trick in this example (reducing the computation of $K[V]^G$ to the computation of $K[W]^H$ with $W \subseteq V$ and $H \subseteq G$ such that $G \cdot W$ is dense in V) works in a more general setting (see Popov and Vinberg [14]). \triangleleft

Example 2.1.4 This is the counterexample of Nagata to Hilbert's fourteenth problem. Take $K = \mathbb{C}$ and complex numbers $a_{i,j}$ algebraically independent over \mathbb{Q} where $i = 1, 2, 3$ and $j = 1, 2, \dots, 16$. Let $G \subset \text{GL}_{32}$ be the group of all block diagonal matrices

$$\begin{pmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_{16} \end{pmatrix},$$

where

$$A_j = \begin{pmatrix} c_j & c_j b_j \\ 0 & c_j \end{pmatrix}$$

for $j = 1, 2, \dots, 16$. Here the c_j and b_j are arbitrary complex numbers such that $c_1 c_2 \cdots c_{16} = 1$ and $\sum_{j=1}^{16} a_{i,j} b_j = 0$ for $i = 1, 2, 3$. Then $K[x_1, \dots, x_{32}]^G$ is not finitely generated (see Nagata [5]). \triangleleft

Example 2.1.5 Let $\mathbb{G}_a = K$ be the additive group. It acts on K^2 by

$$\sigma \cdot (x, y) \mapsto (x, y + \sigma x).$$

Consider the nonreduced subscheme X of K^2 defined by $x^2 = 0$. \mathbb{G}_a also acts on X and its coordinate ring $R = K[x, y]/(x^2)$. It is easy to see that the invariant ring $R^{\mathbb{G}_a}$ is generated by (the images of) xy^n for all n . For every n , xy^n is not in the $R^{\mathbb{G}_a}$ -ideal generated by x, xy, \dots, xy^{n-1} . This shows that $R^{\mathbb{G}_a}$ is not Noetherian and not finitely generated. Although this example is very simple, it does not quite fit into the general setting, since usually we consider actions on affine varieties which are by definition reduced. \triangleleft

Example 2.1.6 Let K be an algebraically closed field of characteristic 0. Roberts [15] found a (nonlinear) action of the additive group \mathbb{G}_a on K^7 such that the invariant ring is not finitely generated. Daigle and Freudenburg [16] found

the following counterexample in dimension 5. Consider the action of \mathbb{G}_a on K^5 defined by

$$\begin{aligned}\sigma \cdot (a, b, x, y, z) = \\ (a, b, x + \sigma a^2, y + \sigma(ax + b) + \frac{1}{2}\sigma^2 a^3, z + \sigma y + \frac{1}{2}\sigma^2(ax + b) + \frac{1}{6}\sigma^3 a^3).\end{aligned}$$

Then $K[a, b, x, y, z]^{\mathbb{G}_a}$ is not finitely generated. For $n \leq 3$ it is known for any rational action of \mathbb{G}_a on K^n that the invariant ring is finitely generated (see Zariski [17]). \triangleleft

Remark 2.1.7 Suppose that K has characteristic 0 and that V is a representation of the additive group \mathbb{G}_a . Weitzenböck proved that $K[V]^{\mathbb{G}_a}$ is finitely generated (see Weitzenböck [18] and Seshadri [19]). The proof is interesting: First one uses the fact that in characteristic 0 every rational representation V of \mathbb{G}_a extends to a representation of SL_2 (see Kraft [20, Lemma III.3.9]). But there is an isomorphism, attributed to Roberts [21],

$$K[V]^{\mathbb{G}_a} \cong K[U \oplus V]^{\mathrm{SL}_2},$$

with U the natural representation of SL_2 (also see Bryant and Kemper [22]). Since the finite generation of the SL_2 -invariants is known, Weitzenböck's result follows. It is still open whether this results extends to positive characteristic.

Remark 2.1.8 We can generalize the notion of invariants. An element $f \in K[X]$ is called a **semi-invariant** or **relative invariant** if there exists a map $\chi: G \rightarrow K^*$ such that $\sigma \cdot f = \chi(\sigma)f$ for all $\sigma \in G$. Because the action of G is regular, χ is necessarily a morphism of algebraic groups. In this case χ is called the **weight** of f .

2.2 Reductive Groups

As we have remarked in the previous section, the invariant ring $K[V]^G$ is not always finitely generated. A sufficient condition for the invariant ring $K[V]^G$ to be finitely generated is that G is a reductive group. There are different notions of reductivity, namely, linearly reductive, geometrically reductive and group theoretically reductive (also referred to as just reductive). In characteristic zero all notions coincide. In positive characteristic geometric reductivity and reductivity are still the same, but linear reductivity is stronger. Typical examples of reductive groups are GL_n , all semi-simple groups including SL_n , O_n and Sp_n , finite groups and tori. In positive characteristic the only linearly reductive groups are finite groups whose order is not divisible by the prime characteristic, tori, and extensions of tori by finite groups whose order are not divisible by the prime characteristic.

If G is a geometrically reductive group, then the invariant ring is finitely generated. In this book, we will only show this for linearly reductive groups.

2.2.1 Linearly Reductive Groups

Let us first give the definition.

Definition 2.2.1 A linear algebraic group G is called **linearly reductive** if for every rational representation V and every $v \in V^G \setminus \{0\}$, there exists a linear invariant function $f \in (V^*)^G$ such that $f(v) \neq 0$.

See Example 2.2.18 for an example of a linear algebraic group which is not linearly reductive. Linearly reductive groups have a “nice” representation theory. As we will see in Theorem 2.2.5, every representation is fully reducible, i.e., is a direct sum of irreducible representations. Another useful property of linearly reductive groups is that there is a notion of “averaging,” the so-called Reynolds operator.

Definition 2.2.2 Suppose that X is an affine G -variety where G is a linear algebraic group. A **Reynolds operator** is a G -invariant projection, i.e., a linear map $\mathcal{R} : K[X] \rightarrow K[X]^G$ such that

- (a) $\mathcal{R}(f) = f$ for all $f \in K[X]^G$;
- (b) \mathcal{R} is G -invariant, i.e., $\mathcal{R}(\sigma \cdot f) = \mathcal{R}(f)$ for all $f \in K[X]$ and all $\sigma \in G$.

For finite groups, the Reynolds operator is just averaging.

Example 2.2.3 Suppose that G is a finite group such that $\text{char}(K)$ does not divide the group order $|G|$. If X is an affine variety on which G acts, then a Reynolds operator is defined by

$$\mathcal{R}(f) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma \cdot f.$$

It is easy to see that the conditions of Definition 2.2.2 are satisfied. \triangleleft

For infinite groups, averaging over the whole group does not make sense. Over \mathbb{C} for example, the group \mathbb{C}^* is not compact. However, it does contain the compact subgroup S^1 of all complex numbers of norm 1. If $f \in \mathbb{C}[X]$ is any regular function, then we can average it over S^1 (using a Haar measure $d\mu$) and the result $\int_{S^1} \sigma \cdot f \, d\mu$ will be S^1 -invariant. The function $\int_{S^1} \sigma \cdot f \, d\mu$ lies in the finite-dimensional subspace of $K[X]$ spanned by all $\sigma \cdot f$ with $\sigma \in \mathbb{C}^*$, in particular $\int_{S^1} \sigma \cdot f \, d\mu$ is also a regular function on X . It is \mathbb{C}^* -invariant because S^1 is Zariski-dense in \mathbb{C}^* . This shows that $\mathcal{R}(f) = \int_{S^1} \sigma \cdot f \, d\mu$ defines a Reynolds operator. This construction of a Reynolds operator can be generalized to other groups. Over \mathbb{C} , a linearly reductive group G always has a maximal compact subgroup C which is Zariski-dense in G (see Anhang II of Kraft [20] or the references there).

In this book we will use an algebraic construction of the Reynolds operator (see Theorem 2.2.5), and we do not need to restrict ourselves to the complex numbers.

Example 2.2.4 Let $\mathbb{G}_m := K^*$ be the multiplicative group. The coordinate ring of \mathbb{G}_m is isomorphic to $K[t, t^{-1}]$. If X is an affine variety with a regular \mathbb{G}_m -action, then the action $\mu : \mathbb{G}_m \times X \rightarrow X$ induces a ring homomorphism

$$\mu^* : K[X] \rightarrow K[\mathbb{G}_m] \otimes K[X] \cong K[X][t, t^{-1}]$$

with the property

$$\mu^*(f)(\sigma, x) = f(\sigma \cdot x).$$

For $f \in K[X]$ write $\mu^*(f) = \sum_i f_i t^i$ (finite sum) with $f_i \in K[X]$ for all i . Define $\mathcal{R}(f) = f_0$. In case the ground field K is \mathbb{C} , this really means we are averaging $f(\sigma \cdot x)$ over all $\sigma \in S^1$. We will check the properties of Definition 2.2.2. First of all, we have

$$\begin{aligned} \sum_i f_i(\tau^{-1} \cdot x) \sigma^i &= \mu^*(f)(\sigma, \tau^{-1} \cdot x) = \\ f(\sigma \tau^{-1} \cdot x) &= \mu^*(f)(\sigma \tau^{-1}, x) = \sum_i f_i(x) \tau^{-i} \sigma^i \end{aligned}$$

for all $\tau, \sigma \in \mathbb{G}_m$ and $x \in X$. It follows that $(\tau \cdot f)(x) = f_i(\tau^{-1} \cdot x) = \tau^{-i} f_i(x)$ for all i , and in particular $f_0 \in K[X]^{\mathbb{G}_m}$. If $f \in K[X]^{\mathbb{G}_m}$, we get $\mu^*(f)(\sigma, x) = f(\sigma \cdot x) = f(x)$, so $\mathcal{R}(f) = f$. Finally, we have

$$\mu^*(\tau \cdot f)(\sigma, x) = (\tau \cdot f)(\sigma \cdot x) = f(\sigma \tau^{-1} \cdot x) = \sum_i f_i(x) \tau^{-i} \sigma^i,$$

so $\mathcal{R}(\tau \cdot f) = \mathcal{R}(f)$. \triangleleft

There are many other properties which characterize linearly reductive groups. In other books one might find different definitions. One important property is the fact that every representation is a direct sum of irreducible ones. Another characterization of linearly reductive groups is that there always exists a Reynolds operator. The next theorem shows that all these notions are equivalent.

Theorem 2.2.5 *The following properties are equivalent:*

- (a) G is linearly reductive;
- (b) for every rational representation V there exists a unique subrepresentation $W \subseteq V$ such that $V = V^G \oplus W$, and we have $(W^*)^G = 0$;
- (c) for every affine G -variety X there exists a unique Reynolds operator $\mathcal{R} : K[X] \rightarrow K[X]^G$;

- (d) for every rational representation V and subrepresentation $W \subseteq V$ there exists a subrepresentation $Z \subseteq V$ such that $V = W \oplus Z$;
- (e) for every rational representation V there exist irreducible subrepresentations $V_1, V_2, \dots, V_r \subseteq V$ such that $V = V_1 \oplus V_2 \oplus \dots \oplus V_r$.

Proof (a) \Rightarrow (b) From (a) and Definition 2.2.1 it follows that $V^G \subseteq V$ and $(V^*)^G \subseteq V^*$ are dual to each other with respect to the canonical pairing $V \times V^* \rightarrow K$. Take $W = ((V^*)^G)^\perp$, then $V = V^G \oplus W$. If $V = V^G \oplus Z$ is another such decomposition, then G acts trivially on $Z^\perp \subseteq V^*$, because Z^\perp is dual to V^G . So $Z^\perp = (V^*)^G$ and $W = Z$. The representation W^* is isomorphic to the complement of $(V^*)^G$ in V^* . Hence $(W^*)^G$ must be trivial.

(b) \Rightarrow (c) For any finite dimensional and G -stable $V \subseteq K[X]$ we have a decomposition $V = V^G \oplus W$ as in (b). If \mathcal{R} is any Reynolds operator $K[X] \rightarrow K[X]^G$, then the restriction of \mathcal{R} to V^G must be the identity and the restriction of \mathcal{R} to W must be 0 because otherwise we would have a nonzero element in $(W^*)^G$. Uniqueness follows from this. Now we will prove existence. Define $\mathcal{R}_V : V = V^G \oplus W \rightarrow V^G$ as the projection onto V^G along W . If V' is another G -stable, finite dimensional subspace with $V \subseteq V'$, then the restriction of $\mathcal{R}_{V'}$ to W is 0 because otherwise there would exist a nonzero element in $(W^*)^G$. Since $f - \mathcal{R}_V(f) \in W$ for $f \in V$, we obtain $0 = \mathcal{R}_{V'}(f - \mathcal{R}_V(f)) = \mathcal{R}_{V'}(f) - \mathcal{R}_V(f)$. So the restriction of $\mathcal{R}_{V'}$ to V is \mathcal{R}_V . For an arbitrary $f \in K[X]$, we define $\mathcal{R}(f) = \mathcal{R}_V(f)$, where $V \subseteq K[X]$ is a finite dimensional G -stable subspace containing f as in Lemma A.1.8. This is well-defined, because if V' is another subspace with these properties, then $\mathcal{R}_V(f) = \mathcal{R}_{V+V'}(f) = \mathcal{R}_{V'}(f)$. The properties in Definition 2.2.2 are easily checked.

(c) \Rightarrow (a) We have $V \subseteq K[V^*]$ as the set of linear functions on V^* . Let \mathcal{R}_V be the restriction of the Reynolds operator $\mathcal{R} : K[V^*] \rightarrow K[V^*]^G$ to V . Suppose that $v \in V^G \setminus \{0\}$. Choose some projection $p : K[V^*]^G \rightarrow K$ such that $p(v) \neq 0$. Let f be the composition $p \circ \mathcal{R}_V : V \rightarrow K$. Clearly $f \in (V^*)^G$ and $f(v) = p(\mathcal{R}_V(v)) = p(v) \neq 0$.

(a) \Rightarrow (d) First assume that W is irreducible. The dual space of $\text{Hom}(W, V)$ is $\text{Hom}(V, W)$. In fact, the pairing is

$$(A, B) \in \text{Hom}(W, V) \times \text{Hom}(V, W) \mapsto \text{Tr}(AB) \in K,$$

where $\text{Tr}(AB)$ is the trace of $AB \in \text{End}(V)$. Let $A \in \text{Hom}(W, V)^G$ be the inclusion. By (a) there exists a $B \in \text{Hom}(V, W)^G$ such that $\text{Tr}(BA) \neq 0$. Because W is irreducible and $BA \in \text{End}(W, W)^G$, BA must be a nonzero multiple of the identity by Schur's Lemma (see Fulton and Harris [23, Schur's Lemma 1.7], the proof there works for arbitrary groups G and arbitrary finite dimensional irreducible representations). We can write $V = W \oplus Z$ where Z is the kernel of B . If W is not irreducible, then take an irreducible subrepresentation $W' \subseteq W$. Then $V = W' \oplus Z'$ for some G -stable complement Z' and $W = W' \oplus W \cap Z'$. By induction hypothesis $W \cap Z'$ has a G -stable complement Z in Z' and we get $V = W \oplus Z$.

(d) \Rightarrow (e), (e) \Rightarrow (a) are left to the reader. \square

Remark 2.2.6 It is worth noting the construction of the Reynolds operator in the previous proof. Suppose that $f \in K[X]$. Choose a finite dimensional G -stable vector space V containing f . This always can be done, for example take for V the vector space spanned by all $\sigma \cdot f$ with $\sigma \in G$ (see Lemma A.1.8). Now $V^G \subseteq V$ has a unique G -stable complement W , and $\mathcal{R}(f)$ is the projection of f onto V^G . From the proof of Theorem 2.2.5 it follows that this is well-defined. \triangleleft

Corollary 2.2.7 If G is linearly reductive and X an affine G -variety, then the Reynolds operator $K[X] \rightarrow K[X]^G$ has the following properties:

- (a) If $W \subseteq K[X]$ is a G -stable subspace, then $\mathcal{R}(W) = W^G$;
- (b) \mathcal{R} is a $K[X]^G$ -module homomorphism, i.e., $\mathcal{R}(fh) = f\mathcal{R}(h)$ iff $f \in K[X]^G$ and $h \in K[X]$.

Proof

- (a) This is clear from Remark 2.2.6.
- (b) Choose a G -stable finite dimensional subspace $V \subseteq K[X]$ with $h \in V$. Then $V = V^G \oplus W$ for some G -stable complement W and $\mathcal{R}(h)$ is the projection of h onto V^G . Notice that $(fW)^G = 0$ because otherwise $(W^*)^G \neq 0$ which contradicts Theorem 2.2.5(b). We have $fV = fV^G \oplus fW$ and $fV^G = (fV)^G$. It follows that $\mathcal{R}(fh)$ is the projection of fh onto fV^G which is $f\mathcal{R}(h)$. \square

Corollary 2.2.8 If G is linearly reductive, V, W are rational representations, and $A : V \rightarrow W$ is a surjective G -equivariant linear map, then $A(V^G) = W^G$.

Proof Let Z be the kernel of A , then there exists a G -stable complement W' such that $V \cong Z \oplus W'$. The restriction of A to W' gives an isomorphism $W' \cong W$ of representations of G , in particular $(W')^G$ maps onto W^G . \square

This is a very useful fact. The following corollary shows that for linearly reductive groups, the computation of invariant rings $K[X]^G$ can always be reduced to the case of a rational representation.

Corollary 2.2.9 Suppose that X is an affine G -variety. There exists a G -equivariant embedding $i : X \hookrightarrow V$ where V is a rational representation of G . The surjective G -equivariant ring homomorphism $i^* : K[V] \rightarrow K[X]$ has the property that $i^*(K[V]^G) = K[X]^G$.

Proof The first statement will be proved in Lemma A.1.9. For any finite dimensional G -stable subspace $W \subseteq K[X]$ there exists a G -stable finite dimensional subspace $Z \subseteq K[V]$ such that i^* maps Z onto W . We have $i^*(Z^G) = W^G$ by Corollary 2.2.8. It follows that $i^*(K[V]^G) = K[X]^G$, since $K[X]^G$ is the union of such W . \square

Now we come to the most important theorem in invariant theory, namely Hilbert's finiteness theorem. It had already been proven by Gordan that $K[V]^{\mathrm{SL}_2}$ is finitely generated (see Gordan [7]). The methods there do not generalize to other groups. It was in 1890 that Hilbert [24] surprised everyone by giving a proof which works for all GL_n , SL_n , in fact, all classical groups. We will see that the proof actually works whenever there is a Reynolds operator, i.e., whenever we are

dealing with a linearly reductive group. The methods Hilbert used were abstract, nonconstructive, and completely new in those days. The proof was criticized for not being constructive and it led Gordan, the “king of invariant theory” at that time, to make his famous exclamation “Das ist Theologie und nicht Mathematik.”¹ Hilbert wrote a paper in 1893 (see Hilbert [25]), in which he gave a constructive proof. The abstract methods of both papers contain many important basics of modern commutative algebra, for example Hilbert’s Basissatz, the Nullstellensatz, the Noether normalization lemma, and Hilbert’s syzygy theorem.

We give the first short and elegant, nonconstructive proof of Hilbert’s finiteness theorem.

Theorem 2.2.10 *If G is a linearly reductive group and V is a rational representation, then $K[V]^G$ is finitely generated over K .*

Proof Let I be the ideal in $K[V]$ generated by all homogeneous invariants of positive degree. Because $K[V]$ is Noetherian, there exist finitely many homogeneous invariants $f_1, \dots, f_r \in K[V]^G$ such $I = (f_1, \dots, f_r)$. We will prove that $K[V]^G = K[f_1, \dots, f_r]$. Suppose $h \in K[V]^G$ homogeneous of degree d . We will prove that $h \in K[f_1, \dots, f_r]$ using induction on d . If $d = 0$, then $h \in K \subseteq K[f_1, \dots, f_r]$. If $d > 0$, we can write

$$h = \sum_{i=1}^r g_i f_i \quad (2.2.1)$$

with $g_i \in K[V]$. Without loss of generality, we may assume that g_i is homogeneous of degree $d - \deg(f_i) < d$. The Reynolds operator $\mathcal{R} : K[V] \rightarrow K[V]^G$ maps $K[V]_d$ onto $K[V]^G_d$ (see Corollary 2.2.7(a)). Applying the Reynolds operator to (2.2.1) and using Corollary 2.2.7(b), we obtain

$$h = \mathcal{R}(h) = \sum_{i=1}^r \mathcal{R}(g_i f_i) = \sum_{i=1}^r \mathcal{R}(g_i) f_i.$$

Because $\mathcal{R}(g_i) \in K[V]^G$ is homogeneous of degree $< d$, we have by induction that $\mathcal{R}(g_i) \in K[f_1, \dots, f_r]$ for all i . We conclude that $h \in K[f_1, \dots, f_r]$. \square

Because of its significance in the above proof, we propose to call the ideal $I = (K[V]^G) K[V]$ in $K[V]$ generated by all homogeneous invariants of positive degree the *Hilbert ideal*.

Corollary 2.2.11 *If G is a linearly reductive group acting regularly on an affine variety X , then $K[X]^G$ is finitely generated.*

Proof Combine Theorem 2.2.10 with Corollary 2.2.9. \square

¹“This is theology and not mathematics.”

Corollary 2.2.12 *Let G be a linearly reductive algebraic group and let $[G, G]$ be its commutator subgroup. Let X be an affine G -variety. Then $K[X]^{[G, G]}$ is spanned by G -semi-invariants.*

Proof If $f \in K[X]^{[G, G]}$, then there exists a finite dimensional G -stable vector space $W \subseteq K[X]$ with $f \in W$. By replacing W with $W^{[G, G]}$, we may assume that $[G, G]$ acts trivially on W . We can write $W = W_1 \oplus W_2 \oplus \cdots \oplus W_r$, with W_i an irreducible representation of G (and of $G/[G, G]$). Since $G/[G, G]$ is abelian, all its irreducible representations are 1-dimensional, say $W_i = K \cdot f_i$. Clearly, every f_i is a G -semi-invariant and f is a linear combination of the f_i . \square

2.2.2 Other Notions of Reductivity

For a linear algebraic group G , the **unipotent radical** $R_u(G)$ is defined as the largest connected normal unipotent subgroup of G . The group G is called **reductive** or **group theoretically reductive** if $R_u(G)$ is trivial (see Definition A.3.6). There are many examples of reductive groups, for example GL_n , SL_n , O_n , SO_n , Sp_n , finite groups, tori and semisimple groups. For details on reductive groups we refer to Sect. A.3 in this book or to one of the books on linear algebraic groups (see Borel [1], Humphreys [2], Springer [3]).

For the proof of the following theorem we refer to Nagata and Miyata [26].

Theorem 2.2.13 *If $\mathrm{char}(K) = 0$, then a linear algebraic group is reductive if and only if it is linearly reductive.*

Definition 2.2.14 A linear algebraic group is called **geometrically reductive** if for every rational representation V and every $v \in V^G \setminus \{0\}$, there exists a homogeneous $f \in K[V]^G$ of degree > 0 such that $f(v) \neq 0$.

Clearly, linear reductivity implies geometric reductivity. The converse is not true, though. For example a nontrivial finite p -group in characteristic p is geometrically reductive, but not linearly reductive. We state the following useful result without proof.

Theorem 2.2.15 *For any characteristic of K , a group is geometrically reductive if and only if it is reductive.*

Proof In Nagata and Miyata [26] it was proven that geometrically reductive groups are reductive. Haboush [27] proved the converse, which had been conjectured by Mumford. \square

Hilbert's finiteness theorem has also been proven for geometrically reductive groups (see Nagata [28]) using some new ideas.

Theorem 2.2.16 *If X is an affine G -variety and G is geometrically reductive, then $K[X]^G$ is finitely generated.*

Franjou and van der Kallen [29] generalized this result to the case where the ground field K is replaced by an arbitrary Noetherian ring. (Of course, they need to work with group schemes and make some adjustments to the definitions.) The converse of Theorem 2.2.16 is also true. Popov [30] proved the following.

Theorem 2.2.17 *If $K[X]^G$ is finitely generated for every affine G -variety X , then G must be reductive.*

Of course even for nonreductive groups G there exist affine G -varieties X such that $K[X]^G$ is finitely generated. To date, no results or algorithms are known that determine whether a given invariant ring $K[X]^G$ is finitely generated. It is also unknown for which linear algebraic groups G the invariant ring $K[V]^G$ is finitely generated for all rational representations V . For example, if $\text{char}(K) = 0$, then Remark 2.1.7 shows that this is true for the additive group \mathbb{G}_a , which, according to the following example, is not reductive. It follows that it also holds for every linear algebraic group whose unipotent radical is isomorphic to \mathbb{G}_a .

Example 2.2.18 Let $\mathbb{G}_a = K$ be the additive group. We define a regular action on K^2 by

$$\sigma \cdot (x, y) = (x + \sigma y, y), \quad \sigma \in \mathbb{G}_a, (x, y) \in K^2.$$

The invariant ring $K[x, y]^{\mathbb{G}_a}$ is equal to $K[y]$. If $v \in K \times \{0\} = (K^2)^{\mathbb{G}_a}$, then every invariant vanishes on v . The group \mathbb{G}_a is therefore not geometrically reductive. \triangleleft

In positive characteristic there exist only few linearly reductive groups, as the following result shows.

Theorem 2.2.19 (Nagata [31], see also Kohls [32]) *Suppose that $\text{char}(K) = p > 0$. A linear algebraic group is linearly reductive if and only if the connected component G° of the identity element is a torus and $|G/G^\circ|$ is not divisible by p .*

Example 2.2.20 Assume that K is a field of characteristic $p > 0$ and let C_p be the cyclic group of order p , generated by σ . As in the previous example, we define an action on K^2 by

$$\sigma \cdot (x, y) = (x + y, y), \quad (x, y) \in K^2.$$

The subspace $K \times \{0\} \subseteq K^2$ does not have a C_p -stable complement. So C_p is not linearly reductive whenever $p = \text{char}(K)$. However, C_p is geometrically reductive. For example, if v is the invariant point $(1, 0)$, then $f(v) \neq 0$ where f is the homogeneous invariant polynomial $f = \prod_{i \in \mathbb{F}_p} (x - iy) = x^p - xy^{p-1}$. \triangleleft

2.3 Categorical Quotients

In this section we give a geometric interpretation of invariant rings.

If G is reductive and X is a G -variety, then $K[X]^G$ is finitely generated and we can define $X//G$ as the affine variety corresponding to the ring $K[X]^G$. The map $\pi: X \rightarrow X//G$ is the morphism corresponding to the inclusion $K[X]^G \subseteq K[X]$, and it is called the **categorical quotient**. Since G is reductive, this is, in fact, a categorical quotient in the sense of geometric invariant theory (see Mumford et al. [33, Definition 0.5 and Theorem 1.1]). Explicitly, if $K[X]^G = K[f_1, \dots, f_m]$, then $X//G \subseteq K^m$ can be defined by the ideal of algebraic relations between the f_i , and $\pi: X \rightarrow X//G$ is given by evaluating the f_i at a point of X . We will study the geometric properties of categorical quotients. We first remark that the categorical quotient is constant on orbits does not always separate all the orbits, as the following example shows.

Example 2.3.1 Let $\mathbb{G}_m = K^*$ be the multiplicative group acting diagonally on $V = K^2$ by

$$\sigma \cdot (x, y) = (\sigma x, \sigma y), \quad \sigma \in \mathbb{G}_m, (x, y) \in K^2.$$

An invariant is continuous and constant on orbits. Since all orbits have the origin contained in their closure, all invariants must be constant, so $K[V]^{\mathbb{G}_m} = K$ and $V//\mathbb{G}_m$ is just a point. On the other hand, there are infinitely many \mathbb{G}_m -orbits, so $\pi: V \rightarrow V//\mathbb{G}_m$ does not separate the orbits. \triangleleft

A few general remarks about the correspondence between ideals and their zeroes are useful here. If $I \subseteq K[X]^G$ is an ideal and $Y = \mathcal{V}(I)$ is its zero set in $X//G$, then the zero set of the ideal $K[X]I \subseteq K[X]$ corresponds to the inverse image $\pi^{-1}(Y)$ (but $K[X]I$ does not have to be a radical ideal even if I is one). On the other hand if $I \subseteq K[X]$ is an ideal, and $Y = \mathcal{V}(I) \subseteq X$ is its zero set, then $I \cap K[X]^G = I^G$ is equal to $I(\pi(Y))$, the vanishing ideal of $\pi(Y)$. For the proofs of the following lemmas we will assume that G is linearly reductive. The results, however, remain true if G is geometrically reductive (see Mumford et al. [33] or Newstead [34]).

Lemma 2.3.2 *If X is a G -variety, then the quotient map $\pi: X \rightarrow X//G$ is surjective.*

Proof Let $\mathfrak{m}_x \subseteq K[X]^G$ be the maximal ideal corresponding to a point $x \in X//G$. If $\pi^{-1}(x) = \emptyset$, then $1 \in \mathfrak{m}_x K[X]$, so we can write $1 = \sum_{i=1}^r a_i f_i$ with $f_i \in \mathfrak{m}_x$ and $a_i \in K[X]$ for all i . Applying the Reynolds operator yields $1 = \mathcal{R}(1) = \sum_{i=1}^r \mathcal{R}(a_i) f_i$, so $1 \in \mathfrak{m}_x$, a contradiction. Therefore $\pi^{-1}(x) \neq \emptyset$. \square

Lemma 2.3.3 *If $Y_1, Y_2 \subseteq X$ are G -stable, then $\overline{\pi(Y_1)} \cap \overline{\pi(Y_2)} = \overline{\pi(Y_1 \cap Y_2)}$.*

Proof Let $I_1 = I(Y_1)$ and $I_2 = I(Y_2)$ be the vanishing ideals of Y_1 and Y_2 , respectively. Then $(I_1 + I_2)^G = \mathcal{R}(I_1 + I_2) = \mathcal{R}(I_1) + \mathcal{R}(I_2) = I_1^G + I_2^G$. \square

Corollary 2.3.4 *If $Y \subseteq X$ is G -stable and closed, then $\pi(Y) \subseteq X//G$ is closed.*

Proof Assume there exists $x \in \overline{\pi(Y)} \setminus \pi(Y)$. Then $\pi^{-1}(x)$ and Y are G -stable and closed, $\pi^{-1}(x) \cap Y = \emptyset$, so $x \in \pi(\pi^{-1}(x)) \cap \overline{\pi(Y)} = \emptyset$ by Lemma 2.3.2 and Lemma 2.3.3. \square

Corollary 2.3.5 *The Zariski topology on $X//G$ is equal to the quotient topology induced by $\pi: X \rightarrow X//G$.*

Proof A subset $Y \subseteq X//G$ is closed if and only $\pi^{-1}(Y)$ is closed. \square

Theorem 2.3.6 *For every $x \in X//G$, the fiber $\pi^{-1}(x)$ contains exactly one closed orbit. This orbit is contained in the Zariski closure of all (other) orbits in $\pi^{-1}(x)$.*

Proof The fiber $\pi^{-1}(x)$ is closed and G -stable and (by Lemma 2.3.2) nonempty. By the Noether property there exists $y \in \pi^{-1}(x)$ such that the orbit closure $\overline{G \cdot y}$ is minimal. Since the orbit $G \cdot y$ is the image of the morphism $G \rightarrow X$, $g \mapsto g \cdot y$, it follows by a theorem of Chevalley (see Hartshorne [35, Exercise II.3.19]) that there is a nonempty subset $U \subseteq G \cdot y$ that is open in $\overline{G \cdot y}$. Replacing U by the union of the images $g \cdot U$ ($g \in G$), we see that $G \cdot y$ itself is open in $\overline{G \cdot y}$. If $G \cdot y \subsetneq \overline{G \cdot y}$, then picking $z \in \overline{G \cdot y} \setminus G \cdot y$ would contradict the minimality of $\overline{G \cdot y}$ since $\overline{G \cdot z} \subseteq \overline{G \cdot y} \setminus G \cdot y$. So we conclude that $G \cdot y$ is closed. The existence of a closed orbit in $\pi^{-1}(x)$ actually holds without the reductivity assumption.

If $z \in \pi^{-1}(x)$, then by Lemma 2.3.3 and Corollary 2.3.4 we have $\{x\} = \pi(\overline{G \cdot z}) \cap \pi(G \cdot y) = \pi(\overline{G \cdot z}) \cap G \cdot y$. So $\overline{G \cdot z} \cap G \cdot y \neq \emptyset$, which means that the orbit $G \cdot y$ lies in the closure of $G \cdot z$. This also shows the uniqueness of $G \cdot y$. \square

Example 2.3.7 Let $\mathbb{G}_m = K^*$ be the multiplicative group acting on $V = K^2$ by

$$\sigma \cdot (x, y) = (\sigma x, \sigma^{-1}y), \quad \sigma \in \mathbb{G}_m, (x, y) \in K^2.$$

It is easy to see that $K[V]^{\mathbb{G}_m} = K[xy]$, so $V//\mathbb{G}_m \cong K$. The quotient map $\pi: V \rightarrow V//\mathbb{G}_m \cong K$ is given by

$$(x, y) \mapsto xy.$$

For $a \neq 0$, the fiber $\pi^{-1}(a)$ is just a single closed orbit. The zero fiber $\pi^{-1}(0)$ is given by $xy = 0$ and consists of three orbits, namely

$$\{(0, 0)\}, \quad \{(x, 0) \mid x \neq 0\}, \quad \{(0, y) \mid y \neq 0\}.$$

The only closed orbit is $\{(0, 0)\}$, and it lies in the closure of the other two orbits. \triangleleft

Corollary 2.3.8 *For two points $x, y \in X$ the equivalence*

$$\pi(x) = \pi(y) \iff \overline{G \cdot x} \cap \overline{G \cdot y} \neq \emptyset$$

holds.

Proof If the orbit closures intersect, then $\pi(x) = \pi(y)$ since π is continuous and constant on orbits. The converse follows from Theorem 2.3.6. \square

Corollary 2.3.8 gives a criterion when orbits can be separated by invariants. It can be paraphrased by saying that the obvious topological obstacle to separate orbits is in fact the only one. Of course, this holds under the hypothesis, made in this section, that G is reductive. Example 2.2.18 shows that the corollary does not extend to nonreductive groups. In that example, every point $(x, 0)$ with $x \in K$ forms a closed orbit with just one point.

The above theorem and its corollary emphasize the importance of orbit closures and containment relations between them. Appendix B in this book deals with two algorithms that determine whether one orbit is contained in the closure of another.

We call $\pi : X \rightarrow X//G$ a **geometric quotient** if there is a 1–1 correspondence between G -orbits in X and points in $X//G$. If G is a finite group, then all G -orbits are closed. It follows that every fiber of $\pi : X \dashrightarrow X//G$ is a single orbit by Theorem 2.3.6. So $X//G$ is a geometric quotient in this case.

As we have seen in Examples 2.3.1 and 2.3.7, a categorical quotient is not always a geometric quotient. Suppose that $\pi : X \rightarrow X//G$ is a geometric quotient and X is a connected G -variety. We have

$$\dim \pi^{-1}(\pi(x)) = \dim G \cdot x$$

for all $x \in X$, since the fibers are the orbits. But

$$\dim G \cdot x = \dim G - \dim G_x \tag{2.3.1}$$

where G_x is the stabilizer of x . Furthermore

$$\dim G_x = \dim \gamma^{-1}(\gamma(e, x))$$

where

$$Z = \{(g, x) \in G \times X \mid g \cdot x = x\}$$

and $\gamma : Z \rightarrow X$ is the projection onto X . Now $\dim G_x$ and $\dim G \cdot x$ depend semicontinuously on x (see Hartshorne [35, Exercise II.3.22]). This means that $\{x \mid \dim G \cdot x \leq C\}$ is Zariski *closed* for all constants C . On the other hand, $\dim \pi^{-1}(\pi(x))$ also depends semicontinuously on x , but in the other direction. This means $\dim \pi^{-1}(\pi(x)) \leq C$ is a Zariski *open* subset of X for all C . We conclude that $\dim \pi^{-1}(\pi(x)) = \dim G \cdot x$ must be a constant function on all connected components of X . We have shown that if X admits a geometric quotient and X is connected, then all the orbits must have the same dimension. This is also sufficient. If all orbits have the same dimension, then no orbit lies in the closure of any other orbit, and by Theorem 2.3.6, π separates the orbits.

In Example 2.3.1, if we remove the origin from V , we obtain a \mathbb{G}_m -action on an open subset which has a geometric quotient. This is a general phenomenon. In fact, a theorem by Rosenlicht [36] states that X always has a dense, open, G -stable subset U such that $U//G$ is a geometric quotient. This holds even if G is not geometric. A constructive version of this result can be found in Kemper [37].

Although not all categorical quotients are geometric, they still have many nice properties. Quotients with certain nice geometric properties are sometimes called “**good quotients**.” We will not give an precise definition here. Nice quotients are often needed for finding so-called moduli spaces, spaces which parametrize certain geometric objects (all nonsingular curves of a given genus, for example). Typically, one needs a “good” or geometric quotient of a projective variety with a G -action. For example, if V is a rational representation of G , one can ask for a “good” quotient for the projective space $\mathbb{P}(V)$. Since the coordinate ring of $V//G$ is homogeneous, we can take the candidate $\mathbb{P}(V//G)$ (the projective variety corresponding to the graded ring $K[V]^G$). Now $\pi : V \rightarrow V//G$ induces a map

$$\tilde{\pi} : \mathbb{P}(V) \rightsquigarrow \mathbb{P}(V//G)$$

which is not well-defined, because for some $v \in V \setminus \{0\}$ we could have $\pi(v) = 0$. But if we exclude these points, we get a well defined “good” quotient

$$\tilde{\pi} : \mathbb{P}(V \setminus \pi^{-1}(0)) \rightarrow \mathbb{P}(V//G).$$

The elements in $V \setminus \pi^{-1}(0)$ are called **semi-stable**. For more details on the subject of geometric invariant theory we refer to Mumford et al. [33] and Newstead [34].

2.4 Separating Invariants

The categorical quotient can be formed if generating invariants for $K[X]^G$ are known. Such a generating set can be large, hard to compute, or even infinite (in the case of nonreductive groups). It is an interesting question whether a smaller set of invariants might also suffice to achieve the same separation properties. In this subsection, X is an affine variety over a field $K = \bar{K}$, and G is any group of automorphisms of the coordinate ring $K[X]$. We do not assume G to be reductive, or even an algebraic group.

Definition 2.4.1 A subset $S \subseteq K[X]^G$ is said to be **separating** if for any two points $x, y \in X$ we have: If there exists an invariant $f \in K[X]^G$ with $f(x) \neq f(y)$, then there exists an element $g \in S$ with $g(x) \neq g(y)$.

Clearly $S \subseteq K[X]^G$ is separating if and only if the subalgebra $K[S] \subseteq K[X]^G$ generated by S is separating. It follows that a subset $S \subseteq K[V]^G$ that generates $K[V]^G$ as a K -algebra is always separating. So the concept of separating invariants is a weakening of the concept of generating invariants. If G is a reductive group

acting regularly on X , then the above definition amounts to saying that for two points $x, y \in X$ with distinct closed G -orbits there exists $g \in S$ with $g(x) \neq g(y)$. Of course Definition 2.4.1 can be generalized to a situation where instead of $K[V]^G$ one considers any set of functions from a set to another set (see Kemper [38]).

Example 2.4.2 Consider the finite group

$$G = \langle \begin{pmatrix} \omega & 0 \\ 0 & \omega \end{pmatrix} \rangle \leq \mathrm{GL}_2(K)$$

with ω a primitive third root of unity. The invariant ring $K[x, y]^G$ is minimally generated by

$$f_1 = x^3, \quad f_2 = x^2y, \quad f_3 = xy^2, \quad f_4 = y^3.$$

We claim that $S := \{f_1, f_2, f_4\}$ is a separating subset. Indeed, we have $f_3 = f_2^2/f_1$, so for $(\xi, \eta) \in K^2$ we obtain

$$f_3(\xi, \eta) = \begin{cases} f_2(\xi, \eta)^2/f_1(\xi, \eta) & \text{if } f_1(\xi, \eta) \neq 0 \\ 0 & \text{if } f_1(\xi, \eta) = 0 \end{cases}.$$

This means that the value of f_3 at any point (ξ, η) is determined by the values of f_1 and f_2 . Therefore S is separating.

Having seen this, one might expect that for all $a, b \in K$ with $(a, b) \neq (0, 0)$ the set $S' := \{f_1, af_2 + bf_3, f_4\}$ should also be separating. But, surprisingly, this is only the case if $ab = 0$. Indeed, if $ab \neq 0$, then for the points

$$v := (b(\omega - 1), a(1 - \omega^2)) \quad \text{and} \quad w := (b(\omega^2 - \omega), a(1 - \omega^2))$$

it is easily verified that $f(v) = f(w)$ for every $f \in S'$, but $G \cdot v \neq G \cdot w$.

The example generalizes to the case where ω is a primitive n th root of unity: then $x^n, x^{n-1}y$ and y^n form a separating subset. \triangleleft

How far away is a separating subalgebra from the invariant ring? A first observation is that if G is reductive, then the map $X//G \rightarrow Y$ of affine varieties induced from the embedding $A \subseteq K[X]^G$ of a separating subalgebra is dominant and injective. If X is irreducible, this implies that the extension $\mathrm{Quot}(A) = K(Y) \subseteq K(X//G) = \mathrm{Quot}(K[X]^G)$ of function fields is finite and purely inseparable (see Humphreys [2, Theorem 4.6]). In particular, if $\mathrm{char}(K) = 0$, the fields of fractions of A and $K[X]^G$ coincide.

We now concentrate on the case that G is reductive and acts by a rational representation, and the separating subalgebra is graded.

Proposition 2.4.3 *Let G be a reductive group and V a rational representation. Moreover, let $A \subseteq K[V]^G$ be a graded, separating subalgebra. Then $K[V]^G$ is integral over A .*

Proof Consider the ideal $A_+K[V]$ in $K[V]$ generated by all homogeneous elements of positive degree in A . Take $v \in \mathcal{V}(A_+K[V])$. Then for every $f \in A$ we have

$$f(v) - f(0) = (f - f(0))(v) = 0.$$

Since A is separating, this implies $f(v) = 0$ for all $f \in K[V]_+^G$, so $v \in \mathcal{V}(K[V]_+^G \cdot K[V])$. (The latter algebraic set is the so-called nullcone, see Definition 2.5.1.) The Nullstellensatz now yields

$$K[V]_+^G \subseteq \sqrt{A_+K[V]} \cap K[V]^G. \quad (2.4.1)$$

Let $I = A_+K[V]^G$ be the ideal in $K[V]^G$ generated by A_+ . Then $IK[V] = A_+K[V]$, and by Newstead [34, Lemma 3.4.2] we have $\sqrt{IK[V]} \cap K[V]^G \subseteq \sqrt{I}$. (This uses the reductivity of G and holds for any ideal in $K[V]^G$.) Using (2.4.1), we obtain

$$K[V]_+^G \subseteq \sqrt{A_+K[V]^G}.$$

Therefore $K[V]^G / (A_+K[V]^G)$ has Krull dimension 0, and thus

$$\dim_K(K[V]^G / (A_+K[V]^G)) < \infty.$$

By the graded version of Nakayama's lemma (see Lemma 3.7.1), this implies that $K[V]^G$ is finitely generated as a module over A , so $K[V]^G$ is integral over A , as claimed. \square

This is readily applicable if $\text{char}(K) = 0$. Indeed, in this case it follows that $K[V]^G$ is the normalization of A , since the fields of fractions coincide and $K[V]^G$ is normal by the following result.

Proposition 2.4.4 *Let R be a normal domain and G a group acting on R by automorphisms. Then the invariant ring R^G is also a normal domain.*

Proof It is clear that R^G is an integral domain. G also acts on $F := \text{Quot}(R)$. Let $f \in \text{Quot}(R^G)$ be integral over R^G . Then $f \in F^G$, and f is integral over R . By the hypothesis f lies in R , hence $f \in R \cap F^G = R^G$. This shows that R^G is indeed normal. \square

It seems that the case of positive characteristic poses more problems, since a purely inseparable field extension is involved. However, we have the following remarkable result. It goes back to van der Kallen [39], with an optimized proof in Franjou and van der Kallen [29, Proposition 22].

Proposition 2.4.5 *Let $A \subseteq B$ be an integral extension of finitely generated algebras over an algebraically closed field characteristic $p > 0$. If the induced map of affine varieties is injective, then there exists a nonnegative integer m such that $b^{p^m} \in A$ for every $b \in B$.*

It is clear that if the conclusion of Proposition 2.4.5 holds, then the extension is integral and the induced map is injective.

Let $A \subseteq K[V]$ be a subalgebra of a polynomial ring of positive characteristic p . Then we call the algebra

$$\hat{A} := \{f \in K[V] \mid f^{p^r} \in A \text{ for some } r \in \mathbb{N}\} \subseteq K[V]$$

the **purely inseparable closure** of A in $K[V]$. If the reader prefers, he or she may substitute our hat-notation by something that expresses the dependence on the inclusion $A \subseteq K[V]$. One nice thing about the purely inseparable closure is that there is an algorithm to compute it (see Sect. 4.9.2).

Theorem 2.4.6 *Let G be a reductive group over K and V a rational representation. Moreover, let $A \subseteq K[V]^G$ be a graded, separating subalgebra.*

- (a) *If $\text{char}(K) = 0$, then $K[V]^G = \tilde{A}$ (the normalization of A).*
- (b) *If $\text{char}(K) > 0$, then $K[V]^G = \hat{A}$.*

Proof The first assertion was already deduced before Proposition 2.4.4. So assume $p = \text{char}(K) > 0$. Since $K[V]^G$ is finitely generated and integral over A (see Proposition 2.4.3), it is also integral over a finitely generated subalgebra of A . So $K[V]^G$ is a Noetherian module over that algebra, and it follows that the submodule A is finitely generated. We have already seen that the map of varieties induced from the embedding $A \subseteq K[V]^G$ is injective. So Propositions 2.4.3 and 2.4.5 yield $K[V]^G \subseteq \hat{A}$. On the other hand, if $f \in A$, then f is a polynomial with $f^q \in A \subseteq K[V]^G$ for a p -power q . So for $\sigma \in G$ we have

$$(\sigma \cdot f - f)^q = \sigma \cdot f^q - f^q = 0,$$

hence $f \in K[V]^G$. □

In positive characteristic, the conclusion of Theorem 2.4.6 implies that A is separating. The following example shows that this is not the case in characteristic 0.

Example 2.4.7 Consider the group $G \cong C_2 \times C_2$ generated by the diagonal matrices

$$\begin{pmatrix} -1 & & & \\ & -1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & & & \\ & 1 & & \\ & & -1 & \\ & & & -1 \end{pmatrix}$$

where $\text{char}(K) = 0$. G acts on the polynomial ring $R := K[x_1, y_1, x_2, y_2]$, and R^G is clearly generated by the invariants

$$f_i := x_i^2, \quad g_i := y_i^2, \quad \text{and} \quad h_i := x_i y_i \quad (i = 1, 2).$$

Consider the subalgebra $A := K[f_1, g_1, f_2, g_2, h]$ with $h := h_1 + h_2$. We claim $\tilde{A} = R^G$. Indeed, we have

$$h_1 = \frac{f_1 g_1 - f_2 g_2 + h^2}{2h} \quad \text{and} \quad h_2 = \frac{f_2 g_2 - f_1 g_1 + h^2}{2h},$$

so the h_i lie in $\text{Quot}(A)$. But they are also integral over A , since $h_i^2 - f_i g_i = 0$. Thus $h_1, h_2 \in \tilde{A}$, which proves our claim. Now consider the points

$$v = (1, -1, 1, 1) \quad \text{and} \quad w = (1, 1, -1, 1).$$

Clearly v and w are in distinct G -orbits, but nevertheless

$$f_i(v) = f_i(w), \quad g_i(v) = g_i(w), \quad \text{and} \quad h(v) = h(w).$$

Therefore A does not separate G -orbits. \triangleleft

It is not surprising that there exist examples like the one above, since in characteristic 0, a graded separating subalgebra $A \subseteq K[V]^G$ corresponds to a variety Y whose normalization \tilde{Y} coincides with $V//G$. But for A to be separating we need the additional hypothesis that all fibers of $\tilde{Y} \rightarrow Y$ have size one. This hypothesis is rather strong, and it would be desirable to have a simple criterion for deciding whether for a given variety Y , all fibers of the normalization $\tilde{Y} \rightarrow Y$ have size one.

Although the proof of the following theorem is very simple, the theorem may be surprising and shows that separating algebras are a useful concept.

Theorem 2.4.8 *Let X be an affine variety and G a group acting on $K[X]$ by automorphisms. Then there exists a finite separating set $S \subseteq K[X]^G$.*

Proof Set $R := K[X]$ and consider the ideal I in $R \otimes_K R$ generated by all $f \otimes 1 - 1 \otimes f$ with $f \in R^G$. Since $R \otimes_K R$ is Noetherian, there exist finitely many invariants $f_1, \dots, f_m \in R^G$ such that

$$I = (f_1 \otimes 1 - 1 \otimes f_1, \dots, f_m \otimes 1 - 1 \otimes f_m).$$

We claim that $\{f_1, \dots, f_m\}$ is separating. Indeed, take $x, y \in X$ and assume that there exists an $f \in K[X]^G$ with $f(x) \neq f(y)$. We have $g_1, \dots, g_m \in R \otimes_K R$ such that

$$f \otimes 1 - 1 \otimes f = \sum_{i=1}^m g_i(f_i \otimes 1 - 1 \otimes f_i).$$

Consider the homomorphism $\varphi: R \otimes_K R \rightarrow K$ of K -algebras sending $g \otimes h$ to $g(x)h(y)$. We have

$$0 \neq f(x) - f(y) = \varphi(f \otimes 1 - 1 \otimes f) = \sum_{i=1}^m \varphi(g_i)(f_i(x) - f_i(y)).$$

Thus $f_i(x) \neq f_i(y)$ for some i , which proves our claim. \square

The point about Theorem 2.4.8 is of course that $K[X]^G$ need not be finitely generated, for example if G is a nonreductive group. So the theorem says that if we are only interested in invariant theory for the sake of separating G -orbits (which is likely to have been one of the original motivations of invariant theory), then we need not worry about finite generation. Theorem 2.4.8 can easily be generalized to the case where $K[X]^G$ is replaced by an arbitrary subset of a finitely generated algebra of functions $X \rightarrow K$ from a set to a Noetherian ring (see Kemper [38]). Unfortunately, the proof of Theorem 2.4.8 is not constructive. But the theorem has been made explicit for some examples of nonfinitely generated invariant rings (see Dufresne and Kohls [40]). Moreover, for the case that G is reductive (and therefore $K[X]^G$ is finitely generated), there is an algorithm for computing a finite separating subset, which is actually a first step towards computing generators for $K[X]^G$. This will be treated in Sect. 4.9.1. In spite of these partial successes, the question of finding an algorithm for constructing a finite separating subset for a general linear algebraic group G is still open.

A defect of reductive groups in positive characteristic is that an epimorphism of representations does not in general remain surjective when restricted to the invariants. In particular, generating invariants are in general not mapped to generating invariants. However, this is true for separating invariants, as the next result shows.

Theorem 2.4.9 *Let G be a linear algebraic group. Then the following two statements are equivalent.*

- (a) *G is reductive.*
- (b) *If G acts regularly on an affine variety X and if $Y \subseteq X$ is a G -stable, closed subvariety, then the restriction map $K[X] \rightarrow K[Y]$ takes every separating subset of $K[X]^G$ to a separating subset of $K[Y]^G$.*

Proof First assume that G is reductive and let $S \subseteq K[X]^G$ be a separating subset. If two points x, y of Y can be separated by an invariant in $K[Y]^G$, then the orbit closures do not meet: $\overline{G(x)} \cap \overline{G(y)} = \emptyset$ (see Corollary 2.3.8). But this also holds in X , therefore x and y can be separated by an invariant from $K[X]^G$ (again by Corollary 2.3.8). Thus there is an $f \in S$ with $f(x) \neq f(y)$. The same inequality holds for the restriction of f to Y . This shows that the image of S under the restriction map is separating.

To prove the converse, let V be a rational representation of G . Then $V^G \subseteq V$ is G -stable and closed. $K[V^G]$ coincides with its own invariant ring, thus two distinct points $v, w \in V^G$ can always be separated by an invariant from $K[V^G]$. By the

assumption (b), this implies that v and w can also be separated by an invariant from $K[V]^G$. Assume $v \neq 0$ and take $w = 0$. Then we have $f \in K[V]^G$ with $f(v) \neq f(0)$. The invariant $f_+ := f - f(0)$ has no constant term, and $f_+(v) \neq 0$. Hence there exists a homogeneous invariant g of positive degree with $g(v) \neq 0$. Thus G is geometrically reductive. \square

Separating invariants take care of some further “defects” of invariant theory in positive characteristic. One such defect is that Weyl’s polarization theorem fails in positive characteristic, even for linearly reductive groups. Good references for polarization and Weyl’s theorem, which will not be treated in this book, are Weyl [41, II.5, Theorem 2.5A] and Kraft and Procesi [42, § 7.1]. But Draisma et al. [43] proved that the polarization theorem holds independently of the characteristic if one formulates it for separating invariants instead of generating invariants. This result was taken further by Grosshans [44]. Along similar lines, the following nice result was obtained by Domokos [45]: If G acts linearly on an n -dimensional vector space V , then for each m there exist separating invariants in $K[V^m]^G$ each of which depend only on at most $2n$ of its m arguments. An even better result holds if G is reductive.

It is also remarkable that there exists a simple general upper bound on the minimal cardinality of a separating subset. In fact, in the setting of Theorem 2.4.8 there exists a separating subset $S \subseteq K[X]^G$ of size

$$|S| \leq 2 \dim(K[X]^G) + 1.$$

This result appears to have been folklore for a while. A proof can be found in Dufresne [46, Proposition 5.1.1], and a generalized version appeared in Kamke and Kemper [47]. In view of the “explosion” that tends to occur with the number of generating invariants as the dimension of the representation goes up (see Example 2.1.2), this result again emphasizes the good behavior of separating invariants.

Further results on separating invariants of finite groups can be found in Sect. 3.12.

2.5 Homogeneous Systems of Parameters

In this section we will assume that G is a reductive group and V is a rational representation. First, we need to introduce the nullcone.

2.5.1 Hilbert’s Nullcone

In this section we give a criterion for a set of homogeneous polynomials $f_1, \dots, f_r \in K[V]^G$ which ensures that $K[V]^G$ is a finite module over $K[f_1, \dots, f_r]$. We will use Hilbert’s notion of the nullcone.

Definition 2.5.1 The **nullcone** $\mathcal{N}_V \subseteq V$ is the zero set of all homogeneous invariant polynomials of positive degree:

$$\mathcal{N}_V = \mathcal{N}_{V,G} := \{v \in V \mid f(v) = 0 \text{ for all } f \in K[V]_+^G\}.$$

There is also a more geometric description of the nullcone. If $\pi : V \rightarrow V//G$ is the categorical quotient, then \mathcal{N}_V is exactly the zero fiber $\pi^{-1}(0)$.

Lemma 2.5.2 *The nullcone \mathcal{N}_V is the set of all $v \in V$ such that the orbit closure $\overline{G \cdot v}$ contains 0.*

Proof The only closed orbit in $\pi^{-1}(0) = \mathcal{N}_V$ must be 0 (see Theorem 2.3.6). All other orbits in \mathcal{N}_V must have 0 in its closure. On the other hand, it is clear that every orbit which has 0 in its closure must be contained in $\pi^{-1}(0) = \mathcal{N}_V$. \square

For a finite group the nullcone only consists of 0.

The following theorem shows that if $v \in \mathcal{N}_V$, then not only does the Zariski closure of $G \cdot v$ contain 0, we also can find a multiplicative subgroup $\mathbb{G}_m \subseteq G$ such that $\mathbb{G}_m \cdot v$ contains 0 in its closure. This statement is known as the Hilbert-Mumford criterion. It was first proved by Hilbert [25] for SL_n , and later in a more general setting by Mumford (see Mumford et al. [33]).

Theorem 2.5.3 *Choose a maximal torus $T \subseteq G$. Let $\mathcal{N}_{V,T}, \mathcal{N}_{V,G} \subseteq V$ be the nullcones with respect to the actions of T and G respectively. Then $\mathcal{N}_{V,G} = G \cdot \mathcal{N}_{V,T}$.*

With the Hilbert-Mumford criterion it is often easy to decide which orbits lie in the nullcone, as the following example shows.

Example 2.5.4 Consider again the binary forms of degree d (see Example 2.1.2). We can choose a maximal torus

$$T = \left\{ \begin{pmatrix} \lambda & 0 \\ 0 & \lambda^{-1} \end{pmatrix} =: \sigma_\lambda \mid \lambda \in K^* \right\}$$

of all diagonal matrices in SL_2 . Let $f = a_0x^d + a_1x^{d-1}y + \cdots + a_dy^d \in V_d$. For $\sigma_\lambda \in T$ we have

$$\sigma_\lambda \cdot f = a_0x^d\lambda^d + a_1x^{d-1}y\lambda^{d-2} + \cdots + a_dy^d\lambda^{-d}.$$

It is clear that $f \in \mathcal{N}_{V_d,T}$ if and only if f is divisible by x^e or y^e where $e = \lfloor \frac{1}{2}d \rfloor + 1$. It follows from Theorem 2.5.3 that $f \in \mathcal{N}_{V_d} = \mathcal{N}_{V_d,\mathrm{SL}_2}$ if and only if f is divisible by $(\sigma \cdot x)^e$ for some $\sigma \in \mathrm{SL}_2$. So $f \in \mathcal{N}_{V_d}$ if and only if f has a zero of multiplicity $> \frac{1}{2}d$. \triangleleft

Lemma 2.5.5 *If $f_1, \dots, f_r \in K[V]^G$ are homogeneous and the zero set $\mathcal{V}(f_1, \dots, f_r)$ is \mathcal{N}_V , then $K[V]^G$ is a finitely generated F -module where $F = K[f_1, \dots, f_r]$.*

Proof Suppose that $K[V]^G = K[h_1, \dots, h_s]$ for some homogeneous invariants h_1, \dots, h_s . Let $\mathfrak{m} = (h_1, \dots, h_s)$ be the maximal homogeneous ideal of $K[V]^G$. The zero set of \mathfrak{m} in $V//G$ is just $\pi(0)$ (which we also call 0). Let J be the ideal generated by f_1, \dots, f_r in $K[V]^G$ and I be the ideal generated by f_1, \dots, f_r in $K[V]$. Suppose $Y := \mathcal{V}(J) \subseteq V//G$ is the zero set of J . Then the zero set $\mathcal{V}(I) \subseteq V$ is equal to $\pi^{-1}(Y)$. On the other hand this zero set must be equal to the nullcone $\pi^{-1}(0)$ and because π is surjective (see Lemma 2.3.2), we get $Y = \{0\}$. By Hilbert's Nullstellensatz there exists an l such that $h_i^l \in J$ for all i . Let S be the set of all monomials in $h_1^{i_1} h_2^{i_2} \cdots h_s^{i_s}$ with $0 \leq i_1, \dots, i_s < l$. It is clear that S generates $K[V]^G$ as an F -module. \square

Appendix C in this book describes a stratification of the nullcone, in which the strata have a much nicer structure than the nullcone itself, and gives an algorithm that computes this stratification.

2.5.2 Existence of Homogeneous Systems of Parameters

Definition 2.5.6 Suppose that $R = \bigoplus_{d=0}^{\infty} R_d$ is a graded algebra over a field K such that $R_0 = K$. A set $f_1, \dots, f_r \in R$ of homogeneous elements is called a **homogeneous system of parameters** if

- (a) f_1, \dots, f_r are algebraically independent and
- (b) R is a finitely generated module over $K[f_1, \dots, f_r]$.

If $f_1, \dots, f_r \in K[V]^G$ is a homogeneous system of parameters, then we call the f_i **primary invariants**. The invariant ring $K[V]^G$ is a finite $K[f_1, \dots, f_r]$ -module, say

$$K[V]^G = Fg_1 + Fg_2 + \cdots + Fg_s,$$

where F is the polynomial ring $K[f_1, \dots, f_r]$ and $g_1, \dots, g_s \in K[V]^G$ homogeneous. The invariants g_1, \dots, g_s are called **secondary invariants**. Some of the algorithms for computing invariant rings will compute primary invariants first, and then calculate a set of secondary invariants (see Sects. 3.5 and 3.7).

Homogeneous systems of parameters always exist for invariant rings. To see this we first need the Noether Normalization Lemma (see Eisenbud [48, Theorem 13.3]).

Lemma 2.5.7 Suppose that $R = \bigoplus_{d=0}^{\infty} R_d$ is a graded ring with $R_0 = K$. Suppose that $f_1, \dots, f_r \in R_d$ and R is a finitely generated F -module where $F = K[f_1, \dots, f_r]$. Then there exist $g_1, \dots, g_s \in R_d$ which are linear combinations of f_1, \dots, f_r such that g_1, \dots, g_s is a homogeneous system of parameters.

Finitely generated graded rings always have homogeneous systems of parameters as the following corollary shows. In particular invariant rings of reductive groups have homogeneous systems of parameters.

Corollary 2.5.8 *If $R = \bigoplus_{d=0}^{\infty} R_d$ is a finitely generated graded algebra with $R_0 = K$, then R has a homogeneous system of parameters.*

Proof Take homogeneous generators $f_1, \dots, f_r \in R$. Set $d_i = \deg(f_i)$ for all i . Let d be the least common multiple of d_1, \dots, d_r and define $f'_i = f_i^{d/d_i}$. Then f'_1, f'_2, \dots, f'_r are homogeneous of degree d . Now apply Lemma 2.5.7. \square

Example 2.5.9 Let $H \subseteq S_n$ act on K^n by permutations. The elementary symmetric polynomials $f_1, \dots, f_n \in K[x_1, \dots, x_n]^{S_n}$ (as defined in Example 2.1.1) are also H -invariant. The polynomial

$$\varphi(t) := (t - x_1)(t - x_2) \cdots (t - x_n) = t^n - f_1 t^{n-1} + f_2 t^{n-2} - \cdots + (-1)^n f_n$$

has exactly x_1, \dots, x_n as zero set. So if $f_1 = f_2 = \cdots = f_n = 0$, then $x_1 = x_2 = \cdots = x_n = 0$. But $\mathcal{V}(f_1, \dots, f_n)$ is exactly Hilbert's nullcone $\mathcal{N}_V = \{0\}$. It follows that $K[x_1, \dots, x_n]^H$ is a finite F -module, with $F = K[f_1, \dots, f_n]$. Because $\dim F = \dim K[x_1, \dots, x_n] = n$, we must have that f_1, \dots, f_n are algebraically independent. This shows that f_1, \dots, f_n is a system of primary invariants (for *any* permutation group $H \subseteq S_n$). \triangleleft

2.6 The Cohen-Macaulay Property of Invariant Rings

In this section K is an arbitrary field (not necessarily algebraically closed). First we will discuss the Cohen-Macaulay property in general. Then we will prove the important result of Hochster and Roberts about the Cohen-Macaulay property of invariant rings.

2.6.1 The Cohen-Macaulay Property

If $f_1, \dots, f_n \in K[V]^G$ are primary invariants, $K[V]^G$ is finitely generated as a module over the subalgebra $A = K[f_1, \dots, f_n]$. It would be very nice if $K[V]^G$ were in fact a *free* module over A . As we will see, this is the case precisely if $K[V]^G$ is Cohen-Macaulay, and the latter condition is always satisfied if G is linearly reductive.

Definition 2.6.1 Let R be a Noetherian ring and M a finitely generated R -module.

- (a) A sequence $f_1, \dots, f_k \in R$ is called **M -regular** if $M/(f_1, \dots, f_k)M \neq 0$ and multiplication by f_i induces an injective map on $M/(f_1, \dots, f_{i-1})M$, for $i = 1, \dots, k$.
- (b) Let $I \subseteq R$ be an ideal with $IM \neq M$. Then the **depth** of I on M is the maximal length k of an M -regular sequence f_1, \dots, f_k with $f_i \in I$, denoted by $\text{depth}(I, M) = k$.

- (c) If R is a local or graded ring with maximal (homogeneous) ideal \mathfrak{m} , we write $\text{depth}(M)$ for $\text{depth}(\mathfrak{m}, M)$.
- (d) If R is a local Noetherian ring with maximal ideal \mathfrak{m} , then M is called **Cohen-Macaulay** if $\text{depth}(M) = \dim(M)$, where $\dim(M)$ is the Krull dimension of $R/\text{Ann}(M)$. If R is not necessarily local, then M is called **Cohen-Macaulay** if for all maximal ideals $\mathfrak{m} \in \text{Supp}(M)$ (i.e., \mathfrak{m} containing $\text{Ann}(M)$), $M_{\mathfrak{m}}$ is Cohen-Macaulay as an $R_{\mathfrak{m}}$ -module.
- (e) R is called Cohen-Macaulay if it is Cohen-Macaulay as a module over itself.

We remark that always $\text{depth}(I, M) \leq \text{ht}(I)$ (the height of I), and in the case of a local ring $\text{depth}(M) \leq \dim(M)$ (see Eisenbud [48, Proposition 18.2]). If R is Cohen-Macaulay, than $\text{depth}(I, R) = \text{ht}(I)$ for every proper ideal $I \subset R$ (see Eisenbud [48, Theorem 18.7]). For more background about the Cohen-Macaulay property we refer the reader to the book of Bruns and Herzog [49].

Lemma 2.6.2 *A polynomial ring over a field is Cohen-Macaulay.*

Proof Let $R = K[x_1, \dots, x_n]$ be a polynomial ring and $P \subseteq R$ a maximal ideal. Then R/P is a finite field extension of K , hence for each $i = 1, \dots, n$ there exists a nonzero polynomial $f_i(x_i)$ which lies in P . It is elementary to check that $f_1(x_1), \dots, f_n(x_n)$ is an R -regular sequence. Hence it is also R_P -regular, so

$$\dim(R_P) = n \leq \text{depth}(P_P, R_P) \leq \text{ht}(P) = n.$$

□

The following proposition gives some important characterizations of the Cohen-Macaulay property for graded algebras.

Proposition 2.6.3 *Let R be a Noetherian graded algebra over a field K with $K = R_0$ the homogeneous part of degree 0. Then the following conditions are equivalent:*

- (a) R is Cohen-Macaulay;
- (b) every homogeneous system of parameters is R -regular;
- (c) if f_1, \dots, f_n is a homogeneous system of parameters, then R is a free module over $K[f_1, \dots, f_n]$;
- (d) there exists a homogeneous system of parameters f_1, \dots, f_n such that R is a free module over $K[f_1, \dots, f_n]$.

A proof of Proposition 2.6.3 can be found in Benson [50, Theorem 4.3.5] or Kemper [51].

Example 2.6.4 (Bruns and Herzog [49, Exercise 2.1.18]) Let $R = K[x^4, x^3y, xy^3, y^4] \subset K[x, y]$ and $S = K[x^4, y^4]$. It is clear that R is finite over S because $(x^3y)^4$ and $(xy^3)^4$ are in S . So x^4, y^4 is a homogeneous system of parameters. If R were Cohen-Macaulay, then x^4, y^4 would be an R -regular sequence. There is a relation $x^4(xy^3)^2 = y^4(x^3y)^2$, but $(x^3y)^2$ does not lie in the R -ideal (x^4) . This shows that R is not Cohen-Macaulay. □

It is the condition (c) in the above proposition that makes the Cohen-Macaulay property very relevant for the computation of invariant rings.

2.6.2 The Hochster-Roberts Theorem

In this section we will prove the following theorem.

Theorem 2.6.5 (Hochster and Roberts [52]) *If G is a linearly reductive group, then $K[V]^G$ is Cohen-Macaulay.*

It was shown in Hochster and Huneke [53] that the result still holds when V is not a representation but a smooth G -variety. Another important generalization can be found in Boutot [54] where it was proven that $K[V]^G$ has rational singularities (this implies that $K[V]^G$ is Cohen-Macaulay). It is hard to overemphasize the importance of the theorem of Hochster and Roberts. Apart from being an important tool for the computation of invariant rings of linearly reductive groups, it provides a good deal of information about the structure of invariant rings: They are finitely generated free modules over a subalgebra which is isomorphic to a polynomial ring. We also have a partial converse of Theorem 2.6.5.

Theorem 2.6.6 (Kemper [55]) *Suppose that G is a reductive group and that for every rational representation the invariant ring $K[V]^G$ is Cohen-Macaulay. Then G is linearly reductive.*

Of course this theorem is vacuous in characteristic 0 (see Theorem 2.2.13), but it shows, for example, that the classical groups in positive characteristic have rational representations with non-Cohen-Macaulay invariant ring. This was made explicit by Kohls [56]. It was also strengthened by Kohls [57] who showed that if G is reductive but not linearly reductive, there exists a rational representation V such that the Cohen-Macaulay defect $\dim(K[V^k]^G) - \text{depth}(K[V^k]^G)$ of the vector invariants tends to infinity with k . The hypothesis that G be reductive is necessary, as the example of additive group \mathbb{G}_a (which is nonreductive and in particular not linearly reductive) shows: over an algebraically closed field of characteristic 0, every invariant ring of a rational representation of \mathbb{G}_a is isomorphic to an invariant ring of SL_2 (see Remark 2.1.7), which is Cohen-Macaulay by Theorem 2.6.5.

We now embark on the proof of Theorem 2.6.5. The special case where G is a finite group whose order is not divisible by the characteristic of K will be proven in Sect. 3.6, since this proof is instructive and much more elementary than the general one. Our version of the general proof is based on an (almost) elementary proof due to Friedrich Knop, who used ideas from Hochster and Huneke [53]. Knop's proof can be found in Bruns and Herzog [49]. The proof we will give here is similar, and is also inspired by lectures of Mel Hochster at the University of Michigan. We will

use methods in positive characteristic. Suppose that R is a finitely generated domain over a finite field K of characteristic $p > 0$. An important notion we will use is tight closure. If I is an ideal of R and q is a power of p , then we will write $I^{[q]}$ for the ideal generated by all q -powers of elements in I . Note that $I^{[q]} \subseteq I^q$, but they do not have to be equal.

Definition 2.6.7 The **tight closure** I^* of an ideal I is the set of all elements $f \in R$ for which there exists an $a \in R$ which is no a zero divisor such that for all sufficiently large p -powers q we have

$$af^q \in I^{[q]}.$$

It is known that if R is regular (i.e., the coordinate ring of a smooth variety), then we have $I = I^*$ for all ideals I (see Hochster and Huneke [53, Theorem 4.4]). Here we will prove a weaker statement.

Theorem 2.6.8 *If $R = K[x_1, \dots, x_n]$ is a polynomial ring over a perfect field K of characteristic p and $I \subseteq R$ is an ideal then $I^* = I$.*

Proof Suppose that $f \in I^*$, i.e., for some $a \in R$ we have

$$af^q \in I^{[q]}$$

for all p -powers $q \geq C$ where C is some constant. By Lemma 2.6.9 below we have

$$a \in \bigcap_{q \geq C} (I^{[q]} : f^q) = \bigcap_{q \geq C} (I : f)^{[q]} \subseteq \bigcap_{q \geq C} (I : f)^q.$$

If $(I : f) \neq R$, then we have $\bigcap_{q \geq C} (I : f)^q = 0$ which contradicts $a \neq 0$. We conclude that $(I : f) = R$ and $f \in I$. \square

Lemma 2.6.9 *If $R = K[x_1, \dots, x_n]$ is a polynomial ring over a perfect field K of characteristic p , then we have*

$$(I^{[q]} : f^q) = (I : f)^{[q]}$$

for all ideals $I \subseteq R$ and all $f \in R$.

Proof The inclusion $(I^{[q]} : f^q) \supseteq (I : f)^{[q]}$ is trivial. We will prove the reverse inclusion. Suppose that $a \in (I^{[q]} : f^q)$, so

$$af^q = \sum_{j=1}^r a_j f_j^q, \tag{2.6.1}$$

where $I = (f_1, \dots, f_r)$. $K[x_1, \dots, x_n]$ is a free module over the subring $K[x_1^q, \dots, x_n^q]$, in fact

$$K[x_1, \dots, x_n] = \bigoplus_i K[x_1^q, \dots, x_n^q]m_i, \quad (2.6.2)$$

where the m_i runs over all monomials $x_1^{d_1} \cdots x_n^{d_n}$ with $0 \leq d_1, \dots, d_n \leq q-1$. In particular, we can write

$$a = \sum_i b_i m_i \quad (2.6.3)$$

with $b_i \in K[x_1^q, \dots, x_n^q]$ for all i , and similarly

$$a_j = \sum_i b_{ij} m_i$$

with $b_{ij} \in K[x_1^q, \dots, x_n^q]$ for all i and j . Using (2.6.2) and (2.6.1) it follows that

$$b_i f^q = \sum_j b_{ij} f_j^q$$

holds for every i . We can write $b_i = c_i^q$ and $b_{ij} = c_{ij}^q$ with $c_i, c_{ij} \in K[x_1, \dots, x_n]$ for all i, j (note that we can take q -th roots of elements in K because K is perfect). We have

$$c_i^q f^q = \sum_j c_{ij}^q f_j^q$$

and taking the q -th root gives

$$c_i f = \sum_j c_{ij} f_j \in I.$$

So $c_i \in (I : f)$ for all i , and from (2.6.3) it follows that $a \in (I : f)^{[q]}$. \square

Lemma 2.6.10 Suppose that V is a representation of a linearly reductive group G . If $I \subseteq K[V]^G$ is an ideal, then $IK[V] \cap K[V]^G = I$.

Proof The inclusion “ \supseteq ” is clear. Conversely, suppose that $f \in K[V]^G$ lies in the ideal $IK[V]$, i.e.,

$$f = \sum_{i=1}^r g_i f_i \quad (2.6.4)$$

with $g_1, \dots, g_r \in K[V]$ and $f_1, \dots, f_r \in I$. Applying the Reynolds operator to (2.6.4) yields

$$f = \mathcal{R}(f) = \sum_{i=1}^r \mathcal{R}(g_i f_i) = \mathcal{R}(g_i) f_i.$$

Since $\mathcal{R}(g_1), \dots, \mathcal{R}(g_r) \in K[V]^G$, this proves that $f \in I$. \square

Because of the previous lemma, Theorem 2.6.5 follows from the theorem below.

Theorem 2.6.11 *Let $R := K[x_1, \dots, x_n]$ be a polynomial ring over a field K . If $S \subseteq R$ is a finitely generated graded subalgebra with the property that $IR \cap S = I$ for every ideal $I \subseteq S$, then S is Cohen-Macaulay.*

Proof Let $f_1, \dots, f_s \in S$ be a homogeneous system of parameters and put $A := K[f_1, \dots, f_s]$. S is a finitely generated A -module, say

$$S = \sum_{i=1}^m A g_i,$$

where we can assume $g_1 = 1$. We are going to prove that f_1, \dots, f_s is a regular sequence in S , which by Proposition 2.6.3 implies that S is Cohen-Macaulay. The idea is to reduce to a statement in positive characteristic which can be proven using the notion of tight closure. Suppose that

$$a_{r+1} f_{r+1} = a_1 f_1 + \cdots + a_r f_r \quad (2.6.5)$$

with $a_1, \dots, a_{r+1} \in S$. We would like to show that $a_{r+1} \in (f_1, \dots, f_r)S$. By the hypothesis we only have to prove that $a_{r+1} \in (f_1, \dots, f_r)R$. So we need to find $b_1, \dots, b_r \in R$ such that $a_{r+1} = b_1 f_1 + \cdots + b_r f_r$. If such b_i exist, we may assume their (total) degrees to be smaller than the degree of a_{r+1} . Thus the existence of b_1, \dots, b_r is equivalent to the solvability of a system of (inhomogeneous) linear equations for the coefficients of the b_i . This system is of the form

$$Mv = w, \quad (2.6.6)$$

where the vector w and the matrix M have entries in K . Assume, by way of contradiction, that

$$a_{r+1} \notin (f_1, \dots, f_r)R. \quad (2.6.7)$$

This means that (2.6.6) has no solution. Thus there exists a nonzero subdeterminant $d \in K$ of the extended matrix $(M|v)$ of rank greater than the rank of M .

Let Z be the smallest subring of K containing all “necessary” elements:

- (a) The ring Z contains all coefficients of f_1, \dots, f_s and g_1, \dots, g_m (as polynomials over K).
- (b) For all i, j we can write

$$g_i g_j = \sum_{l=1}^m p_{i,j,l}(f_1, \dots, f_s) g_l$$

with $p_{i,j,l}$ polynomials with coefficients in K . Let these coefficients also be contained in Z .

- (c) For all i we can write

$$a_i = \sum_{j=1}^m q_{i,j}(f_1, \dots, f_s) g_j$$

where $q_{i,j}$ are polynomials with coefficients in K . These coefficients should also lie in Z .

- (d) Finally, $d^{-1} \in Z$.

Thus $Z \subseteq K$ is a finitely generated ring. Now we put $R_Z := Z[x_1, \dots, x_n]$, $A_Z := Z[f_1, \dots, f_s]$, and $S_Z := A_Z[g_1, \dots, g_m]$. The condition (a) guarantees that $S_Z \subseteq R_Z$, and by (b) we have that $S_Z = \sum_{i=1}^m A_Z g_i$. Because of (c), the Eq. (2.6.5) involves only elements of S_Z . Moreover, the coefficients of (2.6.6) lie in Z . Let $\mathfrak{m} \subset Z$ be a maximal ideal. Since $d^{-1} \in Z$, (2.6.6) has no solutions modulo \mathfrak{m} . This means that

$$a_{r+1} \notin (f_1, \dots, f_r)R_Z + \mathfrak{m}R_Z \quad (2.6.8)$$

for every maximal ideal $\mathfrak{m} \subset Z$.

For the rest of our argument we need to find a maximal ideal \mathfrak{m} such that $A_Z/\mathfrak{m}A_Z \rightarrow S_Z/\mathfrak{m}S_Z$ is injective. For this end, choose a maximal A_Z -linearly independent subset of $\{g_1, \dots, g_m\}$. Without loss, this subset can be assumed to be $\{g_1, \dots, g_{m'}\}$ with $m' \leq m$. Set $F_Z := \sum_{i=1}^{m'} A_Z g_i \subseteq S_Z$. The sum is direct, and there exists a nonzero $c \in A_Z$ such that $c \cdot S_Z \subseteq F_Z$. Since R_Z is a finitely generated ring without zero divisors, the intersection of all maximal ideals of R_Z is zero (see Eisenbud [48, Theorem 4.19], but a much more elementary proof can be given for the case considered here). Thus there exists a maximal ideal $\mathfrak{n} \subset R_Z$ with $c \notin \mathfrak{n}$. Set $\mathfrak{m} := Z \cap \mathfrak{n}$. R_Z/\mathfrak{n} is a field and at the same time a finitely generated ring. From this it easily follows that R_Z/\mathfrak{n} is a finite field. Hence the same is true for

$$k := Z/\mathfrak{m}.$$

In particular, $\mathfrak{m} \subset Z$ is a maximal ideal. Now take an element $f \in A_Z \cap \mathfrak{m}S_Z$. Then

$$cf \in A_Z \cap \mathfrak{m}F_Z = A_Z \cap \bigoplus_{i=1}^{m'} \mathfrak{m}A_Z g_i = \mathfrak{m}A_Z,$$

since $g_1 = 1$ and $g_1, g_2, \dots, g_{m'}$ are independent. Moreover, $\mathfrak{m}A_Z \subset A_Z$ is a prime ideal, since the quotient ring is a polynomial ring over k . Since $c \notin \mathfrak{m}A_Z$, the above implies $f \in \mathfrak{m}A_Z$. Thus we have shown that $A_Z \cap \mathfrak{m}S_Z = \mathfrak{m}A_Z$, so $A_Z/\mathfrak{m}A_Z \rightarrow S_Z/\mathfrak{m}S_Z$ is indeed injective. Set

$$A_k := A_Z/\mathfrak{m}A_Z, \quad S_k := S_Z/\mathfrak{m}S_Z, \quad \text{and} \quad R_k := R_Z/\mathfrak{m}R_Z.$$

Denote the canonical map $S_Z \rightarrow S_k$ by $\bar{\cdot}$. Then $A_k = k[\bar{f}_1, \dots, \bar{f}_s]$ and $S_k = \sum_{i=1}^{m'} A_k \bar{g}_i$. The relation (2.6.5) reduces to

$$\bar{a}_{r+1} \bar{f}_{r+1} = \bar{a}_1 \bar{f}_1 + \dots + \bar{a}_r \bar{f}_r.$$

Let p be the characteristic of k and let q be a power of p . Raising the above equation to the q -th power and multiplying by \bar{c} yields

$$\bar{c} \cdot \bar{a}_{r+1}^q \bar{f}_{r+1}^q = \bar{c} \cdot \bar{a}_1^q \bar{f}_1^q + \dots + \bar{c} \cdot \bar{a}_r^q \bar{f}_r^q \subseteq (\bar{f}_1^q, \dots, \bar{f}_r^q) F_k, \quad (2.6.9)$$

where we put $F_k := \sum_{i=1}^{m'} A_k \bar{g}_i \subseteq S_k$. The latter sum is direct, since $\sum_{i=1}^{m'} \alpha_i g_i \in \mathfrak{m}S_Z$ with $\alpha_i \in A_Z$ implies $c \cdot \sum_{i=1}^{m'} \alpha_i g_i \in \mathfrak{m}F_Z$. Thus $c\alpha_i \in \mathfrak{m}A_Z$ by the freeness of F_Z , and therefore $\alpha_i \in \mathfrak{m}A_Z$. Since $A_k = k[\bar{f}_1, \dots, \bar{f}_s]$ is a polynomial ring (and therefore Cohen-Macaulay by Lemma 2.6.2), and F_k is a free A_k -module, it follows that $\bar{f}_1^q, \dots, \bar{f}_r^q$ is F_k -regular. Hence from (2.6.9) we get

$$\bar{c} \cdot \bar{a}_{r+1}^q \in (\bar{f}_1^q, \dots, \bar{f}_r^q) F_k \subseteq (\bar{f}_1^q, \dots, \bar{f}_r^q) S_k.$$

Application of the canonical map $\hat{\cdot}: R_Z \rightarrow R_k$ now yields

$$\hat{c} \cdot \hat{a}_{r+1}^q \in (\hat{f}_1^q, \dots, \hat{f}_r^q) R_k.$$

Since this is true for every p -power q and since $\hat{c} \neq 0$, this means that $\hat{a}_{r+1} \in (\hat{f}_1, \dots, \hat{f}_r)^*$ (the tight closure of the ideal in R_k generated by the \hat{f}_i). By Theorem 2.6.8 this implies $\hat{a}_{r+1} \in (\hat{f}_1, \dots, \hat{f}_r)$, which contradicts (2.6.8). This shows that the assumption (2.6.7) was false, and we are done. \square

2.7 Hilbert Series of Invariant Rings

An important tool for computing invariants is the Hilbert series. The Hilbert series of a ring contains a lot of information about the ring itself. For example, the dimension and other geometric invariants can be read off the Hilbert series (see Sect. 1.4).

In many cases we already know the Hilbert series $H(K[V]^G, t)$ before knowing generators of $K[V]^G$. For finite groups, $H(K[V]^G, t)$ can be computed using Molien's formula (see Theorem 3.4.2). For arbitrary linearly reductive groups, $H(K[V]^G, t)$ can also be computed (see Sect. 4.6). The Hilbert series often helps to find invariants more efficiently.

If $H(K[V]^G, t)$ is known, then we have a criterion for a set of homogeneous invariants f_1, \dots, f_r to generate $H(K[V]^G, t)$, namely

$$K[V]^G = K[f_1, \dots, f_r] \iff H(K[V]^G, t) = H(K[f_1, \dots, f_r], t). \quad (2.7.1)$$

Algorithm 2.7.1 Criterion (2.7.1) gives us another strategy for computing invariants if $H(K[V]^G, t)$ is known. We start with $S := \emptyset$, an empty set of generators. Suppose we have already found a finite set of homogeneous invariants $S = \{f_1, \dots, f_r\}$. We write $K[S]$ instead of $K[f_1, \dots, f_r]$ for convenience. Compute $H(K[S], t)$ and compare it to $H(K[V]^G, t)$. If they are equal, we are done. If not, then look at the difference

$$H(K[V]^G, t) - H(K[S], t) = kt^d + \text{higher order terms}.$$

This means that $K[f_1, \dots, f_r]$ contains all invariants of degree $< d$ and in degree d we are missing k invariants, i.e., $K[S]_d$ has codimension k in $K[V]_d$. Using linear algebra (we do not want to be more specific at this point), find invariants $g_1, \dots, g_k \in K[V]_d^G$, such that $K[V]_d^G$ is spanned by $K[f_1, \dots, f_r]_d$ and g_1, \dots, g_k . We add g_1, \dots, g_k to our generators, $S := S \cup \{g_1, \dots, g_k\}$. We continue this process until $H(K[V]^G, t) = H(K[S], t)$ or equivalently $K[V]^G = K[S]$.

Let $v_t(H(K[V]^G, t) - H(K[S], t))$ be the smallest integer d such that t^d appears in the power series $H(K[V]^G, t) - H(K[S], t)$. With each step, $v_t(H(K[V]^G, t) - H(K[S], t))$ increases. Suppose that $K[V]^G$ is generated by invariants of degree $\leq D$. After D steps,

$$H(K[V]^G, t) - H(K[S], t) = kt^d + \text{higher order terms},$$

with $d > D$, or $H(K[V]^G, t) = H(K[S], t)$. This means that $K[S]$ contains all invariants of degree $\leq D$, so $K[V]^G = K[S]$. This shows that the algorithm terminates whenever $K[V]^G$ is finitely generated.

Notice that S will be a minimal set of generators for $K[V]^G$. From the above description of the algorithm, it is clear that none of the g_i can be omitted.

We will investigate the structure of $H(K[V]^G, t)$ when G is a linearly reductive group and V is a rational representation. First of all, we know that there is a homogeneous system of parameters f_1, \dots, f_r (or primary invariants) of $K[V]^G$ (see

Corollary 2.5.8). So $K[V]^G$ is a free F -module, where $F \cong K[f_1, \dots, f_r]$, because $K[V]^G$ is Cohen-Macaulay by Theorem 2.6.5 (see Proposition 2.6.3). So there is a decomposition

$$K[V]^G = Fg_1 \oplus Fg_2 \oplus \cdots \oplus Fg_s \quad (2.7.2)$$

with $g_1, \dots, g_s \in K[V]^G$ homogeneous. The decomposition 2.7.2 is often called a **Hironaka decomposition**. By Example 1.4.8, the Hilbert series of $K[f_1, \dots, f_r]$ is equal to $\prod_{i=1}^r (1 - t^{d_i})^{-1}$ where $d_i := \deg(f_i)$ for all i . From (2.7.2) it follows that

$$H(K[V]^G, t) = \frac{\sum_{j=1}^s t^{e_j}}{\prod_{i=1}^r (1 - t^{d_i})}, \quad (2.7.3)$$

where $e_j = \deg(g_j)$ for all j .

The degree of a rational function $\deg(a(t)/b(t))$ is given by $\deg(a(t)) - \deg(b(t))$. Boutot proved that $K[V]^G$ has rational singularities if G is reductive and K has characteristic 0 (see Boutot [54]). A consequence is that $H(K[V]^G, t)$ has degree ≤ 0 if G is connected and semisimple. This inequality was proven earlier by Kempf (see Kempf [58]). It has been conjectured in Popov [59] that $H(K[V]^G, t)$ has degree $\leq -\dim(V)$. In fact, it was shown in Popov [59] that the degree of $H(K[V]^G, t)$ is equal to $-\dim(V)$ for “almost all” representations of a connected semisimple group G . Later, Knop and Littelmann classified all irreducible representations of connected semisimple groups G such that the degree of $H(K[V]^G, t)$ is smaller than $-\dim(V)$ (see Knop and Littelmann [60]). For a more detailed exposition, see Popov [61]. In an attempt to prove Popov’s conjecture, Knop proved the following inequality.

Theorem 2.7.2 (Knop [62]) *Let G be semisimple and connected and let K be a field of characteristic 0. The degree $H(K[V]^G, t)$ is $\leq -r$, where r is the Krull dimension of $K[V]^G$.*

For finite linearly reductive groups (in any characteristic) the same statement follows from Molien’s formula (see Theorem 3.4.2).

The bound on the degree of $H(K[V]^G, t)$ can be used to find upper bounds for $\beta(K[V]^G)$ (see Popov [63], Popov [64]). Recall that $\beta(K[V]^G)$ is the smallest integer d such that the ring of invariants $K[V]^G$ is generated by invariants of degree $\leq d$ (see (2.1.1)). For the moment, we just note the following.

Corollary 2.7.3 *Suppose that G is semisimple and connected and $\text{char}(K) = 0$, or that G is finite and $\text{char}(K) \nmid |G|$. If f_1, \dots, f_r is a homogeneous system of parameters of $K[V]^G$, then*

$$\beta(K[V]^G) \leq \max\{d_1 + d_2 + \cdots + d_r - r, d_1, d_2, \dots, d_r\} \quad (2.7.4)$$

where $d_i := \deg(f_i)$ for all i . In fact, the above degree bound holds for the secondary invariants.

Proof This follows immediately from (2.7.3) and Theorem 2.7.2. □

Remark 2.7.4 If at least two of the polynomials f_1, \dots, f_r are nonlinear, (2.7.4) simplifies to

$$\beta(K[V]^G) \leq d_1 + d_2 + \dots + d_r - r$$

△

Example 2.7.5 Assume $\text{char}(K) = 0$ and let $A_n \subset S_n$ be the alternating group of even permutations acting on $V = K^n$. We saw in Example 2.5.9 that the elementary symmetric polynomials f_1, \dots, f_n defined in Example 2.1.1 form a homogeneous system of parameters. By Corollary 2.7.3 we have $\beta(K[x_1, \dots, x_n]^{A_n}) \leq 1 + 2 + \dots + n - n = \binom{n}{2}$. Let us define $g = \prod_{i < j} (x_i - x_j)$. Then clearly g is A_n -invariant but not S_n -invariant. The degree of g is exactly $\binom{n}{2}$.

We will show that $K[x_1, \dots, x_n]^{A_n} = F \oplus Fg$ where $F = K[x_1, \dots, x_n]^{S_n}$ (which is generated by f_1, \dots, f_n , see Example 2.1.1).

If h is an arbitrary homogeneous A_n -invariant, then $h = h_1 + h_2$ with

$$h_1 = \frac{h + \tau \cdot h}{2}, \quad h_2 = \frac{h - \tau \cdot h}{2},$$

and $\tau = (1\ 2) \in S_n$ is the 2-cycle which interchanges 1 and 2. In this decomposition, h_1 is S_n -invariant and h_2 is an S_n -semi-invariant:

$$\sigma \cdot h_2 = \text{sgn}(\sigma)h_2 \quad \text{for all } \sigma \in S_n,$$

where $\text{sgn}(\sigma)$ is the sign of the permutation $\sigma \in S_n$. It follows that whenever $x_i = x_j$ for $i \neq j$, we have

$$h_2(x_1, \dots, x_n) = -((i\ j) \cdot h_2)(x_1, \dots, x_n) = -h_2(x_1, \dots, x_n),$$

so $h_2(x_1, \dots, x_n) = 0$. Thus h_2 must be divisible by $x_i - x_j$ for all $i < j$, so in fact it is divisible by g . We conclude $h = h_1 + g \cdot (h_2/g)$ and $h_1, h_2/g \in F$.

Notice that g cannot be expressed in A_n -invariants of smaller degree, so the bound from Corollary 2.7.3 is sharp in this case. △

References

1. Armand Borel, *Linear Algebraic Groups*, Graduate Texts in Mathematics **126**, Springer Verlag, New York 1991.
2. James E. Humphreys, *Linear Algebraic Groups*, Springer-Verlag, Berlin, Heidelberg, New York 1981.
3. Tonny A. Springer, *Linear Algebraic Groups*, vol. 9 of *Progress in Mathematics*, Birkhäuser Boston, Inc., Boston 1998.

4. David Hilbert, *Mathematische Probleme*, Archiv für Math. und Physik **1** (1901), 44–63, Gesammelte Abhandlungen Band III (1970), Springer Verlag, Berlin–Heidelberg–New York, 290–329..
5. Masayoshi Nagata, *On the 14th problem of Hilbert*, Am. J. Math. **81** (1959), 766–772.
6. Harm Derksen, Hanspeter Kraft, *Constructive Invariant Theory*, in: *Algèbre non commutative, groupes quantiques et invariants (Reims, 1995)*, vol. 36 of Sémin. Congr., pp. 221–244, Soc. Math. France, Paris 1997.
7. Paul Gordan, *Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Funktion mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist*, J. Reine Angew. Math. **69** (1868), 323–354.
8. Serge Lang, *Algebra*, Addison-Wesley Publishing Co., Reading, Mass. 1985.
9. Tonny A. Springer, *Invariant Theory*, vol. 585 of *Lect. Notes Math.*, Springer-Verlag, New York 1977.
10. Tetsuji Shioda, *On the graded ring of invariants of binary octavics*, Am. J. Math. **89** (1967), 1022–1046.
11. J. Dixmier, D. Lazard, *Minimum number of fundamental invariants for the binary form of degree 7*, J. Symbolic Comput. **6** (1988), 113–115.
12. Andries E. Brouwer, Mihaela Popoviciu, *The invariants of the binary decimic*, J. Symbolic Comput. **45** (2010), 837–843.
13. Andries E. Brouwer, Mihaela Popoviciu, *The invariants of the binary nonic*, J. Symbolic Comput. **45** (2010), 709–720.
14. Vladimir L. Popov, Ernest B. Vinberg, *Invariant theory*, in: N. N. Parshin, I. R. Shafarevich, eds., *Algebraic Geometry IV*, Encyclopaedia of Mathematical Sciences **55**, Springer-Verlag, Berlin, Heidelberg 1994.
15. Paul Roberts, *An infinitely generated symbolic blow-up in a power series ring and a new counterexample to Hilbert's fourteenth problem*, J. Algebra **132** (1990), 461–473.
16. Daniel Daigle, Gene Freudenburg, *A counterexample to Hilbert's fourteenth problem in dimension 5*, J. Algebra **221** (1999), 528–535.
17. Oscar Zariski, *Interpretations algebro-géométriques du quartzième problème de Hilbert*, Bull. Sci. Math. **78** (1954), 155–168.
18. R. Weitzenböck, *Über die Invarianten von linearen Gruppen*, Acta Math. **58** (1932), 231–293.
19. C. S. Seshadri, *On a theorem of Weitzenböck in invariant theory*, J. Math. Kyoto Univ. **1** (1962), 403–409.
20. Hanspeter Kraft, *Geometrische Methoden in der Invariantentheorie*, Aspects of Mathematics **D1**, Vieweg, Braunschweig/Wiesbaden 1985.
21. Michael Roberts, *On the covariants of a binary quantic of the n^{th} degree*, The Quarterly Journal of Pure and Applied Mathematics **4** (1861), 168–178.
22. Roger M. Bryant, Gregor Kemper, *Global degree bounds and the transfer principle for invariants*, J. Algebra **284** (2005), 80–90.
23. William Fulton, Joe Harris, *Representation Theory: A first Course*, vol. 129 of *Graduate Texts in Mathematics*, Springer-Verlag, New York–Berlin–Heidelberg 1991.
24. David Hilbert, *Über die Theorie der algebraischen Formen*, Math. Ann. **36** (1890), 473–534.
25. David Hilbert, *Über die vollen Invariantensysteme*, Math. Ann. **42** (1893), 313–370.
26. Masayoshi Nagata, Takehiko Miyata, *Note on semi-reductive groups*, J. Math. Kyoto Univ. **3** (1963/1964), 379–382.
27. William J. Haboush, *Reductive groups are geometrically reductive*, Ann. of Math. **102** (1975), 67–83.
28. Masayoshi Nagata, *Invariants of a group in an affine ring*, J. Math. Kyoto Univ. **3** (1963/1964), 369–377.
29. Vincent Franjou, Wilberd van der Kallen, *Power reductivity over an arbitrary base*, Doc. Math. Extra volume: Andrei A. Suslin sixtieth birthday (2010), 171–195.
30. Vladimir L. Popov, *On Hilbert's theorem on invariants*, Dokl. Akad. Nauk SSSR **249** (1979), English translation Soviet Math. Dokl. **20** (1979), 1318–1322.

31. Masayoshi Nagata, *Complete reducibility of rational representations of a matrix group*, J. Math. Kyoto Univ. **1** (1961), 87–99.
32. Martin Kohls, *A user friendly proof of Nagata's characterization of linearly reductive groups in positive characteristics*, Linear Multilinear Algebra **59** (2011), 271–278.
33. David Mumford, John Fogarty, Frances Kirwan, *Geometric Invariant Theory*, Ergebnisse der Math. und ihrer Grenzgebiete **34**, third edn., Springer-Verlag, Berlin, Heidelberg, New York 1994.
34. P. E. Newstead, *Introduction to Moduli Problems and Orbit Spaces*, Springer-Verlag, Berlin, Heidelberg, New York 1978.
35. Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, Heidelberg, Berlin 1977.
36. Maxwell Rosenlicht, *A remark on quotient spaces*, Anais Acad. Brasil. Ci. **35** (1963), 487–489.
37. Gregor Kemper, *The computation of invariant fields and a constructive version of a theorem by Rosenlicht*, Transformation Groups **12** (2007), 657–670.
38. Gregor Kemper, *Separating invariants*, J. Symbolic Comput. **44** (2009), 1212–1222.
39. Wilberd van der Kallen, *Lectures on Frobenius splittings and B-modules*, Published for the Tata Institute of Fundamental Research, Bombay 1993, Notes by S. P. Inamdar.
40. Emilie Dufresne, Martin Kohls, *A finite separating set for Daigle and Freudenburg's counterexample to Hilbert's fourteenth problem*, Comm. Algebra **38** (2010), 3987–3992.
41. Hermann Weyl, *The Classical Groups. Their Invariants and Representations*, Princeton University Press, Princeton, N.J. 1939.
42. Hanspeter Kraft, Claudio Procesi, *A primer of invariant theory*, Notes by G. Boffi, Brandeis Lecture Notes 1. Updated version (2000) available at <http://www.math.unibas.ch/~kraft/Papers/KP-Primer.pdf>, 1982.
43. Jan Draisma, Gregor Kemper, David Wehlau, *Polarization of separating invariants*, Canad. J. Math. **60** (2008), 556–571.
44. F. D. Grosshans, *Vector invariants in arbitrary characteristic*, Transform. Groups **12** (2007), 499–514.
45. M. Domokos, *Typical separating invariants*, Transformation Groups **12** (2007), 49–63.
46. Emilie Dufresne, *Separating invariants*, Dissertation, Queen's University, Kingston, Ontario, Canada 2008, <http://hdl.handle.net/1974/1407>.
47. Tobias Kamke, Gregor Kemper, *Algorithmic invariant theory of nonreductive groups*, Qualitative Theory of Dynamical Systems **11** (2012), 79–110.
48. David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York 1995.
49. Winfried Bruns, Jürgen Herzog, *Cohen-Macaulay Rings*, Cambridge University Press, Cambridge 1993.
50. David J. Benson, *Polynomial Invariants of Finite Groups*, Lond. Math. Soc. Lecture Note Ser. **190**, Cambridge Univ. Press, Cambridge 1993.
51. Gregor Kemper, *Computational invariant theory*, The Curves Seminar at Queen's, Volume XII, in: Queen's Papers in Pure and Applied Math. **114** (1998e), 5–26.
52. Melvin Hochster, Joel L. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay*, Adv. in Math. **13** (1974), 115–175.
53. Melvin Hochster, Craig Huneke, *Tight closure, invariant theory, and the Briançon-Skoda theorem*, J. Amer. Math. Soc. **3** (1990), 31–116.
54. Jean-François Boutot, *Singularités rationnelles et quotients par les groupes réductifs*, Invent. Math. **88** (1987), 65–68.
55. Gregor Kemper, *A characterization of linearly reductive groups by their invariants*, Transformation Groups **5** (2000), 85–92.
56. Martin Kohls, *Non Cohen-Macaulay invariant rings of infinite groups*, J. Algebra **306** (2006), 591–609.
57. Martin Kohls, *On the depth of invariant rings of infinite groups*, J. of Algebra **322** (2009), 210–218.

58. George Kempf, *The Hochster-Roberts theorem of invariant theory*, Michigan Math. J. **26** (1979), 19–32.
59. Vladimir L. Popov, *A finiteness theorem for representations with a free algebra of invariants*, Math. USSR Izvest. **20** (1983), 333–354.
60. Friedrich Knop, Peter Littelmann, *Der Grad erzeugender Funktionen von Invariantenringen*, Math. Z. **196** (1987), 211–229.
61. Vladimir L. Popov, *Groups, Generators, Syzygies and Orbits in Invariant Theory*, Translations of Mathematical Monographs **100**, American Mathematical Society, Providence, RI 1992.
62. Friedrich Knop, *Der kanonische Modul eines Invariantenringes*, J. Algebra **127** (1989), 40–54.
63. Vladimir L. Popov, *Constructive invariant theory*, Astérisque **87–88** (1981), 303–334.
64. Vladimir L. Popov, *The constructive theory of invariants*, Math. USSR Izvest. **10** (1982), 359–376.

Chapter 3

Invariant Theory of Finite Groups

The invariant theory of finite groups has enjoyed considerable recent interest, as the appearance of the books by Benson [1], Smith [2], Neusel and Smith [3] and Campbell and Wehlau [4] and of numerous articles on the subject show. In this chapter we focus on computational aspects. As in Chap. 2, the central goal is the calculation of a finite set of generators for the invariant ring, but we will also address some interesting properties which invariant rings of finite groups may or may not have, and how they can be tackled algorithmically. Almost all algorithms treated in this chapter have implementations in various computer algebra systems. In fact, quite a few computer algebra packages for invariant theory were developed during the 1990s, among them the Invariant package [5] in MAS written by Manfred Göbel, the MAPLE package INVAR [6] written by the second author, the MAPLE package SYMMETRY [7] written by Karin Gatermann and F. Guyard, and the MuPAD package PerMuVAR [8] written by Nicolas Thiéry. We mention these packages only in passing, since they are not developed or maintained anymore. In fact, the “market” has consolidated somewhat in the mean time. We’d like to recommend two implementations of invariant theory algorithms that at the time of writing are actively maintained and that represent (or come close to) the state of the art of algorithms.

- The computer algebra system SINGULAR (see Decker et al. [9]) has three packages for invariant theory: finvar, authored by Agnes E. Heydtmann, for invariants of finite groups, ainvar, authored by Gerhard Pfister and Gert-Martin Greuel, for invariants of the additive group \mathbb{G}_a , and rinvar, authored by Thomas Bayer, for invariants of linearly reductive groups.
- The computer algebra system MAGMA (see Bosma et al. [10]) contains a substantial package for invariant theory. The focus is on invariants of finite groups, but algorithms for linearly reductive groups and for invariant fields were also added. Most of the implementation was written by Allan Steel with the collaboration of the second author.

As a further tool for research, a database of invariant rings has been provided by the IWR in Heidelberg (see Kemper et al. [11]). This database focuses on modular invariant rings of finite groups and is meant as a research tool for making experiments, testing and setting up conjectures, and generally for finding interesting examples. The database, together with retrieval software and documentation, is available upon request from the second author.

In this chapter K is a field and G is a finite group acting linearly on a finite dimensional vector space V over K . In other words, V is a module over the group ring KG . If the characteristic of K divides the group order $|G|$, we speak of the **modular case**. Otherwise, we are in the **nonmodular case**, which includes $\text{char}(K) = 0$. The number and degrees of generating invariants, as well as the properties of the invariant ring we will be interested in, do not change if we enlarge the ground field K . We may therefore assume that K is algebraically closed when this assumption is convenient, but we do not make it as a general assumption. Notice that if we regard G as a linear algebraic group, then every linear action on a vector space is rational. Since finite groups are (geometrically) reductive, it follows from Nagata's result (Theorem 2.2.16) that the invariant ring is finitely generated. There is, however, an older and much simpler argument due to Emmy Noether [12].

Proposition 3.0.1 *Let R be a finitely generated algebra over a Noetherian commutative ring K , and let G be a finite group acting on R by automorphisms fixing K elementwise. Then R^G is finitely generated as a K -algebra.*

Proof Let x_1, \dots, x_n be generators for R . The polynomial

$$\prod_{\sigma \in G} (T - \sigma \cdot x_i) = T^m + a_{i,1}T^{m-1} + \cdots + a_{i,m-1}T + a_{i,m} \in R^G[T]$$

provides an integral equation for x_i over R^G . Hence R is finitely generated as a module over the subalgebra $A := K[a_{1,1}, \dots, a_{n,m}]$ generated by the coefficients of these equations. Since A is Noetherian, R is Noetherian as an A -module, and hence the same is true for the submodule R^G . Therefore R^G is a finitely generated module over A . \square

Notice that the above proof is not constructive. The main goal of this chapter can be rephrased by saying that we want to turn the proof into a constructive method for finding generators.

3.1 Homogeneous Components

The most basic task in computational invariant theory is to compute invariants of some given degree d . Recall that the invariant ring $K[V]^G$ is a graded algebra, where $K[V]_d^G$ is the space of homogeneous invariants of degree d (see p. 32). The monomials of degree d in the variables x_1, \dots, x_n form a basis of $K[V]_d$, hence $\dim(K[V]_d) = \binom{n+d-1}{n-1}$, where $n = \dim(V)$.

3.1.1 The Linear Algebra Method

Let $H \leq G$ be a subgroup of G whose invariants of degree d are known (typically, the trivial group), and take a set $S(G/H) \subseteq G$ such that H together with $S(G/H)$ generates G . Take the $|S(G/H)|$ -fold direct sum of $K[V]$, whose components are indexed by the elements of $S(G/H)$, and consider the map

$$K[V]^H \rightarrow \bigoplus_{\sigma \in S(G/H)} K[V], f \mapsto (\sigma \cdot f - f)_{\sigma \in S(G/H)},$$

whose kernel is $K[V]^G$. This map is K -linear (in fact it is a homomorphism of modules over $K[V]^G$), and it preserves the grading. Restriction to the degree- d component yields a linear map $K[V]_d^H \rightarrow K[V]_d^{|S(G/H)|}$, whose kernel is $K[V]_d^G$. This map is explicitly given, so its kernel can be effectively calculated by solving a system of linear equations over K . For $H = 1$, the number of unknowns in this system is $\binom{n+d-1}{n-1}$, and the number of equations is $|S(G/H)| \cdot \binom{n+d-1}{n-1}$. This can become enormous for large values of n and d .

3.1.2 The Reynolds Operator

A further method for calculating the homogeneous component $K[V]_d^G$ is by means of the Reynolds operator, which is only available in the nonmodular case. Recall that for finite groups, the Reynolds operator is simply averaging over the group (see Example 2.2.3).

Algorithm 3.1.1 (available in the nonmodular case) Apply the Reynolds operator to all monomials in $K[V]$ of degree d . This yields a generating set of $K[V]_d^G$ as a vector space. By linear algebra, a basis can be extracted from this.

More generally, let $H \leq G$ be a subgroup such that the index $[G : H]$ is not divisible by the characteristic p of K . Then the **relative Reynolds operator** is defined as

$$\mathcal{R}_{G/H} : K[V]^H \rightarrow K[V]^G, f \mapsto \frac{1}{[G : H]} \sum_{\sigma \in G/H} \sigma \cdot f,$$

where G/H denotes a set of left coset representatives of H in G . $\mathcal{R}_{G/H}$ is independent of the choice of the coset representatives, and it is easily checked that it is a projection of modules over $K[V]^G$. In particular, the images under $\mathcal{R}_{G/H}$ of a basis of $K[V]_d^H$ generate the desired vector space $K[V]_d^G$. Again, it is a problem of linear algebra to select a basis of $K[V]_d^G$ from a generating set. Carrying this idea further, we can also use a chain $H = G_1 < G_2 < \dots < G_{r-1} < G_r = G$ of subgroups. Then $\mathcal{R}_{G/H} = \mathcal{R}_{G_r/G_{r-1}} \circ \dots \circ \mathcal{R}_{G_2/G_1}$, and applying $\mathcal{R}_{G/H}$ to an $f \in K[V]^H$ by composing

the $\mathcal{R}_{G_i/G_{i-1}}$ only requires $\sum_{i=2}^r [G_i : G_{i-1}]$ applications of group elements and even fewer summations. If we want to compute $K[V]_d^G$ with this method, we have the additional benefit that we can select a vector space basis of $K[V]_d^{G_i}$ after having applied $\mathcal{R}_{G_i/G_{i-1}}$ to a basis of $K[V]_d^{G_{i-1}}$, so we need to apply the subsequent relative Reynolds operators to fewer elements.

In the nonmodular case there is a choice between using Algorithm 3.1.1 or the linear algebra method for calculating homogeneous invariants. Kemper and Steel [13] analyzed the computational cost of both approaches. The general tendency is that the Reynolds operator performs better for small $|G|$ and large d .

3.2 Noether's Degree Bound

In Sect. 2.1 after (2.1.1), we mentioned that an a priori upper bound on the degree $\beta(K[V]^G)$ required for generating $K[V]^G$ leads to an algorithm for computing $K[V]^G$: using the methods from Sect. 3.1, compute all invariants up to the degree bound and then, if desired, delete superfluous generators from these by linear algebra. All that is needed for this approach is linear algebra and polynomial arithmetic. Although this algorithm is far from being efficient in most cases, degree bounds have enjoyed considerable interest in all periods of invariant theory.

In this section we will prove that the invariant ring of a finite group G can be generated by homogeneous invariants of degree at most the group order $|G|$, provided that the characteristic of the ground field K does not divide $|G|$. This was proved by Noether [14] in the case that $p := \text{char}(K)$ is zero or bigger than $|G|$. For the case that p is smaller than $|G|$ but $p \nmid |G|$, the question whether Noether's bound always holds (known as the ‘‘Noether gap’’) was open for quite a while. It was never seriously doubted that this is true, but the lack of a proof was for many years an irritating problem, since in almost all other aspects the invariant theory in coprime characteristic parallels that in characteristic zero. (The only remaining notable exception from this rule that we are aware of is Weyl's polarization theorem.) Partial results were obtained by Smith [15] and Richman [16], who independently proved the bound for solvable groups. See also Fleischmann and Lempken [17], Smith [18]. Then Fleischmann [19] and Fogarty [20] independently found proofs for the general statement and thus resolved the Noether gap. Subsequently these proofs were substantially simplified by D. Benson [21]. We will present a version of this simplification. It is in many ways similar to Noether's original proof, in that it is elementary and surprisingly simple, with a little touch of ingenuity, and gives a constructive way to express any invariant in terms of invariants of degree at most $|G|$. We are grateful to David Benson for giving us the permission to include the proof here.

We start by the following lemma, which asserts as a special case that if $p \nmid |G|$, then every homogeneous polynomial of degree at least $|G|$ lies in the ‘‘Hilbert ideal’’ $(K[V]_+^G) K[V]$.

Lemma 3.2.1 (Benson [21], Fogarty [20, Equation (1)]) *Let A be a commutative ring with unit, G a finite group of automorphisms of A , and $I \subseteq A$ a G -stable ideal. If the order of G is invertible in A , then*

$$I^{|G|} \subseteq I^G A.$$

Proof Let $\prod_{\sigma \in G} f_\sigma$ be a product of $|G|$ elements of I , indexed by $\sigma \in G$. For every $\tau \in G$ we have

$$\prod_{\sigma \in G} ((\tau\sigma) \cdot f_\sigma) - f_\sigma = 0.$$

Multiplying this out and summing over all $\tau \in G$ yields

$$\sum_{M \subseteq G} (-1)^{|G \setminus M|} \left(\sum_{\tau \in G} \prod_{\sigma \in M} \tau(\sigma f_\sigma) \right) \cdot \left(\prod_{\sigma \in G \setminus M} f_\sigma \right) = 0. \quad (3.2.1)$$

The summand for $M = \emptyset$ is $\pm |G| \cdot \prod_{\sigma \in G} f_\sigma$, and all other summands lie in $I^G A$. Thus $\prod_{\sigma \in G} f_\sigma \in I^G A$, and the lemma is proved. \square

If we put $A = K[V]$ and $I = K[V]_+$, then Lemma 3.2.1 tells us that every homogeneous polynomial of degree $\geq |G|$ lies in the Hilbert ideal $J := (K[V]_+^G) K[V]$, so J is generated in degrees $\leq |G|$. From this the Noether bound for $K[V]^G$ follows by Hilbert's classical argument (see Theorem 2.2.10). So the proof for the most basic version of the Noether bound is already complete! Nevertheless, we will work a little bit harder to derive a bound which also holds for equivariants. Recall that $(K[V] \otimes_K W)^G$ (with W another KG -module) is the module of equivariants, whose elements can be viewed as polynomial functions $V \rightarrow W$ which commute with the G -actions. In fact, we generalize even further and consider the following situation. Let R be a commutative ring with unit and let $A = \bigoplus_{d=0}^{\infty} A_d$ be a graded, commutative R -algebra with unit. As usual, we write $\beta(A)$ for the least integer k such that A is generated by homogeneous elements of degree at most k as an R -algebra, or $\beta(A) = \infty$ if no such k exists. Let G be a finite group acting on A by degree-preserving R -automorphisms, and let W be an RG -module. We make $A \otimes_R W$ into a graded A -module by setting $(A \otimes_R W)_d := A_d \otimes_R W$. Thus A^G is a graded R -algebra, and $(A \otimes_R W)^G$ is a graded A^G -module. We will prove:

Theorem 3.2.2 *In the above situation, suppose that $|G|$ is invertible in R . Then the following statements hold:*

- (a) $\beta(A^G) \leq |G| \cdot \beta(A)$.
- (b) $(A \otimes_R W)^G$ is generated as an A^G -module by homogeneous elements of degree at most $(|G| - 1) \cdot \beta(A)$.

Proof Write $M := A \otimes_R W$, $\beta := \beta(A)$, and $g := |G|$. Let B be the subalgebra of A^G generated by all homogeneous elements of degree at most $g\beta$. We prove that M^G

is generated as a B -module by homogeneous elements of degree at most $(g - 1)\beta$. From this (a) (as the special case $W = R$) and (b) will follow.

Let $d > (g - 1)\beta$ be an integer. Any element from M_d can be written as a sum of products of the form $t \otimes w$, where $w \in W$ and $t = f_1 \cdots f_k$ is a product of homogeneous elements $f_i \in A_{\leq \beta}$ (i.e., $\deg(f_i) \leq \beta$) with $\deg(t) = d$. For such a product t , the sequence f_1, \dots, f_k contains at least g elements lying in A_+ , say f_1, \dots, f_g . By Lemma 3.2.1, and since $\deg(f_1 \cdots f_g) \leq g\beta$, we obtain $f_1 \cdots f_g \in B_+A$ and therefore $t \in B_+A_{<d}$. We conclude that $M_d \subseteq B_+M_{<d}$. By induction this yields $M = BM_{\leq(g-1)\beta}$. Now by applying the Reynolds operator $\mathcal{R}: M \rightarrow M^G$ we get

$$M^G = \mathcal{R}(M) = B\mathcal{R}(M_{\leq(g-1)\beta}) = BM_{\leq(g-1)\beta}^G,$$

as claimed. \square

In the situation where G acts on vector spaces V and W over a field K we obtain:

Corollary 3.2.3 *Let G be a group and V a finite dimensional representation of G over a field K . Moreover, let $N \trianglelefteq G$ be a normal subgroup of finite index $[G : N]$ such that $\text{char}(K) \nmid [G : N]$. Then we have*

- (a) $\beta(K[V]^G) \leq [G : N] \cdot \beta(K[V]^N)$.
- (b) *If W is another finite dimensional representation over K with $W^N = W$, then the module $(K[V] \otimes_K W)^G$ of equivariants is generated over $K[V]^G$ by homogeneous elements of degree at most $([G : N] - 1) \cdot \beta(K[V]^N)$.*

Proof G/N acts on $A := K[V]^N$ and on W , and we have

$$(K[V] \otimes_K W)^G = (A \otimes_K W)^{G/N}.$$

Now the result follows from Theorem 3.2.2. \square

Corollary 3.2.4 (Noether, Fleischmann, Benson, Fogarty) *Suppose that $\text{char}(K) \nmid |G|$. Then*

$$\beta(K[V]^G) \leq |G|.$$

Remark 3.2.5

- (a) As observed by Peter Fleischmann, one can also consider the summand for $M = G$ in Eq. (3.2.1). This summand is $\sum_{\tau \in G} \tau (\prod_{\sigma \in G} \sigma \cdot f_\sigma)$, and equating it to the negative of the remaining summands yields the inclusion

$$\text{Tr}_G(I^{|G|}) \subseteq A^G I, \quad (3.2.2)$$

where Tr_G denotes the transfer map (or trace) $A \rightarrow A^G$, $f \mapsto \sum_{\tau \in G} \tau \cdot f$. The inclusion (3.2.2) holds in any characteristic, and is of interest in itself. For example, in the nonmodular case the Noether bound can be derived from (3.2.2) by applying the Reynolds operator to it.

- (b) It is reasonable to ask if Corollary 3.2.3(a) also holds if N is no longer assumed to be normal. This is true if $|G|!$ is invertible in K (i.e., $\text{char}(K) = 0$ or $> |G|$, see Schmid [22, Lemma 3.2] or Smith [2, Theorem 2.4.2]). Unfortunately, the proof given above and the one by Fleischmann [19] fail if N is not normal. So there is still a “baby Noether gap” left. \triangleleft

We add two conjectures which generalize Corollary 3.2.4.

Conjecture 3.2.6

- (a) If $K[V]^G$ is Cohen-Macaulay, then $\beta(K[V]^G) \leq |G|$.
(b) Let $I = (K[V]_+^G) K[V]$ be the Hilbert ideal. Then I is generated by homogeneous elements of degree at most $|G|$.

We have plenty of computational evidence for both conjectures. It is particularly striking that we found Conjecture 3.2.6(b) to be true in cases where $\beta(K[V]^G)$ exceeded $|G|$ by far (see Sect. 3.3.1). For example, it can be seen by inspection of the generators given by Campbell and Hughes [23] that the conjecture is true for vector invariants of the indecomposable two-dimensional representation of the cyclic group of order p over $K = \mathbb{F}_p$. Moreover, it was shown by Fleischmann [19, Theorem 4.1] that Conjecture 3.2.6(b) is true if V is a permutation module or, more generally, a trivial source module. Sezer [24] confirmed the conjecture for all indecomposable representations of cyclic groups of prime order.

Remark 3.2.7 One might be tempted to conjecture that Lemma 3.2.1 might also hold in the modular case. However, this is not true. As an example, consider the group

$$G := \left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{pmatrix} \right\rangle \leq \text{GL}_4(\mathbb{F}_2)$$

of order 2. The invariant ring is generated by $x_1, x_3, x_2(x_1 + x_2), x_4(x_3 + x_4)$, and $x_1x_4 + x_2x_3$. Thus the Hilbert ideal is $I := (x_1, x_3, x_2^2, x_4^2)$, hence $x_2x_4 \notin I$. \triangleleft

Improvements of Noether's Bound.

Noether's degree bound is sharp in the sense that no better bound can be given in terms of only the group order—just consider the example of the cyclic group of order n , coprime to $\text{char}(K)$, acting on a one-dimensional vector space by multiplication with a primitive n -th root of unity. However, it was shown by Schmid [22] that if G is not cyclic and $\text{char}(K) = 0$, then $\beta(K[V]^G) < |G|$. Schmid's methods were sharpened by Domokos and Hegedűs [25], who were able to prove the following surprisingly explicit result, which was generalized to the nonmodular case by Sezer [26]:

Theorem 3.2.8 (Domokos and Hegedűs, Sezer) *Let G be a finite, noncyclic group acting on a finite-dimensional vector space V over a field K with $\text{char}(K) \nmid |G|$. Then*

$$\beta(K[V]^G) \leq \begin{cases} \frac{3}{4}|G| & \text{if } |G| \text{ is even,} \\ \frac{5}{8}|G| & \text{if } |G| \text{ is odd} \end{cases}.$$

3.3 Degree Bounds in the Modular Case

The following example shows that Noether's bound does not always hold in the modular case.

Example 3.3.1 Let $G \cong C_2$ act on $R := \mathbb{F}_2[x_1, x_2, x_3, y_1, y_2, y_3]$ by interchanging the x_i and y_i . Consider the ideal $I = (x_i^2, y_i^2, x_i y_i \mid i = 1, 2, 3) \subseteq R$. The four invariants

$$x_1 x_2 x_3 + y_1 y_2 y_3, \quad x_1 x_2 y_3 + y_1 y_2 x_3, \quad x_1 y_2 x_3 + y_1 x_2 y_3, \quad \text{and } y_1 x_2 x_3 + x_1 y_2 y_3$$

are linearly independent modulo I . If R^G were generated in degree at most 2, there would exist at least four products of an invariant of degree 1 and an invariant of degree 2 that are linearly independent modulo I . The vector space of invariants of degree 1 is spanned by the $s_i := x_i + y_i$ ($i = 1, 2, 3$). Modulo I , the vector space of invariants of degree 2 is spanned by

$$u_{i,j} := x_i y_j + x_j y_i \quad \text{and} \quad x_i x_j + y_i y_j = s_i s_j + u_{i,j} \quad (1 \leq i < j \leq 3).$$

Since $s_i u_{i,j} \in I$ and so on, it follows that every product of an invariant of degree 1 and an invariant of degree 2 is contained in

$$\langle s_1 s_2 s_3, s_1 u_{2,3}, s_2 u_{1,3}, s_3 u_{1,2} \rangle_{\mathbb{F}_2} + I.$$

Now the relation

$$s_1 u_{2,3} + s_2 u_{1,3} + s_3 u_{1,2} = \det \begin{pmatrix} s_1 & s_2 & s_3 \\ x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix} = 0 \tag{3.3.1}$$

shows that there cannot exist four products of an invariant of degree 1 and an invariant of degree 2 that are linearly independent modulo I . It follows that Noether's degree bound fails for R^G .

It may be interesting to see an explicit invariant of degree 3 that cannot be expressed as a polynomial in invariants of smaller degree. Forming leading monomials with respect to the lexicographic monomial ordering with $x_1 > x_2 >$

$x_3 > y_1 > y_2 > y_3$, we obtain $\text{LM}(s_1 s_2 s_3) = x_1 x_2 x_3$, $\text{LM}(s_1 u_{2,3}) = x_1 x_2 y_3$, $\text{LM}(s_3 u_{1,2}) = x_1 x_3 y_2$, and $\text{LM}(y_1 x_2 x_3 + x_1 y_2 y_3) = x_1 y_2 y_3$. The distinctness shows that the four invariants are linearly independent modulo I , so $f := y_1 x_2 x_3 + x_1 y_2 y_3$ cannot be expressed by invariants of smaller degree. We will compute generators of R^G in Example 3.7.6(a). \triangleleft

This raises the question how badly Noether's bound fails, and if any a priori bound in the modular case exists. These questions will be answered in this section. First we prove (a special case of) Richman's lower degree bound, which implies that in the modular case there cannot exist an upper degree bound depending only on the group order. Then we present Symonds' upper bound, a very useful a priori upper bound depending only on the group order and the dimension of the representation.

3.3.1 Richman's Lower Degree Bound

It was quite a surprise when in 1990 Richman [27] proved that for the two-dimensional indecomposable module V of the cyclic group $G := C_p$ over a field of characteristic p the vector invariants have the property $\beta(K[V^m]^G) \geq m(p-1)$, where V^m is the direct sum of m copies of V . (Later, equality was proved by Campbell and Hughes [23]. A special case is shown in Example 3.3.1.) Richman proved similar results for another class of groups, which contains the general and special linear groups over a finite field. Then in [28], which was written in 1990 but not published until 1996, he proved that for any group G of order divisible by $p := \text{char}(K)$ and for any faithful, finite dimensional KG -module V the beta number $\beta(K[V^m]^G)$ tends to infinity with m . We will present a short and elementary proof for this statement in the case that $K = \mathbb{F}_p$ is a prime field. This proof was shown to us by Ian Hughes.

We start by fixing an element $\sigma \in G$ whose order is $p = \text{char}(K)$. There exists a basis $x_1, \dots, x_n \in V^*$ such that σ is in Jordan canonical form with respect to this basis. Reordering the x_i and writing $\{x_{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq n\}$ for the corresponding basis of $(V^m)^*$, we obtain

$$\sigma \cdot x_{i,j} = x_{i,j} + \epsilon_j x_{i,j-1} \quad \text{with} \quad \epsilon_j \in \{0, 1\}, \quad \epsilon_n = 1, \quad \epsilon_1 = 0. \quad (3.3.2)$$

Lemma 3.3.2 *Let $t = \prod_{i=1}^m x_{i,n}^{e_i}$ be a monomial in $K[x_{1,n}, \dots, x_{m,n}] \subseteq K[V^m]$. If t occurs in an invariant, then all exponents e_i are divisible by p .*

Proof For $f, g \in K[V^m]$ we have

$$(\sigma - 1)(fg) = \sigma \cdot f \cdot (\sigma - 1)g + g \cdot (\sigma - 1)f. \quad (3.3.3)$$

Let $J \subset K[V^m]$ be the ideal generated by all $x_{i,j}$ with $1 \leq i \leq m$ and $1 \leq j \leq n-1$. Then (3.3.2), (3.3.3), and induction on the degree yield $(\sigma - 1)K[V^m] \subseteq J$. Now let

$I \subset K[V^m]$ be the ideal generated by

$$\{x_{i,j} \mid 1 \leq i \leq m, 1 \leq j \leq n-2\} \cup \{x_{i,n-1}^2 \mid 1 \leq i \leq m\}.$$

We have $\sigma \cdot I \subseteq I$ and $J^2 \subseteq I$. Thus $(\sigma - 1)f \cdot (\sigma - 1)g \in I$ for $f, g \in K[V^m]$, so (3.3.3) shows that $\sigma - 1$ acts as a derivation on $K[V^m]/I$.

Take any $f \in K[V^m]$. Then $f \equiv h + \sum_{i=1}^m x_{i,n-1} g_i \pmod{I}$ with $h, g_i \in K[x_{1,n}, \dots, x_{m,n}]$. Using that $\sigma - 1$ is a derivation modulo I , we easily obtain

$$(\sigma - 1)f \equiv (\sigma - 1)h \pmod{I}.$$

For a monomial $t = \prod_{i=1}^m x_{i,n}^{e_i}$ in h we have

$$(\sigma - 1)t \equiv \sum_{i=1}^m e_i x_{i,n-1} \cdot t/x_{i,n} \pmod{I}.$$

If f is an invariant and $h = \sum_{e_1, \dots, e_n} \alpha_{e_1, \dots, e_n} \prod_{i=1}^m x_i^{e_i}$ with $\alpha_{e_1, \dots, e_n} \in K$, then

$$0 = (\sigma - 1)f \equiv (\sigma - 1)h \equiv \sum_{e_1, \dots, e_n} \alpha_{e_1, \dots, e_n} \sum_{i=1}^m e_i x_{i,n-1} x_{i,n}^{-1} \prod_{k=1}^m x_k^{e_k} \pmod{I}.$$

From this we see that $\alpha_{e_1, \dots, e_n} = 0$ if any e_i is not divisible by p . This concludes the proof. \square

We can now prove the lower degree bound.

Theorem 3.3.3 (Richman [28]) *Suppose that $K = \mathbb{F}_p$ and G is a group of order divisible by p . If G acts faithfully on the K -space V of dimension n , then*

$$\beta(K[V^m]^G) \geq \frac{m}{n-1}.$$

Proof Consider the polynomial

$$f = \sum_{\alpha_1, \dots, \alpha_n \in K} \prod_{i=1}^m (\alpha_1 x_{i,1} + \dots + \alpha_n x_{i,n})^{p-1},$$

which clearly is an invariant. We may assume that $m \geq n$. The coefficient of the monomial

$$t = \prod_{i=1}^{n-1} x_{i,i}^{p-1} \cdot \prod_{i=n}^m x_{i,n}^{p-1}$$

$\inf f$ is

$$\sum_{\alpha_1, \dots, \alpha_n \in K} \prod_{i=1}^{n-1} \alpha_i^{p-1} \cdot \alpha_n^{(m-n+1)(p-1)} = \sum_{\alpha_1, \dots, \alpha_n \in K^*} 1 = (p-1)^n \neq 0,$$

so t occurs in f . Suppose that we have a set of homogeneous generators of $K[V]^G$, then

$$t = t_1 \cdot t_2 \cdots t_r \quad (3.3.4)$$

with t_i monomials occurring in elements of this generating set. We are done if we can show that $\deg(t_k) \geq m/(n-1)$ for some k . Assume that a t_i lies in $K[x_{1,n}, \dots, x_{m,n}]$, then by Lemma 3.3.2 all exponents of t_i must be divisible by p , which is impossible since t_i is a divisor of t by (3.3.4). Hence

$$\deg_{n'}(t_i) > 0 \quad \text{for all } i = 1, \dots, r,$$

where we write $\deg_{n'}(\prod_{i,j} x_{i,j}^{e_{i,j}}) = \sum_{i=1}^m \sum_{j=1}^{n-1} e_{i,j}$. With $u_i := \deg(t_i)$ and $v_i := \deg_{n'}(t_i)$, we have that

$$\frac{u_k}{v_k} \geq \frac{\sum_{i=1}^r u_i}{\sum_{i=1}^r v_i} \quad \text{for some } k = 1, \dots, r, \quad (3.3.5)$$

since otherwise $u_k \cdot \sum_{i=1}^r v_i < v_k \cdot \sum_{i=1}^r u_i$ for all k , and summing over k would yield the contradiction

$$\sum_{k=1}^r u_k \cdot \sum_{i=1}^r v_i < \sum_{k=1}^r v_k \cdot \sum_{i=1}^r u_i.$$

But from (3.3.4) we get that

$$\sum_{i=1}^r u_i = \deg(t) = m(p-1) \quad \text{and} \quad \sum_{i=1}^r v_i = \deg_{n'}(t) = (n-1)(p-1),$$

hence (3.3.5) yields

$$\deg(t_k) = u_k \geq v_k \cdot \frac{m(p-1)}{(n-1)(p-1)} \geq \frac{m}{n-1}.$$

This completes the proof. \square

Let G be a finite group and K a field. We say that (G, K) has a **global degree bound** k if there exists an integer k such that $\beta(K[V]^G) \leq k$ holds for all finite dimensional KG -modules V .

Corollary 3.3.4 *Let G be a finite group and K a field. Then (G, K) has a global degree bound if and only if $\text{char}(K) \nmid |G|$.*

Proof One direction follows from Noether's bound (Corollary 3.2.4), and the other from Theorem 3.3.3, since G has a faithful representation defined over \mathbb{F}_p , for example the regular representation. \square

Remark 3.3.5

- (a) The largest part of Richman's paper [28] is devoted to obtaining a lower degree bound for vector invariants, where the hypothesis that K is the prime field is dropped. The result is

$$\beta(K[V^m]^G) \geq \frac{m(p-1)}{p^{|G|-1} - 1}.$$

What we have presented above is a simplified version of the first part of [28]. The above bound (and the bound from Theorem 3.3.3) was improved by Kemper [29] for the case that G acts by permuting basis of V : Then the bound

$$\beta(K[V^m]^G) \geq m(p-1)$$

holds. This bound is known to be sharp if $G = S_p$ is the symmetric group on $p = n$ letters and $m > 1$ (see Fleischmann [30]).

- (b) Corollary 3.3.4 was generalized by Bryant and Kemper [31], who proved that a linear algebraic group G over a field K has a global degree bound if and only if G is finite and $\text{char}(K) \nmid |G|$. \triangleleft

3.3.2 Symonds' Degree Bound

Perhaps the most significant contribution to invariant theory in recent years has been Symonds' bound, an a priory upper bound for the degrees of generators of $K[V]^G$ that only depends on $|G|$ and $\dim(V)$. In comparison to the now obsolete bound that appeared in the first edition of this book, Symonds' bound is useful and realistic, in particular since it is really a bound for the degrees of secondary invariants.

Theorem 3.3.6 (Symonds [32]) *Let G be a nontrivial, finite group acting linearly on a vector space V over a field K of dimension $n \geq 2$. Then*

$$\beta(K[V]^G) \leq n(|G| - 1).$$

The theorem is a consequence of the following degree bound for secondary invariants:

Theorem 3.3.7 ([32]) *Let G be a finite group acting linearly on a vector space over a field K of dimension n . If $f_1, \dots, f_n \in K[V]^G$ are primary invariants, then there exist secondary invariants $g_i \in K[V]^G$ such that*

$$\deg(g_i) \leq \sum_{i=1}^n (\deg(f_i) - 1).$$

Theorem 3.3.6 follows from Theorem 3.3.7 since, as we will show in Sect. 3.5.1, there always exist primary invariants of degree bounded above by $|G|$, provided that K has enough elements. The latter condition can always be achieved by passing to an algebraic closure, which does not change $\beta(K[V]^G)$. The bound in Theorem 3.3.7 is sharp. In fact, it is attained in many (we are almost tempted to say: in most) instances, such as Example 2.7.5. Apart from degree bounds for the generators (and secondary invariants), the paper also gives good degree bounds for the algebraic relations between the generators.

Both of the above theorems were conjectured by many people, see for instance [33]. In the nonmodular case, they follow easily from the Cohen-Macaulay property and Molien's formula (see Sects. 3.4.1 and 3.7.1). Before Symonds' work, Theorem 3.3.7 was proved for permutation modules with the elementary symmetric polynomials as primary invariants by Göbel [34] (see Sect. 3.10.2). Both theorems were proved by Campbell et al. [35] under the hypothesis that $K[V]^G$ is Gorenstein, and then by Broer [36] under the hypothesis that $K[V]^G$ is Cohen-Macaulay. Theorem 3.3.6 was proved under the hypothesis that $|G|$ is not divisible by $\text{char}(K)^2$ by Hughes and Kemper [37]. All these partial results require much less sophisticated methods than the full results. In fact, the original proof of Theorems 3.3.6 and 3.3.7 in itself is not extremely long, but it makes heavy use of the machinery set up by Karagueuzian and Symonds in the paper [38]. This paper proves the (also very interesting) result that in the setting of Theorem 3.3.7 only finitely many isomorphism types of indecomposable KG -modules occur in the polynomial ring $K[V]$.

Because of the amount of machinery used in the proof, we will not make any attempt to present the ideas here. But we direct the reader to Symonds [39] for an easier proof. As we will see in Sect. 3.7.2, Theorem 3.3.7 gives rise to an easy and rather efficient algorithm for computing secondary invariants in the modular case.

3.4 Molien's Formula

For the computation of the homogeneous invariants of degree d by using the Reynolds operator, it would be a great advantage to know the dimension of $K[V]^G_d$ a priori. These dimensions are encoded in the Hilbert series $H(K[V]^G, t)$ (see Definition 1.4.1). In later sections, especially Sects. 3.5 and 3.7, we will see many more uses of the Hilbert series. In this section we prove Molien's formula, which

holds in the nonmodular case and gives a way for computing the Hilbert series without touching a single invariant. Then we investigate generalizations to the modular case.

3.4.1 Characters and Molien's Formula

We start with the following definitions: If V is a finite dimensional module over the group ring KG , we consider the *sigma-series*

$$\sigma_t(V) := \sum_{d=0}^{\infty} K[V]_d \cdot t^d,$$

which is a formal power series with KG -modules as coefficients. (More precisely, $\sigma_t(V)$ is a formal power series over the representation ring of KG , which by definition is the free \mathbb{Z} -module generated by the isomorphism classes of indecomposable KG -modules). Let p be the characteristic of K (which may be zero) and set $|G| = p^a m$ with $p \nmid m$. Choose an isomorphism between the m -th roots of unity in an algebraic closure \bar{K} and in \mathbb{C} . For $\tau \in G_{p'}$, the subset of G consisting of the elements of order not divisible by p , we can use this isomorphism to lift the eigenvalues of the τ -action on V to characteristic 0. If $\lambda_1, \dots, \lambda_n \in \mathbb{C}$ are the lifted eigenvalues, we define the **Brauer character** as

$$\Phi_\tau(V) := \lambda_1 + \dots + \lambda_n$$

(see, for example, Curtis and Reiner [40, p. 420]), and moreover

$$\det_V^0(1 - t\tau) := (1 - t\lambda_1) \cdots (1 - t\lambda_n) \in \mathbb{C}[t].$$

Of course we can take the usual trace and the usual determinant of $1 - t\tau$ if K has characteristic 0. We can now apply Φ_τ to $\sigma_t(V)$ coefficient-wise, which yields a formal power series over \mathbb{C} .

Lemma 3.4.1 *Let $\tau \in G_{p'}$ be an element of order not divisible by $p = \text{char}(K)$. Then with the above notation we have*

$$\Phi_\tau(\sigma_t(V)) = \frac{1}{\det_V^0(1 - t \cdot \tau^{-1})}. \quad (3.4.1)$$

Proof First note that neither side of (3.4.1) changes if we replace K by its algebraic closure \bar{K} . Hence we may assume K to be algebraically closed. As functions of V , both sides of the equality remain unchanged if we restrict V to the subgroup generated by τ . Hence we can assume that G is cyclic of order coprime to $\text{char}(K)$. Also observe that for finite dimensional KG -modules U and V we have

$K[U \oplus V] = K[U] \otimes_K K[V]$, hence $\sigma_t(U \oplus V) = \sigma_t(U) \cdot \sigma_t(V)$, where multiplication of the coefficients is given by the tensor product. Moreover, Φ_τ is additive and multiplicative. It follows that

$$\Phi_\tau(\sigma_t(U \oplus V)) = \Phi_\tau(\sigma_t(U)) \cdot \Phi_\tau(\sigma_t(V)).$$

The same rule holds for the right-hand side of (3.4.1). Hence we can also assume that V is an indecomposable KG -module, hence it is one-dimensional. But then (3.4.1) is clearly true. \square

We can now prove Molien's formula.

Theorem 3.4.2 (Molien's formula) *Let G be a finite group acting on a finite dimensional vector space V over a field K of characteristic not dividing $|G|$. Then*

$$H(K[V]^G, t) = \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\det_V^0(1 - t \cdot \sigma)}.$$

If K has characteristic 0, then $\det_V^0(1 - t \cdot \sigma)$ can be substituted by $\det_V(1 - t \cdot \sigma)$.

Proof By character theory (see Curtis and Reiner [40, Theorem 18.23]), the operator

$$T(U) = \frac{1}{|G|} \sum_{\sigma \in G} \Phi_\sigma(U)$$

counts the multiplicity of the trivial representation in a KG -module U . Therefore

$$H(K[V]^G, t) = T(\sigma_t(V)),$$

from which Molien's formula follows by Lemma 3.4.1. \square

Because of the great importance of Molien's theorem, the Hilbert series of an invariant ring is sometimes also called the Molien series. Molien's formula is very easy to evaluate in practice. In fact, its summands only depend on the conjugacy class of σ , hence the summation over all elements of G is in fact a summation over the conjugacy classes. Moreover, for any $\sigma \in G$ the coefficients of $\det_V(1 - t \cdot \sigma)$ are (up to signs) the elementary symmetric polynomials in the (lifted) eigenvalues of σ , and these can be expressed in terms of the power sums of the eigenvalues by using Newton's formulae (see Curtis and Reiner [40, p. 314]). But the i -th power sum of lifted eigenvalues of σ is nothing but $\Phi_{\sigma^i}(V)$. Hence there exists a polynomial F_n over \mathbb{Q} in $n + 1$ variables such that $\det_V^0(1 - t \cdot \sigma) = F_n(\Phi_\sigma(V), \dots, \Phi_{\sigma^n}(V), t)$. In other words, we can evaluate Molien's formula if we only know the Brauer character associated to V and the power maps of G , and we do not even have to compute any determinants!

Remark 3.4.3 Suppose that W is another finite dimensional KG -module. Then the following modification of Molien's formula yields the Hilbert series of the module

$(K[V] \otimes_K W)^G$ of equivariants (also called covariants):

$$H((K[V] \otimes_K W)^G, t) = \frac{1}{|G|} \sum_{\sigma \in G} \frac{\Phi_{\sigma^{-1}}(W)}{\det_V^0(1 - t \cdot \sigma)}.$$

This is proved in a similar way as Theorem 3.4.2. Further modifications exist, for example for the case that the polynomial ring $K[V]$ is replaced by the exterior algebra $\Lambda(V)$. \triangleleft

3.4.2 Extensions to the Modular Case

In general, there appears to be no way to get anything similar to Molien's formula in the modular case. But for some special cases, there are extensions.

The first of these is the case that the order $|G|$ is divisible by $p = \text{char}(K)$, but not by p^2 . This case was considered by Hughes and Kemper [41], who gave a “recipe” for computing the Hilbert series $H(K[V]^G, t)$ that has much in common with Molien's formula, although it is more complicated and harder to prove. This generalizes work by Almkvist and Fossum [42], who proved formulas for the case of the cyclic group of order p acting on an indecomposable module. We will give an outline of the recipe from [41] and the ideas behind them.

An important observation in the proof of Lemma 3.4.1 was that the map Φ_σ assigning to each KG -module its Brauer character evaluated at the (fixed) element $\sigma \in G$ provides a homomorphism from the representation ring of KG to \mathbb{C} . Such homomorphisms are called *species*, so every (conjugacy class of an) element of G gives rise to a species. These turn out to be useful only for $\sigma \in G_p$. We sketch how further species can be constructed. Choose a Sylow p -subgroup $P \subseteq G$ (which by assumption is cyclic of order p) and let $N = N_G(P)$ be the normalizer. It is not hard to work out the representation ring of KN , and from this the set of species of KN . This is interesting since composing the restriction map to N with a species of KN gives a species of KG , so we have a source of additional species. Omitting the exact definition, we just mention that these additional species can be conveniently parametrized by elements $\tau \in H$ and by integers k with $1 \leq k < p$. We write them as $\Psi_{\tau,k}$.

A crucial element in the proof of Molien's formula is the fact that in the non-modular case, the “averaging operator” $T = |G|^{-1} \sum_{\sigma \in G} \Phi_\sigma$ “counts invariants,” i.e., $T(U) = \dim(U^G)$ for every KG -module U . In the case considered here, there exists a more complicated averaging operator that counts invariants in the same sense. In order to describe it, we consider the factor group $H := N/P$ and choose a primitive root w modulo p . For $\tau \in H$ and $\rho \in P$ we can write $\tau\rho\tau^{-1} = \rho^{w^{m_\tau}}$ with $0 \leq m_\tau \leq p-2$. With the complex $2p(p-1)$ st root of unity $\zeta := e^{\pi i/(p(p-1))}$, the

averaging operator is given by

$$T = \frac{1}{|G|} \sum_{\sigma \in G_{p'}} \Phi_\sigma - \frac{1}{2p|H|} \sum_{\tau \in H} \sum_{k=1}^{p-1} \frac{(\zeta^{(p-1)k} - \zeta^{-(p-1)k})^2}{(1 - \zeta^{pm_\tau + (p-1)k})(1 - \zeta^{pm_\tau - (p-1)k})} \cdot \Psi_{\tau,k}. \quad (3.4.2)$$

Since

$$H(K[V]^G, t) = T(\sigma_t(V)) \quad (3.4.3)$$

with $\sigma_t(V)$ the sigma-series, the next task is to evaluate the $\Phi_\sigma(\sigma_t(V))$ and $\Psi_{\tau,k}(\sigma_t(V))$. The $\Phi_\sigma(\sigma_t(V))$ were already taken care of in Lemma 3.4.1. For evaluating $\Psi_{\tau,k}(\sigma_t(V))$ we take advantage of the fact that $\Psi_{\tau,k}$ factors through the restriction map to the subgroup N , which we express as $\Psi_{\tau,k}(V) = \Psi_{\tau,k}(V|_N)$. Moreover, if $V|_N = U_1 \oplus U_2$, then

$$\begin{aligned} \Psi_{\tau,k}(\sigma_t(V)) &= \Psi_{\tau,k}(\sigma_t(U_1 \oplus U_2)) = \\ \Psi_{\tau,k}(\sigma_t(U_1) \cdot \sigma_t(U_2)) &= \Psi_{\tau,k}(\sigma_t(U_1)) \cdot \Psi_{\tau,k}(\sigma_t(U_2)), \end{aligned} \quad (3.4.4)$$

where the last equality holds since $\Psi_{\tau,k}$ is a ring homomorphism. The simple structure of N makes it easy to decompose the restriction of V as a direct sum of indecomposable KN -modules, so we are reduced to the situation where $G = N$ (i.e., G has a normal Sylow p -subgroup) and V is indecomposable. In this case the indecomposable modules are well known: They are all given as $V_n \otimes_K V_\chi$, where V_n is n -dimensional ($1 \leq n \leq p$) with a 1-dimensional trivial socle and P acting by a full Jordan block, and V_χ is the KH -module belonging to an irreducible Brauer character χ . Hughes and Kemper [41] proved a formulas for $\Psi_{\tau,k}(\sigma_t(V_n \otimes V_\chi))$, which we show here only for $\chi = 1$ to give the reader an impression:

$$\Psi_{\tau,k}(\sigma_t(V_{n+1})) = \frac{1 - (-1)^{nk} \zeta^{np^2 m_\tau} \cdot t^p}{1 - t^p} \prod_{j=0}^n (1 - \zeta^{npm_\tau + (n-2j)(p-1)k} \cdot t)^{-1}.$$

The formula for $\Psi_{\tau,k}(\sigma_t(V_{n+1} \otimes V_\chi))$ is a bit more convoluted and involves some determinants. Now all ingredients for computing the Hilbert series are in place, and we can give the recipe: evaluate (3.4.3) with T given by (3.4.2), the $\Phi_\sigma(\sigma_t(V))$ given by Lemma 3.4.1, and the $\Psi_{\tau,k}(\sigma_t(V))$ obtained by decomposing the restriction of V to N and using (3.4.4) and the formulas for $\Psi_{\tau,k}(\sigma_t(V_{n+1} \otimes V_\chi))$.

This is much more complicated to state (and prove) than Molien's formula, but not too hard to teach to a computer. Once this is done, the running times can be expected to be essentially the same as for Molien's formula. What is involved in

both cases are computations with rational functions and complex roots of unity. An implementation in MAGMA (see [10]) was written by Kreisel [43].

The paper [41] also gives averaging operators that count the multiplicity of each indecomposable KG -module in a given module, so one can also compute power series whose coefficient count multiplicities of a given indecomposable in the homogeneous parts $K[V]_d$. Apart from computing the Hilbert series of an explicitly given invariant ring, it is sometimes possible to make a generic computation for infinite series of invariant rings. For example, this was done in [41] for the action of $\mathrm{SL}_2(\mathbb{F}_p)$, for general p , on binary forms of degree up to 3. The result was used by Hobson and Shank [44] to compute the invariants of $\mathrm{SL}_2(\mathbb{F}_p)$ acting on binary forms of degree 3. “Generic” Hilbert series of invariant rings for the cyclic group of order p were used by Shank [45], Shank and Wehlau [46], Campbell et al. [47], and Duncan et al. [48] to compute the invariant ring of the cyclic group of order p acting on V_4 and V_5 [45], $V_2 \oplus V_3$ [46], $V_3 \oplus V_3$ [47], and $V_2 \oplus V_2 \oplus V_3$ [48], where V_n denotes the indecomposable module of dimension n . In each of these papers, the authors constructed a graded subalgebra of the invariant ring, worked out its Hilbert series (usually the most demanding part), and compared this to the Hilbert series of the invariant ring that was known from the formulas in Almkvist and Fossum [42] or from a MAGMA program written by the second author for computing generic Hilbert series of invariant rings of cyclic groups of order p .

Another important class of group actions where the Hilbert series can be computed a priori consists of actions where G permutes a basis of V . Then G also permutes the monomials in x_1, \dots, x_n , and a basis of the homogeneous component $K[V]_d^G$ of degree d is given by the sums over the G -orbits of monomials of degree d . The number of such G -orbits is independent of the ground field K . Therefore one can use Molien’s formula pretending to be in characteristic 0, and get the correct result even in the modular case (see Smith [2, Proposition 4.3.4]). If $\sigma \in G \leq S_n$ has a disjoint cycle representation with cycles of lengths l_1, \dots, l_k , then the contribution $1/\det(1 - t \cdot \sigma)$ in Molien’s formula (Theorem 3.4.2) is

$$\frac{1}{(1 - t^{l_1}) \cdots (1 - t^{l_k})}, \quad (3.4.5)$$

so the evaluation is even simpler in this case.

More generally, we can use Molien’s formula to get the Hilbert series of the invariant ring $K[V]^G$ in the case that V is a trivial source module, i.e., a direct summand of a permutation module. More precisely, assume that K has positive characteristic p and let (\tilde{K}, R, K) be a p -modular system (see Curtis and Reiner [40, p. 402]), so $\mathrm{char}(\tilde{K}) = 0$. By Benson [49, Corollary 3.11.4], V lifts to an RG -module \tilde{V} which is also a trivial source module. Now $\tilde{V} := \tilde{K} \otimes_R \tilde{V}$ is a $\tilde{K}G$ -module, and we have the following result.

Proposition 3.4.4 (Kemper [33, Theorem 5]) *In the above situation we have*

$$H(K[V]^G, t) = H(\tilde{K}[\tilde{V}]^G, t) = \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\det_{\tilde{V}}(1 - t \cdot \sigma)}.$$

Example 3.4.5 We present a few examples of trivial source modules.

- (a) If the order of G is not divisible by $p := \text{char}(K)$ (for which we say that G is a p' -group), then every KG -module is a trivial source module by the theorem of Maschke. Furthermore, if W is a trivial source module for a subgroup $H \leq G$, then the induced module $\text{Ind}_H^G(W)$ is also a trivial source module (see Thévenaz [50, Corollary 27.4]). Hence every module which is induced from a p' -subgroup is a trivial source module. An important class of examples are monomial representations, i.e., modules induced from a one-dimensional module of a subgroup.
- (b) Examples of trivial source modules which are not induced from p' -subgroups can be obtained by taking a permutation module $P = \bigoplus_{i=1}^n Ke_i$ with $p \nmid n$ and $V := \{\alpha_1 e_1 + \cdots + \alpha_n e_n \in P \mid \alpha_1 + \cdots + \alpha_n = 0\}$. Then the sequence

$$0 \longrightarrow V \longrightarrow P \longrightarrow K \longrightarrow 0$$

of KG -modules splits, so V is a trivial source module. As a concrete example, consider the natural permutation representation of A_5 over a field of characteristic 2, and take V as above. Applying Proposition 3.4.4 yields

$$H(K[V]^G, t) = \frac{t^{10} + 1}{(1 - t^2)(1 - t^3)(1 - t^4)(1 - t^5)}.$$

□

3.4.3 Extended Hilbert Series

It is interesting to ask if there is a version of Molien's formula which gives information about the homogeneous components $K[V]_d$ in the modular case. For a finite dimensional KG -module V , define $m(V, K)$ to be the multiplicity of the trivial KG -module in a composition series of V . In the nonmodular case we have $m(V, K) = \dim(V^G)$. Consider the **extended Hilbert series**

$$\tilde{H}(K[V], K, t) := \sum_{d=0}^{\infty} m(K[V]_d, K) t^d.$$

Let $\psi: G_{p'} \rightarrow \mathbb{C}$ be the projective indecomposable character of the trivial module K (see Goldschmidt [51, p. 6–11]), which by definition is the Brauer character of the (unique) indecomposable projective module containing K . This can easily be calculated if the Brauer character table X of G is known, the main step being an inversion of X . The following theorem, which can be found in Mitchell [52, Proposition 1.2] (see also Smith [53, p. 218]), gives the appropriate generalization of Molien’s formula in the modular case.

Theorem 3.4.6 *With the above notation, we have*

$$\tilde{H}(K[V], K, t) = \frac{1}{|G|} \cdot \sum_{\sigma \in G_{p'}} \frac{\psi(\sigma)}{\det_V^0(1 - t\sigma)}. \quad (3.4.6)$$

Proof For an irreducible KG -module S we have by Goldschmidt [51, Theorem 6.10] that $1/|G| \sum_{\tau \in G_{p'}} \psi(\tau^{-1}) \Phi_\tau(S)$ equals 1 if $S \cong K$, and 0 otherwise. Since Brauer characters are additive along composition series, it follows that

$$\frac{1}{|G|} \cdot \sum_{\tau \in G_{p'}} \psi(\tau^{-1}) \Phi_\tau(U) = m(U, K)$$

for any finite dimensional KG -module U . Therefore

$$\tilde{H}(K[V], K, t) = \frac{1}{|G|} \cdot \sum_{\tau \in G_{p'}} \psi(\tau^{-1}) \Phi_\tau(\sigma_t(V)).$$

Now the result follows from Lemma 3.4.1. \square

Example 3.4.7 We consider two representations of the group $G = A_5$ in characteristic 2. In this example, the Brauer character tables are taken from the Atlas of Brauer Characters (Jansen et al. [54]), and the projective indecomposable character ψ of the trivial module is constructed from these. These enables us to use Theorem 3.4.6 to compute the extended Hilbert series.

- (a) Since $A_5 \cong \mathrm{SL}_2(\mathbb{F}_4)$ there exists an irreducible two-dimensional module V defined over $K = \mathbb{F}_4$. We calculate the extended Hilbert series of $K[V]$ and obtain

$$\tilde{H}(K[V], K, t) = \frac{t^{14} + t^{12} + t^{10} + 2t^9 + 2t^7 + 2t^5 + t^4 + t^2 + 1}{(1 - t^6)(1 - t^{10})}.$$

- (b) Now we take V as the irreducible module of dimension 4, which occurs as a submodule of the natural permutation module. This module was already considered in Example 3.4.5(b). The extended Hilbert series is

$$\tilde{H}(K[V], K, t) = \frac{t^{10} + t^8 + 3t^7 + 4t^6 + 6t^5 + 4t^4 + 3t^3 + t^2 + 1}{(1 - t^2)(1 - t^3)(1 - t^4)(1 - t^5)}.$$

It is interesting to compare this to the ordinary Hilbert series computed in Example 3.4.5(b). \triangleleft

Remark 3.4.8 If S is an irreducible KG -module, then (3.4.6) gives the generating function $\tilde{H}(K[V], S, t)$ counting the multiplicity of S as a composition factor in $K[V]_d$ if we substitute ψ by the projective indecomposable character of S . One can also easily obtain a formula for the extended Hilbert series $\tilde{H}(K[V] \otimes_K W, S, t)$ of the module of equivariants, where W is another finite dimensional KG -module. \triangleleft

We will see in Sect. 3.5.3 how Theorem 3.4.6 can be used to derive a priori constraints on the degrees of primary invariants.

3.5 Primary Invariants

The first strategic goal in the calculation of an invariant ring of a finite group is often the construction of a homogeneous system of parameters (see Sect. 2.5.2). The invariants occurring in a homogeneous system of parameters are called primary invariants. The existence of a homogeneous system of parameters is guaranteed by the Noether Normalization Theorem (Corollary 2.5.8). We have the following criterion for primary invariants.

Proposition 3.5.1 *Let $f_1, \dots, f_n \in K[V]_+^G$ be homogeneous invariants of positive degree with $n = \dim_K(V)$. Then the following statements are equivalent:*

- (a) f_1, \dots, f_n form a homogeneous system of parameters;
- (b) $\mathcal{V}_{\bar{K}}(f_1, \dots, f_n) = \{0\}$, where $\mathcal{V}_{\bar{K}}(f_1, \dots, f_n)$ is defined as $\{v \in \bar{K} \otimes_K V \mid f_i(v) = 0 \text{ for } i = 1, \dots, n\}$ and \bar{K} is an algebraic closure of K ;
- (c) the Krull dimension $\dim(K[V]/(f_1, \dots, f_n))$ is zero;
- (d) $\dim(K[V]/(f_1, \dots, f_i)) = n - i$ for $i = 1, \dots, n$.

Proof Since $K[V]$ is integral over $K[V]^G$ (see the proof of Proposition 3.0.1), it follows by Eisenbud [55, Proposition 9.2] that

$$\dim(K[V]^G) = \dim(K[V]) = n.$$

Therefore any homogeneous system of parameters in $K[V]^G$ must have n elements, and (a) is equivalent to the condition that $K[V]^G$ is a finitely generated module over the subalgebra $A := K[f_1, \dots, f_n]$, which in turn is equivalent to the condition that $K[V]$ is a finitely generated module over A . By the graded version of Nakayama's lemma (see Lemma 3.7.1 p. 100), this is equivalent to

$$\dim_K(K[V]/(f_1, \dots, f_n)) < \infty.$$

A K -algebra is of finite K -dimension if and only if its Krull dimension is zero. So we have shown the equivalence of (a) and (c). By the principal ideal theorem (see

Eisenbud [55, Theorem 10.2]), (c) and (d) are equivalent. Finally, (b) is equivalent to (c) since the ideal (f_1, \dots, f_n) is homogeneous. \square

Proposition 3.5.1 is the key to all algorithms known to the authors for constructing primary invariants.

3.5.1 Dade's Algorithm

It is important to note that there are many choices of a homogeneous system of parameters. For example, one can substitute any element in a homogeneous system of parameters by a power of itself. As we will see in Sect. 3.7, it is crucial for the efficiency of subsequent calculations that a homogeneous system of parameters be chosen whose degrees are as small as possible. More precisely, one usually wants to minimize the product $\prod_{i=1}^n \deg(f_i)$ (see Theorem 3.9.1). An algorithm for the construction of a homogeneous system of parameters for $K[V]^G$ was given by Dade (see Stanley [56], Reiner and Smith [57]). It is based on the following observation.

Proposition 3.5.2 *Let $n := \dim(V)$ and suppose that $l_1, \dots, l_n \in V^* \setminus \{0\}$ are linear forms such that*

$$l_i \notin \bigcup_{\sigma_1, \dots, \sigma_{i-1} \in G} \langle \sigma_1 \cdot l_1, \dots, \sigma_{i-1} \cdot l_{i-1} \rangle_{K\text{-vector space}} \quad \text{for } i = 2, \dots, n.$$

Let f_i be the product over all l in the G -orbit of l_i . Then $\{f_1, \dots, f_n\}$ is a homogeneous system of parameters of $K[V]^G$.

Proof We show that condition (b) from Proposition 3.5.1 is satisfied. Take $v \in \mathcal{V}_{\bar{K}}(f_1, \dots, f_n)$. Then $(\sigma_i \cdot l_i)(v) = 0$ for some $\sigma_i \in G$. But the assumption says that $\sigma_1 \cdot l_1, \dots, \sigma_n \cdot l_n$ form a basis of V^* , hence $v = 0$. \square

It is clear how Proposition 3.5.2 can be turned into an algorithm, provided that the ground field K is large enough to make the avoidance of a union of at most $|G|^{n-1}$ proper subspaces possible. This algorithm is simple and quick, but the main drawback is that it tends to produce invariants whose degrees are of the same order of magnitude as $|G|$. For some experimental data on this see Kemper [58]. In that paper, various other approaches for the calculation of a homogeneous system of parameters are explored, with the outcome that a computable criterion to decide whether a given degree vector d_1, \dots, d_n represents the degrees of a homogeneous system of parameters is required in order to obtain an algorithm which always produces an optimal homogeneous system of parameters.

3.5.2 An Algorithm for Optimal Homogeneous Systems Parameters

The following provides a criterion for the existence of primary invariants of given degrees.

Theorem 3.5.3 (Kemper [58]) *Let d_1, \dots, d_k be positive integers, and assume that K is an infinite field. Then the following are equivalent:*

- (a) *There exist homogeneous $f_1, \dots, f_k \in K[V]^G$ with $\deg(f_i) = d_i$ such that*

$$\dim(K[V]/(f_1, \dots, f_k)) = n - k;$$

- (b) *for each subset $\mathcal{I} \subseteq \{1, \dots, k\}$ the inequality*

$$\dim(K[V]/(K[V]_{d_i}^G \mid i \in \mathcal{I})) \leq n - |\mathcal{I}|$$

holds. Here $(K[V]_{d_i}^G \mid i \in \mathcal{I})$ denotes the ideal in $K[V]$ generated by the union of all homogeneous components $K[V]_{d_i}^G$ with $i \in \mathcal{I}$.

The implication “(a) \Rightarrow (b)” also holds if K is a finite field.

Observe that the ideals $(K[V]_{d_i}^G \mid i \in \mathcal{I}) \subseteq K[V]$ for $\mathcal{I} \subseteq \{1, \dots, n\}$ can be calculated since K -bases for the subspaces $K[V]_{d_i}^G$ can be obtained by the methods of Sect. 3.1. Moreover, the dimensions of these ideals can be computed by using Gröbner basis methods (see Sect. 1.2.5).

We obtain the following rough idea of an algorithm for the construction of an optimal homogeneous system of parameters.

Algorithm 3.5.4 (Optimal primary invariants, rough algorithm)

- (1) Loop through all degree vectors $(d_1, \dots, d_n) \in \mathbb{N}^n$, ordered by rising values of $\prod_{i=1}^n d_i$, until one is found which satisfies the conditions in (b) of Theorem 3.5.3.
- (2) Loop through all $f_1 \in K[V]_{d_1}^G$ until f_1 is found such that (d_2, \dots, d_n) satisfies the conditions in (b) of Theorem 3.5.3, with $K[V]$ replaced by $K[V]/(f_1)$.
- (3) By recursion, obtain f_2, \dots, f_n of degrees d_2, \dots, d_n such that f_1, \dots, f_n is the desired homogeneous system of parameters.
- (4) If the loop through $K[V]_{d_i}^G$ fails at some level in the recursion (which by Theorem 3.5.3 can only happen if K is finite), go back into the loop (1) and choose a new degree vector (d_1, \dots, d_n) .

To make the algorithm more precise, one has to specify a procedure to enumerate the (usually infinite) vector space $K[V]_{d_i}^G$ in such a way that for a nonzero polynomial f on $K[V]_{d_i}^G$, a vector where f does not vanish is found after finitely many steps. For details, we refer to [58] and remark here that there is no theoretical or practical difficulty involved in this task. While it is clear that the above algorithm terminates

and produces a homogeneous system of parameters with a minimal degree product, it still appears quite appalling, since it involves up to 2^n Gröbner basis computations for testing the conditions from (b) of Theorem 3.5.3 for each degree vector, and a further minimum of 2^n Gröbner basis computations for the recursive construction of the f_i .

However, with a few modifications the algorithm becomes quite feasible. Most importantly, some strong and easily testable restrictions can be applied on degree vectors before they are passed to the recursive loops. We will discuss such restrictions below. Furthermore, in the recursive loops as few of the conditions from (b) of Theorem 3.5.3 as possible are applied. This way a refined algorithm is obtained, which is given in detail in [58]. The approach of trying to get along with testing only a minimal number of conditions from (b) of Theorem 3.5.3 is justified by the fact that the subset of $K[V]_{d_1}^G \times \cdots \times K[V]_{d_n}^G$ consisting of those (f_1, \dots, f_n) which form a homogeneous system of parameters is Zariski-open (see [58, Proposition 1]). This means that the refined algorithm probabilistically only requires one Gröbner basis computation. It is implemented in MAGMA (see Bosma et al. [10]), and experience shows that it works quite well.

3.5.3 Constraints on the Degrees of Primary Invariants

Let f_1, \dots, f_n be primary invariants of degrees d_1, \dots, d_n . By Remark 1.4.3, the Hilbert series of $A := K[f_1, \dots, f_n]$ is

$$H(A, t) = \frac{1}{(1 - t^{d_1}) \cdots (1 - t^{d_n})}. \quad (3.5.1)$$

By looking at a graded free resolution of $K[V]^G$ as a module over A (see Sect. 1.3.2), we conclude that the Hilbert series of $K[V]^G$ can be written as

$$H(K[V]^G, t) = \frac{f(t)}{(1 - t^{d_1}) \cdots (1 - t^{d_n})} \quad \text{with } f(t) \in \mathbb{Z}[t]. \quad (3.5.2)$$

Multiplying this by $(1 - t)^n$ and substituting $t = 1$ yields the value $f(1)/(d_1 \cdots d_n)$, hence $H(K[V]^G, t)$ has a pole at $t = 1$ of order at most n . Therefore we have a Laurent series expansion

$$H(K[V]^G, t) = \frac{a_0}{(1 - t)^n} + \frac{a_1}{(1 - t)^{n-1}} + \dots$$

about $t = 1$, with $a_0 = f(1)/(d_1 \cdots d_n)$. Since $H(K[V]^G, t)$ is coefficient-wise bounded from below by $H(A, t) = \prod_{i=1}^n (1 - t^{d_i})^{-1}$, the coefficient a_0 must be nonzero. This coefficient is the degree of $K[V]^G$ (see Definition 1.4.7). Since $f(1)$ is

an integer, the product $d_1 \cdots d_n$ is a multiple of $1/\deg(K[V]^G)$. On the other hand $\deg(K[V]^G) = 1/|G|$ by Smith [2, Theorem 5.5.3]. To summarize:

Proposition 3.5.5 *If d_1, \dots, d_n are the degrees of primary invariants of $K[V]^G$, then the product $d_1 \cdots d_n$ is divisible by $|G|$.*

An alternative proof using Galois theory is contained in the proof of Theorem 3.9.1. In addition, we know from Campbell et al. [59] and Kemper [29] that the least common multiple of the d_i is divisible by the exponent of G . These results pose restrictions on the degrees d_1, \dots, d_n which are applicable for any finite group. A stronger restriction is obtained by using Eq. (3.5.2) directly in cases where the Hilbert series is known (e.g., if $\text{char}(K)^2 \nmid |G|$). Indeed, picking the smallest d_i such that $H(K[V]^G, t) \cdot \prod_{i=1}^n (1-t^{d_i})$ is a polynomial with integral coefficients often yields the actual degrees of an optimal homogeneous system of parameters. In the nonmodular case, one even knows that the coefficients of $f(t)$ are nonnegative (see Eq. (3.7.1)).

Example 3.5.6

- (a) We consider the permutation group G of order 4 generated by $(1\ 2)(3\ 4)$ and $(1\ 4)(2\ 3)$. Let V be the natural four-dimensional permutation module over $K = \mathbb{Q}$. Molien's formula yields

$$\begin{aligned} H(K[V]^G, t) &= \frac{1}{4} \left(\frac{1}{(1-t)^4} + \frac{3}{(1-t^2)^2} \right) = \\ &\quad \frac{t^2 - t + 1}{(1-t)^2(1-t^2)^2} = \frac{1+t^3}{(1-t)(1-t^2)^3}, \end{aligned}$$

so $(1, 2, 2, 2)$ is the smallest possible degree vector for primary invariants. Indeed, we find

$$\begin{aligned} f_1 &= x_1 + x_2 + x_3 + x_4, & f_2 &= (x_1 - x_2 + x_3 - x_4)^2, \\ f_3 &= (x_1 - x_2 - x_3 + x_4)^2, & f_4 &= (x_1 + x_2 - x_3 - x_4)^2. \end{aligned}$$

- (b) Now take the abelian group G of order 8 generated by the matrices

$$\begin{pmatrix} 1 & & \\ & 1 & \\ & & i \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} -1 & & \\ & -1 & \\ & & 1 \end{pmatrix} \in \text{GL}_3(\mathbb{C}).$$

This is an example of Stanley (see Sloane [60]). Molien's formula yields

$$H(K[V]^G, t) = \frac{1}{(1-t^2)^3},$$

so the degree vector $(d_1, d_2, d_3) = (2, 2, 2)$ meets the restriction posed by Eq. (3.5.2), and is minimal with that property. But $K[V]_2^G$ is generated by x_1^2, x_1x_2 and x_2^2 , so we obtain the Krull dimension $\dim(K[V]^G/(K[V]_2^G)) = 1$. But the condition in Theorem 3.5.3(b) for $\mathcal{I} = \{1, 2, 3\}$ is $\dim(K[V]^G/(K[V]_2^G)) \leq 3 - |\mathcal{I}| = 0$, hence there are no primary invariants of degrees $(2, 2, 2)$. The degree vector with the second-lowest product is $(d_1, d_2, d_3) = (2, 2, 4)$, and here our algorithm readily finds primary invariants

$$f_1 = x_1^2, \quad f_2 = x_2^2, \quad f_3 = x_3^4.$$

△

Although one might argue that the extended Hilbert series $\tilde{H}(K[V], K, t)$ does not have much significance to invariant theory, it is still true that it poses the same type of constraints on the degrees of primary invariants as $H(K[V]^G, t)$, as the following theorem shows.

Theorem 3.5.7 (Kemper [33]) *Suppose that $f_1, \dots, f_n \in K[V]^G$ are primary invariants of degrees d_1, \dots, d_n . Then we can write $\tilde{H}(K[V], K, t)$ in the form*

$$\tilde{H}(K[V], K, t) = \frac{f(t)}{(1 - t^{d_1}) \cdots (1 - t^{d_n})} \quad (3.5.3)$$

with $f(t) \in \mathbb{Z}[t]$.

Remark 3.5.8 It is straightforward to generalize Theorem 3.5.7 to the series $\tilde{H}(K[V], S, t)$ for an irreducible KG -module S (see Remark 3.4.8). □

Example 3.5.9 We take another look at the two representations of the group $G = A_5$ in characteristic 2 considered in Example 3.4.7.

(a) For the module considered in Example 3.4.7(a), we obtained

$$\tilde{H}(K[V], K, t) = \frac{t^{14} + t^{12} + t^{10} + 2t^9 + 2t^7 + 2t^5 + t^4 + t^2 + 1}{(1 - t^6)(1 - t^{10})}.$$

This is the representation in the form (3.5.3) with the smallest possible degrees d_i . (More precisely, this is the representation in which the product d_1d_2 is minimal, and among those representations with minimal d_1d_2 , the sum $d_1 + d_2$ is minimal.) It turns out that the smallest degrees which are possible for primary invariants are $d_1 = 5$ and $d_2 = 12$ here, which corresponds to the representation

$$\begin{aligned} \tilde{H}(K[V], K, t) = \\ \frac{t^{15} + t^{13} + t^{11} + t^{10} + t^9 + t^8 + t^7 + t^6 + t^5 + t^4 + t^2 + 1}{(1 - t^5)(1 - t^{12})} \end{aligned}$$

with the second-lowest d_1 and d_2 . So it can be said that $\tilde{H}(K[V], K, t)$ contains strong restrictions on the degrees of a homogeneous system of parameters.

(b) For the module considered in Example 3.4.7(b), we obtained

$$\tilde{H}(K[V], K, t) = \frac{t^{10} + t^8 + 3t^7 + 4t^6 + 6t^5 + 4t^4 + 3t^3 + t^2 + 1}{(1 - t^2)(1 - t^3)(1 - t^4)(1 - t^5)}.$$

Here the denominator corresponds to the degrees of an optimal homogeneous system of parameters. \triangleleft

3.6 Cohen-Macaulayness

The Cohen-Macaulay property was defined in Sect. 2.6, and it was shown in Proposition 2.6.3 that a graded algebra is Cohen-Macaulay if and only if it is free as a module over the subalgebra generated by a homogeneous system of parameters. As we will see in Sect. 3.7, knowing that an invariant ring $K[V]^G$ is Cohen-Macaulay reduces the computation of generators of $K[V]^G$ as a module over the subalgebra generated by primary invariants to pure linear algebra. In the case of finite groups we have:

Theorem 3.6.1 (Hochster and Eagon [61]) *If $\text{char}(K)$ does not divide the group order $|G|$, then $K[V]^G$ is Cohen-Macaulay.*

Proof Let f_1, \dots, f_n be primary invariants. By Proposition 3.5.1, f_1, \dots, f_n also is a homogeneous system of parameters for $K[V]$, hence f_1, \dots, f_n is a $K[V]$ -regular sequence by Lemma 2.6.2 and Proposition 2.6.3. Suppose that for some $i \in \{1, \dots, n\}$ we have

$$g_i f_i = g_1 f_1 + \cdots + g_{i-1} f_{i-1}$$

with $g_1, \dots, g_i \in K[V]^G$. Then g_i lies in the ideal generated by f_1, \dots, f_{i-1} in $K[V]$, so

$$g_i = h_1 f_1 + \cdots + h_{i-1} f_{i-1}$$

with $h_j \in K[V]$. Now we apply the Reynolds operator and obtain

$$g_i = \mathcal{R}(g_i) = \mathcal{R}(h_1)f_1 + \cdots + \mathcal{R}(h_{i-1})f_{i-1}.$$

Therefore g_i lies in the $K[V]^G$ -ideal generated by f_1, \dots, f_{i-1} . Thus $K[V]^G$ is Cohen-Macaulay by Proposition 2.6.3(b). \square

Remark 3.6.2 We have several generalizations of Theorem 3.6.1.

- (a) Let W be another finitely generated KG -module. Then $(K[V] \otimes_K W)^G$ is Cohen-Macaulay as a module over $K[V]^G$ if $\text{char}(K) \nmid |G|$. The proof is analogous to the proof of Theorem 3.6.1 and uses that $K[V] \otimes_K W$ is Cohen-Macaulay. It is interesting to remark that although Theorem 3.6.1 holds for linearly reductive groups G by Hochster and Roberts [62], the generalization to covariants becomes false in general (see Van den Bergh [63]).
- (b) Suppose that $H \leq G$ is a subgroup such that $\text{char}(K)$ does not divide the index $[G : H]$. Then if $K[V]^H$ is Cohen-Macaulay, so is $K[V]^G$. This is a result of Campbell et al. [64]. The proof is again analogous to the proof of Theorem 3.6.1 and uses the relative Reynolds operator. Together with a result of Ellingsrud and Skjelbred [65] it follows that $K[V]^G$ is Cohen-Macaulay if $\dim_K(V) \leq 3$ (see also Smith [66]).
- (c) This was generalized further by Kemper [67, Theorem 1.1] who showed that for a commutative ring R and a group of automorphisms G with a subgroup $H \subseteq G$ such that R^H is Noetherian and the index $(G : H)$ is finite and invertible in R , the inequality

$$\text{def}(R^G) \leq \text{def}(R^H)$$

holds. Here

$$\text{def}(R) := \sup \{\dim(R_P) - \text{depth}(R_P) \mid P \in \text{Spec}(R)\}$$

denotes the Cohen-Macaulay defect of a Noetherian ring R . \triangleleft

The following is an example of a modular invariant ring which is not Cohen-Macaulay.

Example 3.6.3 Let $G = \langle \sigma \rangle \cong C_p$ be the cyclic group of order $p := \text{char}(K) > 0$, and consider the action on $K[V] = K[x_1, x_2, x_3, y_1, y_2, y_3]$ by

$$\sigma \cdot x_i = x_i \quad \text{and} \quad \sigma \cdot y_i = y_i + x_i.$$

We have invariants x_i and $u_{i,j} := x_i y_j - x_j y_i$ ($1 \leq i < j \leq 3$). By Proposition 3.5.1 the sequence x_1, x_2, x_3 can be extended to a homogeneous system of parameters for $K[V]^G$. But the relation

$$u_{2,3}x_1 - u_{1,3}x_2 + u_{1,2}x_3 = \det \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \\ y_1 & y_2 & y_3 \end{pmatrix} = 0$$

shows that x_1, x_2, x_3 is not $K[V]^G$ -regular, since $u_{1,2}$ does not lie in the $K[V]^G$ -ideal generated by x_1 and x_2 . Hence $K[V]^G$ is not Cohen-Macaulay by Proposition 2.6.3. Notice that in this example the KG -module V is the direct sum of three copies of a

two-dimensional KG -module U . For a sum of one or two copies of U the invariant ring is still Cohen-Macaulay.

For $p = 2$ we have already seen this example in the guise of Example 3.3.1, in which Noether's degree bound fails. \triangleleft

It is an open problem to give a simple characterization which tells us when the invariant ring of finite group together with a modular representation is Cohen-Macaulay. At least it is known that for a group G and a field K whose characteristic divides $|G|$, there exists a finite dimensional KG -module V such that $K[V]^G$ is not Cohen-Macaulay (Kemper [68]). More precisely, it is shown in [68] that if U is a faithful KG -module, then for the direct sum $V = U^k := \bigoplus_{i=1}^k U$ of sufficiently many copies of U the invariant ring $K[V]^G$ is not Cohen-Macaulay. In fact, by Gordeev and Kemper [69], the Cohen-Macaulay defect (see Remark 3.6.2) tends to infinity with k . The proof uses the cohomology $H^*(G, K[V])$ with values in the polynomial ring, which becomes a module over $K[V]^G = H^0(G, K[V])$ via the cup product. The relevance of $H^*(G, K[V])$ to the Cohen-Macaulay property is given by the following proposition.

Proposition 3.6.4 ([68]) *Suppose that for a nonnegative integer r we have $H^i(G, K[V]) = 0$ for $0 < i < r$. (This condition is vacuous if $r \leq 1$.) Then a $K[V]$ -regular sequence $f_1, \dots, f_{r+2} \in K[V]^G$ is $K[V]^G$ -regular if and only if multiplication by the f_i induces an injective map*

$$H^r(G, K[V]) \longrightarrow \bigoplus_{i=1}^{r+2} H^r(G, K[V]).$$

This prompts the study of the annihilator $I := \text{Ann}_{K[V]^G}(H^+(G, K[V]))$, where $H^+(G, K[V]) := \bigoplus_{i>0} H^i(G, K[V])$, and its variety $\mathcal{V}_V(I)$. For simplicity, we assume that K is algebraically closed and write $p := \text{char}(K)$.

Proposition 3.6.5 ([70]) *With the above notation, we have*

$$\mathcal{V}(I) = \bigcup_{\substack{\sigma \in G \\ \text{ord}(\sigma)=p}} V^\sigma.$$

If $V = U^k$ with U a faithful KG -module, it follows that the height of the annihilator I is at least k . Together with Proposition 3.6.4 and the fact that $H^r(G, K) \neq 0$ for some positive r (see Benson [71, Theorem 4.1.3]), this yields the result about non-Cohen-Macaulayness of vector invariants mentioned above. If G is a p -group with $p = \text{char}(K)$, then a closer look at the geometry of the annihilator of the elements in $H^1(G, K)$ yields the following theorem.

Theorem 3.6.6 ([68]) *Assume that G is a p -group with $p := \text{char}(K)$ and that $K[V]^G$ is Cohen-Macaulay. Then G is generated by bireflections, i.e., by $\sigma \in G$ that fix a subspace $U \subseteq V$ of codimension 2 pointwise.*

A generalization by Gordeev and Kemper [69] says that if $k = \text{def}(K[V]^G)$ is the Cohen-Macaulay defect, then G is generated by p' -elements and by elements fixing a subspace of codimension $k+2$ pointwise (i.e., by $(k+2)$ -reflections). It is interesting to compare the above theorem to a result of Kac and Watanabe [72], which says that any finite linear group whose invariant ring is a complete intersection (a much stronger property than being Cohen-Macaulay!) is generated by bireflections. A corollary from Theorem 3.6.6 is that if G is a p -group acting faithfully on V , then $K[V^3]^G$ is not Cohen-Macaulay. A more elementary proof for this result was given by Campbell et al. [35].

3.7 Secondary Invariants

In this section we assume that primary invariants $f_1, \dots, f_n \in K[V]^G$ have been constructed, so $K[V]^G$ is generated by homogeneous invariants g_1, \dots, g_m as a module over $A := K[f_1, \dots, f_n]$. Such generators g_i are called secondary invariants (see Sect. 2.5.2). Together with the primary invariants, the g_i generate $K[V]^G$ as an algebra over K . It should be emphasized that neither primary nor secondary invariants are uniquely determined, and that being a primary or a secondary invariant is not an intrinsic property of an invariant. This section is devoted to the task of finding secondary invariants. We will give entirely different algorithms for the nonmodular and the modular case (the nonmodular one being much easier). In Sect. 3.11.2 a third algorithm will be given, which works in all cases, but only performs well if the invariant ring has a nice structure. The following graded version of Nakayama's lemma is of crucial importance to the finding of secondary invariants.

Lemma 3.7.1 (graded Nakayama Lemma) *Let R be a (nonnegatively) graded algebra over a field $K = R_0$ and M a nonnegatively graded R -module. We write $R_+ := \bigoplus_{d>0} R_d$ for the unique homogeneous maximal ideal. Then for a subset $S \subseteq M$ of homogeneous elements the following two conditions are equivalent:*

- (a) *S generates M as an R -module;*
- (b) *S generates M/R_+M as a vector space over K . Here R_+M is the submodule of M generated by the elements $a \cdot g$ with $a \in R_+$ and $g \in M$.*

In particular, a generating set S for M is of minimal cardinality if no proper subset of S generates M .

Proof Clearly if S generates M , it also generates M/R_+M as a K -vector space.

Conversely, suppose that S generates M/R_+M and let $g \in M$ be homogeneous of some degree d . Then by assumption

$$g = \sum_{i=1}^m \alpha_i g_i + \sum_{j=1}^r a_j h_j$$

with $g_1, \dots, g_m \in S$, $\alpha_i \in K$, $a_j \in R_+$ and $h_j \in M$. By multiplying out homogeneous parts and omitting those summands which are not of degree d , we can assume that the a_j and h_j are homogeneous with $\deg(a_j h_j) = d$. Hence $\deg(h_j) < d$ and h_j lies in the submodule spanned by S by induction on d . Hence g lies in the module spanned by S .

The last remark on minimality follows from the corresponding property of vector spaces. \square

It follows that homogeneous invariants g_1, \dots, g_m generate $K[V]^G$ as a module over A if and only if their images generate the quotient $K[V]^G/A_+K[V]^G$ as a vector space over K . Thus a nonredundant system of secondary invariants has minimal cardinality, and moreover the degrees of such a system are uniquely determined. We have entirely different algorithms for the modular and nonmodular case.

3.7.1 The Nonmodular Case

We assume that the characteristic of K is not a divisor of the group order $|G|$. As we shall see, this has several beneficial effects on the efficiency of our algorithms. First, the invariant ring is always Cohen-Macaulay by Theorem 3.6.1. From the above remark, it follows that any system g_1, \dots, g_m of secondary invariants from which none can be omitted is a system of free generators. Let e_1, \dots, e_m be the degrees of the g_i . Then it follows from the additivity of the Hilbert series with respect to direct sums and from Eq. (3.5.1) that

$$H(K[V]^G, t) = \frac{t^{e_1} + \cdots + t^{e_m}}{(1 - t^{d_1}) \cdots (1 - t^{d_n})}, \quad (3.7.1)$$

where $d_i = \deg(f_i)$ are the degrees of the (chosen) primary invariants. In fact, this is a special case of Eq. (2.7.3). Furthermore, we can easily calculate the Hilbert series by Molien's formula, at least if the group is of reasonably small order (which, by the authors' experience, is always fulfilled if primary invariants could be successfully computed). Thus comparing Eq. (3.7.1) and Theorem 3.4.2 yields complete information about the degrees of the secondary invariants.

In order to find the g_i most efficiently, we use Lemma 3.7.1 again. Let $g_1, \dots, g_m \in K[V]^G$ be homogeneous invariants, with $m = \prod_{i=1}^n d_i/|G|$. Then the g_i are secondary invariants if and only if they generate $K[V]^G/A_+K[V]^G$ as a vector space over K . Since the number of g_i is correct, this is equivalent to the condition that the g_i are linearly independent modulo $A_+K[V]^G$. The ideal $A_+K[V]^G$ in $K[V]^G$ is generated by f_1, \dots, f_n , but one cannot calculate with an ideal in $K[V]^G$ before $K[V]^G$ itself is known. To circumvent this problem, consider the map

$$K[V]^G \rightarrow K[V]/(f_1, \dots, f_n)K[V], f \mapsto f + (f_1, \dots, f_n)K[V].$$

Clearly $A_+K[V]^G$ lies in the kernel. Conversely, an element f in the kernel has the form $f = h_1f_1 + \dots + h_nf_n$, and applying the Reynolds operator yields $f = \mathcal{R}(f) = \mathcal{R}(h_1)f_1 + \dots + \mathcal{R}(h_n)f_n \in A_+K[V]^G$. Therefore we have an embedding

$$K[V]^G/A_+K[V]^G \hookrightarrow K[V]/(f_1, \dots, f_n)K[V],$$

and conclude that g_1, \dots, g_m are secondary invariants if and only if they are linearly independent modulo the ideal $I := (f_1, \dots, f_n)$ in $K[V]$. Now let \mathcal{G} be a Gröbner basis of I with respect to any monomial ordering, and let $\text{NF}_{\mathcal{G}}$ denote the normal form with respect to \mathcal{G} . Such a Gröbner basis has already been calculated in the process of finding the primary invariants f_i (see Sect. 3.5), so there is no extra cost involved. Then for $\alpha_1, \dots, \alpha_m \in K$ we have

$$\alpha_1g_1 + \dots + \alpha_mg_m \in I \iff \alpha_1 \text{NF}_{\mathcal{G}}(g_1) + \dots + \alpha_m \text{NF}_{\mathcal{G}}(g_m) = 0,$$

so all we have to do is check the linear independence of the normal forms of the g_i .

We obtain the following algorithm:

Algorithm 3.7.2 (Secondary invariants in the nonmodular case)

- (1) Let \mathcal{G} be a Gröbner basis of the ideal $(f_1, \dots, f_n) \subseteq K[V]$ generated by the primary invariants. (\mathcal{G} was already calculated when the f_i were constructed.)
- (2) Calculate the degrees e_1, \dots, e_m by using Molien's formula (Theorem 3.4.2) and comparing to (3.7.1).
- (3) For $i = 1, \dots, m$ perform the following two steps:
- (4) Calculate a basis of the homogeneous component $K[V]_{e_i}^G$ by using the methods from Sect. 3.1.
- (5) Select an element g_i from this basis such that the normal form $\text{NF}_{\mathcal{G}}(g_i)$ lies outside the K -vector space generated by the polynomials $\text{NF}_{\mathcal{G}}(g_1), \dots, \text{NF}_{\mathcal{G}}(g_{i-1})$.
- (6) The invariants g_1, \dots, g_m are secondary invariants.

Remark 3.7.3 Algorithm 3.7.2 can be substantially optimized in (at least) two ways.

- (a) One can try to use products of secondary invariants of smaller degrees as new secondary invariants. This is very often successful and has two benefits: It can save the calculation of homogeneous components $K[V]_{e_i}^G$ for some large e_i , and it actually produces a minimal system of generators of $K[V]^G$ as an algebra over $A = K[f_1, \dots, f_n]$.
- (b) If all products of known secondary invariants have been exhausted and the computation of “new” invariants becomes necessary, and if furthermore the Reynolds operator \mathcal{R}_G is used to produce them, then it is enough to apply \mathcal{R}_G to generators of $K[V]$ as a module over $A = K[f_1, \dots, f_n]$. But by Lemma 3.7.1, such generators are given by a basis of $K[V]/(f_1, \dots, f_n)$, which in turn can be chosen to consist of those monomials which lie outside $L(f_1, \dots, f_n)$. The leading ideal is known by the Gröbner basis \mathcal{G} . Thus it is enough to apply the

Reynolds operator to all monomials of degree e_i which are not divisible by the leading monomial of any polynomial in \mathcal{G} , and of course one can stop as soon as enough new invariants are produced. \triangleleft

Example 3.7.4

- (a) We can now finish the computation of the invariant ring from Example 3.5.6(a). From the Hilbert series we see that the secondary invariants are of degrees 0 and 3. Using the above algorithm yields secondary invariants

$$g_1 = 1, \quad g_2 = x_1^3 + x_2^3 + x_3^3 + x_4^3.$$

- (b) In Aslaksen et al. [73], the authors considered the permutation representation of degree 6 of the symmetric group $G = S_4$ given by $(1\ 4\ 6\ 3)(2\ 5)$ and $(2\ 4)(3\ 5)$. (This is the action of S_4 on subsets of two elements in $\{1, \dots, 4\}$.) The ground field is $K = \mathbb{Q}$. Molien's formula yields

$$H(K[V]^G, t) = \frac{1 + t^3 + t^4 + t^5 + t^6 + t^9}{(1-t)(1-t^2)^2(1-t^3)^2(1-t^4)}.$$

Indeed, we find primary invariants of degrees 1,2,2,3,3,4. As secondary invariants we obtain

$$1, g_3, g_4, g_5, g_3^2, g_4 g_5,$$

where each g_i has degree i . Note that we only had to compute invariants of degrees up to 5. The complete computation takes about one second in MAGMA on a Sun workstation, and confirms the results from [73].

- (c) A three-dimensional representation of the group $G = A_5$ over $K = \mathbb{R}$ is given by

$$(1\ 2\ 4) \mapsto \begin{pmatrix} 1 & \alpha & 0 \\ 0 & 0 & 1 \\ 0 & -1 & -1 \end{pmatrix}, \quad (1\ 2\ 3\ 4\ 5) \mapsto \begin{pmatrix} -\alpha & -\alpha & 0 \\ 0 & 0 & -1 \\ \alpha & 1 & 1 \end{pmatrix}$$

with $\alpha = (1 + \sqrt{5})/2$. The Hilbert series is

$$H(K[V]^G, t) = \frac{1 + t^{15}}{(1-t^2)(1-t^6)(1-t^{10})},$$

and MAGMA finds primary invariants of degrees 2, 6, 10 and secondary invariants of degrees 0 and 15 in about half a second. \triangleleft

3.7.2 The Modular Case

Almost everything we used in the nonmodular case is missing in the modular case: The Cohen-Macaulay property fails in general, we do not have Molien's formula and no Reynolds operator. Before Symonds' bound (Theorem 3.3.7) was available, an algorithm using the computation of a syzygy module by Gröbner basis techniques was the state of the art. This was described in the first edition of this book, and a variant for computing invariant rings of finite groups acting on finitely generated algebras over a field will be presented in Sect. 3.13. Having Symonds' degree bound, we obtain the following, rather obvious algorithm.

Algorithm 3.7.5 (Secondary invariants in the modular case)

- (1) Assume that primary invariants f_1, \dots, f_n have already been constructed. Set $A := K[f_1, \dots, f_n]$, $m := 1$, $g_1 := 1$ and $M := A$.
- (2) For $d := 1, \dots, \sum_{i=1}^n (\deg(f_i) - 1)$ perform steps 3–5.
- (3) Compute a basis B_d of $K[V]_d^G$ (using the methods of Sect. 3.1.1).
- (4) Choose $g_{m+1}, \dots, g_{m+k} \in B_d$ minimally such that the homogeneous part M_d together with g_{m+1}, \dots, g_{m+k} generates $K[V]_d^G$ as a vector space.
- (5) Set $M := M + \sum_{i=1}^k A \cdot g_{m+i}$ and $m := m + k$.
- (6) At this point, $M = K[V]^G$ and g_1, \dots, g_m is a minimal system of secondary invariants.

Notice that Algorithm 3.7.5 only requires linear algebra and polynomial arithmetic.

Example 3.7.6

- (a) Let $G \cong C_2$ act on $R := \mathbb{F}_2[x_1, x_2, x_3, y_1, y_2, y_3]$ by interchanging the x_i and y_i . We have already considered the invariant ring R^G in Example 3.3.1 and found that it does not satisfy Noether's degree bound. We will now use Algorithm 3.7.5 to compute the invariant ring. Since we wish to do the calculation by hand and the linear algebra involved in step 4 involves 56 equations, we will argue in a different way.

Using the remark before Proposition 3.4.4, we can calculate the Hilbert series of R^G by Molien's formula and get

$$H(R^G, t) = \frac{1}{2(1-t)^6} + \frac{1}{(1-t^2)^3} = \frac{1+3t^2}{(1-t)^3(1-t^2)^3}. \quad (3.7.2)$$

We choose the primary invariants

$$s_i := x_i + y_i \quad \text{and} \quad p_i := x_i y_i \quad (i = 1, 2, 3).$$

Set $A := \mathbb{F}_2[s_1, s_2, s_3, p_1, p_2, p_3]$. There are no secondary invariants of degree 1. In degree 2 we have the invariants

$$u_{i,j} := x_i y_j + x_j y_i \quad (1 \leq i < j \leq 3),$$

which were already considered in Example 3.3.1. The rational function field $\text{Quot}(R)$ is a Galois extension of $L := \text{Quot}(A)$ with group $C_2 \times C_2 \times C_2$. A subgroup of index 2 fixes $u_{1,2}$, but the subfield $L(u_{1,2}, u_{1,3})$ is only fixed by the trivial subgroup of G . By Galois theory, this implies that 1, $u_{1,2}$ and $u_{1,3}$ are linearly independent over L . So the kernel of the map

$$\varphi: L^4 \rightarrow \text{Quot}(R), \quad (a, b, c, d) \mapsto a + bu_{2,3} + cu_{1,3} + du_{1,2}$$

has dimension at most 1. Now the relation (3.3.1) from Example 3.3.1 shows that $\ker(\varphi) = L \cdot (0, s_1, s_2, s_3)$. This implies that the kernel of

$$\varphi|_{A^4}: A^4 \rightarrow M := A + A \cdot u_{2,3} + A \cdot u_{1,3} + A \cdot u_{1,2}$$

is $A \cdot (0, s_1, s_2, s_3)$. So the Hilbert series is

$$H(M, t) = \frac{1 + 3t^2}{(1-t)^3(1-t^2)^3} \cdot (1-t^3).$$

This shows that the $u_{i,j}$ are a possible choice for secondary invariants of degree 2. Comparing with (3.7.2) shows that in degree 3 we have $\dim(M_3) = \dim(R_3^G) - 1$, so there is precisely one secondary invariant of degree 3. As we have already seen in Example 3.3.1, $f = y_1 x_2 x_3 + x_1 y_2 y_3$ is a possible choice for this.

By Theorem 3.3.7, the maximal degree of a secondary invariant is 3, so we are done. We conclude that R^G is (minimally) generated by the $s_i, p_i, u_{i,j}$, and f .

- (b) Let G be the 3-modular reduction of the Weyl group of type H_4 . This is a subgroup of order 14 400 of $\text{GL}_4(\mathbb{F}_9)$. We will calculate the invariant ring of this group in Sect. 3.11. Here we look at a p -Sylow subgroup P of G , for $p = 3$. P has order 9 and can be generated by the matrices

$$\begin{pmatrix} 1 & 0 & 0 & 0 \\ w+1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ w & 0 & -1 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ w-w & w & 1 & \end{pmatrix} \in \text{GL}_4(\mathbb{F}_9),$$

where $w^2 - w - 1 = 0$. The computation of primary and secondary invariants by MAGMA takes about 0.4 s. The result are primary invariants of degrees 1, 2, 3, 9 and secondary invariants of degrees 0, 3, 4, 7, 8, 11. In this example, the number of secondary invariants equals $\prod_{i=1}^n \deg(f_i)/|P|$. As we will see

in Theorem 3.9.1, this means that $K[V]^P$ and therefore also $K[V]^G$ is Cohen-Macaulay. \triangleleft

3.8 Minimal Algebra Generators and Syzygies

Let R be a graded algebra over $K = R_0$ and $g_1, \dots, g_r \in R_+$ homogeneous of positive degree. Then it is seen by a similar (but easier) argument as the one used in the proof of Theorem 2.2.10 that g_1, \dots, g_r generate R as an algebra over K if and only if they generate the ideal $R_+ \subseteq R$. Moreover, by Lemma 3.7.1, this is equivalent to the condition that the images of the g_i generate the quotient R_+/R_+^2 as a vector space over K . Hence a homogeneous system of algebra generators has minimal cardinality if no generator is superfluous, and then the number and degrees of the generators are uniquely determined. In particular the maximal degree $\beta(R)$ (see Eq. (2.1.1)) of a generator is well defined. One also sees that $\beta(R)$ remains unchanged under extensions of the ground field, i.e., if we pass from R to $R \otimes_K L$ for $L \geq K$ a field extension.

3.8.1 Algebra Generators from Primary and Secondary Invariants

It is clear that the invariant ring $K[V]^G$ is generated as a K -algebra by the primary and secondary invariants. Although the secondary invariants are minimal module-generators, they need not be minimal as algebra-generators. For example, 1 is always a secondary invariant, but it is redundant as an algebra-generator. To test whether a given generator f within a system S of homogeneous algebra-generators is redundant is a linear algebra problem. The procedure is to set up a general element of the same degree as f in the algebra generated by $S \setminus \{f\}$ with unknown coefficients, equating to f and extracting the corresponding system of linear equations by comparison of coefficients. The system is solvable if and only if f can be omitted from S . Starting with S as the union of the primary and secondary invariants, one thus gets a minimal system of algebra-generators, and by the above, $\beta(K[V]^G)$ is its maximal degree.

Example 3.8.1 In Example 3.7.4, we have $\beta(K[V]^G) = 3, 5, 15$ in part (a), (b), (c), respectively. In Example 3.7.6(a), we have seen $\beta(K[V]^G) = 3$. In Example 3.7.6(b), we obtain minimal algebra generators of degrees 1, 2, 3, 3, 4, 9, so the secondary invariants of degrees 7, 8, 11 are redundant. We obtain $\beta(K[V]^G) = 9 = |G|$, which confirms a conjecture made by Kemper et al. [11] that Noether's degree bound holds if the invariant ring is Cohen-Macaulay. \triangleleft

3.8.2 Direct Computation of Algebra Generators: King's Algorithm

A different algorithm for computing generators of $K[V]^G$ in the nonmodular case was given by King [74]. This algorithm calculates algebra-generators directly, omitting the prior calculation of primary and secondary invariants. The key idea is that the arguments used before Algorithm 3.7.2 apply to any graded subalgebra $A \subseteq K[V]^G$, not just to subalgebras generated by primary invariants, and that such a subalgebra can grow during the computation. The algorithm uses truncated Gröbner bases. Recall that a finite subset $\mathcal{G} \subseteq I$ of an ideal in a polynomial ring is called a d -truncated Gröbner basis (with respect to some monomial ordering) if every monomial in $L(I)$ of degree $\leq d$ is contained in $L(\mathcal{G})$ (see Kreuzer and Robbiano [75, Section 4.5.B]). If I is a homogeneous ideal, a d -truncated Gröbner basis can be computed by Buchberger's algorithm (Algorithm 1.1.9), but s-polynomials of degree $> d$ may (and should) be skipped. Using truncated Gröbner bases avoids the dreaded doubly exponential worst case behavior of full Gröbner bases (see Remark 1.1.10). We present a variant of King's algorithm that completely avoids full Gröbner basis, so it could be called “essentially Gröbner basis free.”

Algorithm 3.8.2 (Algebra-generators of $K[V]^G$ in the nonmodular case)

- (1) Set $S := \emptyset$, $\mathcal{G} := \emptyset$ and choose a monomial ordering on $K[V]$. Choose an integer b such that $\beta(K[V]^G) \leq b$ (e.g., $b = |G|$).
- (2) For $d = 1, 2, \dots, b$ perform steps a–d.
 - (a) Let \mathcal{G} be a d -truncated Gröbner basis of (S) . (In fact, it suffices to start from the current set \mathcal{G} and adjoin normal forms with respect to \mathcal{G} of all s-polynomials $h = \text{spol}(f, g)$, $f, g \in \mathcal{G}$, such that $\deg(h) = d$.)
 - (b) Let M be the set of all monomials from $K[V]$ of degree d that are not divisible by any $\text{LM}(g)$, $g \in \mathcal{G}$.
 - (c) If $M = \emptyset$ then go to step 3.
 - (d) For all $t \in M$ perform the following two steps.
 - (i) Set $f := \frac{1}{|\mathcal{G}|} \sum_{\sigma \in \mathcal{G}} \sigma \cdot t$.
 - (ii) If $g := \text{NF}_{\mathcal{G}}(f) \neq 0$ then adjoin f to S and g to \mathcal{G} .
- (3) Now S is a minimal generating set of $K[V]^G$ as an algebra.

Theorem 3.8.3 *Algorithm 3.8.2 is correct.*

Proof We will show by induction on d that after each passage through the loop a–d, the set $K[V]_{\leq d}^G$ of homogeneous invariants of degree $\leq d$ is contained in the subalgebra $K[S]$ generated by S . For the proof, we assume that S is the set resulting from the passage through the loop for degree $d-1$, so $K[V]_{\leq d}^G \subseteq K[S]$. Let $f \in K[V]_d^G$ be a homogeneous invariant of degree d . Since

$$f - \text{NF}_{\mathcal{G}}(f) \in (\mathcal{G}) \subseteq (S),$$

we can write $f - \text{NF}_{\mathcal{G}}(f) = \sum_{i=1}^r g_i f_i$ with $f_i \in S$ homogeneous and $g_i \in K[V]$. We may assume the g_i to be homogeneous of degree $d - \deg(f_i) < d$. Applying the Reynolds operator $\mathcal{R} = \frac{1}{|G|} \sum_{\sigma \in G} \sigma$ yields

$$f - \mathcal{R}(\text{NF}_{\mathcal{G}}(f)) = \sum_{i=1}^r \mathcal{R}(g_i) f_i \in K[S].$$

Observe that $\text{NF}_{\mathcal{G}}(f)$ lies in the K -span $\langle M \rangle_K$ of the set M produced in step b. Therefore $\mathcal{R}(\text{NF}_{\mathcal{G}}(f)) \in \langle \mathcal{R}(M) \rangle_K$, and from the above equation we conclude

$$K[V]_d^G \subseteq K[S] + \langle \mathcal{R}(M) \rangle_K. \quad (3.8.1)$$

So we need to show that after step d has been executed, the algebra generated by the “new” set S contains all $\mathcal{R}(t)$ with $t \in M$. Let f_1, \dots, f_m be the invariants that have already been adjoined to S after some passages through steps i and ii, and let g_1, \dots, g_m be the corresponding normal forms. We write $S' := S \cup \{f_1, \dots, f_m\}$ and $\mathcal{G}' := \mathcal{G} \cup \{g_1, \dots, g_m\}$. Observe that \mathcal{G}' is a d -truncated Gröbner basis of (S') since no s-polynomials of degree $\leq d$ can arise from g_1, \dots, g_m and elements from \mathcal{G}' . For an element $t \in M$ the condition $\text{NF}_{\mathcal{G}'}(\mathcal{R}(t)) = 0$ is therefore equivalent to $\mathcal{R}(t) \in (S')$, which (by the above argument) is equivalent to $\mathcal{R}(t) \in K[S']$. This means that after step d has been executed, all $\mathcal{R}(t)$ with $t \in M$ lie in the algebra generated by the “new” set S , and only such elements have been included that make the algebra larger. This proves the claim and also the minimality of the generating set S . From the observation that \mathcal{G} remains a d -truncated Gröbner basis throughout the passage through steps a–d, it also follows that the procedure in step a will produce a correct result when passing to degree $d + 1$.

Now assume $M = \emptyset$. Then (3.8.1) implies $K[V]_{\leq d}^G \subseteq K[S]$ (with S still the set resulting from the loop for degree $d - 1$). But $M = \emptyset$ means that every monomial of degree d is divisible by some $\text{LM}(g)$ with $g \in \mathcal{G}$, and then the same will hold for every monomial of degree $\geq d$. Therefore if $M = \emptyset$ occurs for some d , it will occur for all the following d as well, and $K[V]^G = K[S]$ follows. So the “early termination condition” in step c is correct. \square

Remark 3.8.4 We make a few remarks on Algorithm 3.8.2 and possible optimizations.

- (a) Let d be the highest degree for which the early termination criterion in step c is not satisfied. It follows from Lemma 3.2.1 and the remark following it that $d \leq |G|$. Moreover, if $f_1, \dots, f_n \in K[V]^G$ are primary invariants, then $d \leq \sum_{i=1}^n \deg(f_i) - n$ (provided that $\dim(V^G) < n - 1$). In most cases, this bound is significantly smaller than $|G|$. On the other hand, the correctness of the algorithm implies $\beta(K[V]^G) \leq d$. King [74] reports that this is often an equality, with the natural action of the symmetric group a notable exception. Indeed, if $K[V]^G = K[f_1, \dots, f_n]$ is a polynomial ring, then $d = \sum_{i=1}^n \deg(f_i) - n$ (again provided that $\dim(V^G) < n - 1$). In this (and in other) cases, the inequality

$\beta(K[V]^G) \leq d$ will be strict. It will also be frequent that even in some degrees that are less than $\beta(K[V]^G)$, no new invariants are required. In order to avoid unnecessary computations of invariants, one may compute $\dim(K[V]_d^G)$ (using Molien's formula) and $\dim(K[S]_d)$ (by linear algebra methods), and abort the loop in step d of the algorithm when $\dim(K[V]_d^G) - \dim(K[S]_d)$ invariants of degree d have been adjoined.

- (b) If G is a large group, the application of the Reynolds operator in step i of the algorithm can be rather costly. An alternative is to compute a basis of $K[V]_d^G$ as in Sect. 3.1.1 and then run through all invariants f from this basis. If this is done, the only purpose of \mathcal{G} and M is to provide an early termination condition. As explained above, this is very important especially for $|G|$ large.
- (c) When the algorithm terminates, \mathcal{G} will end up being a (full) Gröbner basis of the Hilbert ideal $(K[V]_+^G)$. The polynomials from \mathcal{G} have degrees $\leq d + 1$ with d as in (a). The benefit of using only truncated Gröbner bases during the course of the calculation lies in the fact that the full Gröbner bases of the ideals occurring during the computation do not satisfy any nice degree bounds. \triangleleft

King's algorithm is implemented in SINGULAR and in MAGMA. It outperforms the alternative algorithm (via primary and secondary invariants) in many examples, and is probably faster as a general rule. This is why it has become the standard in MAGMA for computing algebra-generators of $K[V]^G$. So King's algorithm seems to be superior not only in its simplicity but also in its effectiveness.

3.8.3 Computing Syzygies

Suppose now that we have generators h_1, \dots, h_r of a K -algebra R . Then we have a presentation of R if we know the kernel I of the map

$$\Phi: K[t_1, \dots, t_r] \rightarrow R, \quad t_i \mapsto h_i,$$

where the t_i are indeterminates. It is one of the basic tasks in invariant theory to compute generators of I as an ideal in the polynomial ring $K[t_1, \dots, t_r]$. The elements of I are usually called **syzygies**. Often the term "syzygies" is used for elements in the kernel of a map of modules, not algebras (see Sect. 1.3). But in fact we have a special case here, since R becomes a module over $K[t_1, \dots, t_r]$ via Φ , and then Φ is a module-homomorphism. We have shown how kernels of maps between free modules over a polynomial ring can be computed. But here the situation is different since R is usually not free, so we need different methods. The first of these takes advantage of the fact that in our situation $R = K[V]^G$ is embedded into the polynomial ring $K[V]$. Therefore we can use the standard Gröbner basis method for calculating the relations between the polynomials h_i (see Sect. 1.2.2). If generators of $K[V]^G$ were computed by King's algorithm, this is in fact the only method known

to the authors. The computation may be sped up by using a degree bound for the syzygies (in the nonmodular case) found by Derkens [76].

If the h_i are subdivided into primary and secondary invariants, another method is available. First, I becomes a homogeneous ideal if we set $\deg(t_i) = \deg(h_i)$. We also use that in our situation the set $\{h_1, \dots, h_r\}$ is the union of a homogeneous system of parameters $\{f_1, \dots, f_n\}$ and a set of secondary invariants $\{g_1, \dots, g_m\}$. Since the f_i are algebraically independent, we are looking for the kernel I of the map

$$A[t_1, \dots, t_m] \rightarrow K[V]^G, \quad t_i \mapsto g_i,$$

where $A = K[f_1, \dots, f_n]$, and the t_i are again indeterminates. Suppose that $S \subseteq I$ is a set of relations containing

- (a) generators for the A -module $I \cap (\bigoplus_{i=1}^m A \cdot t_i)$ of A -linear relations between the g_i , and
- (b) for each $1 \leq i \leq j \leq m$ a relation of the form $t_i t_j - f_{i,j}$ with $f_{i,j} \in \bigoplus_{k=1}^m A \cdot t_k$.

Then it is easy to show that S generates I (see Kemper and Steel [13, Proposition 12]). In other words, all that we have to know are the linear relations between the g_i with coefficients in A and the representation of each product $g_i g_j$ as an element of $\bigoplus_{k=1}^m A \cdot g_k$.

In the case that $K[V]^G$ is Cohen-Macaulay there are no A -linear relations. If $K[V]^G$ is not Cohen-Macaulay, the A -linear relations can be obtained by choosing free generators of $K[V]$ as an A -module (which is the same as setting up an isomorphism $A' \rightarrow K[V]$). With this, the secondary invariants can be represented as vectors in A' , and their A -linear relations can be computed by the methods from Sect. 1.3.1. Alternatively, a degree bound by Symonds [32] may be used to compute the A -linear relations by linear algebra methods. This degree bound says that the syzygies are generated in degrees bounded above by $2 \sum_{i=1}^n (d_i - 1)$, where the d_i are the degrees of the primary invariants.

The representation of a product $g_i g_j$ or, more generally, any homogeneous element $f \in R$ of degree d , say, as an element of $\bigoplus_{i=1}^m A \cdot g_i$ can be calculated by equating f to a general element of $\bigoplus_{i=1}^m A \cdot g_i$ of degree d with unknown coefficients and solving the resulting inhomogeneous system of linear equations over K . This approach usually performs better than the Gröbner basis method. Nevertheless, the computation of relations can sometimes be quite expensive.

It is often important to obtain a *minimal* system of generators for the ideal I . Since $K[V]^G$ is a graded algebra, Lemma 3.7.1 applies again and tells us that it is enough to omit superfluous generators. If the linear algebra method is used, one can go a bit further by detecting superfluous relations even before calculating them: It is quite easy to decide whether the ideal generated by the relations that have already been computed at some point contains a relation giving the desired representation for a product $g_i g_j$. In fact, this again comes down to the solution of a system of linear equations.

A Noetherian graded algebra R is said to be a **complete intersection** if the minimal number of generators minus the minimal number of generating relations between them is equal to the Krull dimension $\dim(R)$. In other words, the dimension of the variety $\mathcal{V}_{\bar{K}}(r_1, \dots, r_i)$ decreases by 1 with each new generating relation r_i as it enters into the ideal. In Example 3.7.4(a) and (c) the invariant rings are complete intersections.

A complete classification of all finite linear groups over \mathbb{C} whose invariant rings are complete intersections was given independently by Nakajima [77, 78] and Gordeev [79].

3.9 Properties of Invariant Rings

One of the reasons to calculate generators of an invariant ring $K[V]^G$ is that one wants to understand its structural properties. This applies especially (but not only) in the modular case, where many questions are still unanswered. In this section we address various properties and quantities associated to $K[V]^G$, and give methods to calculate them. There is the following hierarchy of “standard” properties that are of interest for an invariant ring (or any graded algebra R over a field $K = R_0$):

$$\begin{aligned} K[V]^G \text{ polynomial} &\Rightarrow K[V]^G \text{ complete intersection} \Rightarrow \\ K[V]^G \text{ Gorenstein} &\Rightarrow K[V]^G \text{ Cohen-Macaulay}. \end{aligned}$$

All these properties will be addressed in this section. We have already dealt with the computation of $\beta(K[V]^G)$ and the complete intersection property in Sect. 3.8. The following Sects. 3.9.1, 3.9.2 and 3.9.3 are only relevant in the modular case.

3.9.1 The Cohen-Macaulay Property

After secondary invariants have been calculated, the Cohen-Macaulay property of $K[V]^G$ can be tested by simply counting their number, as the following result shows.

Theorem 3.9.1 *Assume that the action of G on V is faithful, let $f_1, \dots, f_n \in K[V]^G$ be primary invariants of degrees d_1, \dots, d_n , and let g_1, \dots, g_m be a minimal system of secondary invariants. Then*

$$m \geq \frac{d_1 \cdots d_n}{|G|}$$

with equality if and only if $K[V]^G$ is Cohen-Macaulay.

Proof Let h_1, \dots, h_r be minimal homogeneous generators for $K[V]$ as a module over $A := K[f_1, \dots, f_n]$. Since $K[V]$ is Cohen-Macaulay by Lemma 2.6.2, Eq. (3.7.1) yields

$$H(K[V], t) = \frac{t^{\deg(h_1)} + \dots + t^{\deg(h_r)}}{(1 - t^{d_1}) \cdots (1 - t^{d_n})}.$$

On the other hand, we have

$$H(K[V], t) = \frac{1}{(1 - t)^n}$$

by Eq. (3.5.1). Equating, multiplying by $(1 - t)^n$ and setting $t := 1$ yields

$$r = d_1 \cdots d_n.$$

The h_i generate the rational function field $K(V)$ as a vector space over $K(f_1, \dots, f_n) = \text{Quot}(A)$. By the Cohen-Macaulay property of $K[V]$, they are also linearly independent over $\text{Quot}(A)$. Hence the degree of the extension is

$$[K(V) : \text{Quot}(A)] = r = d_1 \cdots d_n.$$

By Galois theory it follows that

$$[K(V)^G : \text{Quot}(A)] = \frac{d_1 \cdots d_n}{|G|}. \quad (3.9.1)$$

(This provides an alternative proof of Proposition 3.5.5.) Since g_1, \dots, g_m generate $K(V)^G$ as a vector space over $\text{Quot}(A)$, the claimed inequality follows. Moreover, we have equality if and only if the g_i are linearly independent over $\text{Quot}(A)$, which by Proposition 2.6.3 is equivalent to the Cohen-Macaulay property of $K[V]^G$. \square

3.9.2 Free Resolutions and Depth

If $K[V]^G$ is not Cohen-Macaulay, it is not free as a module over a subalgebra $A \subseteq K[V]^G$ generated by primary invariants. Then it is interesting to calculate a free resolution of $K[V]^G$ over A . As in the computation of A -linear relations (see Sect. 3.8.3), the first step is to set up an isomorphism $A^r \rightarrow K[V]$ and computing the preimages of the secondary invariants. This provides generators of a submodule $M \cong K[V]^G$ of A^r . Now Algorithm 1.3.4 can be used to calculate a graded free resolution

$$0 \longrightarrow F_r \longrightarrow \dots \longrightarrow F_1 \longrightarrow F_0 \longrightarrow M \longrightarrow 0 \quad (3.9.2)$$

of $K[V]^G \cong M$ (as an A -module). By the method given in Sect. 1.3.2 this can be transformed into a minimal free resolution, so let us assume that (3.9.2) is minimal. In particular, the number $r = \text{hdim}_A(K[V]^G)$ is the homological dimension of $K[V]^G$ (as an A -module). This is an interesting invariant that provides a measure of the complexity of the invariant ring. From this, we can also compute the depth of $K[V]^G$ as an A -module by the Auslander-Buchsbaum formula (see Benson [1, Theorem 4.4.4]), which yields

$$\text{depth}_A(K[V]^G) = \text{depth}(A) - \text{hdim}_A(K[V]^G) = n - r, \quad (3.9.3)$$

where $n = \dim_K(V)$. The following lemma shows that the depth of $K[V]^G$ as a module over A is the same as the depth as a module over itself.

Lemma 3.9.2 *Let M be a finitely generated graded module over a Noetherian graded algebra R over a field $K = R_0$, and let $A \subseteq R$ be a Noetherian graded subalgebra over which R is integral. Then*

$$\text{depth}(R_+, M) = \text{depth}(A_+, M).$$

Proof The inequality $\text{depth}(A_+, M) \leq \text{depth}(R_+, M)$ is clear. To show the reverse inequality, let $f_1, \dots, f_k \in A_+$ be a maximal M -regular sequence. By Bruns and Herzog [80, Theorem 1.2.5], it suffices to show that f_1, \dots, f_k is also a maximal M -regular sequence in R_+ . Every element of A_+ is a zero divisor on $M/(f_1, \dots, f_k)M$, hence by Eisenbud [55, Theorem 3.1], A_+ is contained in the union of the associated primes in R of $M/(f_1, \dots, f_k)M$. By the prime avoidance lemma (see Eisenbud [55, Lemma 3.3]), A_+ lies in some $P \in \text{Ass}_R(M/(f_1, \dots, f_k)M)$. The same is true for the ideal A_+R generated by A_+ in R . But since R is integral over A , only one prime ideal of R contains A_+R , namely R_+ . Hence $P = R_+$, and again by Eisenbud [55, Theorem 3.1], f_1, \dots, f_k is a maximal M -regular sequence in R_+ . \square

Now Eq. (3.9.3) and Lemma 3.9.2 allow the computation of the depth of $K[V]^G$ (as a module over itself). Lemma 3.9.2 and Eq. (3.9.3) also imply that the homological dimension of $K[V]^G$ over A is independent of the choice of primary invariants. Usually the computation of the minimal free resolution required to evaluate Eq. (3.9.3) is fairly easy once the secondary invariants have been found (see Sect. 1.3.2). However, there is no algorithm known for calculating the depth of the invariant ring of a finite group without first computing generators for the invariant ring.

Only in special cases do we have formulas for the depth of a modular invariant ring, or easy methods to calculate it. The first result in this direction is given by the celebrated formula of Ellingsrud and Skjelbred [65], which says that for G a cyclic p -group (with $p = \text{char}(K)$) we have

$$\text{depth}(K[V]^G) = \min\{\dim_K(V^G) + 2, \dim_K(V)\}.$$

This was generalized by Campbell et al. [81] to the class of so-called shallow groups. We will not include the definition of shallowness here but just remark that it is still a rather limited class of groups, which contains all abelian groups with cyclic Sylow p -subgroup ($p = \text{char}(K)$). For a shallow group the above formula holds with V^G replaced by V^P with $P \leq G$ a Sylow p -subgroup. A further interesting result of Shank and Wehlau [82] says that for $G = \text{SL}_2(p)$ acting on binary forms (see Example 2.1.2) of degree d with $1 < d < p$ and $\gcd(d, p - 1) \leq 2$ the depth of the invariant ring is 3. These results were generalized by Kemper [70]. One of the results is the following.

Theorem 3.9.3 *Suppose that $|G|$ is divisible by $p := \text{char}(K)$ but not by p^2 . Let r be the smallest positive number such that $H^r(G, K[V]) \neq 0$. Then*

$$\text{depth}(K[V]^G) = \min \{\dim_K(V^P) + r + 1, \dim_K(V)\},$$

where $P \leq G$ is a Sylow p -subgroup.

Among other ingredients, Proposition 3.6.5 is used in the proof. Theorem 3.9.3 reduces the computation of the depth to the problem of determining the smallest $r > 0$ with $H^r(G, K[V]) \neq 0$. At first glance, this seems to be an even harder problem than computing the invariant ring $K[V]^G = H^0(G, K[V])$. But it is for the same class of groups ($p^2 \nmid |G|$) that Hughes and Kemper [41] developed a method for finding generating functions encoding the multiplicities of the indecomposable KG -modules in the symmetric powers $K[V]_d$. They obtained formulas that are similar to the ones presented in Sect. 3.4.2. Since it is known for which indecomposable KG -modules U and for which i one has $H^i(G, U) \neq 0$, it is quite easy to derive formulas for the Hilbert series

$$H(H^i(G, K[V]), t) := \sum_{d=0}^{\infty} \dim_K(H^i(G, K[V]_d)) t^d.$$

From these the smallest r with $H^r(G, K[V]) \neq 0$ can be found. This provides a procedure for determining the depth in the case $p^2 \nmid |G|$ which is roughly of the same computational difficulty as the evaluation of Molien's formula. This procedure was implemented in MAGMA by Denis Vogel.

In Fleischmann et al. [83] it is shown that the right hand side of the equation in Theorem 3.9.3 is always a lower bound for the depth. The paper also studies situations where equality holds. One result says that if G has a cyclic Sylow p -subgroup P and is p -nilpotent (i.e., there exists a normal subgroup of index $|P|$), then

$$\text{depth}(K[V]^G) = \min \{\dim_K(V^P) + 2, \dim_K(V)\}.$$

3.9.3 The Hilbert Series

If $K[V]^G$ is Cohen-Macaulay, its Hilbert series is given by the formula (3.7.1). More generally, if a graded free resolution (3.9.2) of length r of the invariant ring $K[V]^G$ as a module over the subalgebra A generated by primary invariants has been calculated, then for the Hilbert series we obtain

$$H(R, t) = \sum_{i=0}^r (-1)^i H(F_i, t)$$

(see Remark 1.4.4). Observe that the free generators of F_i must be of the right degrees to make the maps in (3.9.2) degree-preserving. If these degrees are $e_{i,1}, \dots, e_{i,s_i}$, then

$$H(F_i, t) = (t^{e_{i,1}} + \dots + t^{e_{i,s_i}}) \cdot H(A, t) = \frac{t^{e_{i,1}} + \dots + t^{e_{i,s_i}}}{(1 - t^{d_1}) \cdots (1 - t^{d_n})},$$

where $d_i = \deg(f_i)$ (see Eq. (3.5.1)). Thus the Hilbert series of $K[V]^G$ is an easy by-product of the resolution.

3.9.4 Polynomial Invariant Rings and Reflection Groups

The simplest structure that a (graded) algebra can have is that it is isomorphic to a polynomial ring, i.e., it is generated by algebraically independent elements. Then we will say for simplicity that it is polynomial. Since we know how to calculate a minimal system of generators for an invariant ring $K[V]^G$ of a finite group (see Sect. 3.8), there is a way to decide whether $K[V]^G$ is polynomial. However, there is a much more efficient algorithm for this, which does not involve the computation of primary or secondary invariants and reduces the question to linear algebra. It is based on the following result.

Theorem 3.9.4 (Kemper [84]) *Assume that the action of G on V is faithful, and let $f_1, \dots, f_n \in K[V]^G$ be homogeneous invariants with $n = \dim(V)$. Then the following statements are equivalent:*

- (a) $K[V]^G = K[f_1, \dots, f_n]$ (in particular, $K[V]^G$ is a polynomial algebra).
- (b) The f_i are algebraically independent over K and

$$\prod_{i=1}^n \deg(f_i) = |G|. \tag{3.9.4}$$

- (c) The Jacobian determinant $\mathfrak{J} = \det(\partial f_i / \partial x_j)$ is non-zero and $\prod_{i=1}^n d_i = |G|$.

Proof We first prove the equivalence of (a) and (b). Set $d_i := \deg(f_i)$. Assume that $K[V]^G = K[f_1, \dots, f_n]$. Then f_1, \dots, f_n form a system of primary invariants. In particular, the f_i are algebraically independent. Moreover, there is only one secondary invariant (the constant 1). From this, Eq. (3.9.4) follows by Theorem 3.9.1.

Conversely, assume that the conditions in (b) hold. If we can show that f_1, \dots, f_n form a system of primary invariants, then it follows by Proposition 3.11.2 (which appears on p. 134) that $K[V]^G = K[f_1, \dots, f_n]$. Therefore we have to show that the f_i form a system of primary invariants, which by Proposition 3.5.1 is equivalent to

$$\mathcal{V}_{\bar{K}}(f_1, \dots, f_n) = \{0\}, \quad (3.9.5)$$

where \bar{K} is an algebraic closure of K . We take additional indeterminates t_1, \dots, t_n and x_0 and an algebraic closure \tilde{K} of $K(t_1, \dots, t_n)$ which contains \bar{K} . By Bézout's theorem (see Fulton [85, Example 12.3.7], where no assumption is made on the dimension of the zero manifold), the projective algebraic set $\mathcal{V} \subseteq \mathbb{P}^n(\tilde{K})$ given by

$$f_1(x_1, \dots, x_n) - t_1 x_0^{d_1} = \dots = f_n(x_1, \dots, x_n) - t_n x_0^{d_n} = 0$$

has at most $\prod_{i=1}^n d_i = |G|$ irreducible components. So (3.9.5) will follow if we can show that there are at least $|G|$ components of \mathcal{V} with $x_0 \neq 0$. By the assumption, $K(x_1, \dots, x_n)$ is a finite field extension of $K(f_1, \dots, f_n)$, so each x_i has a minimal polynomial over $K(f_1, \dots, f_n)$, say $g_i(x_i, f_1, \dots, f_n) = 0$. If $(\xi_1, \dots, \xi_n) \in \tilde{K}^n$ is a solution of

$$f_1(x_1, \dots, x_n) - t_1 = \dots = f_n(x_1, \dots, x_n) - t_n = 0, \quad (3.9.6)$$

then $g_i(\xi_i, t_1, \dots, t_n) = 0$. Hence there are only finitely many solutions of (3.9.6), and each constitutes a component of its own in \mathcal{V} . We shall complete the proof by giving $|G|$ solutions of (3.9.6).

Via the isomorphism $K(f_1, \dots, f_n) \rightarrow K(t_1, \dots, t_n), f_i \mapsto t_i$, form

$$L := K(t_1, \dots, t_n) \otimes_{K(f_1, \dots, f_n)} K(x_1, \dots, x_n),$$

which is a finite field extension of $K(t_1, \dots, t_n)$ and can therefore be assumed to lie inside \tilde{K} . Take a $\sigma \in G$ and set $\xi_i := 1 \otimes \sigma \cdot x_i \in L$. Then

$$f_i(\xi_1, \dots, \xi_n) = 1 \otimes f_i(\sigma \cdot x_1, \dots, \sigma \cdot x_n) = 1 \otimes \sigma \cdot f_i = 1 \otimes f_i = t_i \otimes 1.$$

Hence the elements of G give rise to $|G|$ distinct solutions of (3.9.6). This yields $|G|$ components of \mathcal{V} with $x_0 \neq 0$, which completes the proof of the equivalence of (a) and (b).

The equivalence of (a) and (b) with (c) follows from the fact that $\mathfrak{J} \neq 0$ if and only if $K(x_1, \dots, x_n)$ is a finite separable field extension of $K(f_1, \dots, f_n)$ (see, for example, Benson [1, Prop. 5.4.2]). \square

We obtain the following algorithm.

Algorithm 3.9.5 (Test if $K[V]^G$ is polynomial) Build a graded subalgebra $R \subseteq K[V]^G$ as follows: Loop through the degrees $d = 1, 2, \dots$. For each degree, compute $K[V]_d^G$ by the methods of Sect. 3.1. Choose $f_{d,1}, \dots, f_{d,m_d} \in K[V]_d^G$ which provide a basis of the quotient space $K[V]_d^G / R_d$. Then $f_{d,1}, \dots, f_{d,m_d}$ are new generators of R . If the degree product of all generators does not divide $|G|$, or if the number of generators exceeds n , then $K[V]^G$ is not polynomial. On the other hand, if at some stage there are n generators such that the product of their degrees equals $|G|$, then compute their Jacobian determinant. It is nonzero if and only if $K[V]^G$ is polynomial.

The above algorithm is certain to terminate, since there must be at least n generators for $K[V]^G$ (since $\dim(K[V]^G) = n$).

In the nonmodular case, the question when an invariant ring of a finite group is polynomial is settled by the famous theorem of Shephard and Todd [86], Chevalley [87], and Serre [88], which says that $K[V]^G$ is a polynomial ring if and only if the group G is generated by elements which act on V as reflections, i.e., by nonidentity elements σ which fix a codimension-1 subspace of V . (Regarding G as a subgroup of $\mathrm{GL}(V)$, we simply say that G is a **reflection group**.) It was also proved by J.P. Serre that in the modular case G has to be a reflection group if $K[V]^G$ is a polynomial ring (see Benson [1, Theorem 7.1.2] for a proof). An interesting extension of this result was given by Dufresne [89]. This will be discussed in Sect. 3.12. The following example shows that in the modular case an invariant ring of a reflection group need not be polynomial.

Example 3.9.6 (Nakajima [90]) Consider the group

$$G := \left\{ \begin{pmatrix} 1 & 0 & a+b & b \\ 0 & 1 & b & b+c \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{GL}_4(\mathbb{F}_q) \mid a, b, c \in \mathbb{F}_q \right\},$$

which is an abelian reflection group of order q^3 . We make the convention that the columns of the matrices stand for the images of the indeterminates x_i . By way of contradiction, assume that $K[V]^G$ is a polynomial ring. There are two invariants of degree 1, namely $f_1 = x_1$ and $f_2 = x_2$. By Theorem 3.9.4 there are two further generators f_3 and f_4 . If $\deg(f_3) \leq \deg(f_4)$, then $\deg(f_4) > q$, and both degrees are powers of $p := \mathrm{char}(\mathbb{F}_q)$. Hence any invariant of degree $q+1$ must have the form $g_1 \cdot f_3^k + g_2$ with $g_1, g_2 \in K[x_1, x_2]$. But it is easily verified that

$$x_1^q x_3 - x_1 x_3^q + x_2^q x_4 - x_2 x_4^q$$

is an invariant which is not of the above form. This contradiction shows that $K[V]^G$ is not a polynomial ring.

For $q = p$ a prime, this example appeared in Nakajima [90]. Nakajima achieved much further reaching results on the polynomiality of invariants of reflection groups

in [91, 92]. In [92], he gave a characterization of all p -groups over \mathbb{F}_p which have polynomial invariant rings. \triangleleft

The following result is a strong tool to prove that an invariant ring is not a polynomial ring.

Proposition 3.9.7 (Serre [88]) *Suppose that $K[V]^G$ is a polynomial ring. Then for all linear subspaces $W \subseteq V$ the invariant ring $K[V]^{G_W}$ of the point-wise stabilizer $G_W := \{\sigma \in G \mid W \subseteq V^\sigma\}$ is also a polynomial ring. In particular, G_W is a reflection group.*

Proposition 3.9.7 was used by Nakajima [90] to prove that the invariant rings of many classical groups (over finite fields) are not isomorphic to polynomial rings. Later Kemper and Malle [93] classified the irreducible linear groups (i.e., finite groups G with an irreducible KG -module V) for which $K[V]^G$ is a polynomial ring. This classification was obtained by going through a complete list of all finite irreducible modular reflection groups given by Kantor [94], Wagner [95, 96], Zalesskii and Serezkin [97, 98]. Table 3.1 gives an overview of the finite irreducible modular reflection groups, and which of them have polynomial invariant rings.

Most of the notation used in Table 3.1 should be clear. The representations of the symmetric group S_n are the representation called V in Example 3.9.9 below for $p \nmid n$, and U from Example 3.9.9 for $p \mid n$. $W_p(G_i)$ means the p -modular reduction of the complex reflection group appearing as number i in the classification of Shephard and Todd [86]. The groups $EJ_3(5), J_4(4)$ only appear in positive characteristic (5 and 2, respectively). For the exceptional groups (i.e., those appearing in the last row) whose invariant rings turned out to be polynomial, this was in most cases proved by explicitly constructing generating invariants using a computer. In each instance

Table 3.1 Finite irreducible modular reflection groups

Group	$K[V]^G$ polynomial	$K[V]^G$ not polynomial
G imprimitive	All	—
$n = \dim(V) \leq 2$	All	—
$SL_n(q) \leq G \leq GL_n(q)$	All	—
$\Omega_n^{(\pm)}(q) < G \leq O_n^{(\pm)}(q), G \neq SO_n^{(\pm)}(q)$	$O_3(q), R^+O_3(q), O_4^-(q)$	All others
$SU_n(q^2) \leq G \leq U_n(q^2)$	$U_3(q^2)$	All others
$G = Sp_n(q), n \geq 4$ even	—	All
$G = S_{n+1}, p \nmid (n+1)$	All	—
$G = S_{n+2}, p \mid (n+2), n \geq 5$	—	All
$G = W_p(G_i)$ ($i = 23, \dots, 37$), $G = EJ_3(5), G = J_4(4)$	All except \rightarrow	$W_7(G_{24}), W_3(G_{28}),$ $W_3(G_{30}), W_5(G_{30}),$ $W_3(G_{31}), W_5(G_{32}),$ $W_3(G_{33}), W_2(G_{34}),$ $W_3(G_{36}), W_3(G_{37}),$ $W_5(G_{37})$

where $K[V]^G$ is not polynomial, Proposition 3.9.7 was used, so the following result emerges:

Theorem 3.9.8 (Kemper and Malle [93]) *The invariant ring $K[V]^G$ of a finite group G acting irreducibly on V is a polynomial ring if and only if G is a reflection group and $K[V]^{G_W}$ is a polynomial ring for every nonzero linear subspace $W \leq V$.*

It may be worth noting that in the above theorem it does not suffice to demand that G_W be a reflection group for all subspaces W (see Campbell et al. [99] for a nonirreducible counter example and Kemper and Malle [93, Example 2.2] for an irreducible counter example).

Another noteworthy fact about the paper [93] is that 5 years after its appearance it was discovered by Kasper Andersen that the authors had used Proposition 3.9.7 incorrectly. In fact, the convention adopted in [93] is that the polynomial ring is $S(V)$ (the symmetric algebra of V , rather than its dual V^*). Then the authors applied Proposition 3.9.7 to point-wise stabilizers of subspaces $W \leq V$. But according to their convention, they should have used subspaces $W \leq V^*$. Drawing attention to this inconsistency is far from being pedantic. In fact, it was pointed out by Andersen that Kemper and Malle's way of applying Proposition 3.9.7 might very well have resulted in incorrectly sending the group $W_5(G_{29})$ to the right hand column of Table 3.1. It is precisely the symmetric group S_5 with its four-dimensional representation discussed in Example 3.9.9 below that occurs as a stabilizer here. What really happened is that the authors had already proved by computations that $W_5(G_{29})$ has a polynomial invariant ring, so they did not even start to apply Proposition 3.9.7 to it. After hearing about their error from Andersen, the authors had to reconsider all cases where they had applied Proposition 3.9.7. Luckily, it turned out that the final results summarized in Table 3.1 and Theorem 3.9.8 all remain correct. In most of the cases the point-wise stabilizers G_W found by the authors are not generated by reflections, which means that $S(V)^{G_W}$ as well as $S(V^*)^{G_W}$ are not polynomial rings; so no trouble can arise in these cases.

Qualitatively speaking, “most” invariant rings of modular reflection groups are not polynomial rings. This raises the question what the structure of these invariant rings is. Could it be, for instance, that the invariant ring of a modular reflection group is always a complete intersection? For example, the invariant rings of symplectic groups were determined by Carlisle and Kropholler [100], and found to be all complete intersections (see also Benson [1, Section 8.3]). Nevertheless, all hopes of finding nice properties which hold in general for such rings are crushed by examples such as the following.

Example 3.9.9 Let n be a multiple of $p := \text{char}(K)$ and consider the symmetric group $G = S_n$. Let $W = K^n$ be the natural KG -module with basis e_1, \dots, e_n , and consider the modules

$$V := W/K \cdot (e_1 + \dots + e_n) \quad \text{and}$$

$$U := \{\alpha_1 e_1 + \dots + \alpha_n e_n + K(e_1 + \dots + e_n) \in V \mid \alpha_1 + \dots + \alpha_n = 0\}.$$

G acts on U and V as a reflection group, and U is irreducible (at least for $p > 2$). Now assume $p \geq 5$. Then by Kemper [68, Corollary 2.8], $K[V]^G$ is not Cohen-Macaulay, and if moreover $n > 5$, then also $K[U]^G$ is not Cohen-Macaulay. If we restrict further and consider $G = S_p$, we even obtain the depths of $K[V]^G$ and $K[U]^G$ by [70, Section 3.2]: The result is 3 in both cases.

Hence we have two series of modular reflection groups (one irreducible and the other a mod- p reduction from a characteristic 0 reflection group) such that the homological dimension of their invariant rings grows arbitrarily large! On the other hand, it is known from Kemper and Malle [101] that the invariant field $K(U)^G$ is purely transcendental over K , so it is the field of fractions of some polynomial ring. A further fact seems even more bizarre: The invariant ring $K[V^*]^G = S(V)^G$ of the dual of V is a polynomial ring, generated by the (residue classes of) the elementary symmetric polynomials of degrees ≥ 2 in the e_i . Thus we have modules whose invariant rings have arbitrarily bad properties, but the invariants of the dual modules have the nicest possible structure! \triangleleft

In Sect. 3.11.3 we will come back to the question of the structure of nonpolynomial invariant rings of modular reflection groups.

3.9.5 The Gorenstein Property

Another property of invariant rings that has received considerable attention is the Gorenstein property. The following is one of various equivalent ways to define this property. Let $A \subseteq K[V]^G$ be a subalgebra generated by a set of primary invariants. Then $\text{Hom}_A(K[V]^G, A)$ becomes a $K[V]^G$ -module by $(f \cdot \varphi)(g) = \varphi(f \cdot g)$ for $f, g \in K[V]^G$ and $\varphi \in \text{Hom}_A(K[V]^G, A)$. Now $K[V]^G$ is called **quasi-Gorenstein** if $\text{Hom}_A(K[V]^G, A)$ is free of rank one as a $K[V]^G$ -module. It is called **Gorenstein** if it is quasi-Gorenstein and Cohen-Macaulay. These notions do not depend on the choice of A . They can be generalized to any finitely generated algebra over a field. The Gorenstein property can be characterized in terms of the Hilbert series. In fact, $K[V]^G$ is Gorenstein if and only if it is Cohen-Macaulay and the Hilbert series satisfies the identity

$$H(K[V]^G, 1/t) = (-1)^n t^{n+\delta} \cdot H(K[V]^G, t) \quad (3.9.7)$$

for some $\delta \in \mathbb{Z}$, where $n = \dim(V)$ (see Stanley [102]). If $H(K[V]^G, t)$ is given as in (3.7.1), this means that the numerator is palindromic. If $K[V]^G$ is Gorenstein, it follows that

$$\delta = -\deg(H(t)) - n = \sum_{i=1}^n (d_i - 1) - e_m \geq 0,$$

where the d_i are the degrees of the primary invariants and e_m is the maximal degree of a secondary invariant. Moreover, the free generator of $\text{Hom}_A(K[V]^G, A)$ has degree $-e_m = \delta - \sum_{i=1}^n (d_i - 1)$. We call $K[V]^G$ **graded Gorenstein** if in addition $\delta = 0$. For example, the invariant rings in Example 3.7.4(a)–(c) and Example 3.7.6(b) are graded Gorenstein. If $K[V]^G$ is polynomial, it is Gorenstein but not graded Gorenstein unless $|G| = 1$. More generally, if $K[V]^G$ is a complete intersection, it is Gorenstein. In the nonmodular case we have the following classical result, whose proof can be found in Stanley [56] and Benson [1, Section 4.5].

Theorem 3.9.10 (Watanabe [103, 104]) *In the nonmodular case, $K[V]^G$ is graded Gorenstein if and only if G acts on V by transformations which lie in $\text{SL}(V)$.*

This result has been extended by various authors, e.g. Peskin [105], Broer [106], Braun [107], and Fleischmann and Woodcock [108]. Perhaps best suited in the context of this book is Broer's result in [106]. The main tool is the **Dedekind different**, whose inverse is defined (in analogy to number theory) as the fractional ideal

$$\mathcal{D}^{-1} := \left\{ f \in \text{Quot}(K[V]) \mid \sum_{\sigma \in G} \sigma \cdot fg \in K[V]^G \text{ for every } g \in K[V] \right\}.$$

It turns out that this is a principal fractional ideal generated by the inverse of a homogeneous polynomial $\theta \in K[V]$, so $\mathcal{D}^{-1} = \theta^{-1}K[V]$. Since \mathcal{D}^{-1} is G -stable, θ is a semi-invariant:

$$\sigma \cdot \theta = \chi(\sigma) \cdot \theta \quad \text{for all } \sigma \in G$$

with χ a linear character, which Broer calls the **differential character**. Moreover, he calls the degree $\delta = \deg(\theta)$ the **differential degree**. Before saying something about the computation of θ , χ , and ρ , we state the main result about the Gorenstein property.

Theorem 3.9.11 (Broer [106]) *The invariant ring $K[V]^G$ is quasi-Gorenstein if and only if $\chi(\sigma) = \det_V(\sigma)$ for every $\sigma \in G$. Moreover, if $K[V]^G$ is Gorenstein, then (3.9.7) holds with δ being the differential degree.*

Notice that the theorem makes no hypothesis on $\text{char}(K)$. The theorem is useful since θ , and from it χ and δ , can be computed explicitly. In fact,

$$\theta = \prod_{i=1}^s \alpha_i^{m_i}$$

with the product running over linear forms $\alpha_1, \dots, \alpha_s$ defining the reflection hyperplanes $H_1, \dots, H_s \subset V$ of G , and the positive integers m_i can be calculated from the invariant ring of a Sylow subgroup of the point-wise stabilizer G_{H_i} , which is a polynomial ring. The precise recipe for the m_i is given in [106, Section 2.6]. If

$K = \mathbb{F}_p$ or $\text{char}(K) = 0$, then m_i only depends on the order $|G_{H_i}|$. From the above formula we learn that the differential degree δ is zero if and only if G contains no reflections, and in this case $\chi = 1$. In particular, Theorem 3.9.10 is a consequence of Theorem 3.9.11.

The situation is particularly nice if the invariant ring of the (normal) subgroup $W \subseteq G$ generated by all reflections is polynomial. In fact, if $K[V]^W = K[f_1, \dots, f_n]$, then θ can be taken as the Jacobian determinant

$$\theta = \det\left(\frac{\partial f_i}{\partial x_j}\right).$$

It is not hard to work out the action of G on the Jacobian determinant, which we describe now. The factor group G/W acts on $K[V]^W$ and therefore also on the n -dimensional vector space $L := K[V]_+^W / (K[V]_+^W)^2$. Explicitly, each $\sigma \in G$ transforms an f_i into a linear combination of f_j 's of equal degree and products of f_j 's of lower degree, and the action on L disregards the products of f_j 's of lower degree. Of course, if $|W| = 1$, then $L = V^*$. Now it turns out that

$$\sigma \cdot \theta = \det_V(\sigma) \det_L(\sigma W) \cdot \theta,$$

so $\chi = \det_V \cdot \det_L$. We obtain the following corollary of Theorem 3.9.11, which was shown to the second author by Amiram Braun. In fact, the corollary is not stated in any of the papers cited above, and Amiram Braun has an independent proof of it.

Corollary 3.9.12 *Let $W \subseteq G$ be the subgroup generated by all reflections in G and assume that the invariant ring $K[V]^W$ is polynomial. Set $L := K[V]_+^W / (K[V]_+^W)^2$. Then the invariant ring $K[V]^G$ is quasi-Gorenstein if and only if G/W acts on L by transformations which lie in $\text{SL}(L)$.*

Of course, the hypothesis on $K[V]^W$ is automatically satisfied if $\text{char}(K)$ does not divide $|W|$. So Corollary 3.9.12 is always applicable in the nonmodular case or when G contains no reflections. Since the question of the Gorenstein property is not completely answered in the nonmodular case by Watanabe's results, the corollary gives new information even in this case. The following example is adapted from Braun [109]. It shows how the action on L may fail to lie in $\text{SL}(L)$ even when the action on V lies in $\text{SL}(V)$.

Example 3.9.13 Let q be an odd prime power and consider the group

$$G = \left\{ \sigma_{a,b} := \begin{pmatrix} a & ab \\ 0 & a^{-1} \end{pmatrix} \mid a \in \mathbb{F}_{q^2}, b \in \mathbb{F}_q, a^{2(q-1)} = 1 \right\} \subseteq \text{SL}_2(\mathbb{F}_{q^2})$$

of order $2q(q-1)$. The reflections in G generate $W = \{\sigma_{1,b} \mid b \in \mathbb{F}_q\}$, whose invariant ring is

$$K[V]^W = K[x_1, \underbrace{x_2^q - x_1^{q-1}x_2}_{=:f}].$$

(Of course, we assume $\mathbb{F}_{q^2} \subseteq K$.) This can be seen, for example, by Theorem 3.9.4. We have $\sigma_{a,b}(x_1) = ax_1$ and $\sigma_{a,b}(f) = a^{-q}f_2$, so $\sigma_{a,b}$ acts on L by $\begin{pmatrix} a & 0 \\ 0 & a^{-q} \end{pmatrix}$. The determinant $\det_L(\sigma_{a,b}) = a^{q-1}$ takes the values ± 1 . So Corollary 3.9.12 tells us that $K[V]^G$ is not Gorenstein. Since $K[V]^G$ is Cohen-Macaulay (as can be seen, for example, by Remark 3.6.2(b)), this provides a counterexample to Conjecture 5 of Kemper et al. [11], as was pointed out by Braun [109].

We can independently verify that $K[V]^G$ is not Gorenstein by computing it. We get as primary invariants $x_1^{2(q-1)}$ and $f^{2(q-1)}$, and as secondary invariants

$$g_i := x_1^{\left\lfloor \frac{qi-2(q-1)}{2(q-1)} \right\rfloor} f^i \quad (i = 0, \dots, 2q-3).$$

The sequence of degrees of secondary invariants fails to display the palindromicity of Gorenstein invariant rings. For example, for $q = 3$, the g_i have the degrees 0, 6, 8, 10. \triangleleft

The paper of Fleischmann and Woodcock [108] generalizes Theorem 3.9.11 to the case where G acts on a finitely generated algebra A over a field K such that A is a unique factorization domain and $A^\times = K^\times$. The paper gives a criterion when A^G is quasi-Gorenstein that is similar to, but more complicated than Theorem 3.9.11.

3.10 Permutation Groups

In this section we deal with the special case that G acts on V by permutations of a basis B of V . If $x_1, \dots, x_n \in V^*$ form a dual basis of B , then G also permutes the x_i , and $K[V] = K[x_1, \dots, x_n]$. Clearly all facts and methods from the previous sections hold for this case as well, but we shall see that much more can be said.

3.10.1 Direct Products of Symmetric Groups

Let us first look at the example of symmetric groups and, more generally, direct products of such.

Theorem 3.10.1 *Let $G = S_{n_1} \times \dots \times S_{n_r}$ be a direct product of symmetric groups acting on $R := K[x_{1,1}, \dots, x_{1,n_1}, \dots, x_{r,1}, \dots, x_{r,n_r}]$ by*

$$(\sigma_1, \dots, \sigma_r) \cdot x_{i,j} = x_{i,\sigma_i(j)}. \quad (3.10.1)$$

Then R^G is generated by the elementary symmetric polynomials

$$s_{i,j} := \sum_{\substack{\mathcal{I} \subseteq \{1, \dots, n_i\} \\ |\mathcal{I}|=j}} \prod_{k \in \mathcal{I}} x_{i,k} \quad (1 \leq i \leq r, 1 \leq j \leq n_i). \quad (3.10.2)$$

R^G is isomorphic to a polynomial ring. This holds independent of the characteristic of K .

Proof We give two alternative proofs. First, observe that

$$\prod_{j=1}^{n_i} (T - x_{i,j}) = T^{n_i} - s_{i,1} T^{n_i-1} + \cdots + (-1)^{n_i-1} s_{i,n_i-1} T + (-1)^{n_i} s_{i,n_i}.$$

If follows that the $s_{i,j}$ form a homogeneous system of parameters. Moreover, the product of their degrees is equal to the group order. Now the result follows from Theorem 3.9.4.

The second proof gives an algorithm for expressing any invariant in terms of the $s_{i,j}$. Indeed, fix the lexicographic monomial ordering with

$$x_{1,1} > x_{1,2} > \cdots > x_{1,n_1} > x_{2,1} > \cdots > x_{r,n_r}.$$

If $\prod_{i,j} x_{i,j}^{e_{ij}}$ is the leading monomial of a nonzero invariant f , then $e_{i,1} \geq e_{i,2} \geq \cdots \geq e_{i,n_i}$ for all i . The leading monomial of $s_{i,j}$ is $x_{i,1} \cdots x_{i,j}$, therefore f has the same leading monomial as

$$\prod_{i=1}^r \prod_{j=1}^{n_i} s_{i,j}^{e_{ij}-e_{i,j-1}},$$

where we set $e_{i,0} := 0$. We obtain the following algorithm.

Algorithm 3.10.2 Let f be an $(S_{n_1} \times \cdots \times S_{n_r})$ -symmetric polynomial in R^G .

- (1) Set $F := 0$ and $g := f$.
- (2) While $g \neq 0$, perform the steps (3)–(5).
- (3) Let $\text{LM}(g) =: \prod_{i,j} x_{i,j}^{e_{ij}}$ and $\text{LC}(g) =: c$.
- (4) Set

$$g := g - c \cdot \prod_{i=1}^r \prod_{j=1}^{n_i} s_{i,j}^{e_{ij}-e_{i,j-1}}.$$

- (5) Set

$$F := F + c \cdot \prod_{i=1}^r \prod_{j=1}^{n_i} T_{i,j}^{e_{ij}-e_{i,j-1}}$$

with indeterminates $T_{i,j}$.

- (6) When $g = 0$ is reached, we have

$$f = F(s_{1,1}, \dots, s_{r,n_r}).$$

The termination of the algorithm is guaranteed by the fact that each new g is an invariant of smaller leading term than the previous one, and of maximal total degree at most the maximal total degree d of f . But there are only finitely many monomials of degree $\leq d$. \square

Remark 3.10.3 A third proof of Theorem 3.10.1 would be to use the fact that for $G_1 \leq \mathrm{GL}(V_1)$ and $G_2 \leq \mathrm{GL}(V_2)$ we have

$$K[V_1 \oplus V_2]^{G_1 \times G_2} \cong K[V_1]^{G_1} \otimes_K K[V_2]^{G_2},$$

and that $K[x_1, \dots, x_n]^{S_n}$ is generated by the elementary symmetric polynomials in x_1, \dots, x_n . But then we would have to prove this latter fact, which amounts to more or less the same as proving Theorem 3.10.1. \triangleleft

The second proof tells us that the elementary symmetric polynomials form a SAGBI basis of the invariant ring, according to the following definition.

Definition 3.10.4 Let $>$ be a monomial ordering on the polynomial ring $K[x_1, \dots, x_n]$. For a subalgebra $A \subseteq K[x_1, \dots, x_n]$, write $L(A)$ for the algebra generated by all leading monomials of nonzero elements from A . A subset $S \subseteq A$ is called a **SAGBI basis** of A if the algebra generated by all leading monomials of elements from S equals $L(A)$:

$$K[\mathrm{LM}(f) \mid f \in S] = L(A).$$

If S is a SAGBI basis of A then it also generates A as an algebra, and we have an algorithm such as Algorithm 3.10.2 to rewrite an element of A as a polynomial in the elements of S . SAGBI bases were invented independently by Robbiano and Sweedler [110] and Kapur and Madlener [111]. Unfortunately, even finitely generated subalgebras of $K[x_1, \dots, x_n]$ often do not have finite SAGBI bases. We shall see such examples in Sect. 3.10.3.

3.10.2 Göbel's Algorithm

It follows from Theorem 3.10.1 that the elementary symmetric polynomials can serve as a homogeneous system of parameters for any permutation group $G \leq S_n$. However, it is not clear how the fact that G is a permutation group can be used to facilitate the computation of secondary invariants. It is the algorithm of Göbel [34] which gives a surprising answer to this question. The upshot is that secondary invariants can be chosen among the orbit sums of so-called special monomials (see below). Göbel's algorithm itself gives a representation of an invariant in terms of elementary symmetric polynomials and such orbit sums. We present a generalization of Göbel's algorithm to the case where G is a subgroup of the direct product

$S_{n_1} \times \cdots \times S_{n_r}$. The elementary symmetric polynomials $s_{i,j}$ defined by (3.10.2) will act as primary invariants. We will need the following notation.

G will be a subgroup of the direct product $S_{n_1} \times \cdots \times S_{n_r}$ acting on $R := K[x_{1,1}, \dots, x_{1,n_1}, \dots, x_{r,1}, \dots, x_{r,n_r}]$ as in (3.10.1). We write

$$M := \left\{ \prod_{i=1}^r \prod_{j=1}^{n_i} x_{i,j}^{e_{i,j}} \mid e_{i,j} \in \mathbb{N}_0 \right\}, \quad \text{and} \quad T := \{a \cdot t \mid 0 \neq a \in K, t \in M\}$$

for the set of monomials and terms, respectively. For $f \in R$ with $f = \sum_{t \in M} a_t \cdot t$ let $T(f) := \{a_t \cdot t \mid a_t \neq 0\} \subset T$. For $t \in T$, set

$$\text{orb}_G(t) := \sum_{t' \in \{\sigma \cdot t \mid \sigma \in G\}} t' = \sum_{\sigma \in G/G_t} \sigma \cdot t \in R^G,$$

where G_t is the stabilizer. Note that every element of the orbit enters only once into the sum, so $\text{orb}_G(t)$ is in general not equal to the transfer of t . A monomial $t = \prod_{i=1}^r \prod_{j=1}^{n_i} x_{i,j}^{e_{i,j}} \in M$ is called **special** if for each $i \in \{1, \dots, r\}$ we have

$$\{e_{i,1}, \dots, e_{i,n_i}\} = \{0, \dots, k_i\} \quad \text{with} \quad k_i \in \mathbb{N}_0,$$

where mutually equal $e_{i,j}$ are counted only once, as we are considering the *set* of the $e_{i,j}$. In other words, the exponents in each block cover a range without gaps starting from 0. We write M_{spec} for the set of all special monomials. Observe that for a special term t the total degree is bounded by

$$\begin{aligned} \deg(t) &\leq 1 + 2 + \cdots + (n_1 - 1) + \cdots + 1 + 2 + \cdots + (n_r - 1) \\ &= \binom{n_1}{2} + \cdots + \binom{n_r}{2}. \end{aligned} \quad (3.10.3)$$

In particular, M_{spec} is a finite set. To each term $t \in T$ we associate a special term \tilde{t} by applying the following step iteratively: Let $k \in \mathbb{N}_0$ be minimal with $k \notin \{e_{i,1}, \dots, e_{i,n_i}\}$ but $k < \max\{e_{i,1}, \dots, e_{i,n_i}\}$ for some i . Then lower all $e_{i,j}$ with $e_{i,j} > k$ by 1. Repeat this step until a special term \tilde{t} is obtained. We write $\tilde{t} := \text{Red}(t)$. Loosely speaking, $\text{Red}(t)$ is obtained by shoving the exponents in each block together.

Lemma 3.10.5 *For $t \in T$ and $\sigma \in S_{n_1} \times \cdots \times S_{n_r}$ we have:*

- (a) $\sigma \cdot \text{Red}(t) = \text{Red}(\sigma \cdot t)$,
- (b) $\sigma \cdot \text{Red}(t) = \text{Red}(t) \Leftrightarrow \sigma \cdot t = t$.

Proof Part (a) follows directly from the definition of $\text{Red}(t)$. Hence if $\sigma \cdot t = t$, then $\sigma \cdot \text{Red}(t) = \text{Red}(t)$. If, on the other hand, $\sigma \cdot \text{Red}(t) = \text{Red}(t)$, then

$\text{Red}(\sigma \cdot t) = \text{Red}(t)$, so $\sigma \cdot t$ and t have the same coefficient a . As the application of Red does not change the ordering of the exponents, we conclude $\sigma \cdot t = t$. \square

We introduce a relation \succ on T as follows: For $t = \prod_{i=1}^r \prod_{j=1}^{n_i} x_{i,j}^{e_{i,j}}$ and $t' = \prod_{i=1}^r \prod_{j=1}^{n_i} x_{i,j}^{e'_{i,j}}$ choose permutations $\sigma_1, \sigma'_1 \in S_{n_1}, \dots, \sigma_r, \sigma'_r \in S_{n_r}$ such that for all $i \in \{1, \dots, r\}$ and for $1 \leq j_1 \leq j_2 \leq n_i$ we have

$$e_{i,\sigma_i(j_1)} \geq e_{i,\sigma_i(j_2)} \quad \text{and} \quad e'_{i,\sigma'_i(j_1)} \geq e'_{i,\sigma'_i(j_2)}.$$

Then we say that $t \succ t'$ if there exists an $i_0 \in \{1, \dots, r\}$ and a $j_0 \in \{1, \dots, n_{i_0}\}$ such that

$$e_{i,\sigma_i(j)} = e'_{i,\sigma'_i(j)} \quad \text{if } i < i_0 \text{ or if } i = i_0 \text{ and } j < j_0,$$

and furthermore

$$e_{i_0,\sigma_{i_0}(j_0)} > e'_{i_0,\sigma'_{i_0}(j_0)}.$$

Less formally, one can think of the relation \succ as first comparing the biggest exponent in the first block, then the second-biggest, and so on. If the exponents in the first block agree (up to permutations), the same comparison is performed on the second block and so on. We write $t \preceq t'$ if $t \succ t'$ does not hold. Note that \preceq is not an order even when restricted to M , since $t \preceq t'$ and $t' \preceq t$ fail to imply $t = t'$. But \succ and \preceq are transitive relations, and there exist no infinite, strictly decreasing chains of monomials. We are ready to prove the central lemma (compare Göbel [34, Lemma 3.10]).

Lemma 3.10.6 *Let $t \in T$ be a term and set $u := t / \text{Red}(t) \in M$. Then with $\hat{G} := S_{n_1} \times \dots \times S_{n_r}$ we have*

- (a) $t \succ s$ for all $s \in T(\text{orb}_{\hat{G}}(u) \cdot \text{Red}(t) - t)$,
- (b) $t \succ s$ for all $s \in T(\text{orb}_{\hat{G}}(u) \cdot \text{orb}_G(\text{Red}(t)) - \text{orb}_G(t))$.

Proof

- (a) Obviously t lies in $T(\text{orb}_{\hat{G}}(u) \cdot \text{Red}(t))$. We have to show that $t \succ s$ for all other $s \in T(\text{orb}_{\hat{G}}(u) \cdot \text{Red}(t))$. So take such an s and assume that $t \preceq s$. Clearly $s = (\sigma_1, \dots, \sigma_r) \cdot u \cdot \text{Red}(t)$ with $(\sigma_1, \dots, \sigma_r) \in \hat{G}$. If we can show that $(\sigma_1, \dots, \sigma_r) \cdot u = u$, then $s = t$ and (a) is proved.

Let $\text{Red}(t) = a \prod_{i=1}^r \prod_{j=1}^{n_i} x_{i,j}^{e_{i,j}}$ and $u = \prod_{i=1}^r \prod_{j=1}^{n_i} x_{i,j}^{d_{i,j}}$. Thus t and s have exponents $e_{i,j} + d_{i,j}$ and $e_{i,j} + d_{i,\sigma_i(j)}$, respectively. By renumbering the $x_{i,j}$, we may assume that $e_{i,j} \geq e_{i,j'}$ for $j \leq j'$, and then also $d_{i,j} \geq d_{i,j'}$ by the construction of $\text{Red}(t)$. Let k be maximal with $d_{1,1} = d_{1,2} = \dots = d_{1,k}$. Then $t \preceq s$ implies that σ_1 must permute the set $\{1, \dots, k\}$, since the biggest exponents in the first block of t and s must coincide. Proceeding analogously for the second-highest exponents $d_{1,k+1}, \dots, d_{1,l}$, we conclude that σ_1 also permutes $\{k+1, \dots, l\}$, and

finally arrive at $\sigma_1 \cdot \prod_{j=1}^{n_1} x_{1,j}^{d_{1,j}} = \prod_{j=1}^{n_1} x_{1,j}^{d_{1,j}}$. The same argument shows that σ_2 fixes the second block of u , and so on. Thus indeed $(\sigma_1, \dots, \sigma_r) \cdot u = u$.

(b) For $\sigma \in G$ we have by (a)

$$\sigma \cdot t \succ s \quad \text{for all } s \in T \left(\text{orb}_{\hat{G}} \left(\frac{\sigma \cdot t}{\text{Red}(\sigma \cdot t)} \right) \cdot \text{Red}(\sigma \cdot t) - \sigma \cdot t \right),$$

hence also $t \succ s$ for these s . But by Lemma 3.10.5(a)

$$\text{orb}_{\hat{G}} \left(\frac{\sigma \cdot t}{\text{Red}(\sigma \cdot t)} \right) \cdot \text{Red}(\sigma \cdot t) = \text{orb}_{\hat{G}}(\sigma \cdot u) \cdot \sigma \cdot \text{Red}(t) = \text{orb}_{\hat{G}}(u) \cdot \sigma \cdot \text{Red}(t).$$

Therefore

$$t \succ s \quad \text{for all } s \in T \left(\text{orb}_{\hat{G}}(u) \cdot \sigma \cdot \text{Red}(t) - \sigma \cdot t \right).$$

Now by Lemma 3.10.5(b), the $\sigma \in G$ fixing t are the same that fix $\text{Red}(t)$, so summation over coset representatives σ of the stabilizer of t in G yields the result. \square

We can give Göbel's algorithm now. The purpose of the algorithm is to write an invariant as a linear combination of orbits sums of special monomials, where the coefficients of this linear combination are polynomials in the elementary symmetric polynomials $s_{i,j}$.

Algorithm 3.10.7 (Göbel's algorithm) Let $G \leq \hat{G} := S_{n_1} \times \dots \times S_{n_r}$ be a subgroup acting on $R := K[x_{1,1}, \dots, x_{1,n_1}, \dots, x_{r,1}, \dots, x_{r,n_r}]$ as in (3.10.1). Given an invariant $f \in R^G$, perform the following steps.

- (1) Set $g := f$, and for each $t \in M_{\text{spec}}$ set $F_t := 0$.
- (2) While $g \neq 0$, perform steps i–iv.

- (i) Choose $t \in T(g)$ which is maximal with respect to the relation \succ .
- (ii) Compute $\text{Red}(t) =: a \cdot \tilde{t}$ with $\tilde{t} \in M_{\text{spec}}$ and set $u := t / \text{Red}(t)$.
- (iii) Use Algorithm 3.10.2 to represent $\text{orb}_{\hat{G}}(u)$ in terms of the elementary symmetric polynomials (3.10.2):

$$\text{orb}_{\hat{G}}(u) = F(s_{1,1}, \dots, s_{1,n_1}, \dots, s_{r,1}, \dots, s_{r,n_r})$$

with F a polynomial.

- (iv) Set

$$g := g - \text{orb}_{\hat{G}}(u) \cdot \text{orb}_G(\text{Red}(t))$$

and $F_{\tilde{t}} := F_{\tilde{t}} + aF$.

(3) When $g = 0$ is reached, we have

$$f = \sum_{t \in M_{\text{spec}}} F_t(s_{1,1}, \dots, s_{1,n_1}, \dots, s_{r,1}, \dots, s_{r,n_r}) \cdot \text{orb}_G(t). \quad (3.10.4)$$

It is clear that Algorithm 3.10.7 is correct if it terminates.

Theorem 3.10.8 *Algorithm 3.10.7 terminates after a finite number of steps.*

Proof Each pass through the while-loop (i)–(iv) replaces g by

$$g - \text{orb}_G(t) + (\text{orb}_G(t) - \text{orb}_{\hat{G}}(u) \cdot \text{orb}_G(\text{Red}(t))).$$

Since G permutes the terms in $T(g)$, each term of $\text{orb}_G(t)$ is also a term of g . Therefore and by Lemma 3.10.6, some maximal terms are removed from g , and only strictly smaller terms are added. Hence after a finite number of steps the maximum of $T(g)$ with respect to $>$ decreases strictly, and iterating further eventually yields $g = 0$, since every strictly decreasing sequence of terms is finite. \square

Algorithm 3.10.7 was implemented by Göbel [5] in the computer algebra system MAS (see Kredel [112]). This forms a package in MAS which is now included in the standard distribution.

It is clear from (3.10.4) that the orbit sums of the special monomials form a (usually nonminimal) system of secondary invariants. The number of orbit sums of special monomials was studied by Göbel [113]. Since the degree of a special monomial is bounded from above by (3.10.3), we obtain the following degree bound, which is a special case of Symonds' bound (Theorem 3.3.7).

Corollary 3.10.9 *Let $G \leq S_{n_1} \times \cdots \times S_{n_r}$ be a subgroup acting on $R := K[x_{1,1}, \dots, x_{1,n_1}, \dots, x_{r,1}, \dots, x_{r,n_r}]$ as in (3.10.1). If one chooses the elementary symmetric polynomials $s_{i,j}$ ($1 \leq i \leq r$, $1 \leq j \leq n_r$) given by (3.10.2) as primary invariants, then the secondary invariants have degrees at most*

$$\binom{n_1}{2} + \cdots + \binom{n_r}{2}.$$

In particular,

$$\beta(R^G) \leq \max\{\binom{n_1}{2} + \cdots + \binom{n_r}{2}, n_1, \dots, n_r\}.$$

Remark 3.10.10

- (a) Although this is not stated in Corollary 3.10.9, the bound for the secondary invariants continues to hold when K is replaced by any commutative ring.

- (b) With an appropriate generalization of the notion of special monomials, Göbel's algorithm and degree bound can be generalized to monomial groups, i.e., groups consisting of permutation matrices where the 1's may be replaced by roots of unity (see Kemper [33]). Again, the degree bound obtained for the secondary invariants is a special case of Symonds' bound. \triangleleft

3.10.3 SAGBI Bases

We have seen in Sect. 3.10.1 that the invariant ring of a direct product of symmetric groups has a finite SAGBI basis. The following example shows that invariant rings of finite groups do not always have finite SAGBI bases, even in characteristic 0.

Example 3.10.11 (Göbel [34]) Consider the action of the cyclic group $G = \langle \sigma \rangle \cong C_3$ of order 3 on $R := K[x_1, x_2, x_3]$ by $\sigma: x_1 \mapsto x_2 \mapsto x_3 \mapsto x_1$. Fix the lexicographic monomial ordering with $x_1 > x_2 > x_3$. In order to show that R^G has no finite SAGBI basis, we have to convince ourselves that the leading algebra $L(R^G)$ is not finitely generated as an algebra over K . So assume, by way of contradiction, that $L(R^G)$ is finitely generated. Then the quotient $L(R^G)_+ / (L(R^G)_+)^2$ is finitely generated as a K -vector space, so there exists an integer N such that $\text{LM}(f) \in (L(R^G)_+)^2$ for every homogeneous invariant f of degree at least N . But we have

$$\text{LM}(x_1^{i-1}x_2^i + x_2^{i-1}x_3^i + x_1^ix_3^{i-1}) = x_1^ix_3^{i-1},$$

which does not lie in $(L(R^G)_+)^2$, since there is no monomial $x_1^jx_3^k$ with $j \leq k$ in $L(R^G)_+$. Hence there is no bound N , and $L(R^G)$ is indeed not finitely generated. \triangleleft

Even more discouraging is a result of Göbel which gives a converse to Theorem 3.10.1

Theorem 3.10.12 (Göbel [114]) *Let $G \leq S_n$ be a permutation group acting on $R := K[x_1, \dots, x_n]$ by $\sigma \cdot x_i = x_{\sigma(i)}$. Then there exists a finite SAGBI basis of the invariant ring R^G with respect to the lexicographic monomial ordering if and only if G is a direct product of symmetric groups acting as in (3.10.1).*

The “if” direction is Theorem 3.10.1, and the “only if” direction is the main result of [114]. We do not give the proof here.

It may seem that Theorem 3.10.12 shatters all hope that SAGBI bases can be of any use in invariant theory of finite groups. However, whether or not a finite SAGBI basis exists depends very much on the basis of V that is chosen. Indeed, SAGBI bases for the invariant ring of the cyclic group of order p acting in various ways were computed by Shank [45], Shank and Wehlau [46], Campbell et al. [47], and Duncan et al. [48]. They used bases of V such that the action assumes upper triangular form, and the graded reverse lexicographic monomial ordering. Obtaining a SAGBI basis is a crucial element in this approach, since this enables him to compute the Hilbert

series of a subalgebra of the invariants and comparing this to the “target” Hilbert series (see Sect. 3.4.2). More generally, we have the following result.

Proposition 3.10.13 (Shank [115], Shank and Wehlau [116]) *Let G be a finite group and V a KG -module whose dual V^* has a basis x_1, \dots, x_n such that*

$$\sigma \cdot x_i \in Kx_i \oplus \cdots \oplus Kx_n$$

for every $\sigma \in G$ and every $i = 1, \dots, n$. Then $K[V]^G$ has a finite SAGBI basis with respect to any monomial ordering with $x_1 > x_2 > \cdots > x_n$.

Proof By the special form of the action, the invariant $N_i := \prod_{\sigma \in G} (\sigma \cdot x_i)$ has the leading monomial

$$\text{LM}(N_i) = x_i^{|G|}.$$

Hence $A := K[x_1^{|G|}, \dots, x_n^{|G|}]$ is contained in $L(K[V]^G)$. But $K[V]$ is finitely generated as a module over A and hence a Noetherian module. Therefore the submodule $L(K[V]^G)$ is also Noetherian over A . Thus $L(K[V]^G)$ is finitely generated. \square

Remark 3.10.14 If G is a p -group with $p = \text{char}(K)$, then a basis as required in Proposition 3.10.13 always exists. For example, the invariant ring considered in Example 3.10.11 does have a finite SAGBI basis in the case $\text{char}(K) = 3$ (but only after changing the vector space basis). \triangleleft

SAGBI bases are also used by Stillman and Tsai [117] to compute invariants of tori and finite abelian groups.

3.11 Ad Hoc Methods

It quite often happens that the algorithms given in the above sections (especially Sects. 3.5 and 3.7) are not feasible due to large time or memory requirements. In such cases one has to put one’s hope in ad hoc methods, which may work and produce the invariant ring. The chances of success are particularly high if one already has a guess of a nice structure of the invariant ring. In any case, ad hoc methods depend on a mixture of experience, luck and optimism. The methods that we employ in this section are far from covering all the ad hoc methods for computing invariants that are around. For example, Shank and Wehlau [116] provide an assortment of methods which are well suited for the computation of invariants of p -groups in characteristic p . We will give an account of some methods in this section, and use the following example throughout. Let $G := W_3(H_4)$ be the 3-modular reduction of the Weyl group of type H_4 of order 14 400. According to the classification of Shephard and Todd [86], $G = W_3(G_{30})$ is the 3-modular reduction

of the irreducible complex reflection group number 30. Thus G is generated by reflections, but since its order is a multiple of the characteristic of K , the invariant ring need not be isomorphic to a polynomial ring (see Sect. 3.9.4). So the question is whether $K[V]^G$ is a polynomial ring or not, and if not, what structure it has then. G is a subgroup of $\mathrm{GL}_4(\mathbb{F}_9)$ and can be generated by the full permutation group S_4 together with the matrices

$$\begin{pmatrix} -1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & -1 & -1 & \zeta^2 \\ -1 & 0 & -1 & \zeta^2 \\ -1 & -1 & 0 & \zeta^2 \\ \zeta^2 & \zeta^2 & \zeta^2 & -1 \end{pmatrix},$$

where $\zeta \in \mathbb{F}_9$ is an element of order 8. Trying the standard algorithms on this group quickly shows that even the construction of primary invariants runs into serious memory problems. In Example 3.7.6(b) we have calculated the invariant ring of a Sylow p -subgroup of G , for $p = 3$, and seen that this invariant ring is Cohen-Macaulay. It follows by Remark 3.6.2(b) that the invariant ring $K[V]^G$ of G is also Cohen-Macaulay.

All explicit calculations in this section were done in MAGMA.

3.11.1 Finding Primary Invariants

The following observation gives lower bounds for the degrees of primary invariants.

Proposition 3.11.1 *For a finite group G and an n -dimensional KG -module V , let $J_d \subseteq K[V]$ be the ideal generated by the homogeneous invariants $K[V]_k^G$ with $0 < k \leq d$. If $d_1 \leq \dots \leq d_n$ are the degrees of primary invariants, then*

$$d_i \geq \min\{d \mid \dim(R/J_d) \leq n - i\}.$$

Proof By Proposition 3.5.1(d) we have

$$n - i = \dim(K[V]/(f_1, \dots, f_i)) \geq \dim(K[V]/J_{d_i}).$$

This yields the result. \square

We now apply Proposition 3.11.1 to the group $G = W_3(H_4)$. The computation of the homogeneous components $K[V]_d^G$ is feasible up to degrees around $d = 40$, and Proposition 3.11.1 yields

$$d_1 \geq 2, \quad d_2 \geq 10, \quad \text{and} \quad d_3 \geq 36,$$

but no information on the last degree d_4 (except that $d_4 > 40$). By trying random invariants f_2, f_{10}, f_{36} of degrees 2, 10 and 36 (computed by the method of Sect. 3.1.1), we are lucky enough to arrive at an ideal (f_2, f_{10}, f_{36}) of dimension 1, so there is only one further primary invariant missing. We have

$$f_2 = x_1^2 + x_2^2 + x_3^2 + x_4^2, \quad f_{10} = x_1^{10} + x_2^{10} + x_3^{10} + x_4^{10},$$

but f_{36} is much more complicated. By Proposition 3.5.5 the degree d_4 of the missing primary invariant must be a multiple of $|G|/(d_1 d_2 d_3) = 20$. Since $d_4 > 40$, we might hope to find the last primary invariant of degree 60. However, it is impossible due to time and storage problems to compute all invariants of degree 60. Instead, we try to construct a polynomial f_{60} of degree 60 by using Steenrod operations.

Steenrod operations are a very helpful tool in modular invariant theory, and we briefly explain their definition following Smith [2]. Suppose $K = \mathbb{F}_q$ is a finite field. We take an additional indeterminate T and define a homomorphism $P: K[V] \rightarrow K[V][T]$ of K -algebras by sending an $x \in V^*$ to $x + x^q \cdot T \in K[V][T]$. It is easily checked that P commutes with the action of $\mathrm{GL}(V)$ on $K[V]$. For $f \in K[V]$, write

$$P(f) = \sum_{i \geq 0} \mathcal{P}^i(f) \cdot T^i.$$

Then $\mathcal{P}^i(f)$ is the i -th Steenrod operation on f . It follows from the $\mathrm{GL}(V)$ -compatibility of P that Steenrod operations applied to invariants yield invariants again. It is also easy to check that for a homogeneous f

$$\deg(\mathcal{P}^i(f)) = \deg(f) + i(q - 1)$$

if $\mathcal{P}^i(f)$ is nonzero, and $\mathcal{P}^i(f) = 0$ if $i > \deg(f)$. Let us note here that the Steenrod operations provide a modular invariant ring with an additional structure of an unstable algebra over the Steenrod algebra (see Smith [2, p. 296]). This structure has been successfully used to prove results in modular invariant theory (see Adams and Wilkerson [118], Bourguiba and Zarati [119], Neusel [120], to mention just a few). For an approach to the Steenrod algebra which is different from the one presented above, the reader might turn to Wood [121].

In this book we only use Steenrod operations to produce new invariants from old ones. In the case $G = W_3(H_4)$, we first note that $f_{10} = -\mathcal{P}^1(f_2)$. Now $f_{60} := \mathcal{P}^3(f_{36})$ has the desired degree 60, and indeed we are lucky enough to find that the ideal generated by f_2, f_{10}, f_{36} and f_{60} has dimension 0. Thus a complete system of primary invariant is found. Since this system is optimal in the sense that no primary invariants of smaller degrees could be chosen, we conclude already here that $K[V]^G$ is not a polynomial ring, since

$$\frac{\deg(f_2) \cdot \deg(f_{10}) \cdot \deg(f_{36}) \cdot \deg(f_{60})}{|G|} = 3, \tag{3.11.1}$$

and this quotient should be 1 if $K[V]^G$ were polynomial by Theorem 3.9.4.

3.11.2 Finding Secondary Invariants

We start by presenting an alternative algorithm for computing secondary invariants. The reason why we put this into the section on ad hoc methods is that we believe that the algorithm will only perform better than the ones given in Sect. 3.7 if the invariant ring has a nice structure (see Remark 3.11.5(e)). The algorithm is based on the following result.

Proposition 3.11.2 *Suppose that $R \subseteq K[V]^G$ is a subalgebra of an invariant ring of a finite group. Then $R = K[V]^G$ if and only if all of the following three conditions hold:*

- (a) *R contains a system of primary invariants f_1, \dots, f_n .*
- (b) $[Quot(R) : K(f_1, \dots, f_n)] = \frac{\deg(f_1) \cdots \deg(f_n)}{|G|}$.
- (c) *R is normal.*

In (b), $[Quot(R) : K(f_1, \dots, f_n)]$ denotes the degree of $Quot(R)$ as a field extension of the subfield generated by the f_i .

Proof First suppose that $R = K[V]^G$. Then (a) holds, and Lemma 3.11.3 below shows that $Quot(R) = K(V)^G$, hence (b) follows from Eq. (3.9.1). Since the polynomial ring $K[V]$ is normal, (c) follows from Proposition 2.4.4.

Now suppose that (a)–(c) hold for R , and take any invariant $f \in K[V]^G$. It follows from (b) and Eq. (3.9.1) that $Quot(R) = K(V)^G$, hence $f \in Quot(R)$. Moreover, f is integral over R by (a), hence (c) implies that $f \in R$. \square

In the above proof we used the following result, which is interesting in itself.

Lemma 3.11.3 *Let $K(V) := Quot(K[V])$ be the rational function field on V , and $K(V)^G := \{f \in K(V) \mid \sigma \cdot f = f \ \forall \sigma \in G\}$ the invariant field. Then*

$$K(V)^G = Quot(K[V]^G).$$

Proof Clearly $Quot(K[V]^G) \subseteq K(V)^G$. Conversely, take $f/g \in K(V)$ with $f, g \in K[V]$ such that $f/g \in K(V)^G$. Then

$$\frac{f}{g} = \frac{f \cdot \prod_{\sigma \in G \setminus \{\text{id}\}} \sigma \cdot g}{\prod_{\sigma \in G} \sigma \cdot g} \in Quot(K[V]^G),$$

since the denominator of the right hand fraction is G -invariant, and therefore also the numerator. \square

It is quite easy to turn Proposition 3.11.2 into an algorithm. Indeed, if $R = K[f_1, \dots, f_n, g_1, \dots, g_m]$, we have Gröbner basis methods for computing the relations between the f_i and g_j (see Sect. 1.2.2). From these, the degree of $Quot(R)$ over $K(f_1, \dots, f_n)$ can easily be determined. (Sweedler [122] would be a reference for the relevant algorithms, but in our special situation it is almost immediately clear

what to do.) Moreover, the relations can be used to check whether R is normal (see Sect. 1.6), or to extend R if it is not. We obtain the following algorithm. It computes generators for $K[V]^G$ as an algebra over K . If needed, secondary invariants can then be constructed from these.

Algorithm 3.11.4 (Calculate generators of $K[V]^G$) Let G be a finite group and V a finite dimensional KG -module, where K is a perfect field. Suppose we are given primary invariants f_1, \dots, f_n . To obtain homogeneous invariants g_1, \dots, g_m which together with f_1, \dots, f_n generate $K[V]^G$ as a K -algebra, proceed as follows.

- (1) If $\deg(f_1) \cdots \deg(f_n) = |G|$, then by Theorem 3.9.4 $K[V]^G$ is generated by the f_i and we are done. Otherwise, set $m := 1$.
- (2) Let g_m be a homogeneous invariant of minimal degree not contained in $R_{m-1} := K[f_1, \dots, f_n, g_1, \dots, g_{m-1}]$. Invariants can be found by the methods of Sect. 3.1, and membership in R_{m-1} can be tested by linear algebra.
- (3) Using a monomial ordering “ $>$ ” with

$$Y_j \gg T_1, \dots, T_n, Y_1, \dots, Y_{j-1}$$

for all $j = 1, \dots, m$, compute a Gröbner basis \mathcal{G} of the kernel I of the map

$$\Phi: K[T_1, \dots, T_n, Y_1, \dots, Y_m] \rightarrow R_m, \quad T_i \mapsto f_i, \quad Y_j \mapsto g_j.$$

This can be done by the methods of Sect. 1.2.2. Assigning degrees $\deg(T_i) := \deg(f_i)$ and $\deg(Y_j) := \deg(g_j)$ makes I into a homogeneous ideal, and we can assume that the polynomials from \mathcal{G} are also homogeneous.

- (4) Let e_j be the minimal Y_j -degree of a polynomial in \mathcal{G} involving the variable Y_j but none of Y_{j+1}, \dots, Y_m . If

$$e_1 \cdots e_m < \frac{\deg(f_1) \cdots \deg(f_n)}{|G|},$$

then set $m := m + 1$ and go back to step (2).

- (5) Choose an $(m \times m)$ -minor $f \in K[T_1, \dots, T_n, Y_1, \dots, Y_m]$ of the Jacobian matrix of the polynomials in \mathcal{G} such that $f \notin I$, and set $J := \sqrt{I + (f)}$.
- (6) Choose a homogeneous $g \in J \setminus I$ (e.g., $g = f$), and compute the colon ideal $(g \cdot J + I) : J$. If this ideal is contained in $(g) + I$, then we are done.
- (7) Otherwise, choose a homogeneous $h \in ((g \cdot J + I) : J) \setminus ((g) + I)$ and set $m := m + 1$ and $g_m := \Phi(h)/\Phi(g)$.
- (8) Compute a homogeneous generating set \mathcal{G} of the kernel I of the map

$$\Phi: K[T_1, \dots, T_n, Y_1, \dots, Y_m] \rightarrow R_m, \quad T_i \mapsto f_i, \quad Y_j \mapsto g_j$$

(possibly using Lemma 1.3.2), and go back to step (5).

The following remark contains a justification why the algorithm is correct.

Remark 3.11.5

- (a) In step (4), a polynomial of minimal positive Y_j -degree involving only T_1, \dots, T_m and Y_1, \dots, Y_j provides a minimal polynomial for g_j over the field $K(f_1, \dots, f_n, g_1, \dots, g_{j-1})$. Therefore

$$e_j = [K(f_1, \dots, f_n, g_1, \dots, g_j) : K(f_1, \dots, f_n, g_1, \dots, g_{j-1})],$$

and it follows that the product of the e_j is the degree of $K(f_1, \dots, f_n, g_1, \dots, g_n)$ over $K(f_1, \dots, f_n)$. Thus when we get to step (5), the properties (a) and (b) of Proposition 3.11.2 are already satisfied.

- (b) By the remark preceding Algorithm 1.6.4, the ideal J formed in step (5) satisfies the assumption of Theorem 1.6.2. Moreover, f is homogeneous since the elements of \mathcal{G} are homogeneous.
- (c) Steps (6) and (7) are applications of Theorem 1.6.2. Note that $\Phi(h)$ will automatically be divisible by $\Phi(g)$ (as polynomials in $K[V]$).
- (d) Algorithm 3.11.4 is not guaranteed to produce a minimal set $\{g_1, \dots, g_m\}$ of invariants which together with the f_i generates $K[V]^G$. But such a set can be obtained by eliminating redundant generators. Moreover, secondary invariants can be constructed by taking products of the g_j .
- (e) Experience shows that in cases where the invariant ring is not a complete intersection, it is usually more expensive to compute relations between generating invariants than to compute the invariant ring itself using the “standard” algorithms from Sect. 3.7. Since Algorithm 3.11.4 requires the computation of relations in each loop, we conclude that its performance is worse than that of the standard algorithms unless $K[V]^G$ has a nice structure. \triangleleft

We return to the example $G = W_3(H_4)$. In Sect. 3.11.1 we have found primary invariants of degrees 2, 10, 36 and 60. We have also seen in Example 3.7.6(b) that the invariant ring of a Sylow 3-subgroup of G is Cohen-Macaulay. Hence by Remark 3.6.2(b) the invariant ring $K[V]^G$ of G is also Cohen-Macaulay. Thus by Theorem 3.9.1 and Eq. (3.11.1) the number of secondary invariants is 3. The first secondary invariant is always 1. In order to find the next one, we search for a homogeneous invariant of minimal degree not contained in $A := K[f_2, f_{10}, f_{36}, f_{60}]$. The membership test is done by equating an invariant from a basis of $K[V]_d^G$ (computed by the methods of Sect. 3.1) to a general element of A of degree d and checking solvability of the corresponding linear system. We find the next secondary, g_{22} , in degree 22. Now we boldly make the guess that the secondary invariants are 1, g_{22} and g_{22}^2 . In other words, we wish to show that $K[V]^G$ is generated as an algebra by the f_i and g_{22} . The property (b) of Proposition 3.11.2 is clearly satisfied, since $g_{22} \notin K(f_2, f_{10}, f_{36}, f_{60})$ and $[K(V)^G : K(f_2, f_{10}, f_{36}, f_{60})] = 3$.

In order to show property (c) of Proposition 3.11.2, we have to get a presentation for the algebra generated by the f_i and g_{22} . It is hopeless to get this by the standard methods of Sect. 1.2.2. But if it is true that 1, g_{22} and g_{22}^2 form a system of secondary

invariants, then g_{22}^3 will be an A -linear combination of 1, g_{22} and g_{22}^2 . Equating g_{22}^3 to such a linear combination of degree 66 with unknown coefficients, we see that the corresponding linear system is solvable indeed and obtain the relation

$$\begin{aligned} g_{22}^3 + (f_2^{11} - f_2 f_{10}^2) g_{22}^2 + \\ (f_2^{17} f_{10} - f_2^7 f_{10}^3 - f_2^{12} f_{10}^2 + f_2^4 f_{36} + f_2^2 f_{10}^4) g_{22} + \\ + f_2^{18} f_{10}^3 - f_2^{28} f_{10} + f_{10}^3 f_{36} + f_2^{15} f_{36} - \\ f_2^{13} f_{10}^4 - f_2^5 f_{10}^2 f_{36} + f_2^8 f_{10}^5 - f_2^3 f_{60} = 0. \end{aligned} \quad (3.11.2)$$

We claim that this relation generates the kernel I of

$$\Phi: K[T_2, T_{10}, T_{36}, T_{60}, Y_{22}] \rightarrow K[f_2, f_{10}, f_{36}, f_{60}, g_{22}], \quad T_i \mapsto f_i, \quad Y_{22} \mapsto g_{22}.$$

Indeed, if there existed a relation not divisible by (3.11.2), then the division algorithm would yield a relation of Y_{22} -degree smaller than 3, in contradiction to $[K(f_2, f_{10}, f_{36}, f_{60}, g_{22}) : K(f_2, f_{10}, f_{36}, f_{60})] = 3$.

We can now go into step (5) of Algorithm 3.11.4. As a (1×1) -minor of the Jacobian matrix we choose the derivative of the relation with respect to T_{60} , which is $-T_2^3$. Hence $T_2 \in J = \sqrt{I + (T_2^3)}$. On the other hand,

$$I + (T_2) = (T_2, Y_{22}^3 + T_{10}^3 T_{36})$$

is a prime ideal, so it is equal to J . Choose $g = T_2$. We have to show that $(g \cdot J + I) : J \subseteq (g) + I$, so take any $h \in (g \cdot J + I) : J$. Then $T_2 h \in T_2 \cdot J + I$, so, writing r for the relation (3.11.2), we have

$$T_2 h = h_1 T_2^2 + h_2 r$$

with polynomials h_1, h_2 . Thus T_2 divides $h_2 r$, but it does not divide r , so $h_2 = h_3 T_2$ with another polynomial h_3 . Dividing by T_2 , we obtain

$$h = h_1 T_2 + h_3 r \in (T_2) + I.$$

It follows that indeed $(g \cdot J + I) : J \subseteq (g) + I$, and we conclude from Proposition 3.11.2 that $K[V]^G = K[f_2, f_{10}, f_{36}, f_{60}, g_{22}]$. Therefore even though $K[V]^G$ is not a polynomial ring, it is a complete intersection (more specifically, a hypersurface, i.e., a K -algebra of Krull dimension n that is generated by $n+1$ elements).

3.11.3 The Other Exceptional Reflection Groups

The previous calculation showed us that the invariant ring of $W_3(G_{30})$ is a hypersurface. But what about the other finite irreducible reflection group that appear in Table 3.1 p. 118 and have nonpolynomial invariant rings? The second author used methods like those described above to determine the structure of the invariant rings of the *exceptional* reflection groups, i.e., those groups appearing in the last row of Table 3.1. The results are summarized in Table 3.2.

In Table 3.2 we list the relevant finite irreducible complex reflection groups according to the classification of Shephard and Todd [86]. For each of these, we give the dimension of the action, the group order, and the structures of the invariant rings of the p -modular reduction $W_p(G_i)$ for those primes p where nonpolynomial invariants rings occur. A “–” in the table signifies that the corresponding reduction becomes reducible or isomorphic to a classical group. “PR”, “HS”, and “nCM” mean that the invariant ring is a polynomial ring, a hypersurface, or not Cohen-Macaulay, respectively. It is probably a coincidence that in this table nothing appears between hypersurface and non-Cohen-Macaulay. For the results on non-Cohen-Macaulayness, Theorem 3.9.3 (with the algorithm for computing cohomology described after Theorem 3.9.3) and the following proposition was used.

Proposition 3.11.6 (Kemper [123], Korollar 5.14, or 124]) *Suppose that $K[V]^G$ is Cohen-Macaulay. Then for every linear subspace $W \subseteq V$ the invariant ring $K[V]^{G_W}$ of the point-wise stabilizer G_W is also Cohen-Macaulay.*

The above proposition is very similar in style to Proposition 3.9.7, and in fact a unified proof can be given for both (see [124]).

Table 3.2 Invariant rings of exceptional modular reflection groups

G	$\dim(V)$	$ G $	$p = 2$	$p = 3$	$p = 5$	$p = 7$
G_{24}	3	336	PR	PR	PR	HS
G_{28}	4	1152	–	HS	PR	PR
G_{30}	4	14,400	–	HS	HS	PR
G_{31}	4	46,080	HS	HS	PR	PR
G_{32}	4	155,520	–	–	nCM	PR
G_{33}	5	51,840	–	HS	PR	PR
G_{34}	6	39,191,040	HS	–	PR	PR
G_{36}	7	2,903,040	–	nCM	PR	PR
G_{37}	8	696,729,600	–	nCM	nCM	PR

3.12 Separating Invariants

Let us pick up the topic of separating subalgebras, as introduced in Sect. 2.4.

3.12.1 Degree Bounds

Recall that Noether's degree bound fails in the modular case. But instead of asking for degree bounds for generating invariants, we will now ask for degree bounds for separating invariants. The next theorem gives a way for calculating separating invariants *explicitly* for any finite group. All that is required is multiplying out a (large) polynomial.

Theorem 3.12.1 *Let x_1, \dots, x_n be a basis of V^* and form the polynomial*

$$F := \prod_{\sigma \in G} \left(T - \sum_{i=1}^n U^{i-1} \cdot (\sigma \cdot x_i) \right) \in K[V]^G[U, T]$$

with U and T indeterminates. Then the coefficients of F (as a polynomial in U and T) generate a separating subalgebra of $K[V]^G$.

Proof Let $v, w \in V$ such that all coefficients of F agree on v and w . Then

$$\prod_{\sigma \in G} \left(T - \sum_{i=1}^n U^{i-1} \cdot (\sigma \cdot x_i)(v) \right) = \prod_{\sigma \in G} \left(T - \sum_{i=1}^n U^{i-1} \cdot (\sigma \cdot x_i)(w) \right),$$

so there exists $\sigma \in G$ such that $\sum_{i=1}^n U^{i-1} \cdot x_i(w) = \sum_{i=1}^n U^{i-1} \cdot \sigma \cdot x_i(v)$. This implies $w = \sigma^{-1} \cdot v$, so v and w lie in the same G -orbit, and therefore $f(v) = f(w)$ for all $f \in K[V]^G$. \square

Remark 3.12.2 It is straightforward to generalize Theorem 3.12.1 in various directions: K may be substituted by an integral domain, and X may be substituted by an affine variety X on which G acts. In the second case, it suffices that $x_1, \dots, x_n \in K[X]$ separate points from X . A statement that contains all these (and more) generalizations can be found in Kemper [125, Theorem 16]. \triangleleft

In order to consider degree bounds for separating invariants we define

$$\beta_{\text{sep}}(K[V]^G) := \min \left\{ k \in \mathbb{N}_0 \mid \bigoplus_{d=1}^k K[V]_d^G \text{ is a separating subset} \right\}.$$

It follows immediately from Theorem 3.12.1 that Noether's degree bound holds for separating invariants without any hypothesis on $\text{char}(K)$.

Corollary 3.12.3 $\beta_{\text{sep}}(K[V]^G) \leq |G|$.

Remark 3.12.4 By Kemper [125, Corollary 24], the following relative version holds: If $G \subseteq \text{GL}(V)$ (which need not be finite) and $H \subseteq G$ is a subgroup of finite index, then

$$\beta_{\text{sep}}(K[V]^G) \leq [G : H] \cdot \beta_{\text{sep}}(K[V]^H).$$

△

We obtain the following consequence from Corollary 3.12.3 and Theorem 2.4.6:

Corollary 3.12.5 *Let $A \subseteq K[V]^G$ be the subalgebra generated by all homogeneous invariants of degree $\leq |G|$. If $p = \text{char}(K) > 0$, then there exists a p -power q such that $f^q \in A$ for every $f \in K[V]^G$.*

3.12.2 Polynomial Separating Subalgebras and Reflection Groups

Recall that the invariant ring $K[V]^G$ can only be polynomial if G is generated by reflections (see Sect. 3.9.4). This result is attributed to J.P. Serre. The following theorem gives a very nice and interesting generalization. Before stating it we make a remark about how separating invariants should be understood geometrically. If K is a finite field, there exist finite groups (such as $\text{GL}(V)$) that have only two orbits. By Theorem 3.12.1 there always exists a homogeneous invariant f that is nonconstant on V , so $A = K[f]$ is a separating subalgebra. This is undesired since, for example, the assertion of Proposition 2.4.3 is violated. Another undesired example is that $x^3 \in \mathbb{R}[x]$ is separating for the trivial group. To give the term separating invariants a truly geometric meaning, we should therefore, as in Proposition 2.4.3 make the assumption that K is algebraically closed. Going a little less far, we follow Dufresne [89] and call a subset $S \subseteq K[V]^G$ **geometrically separating** if any two points in $\overline{K} \otimes V$ (with \overline{K} an algebraic closure of K) that can be separated by an invariant from $K[V]^G$ can also be separated by an invariant from S . It is clear that every generating set in $K[V]^G$ is geometrically separating.

Theorem 3.12.6 (Dufresne [89]) *Suppose that $K[V]^G$ has a geometrically separating subset of size $n = \dim(V)$. Then G is generated by reflections.*

We will present a proof for this theorem. The proof is much simpler than the original proof of the less general result of Serre, and quite different. It relies on Hartshorne's connectedness theorem, which can be stated as follows:

Theorem 3.12.7 (Hartshorne [126] or Eisenbud [55, Theorem 18.12]) *Let R be a Noetherian ring such that $\text{Spec}(R)$ is connected, and let $I, J \subseteq R$ be*

two nonnilpotent ideals (i.e., $I, J \not\subseteq \sqrt{\{0\}}$) such that $I \cap J$ is nilpotent. Then $\text{depth}(I + J, R) \leq 1$. In particular, if R is Cohen-Macaulay, then $\text{ht}(I + J) \leq 1$.

In more geometric terms, the theorem says that if R is Cohen-Macaulay and $X := \text{Spec}(R)$ (which is assumed to be connected) is written as a union of two proper, closed subsets $Y, Z \subset X$, then $Y \cap Z$ has codimension at most 1. In other words, removing a closed subset of codimension ≥ 2 from X does not disconnect it. This property is usually expressed by saying that X is connected in codimension one. An equivalent statement is the following: If Z and Z' are irreducible components of X , then there exists a sequence $Z = Z_1, Z_2, \dots, Z_r = Z'$ of irreducible components Z_i such that each $Z_i \cap Z_{i+1}$ has codimension at most one.

We will apply the connectedness theorem in the case where $R = K[x_1, \dots, x_n]/I$ is a quotient of a polynomial ring over an algebraically closed field. Then the above statements hold for the affine variety $X = \mathcal{V}(I)$: If R is Cohen-Macaulay and X is connected, then it is connected in codimension one. Hartshorne [126] also showed that if R is a complete intersection, i.e., I can be generated by $n - \dim(R)$ polynomials, then the hypothesis that R is Cohen-Macaulay holds. Here I is not assumed to be a radical ideal or homogeneous.

Proof of Theorem 3.12.6 We may assume K to be algebraically closed. Consider the so-called graph of the action

$$X := \{(v, \sigma \cdot v) \mid v \in V, \sigma \in G\} \subseteq V \oplus V.$$

The irreducible components of X are the $Z_\sigma = \{(v, \sigma \cdot v) \mid v \in V\} \cong V$ (for $\sigma \in G$), and therefore $\dim(X) = n$. For $\sigma, \tau \in G$ we have

$$Z_\sigma \cap Z_\tau = \{(v, \sigma \cdot v) \mid v \in V, \sigma \cdot v = \tau \cdot v\} \cong V^{\sigma^{-1}\tau}. \quad (3.12.1)$$

This implies $Z_\sigma \cap Z_\tau \neq \emptyset$, so X is connected. If $f_1, \dots, f_n \in K[V]^G$ are separating invariants, then

$$X = \mathcal{V}(\Delta f_1, \dots, \Delta f_n)$$

with $\Delta f_i \in K[V \oplus V]$ defined by $\Delta f_i(v, w) = f_i(v) - f_i(w)$ for $v, w \in V$. So $R := K[V \oplus V]/(\Delta f_1, \dots, \Delta f_n)$ is a complete intersection. Hence by Hartshorne's connectedness theorem, X is connected in codimension one. It follows that for every $\sigma \in G$ there exists a sequence $\text{id} = \sigma_1, \sigma_2, \dots, \sigma_r = \sigma$ such that $Z_{\sigma_i} \cap Z_{\sigma_{i+1}}$ has codimension at most one in X . By (3.12.1) this implies that all $\sigma_i^{-1}\sigma_{i+1}$ are reflections. Since

$$\sigma = \sigma_r = (\sigma_1^{-1}\sigma_2)(\sigma_2^{-1}\sigma_3) \cdots (\sigma_{r-2}^{-1}\sigma_{r-1})(\sigma_{r-1}^{-1}\sigma_r),$$

it follows that G is generated by reflections. \square

Dufresne [89] also gave an example of an invariant ring $K[V]^G$ that is not polynomial but has a geometric separating subset of size $n = \dim(V)$. So Theorem 3.12.6 is really more general than Serre's result. But the story does not end here. Recently, Dufresne and Jeffries [127] proved that if there exists a geometric separating subset of size $n + k$ then G is generated by $(k + 1)$ -reflections, i.e., by elements fixing a subspace of codimension $k + 1$ pointwise. They obtained this result by applying a connectedness theorem going back to Grothendieck instead of Theorem 3.12.7. The paper even makes the stronger assertion that all point-wise stabilizers G_W of subspaces $W \subseteq V$ are generated by $(k + 1)$ -reflections. This generalizes Proposition 3.9.7.

A further remarkable result of Dufresne [89] says that if $K[V]^G$ has a graded separating subalgebra $A \subseteq K[V]^G$ that is a complete intersection, then G is generated by bireflections. This generalizes a result by Kac and Watanabe [72].

Theorem 3.12.6 was generalized in another direction:

Theorem 3.12.8 (Reimers [128]) *Let G be a finite group acting on an affine variety X over an algebraically closed field K . Suppose that X is connected and Cohen-Macaulay and that G is generated by elements σ with $X^\sigma \neq \emptyset$. If $K[X]^G$ has a separating subset of size $n = \dim(X)$, then G is generated by elements that fix a hypersurface in X .*

Example 2.4.2 and the “meta-theorem” that anomalies of positive characteristic tend to go away when one considers separating invariants instead of generating invariants raise hopes that also structural properties get better when one considers separating subalgebras. Might it be true, for example, that there always exists a separating subalgebra $A \subseteq K[V]^G$ that is Cohen-Macaulay? But such hopes were dampened by results of Dufresne et al. [129], who proved that for several classes of non-Cohen-Macaulay invariant rings there exists no graded separating subalgebra that is Cohen-Macaulay.

In Theorem 3.12.8 we have mentioned actions on affine varieties X almost for the first time in this chapter. The following section deals with the computations of invariant rings of actions on affine varieties and, more generally, on finitely generated algebras.

3.13 Actions on Finitely Generated Algebras

Noether's finiteness result says that R^G is finitely generated if G is a finite group acting on a finitely generated algebra R over a Noetherian ring K . After mentioning this result on page 72, we stated the goal of making it constructive. But so far we have only achieved this for the special case that K is a field, R is a polynomial ring and G acts by linear transformations of the indeterminates. In this section we consider more general settings. Most room will be given to the case in which K is a field. For this case we will propose an algorithm that is similar to the one given

by Kamke [130, Section 2.1]. We will present the algorithm in a somewhat informal way.

So assume that R is a finitely generated algebra over a field K and that a finite group G acts on R by automorphisms of algebras. The first step is to choose a finite-dimensional, G -stable K -subspace $V \subseteq R$ that generates R as an algebra. If R is given as the quotient of a polynomial ring $K[x_1, \dots, x_n]$ by an ideal I , then V can be taken as the span of the orbits $G \cdot (x_i + I)$. Computations in R can be performed by the normal form map given by a Gröbner basis of I (see Sect. 1.1.3). The choice of V gives rise to a G -equivariant epimorphism $\psi: S(V) = K[V^*] \rightarrow R$ from the symmetric algebra of V (which is equal to the polynomial ring on the dual space) to R . In the nonmodular case, ψ restricts to an epimorphism $K[V^*]^G \rightarrow R^G$, so computing generators of $K[V^*]^G$ and applying ψ yields generators of R^G . In the modular case, we have to do more. Using methods from Sect. 1.2.2, we can compute the kernel $J = \ker(\psi) \subseteq K[V^*]$.

Now we construct primary invariants in $K[V^*]^G$. This yields a monomorphism $\varphi: K[y_1, \dots, y_n] =: P \rightarrow K[V^*]^G \subseteq K[V^*]$ from a polynomial ring P to the invariant ring, making $K[V^*]^G$, and therefore also $K[V^*]$, into finitely generated P -modules. (Also R^G and R become P -modules via ψ .) By the Cohen-Macaulay property, $K[V^*]$ is free over P . Choosing free generators (which can be done by choosing the monomials that are not divisible by any leading monomial appearing in a Gröbner basis of the ideal generated by the $\varphi(y_i)$) gives rise to an isomorphism $\eta: P^r \rightarrow K[V^*]$. If J is generated by $h_1, \dots, h_k \in K[V^*]$, then the $\eta^{-1}(\eta(e_j)h_t)$ (with e_j the j th standard basis vector, $j = 1, \dots, r$, and $t = 1, \dots, k$) generate $\eta^{-1}(J)$ as a P -module. Let $\Theta: P^m \rightarrow P^r$ be the map sending the standard basis vectors of P^m to these generators. (So $m = rk$.) We obtain the following commutative diagram with exact rows and columns:

$$\begin{array}{ccccccc}
& & 0 & & 0 & & \\
& & \uparrow & & \uparrow & & \\
0 & \longrightarrow & J & \longrightarrow & K[V^*] & \xrightarrow{\psi} & R \longrightarrow 0 \\
& & \uparrow & & \uparrow \eta & & \\
P^m & \xrightarrow{\Theta} & P^r & & & & \\
& & \uparrow & & & & \\
& & 0 & & & &
\end{array}$$

Assume that G is generated by given elements $\sigma_1, \dots, \sigma_s$. Then the invariant ring R^G is the kernel of the map

$$\underline{\sigma} - \underline{\text{id}}: R \rightarrow R^s, \quad a \mapsto (\sigma_1 \cdot a - a, \dots, \sigma_s \cdot a - a).$$

The G -action extends from $K[V^*]$ to P^r via η , giving rise to maps $\underline{\sigma} - \underline{\text{id}}: K[V^*] \rightarrow K[V^*]^s$ and $\underline{\sigma} - \underline{\text{id}}: P^r \rightarrow P^{rs}$ defined as above. Writing ψ^s , η^s , and Θ^s for the maps

between the s -fold direct sums, we obtain the following commutative diagram of P -modules with exact rows and columns:

$$\begin{array}{ccccccc}
 & & J^s & \longrightarrow & K[V^*]^s & \xrightarrow{\psi^s} & R^s \\
 & \nearrow & \nearrow \eta^s & & \uparrow \underline{\sigma} - \text{id} & & \uparrow \underline{\sigma} - \text{id} \\
 P^{ms} & \xrightarrow{\Theta^s} & P^{rs} & & K[V^*] & \xrightarrow{\psi} & R \\
 \uparrow \underline{\sigma} - \text{id} & & \uparrow \eta & & & & \uparrow \\
 M & \xrightarrow{\pi} & P^r & & & & R^G
 \end{array}$$

Here M is the pullback. Explicitly,

$$M := \{(f, g) \in P^r \oplus P^{ms} \mid (\underline{\sigma} - \underline{\text{id}})(f) - \Theta^s(g) = 0\},$$

so M can be computed as a syzygy module by the methods from Sect. 1.3.1. A diagram chase shows that

$$R^G = \psi(\eta(\pi(M))),$$

so applying $\psi \circ \eta \circ \pi$ to a generating set of M will produce a generating set of R^G as a module over the subalgebra $\psi(\varphi(P))$. Moreover, the $\varphi(y_i)$ together with the images of generators of M under $\eta \circ \pi$ generate the preimage $\psi^{-1}(R^G) \subseteq K[V^*]$ as a K -algebra. This may be minimized (if desired) and then sent to a generating set of R^G by ψ .

Example 3.13.1 Let K be a field of positive characteristic p and $R = K[x_1, x_2]/(x_1^2)$ with an action of $G = \langle \sigma \rangle \cong C_p$ by

$$\sigma(\bar{x}_1) = \bar{x}_1 \quad \text{and} \quad \sigma(\bar{x}_2) = \bar{x}_1 + \bar{x}_2,$$

where the bars indicate residue classes in R . The case $p = 2$ of this example was considered by Kamke [130, Example 2.1]. We will run the above algorithm on this example and use the notation of the algorithm. We choose $K[V^*] = K[x_1, x_2]$ and

$$\varphi: K[y_1, y_2] =: P \rightarrow K[V^*], y_1 \mapsto x_1, y_2 \mapsto x_2^p - x_1^{p-1}x_2.$$

An obvious choice for free generators of $K[V^*]$ over P would be $1, x_2, \dots, x_2^{p-1}$. For our purposes, choosing $h_1 := x_2^{p-1}$ and $h_{i+1} := \frac{\sigma \cdot h_i - h_i}{x_1}$ ($i = 1, \dots, p-1$) is better. In particular, $h_p = (p-1)!$. With $\eta: P^p \rightarrow K[V^*]$ sending the standard basis vector e_i to h_i , we get

$$(\sigma - \text{id})(e_i) = y_1 e_{i+1} \quad (i < p) \quad \text{and} \quad (\sigma - \text{id})(e_p) = 0.$$

With

$$\Theta: P^p \rightarrow P^p, e_i \mapsto y_1^2 e_i$$

we have $\text{im}(\eta \circ \Theta) = \ker(\psi)$. Now we compute M . Let $f = \sum_{i=1}^p f_i e_i$ and $g = \sum_{i=1}^p g_i e_i \in P^p$. Then $(f, g) \in M$ if and only if

$$\sum_{i=2}^p y_1 f_{i-1} e_i = \sum_{i=1}^p y_1^2 g_i e_i$$

Hence $\pi(M)$ is generated by $y_1 e_i$ ($i = 1, \dots, p - 1$) and e_p , and $\eta(\pi(M)) = \psi^{-1}(R^G)$ is generated (as a module over the subalgebra $K[x_1, x_2^p - x_1^{p-1}x_2]$) by $x_1 h_i$ ($i = 1, \dots, p - 1$) and 1, or, alternatively, by $x_1 x_2^i$ ($i = 1, \dots, p - 1$) and 1. We obtain

$$R^G = K[\bar{x}_1, \bar{x}_1 \bar{x}_2, \dots, \bar{x}_1 \bar{x}_2^{p-1}, \bar{x}_2^p].$$

Notice that $K[V^*]^G = K[x_1, x_2^p - x_1^{p-1}x_2]$, so in this example not every invariant from R^G comes from an invariant in $K[V^*]^G$. It is interesting to compare this example to Example 2.1.5.

A variant of this example arises by replacing every occurrence of x_1^2 and y_1^2 by $x_1 - 1$ and $y_1 - 1$, respectively. Then the computation of $\pi(M)$ yields the generators $(y_1 - 1)e_i$ ($i = 1, \dots, p - 1$) and e_p , so $\psi^{-1}(R^G)$ is generated only by 1. In this case $R = K[x]$ is a univariate polynomial ring with $\sigma \cdot x = x + 1$, and we get

$$K[x]^G = K[x^p - x].$$

◇

Of course, in the special case $R = K[V]$ we obtain an alternative algorithm for computing secondary invariants in the modular case. That is the algorithm we presented in the first edition of this book.

What can be done if K is not a field but a ring? Since over a field all known algorithms involve Gröbner basis computations, it seems reasonable to assume that we will depend on them when working over a ring, too. Gröbner bases can be defined over any ring. In fact, Definition 1.1.3 generalizes to the case in which K is a ring if one substitutes the leading monomial $\text{LM}(g)$ in the definition of a leading ideal $L(S)$ by the leading term $\text{LT}(g)$. A good source for Gröbner bases over rings is Chapter 4 of the book by Adams and Loustaunau [131]. There it is explained that the computation of Gröbner bases over a ring K is possible if one can solve linear equations over K . More precisely, we need to assume that there is an algorithm for computing the set S of solutions $(c_1, \dots, c_r) \in K^r$ of a linear equation $a_1 c_1 + \dots + a_r c_r = b$ with $b, a_i \in K$, and also that K is Noetherian. (In case of solvability, S should be given as a coset of a finitely generated submodule.) Rings

with these properties are sometimes called **Zacharias rings**. It is easy to see that every Euclidean ring, and in particular \mathbb{Z} , is a Zacharias ring.

If K is a Zacharias ring, then also the methods of Sect. 1.3.1 for computing syzygy modules can be adapted. Since a syzygy computation is at the heart of the algorithm we described above, this nourishes the hope that the algorithm can be adapted to the ring situation. What is missing is the existence of primary invariants: Since Noether normalization works only over fields, the subalgebra generated by primary invariants must be replaced by something else. In fact, it turns out that it can be replaced by any subalgebra $A \subseteq R^G$ over which R is integral. The difficulties arising from the fact that the generators of A cannot in general be chosen to be algebraically independent can be overcome. This leads to an algorithm presented in Kemper [132]. This algorithm computes invariant rings of finite groups acting on finitely generated algebras over Zacharias rings. Under the assumption that Gröbner basis computation are unavoidable, this constitutes a constructive version of Noether's finiteness result [12] in a maximally general situation. The conjecture that the computation of invariant rings of finite groups is possible *only* over Zacharias rings is further supported by the fact that even computing polynomial invariants of degree one amounts to solving systems of linear equations.

Example 3.13.2 Consider the action of $G \cong C_2$ on $R := \mathbb{Z}[x_1, x_2]/(x_1^2 - x_2^2)$ by exchanging \bar{x}_1 and \bar{x}_2 (where the bars indicate classes modulo $(x_1^2 - x_2^2)$). Applying the algorithm from [132] yields

$$R^G = \mathbb{Z}[\bar{x}_1 + \bar{x}_2, \bar{x}_1\bar{x}_2, \bar{x}_1^2].$$

With f_i standing for the i th generating invariant, we have the relation $2f_3 = f_1^2 - 2f_2$, so f_3 would be redundant if we were computing over a ring in which 2 is invertible. But over \mathbb{Z} we see that although the G -equivariant map $\mathbb{Z}[x_1, x_2] \rightarrow R$ is surjective, its restriction to invariants is not. \triangleleft

The algorithm from [132] for computing invariant rings of finite groups acting on finitely generated algebras over Zacharias rings is hard to implement and far from efficient. Another algorithm, based on completely different ideas, will be outlined in Remark 4.10.7 of this book. The scope of that algorithm is limited to actions on finitely generated *domains* over Zacharias rings, but it has been implemented and it is much more efficient. An important special case to which the algorithm applies is the case of multiplicative invariants: One considers a subgroup $G \subseteq \mathrm{GL}_n(\mathbb{Z})$ acting on the Laurent polynomial ring $K[x_1, \dots, x_n, x_1^{-1}, \dots, x_n^{-1}]$ over a ring K by transforming the exponent vectors of monomials in the obvious way. A very nice source on multiplicative invariant theory is the book by Lorenz [133]. Since one can reduce to the case that G is finite and $K = \mathbb{Z}$, the algorithm applies, giving a solution to Problem 7 in [133] (which calls for finding an algorithm for computing multiplicative invariant rings). We finish the section with an example.

Example 3.13.3

- (1) We consider multiplicative invariants of the dihedral group $G \subseteq \mathrm{GL}_2(\mathbb{Z})$ of order 8 generated by $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$. The group acts on the Laurent polynomial ring $\mathbb{Z}[x, y, x^{-1}, y^{-1}]$ by $x \leftrightarrow y$ and $x \mapsto x^{-1}$, $y \mapsto y$. Using the implementation of the algorithm from Remark 4.10.7 yields the invariant ring

$$\mathbb{Z}[x, y, x^{-1}, y^{-1}]^G = \mathbb{Z}[x + y + x^{-1} + y^{-1}, xy + xy^{-1} + x^{-1}y + x^{-1}y^{-1}].$$

- (2) Perhaps the easiest example of an invariant ring that is not Cohen-Macaulay and violates Noether's degree bound is the one from Example 3.3.1 (see also Example 3.6.3). Here we consider the invariant ring over the integers. So let $G \cong C_2$ act on $\mathbb{Z}[x_1, x_2, x_3, y_1, y_2, y_3]$ by interchanging the x_i and y_i . Using the algorithm described in Remark 4.10.7 yields

$$\mathbb{Z}[x_1, x_2, x_3, y_1, y_2, y_3]^G = \mathbb{Z}[s_1, s_2, s_3, p_1, p_2, p_3, u_{1,2}, u_{1,3}, u_{2,3}, f]$$

with

$$s_i = x_i + y_i, \quad p_i = x_i y_i, \quad u_{i,j} = x_i y_j + y_i x_j, \quad \text{and } f = y_1 x_2 x_3 + x_1 y_2 y_3.$$

The generators correspond exactly to the ones in characteristic 2 worked out in Example 3.7.6(a). The significance of this example is that the above generators map to generators of $K[x_1, x_2, x_3, y_1, y_2, y_3]^G$ for any field (or even ring) K . The relation

$$2f = s_3 u_{1,2} - s_1 u_{2,3} + s_2 u_{1,3}$$

shows that Noether's degree bound holds if 2 is invertible in K . \triangleleft

References

1. David J. Benson, *Polynomial Invariants of Finite Groups*, Lond. Math. Soc. Lecture Note Ser. **190**, Cambridge Univ. Press, Cambridge 1993.
2. Larry Smith, *Polynomial Invariants of Finite Groups*, A. K. Peters, Wellesley, Mass. 1995.
3. Mara D. Neusel, Larry Smith, *Invariant Theory of Finite Groups*, Mathematical Surveys and Monographs **94**, American Mathematical Society, Providence, RI 2002.
4. H. E. A. Eddy Campbell, David L. Wehlau, *Modular Invariant Theory*, Encyclopaedia of Mathematical Sciences **139**, Springer-Verlag, Berlin 2011.
5. Manfred Göbel, *The invariant package of MAS*, in: Hubert Comon, ed., *Rewriting Techniques and Applications, 8th International Conference*, Lecture Notes in Computer Science **1232**, pp. 327–330, Springer-Verlag, Berlin, Heidelberg, New York 1997.
6. Gregor Kemper, *The Invar package for calculating rings of invariants*, Preprint **93–34**, IWR, Heidelberg, 1993a.
7. Karin Gatermann, F. Guyard, *The Symmetry package in Maple*, 1996.

8. Nicolas M. Thiéry, *PerMuVAR, a library for mupad for computing in invariant rings of permutation groups*, <http://permuvvar.sf.net/>.
9. Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, Hans Schönemann, SINGULAR 4-0-2 — A computer algebra system for polynomial computations, <http://www.singular.uni-kl.de>, 2015.
10. Wieb Bosma, John J. Cannon, Catherine Playoust, *The Magma algebra system I: The user language*, J. Symb. Comput. **24** (1997), 235–265.
11. Gregor Kemper, Elmar Körding, Gunter Malle, B. Heinrich Matzat, Denis Vogel, Gabor Wiese, *A database of invariant rings*, Exp. Math. **10** (2001), 537–542.
12. Emmy Noether, *Der Endlichkeitssatz der Invarianten endlicher linearer Gruppen der Charakteristik p* , Nachr. Ges. Wiss. Göttingen (1926), 28–35.
13. Gregor Kemper, Allan Steel, *Some algorithms in invariant theory of finite groups*, in: P. Dräxler, G.O. Michler, C. M. Ringel, eds., *Computational Methods for Representations of Groups and Algebras, Euroconference in Essen, April 1–5 1997*, Progress in Mathematics **173**, pp. 267–285, Birkhäuser, Basel 1999.
14. Emmy Noether, *Der Endlichkeitssatz der Invarianten endlicher Gruppen*, Math. Ann. **77** (1916), 89–92.
15. Larry Smith, *Noether’s bound in the invariant theory of finite groups*, Arch. der Math. **66** (1996), 89–92.
16. David R. Richman, *Explicit generators of the invariants of finite groups*, Adv. in Math. **124** (1996), 49–76.
17. Peter Fleischmann, Wolfgang Lempken, *On degree bounds for invariant rings of finite groups over finite fields*, in: *Finite Fields: Theory, Applications, and Algorithms* (Waterloo, ON, 1997), pp. 33–41, Amer. Math. Soc., Providence, RI 1999.
18. Larry Smith, *Putting the squeeze on the Noether gap—the case of the alternating groups A_n* , Math. Ann. **315** (1999), 503–510.
19. Peter Fleischmann, *The Noether bound in invariant theory of finite groups*, Adv. in Math. **156** (2000), 23–32.
20. John Fogarty, *On Noether’s bound for polynomial invariants of a finite group*, Electron. Res. Announc. Amer. Math. Soc. **7** (2001), 5–7.
21. David J. Benson, *Noether’s degree bound*, private communication, 2000.
22. Barbara J. Schmid, *Finite groups and invariant theory*, in: P. Dubreil, M.-P. Malliavin, eds., *Topics in Invariant Theory*, Lect. Notes Math. **1478**, Springer-Verlag, Berlin, Heidelberg, New York 1991.
23. H. E. A. Campbell, I. P. Hughes, *Vector invariants of $U_2(\mathbb{F}_p)$: A proof of a conjecture of Richman*, Adv. in Math. **126** (1997), 1–20.
24. Müfit Sezer, *A note on the Hilbert ideals of a cyclic group of prime order*, J. Algebra **318** (2007), 372–376.
25. Mátyás Domokos, Pál Hegedűs, *Noether’s bound for polynomial invariants of finite groups*, Arch. Math. **74** (2000), 161–167.
26. Müfit Sezer, *Sharpening the generalized Noether bound in the invariant theory of finite groups*, J. Algebra **254** (2002), 252–263.
27. David R. Richman, *On vector invariants over finite fields*, Adv. in Math. **81** (1990), 30–65.
28. David R. Richman, *Invariants of finite groups over fields of characteristic p* , Adv. in Math. **124** (1996), 25–48.
29. Gregor Kemper, *Lower degree bounds for modular invariants and a question of I. Hughes*, Transformation Groups **3** (1998d), 135–144.
30. Peter Fleischmann, *A new degree bound for vector invariants of symmetric groups*, Trans. Amer. Math. Soc. **350** (1998), 1703–1712.
31. Roger M. Bryant, Gregor Kemper, *Global degree bounds and the transfer principle for invariants*, J. Algebra **284** (2005), 80–90.
32. Peter Symonds, *On the Castelnuovo-Mumford regularity of rings of polynomial invariants*, Ann. of Math. (2) **174** (2011), 499–517.

33. Gregor Kemper, *Hilbert series and degree bounds in invariant theory*, in: B. Heinrich Matzat, Gert-Martin Greuel, Gerhard Hiss, eds., *Algorithmic Algebra and Number Theory*, pp. 249–263, Springer-Verlag, Heidelberg 1999.
34. Manfred Göbel, *Computing bases for rings of permutation-invariant polynomials*, J. Symb. Comput. **19** (1995), 285–291.
35. H. E. A. Campbell, A. V. Geramita, I. P. Hughes, R. J. Shank, D. L. Wehlau, *Non-Cohen-Macaulay vector invariants and a Noether bound for a Gorenstein ring of invariants*, Canad. Math. Bull. **42** (1999), 155–161.
36. Abraham Broer, *Remarks on invariant theory of finite groups*, preprint, Université de Montréal, Montréal, 1997.
37. Ian Hughes, Gregor Kemper, *Symmetric powers of modular representations, Hilbert series and degree bounds*, Comm. in Algebra **28** (2000), 2059–2088.
38. Dikran B. Karagueuzian, Peter Symonds, *The module structure of a group action on a polynomial ring: a finiteness theorem*, J. Amer. Math. Soc. **20** (2007), 931–967.
39. Peter Symonds, *Group actions on rings and the Čech complex*, Adv. Math. **240** (2013), 291–301.
40. Charles W. Curtis, Irving Reiner, *Methods of Representation Theory I*, J. Wiley & Sons, New York 1981.
41. Ian Hughes, Gregor Kemper, *Symmetric powers of modular representations for groups with a Sylow subgroup of prime order*, J. of Algebra **241** (2001), 759–788.
42. Gert Almkvist, Robert M. Fossum, *Decompositions of exterior and symmetric powers of indecomposable $\mathbb{Z}/p\mathbb{Z}$ -modules in characteristic p and relations to invariants*, in: *Sém. d'Algèbre P. Dubreil*, Lecture Notes in Math. **641**, pp. 1–111, Springer-Verlag, Berlin, Heidelberg, New York 1976–1977.
43. Andreas Kreisel, *Hilbertreihen von Invariantenringen*, Diplomarbeit, Technische Universität München, 2012.
44. Ashley Hobson, R. James Shank, *The invariants of the third symmetric power representation of $SL_2(\mathbb{F}_p)$* , J. Algebra **333** (2011), 241–257.
45. R. James Shank, *S.A.G.B.I. bases for rings of formal modular seminvariants*, Comment. Math. Helvetici **73** (1998), 548–565.
46. R. James Shank, David L. Wehlau, *Noether numbers for subrepresentations of cyclic groups of prime order*, Bull. London Math. Soc. **34** (2002), 438–450.
47. H. E. A. Campbell, B. Fodden, David L. Wehlau, *Invariants of the diagonal C_p -action on V_3* , J. Algebra **303** (2006), 501–513.
48. Alexander Duncan, Michael LeBlanc, David L. Wehlau, *A SAGBI basis for $\mathbb{F}[V_2 \oplus V_2 \oplus V_3]^{C_p}$* , Canad. Math. Bull. **52** (2009), 72–83.
49. David J. Benson, *Representations and Cohomology I*, Cambridge Studies in Advanced Mathematics **30**, Cambridge Univ. Press, Cambridge 1991.
50. Jacques Thévenaz, *G-Algebras and Modular Representation Theory*, Clarendon Press, Oxford 1995.
51. David M. Goldschmidt, *Lectures on Character Theory*, Publish or Perish, Inc., Berkeley 1980.
52. Stephen A. Mitchell, *Finite complexes with $A(n)$ -free cohomology*, Topology **24** (1985), 227–246.
53. Larry Smith, *Polynomial invariants of finite groups: A survey of recent developments*, Bull. Amer. Math. Soc. **34** (1997), 211–250.
54. Christoph Jansen, Klaus Lux, Richard Parker, Robert Wilson, *An Atlas of Brauer Characters*, Clarendon Press, Oxford 1995.
55. David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York 1995.
56. Richard P. Stanley, *Invariants of finite groups and their applications to combinatorics*, Bull. Amer. Math. Soc. **1(3)** (1979), 475–511.
57. Victor Reiner, Larry Smith, *Systems of parameters for rings of invariants*, preprint, Göttingen, 1996.

58. Gregor Kemper, *An algorithm to calculate optimal homogeneous systems of parameters*, J. Symb. Comput. **27** (1999), 171–184.
59. H. E. A. Campbell, A. V. Geramita, I. P. Hughes, G. G. Smith, D. L. Wehlau, *Hilbert functions of graded algebras*, The Curves Seminar at Queen's, Volume XI, in: Queen's Papers in Pure and Applied Math. **105** (1997), 60–74.
60. N. J. A. Sloane, *Error-correcting codes and invariant theory: New applications of a nineteenth-century technique*, Amer. Math. Monthly **84** (1977), 82–107.
61. Melvin Hochster, John A. Eagon, *Cohen-Macaulay rings, invariant theory, and the generic perfection of determinantal loci*, Amer. J. of Math. **93** (1971), 1020–1058.
62. Melvin Hochster, Joel L. Roberts, *Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay*, Adv. in Math. **13** (1974), 115–175.
63. Michel Van den Bergh, *Modules of covariants*, in: *Proceedings of the International Congress of Mathematics, ICM '94*, vol. 1, pp. 352–362, Birkhäuser, Basel 1995.
64. H. E. A. Campbell, I. P. Hughes, R. D. Pollack, *Rings of invariants and p-Sylow subgroups*, Canad. Math. Bull. **34(1)** (1991), 42–47.
65. Geir Ellingsrud, Tor Skjelbred, *Profondeur d'anneaux d'invariants en caractéristique p*, Compos. Math. **41** (1980), 233–244.
66. Larry Smith, *Some rings of invariants that are Cohen-Macaulay*, Can. Math. Bull. **39** (1996), 238–240.
67. Gregor Kemper, *The Cohen–Macaulay property and depth in invariant theory*, in: *Proceedings of the 33rd Symposium on Commutative Algebra in Japan*, pp. 53–63, 2012, <https://sites.google.com/site/commalg33/proceedings>.
68. Gregor Kemper, *On the Cohen–Macaulay property of modular invariant rings*, J. of Algebra **215** (1999), 330–351.
69. Nikolai Gordeev, Gregor Kemper, *On the branch locus of quotients by finite groups and the depth of the algebra of invariants*, J. Algebra **268** (2003), 22–38.
70. Gregor Kemper, *The depth of invariant rings and cohomology*, with an appendix by Kay Magaard, J. of Algebra **245** (2001), 463–531.
71. David J. Benson, *Representations and Cohomology II*, Cambridge Studies in Advanced Mathematics **31**, Cambridge Univ. Press, Cambridge 1991.
72. Victor G. Kac, Kei-Ichi Watanabe, *Finite linear groups whose ring of invariants is a complete intersection*, Bull. Amer. Math. Soc. **6** (1982), 221–223.
73. Helmer Aslaksen, Shih-Ping Chan, Tor Gulliksen, *Invariants of S_4 and the shape of sets of vectors*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), 53–57.
74. Simon A. King, *Minimal generating sets of non-modular invariant rings of finite groups*, J. Symbolic Comput. **48** (2013), 101–109.
75. Martin Kreuzer, Lorenzo Robbiano, *Computational Commutative Algebra 2*, Springer-Verlag, Berlin 2005.
76. Harm Derksen, *Degree bounds for syzygies of invariants*, Adv. Math. **185(2)** (2004), 207–214.
77. Haruhisa Nakajima, *Quotient singularities which are complete intersections*, Manuscr. Math. **48** (1984), 163–187.
78. Haruhisa Nakajima, *Quotient complete intersections of affine spaces by finite linear groups*, Nagoya Math. J. **98** (1985), 1–36.
79. Nikolai L. Gordeev, *Finite linear groups whose algebras of invariants are complete intersections*, Izv. Akad. Nauk SSSR Ser. Mat. **50** (1986), 343–392, English translation in: Math. USSR, Izv. **28** (1987), 335–379.
80. Winfried Bruns, Jürgen Herzog, *Cohen-Macaulay Rings*, Cambridge University Press, Cambridge 1993.
81. H. E. A. Campbell, I. P. Hughes, G. Kemper, R. J. Shank, D. L. Wehlau, *Depth of modular invariant rings*, Transformation Groups **5** (2000), 21–34.
82. R. James Shank, David L. Wehlau, *On the depth of the invariants of the symmetric power representations of $SL_2(\mathbf{F}_p)$* , J. of Algebra **218** (1999), 642–653.

83. Peter Fleischmann, Gregor Kemper, R. James Shank, *Depth and cohomological connectivity in modular invariant theory*, Trans. Amer. Math. Soc. **357** (2005), 3605–3621.
84. Gregor Kemper, *Calculating invariant rings of finite groups over arbitrary fields*, J. Symb. Comput. **21** (1996b), 351–366.
85. William Fulton, *Intersection Theory*, Springer-Verlag, Berlin, Heidelberg, New York 1984.
86. G. C. Shephard, J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274–304.
87. Claude Chevalley, *Invariants of finite groups generated by reflections*, Amer. J. Math. **77** (1955), 778–782.
88. Jean-Pierre Serre, *Groupes finis d'automorphismes d'anneaux locaux réguliers*, in: *Colloque d'Algèbre*, pp. 8–01 – 8–11, Secrétariat mathématique, Paris 1968.
89. Emilie Dufresne, *Separating invariants and finite reflection groups*, Adv. Math. **221**(6) (2009), 1979–1989.
90. Haruhisa Nakajima, *Invariants of finite groups generated by pseudo-reflections in positive characteristic*, Tsukuba J. Math. **3** (1979), 109–122.
91. Haruhisa Nakajima, *Modular representations of abelian groups with regular rings of invariants*, Nagoya Math. J **86** (1982), 229–248.
92. Haruhisa Nakajima, *Regular rings of invariants of unipotent groups*, J. Algebra **85** (1983), 253–286.
93. Gregor Kemper, Gunter Malle, *The finite irreducible linear groups with polynomial ring of invariants*, Transformation Groups **2** (1997b), 57–89.
94. William M. Kantor, *Subgroups of classical groups generated by long root elements*, Trans. Amer. Math. Soc. **248** (1979), 347–379.
95. Ascher Wagner, *Collineation groups generated by homologies of order greater than 2*, Geom. Dedicata **7** (1978), 387–398.
96. Ascher Wagner, *Determination of the finite primitive reflection groups over an arbitrary field of characteristic not 2, I*, Geom. Dedicata **9** (1980), 239–253.
97. A.E. Zalesskii, V.N. Serezin, *Linear groups generated by transvections*, Math. USSR, Izv. **10** (1976), 25–46.
98. A.E. Zalesskii, V.N. Serezin, *Finite linear groups generated by reflections*, Math. USSR, Izv. **17** (1981), 477–503.
99. H. E. A. Campbell, I. P. Hughes, R. J. Shank, *Preliminary notes on rigid reflection groups*, available at <http://www.ukc.ac.uk/ims/math/people/R.J.Shank/>, 1996.
100. David Carlisle, Peter H. Kropholler, *Modular invariants of finite symplectic groups*, preprint, Queen Mary, University of London, 1992.
101. Gregor Kemper, Gunter Malle, *Invariant fields of finite irreducible reflection groups*, Math. Ann. **315** (1999), 569–586.
102. Richard P. Stanley, *Hilbert functions of graded algebras*, Adv. Math. **28** (1978), 57–83.
103. Keiichi Watanabe, *Certain invariant subrings are Gorenstein I*, Osaka J. Math. **11** (1974), 1–8.
104. Keiichi Watanabe, *Certain invariant subrings are Gorenstein II*, Osaka J. Math. **11** (1974), 379–388.
105. Barbara R. Peskin, *On the dualizing sheaf of a quotient scheme*, Comm. Algebra **12**(15–16) (1984), 1855–1869.
106. Abraham Broer, *The direct summand property in modular invariant theory*, Transform. Groups **10** (2005), 5–27.
107. Amiram Braun, *On the Gorenstein property for modular invariants*, J. Algebra **345** (2011), 81–99.
108. Peter Fleischmann, Chris Woodcock, *Relative invariants, ideal classes and quasi-canonical modules of modular rings of invariants*, J. Algebra **348** (2011), 110–134.
109. Amiram Braun, *The Gorenstein property and the Kemper et al. conjecture*, preprint, available at <http://homepages.abdn.ac.uk/mth192/pages/papers/b/braun/Goren.dvi>, 2012.

110. Lorenzo Robbiano, Moss Sweedler, *Subalgebra bases*, in: W. Bruns, A. Simis, eds., *Commutative Algebra*, Lecture Notes in Math. **1430**, pp. 61–87, Springer-Verlag, New York 1990.
111. D. Kapur, K. Madlener, *A completion procedure for computing a canonical basis of a k -subalgebra*, in: E. Kaltofen, S. Watt, eds., *Proceedings of Computers and Mathematics* **89**, pp. 1–11, MIT, Cambridge, Mass. 1989.
112. Heinz Kredel, *MAS: Modula-2 algebra system*, in: V. P. Gerdt, V. A. Rostovtsev, D. V. Shirkov, eds., *Fourth International Conference on Computer Algebra in Physical Research*, pp. 31–34, World Scientific Publishing, Singapore 1990.
113. Manfred Göbel, *On the number of special permutation-invariant orbits and terms*, Appl. Algebra Engrg. Comm. Comput. **8** (1997), 505–509.
114. Manfred Göbel, *A constructive description of SAGBI bases for polynomial invariants of permutation groups*, J. Symb. Comput. **26** (1998), 261–272.
115. R. James Shank, *SAGBI bases in modular invariant theory*, presented at the Workshop on Symbolic Computation in Geometry and Analysis, MSRI (Berkeley), October 1998.
116. R. James Shank, David L. Wehlau, *Computing modular invariants of p -groups*, J. Symbolic Comput. **34** (2002), 307–327.
117. Michael Stillman, Harrison Tsai, *Using SAGBI bases to compute invariants*, J. Pure Appl. Algebra (1999), 285–302.
118. J. F. Adams, C. W. Wilkerson, *Finite H -spaces and algebras over the Steenrod algebra*, Ann. of Math. (1980), 95–143.
119. Dorra Bourguiba, Said Zarati, *Depth and the Steenrod algebra*, Invent. math. **128** (1997), 589–602.
120. Mara D. Neusel, *Inverse invariant theory and Steenrod operations*, Mem. Amer. Math. Soc. **146** (2000).
121. R. M. W. Wood, *Differential operators and the Steenrod algebra*, Proc. Lond. Math. Soc. **75** (1997), 194–220.
122. Moss Sweedler, *Using Gröbner bases to determine the algebraic and transcendental nature of field extensions: Return of the killer tag variables*, in: Gérard Cohen, Teo Mora, Oscar Moreno, eds., *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Springer-Verlag, Berlin, Heidelberg, New York 1993.
123. Gregor Kemper, *Die Cohen-Macaulay-Eigenschaft in der modularen Invariantentheorie*, Habilitationsschrift, Universität Heidelberg, 1999.
124. Gregor Kemper, *Loci in quotients by finite groups, pointwise stabilizers and the Buchsbaum property*, J. reine angew. Math. **547** (2002), 69–96.
125. Gregor Kemper, *Separating invariants*, J. Symbolic Comput. **44** (2009), 1212–1222.
126. Robin Hartshorne, *Complete intersections and connectedness*, Amer. J. Math. **84** (1962), 497–508.
127. Emilie Dufresne, Jack Jeffries, *Separating invariants and local cohomology*, preprint, available at <http://arxiv.org/abs/1309.6012>, 2013.
128. Fabian Reimers, *Polynomial separating algebras and reflection groups*, preprint, Technische Universität München, 2013, <http://arxiv.org/abs/1307.7522>.
129. Emilie Dufresne, Jonathan Elmer, Martin Kohls, *The Cohen-Macaulay property of separating invariants of finite groups*, Transform. Groups **14** (2009), 771–785.
130. Tobias Kamke, *Algorithms for the computation of invariant rings*, Dissertation, Technische Universität München, 2009.
131. William W. Adams, Phillippe Loustaunau, *An Introduction to Gröbner Bases*, Graduate Studies in Mathematics **3**, American Mathematical Society, Providence, RI 1994.
132. Gregor Kemper, *Using extended Derksen ideals in computational invariant theory*, J. Symbolic Comput. (2015), to appear.
133. Martin Lorenz, *Multiplicative Invariant Theory*, Encyclopaedia of Mathematical Sciences **135**, Springer-Verlag, Berlin 2005.

Chapter 4

Invariant Theory of Infinite Groups

4.1 Computing Invariants of Linearly Reductive Groups

Throughout this section G will be a linearly reductive group over an algebraically closed field K and V will be an n -dimensional rational representation. We will present an algorithm for computing generators of the invariant ring $K[V]^G$ (see Derksen [1]). This algorithm is actually quite simple and it is easy to implement. The essential step is just one Gröbner basis computation. We will also need the Reynolds operator. For now, the Reynolds operator \mathcal{R} is just a black box which has the required properties (see Definition 2.2.2). In Sect. 4.5 we will study how to compute the Reynolds operator for several examples of linearly reductive groups.

4.1.1 The Heart of the Algorithm

We will discuss the theoretical results on which the algorithm is based. Suppose that G is a linearly reductive group and V is an n -dimensional rational representation of G . As in the proof of Hilbert's finiteness theorem (Theorem 2.2.10) we take $I \subseteq K[V]$ to be the Hilbert ideal, i.e., the ideal generated by all homogeneous invariants of degree > 0 . As the proof of Theorem 2.2.10 shows, if I is generated by homogeneous invariants f_1, \dots, f_r , then f_1, \dots, f_r will generate the invariant ring $K[V]^G$ as a K -algebra. If $f_1, \dots, f_r \in K[V]$ are *any* homogeneous generators of I (not necessarily invariant), then by the following proposition we can obtain generators of $K[V]^G$ using the Reynolds operator \mathcal{R} (see Definition 2.2.2).

Proposition 4.1.1 *If $I = (f_1, \dots, f_r)$ with $f_1, \dots, f_r \in K[V]$ homogeneous, then $I = (\mathcal{R}(f_1), \dots, \mathcal{R}(f_r))$ and $K[V]^G = K[\mathcal{R}(f_1), \dots, \mathcal{R}(f_r)]$.*

Proof Suppose that $K[V]^G$ is generated by homogeneous elements h_1, \dots, h_s . Let \mathfrak{m} be the homogeneous maximal ideal of $K[V]$. Then the images of h_1, \dots, h_s modulo

$\mathfrak{m}I$ span the vector space $I/\mathfrak{m}I$. Notice that $\mathcal{R}(I) \subseteq I$ and $\mathcal{R}(\mathfrak{m}I) \subseteq \mathfrak{m}I$, because I and $\mathfrak{m}I$ are G -stable (see Corollary 2.2.7). Now \mathcal{R} induces a map $I/\mathfrak{m}I \rightarrow I/\mathfrak{m}I$ which is the identity because $I/\mathfrak{m}I$ is spanned by the images of invariants. Notice that the images of f_i and $\mathcal{R}(f_i)$ in $I/\mathfrak{m}I$ are the same. It follows that $I/\mathfrak{m}I$ is spanned by the images of $\mathcal{R}(f_1), \dots, \mathcal{R}(f_r)$. By the graded Nakayama Lemma (Lemma 3.7.1), $I = (\mathcal{R}(f_1), \dots, \mathcal{R}(f_r))$. From the proof of Theorem 2.2.10 it follows that $K[V]^G = K[\mathcal{R}(f_1), \dots, \mathcal{R}(f_r)]$. \square

Remark 4.1.2 If $f_1, \dots, f_r \in K[V]$ is a minimal set of homogeneous ideal generators of I , then the images of f_1, \dots, f_r in $I/\mathfrak{m}I$ will form a vector space basis. So $\mathcal{R}(f_1), \dots, \mathcal{R}(f_r)$ are homogeneous invariants whose images form a basis of $I/\mathfrak{m}I$. It follows that $\{\mathcal{R}(f_1), \dots, \mathcal{R}(f_r)\}$ is a minimal set of generators of $K[V]^G$. \triangleleft

Let $\psi : G \times V \rightarrow V \times V$ be the map defined by $\psi(\sigma, v) = (v, \sigma \cdot v)$. We will identify $K[V \times V]$ with the polynomial ring $K[x, y]$ where x and y are abbreviations for x_1, \dots, x_n and y_1, \dots, y_n . Let B be the image of ψ and let \bar{B} be its Zariski closure. Suppose that $(w, 0) \in \bar{B}$. If $f \in K[V]^G$ is a homogeneous invariant of degree > 0 , then $f(x) - f(y)$ vanishes on B , because $f(v) - f(\sigma \cdot v) = 0$ for all $v \in V$ and $\sigma \in G$. So $f(x) - f(y)$ also vanishes on \bar{B} , in particular $f(w) - f(0) = f(w) = 0$. It follows that $w \in \mathcal{N}_V$, where \mathcal{N}_V is Hilbert's nullcone (see Definition 2.5.1). Conversely, if $w \in \mathcal{N}_V$, then $\{w\} \times G \cdot w \subset B$, so $(w, 0) \in \bar{B}$ because 0 lies in the Zariski closure of the orbit $G \cdot w$ (see Lemma 2.5.2). We have proven

$$\bar{B} \cap (V \times \{0\}) = \mathcal{N}_V \times \{0\}. \quad (4.1.1)$$

Equation (4.1.1) is also true if G is geometrically reductive and not linearly reductive. Let $\mathfrak{b} \subseteq K[V \times V]$ be the vanishing ideal of \bar{B} . The left-hand side of Eq. (4.1.1) is the zero set of the ideal $\mathfrak{b} + (y_1, y_2, \dots, y_n)$ and the right-hand side is the zero set of the ideal $I + (y_1, \dots, y_n)$ (where $I \subset K[x] \subset K[x, y]$ is as before). The following theorem shows that in fact both ideals are the same under the assumption that G is linearly reductive.

Theorem 4.1.3 If $f_1(x, y), f_2(x, y), \dots, f_r(x, y) \in K[x, y]$ are homogeneous and generate the ideal \mathfrak{b} , then $f_1(x, 0), f_2(x, 0), \dots, f_r(x, 0)$ generate I .

Proof An equivalent statement of the theorem is that

$$\mathfrak{b} + (y_1, \dots, y_n) = I + (y_1, \dots, y_n).$$

“ \supseteq ”: If $f \in K[V]^G$ is a homogeneous invariant of positive degree, then $f(x) = (f(x) - f(y)) + f(y)$. Now $f(y) \in (y_1, \dots, y_n)$ and $f(x) - f(y) \in \mathfrak{b}$ because $f(x) - f(y)$ vanishes on \bar{B} : $(f(x) - f(y))(v, \sigma \cdot v) = f(v) - f(\sigma \cdot v) = 0$ for all $v \in V$ and $\sigma \in G$. Since I is generated by homogeneous invariants of degree > 0 , we have shown this inclusion.

“ \subseteq ”: Suppose that $f(x) \in (y_1, \dots, y_n) + \mathfrak{b}$. We can write

$$f(x) = \sum_i c_i(x) f_i(y) + b(x, y), \quad (4.1.2)$$

where $c_i(x) \in K[x]$, $f_i(y) \in (y_1, \dots, y_n) \subset K[y]$ homogeneous for all i and $b(x, y) \in \mathfrak{b}$. We will view $V \times V$ as a G -variety where G acts as usual on the second factor and trivially on the first. The corresponding Reynolds operator

$$\mathcal{R}_y : K[x, y] \rightarrow K[x, y]^G = K[y]^G[x]$$

is a $K[x]$ -module homomorphism (see Corollary 2.2.7) and the restriction to $K[y]$ is the Reynolds operator $K[y] \rightarrow K[y]^G$. Let us apply \mathcal{R}_y to Eq. (4.1.2):

$$f(x) = \mathcal{R}_y(f(x)) = \sum_i c_i(x) \mathcal{R}_y(f_i(y)) + \mathcal{R}_y(b(x, y)). \quad (4.1.3)$$

Let $\Delta : V \hookrightarrow V \times V$ be the diagonal morphism $v \mapsto (v, v)$. The corresponding algebra homomorphism $\Delta^* : K[x, y] \rightarrow K[x]$ is defined by $p(x, y) \mapsto p(x, x)$. We apply Δ^* to Eq. (4.1.3):

$$f(x) = \sum_i c_i(x) \mathcal{R}(f_i(x)).$$

In fact, $\Delta^*(\mathcal{R}_y(b(x, y))) = 0$, because $\mathcal{R}_y(b(x, y)) \in \mathfrak{b}$ (\mathfrak{b} is G -stable, see Corollary 2.2.7) and $\Delta(V) \subset \overline{B}$. Since $\mathcal{R}(f_i(x))$ is a homogeneous invariant of degree > 0 , we conclude $f \in I$. \square

Remark 4.1.4 Theorem 4.1.3 can be generalized in the following way. Let X be an arbitrary affine G -variety, and let again \overline{B} be the Zariski closure of the image of the map $\psi : G \times X \rightarrow X \times X$ defined by $(\sigma, x) \mapsto (x, \sigma \cdot x)$. Let $\mathfrak{b} \subset K[X \times X] \cong K[X] \otimes K[X]$ be the vanishing ideal of \overline{B} . A proof, similar to the one of Theorem 4.1.3, shows that if $J \subset K[X]$ is any G -stable ideal, then

$$(\mathfrak{b} + K[X] \otimes J) \cap (K[X] \otimes K)$$

is the ideal in $K[X]$ generated by $J \cap K[X]^G$. In a more algebraic setting, this generalization is carried out in Theorem 4.2.6. In geometric terms this means that if $W \subset X$ is any G -stable subset, then

$$\overline{p_1((X \times W) \cap \overline{B})} = \pi^{-1}(\pi(W)),$$

where $p_1 : X \times X \rightarrow X$ is the projection onto the first factor, and $\pi : X \rightarrow X//G$ is the categorical quotient (see Sect. 2.3). This geometric statement is also true if G is only geometrically reductive. \triangleleft

Example 4.1.5 Let $K = \overline{\mathbb{F}}_2$, the algebraic closure of the field of 2 elements. Let G be the group of order 2, generated by σ . The group G acts on $V := K^4$ by

$$\sigma \cdot (x_1, x_2, x_3, x_4) = (x_2, x_1, x_4, x_3).$$

The invariant ring is generated by $x_1 + x_2$, $x_3 + x_4$, x_1x_2 , x_3x_4 , $x_1x_3 + x_2x_4$. The image B of $\psi : G \times V \rightarrow V \times V$ is the union of the diagonal $\{(v, v) \mid v \in V\}$ and $\{(v, \sigma \cdot v) \mid v \in V\}$. It is easy to check that $f := (x_1 + y_2)(x_3 + y_3)$ vanishes on B . Now $f(x, 0) = x_1x_3$ does not lie in the ideal

$$I = (x_1 + x_2, x_3 + x_4, x_1x_2, x_3x_4, x_1x_3 + x_2x_4).$$

This shows that Theorem 4.1.3 is not always true if G is only geometrically reductive. Notice also that $x_1x_3 + x_2x_4$ lies in the ideal generated by $x_1 + x_2$ and $x_3 + x_4$ because $x_1x_3 + x_2x_4 = x_3(x_1 + x_2) + x_2(x_3 + x_4)$. So in fact I is generated by the invariants $x_1 + x_2$, $x_3 + x_4$, x_1x_2 , x_3x_4 . However, these invariants do not generate the invariant ring. The proof of Theorem 2.2.10 does not generalize to geometrically reductive groups. \triangleleft

4.1.2 The Input: The Group and the Representation

We will concentrate for the moment on the input of the algorithm. We will need a convenient way to tell the algorithm what group and which representation we are dealing with. We will represent an algebraic group G by its affine coordinate ring and the representation V is given by a polynomial map $\rho : G \rightarrow \mathrm{GL}(V) \subset \mathrm{End}(V)$.

Let us start with a linearly reductive group G . We will view G as an affine algebraic group. Since G is an affine variety, there exists a closed embedding $G \hookrightarrow K^l$ for some positive integer l . We will view G as a Zariski closed subset of K^l . This gives us a surjective ring homomorphism $K[z_1, z_2, \dots, z_l] \twoheadrightarrow K[G]$, whose kernel will be denoted by $I(G)$. Suppose that V is an n -dimensional rational representation. By choosing a basis of V , we will identify $V \cong K^n$ and $\mathrm{End}(V) \cong \mathrm{Mat}_{n,n}(K)$, where $\mathrm{Mat}_{m,n}(K)$ is the set of $m \times n$ matrices with entries in K . The G -action on V defines a group homomorphism $\rho : G \rightarrow \mathrm{GL}(V) \subset \mathrm{End}(V) \cong \mathrm{Mat}_{n,n}(K)$ which is also a morphism of affine varieties. We can choose $a_{i,j} \in K[z_1, \dots, z_l]$, $1 \leq i, j \leq n$ (which are unique modulo $I(G)$), such that

$$\rho(g) = \begin{pmatrix} a_{1,1}(g) & a_{1,2}(g) & \cdots & a_{1,n}(g) \\ a_{2,1}(g) & a_{2,2}(g) & \cdots & a_{2,n}(g) \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1}(g) & a_{n,2}(g) & \cdots & a_{n,n}(g) \end{pmatrix}.$$

So the G -action is represented by the matrix $A = (a_{i,j})_{i,j=1}^n \in \mathrm{Mat}_{n,n}(K[z_1, \dots, z_l])$.

The input of the algorithm for computing invariants will be the matrix A together with a set of generators of the ideal $I(G) \subset K[z_1, \dots, z_l]$. We could have chosen a different embedding $G \hookrightarrow K^l$. Sometimes there is no canonical choice for the embedding. Since we are going to do Gröbner basis computations, it is advisable

to take l , the number of variables, small. We also would like the generators of $I(G)$ to have small degree, and $I(G)$ should have a “small” Gröbner basis.

Example 4.1.6 Let $T = (K^*)^r$ be the r -dimensional torus. We have a closed embedding $i : T \hookrightarrow K^{r+1}$ defined by

$$(t_1, t_2, \dots, t_r) \in T \mapsto (t_1, t_2, \dots, t_r, (t_1 t_2 \cdots t_r)^{-1}) \in K^{r+1}.$$

The image is given by the equation $z_1 z_2 \cdots z_{r+1} = 1$. So $K[T] \cong K[z_1, \dots, z_{r+1}] / I(T)$ where $I(T)$ is the ideal generated by the polynomial $z_1 z_2 \cdots z_{r+1} - 1$.

Suppose that V is an n -dimensional representation of T . We can always choose a basis of V such that the action of T is diagonal. The action is given by

$$\sigma \cdot (x_1, \dots, x_n) = (\chi_1(\sigma)x_1, \dots, \chi_n(\sigma)x_n),$$

where χ_1, \dots, χ_n are one-dimensional **characters** of T , i.e., $\chi_i : T \rightarrow \mathbb{G}_m = K^*$ is a homomorphism of algebraic groups for all i . We can write $\chi_i(t_1, \dots, t_r) = t_1^{b_{i,1}} t_2^{b_{i,2}} \cdots t_r^{b_{i,r}}$ with $b_{i,j} \in \mathbb{Z}$ for all i, j . The r -tuple $(b_{i,1}, \dots, b_{i,r})$ is called a **weight**. Define $c_{i,r+1} := \max\{0, -b_{i,1}, -b_{i,2}, \dots, -b_{i,r}\}$ for all i and $c_{i,j} = c_{i,r+1} + b_{i,j}$ for all i, j with $j \leq r$. Let

$$A = \begin{pmatrix} \underline{z}^{c_1} & 0 & \cdots & 0 \\ 0 & \underline{z}^{c_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \underline{z}^{c_n} \end{pmatrix},$$

where \underline{z}^c is an abbreviation for $\prod_{j=1}^{r+1} z_j^{c_{i,j}}$. Then A represents the T -action on V . \triangleleft

Example 4.1.7 The group SL_q has a natural embedding into $\mathrm{Mat}_{q,q}(K) \cong K^{q^2}$, namely it is the set of all matrices $B \in \mathrm{Mat}_{q,q}(K)$ such that $\det(B) = 1$. Therefore, the coordinate ring of SL_q is $K[\{z_{i,j}\}_{i,j=1}^q] / I(\mathrm{SL}_q)$ where $I(\mathrm{SL}_q)$ is generated by the polynomial $\det((z_{i,j})_{i,j=1}^q) - 1$. For convenience we use here a double indexing of the z -variables instead of a single indexing. The natural representation of SL_q is just given by the matrix

$$A = \begin{pmatrix} z_{1,1} & z_{1,2} & \cdots & z_{1,q} \\ z_{2,1} & z_{2,2} & \cdots & z_{2,q} \\ \vdots & \vdots & \ddots & \vdots \\ z_{q,1} & z_{q,2} & \cdots & z_{q,q} \end{pmatrix}.$$

Let us consider the action of SL_2 on the binary forms of degree 2 (see Example 2.1.2). As a basis of V_2 we can take x^2 , xy and y^2 . On this basis, the action

is represented by the matrix

$$\begin{pmatrix} z_{1,1}^2 & z_{1,1}z_{1,2} & z_{1,2}^2 \\ 2z_{1,1}z_{2,1} & z_{2,1}z_{1,2} + z_{1,1}z_{2,2} & 2z_{1,2}z_{2,2} \\ z_{2,1}^2 & z_{2,1}z_{2,2} & z_{2,2}^2 \end{pmatrix}.$$

△

Example 4.1.8 Let G be the symmetric group S_3 . As an affine variety it is just a set of 6 points and we can identify G with $\{1, 2, 3, 4, 5, 6\} \subset K$ (assume that $\text{char}(K) = 0$ or $\text{char}(K) > 6$). We let $1, 2, 3, 4, 5, 6 \in K$ correspond to the elements $e, (1 2), (1 3), (2 3), (1 2 3), (1 3 2)$ (the elements of S_3 are represented by their cycle structure). So G is embedded in K and $K[G] \cong K[z]/I(G)$ where $I(G)$ is the ideal generated by $(z - 1)(z - 2) \cdots (z - 6)$. Let $V \cong K^3$ be the 3-dimensional representation, where S_3 acts by permuting the coordinates. The action of the elements of S_3 is given by the permutation matrices

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

By interpolation we can find a matrix $A \in \text{Mat}_{3,3}(K[z])$ such that $A(1), A(2), \dots, A(6)$ are exactly the permutation matrices above:

$$A = \begin{pmatrix} a_{1,1} & a_{1,2} & a_{1,3} \\ a_{2,1} & a_{2,2} & a_{2,3} \\ a_{3,1} & a_{3,2} & a_{3,3} \end{pmatrix}$$

with

$$\begin{aligned} a_{1,1} &= \frac{(z-2)(z-3)(z-5)(z-6)(3z-2)}{40}, & a_{1,2} &= \frac{(z-1)(z-3)(z-4)(z-5)(3z-16)}{60}, \\ a_{1,3} &= \frac{(z-1)(z-2)(z-4)(z-6)(-3z+13)}{24}, & a_{2,1} &= \frac{(z-1)(z-3)(z-4)(z-6)(3z-11)}{40}, \\ a_{2,2} &= \frac{(z-2)(z-4)(z-5)(z-6)(-11z+13)}{120}, & a_{2,3} &= \frac{(z-1)(z-2)(z-3)(z-5)(11z-64)}{120}, \\ a_{3,1} &= \frac{(z-1)(z-2)(z-4)(z-5)(-3z+19)}{40}, & a_{3,2} &= \frac{(z-1)(z-2)(z-3)(z-6)^2}{24}, \\ a_{3,3} &= \frac{(z-3)(z-4)(z-5)(z-6)(4z-3)}{120}. \end{aligned}$$

Instead of identifying S_3 with $\{1, 2, \dots, 6\} \subset K$ we could have identified S_3 with the sixth roots of unity in K , or with all pairs $(z, w) \in K^2$ with $z^2 = w^3 = 1$. The last identification may be the most natural one and generalizes to all S_n : For each i , let ζ_i be a primitive i -th root of unity. We define a map

$$\{(z_2, z_3, \dots, z_n) \mid z_2^2 = z_3^3 = \dots = z_n^n = 1\} \rightarrow S_n$$

by

$$(\zeta_2^{k_2}, \zeta_3^{k_3}, \dots, \zeta_n^{k_n}) \mapsto (1\ 2)^{k_2}(1\ 2\ 3)^{k_3} \cdots (1\ 2 \cdots n)^{k_n} \quad (4.1.4)$$

for all integers k_2, \dots, k_n . Suppose that

$$(1\ 2)^{k_2}(1\ 2\ 3)^{k_3} \cdots (1\ 2 \cdots n)^{k_n} = (1\ 2)^{l_2}(1\ 2\ 3)^{l_3} \cdots (1\ 2 \cdots n)^{l_n},$$

then $(1\ 2 \cdots n)^{k_n - l_n}$ lies in S_{n-1} , so $k_n \equiv l_n \pmod{n}$. We have

$$(1\ 2)^{k_2}(1\ 2\ 3)^{k_3} \cdots (1\ 2 \cdots n - 1)^{k_{n-1}} = (1\ 2)^{l_2}(1\ 2\ 3)^{l_3} \cdots (1\ 2 \cdots n - 1)^{l_{n-1}},$$

and repeating the argument gives $k_{n-1} \equiv l_{n-1} \pmod{n-1}, \dots, k_2 \equiv l_2 \pmod{2}$. This shows that (4.1.4) is injective, and comparing cardinalities shows that it is a bijection onto S_n . The identification (4.1.4) embeds S_n into K^{n-1} and $K[S_n] \cong K[z_2, z_3, \dots, z_n]/I(S_n)$ where $I(S_n) = (z_2^2 - 1, z_3^3 - 1, \dots, z_n^n - 1)$. \triangleleft

4.1.3 The Algorithm

In view of Theorem 4.1.3 and Proposition 4.1.1, the computation of generators of the invariant ring boils down to finding generators of the ideal \mathfrak{b} . As before, \mathfrak{b} is the vanishing ideal of the Zariski closure of the image B of the map $\psi : G \times V \rightarrow V \times V$, defined by $(\sigma, v) \mapsto (v, \sigma \cdot v)$.

There is a general procedure for computing the vanishing ideal of the image of a morphism of affine varieties using Gröbner bases (see Sect. 1.2.1): If $\varphi : X \rightarrow Y$ is a morphism of affine varieties, one can consider the graph $\Gamma \subset X \times Y$, defined by $\Gamma = \{(v, \varphi(v)) \mid v \in X\}$. Then $\varphi(X)$ is the projection of $\Gamma \subseteq X \times Y$ onto Y . Let $I(\Gamma) \subseteq K[X \times Y]$ be the vanishing ideal of Γ . An element $f \in K[Y]$ vanishes on $\varphi(X)$ if and only if it vanishes on Γ as a function in $\underline{K[X \times Y]}$. In other words, $I(\Gamma) \cap K[Y]$ is the vanishing ideal of $\varphi(X)$ (and of $\varphi(X)$). The intersection $I(\Gamma) \cap K[Y]$ can be computed using Gröbner basis techniques (see Algorithm 1.2).

In our case, we should consider the subset of $(G \times V) \times (V \times V)$ defined by $\{(\sigma, v, v, \sigma \cdot v) \mid \sigma \in G, v \in V\}$. One of the V -factors is redundant. Since we want to minimize the number of variables, we consider instead $\Gamma \subseteq G \times V \times V$ defined by $\{(\sigma, v, \sigma \cdot v) \mid \sigma \in G, v \in V\}$. As in the previous section, we will view G as a Zariski closed subset of K^l . Now $\Gamma \subseteq G \times V \times V \subseteq K^l \times V \times V$ and B is the projection of Γ onto $V \times V$. The coordinate ring of $K^l \times V \times V$ is the polynomial ring $K[z, x, y] = K[x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_l]$. Let $I(\Gamma)$ be the ideal of Γ . We have $\mathfrak{b} = I(\Gamma) \cap K[x, y]$. In other words: We get the ideal \mathfrak{b} from $I(\Gamma)$ by eliminating the variables z_1, \dots, z_l .

Generators of the ideal $I(\Gamma)$ can be given explicitly. The graph Γ is a Zariski closed subset of $K^l \times V \times V$. First of all, we will need generators $h_1, \dots, h_t \in K[z]$ of the ideal $I(G) \subseteq K[z]$, to define $G \subseteq K^l$. The equation

$$\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix} = {}^t A \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}$$

(with ${}^t A$ the transpose of the matrix A from Sect. 4.1.2) gives us the relations $y_i = \sum_j a_{i,j} x_j$. The ideal $I(\Gamma)$ is generated by all

$$h_1, h_2, \dots, h_t \quad \text{and} \quad \left\{ y_i - \sum_{j=1}^n a_{i,j} x_j \mid i = 1, 2, \dots, n \right\}.$$

Choose a monomial ordering “ $>$ ” on $K[z, x, y]$ such that $z_i \gg x_j$ and $z_i \gg y_j$ for $i = 1, \dots, l, j = 1, \dots, n$ (see on p. 4), i.e., z_i is larger than any monomial in $x_1, \dots, x_n, y_1, \dots, y_n$. An example of such an ordering is the lexicographic ordering with $z_1 > z_2 > \dots > z_l > x_1 > \dots > y_n$. Suppose that \mathcal{G} is a Gröbner basis for $I(\Gamma)$. If $f \in \mathfrak{b} = I(\Gamma) \cap K[x, y]$, then the leading monomial $\text{LM}(f)$ is divisible by $\text{LM}(g)$ for some $g \in \mathcal{G}$. It follows that $\text{LM}(g) \in K[x, y]$, and by our choice of the monomial ordering, every monomial appearing in g lies in $K[x, y]$. This shows that $\mathcal{G} \cap K[x, y]$ is a Gröbner basis for $\mathfrak{b} = I(\Gamma) \cap K[x, y]$.

Algorithm 4.1.9 Suppose that G is a linearly reductive algebraic group acting rationally on an n -dimensional vector space. As in Sect. 4.1.2, we will view G as an affine variety in K^l given by the vanishing ideal $I(G) \subseteq K[z_1, \dots, z_l]$. The representation of G on V is given by a matrix $A = (a_{i,j})_{i,j=1}^n$ with $a_{i,j} \in K[z_1, \dots, z_l]$. The following steps will give generators of the invariant ring $K[V]^G$:

- (1) Input: ideal generators $h_1, \dots, h_t \in K[z_1, \dots, z_l]$ such that $h_1 = h_2 = \dots = h_t = 0$ defines an affine variety isomorphic to G ; a matrix $A = (a_{i,j})_{i,j=1}^n$ with $a_{i,j} \in K[z_1, \dots, z_l]$ for all i, j , corresponding to the representation of G on V .
- (2) Choose a monomial ordering “ $>$ ” on $K[x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_l]$ such that $z_i \gg x_j$ and $z_i \gg y_j$ for $i = 1, \dots, l, j = 1, \dots, n$ (see p. 4). Compute a Gröbner basis \mathcal{G} of the ideal

$$\left(h_1, \dots, h_t, \left\{ y_i - \sum_{j=1}^n a_{i,j} x_j \mid i = 1, \dots, n \right\} \right).$$

- (3) $\mathcal{B} = \mathcal{G} \cap K[x_1, \dots, x_n, y_1, \dots, y_n]$ (\mathcal{B} is a Gröbner basis of \mathfrak{b}).
- (4) $\mathcal{I} = \{f(x, 0) \mid f \in \mathcal{B}\}$ (\mathcal{I} is a generating set for I , see Theorem 4.1.3).
- (5) Output: $\{\mathcal{R}(f) \mid f \in \mathcal{I}\}$ (generators of the invariant ring, see Proposition 4.1.1).

At the beginning of Sect. 4.5 we will present a variant of step 5 that does not use the Reynolds operator.

Example 4.1.10 We give a simple illustrative example. Let $G = C_2$ the cyclic group of order 2, and assume $\text{char}(K) \neq 2$. We can identify G as an affine variety with the set $\{-1, 1\} \subset K$. So $G \subset K$ has the vanishing ideal $I(G) = (z^2 - 1) \subset K[z]$. We consider the representation of G on $V = K^2$ which interchanges the two coordinates. This representation is given for example by the matrix

$$A = \begin{pmatrix} \frac{z+1}{2} & \frac{1-z}{2} \\ \frac{1-z}{2} & \frac{z+1}{2} \end{pmatrix}.$$

For $z = 1$ we get the identity matrix and for $z = -1$ we get the permutation matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

We follow the steps of the algorithm:

- (1) Input: G is given by the equation $z^2 - 1 \in K[z]$. The representation is given by the matrix

$$A = \begin{pmatrix} \frac{z+1}{2} & \frac{1-z}{2} \\ \frac{1-z}{2} & \frac{z+1}{2} \end{pmatrix}.$$

- (2) Let “ $>$ ” be the lexicographic ordering on $K[z, x_1, x_2, y_1, y_2]$ with $z > x_1 > x_2 > y_1 > y_2$. We compute a Gröbner basis \mathcal{G} of the ideal

$$(z^2 - 1, y_1 - \frac{z+1}{2}x_1 - \frac{1-z}{2}x_2, y_2 - \frac{1-z}{2}x_1 - \frac{z+1}{2}x_2).$$

A reduced Gröbner basis is:

$$\begin{aligned} \mathcal{G} = \{ &z^2 - 1, zx_2 - zy_2 + x_2 - y_2, zy_1 - zy_2 + 2x_2 - y_1 - y_2, x_1 + x_2 - y_1 - y_2, \\ &x_2^2 + y_1y_2 - y_1x_2 - x_2y_2 \}. \end{aligned} \quad (4.1.5)$$

(3)

$$\mathcal{B} = \mathcal{G} \cap K[x_1, x_2, y_1, y_2] = \{x_1 + x_2 - y_1 - y_2, x_2^2 + y_1y_2 - y_1x_2 - x_2y_2\}.$$

- (4) We substitute $y_1 = y_2 = 0$ in \mathcal{B} :

$$\mathcal{I} = \{x_1 + x_2, x_2^2\}.$$

- (5) We apply the Reynolds operator: $\mathcal{R}(x_1 + x_2) = x_1 + x_2$, because $x_1 + x_2$ is already invariant; $\mathcal{R}(x_2^2) = (x_2^2 + x_1^2)/2$. So the output is: $x_1 + x_2, (x_1^2 + x_2^2)/2$. These are generators of the invariant ring $K[x_1, x_2]^{C_2}$.

△

Example 4.1.11 We take the multiplicative group \mathbb{G}_m . As in Example 4.1.6, we embed \mathbb{G}_m into K^2 and \mathbb{G}_m is defined by the equation $z_1 z_2 = 1$. The group acts diagonally on $V \cong K^4$ with weights $-5, -3, 2, 4$. We use the algorithm to compute $K[x_1, x_2, x_3, x_4]^{\mathbb{G}_m}$.

- (1) The group $\mathbb{G}_m \subset K^2$ is defined as an affine variety by $z_1 z_2 = 1$. The representation is given by the matrix

$$A = \begin{pmatrix} z_2^5 & 0 & 0 & 0 \\ 0 & z_2^3 & 0 & 0 \\ 0 & 0 & z_1^2 & 0 \\ 0 & 0 & 0 & z_1^4 \end{pmatrix}.$$

- (2) We choose a lexicographic ordering “ $>$ ” on $K[z_1, z_2, x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4]$ with $z_1 > z_2 > x_1 > x_2 > x_3 > x_4 > y_1 > y_2 > y_3 > y_4$.

$$\begin{aligned} \mathcal{G} = \{ & x_3^2 y_4 - x_4 y_3^2, x_2^2 x_4^2 y_3 - x_3 y_2^2 y_4^2, x_2^2 x_3 x_4 - y_2^2 y_3 y_4, x_2^2 x_3^3 - y_2^2 y_3^3, \\ & x_2^4 x_4^3 - y_2^4 y_4^3, x_1 y_2^3 y_4 - x_2^3 x_4 y_1, x_1 y_2^3 y_3^2 - x_2^3 x_3^2 y_1, x_1 x_4 y_2 y_3 - x_2 x_3 y_1 y_4, \\ & x_1 x_3 y_2 - x_2 y_1 y_3, x_1 x_2 x_4^2 - y_1 y_2 y_4^2, x_1 x_2 x_3^2 x_4 - y_1 y_2 y_3^2 y_4, x_1 x_2 x_3^4 - y_1 y_2 y_3^4, \\ & x_1^2 y_2^4 y_3 - x_2^4 x_3 y_1^2, x_1^2 x_4 y_2^2 - x_2^2 y_1^2 y_4, x_1^2 x_3^3 y_3 - x_3 y_1^2 y_4^3, x_1^2 x_3 x_4^2 - y_1^2 y_3 y_4^2, \\ & x_1^2 x_3^3 x_4 - y_1^2 y_3^3 y_4, x_1^2 x_3^5 - y_1^2 y_3^5, x_1^2 y_2^5 - x_2^5 y_1^3, x_1^3 x_4^3 y_2 - x_2 y_1^3 y_4^3, x_1^4 x_4^5 - y_1^4 y_4^5, \\ & z_2 y_2 y_4 - x_2 x_4, z_2 y_2 y_3^2 - x_2 x_3^2, z_2 y_1 y_3 y_4 - x_1 x_3 x_4, z_2 y_1 y_3^3 - x_1 x_3^3, \\ & z_2 y_1 y_4^4 - x_1^3 x_4^4, z_2 x_3 y_1 y_4^2 - x_1 x_4^2 y_3, z_2 x_2 y_1^2 y_4^2 - x_1^2 x_4^2 y_2, z_2 x_2 x_4 y_3 - x_3 y_2 y_4, \\ & z_2 x_2 x_3 - y_2 y_3, z_2 x_2^2 y_1 - x_1 y_2^2, z_2 x_3^3 x_4^2 - y_2^3 y_4^2, z_2 x_1 y_2^2 y_3 - x_2^2 x_3 y_1, \\ & z_2 x_1 x_4 - y_1 y_4, z_2 x_1 x_3^2 - y_1 y_3^2, z_2 x_1^2 y_2^3 - x_2^3 y_1^2, z_2^2 y_3 - x_3, z_2^2 y_1^2 y_4^3 - x_1^2 x_4^3, \\ & z_2^2 x_3 y_4 - x_4 y_3, z_2^2 x_2 y_1 y_4 - x_1 x_4 y_2, z_2^2 x_2^2 x_4 - y_2^2 y_4, z_2^2 x_1 y_2 - x_2 y_1, \\ & z_2^3 y_1 y_4^2 - x_1 x_4^2, z_2^3 x_2 - y_2, z_2^3 x_1 x_3 - y_1 y_3, z_2^4 y_4 - x_4, z_2^5 x_1 - y_1, z_1 y_2 - z_2^2 x_2, \\ & z_1 y_1 - z_2^4 x_1, z_1 x_4 - z_2^3 y_4, z_1 x_3 - z_2 y_3, z_1 z_2 - 1 \}. \end{aligned} \quad (4.1.6)$$

- (3) Now we take the intersection $\mathcal{B} = \mathcal{G} \cap K[x_1, x_2, x_3, x_4, y_1, y_2, y_3, y_4]$:

$$\mathcal{B} = \{ x_3^2 y_4 - x_4 y_3^2, x_2^2 x_4^2 y_3 - x_3 y_2^2 y_4^2, x_2^2 x_3 x_4 - y_2^2 y_3 y_4, x_2^2 x_3^3 - y_2^2 y_3^3,$$

$$\begin{aligned}
& x_2^4x_4^3 - y_2^4y_4^3, x_1y_2^3y_4 - x_2^3x_4y_1, x_1y_2^3y_3^2 - x_2^3x_3^2y_1, x_1x_4y_2y_3 - x_2x_3y_1y_4, \\
& x_1x_3y_2 - x_2y_1y_3, x_1x_2x_4^2 - y_1y_2y_4^2, x_1x_2x_3^2x_4 - y_1y_2y_3^2y_4, x_1x_2x_3^4 - y_1y_2y_3^4, \\
& x_1y_2^4y_3 - x_2^4x_3y_1^2, x_1^2x_4y_2^2 - x_2^2y_1^2y_4, x_1^2x_3^3y_3 - x_3y_1^2y_4^3, x_1^2x_3x_4^2 - y_1^2y_3y_4^2, \\
& x_1^2x_3^3x_4 - y_1^2y_3y_4, x_1^2x_3^5 - y_1^2y_3^5, x_1^3y_2^5 - x_2^5y_1^3, x_1^3x_4y_2 - x_2y_1^3y_4^3, \\
& x_1^4x_4^5 - y_1^4y_4^5. \quad (4.1.7)
\end{aligned}$$

(4) We substitute $y_1 = y_2 = y_3 = y_4 = 0$ to obtain:

$$\begin{aligned}
\mathcal{I} = & \{x_2^2x_3x_4, x_2^2x_3^3, x_2^4x_4^3, x_1x_2x_4^2, x_1x_2x_3^2x_4, x_1x_2x_3^4, \\
& x_1^2x_3x_4^2, x_1^2x_3^3x_4, x_1^2x_3^5, x_1^4x_4^5\}.
\end{aligned}$$

(5) The elements of \mathcal{I} are already invariant, so we do not have to apply the Reynolds operator here (this is typical for invariants of a diagonal action). The generators of $K[x_1, x_2, x_3, x_4]^{\mathbb{G}_m}$ are therefore:

$$\begin{aligned}
& x_2^2x_3x_4, x_2^2x_3^3, x_2^4x_4^3, x_1x_2x_4^2, x_1x_2x_3^2x_4, \\
& x_1x_2x_3^4, x_1^2x_3x_4^2, x_1^2x_3^3x_4, x_1^2x_3^5, x_1^4x_4^5.
\end{aligned}$$

In the torus case Algorithm 4.1.9 does the same as Algorithm 1.4.5 in Sturmfels [2].

△

Example 4.1.12 Let us do a simple example with a nice group. We take $G = \mathrm{SL}_2$ acting on the binary forms of degree 2.

(1) Input: The group is given by $z_{1,1}z_{2,2} - z_{1,2}z_{2,1} - 1 \in K[z_{1,1}, z_{1,2}, z_{2,1}, z_{2,2}]$ and the representation is given by the matrix

$$\rho = \begin{pmatrix} z_{1,1}^2 & z_{1,1}z_{1,2} & z_{1,2}^2 \\ 2z_{1,1}z_{2,1} & z_{1,1}z_{2,2} + z_{1,2}z_{2,1} & 2z_{1,2}z_{2,2} \\ z_{2,1}^2 & z_{2,1}z_{2,2} & z_{2,2}^2 \end{pmatrix}.$$

(2) We choose the lexicographic ordering with

$$z_{1,1} > z_{2,1} > z_{1,2} > z_{2,2} > x_1 > x_2 > x_3 > y_1 > y_2 > y_3$$

on $K[z_{1,1}, z_{2,1}, z_{1,2}, z_{2,2}, x_1, x_2, x_3, y_1, y_2, y_3]$. We have

$$\begin{aligned}
I(\Gamma) = & (z_{1,1}z_{2,2} - z_{2,1}z_{1,2} - 1, y_1 - z_{1,1}^2x_1 - 2z_{1,1}z_{2,1}x_2 - z_{2,1}^2x_3, \\
& y_2 - z_{1,1}z_{1,2}x_1 - (z_{1,1}z_{2,2} + z_{2,1}z_{1,2})x_2 - z_{2,1}z_{2,2}x_3, \\
& y_3 - z_{1,2}^2x_1 - 2z_{1,2}z_{2,2}x_2 - z_{2,2}^2x_3). \quad (4.1.8)
\end{aligned}$$

A reduced Gröbner basis is

$$\begin{aligned}
\mathcal{G} = \{ & z_{1,1}z_{2,2} - z_{2,1}z_{1,2} - 1, 2z_{1,1}x_1 - 2z_{2,2}y_1 + z_{2,1}y_2 + z_{2,1}x_2, \\
& x_2z_{1,1} - z_{1,1}y_2 + 2z_{2,1}x_3 + 2z_{1,2}y_1, -z_{1,2}y_2 + 2z_{1,1}y_3 - z_{1,2}x_2 - 2z_{2,2}x_3, \\
& 2x_1z_{1,1}z_{1,2} + 2x_1 - 2z_{2,2}^2y_1 + z_{2,2}z_{2,1}y_2 + z_{2,2}z_{2,1}x_2, \\
& -y_2 + 2z_{2,1}z_{2,2}x_3 + 2z_{1,2}z_{2,2}y_1 - z_{1,2}z_{2,1}y_2 + x_2z_{2,1}z_{1,2} + x_2, \\
& -z_{2,2}y_2 + 2z_{1,2}x_1 + x_2z_{2,2} + 2z_{2,1}y_3, -y_3 + z_{1,2}^2x_1 + z_{1,2}z_{2,2}x_2 + z_{2,2}^2x_3, \\
& -4y_3x_3 + 4x_3z_{1,2}z_{2,2}x_2 + 4z_{2,2}^2x_3^2 + 4z_{1,2}^2y_3y_1 - z_{1,2}^2y_2^2 + z_{1,2}^2x_2^2, \\
& -4y_3y_1 + y_2^2 + 4x_1x_3 - x_2^2 \}. \tag{4.1.9}
\end{aligned}$$

(3) The intersection $\mathcal{B} = \mathcal{G} \cap K[x_1, x_2, x_3, y_1, y_2, y_3]$ is equal to

$$\mathcal{B} = \{-4y_3y_1 + y_2^2 + 4x_1x_3 - x_2^2\}.$$

(4) Substituting $y_1 = y_2 = y_3 = 0$, we obtain

$$\mathcal{I} = \{4x_1x_3 - x_2^2\}.$$

(5) We do not have to apply the Reynolds operator, because $4x_1x_3 - x_2^2$ is already invariant. In fact, it is the discriminant up to a sign. So we conclude

$$K[x_1, x_2, x_3]^{\text{SL}_2} = K[x_2^2 - 4x_1x_3].$$

Compare this to Example 2.1.2

△

In Example 5.9.1 we will consider a situation where the set \mathcal{I} of generators of I does not consist entirely of invariants. We will replace the application of the Reynolds operator (step 5) by a different approach, which comes down to solving a linear system in order to determine invariant generators of the ideal I .

4.2 Improvements and Generalizations

Algorithm 4.1.9 works in a general setting. It is quite fast for tori. In that case, every polynomial in the Gröbner basis of $I(\Gamma)$, and even every polynomial appearing in the Buchberger algorithm is a difference between two monomials. This makes the Gröbner basis computation quite efficient. For examples other than tori, the speed varies. Sometimes the Gröbner basis computation can be quite time consuming. If more is known about the group or the representation, this might be used to improve

the algorithm. In this section we discuss an adaptation of Algorithm 4.1.9 which might speed up the computation. We will also see how the algorithm generalizes to the computation of the *module of covariants*, the *ring of covariants* and to rings of invariants of graded rings.

4.2.1 Localization of the Invariant Ring

We do not necessarily need generators of the ideal $\mathfrak{b} \subset K[x, y]$ for the algorithm to work. Instead of \mathfrak{b} we might use another ideal with sufficiently nice properties. Let \mathfrak{c} be the ideal generated by all $f(x) - f(y)$, with $f \in K[V]^G$. The following corollary follows from Theorem 4.1.3.

Corollary 4.2.1 *Suppose that $f_1(x, y), f_2(x, y), \dots, f_r(x, y)$ are homogeneous and generate a homogeneous ideal $\mathfrak{a} \subset K[x_1, \dots, x_n, y_1, \dots, y_n]$ with $\mathfrak{c} \subseteq \mathfrak{a} \subseteq \mathfrak{b}$. Then $I = (f_1(x, 0), \dots, f_r(x, 0))$ where $I \subset K[V]$ is the ideal generated by all homogeneous invariants of positive degree.*

Proof If $\mathfrak{a} = \mathfrak{b}$, then the corollary follows from Theorem 4.1.3 and if $\mathfrak{a} = \mathfrak{c}$, then the statement is trivial. It follows that the corollary is true for all \mathfrak{a} with $\mathfrak{c} \subseteq \mathfrak{a} \subseteq \mathfrak{b}$.

□

The corollary gives us more flexibility. Such an ideal \mathfrak{a} might be easier to compute than the ideal \mathfrak{b} . Also, a Gröbner basis of such an ideal \mathfrak{a} might be smaller than the Gröbner basis of \mathfrak{b} .

Sometimes we know the invariant ring $K[V]_h^G$ for some localization $K[V]_h$, but we do not know the invariant ring $K[V]^G$ itself. In that case, the following proposition gives an ideal $\mathfrak{a} \subset K[V \times V]$ which satisfies the conditions in Corollary 4.2.1.

Proposition 4.2.2 *Let $h \in K[V]^G$ be homogeneous and suppose that the localization $K[V]_h^G$ is generated by $h, 1/h$ and $f_1, \dots, f_r \in K[V]^G$. Let $\mathfrak{a}' \subset K[z, x_1, \dots, x_n, y_1, \dots, y_n]$ be the ideal*

$$(zh(x) - 1, h(x) - h(y), f_1(x) - f_1(y), f_2(x) - f_2(y), \dots, f_r(x) - f_r(y)).$$

Then $\mathfrak{a} = \mathfrak{a}' \cap K[x, y]$ satisfies $\mathfrak{c} \subseteq \mathfrak{a} \subseteq \mathfrak{b}$.

Proof Suppose that $f \in K[V]^G$ is homogeneous. For some positive power k , $h^k f$ lies in the ring generated by h, f_1, \dots, f_r . This implies that $h^k(x)f(x) - h^k(y)f(y) \in \mathfrak{a}'$. Modulo \mathfrak{a}' , $z^k(h^k(x)f(x) - h^k(y)f(y))$ is equal to $f(x) - f(y)$, so $f(x) - f(y) \in \mathfrak{a}'$. This shows that $\mathfrak{c} \subseteq \mathfrak{a}'$.

Clearly \mathfrak{a}' vanishes on all $(1/h(v), v, v) \in K \times V \times V$ with $h(v) \neq 0$. This shows that \mathfrak{a} vanishes on the diagonal $\Delta(V) = \{(v, v) \mid v \in V\} \subset V \times V$. Let

$$I(\Delta(V)) = (x_1 - y_1, \dots, x_n - y_n) \subset K[V \times V]$$

be the vanishing ideal of $\Delta(V)$. The ideals \mathfrak{a}' and \mathfrak{a} are G -stable (with G acting trivially on z and on the y_i), so $\mathfrak{a} \subseteq \sigma \cdot I(\Delta(V))$ for all $\sigma \in G$. We have $\mathfrak{a} \subseteq \mathfrak{b}$ because the intersection of all $\sigma \cdot I(\Delta(V))$ is equal to \mathfrak{b} . \square

Notice that again we can compute the ideal \mathfrak{a} by elimination (see Algorithm 1.2.1). Namely, choose a monomial ordering “ $>$ ” on $K[z, x_1, \dots, x_n, y_1, \dots, y_n]$ such that $z \gg x_i$ and $z \gg y_i$ for $i = 1, \dots, n$. If \mathcal{G} is a Gröbner basis of $\mathfrak{a}' \subset K[z, x, y]$, then $\mathcal{G} \cap K[x, y]$ is a Gröbner basis of \mathfrak{a} .

Often, it is much easier to find a localization of the invariant ring $K[V]_h^G$ ($h \in K[V]^G$ homogeneous), than to find the invariant ring itself.

Suppose V is a representation of G containing a $v \in V$ such that $G \cdot v$ is a closed orbit, and the stabilizer of v is trivial. It is a consequence of Luna’s slice theorem (see Luna [3]) that there exists an affine variety U and an étale G -equivariant map

$$\gamma : G \times U \rightarrow V$$

such that the image of γ contains v (G acts on the left on G and trivially on U). In other words, the action is locally trivial in an étale neighborhood of v . For some groups, called **special groups**, we can actually choose a Zariski open neighborhood, i.e., we may assume that γ is an open immersion. Examples of such special groups are SL_q and GL_q . Now $K[G \times U]$ is just a localization $K[V]_h$ with respect to some semi-invariant h and $K[G \times U]^G$ is just equal to $K[U]$.

We will discuss this more explicitly in the case $G = \mathrm{SL}_q$ and we will show how we can use Proposition 4.2.2 to improve Algorithm 4.1.9.

Proposition 4.2.3 *Let $W \cong K^q$ be the natural representation of SL_q and suppose that V is a representation of $G = \mathrm{SL}_q$ (extendible to a GL_q -representation). Suppose that*

$$\varphi_1, \varphi_2, \dots, \varphi_q : V \rightarrow W$$

are SL_q -equivariant morphisms. We can view $\varphi = (\varphi_1, \dots, \varphi_q)$ as a $q \times q$ matrix with entries in $K[V]$. We assume that $h := \det(\varphi) \neq 0$. For $f \in K[V]$, define $\varphi \cdot f \in K[V]_h^G$ by $(\varphi \cdot f)(v) = f(\varphi(v)^{-1} \cdot v)$, where $\varphi(v)^{-1} \in \mathrm{GL}_q(K)$ is applied to v by the action extended from G to GL_q . Then the ring $K[V]_h^G$ is generated by

$$1/h, h, \varphi \cdot x_1, \varphi \cdot x_2, \dots, \varphi \cdot x_n,$$

where $x_1, \dots, x_n \in K[V]$ form a basis of V^ .*

Proof We have $\varphi(\sigma \cdot v) = \sigma\varphi(v)$ for all $v \in V$ and $\sigma \in G$. This shows that h is SL_q -invariant. If $f \in K[V]$, then $\varphi \cdot f$ is SL_q invariant: For $\sigma \in \mathrm{SL}_q$ we have

$$\sigma \cdot f(\varphi(v)^{-1} \cdot v) = f(\varphi^{-1}(\sigma^{-1} \cdot v)\sigma^{-1} \cdot v) = f(\varphi^{-1}(v)\sigma\sigma^{-1} \cdot v) = f(\varphi^{-1}(v) \cdot v).$$

Note that φ^{-1} is a matrix with coefficients in $K[V]_h$. If $f \in K[V]^G$ is a GL_q -semi-invariant, then

$$h^k f(x_1, \dots, x_n) = \varphi \cdot f(x_1, \dots, x_n) = f(\varphi \cdot x_1, \dots, \varphi \cdot x_n)$$

for some integer k , so f lies in the ring generated by $h, 1/h, \varphi \cdot x_1, \dots, \varphi \cdot x_n$. This completes the proof because $K[V]^{\mathrm{SL}_q}$ is spanned by GL_q -semi-invariants (see Corollary 2.2.12). \square

An SL_q -equivariant morphism $\varphi_i : V \rightarrow W$ as above is called a covariant with values in W (see Definition 4.2.9)

Example 4.2.4 Let us consider SL_2 and $V = V_1 \oplus V_2$. We identify $K[V_1] \cong K[x_1, x_2]$, $K[V_2] \cong K[x_3, x_4, x_5]$, and $K[V] \cong K[x_1, x_2, x_3, x_4, x_5]$. The action on the functions x_1, \dots, x_5 is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \begin{pmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \end{pmatrix} = \begin{pmatrix} (ad - bc)^{-1}(dx_1 - bx_2) \\ (ad - bc)^{-1}(ax_2 - cx_1) \\ (ad - bc)^{-2}(d^2x_3 - bdx_4 + b^2x_5) \\ (ad - bc)^{-2}(-2cdx_3 + (bc + ad)x_4 - 2abx_5) \\ (ad - bc)^{-2}(c^2x_3 - acx_4 + a^2x_5) \end{pmatrix}. \quad (4.2.1)$$

We take

$$\varphi_1 = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, \quad \varphi_2 = \begin{pmatrix} 2x_2x_3 - x_1x_4 \\ x_2x_4 - 2x_1x_5 \end{pmatrix}.$$

The matrix φ is given by

$$\varphi = \begin{pmatrix} x_1 & 2x_2x_3 - x_1x_4 \\ x_2 & x_2x_4 - 2x_1x_5 \end{pmatrix}.$$

Thus $h = \det(\varphi) = 2x_1x_2x_4 - 2x_1^2x_5 - 2x_2^2x_3$. We use $a = x_1$, $b = 2x_2x_3 - x_1x_4$, $c = x_2$ and $d = x_2x_4 - 2x_1x_5$ in (4.2.1) to obtain

$$\varphi \cdot x_1 = 1, \quad \varphi \cdot x_2 = 0, \quad \varphi \cdot x_3 = (x_4^2 - 4x_3x_5)/h, \quad \varphi \cdot x_4 = 0, \quad \varphi \cdot x_5 = -1/4h.$$

We take the ideal

$$\begin{aligned} \mathfrak{a}' = (zx_1x_2x_4 - zx_1^2x_5 - zx_2^2x_3 - 1, x_1x_2x_4 - x_1^2x_5 - x_2^2x_3 - y_1y_2y_4 + y_1^2y_5 + y_2^2y_3, \\ x_4^2 - 4x_3x_5 - y_4^2 + 4y_3y_5). \end{aligned} \quad (4.2.2)$$

We use the lexicographic ordering with $z > x_1 > x_2 > \dots > y_5$ and compute a Gröbner basis:

$$\begin{aligned} \mathcal{G} = \{ & zy_1y_2y_4 - zy_1^2y_5 - zy_2^2y_3 - 1, -4x_3x_1x_2x_4 + 4x_2^2x_3^2 + 4x_3y_1y_2y_4 - \\ & 4x_3y_1^2y_5 - 4x_3y_2^2y_3 + x_1^2x_4^2 - x_1^2y_4^2 + 4x_1^2y_3y_5, x_1x_2x_4 - x_1^2x_5 - x_2^2x_3 - y_1y_2y_4 + \\ & y_1^2y_5 + y_2^2y_3, x_4^2 - 4x_3x_5 - y_4^2 + 4y_3y_5 \}. \end{aligned} \quad (4.2.3)$$

A Gröbner basis \mathcal{A} of $\mathfrak{a} = \mathfrak{a}' \cap K[x, y]$ is obtained by intersecting \mathcal{G} with $K[x, y]$:

$$\begin{aligned} \mathcal{A} = \{ & -4x_3x_1x_2x_4 + 4x_2^2x_3^2 + 4x_3y_1y_2y_4 - 4x_3y_1^2y_5 - 4x_3y_2^2y_3 + x_1^2x_4^2 - x_1^2y_4^2 + \\ & 4x_1^2y_3y_5, x_1x_2x_4 - x_1^2x_5 - x_2^2x_3 - y_1y_2y_4 + y_1^2y_5 + y_2^2y_3, \\ & x_4^2 - 4x_3x_5 - y_4^2 + 4y_3y_5 \}. \end{aligned} \quad (4.2.4)$$

We substitute $y_1 = y_2 = y_3 = 0$ to get generators of the ideal I :

$$I = (-4x_3x_1x_2x_4 + 4x_2^2x_3^2 + x_1^2x_4^2, x_1x_2x_4 - x_1^2x_5 - x_2^2x_3, x_4^2 - 4x_3x_5).$$

The first generator lies in the ideal generated by the latter two. Therefore

$$I = (x_1x_2x_4 - x_1^2x_5 - x_2^2x_3, x_4^2 - 4x_3x_5)$$

and since these two generators are already SL_2 -invariant, we do not have to apply the Reynolds operator and conclude

$$K[V]^{\mathrm{SL}_2} = K[x_1x_2x_4 - x_1^2x_5 - x_2^2x_3, x_4^2 - 4x_3x_5].$$

□

The following proposition shows that under mild conditions, a morphism $\varphi : V \rightarrow W^q$ as in Proposition 4.2.3 can be found.

Proposition 4.2.5 *Suppose that V is a representation of SL_q , $v \in V$ has trivial stabilizer and the orbit $\mathrm{SL}_q \cdot v$ is closed. Then there exist SL_q -equivariant morphisms $\varphi_1, \dots, \varphi_q : V \rightarrow W$ such that $\det(\varphi) \neq 0$ where $\varphi = (\varphi_1, \dots, \varphi_q)$. Here, as before, W denotes the natural representation of SL_q .*

Proof We will identify SL_q with the orbit $\mathrm{SL}_q \cdot v$ in V . The inclusion $\mathrm{SL}_q \cdot v \hookrightarrow V$ induces a surjective SL_q -equivariant ring homomorphism $K[V] \twoheadrightarrow K[\mathrm{SL}_q]$ whose kernel we denote by J . Choose a basis of W . There is a SL_q -equivariant embedding $\psi = (\psi_1, \dots, \psi_q) : \mathrm{SL}_q \rightarrow W^q$ which identifies SL_q with the linear maps $K^q \rightarrow W$ with determinant equal to 1 (with respect to the chosen bases). In particular we

have $\det(\psi) \neq 0$. For each i , $\psi_i : \mathrm{SL}_q \cdot v \rightarrow W$ is dominant because $\mathrm{SL}_q \cdot v$ maps to the dense orbit of W . The morphism $\psi_i : \mathrm{SL}_q \cdot v \rightarrow W$ corresponds to an injective ring homomorphism $\psi_i^* : K[W] \cong S(W^*) \rightarrow K[\mathrm{SL}_q] \cong K[V]/J$. Choose a subrepresentation $W_i \subset K[V]$ isomorphic to W^* such that $W_i + J = \psi_i^*(W^*)$. The inclusion $W^* \cong W_i \subset K[V]$ defines an SL_q -equivariant morphism $\varphi_i : V \rightarrow W$ which extends ψ_i . In particular $\det(\varphi) + J = \det(\psi) \neq 0$, so $\det(\varphi) \neq 0$. \square

4.2.2 Generalization to Arbitrary Graded Rings

Let us prove the results of Sect. 4.1.1 in the most general (but less geometric) setting. Let R be an arbitrary commutative algebra of finite type over K . Suppose that G is a linearly reductive group acting rationally on R by automorphisms, i.e., there exists a map $\hat{\mu} : R \rightarrow R \otimes K[G]$ such that if

$$\hat{\mu}(f) = \sum_i f_i \otimes g_i,$$

then $\sigma \cdot f = \sum_i f_i g_i(\sigma)$ (see Definition A.1.7). We define a homomorphism $\Delta^* : R \otimes R \rightarrow R$ by $\Delta^*(f \otimes h) = fh$.

Theorem 4.2.6 *Suppose that $\mathfrak{a} \subset R \otimes R$ is an ideal with the following properties:*

- (1) \mathfrak{a} is G -stable (G acts trivially on the first factor of $R \otimes R$, and as usual on the second);
- (2) for every $f \in R^G$ we have $f \otimes 1 - 1 \otimes f \in \mathfrak{a}$;
- (3) $\Delta^*(\mathfrak{a}) = \{0\}$, i.e., \mathfrak{a} lies in the kernel of Δ^* .

Assume that J is a G -stable ideal of R . Then

$$(R \otimes J + \mathfrak{a}) \cap R \otimes 1 = J' \otimes 1,$$

where J' is the ideal in R generated by $J \cap R^G$.

Proof “ \supseteq ”: Clearly, if $f \in J \cap R^G$, then

$$f \otimes 1 = (f \otimes 1 - 1 \otimes f) + 1 \otimes f$$

and $f \otimes 1 - 1 \otimes f \in \mathfrak{a}$ and $1 \otimes f \in R \otimes J$.

“ \subseteq ”: Suppose that $f \otimes 1$ lies in $R \otimes J + \mathfrak{a}$, say

$$f \otimes 1 = \sum_i f_i \otimes h_i + a \tag{4.2.5}$$

with $f_i \in R$, $h_i \in J$ for all i and $a \in \mathfrak{a}$. We apply $\text{id} \otimes \mathcal{R} : R \otimes R \rightarrow R \otimes R^G$ to (4.2.5), where \mathcal{R} is the Reynolds operator and id is the identity:

$$f \otimes 1 = \sum_i f_i \otimes \mathcal{R}(h_i) + (\text{id} \otimes \mathcal{R})(a) \quad (4.2.6)$$

Let us apply Δ^* to (4.2.6):

$$f = \sum_i f_i \mathcal{R}(h_i).$$

Notice that $\Delta^*((\text{id} \otimes \mathcal{R})(a)) = 0$ because \mathfrak{a} is G -stable, so $(\text{id} \otimes \mathcal{R})(a) \in \mathfrak{a}$. Now for every i , $\mathcal{R}(h_i) \in R^G \cap J$ because J is G -stable. This proves that $f \in J'$. \square

Suppose that $R = \bigoplus_{d=0}^{\infty} R_d$ is graded and $R_0 = K$. We assume that G acts homogeneously, i.e., on each component R_d .

Proposition 4.2.7 *Let I be the ideal generated by all homogeneous invariants of positive degree. If $I = (f_1, \dots, f_r)$ with f_i homogeneous for all i , then $R^G = R[\mathcal{R}(f_1), \dots, \mathcal{R}(f_r)]$.*

Proof This proof is exactly the same as the proof of Proposition 4.1.1. \square

Using the construction of Lemma A.1.9, we can find a representation V of G and a G -equivariant surjective ring homomorphism $\varphi : K[V] \twoheadrightarrow R$. In fact, we may assume that $K[V]$ is graded, i.e., $K[V] = \bigoplus_{d=0}^{\infty} K[V]_d$, φ is surjective, and $V^* \subset K[V]$ is spanned by homogeneous functions, say spanned by $x_1, \dots, x_n \in V^*$ (possibly not all of the same degree). Let $I_R = (u_1, \dots, u_p) \subset K[x_1, \dots, x_n]$ be the kernel. This is a homogeneous ideal.

We write $K[G] \cong K[z_1, \dots, z_l]/I(G)$ where $I(G) = (h_1, \dots, h_t)$. As usual, the action of G on V is given by

$$\rho(g) = \begin{pmatrix} a_{1,1}(g) & a_{1,2}(g) & \cdots & a_{1,n}(g) \\ a_{2,1}(g) & a_{2,2}(g) & \cdots & a_{2,n}(g) \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1}(g) & a_{n,2}(g) & \cdots & a_{n,n}(g) \end{pmatrix}, \quad g \in G,$$

with $a_{i,j} \in K[z_1, \dots, z_l]$ for all i, j .

The following algorithm is an obvious generalization of Algorithm 4.1.9.

Algorithm 4.2.8

- (1) Input: ideal generators $h_1, \dots, h_t \in K[z_1, \dots, z_l]$ such that the ideal (h_1, \dots, h_t) defines the group G ; a matrix $A = (a_{i,j})_{i,j=1}^n$ with $a_{i,j} \in K[z_1, \dots, z_l]$ defining the representation of G on V ; $u_1, \dots, u_p \in K[x_1, \dots, x_n]$ defining the homogeneous ideal I_R .

- (2) Choose a monomial ordering “ $>$ ” on $K[z_1, \dots, z_l, x_1, \dots, x_n, y_1, \dots, y_n]$ such that $z_i \gg x_j$ and $z_i \gg y_j$ for $i = 1, \dots, l, j = 1, \dots, n$ (see p. 4). Compute a Gröbner basis \mathcal{G} of the ideal generated by

$$h_1(z), \dots, h_t(z), u_1(x), \dots, u_p(x), u_1(y), \dots, u_p(y), \quad \text{and}$$

$$\{y_i - \sum_{j=1}^n a_{j,i}(z)x_j \mid i = 1, \dots, n\}.$$

- (3) $\mathcal{B} = \mathcal{G} \cap K[x_1, \dots, x_n, y_1, \dots, y_n]$.
(4) $\mathcal{I} = \{f(x, 0) \mid f \in \mathcal{B}\}$.
(5) Output: $\{\mathcal{R}(f) \mid f \in \mathcal{I}\}$. These are modulo I_R generators of $(K[V]/I_R)^G$.

Proof We prove the correctness of the algorithm. Let $X \subseteq V$ be the zero set of u_1, \dots, u_p , so $R \cong K[X]$. The ideal in Step (2) is equal to

$$I(\Gamma) \subseteq K[z_1, \dots, z_l, x_1, \dots, x_n, y_1, \dots, y_n],$$

where $\Gamma = \{(\sigma, x, \sigma \cdot x) \mid \sigma \in G, x \in X\}$. Let us write $\mathfrak{b} = I(\Gamma) \cap K[x, y]$. We have

$$R \otimes R \cong K[x, y]/(u_1(x), \dots, u_p(x), u_1(y), \dots, u_p(y)).$$

Let $\mathfrak{a} \in R \otimes R$ be the image of the ideal \mathfrak{b} . We prove that \mathfrak{a} has the desired properties of Theorem 4.2.6. First of all, if $f \in R^G$, then there exists an $\tilde{f} \in K[V]^G$ whose image modulo I_R is equal to f . It is easy to see that $\tilde{f}(x) - \tilde{f}(y) \in \mathfrak{b}$, so $f \otimes 1 - 1 \otimes f \in \mathfrak{a}$. Also note that if $\mathfrak{m}_e \subset K[z_1, \dots, z_l]$ is the maximal ideal corresponding to the identity element, then

$$\mathfrak{m}_e + I(\Gamma) =$$

$$\mathfrak{m}_e + (u_1(x), \dots, u_p(x), u_1(y), \dots, u_p(y), x_1 - y_1, x_2 - y_2, \dots, x_n - y_n).$$

This shows that

$$\mathfrak{b} \subseteq (u_1(x), \dots, u_p(x), u_1(y), \dots, u_p(y), x_1 - y_1, x_2 - y_2, \dots, x_n - y_n)$$

and \mathfrak{a} lies in the kernel of Δ^* . In Step (3) we obtain a Gröbner basis \mathcal{B} of \mathfrak{b} . The correctness of the algorithm now follows from Theorem 4.2.6 and Proposition 4.2.7. \square

4.2.3 Covariants

Invariants and semi-invariants are special cases of so-called covariants. In this section we will study covariants, and how to compute them.

Definition 4.2.9 Suppose that X is a G -variety and W is a G -module. A **covariant** (sometimes also called an **equivariant**) of X with values in W is a G -equivariant morphism $\varphi : X \rightarrow W$. For fixed X and W , we will denote the set of covariants with values in W by $\text{Mor}(X, W)^G$.

If $W = K$ is the trivial representation, then $\text{Mor}(X, K)^G = K[X]^G$ is the ring of invariants. In general $\text{Mor}(X, K)^G$ carries the structure of a vector space. Also, if $f \in K[X]^G$, and $\varphi : X \rightarrow W$ is a covariant, then $f\varphi$ (scalar multiplication on W) is also a covariant. In this way $\text{Mor}(X, W)^G$ is a $K[X]^G$ -module. We will call $\text{Mor}(X, W)^G$ the **module of covariants** with values in W .

Theorem 4.2.10 *For a linearly reductive group G and an affine G -variety, the module of covariants is finitely generated.*

Proof See Popov and Vinberg [4, Theorem 3.24]. □

A covariant $\varphi : X \rightarrow W$ naturally induces a ring homomorphism $\varphi^* : K[W] \rightarrow K[X]$. Since $K[W]$ is the symmetric algebra on W^* , we obtain $\varphi^* : S(W^*) \rightarrow K[X]$. This homomorphism is uniquely determined by its restriction to the linear part W^* and every linear map $\varphi^* : W^* \rightarrow K[X]$ induces a unique $\varphi^* : S(W^*) \rightarrow K[X]$. In this way, we can identify $\text{Mor}(X, W)^G$ with the space $\text{Hom}(W^*, K[X])^G$ of G -equivariant linear maps from W^* to $K[X]$. In other words

$$\text{Mor}(X, W)^G \cong (W \otimes K[X])^G. \quad (4.2.7)$$

Let us write $K[W^*] \cong K[y_1, \dots, y_m]$. Then $K[X \times W^*] \cong K[X][y_1, \dots, y_m]$. Let \mathfrak{m}_y be the ideal in $K[X \times W^*]$ generated by y_1, \dots, y_m . We have a grading on $K[X \times W^*]$ given by the degree in the y -variables. The degree 0 part is equal to $K[X \times W^*]_0 = K[X]$, and the degree 1 part is equal to $K[X] \otimes W$. So we have an isomorphism of $K[X]$ -modules

$$K[X \times W^*]/\mathfrak{m}_y^2 \cong K[X] \oplus K[X] \otimes W.$$

Taking invariants, we get

$$(K[X \times W^*]/\mathfrak{m}_y^2)^G \cong K[X]^G \oplus (K[X] \otimes W)^G,$$

and, as remarked before, $(K[X] \otimes W)^G$ is the module of covariants with values in W . Suppose $f_1, \dots, f_r, u_1, \dots, u_s$ are homogeneous generators of $(K[X \times W^*]/\mathfrak{m}_y^2)^G$. We assume that f_1, \dots, f_r have degree 0, and u_1, \dots, u_s have degree 1. Then f_1, \dots, f_r must be generators of $K[X]^G$. The polynomials u_1, \dots, u_s are $K[X]^G$ -module generators of the module of covariants $(K[X] \otimes W)^G$.

Suppose V is a representation of G . The previous discussion shows that in order to compute the module of *covariants* with values in W , we need to compute the ring of *invariants* of $K[V \times W^*]/\mathfrak{m}_y^2$. This can be done by using Algorithm 4.2.8.

Let X be an affine G -variety with G linearly reductive. Let $B \subset G$ be a Borel subgroup with $B = T \ltimes U$ where T is a maximal torus and U is the maximal unipotent subgroup in B . The **ring of covariants** is defined as $K[X]^U$. The relation to modules of covariants is the following. Suppose that V_λ is an irreducible representation with highest weight λ (see Theorem A.5.1). Let $v_\lambda \in V_\lambda$ be the highest weight vector. A covariant $\varphi \in \text{Hom}(V_\lambda, K[X])^G$ is uniquely determined by $\varphi(v_\lambda) \in K[X]^U$ because the orbit $G \cdot v_\lambda$ spans the vector space V_λ .

The ring of covariants is finitely generated (see Khadzhiev [5] and Grosshans [6]). Let U act on G by multiplication on the right. The quotient G/U is a quasi-affine variety. We will study $K[G]^U = K[G/U]$. Let V_λ be an irreducible representation with λ a dominant weight (see Theorem A.5.1). From (4.2.7) with $X = G/U$ follows that

$$(K[G]^U \otimes V_\lambda)^G = \text{Mor}(G/U, V_\lambda)^G. \quad (4.2.8)$$

A G -equivariant morphism $\varphi : G/U \rightarrow V_\lambda$ is determined by $\varphi(eU) \in V_\lambda^U$, where $e \in G$ is the unit element. The space V_λ^U is 1-dimensional and spanned by a highest weight vector v_λ . It follows from (4.2.8) that the module of covariants $(K[G]^U \otimes V_\lambda)^G$ is 1-dimensional. In other words, every irreducible representation appears exactly once in $K[G]^U$. We can write

$$K[G]^U = K[G/U] = \bigoplus_{\lambda \in X(T)_+} V_\lambda,$$

where $X(T)_+$ is the set of dominant weights. The multiplicative structure of $K[G]^U$ can be understood as well. For dominant weights λ, μ , the λ -weightspace of V_λ and the μ -weightspace of V_μ are one dimensional. Now $V_\lambda \otimes V_\mu$ has maximal weight $\lambda + \mu$, and the $\lambda + \mu$ -weight space of $V_\lambda \otimes V_\mu$ is one-dimensional. This shows that $V_\lambda \otimes V_\mu$ contains a unique copy of $V_{\lambda+\mu}$. Now there exists a unique nonzero projection (up to scalar multiplication)

$$V_\lambda \otimes V_\mu \rightarrow V_{\lambda+\mu},$$

and this projection defines the multiplication in $K[G]^U$.

Example 4.2.11 If $G = \text{SL}_2$ and U is the set of all

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \quad a \in K.$$

The subgroup U is a maximal unipotent subgroup of SL_2 . The coordinate ring of SL_2 is $K[z_{1,1}, z_{1,2}, z_{2,1}, z_{2,2}] / (z_{1,1}z_{2,2} - z_{1,2}z_{2,1} - 1)$. We let U act on SL_2 by

right multiplication. It is easy to check that $K[\mathrm{SL}_2]^U = K[z_{1,1}, z_{1,2}]$ which is SL_2 -equivariantly isomorphic to $K[V_1]$ where V_1 is the space of binary forms of degree 1. Notice that $K[V_1] \cong \bigoplus_{d \geq 0} V_d$ as an SL_2 -representation, where V_d is the space of binary forms of degree d . \triangleleft

Let V be a rational representation of G . We consider $X_1 = G \times V$ and $X_2 = G \times V$ with an action of $G \times U$ on both X_1 and X_2 as follows

$$(\tau, \gamma) \cdot (\sigma, v) = (\tau\sigma\gamma^{-1}, \gamma v), \quad \tau \in G, \gamma \in U, (\sigma, v) \in X_1.$$

$$(\tau, \gamma) \cdot (\sigma, v) = (\tau\sigma\gamma^{-1}, \tau v), \quad \tau \in G, \gamma \in U, (\sigma, v) \in X_2.$$

The morphism $\psi : X_1 \rightarrow X_2$ defined by

$$(\sigma, v) \mapsto (\sigma, \sigma \cdot v)$$

defines a $G \times U$ -equivariant isomorphism between X_1 and X_2 .

Since $K[X_1]^{G \times U} = K[V]^U$ and $K[X_2]^{G \times U} = (K[G]^U \otimes K[V])^G$, we conclude

$$(K[G]^U \otimes K[V])^G \cong K[V]^U \tag{4.2.9}$$

(see also Popov and Vinberg [4, Lemma 3.10]). In fact, $K[G]^U$ can be graded in a natural way and using Algorithm 4.2.8 one can compute $K[V]^U$.

Example 4.2.12 Consider $G = \mathrm{SL}_2$ with maximal unipotent subgroup U (see Example 4.2.11). If V is any rational representation of SL_2 , then it follows from (4.2.9) that the ring of covariants is equal to

$$K[V_1 \oplus V]^{\mathrm{SL}_2} \cong (K[\mathrm{SL}_2]^U \otimes K[V])^{\mathrm{SL}_2} \cong K[V]^U.$$

\triangleleft

4.3 Invariants of Tori

In this section we introduce a new algorithm for computing invariants of tori. Although Algorithm 4.1.9 is efficient for most examples, the algorithm here is simpler and more efficient. Where Algorithm 4.1.9 (and equivalently Algorithm 1.4.5 of Sturmfels [2]) uses a Gröbner basis computation, the algorithm here relies only on divisibility tests of two monomials. The computation of torus invariants is equivalent to an integer programming problem (see Sturmfels [2, Section 1.4]) and has therefore a large scope of applications. For example, the computation of SAGBI bases involves the solution of a great number of integer programming problems (see Robbiano and Sweedler [7]).

Suppose that $T = (K^*)^r$ is a torus acting diagonally on an n -dimensional vector space V . We can identify $K[V] \cong K[x_1, \dots, x_n]$. If $\omega = (\omega^{(1)}, \dots, \omega^{(r)}) \in \mathbb{Z}^r$ is a weight, then we write t^ω instead of $t_1^{\omega^{(1)}} \cdots t_r^{\omega^{(r)}}$. For $i = 1, \dots, n$ let ω_i be the weight with which T acts on the variable x_i , i.e.,

$$t \cdot x_i = t^{\omega_i} x_i.$$

If $m = x_1^{a_1} x_2^{a_2} \cdots x_n^{a_n}$, then T acts on m with weight $a_1\omega_1 + \cdots + a_n\omega_n$. We also say that m has this weight. The idea of the algorithm is to choose a suitable finite set \mathcal{C} of weights, and then produce sets S_ω , $\omega \in \mathcal{C}$ of monomials of weight ω . These sets grow during the course of the algorithm, until upon termination we have that S_0 generates $K[V]^G$ (this will be guaranteed by the choice of \mathcal{C}). We now present the algorithm.

Algorithm 4.3.1 This algorithm computes a minimal set of generating invariants of a torus.

- (1) Input: Weights $\omega_1, \dots, \omega_n \in \mathbb{Z}^r$ defining an action of $T = (K^*)^r$ on $K[x_1, \dots, x_n]$.
- (2) If T is one-dimensional (i.e., $r = 1$), then let $\mathcal{C} \subset \mathbb{Z}^r$ be the set of integral points in the convex hull of $\omega_1, \dots, \omega_n$. If $r > 1$, then let $\mathcal{C} \subset \mathbb{Z}^r$ be the set of integral points in the convex hull of $2r\omega_1, \dots, 2r\omega_n, -2r\omega_1, \dots, -2r\omega_n$.
- (3) Define $S_\omega := \emptyset$ for all $\omega \in \mathcal{C}$. Then put $S_{\omega_i} := S_{\omega_i} \cup \{x_i\}$ for $i = 1, 2, \dots, n$. Finally put $U_\omega := S_\omega$ for all $\omega \in \mathcal{C}$.
- (4) If $U_\omega = \emptyset$ for all $\omega \in \mathcal{C}$ then terminate the algorithm with output S_0 . Otherwise, choose $\omega \in \mathcal{C}$ such that $U_\omega \neq \emptyset$ and choose $m \in U_\omega$.
- (5) For i from 1 to n perform steps (6)–(7).
- (6) Put $u := mx_i$ and let $v = \omega \cdot \omega_i$ be its weight.
- (7) If $v \in \mathcal{C}$ and u is not divisible by any element of S_v , then put $S_v := S_v \cup \{u\}$, $U_v := U_v \cup \{u\}$.
- (8) Set $U_\omega := U_\omega \setminus \{m\}$. Go to Step 4.

Proof of Algorithm 4.3.1 We first show that the algorithm terminates. Note that a monomial m lies in the ideal generated by S_ω if and only if m is divisible by one of the elements of S_ω . Ideals are finitely generated. This means that after a certain number of steps in the algorithm, the sets S_ω , $\omega \in \mathcal{C}$ will not increase anymore. If the sets S_ω do not increase, then the sets U_ω will not increase either. At each step in the loop the sum of the cardinalities of U_ω , $\omega \in \mathcal{C}$ decreases by 1. After a finite number of steps, $U_\omega = \emptyset$ for all $\omega \in \mathcal{C}$ and the algorithm terminates.

We now prove that after termination of the algorithm, S_0 is a generating set of invariants. Suppose that m is an invariant monomial of degree d and m is not divisible by a nonconstant invariant monomial of smaller degree. We will show that m lies in S_0 after termination of the algorithm. By Lemma 4.3.2 below we can write

$$m = x_{i_1} x_{i_2} \cdots x_{i_d}$$

with $i_1, \dots, i_d \in \{1, 2, \dots, n\}$ such that for every j , the weight v_j of

$$m_j := x_{i_1} x_{i_2} \cdots x_{i_j} \quad (4.3.1)$$

lies in \mathcal{C} . The monomial $m_1 = x_{i_1}$ lies in S_{v_1} right from the start. We will show that as the algorithm runs, m_2 is added to S_{v_2} , m_3 is added to S_{v_3} , etc., until finally $m = m_d$ is added to $S_{v_d} = S_0$. Suppose at a certain step, m_j is added to S_{v_j} . Then m_j is also added to U_{v_j} and after a few more steps $u = m_{j+1} = m_j x_{j+1}$ will be tested in Step 7. Suppose that m_{j+1} is divisible by another monomial of $S_{v_{j+1}}$, say $m_{j+1} = vw$ with $w \in S_{v_{j+1}}$ and v an invariant monomial. If v is constant then m_{j+1} was already added to $S_{v_{j+1}}$. Otherwise, m_{j+1} is divisible by the nonconstant invariant monomial v and therefore m is divisible by v which is in contradiction with our assumptions on m . If m_{j+1} is not divisible by any monomial of $S_{v_{j+1}}$ then m_{j+1} is added to $S_{v_{j+1}}$. In this way we see that after the algorithm terminates, we have $m_j \in S_{v_j}$ for $j = 1, 2, \dots, d$. In particular $m = m_d \in S_{v_d} = S_0$. This shows that S_0 is a set of generators of $K[V]^T$. In fact, since every monomial in S_0 is not divisible by any other monomial in S_0 , S_0 consists of a *minimal* set of generators of $K[V]^T$. \square

Lemma 4.3.2 *Suppose that $\omega_1, \dots, \omega_d \in \mathbb{R}^r$ such that $\sum_{i=1}^d \omega_i = 0$. If $r = 1$, let \mathcal{C} be the convex hull of $\omega_1, \dots, \omega_d$. If $r > 1$, let \mathcal{C} be the convex hull of*

$$2r\omega_1, \dots, 2r\omega_d, -2r\omega_1, \dots, -2r\omega_d.$$

Then there exists a permutation σ of $\{1, \dots, d\}$, such that for every $j \leq d$ we have

$$\omega_{\sigma(1)} + \cdots + \omega_{\sigma(j)} \in \mathcal{C}.$$

Proof We first do the case $r = 1$. We can take $\sigma(1) = 1$. For $i > 1$ we can define $\sigma(i)$ as follows. If $\omega_1 + \cdots + \omega_{i-1} \geq 0$ then we can choose $\sigma(i) \in \{1, 2, \dots, d\} \setminus \{\sigma(1), \dots, \sigma(i-1)\}$ such that $\omega_{\sigma(i)} \leq 0$. If $\omega_1 + \cdots + \omega_{i-1} < 0$, then we can choose $\sigma(i) \in \{1, \dots, d\} \setminus \{\sigma(1), \dots, \sigma(i-1)\}$ such that $\omega_{\sigma(i)} > 0$. It is now clear that

$$\omega_{\sigma(1)} + \cdots + \omega_{\sigma(j)} \in \mathcal{C}$$

for all j .

Let us now treat the case $r > 1$. We can define a norm $\|\cdot\|$ on \mathbb{R}^r by

$$\|\omega\| = \inf\{|\lambda|^{-1} \mid 0 \neq \lambda \in \mathbb{R},$$

$\lambda\omega$ lies in the convex hull of $\omega_1, \dots, \omega_n, -\omega_1, \dots, -\omega_n\}$.

Then we have $\|\omega_i\| \leq 1$ for all i . Moreover, $\|\omega\| \leq 2r$ if and only if $\omega \in \mathcal{C}$. A theorem of Bárány and Grinberg (see Beck and Sós [8, Corollary 4.9]) tells us that $\|\omega_i\| \leq 1$ and $\sum_{i=1}^n \omega_i = 0$ imply the existence of a permutation σ such that

$$\|\omega_{\sigma(1)} + \cdots + \omega_{\sigma(j)}\| \leq 2r$$

for all j . So we have

$$\omega_{\sigma(1)} + \cdots + \omega_{\sigma(j)} \in \mathcal{C}$$

for all j . \square

Remark 4.3.3 Note that in the norm $\|\cdot\|$ in the above proof is constructed in such a way that $\|\omega_i\| \leq 1$ and the set $\{\omega \in \mathbb{R}^r \mid \|\omega\| \leq 2r\}$ is as small as possible. This means that the set \mathcal{C} in Algorithm 4.3.1 is the smallest possible set that allows the application of the theorem of Bárány and Grinberg for the proof of correctness. \triangleleft

Example 4.3.4 Suppose that a one-dimensional torus $T = \mathbb{G}_m$ acts diagonally on a 4-dimensional vector space V . Then $K[V] \cong K[x_1, x_2, x_3, x_4]$. Suppose that the weights of the monomial x_1, x_2, x_3, x_4 are $-3, -1, 1, 2$ respectively. Then $\mathcal{C} = \{-3, -2, -1, 0, 1, 2\}$. The course of the algorithm can be summarized in the following table.

	S_{-3}	S_{-2}	S_{-1}	S_0	S_1	S_2
1	x_1		x_2		x_3	x_4
2		x_1x_3 x_2^2	x_1x_4	x_2x_3	x_2x_4	x_3^2
3	x_2^3	$x_1x_2x_4$	$x_1x_3^2$	$x_2^2x_4$ $x_1x_3x_4$	$x_1x_4^2$	
4		$x_1^2x_4^2$		$x_1x_2x_4^2$ $x_1x_3^3$		
5				$x_1^2x_4^3$		

At the start, we take $S_{-3} = \{x_1\}$, $S_{-2} = \{x_2\}$, $S_1 = \{x_3\}$, $S_2 = \{x_4\}$. Then we look at monomials of degree 2, i.e., we multiply elements of the S_i 's with x_1, x_2, x_3 and x_4 . Monomials like $x_1^2, x_1x_2, x_2^2, x_4^2, x_3x_4$ have weights which do not lie in \mathcal{C} . The other monomials $x_1x_3, x_1x_4, x_2^2, x_2x_3, x_2x_4, x_3^2$ are added to the appropriate S_i 's and U_i 's. If we take now for example $x_2^2 \in U_{-2}$ and multiply it with x_3 , then $x_3x_2^2$ is divisible by $x_2 \in S_{-1}$. Therefore $x_3x_2^2$ will not be added to S_{-1} . The algorithm continues in this way and after termination we get $S_0 = \{x_2x_3, x_2^2x_4, x_1x_3x_4, x_1x_2x_4^2, x_1x_2^2, x_1^2x_2^3\}$. We conclude

$$K[x_1, x_2, x_3, x_4]^T = K[x_2x_3, x_2^2x_4, x_1x_3x_4, x_1x_2x_4^2, x_1x_2^2, x_1^2x_2^3].$$

Remark 4.3.5 The algorithm can also be used for invariants of any finite abelian linearly reductive groups G . One may again assume that G acts diagonally. For \mathcal{C} one has to take the set of *all* irreducible characters of G .

4.4 Invariants of SL_n and GL_n

In this section we briefly discuss some classical results on the invariant theory of SL_n and GL_n . The theorems of this section can all be found in §9.3 and §9.4 of Popov and Vinberg [4]. Our base field K is assumed to be of characteristic 0. Suppose that V is an n -dimensional vector space. Let V^* be the dual space of V and let $\langle \cdot, \cdot \rangle : V \times V^* \rightarrow K$ be the canonical pairing. We will study invariants of the representation $V^r \oplus (V^*)^s$. For each $i \leq r$ and each $j \leq s$ we have an invariant

$$V^r \oplus (V^*)^s \ni (v_1, \dots, v_r, w_1, \dots, w_s) \mapsto \langle v_i, w_j \rangle,$$

which we symbolically denote by $\langle i, j \rangle$.

Theorem 4.4.1 (First Fundamental Theorem for GL_n) *The invariant ring*

$$K[V^r \oplus (V^*)^s]^{\mathrm{GL}_n}$$

is generated by all $\langle i, j \rangle$.

Remark 4.4.2 Suppose that W and Z are finite dimensional vector spaces. Let

$$\pi : \mathrm{Hom}(W, V) \times \mathrm{Hom}(V, Z) \rightarrow \mathrm{Hom}(W, Z)$$

be the composition map. Let $Y \subset \mathrm{Hom}(W, Z)$ be the image of π . It is easy to see that Y is the set of all $A \in \mathrm{Hom}(W, Z)$ of rank at most $\min(n, \dim(W), \dim(Z))$ with $n = \dim(V)$ (in particular, Y is Zariski-closed). Note that $\mathrm{Hom}(W, V)$ is isomorphic to V^r and $\mathrm{Hom}(V, Z)$ is isomorphic to $(V^*)^s$ as representations of $\mathrm{GL}(V)$, where $r := \dim(W)$ and $s := \dim(Z)$. Now Theorem 4.4.1 shows that $\pi : \mathrm{Hom}(W, V) \times \mathrm{Hom}(V, Z) \rightarrow Y$ is the categorical quotient with respect to the action of $\mathrm{GL}(V)$. \triangleleft

In the previous remark, the ideal $I(Y) \subset K[\mathrm{Hom}(W, Z)]$ of Y is generated by all $(n+1) \times (n+1)$ minors. In the notation of Theorem 4.4.1 this means that we have the following description of the relations between the generating invariants (see also Popov and Vinberg [4, §9.4]).

Theorem 4.4.3 (Second Fundamental Theorem for GL_n) *All polynomial relations between the invariants $\langle i, j \rangle$ are generated by*

$$\det \begin{pmatrix} \langle i_1, j_1 \rangle & \langle i_1, j_2 \rangle & \cdots & \langle i_1, j_{n+1} \rangle \\ \langle i_2, j_1 \rangle & \langle i_2, j_2 \rangle & & \langle i_2, j_{n+1} \rangle \\ \vdots & & \ddots & \vdots \\ \langle i_{n+1}, j_1 \rangle & \langle i_{n+1}, j_2 \rangle & \cdots & \langle i_{n+1}, j_{n+1} \rangle \end{pmatrix}$$

with $1 \leq i_1 < i_2 < \cdots < i_{n+1} \leq r$ and $1 \leq j_1 < j_2 < \cdots < j_{n+1} \leq s$.

Let us describe invariants for $\mathrm{SL}(V)$. Besides the $\mathrm{GL}(V)$ invariants which we already found, we also have invariant determinants. If $1 \leq i_1 < i_2 < \dots < i_n \leq r$, we have a **bracket invariant**

$$V^r \oplus (V^*)^s \ni (v_1, \dots, v_r, w_1, \dots, w_s) \mapsto \det(v_{i_1} v_{i_2} \cdots v_{i_n}),$$

which will be denoted by $[i_1 i_2 \cdots i_n]$. Similarly for $1 \leq j_1 < j_2 < \dots < j_n \leq s$ we have an invariant

$$V^r \oplus (V^*)^s \ni (v_1, \dots, v_r, w_1, \dots, w_s) \mapsto \det(w_{j_1} w_{j_2} \cdots w_{j_n}),$$

which will be denoted by $|j_1 j_2 \dots j_n|$.

Theorem 4.4.4 (First Fundamental Theorem for SL_n) *The invariant ring*

$$K[V^r \oplus (V^*)^s]^{\mathrm{SL}_n}$$

is generated by all $\langle i, j \rangle$ ($1 \leq i \leq r, 1 \leq j \leq s$), all $[i_1 i_2 \cdots i_n]$ ($1 \leq i_1 < i_2 < \dots < i_n \leq r$) and all $|j_1 j_2 \cdots j_n|$ ($1 \leq j_1 < j_2 < \dots < j_n \leq s$).

For a description of the relations between all these invariants, see for example Popov and Vinberg [4, §9.4]. Let us just explain the case where $s = 0$. In that case the invariant ring $K[V^r]^{\mathrm{SL}_n}$ is generated by all $[i_1 i_2 \cdots i_n]$ with $1 \leq i_1 < i_2 < \dots < i_n \leq r$.

Theorem 4.4.5 (Second Fundamental Theorem for SL_n) *All relations between the generating invariants in $K[V^r]^{\mathrm{SL}_n}$ are generated by*

$$\sum_{k=1}^{n+1} (-1)^{k-1} [i_1 i_2 \cdots i_{n-1} j_k] [j_1 j_2 \cdots \widehat{j_k} \cdots j_{n+1}]$$

with $1 \leq i_1 < i_2 < \dots < i_{n-1} \leq r$ and $1 \leq j_1 < j_2 < \dots < j_{n+1} \leq r$.

The generating relations in Theorem 4.4.5 are called **Grassmann-Plücker relations**. Similar descriptions for generating invariants and their relations exist for other classical groups as well (see Popov and Vinberg [4, §9.4]).

Example 4.4.6 If V is 2-dimensional, then $K[V^4]^{\mathrm{SL}_2}$ is generated by $[1\ 2]$, $[1\ 3]$, $[1\ 4]$, $[2\ 3]$, $[2\ 4]$ and $[3\ 4]$. There is one Plücker relation, namely

$$[1\ 2][3\ 4] - [1\ 3][2\ 4] + [1\ 4][2\ 3].$$

□

We refer to Sturmfels [2, Chap. 3] for more details. The invariant ring $K[V^r]^{\mathrm{SL}_n}$ is generated by all brackets, and sometimes it is called the bracket ring. To present the invariant ring $K[V^r]^{\mathrm{SL}_n}$, one can start with the polynomial ring on all brackets, and

then divide out the ideal $I_{r,n}$ of all relations as in Theorem 4.4.5. In Sturmfels [2, Chap. 3] more general generators of $I_{r,n}$ are described. In fact, a Gröbner basis of $I_{r,n}$ is given. The so-called straightening algorithm of Young can be related to finding the normal form with respect to this Gröbner basis (see Sturmfels [2], Sturmfels and White [9], Young [10] and Hodge and Pedoe [11]).

4.4.1 Binary Forms

Let us now study the invariants for SL_2 . The base field K will be algebraically closed and of characteristic 0. We will give an introduction to the so called symbolic method. Denote the space of binary forms of degree d by V_d , so

$$V_d = \{a_0x^d + a_1x^{d-1}y + \cdots + a_dy^d \mid a_0, \dots, a_d \in K\}.$$

The action of SL_2 on V_d is given by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot p(x, y) = p(ax + cy, bx + dy)$$

for every $p(x, y) \in V_d$. The coordinate ring $K[V_d]$ can be identified with $K[a_0, \dots, a_d]$. Let us put $V = V_1$. Notice that we have a surjective map $\pi : V^d \rightarrow V_d = S^d(V)$ defined by

$$(f_1, f_2, \dots, f_d) \mapsto f_1 f_2 \cdots f_d.$$

Let $T = \mathbb{G}_m^{d-1}$, the $(d-1)$ -dimensional torus. We can define an action of T on V^d by

$$(\sigma_1, \sigma_2, \dots, \sigma_{d-1}) \cdot (f_1, \dots, f_d) = (\sigma_1 f_1, \sigma_1^{-1} \sigma_2 f_2, \dots, \sigma_{d-2}^{-1} \sigma_{d-1} f_{d-1}, \sigma_{d-1}^{-1} f_d).$$

The symmetric group S_d also acts on V^d by permuting the factors. Combining the two actions gives an action of the semidirect product $S_d \ltimes T$ on V^d . For a nonzero $f \in V_d$, the fiber $\pi^{-1}(f)$ is exactly the set of all possible factorizations of f into d linear forms, so the fiber $\pi^{-1}(f)$ is exactly one $S_d \ltimes T$ -orbit. It follows that the dual homomorphism $\pi^* : K[V_d] \hookrightarrow K[V^d]$ induces an isomorphism $K[V_d] \cong K[V^d]^{S_d \ltimes T}$. Moreover, we have

$$K[V_d]^{\mathrm{SL}_2} \cong (K[V^d]^{S_d \ltimes T})^{\mathrm{SL}_2} = (K[V^d]^{S_d \ltimes T})^{S_d} = ((K[V^d]^{\mathrm{SL}_2})^T)^{S_d}.$$

This is very nice because we have a good description of $K[V^d]^{\mathrm{SL}_2}$: it is generated by all brackets $[i \ j]$ with $1 \leq i < j \leq d$ and the relations are all Plücker relations

$$[i \ j][k \ l] - [i \ k][j \ l] + [i \ l][j \ k]$$

with $i < j < k < l$ by Theorems 4.4.4 and 4.4.5. We would like to find all $S_d \times T$ -invariant bracket-polynomials. Let us first describe the T -invariant bracket polynomials. Every bracket monomial is a semi-invariant for T . It is easy to see that a bracket monomial is invariant if and only if every integer between 1 and d appears the same number of times. We will call such a monomial *regular*. A bracket polynomial is called regular if all of its monomials are regular.

Example 4.4.7 For $d = 3$ we have that

$$[1\ 2][1\ 3][2\ 3]$$

is T -invariant, because 1, 2 and 3 all appear twice. \triangleleft

From the previous considerations it follows that $K[V^d]^{SL_2 \times T}$ is the set of all regular bracket polynomials. Notice that if $i > j$, we can also define $[i\ j]$ by $[i\ j] = -[j\ i]$. The action of S_d on $K[V^d]^{SL_2}$ is given by $\sigma \cdot [i\ j] = [\sigma(i)\ \sigma(j)]$. We call a bracket polynomial symmetric if it is invariant under S_d . The invariant ring $K[V_d]^{SL_2}$ can be identified with all *symmetric* regular bracket polynomials.

Example 4.4.8 For $d = 3$ the bracket monomial

$$[1\ 2][1\ 3][2\ 3]$$

is *not* symmetric, because if we interchange 1 and 2, we get

$$[2\ 1][2\ 3][1\ 3] = -[1\ 2][1\ 3][2\ 3].$$

However,

$$([1\ 2][1\ 3][2\ 3])^2$$

is symmetric and regular. This polynomial corresponds to the discriminant in $K[V_3]^{SL_2}$. In fact, for any d we have a symmetric bracket monomial

$$([1\ 2][1\ 3] \cdots [1\ d][2\ 3][2\ 4] \cdots [2\ d] \cdots [d-1\ d])^2,$$

which corresponds to the discriminant in $K[V_d]^{SL_2}$. \triangleleft

To obtain invariants for the binary forms of degree d , one can just take a regular bracket monomial and symmetrize it over the symmetric group S_d . However, the invariant obtained in this way can be zero.

Example 4.4.9 For $d = 4$, we can take $[1\ 2]^2[3\ 4]^2$ and symmetrize it to

$$[1\ 2]^2[3\ 4]^2 + [1\ 3]^2[2\ 4]^2 + [1\ 4]^2[2\ 3]^2,$$

which is a nonzero invariant. Another invariant can be obtained by symmetrizing $[1\ 2]^2[3\ 4]^2[1\ 3][2\ 4]$. Both invariants together generate $K[V_4]^{\mathrm{SL}_2}$. \triangleleft

The method explained above generalizes to simultaneous invariants of several binary forms. The ring of covariants on binary forms of degree d is isomorphic to $K[V_d \oplus V]^{\mathrm{SL}_2}$. We have

$$K[V_d \oplus V]^{\mathrm{SL}_2} \cong (K[V^d \oplus V]^{\mathrm{SL}_2})^{S_d \ltimes T}.$$

To describe covariants, we add another symbol, say \mathbf{u} , to our alphabet $\{1, 2, \dots, d\}$ corresponding to the extra copy of V . Covariants are now polynomials in the brackets $[i\ j]$, $1 \leq i < j \leq d$ and the brackets $[i\ \mathbf{u}]$ with $1 \leq i \leq r$. Again, a bracket monomial is called regular if every integer between 1 and d appears the same number of times, and a bracket polynomial is called regular if all its bracket monomials are regular. The set of covariants are exactly all symmetric regular bracket polynomials.

Example 4.4.10 The **Hessian** of a binary form f of degree d is defined by

$$H(f) := \frac{\partial^2 f}{(\partial x)^2} \frac{\partial^2 f}{(\partial y)^2} - \left(\frac{\partial^2 f}{\partial x \partial y} \right)^2.$$

The corresponding bracket polynomial is the symmetrization of

$$([1\ 2][3\ \mathbf{u}][4\ \mathbf{u}] \cdots [d\ \mathbf{u}])^2.$$

\triangleleft

4.5 The Reynolds Operator

In this section we will study the Reynolds operator, which is required in Algorithm 4.1.9. But first we will present a variant of step 5 of the algorithm that does not use the Reynolds operator. Observe that the set \mathcal{B} computed in the algorithm is automatically homogeneous, and therefore also \mathcal{I} is homogeneous. The Reynolds operator preserves degree. So instead of applying the Reynolds operator to the elements $f \in \mathcal{I}$, we can compute a basis of the space $K[V]_d^G$ of homogeneous invariants of degree $d = \deg(f)$ for every $f \in \mathcal{I}$. Then the union of these bases generates $K[V]^G$. The following algorithm computes a basis of $K[V]_d^G$. The algorithm works for all linear algebraic groups, not just linearly reductive ones.

Algorithm 4.5.1 (Spaces of homogeneous invariants) Let G be a linear algebraic group acting rationally on a vector space V . Assume that G and the action are given as in Algorithm 4.1.9. To compute a basis of the space $K[V]_d^G$ of homogeneous invariants of a given degree d , perform the following steps.

- (1) Compute a Gröbner basis \mathcal{G} of $I(G)$ with respect to an arbitrarily chosen monomial ordering.
- (2) Let $\{h_1, \dots, h_r\} \subset K[V]$ be the set of monomials of degree d .
- (3) Compute a basis C of the vector space of all $(\alpha_1, \dots, \alpha_r) \in K^r$ with

$$\sum_{i=1}^r \alpha_i \text{NF}_{\mathcal{G}} \left(h_i \left(\sum_{j=1}^n a_{j,1}x_j, \dots, \sum_{j=1}^n a_{j,n}x_j \right) - h_i \right) = 0.$$

- (4) Now

$$B := \left\{ \sum_{i=1}^r \alpha_i h_i \mid (\alpha_1, \dots, \alpha_r) \in C \right\}$$

is a basis of $K[V]_d^G$.

The correctness of the algorithm follows from the linearity of the normal form map and the fact that for $f \in K[V]$ one has $f \in K[V]^G$ if and only if

$$f \left(\sum_{j=1}^n a_{j,1}x_j, \dots, \sum_{j=1}^n a_{j,n}x_j \right) - f \in I(G) \cdot K[x_1, \dots, x_n, z_1, \dots, z].$$

Since Algorithm 4.5.1 requires the (pre-)computation of a much smaller Gröbner basis than the one required in Algorithm 4.1.9 and in addition only polynomial arithmetic and linear algebra, the cost of applying it will be dwarfed by the cost of step 2 in Algorithm 4.1.9.

After this prelude we turn to the Reynolds operator.

Example 4.5.2 For finite groups G we have seen that the Reynolds operator $\mathcal{R} : K[X] \rightarrow K[X]^G$ is just averaging over the group (see Example 2.2.3 and Sect. 3.1.2).

$$\mathcal{R}(f) = \frac{1}{|G|} \sum_{\sigma \in G} \sigma \cdot f.$$

□

Example 4.5.3 Suppose that $G = T$ is a torus. If $\dim T = 1$ the Reynolds operator was studied in Example 2.2.4. This easily generalizes to an r -dimensional torus T . Let X be an affine T -variety. The coordinate ring $K[T]$ can be identified with the ring of Laurent polynomials in r variables $K[z_1, \dots, z_r, z_1^{-1}, \dots, z_r^{-1}]$. The action $\mu : T \times X \rightarrow X$ corresponds to a ring homomorphism $\mu^* : K[X] \rightarrow K[T] \otimes K[X]$. If $f \in K[X]$, then $\mu^*(f)$ is a Laurent polynomial in z_1, \dots, z_r with coefficients in $K[X]$. Now $\mathcal{R}(f)$ is the coefficient of $z_1^{e_1} z_2^{e_2} \cdots z_r^{e_r}$ in $\mu^*(f)$. □

Suppose that G is an arbitrary linearly reductive group. Let G° be the connected component of the identity and let $[G^\circ, G^\circ]$ be the commutator subgroup of G° . Then G/G° is a finite group, $G^\circ/[G^\circ, G^\circ]$ is a torus and $[G^\circ, G^\circ]$ is semi-simple. Because of the following lemma, computing the Reynolds operator for G can be reduced to computing the Reynolds operator for the connected semi-simple group $[G^\circ, G^\circ]$.

Lemma 4.5.4 *Suppose that G has a normal subgroup N and that X is an affine G -variety. Let $\mathcal{R}_G : K[X] \rightarrow K[X]^G$ be the Reynolds operator with respect to G , $\mathcal{R}_N : K[X] \rightarrow K[X]^N$ the Reynolds operator with respect to N and $\mathcal{R}_{G/N} : K[X]^N \rightarrow K[X]^G$ be the Reynolds operator with respect to G/N . Then we have $\mathcal{R}_G = \mathcal{R}_{G/N}\mathcal{R}_N$.*

Proof This is clear from the definition of the Reynolds operator (Definition 2.2.2). \square

4.5.1 The Dual Space $K[G]^*$

Let $K[G]^*$ be the dual space to $K[G]$. It is very natural to study $K[G]^*$ because it contains all important operators, such as the Reynolds operator and the Casimir operator. We will give a brief overview of the main properties of $K[G]^*$ in this section. For details and proofs, see Appendix A.2. First of all, to every $\sigma \in G$ we can associate a linear map $\epsilon_\sigma : K[G] \rightarrow K$ defined by

$$f \mapsto f(\sigma).$$

An important object we need is the **Lie algebra** \mathfrak{g} of G . We define the Lie algebra as the set of all point derivations at the identity element $e \in G$ (see Definition A.2.4). In particular \mathfrak{g} is contained in $K[G]^*$.

The space $K[G]^*$ has the structure of an associative algebra. Let $m : G \times G \rightarrow G$ be the multiplication map and let $m^* : K[G] \rightarrow K[G] \otimes K[G]$ be the dual homomorphism. For every $\delta, \gamma \in K[G]^*$, the **convolution** $\delta * \gamma$ is defined as the composition

$$(\delta \otimes \gamma) \circ m^* : K[G] \rightarrow K[G] \otimes K[G] \rightarrow K.$$

One can show that $*$ defines an associative K -bilinear multiplication (see Proposition A.2.2). The unit element of $K[G]^*$ is $\epsilon := \epsilon_e$ where $e \in G$ is the identity.

Remark 4.5.5 For any $\delta, \gamma \in \mathfrak{g}$, we have

$$[\delta, \gamma] = \delta * \gamma - \gamma * \delta \in \mathfrak{g},$$

and this defines the Lie algebra structure on \mathfrak{g} (see Proposition A.2.5).

Example 4.5.6 Let $G = \mathrm{GL}_n$ and write \mathfrak{gl}_n for its Lie algebra. For every $n \times n$ matrix A we can define $\partial_A \in \mathfrak{gl}_n$, the derivative in direction A at the identity matrix I by

$$\partial_A f := \left. \frac{d}{dt} f(I + tA) \right|_{t=0}$$

for all $f \in K[\mathrm{GL}_n]$. Let $z_{i,j}$, $1 \leq i, j \leq n$, be the coordinate functions and let Z be the matrix $(z_{i,j})_{i,j=1,\dots,n}$. We write $\partial_A Z$ for the matrix $(\partial_A(z_{i,j}))_{i,j=1,\dots,n}$. We have

$$\partial_A Z = \left. \frac{d}{dt} I + tA \right|_{t=0} = A.$$

By definition

$$(\partial_A * \partial_B)f = \left. \frac{d}{dt} \frac{d}{ds} f((I + tA)(I + sB)) \right|_{t=s=0}$$

and

$$[\partial_A, \partial_B]f = \left. \frac{d}{dt} \frac{d}{ds} (f((I + tA)(I + sB)) - f((I + sB)(I + tA))) \right|_{t=s=0}.$$

Applying this to Z yields

$$\begin{aligned} [\partial_A, \partial_B]Z &= \left. \frac{d}{dt} \frac{d}{ds} ((I + tA)(I + sB) - (I + sB)(I + tA)) \right|_{t=s=0} = \\ &AB - BA = [A, B] = \partial_{[A,B]}Z. \end{aligned}$$

This shows that $\partial_{[A,B]} = [\partial_A, \partial_B]$. So the Lie algebra \mathfrak{gl}_n is canonically isomorphic to the Lie algebra $\mathrm{Mat}_{n,n}(K)$. A basis of \mathfrak{gl}_n is given by all $\partial_{i,j}$ with $1 \leq i, j \leq n$ where $\partial_{i,j}$ is defined by $\partial_{i,j} = \partial_{E_{i,j}}$ and $E_{i,j}$ is the matrix with a 1 at entry (i, j) and 0's everywhere else. \triangleleft

Remark 4.5.7 Suppose that $H \subset G$ is a Zariski closed subgroup of G . The Lie algebras of G and H are \mathfrak{g} and \mathfrak{h} respectively. Let I be the kernel of the surjective ring homomorphism $K[G] \rightarrow K[H]$. Clearly every point derivation of H at e can be seen as a point derivation on G . On the other hand, $\delta \in \mathfrak{g}$ is a point derivation on H if and only if $\delta(I) = \{0\}$. If I is generated by $f_1, \dots, f_r \in K[G]$, then this is equivalent to $\delta(f_1) = \delta(f_2) = \dots = \delta(f_r) = 0$. \triangleleft

Example 4.5.8 The subgroup $\mathrm{SL}_n \subset \mathrm{GL}_n$ is determined by $\det(Z) = 1$. We can view the Lie algebra \mathfrak{sl}_n as a subalgebra of \mathfrak{gl}_n . Let $\partial_A \in \mathfrak{gl}_n$. By Remark 4.5.7,

$\partial_A \in \mathfrak{sl}_n$ if and only if

$$\begin{aligned} 0 = \partial_A(\det(Z) - 1) &= \frac{d}{dt} \det(I + tA) \Big|_{t=0} = \\ &\quad \frac{d}{dt}(1 + t \operatorname{Tr}(A) + \dots) \Big|_{t=0} = \operatorname{Tr}(A), \end{aligned}$$

where $\operatorname{Tr}(A)$ is the trace of A . Thus \mathfrak{sl}_n is the set of all $\partial_A \in \mathfrak{gl}_n$ with $\operatorname{Tr}(A) = 0$. A basis of \mathfrak{sl}_n is given by all $\partial_{i,j}$ with $i \neq j$ and $\partial_{i,i} - \partial_{i+1,i+1}$ for $i = 1, \dots, n-1$. \triangleleft

Example 4.5.9 Let $G = O_n$ be the orthogonal group and let \mathfrak{o}_n be its Lie algebra. The group $O_n \subset \operatorname{GL}_n$ is determined by the relation $'ZZ = I$ where $'Z$ is the transposed matrix of Z . We can view \mathfrak{o}_n as a subspace of \mathfrak{gl}_n . We have

$$\partial_A('ZZ - I) = \frac{d}{dt}(I + 'At)(I + At) \Big|_{t=0} = A + 'A.$$

From Remark 4.5.7 it follows that $\mathfrak{o}_n \subset \mathfrak{gl}_n$ is the set of all ∂_A with $A + 'A = 0$. A basis of \mathfrak{o}_n is given by all $\partial_{i,j} - \partial_{j,i}$ with $1 \leq i < j \leq n$. \triangleleft

Suppose that X is an affine G -variety. G acts rationally on $K[X]$, so this action extends to an action of $K[G]^*$ on $K[X]$. In particular, we have $\epsilon_\sigma \cdot f = \sigma \cdot f$ for all $\sigma \in G$ and $f \in K[X]$. If $\delta \in \mathfrak{g}$, then δ acts on $K[X]$ as a derivation.

Proposition 4.5.10 *Let $\mathcal{R}_G : K[G] \rightarrow K$ be the Reynolds operator. If X is an affine G -variety, then the Reynolds operator $\mathcal{R}_X : K[X] \rightarrow K[X]^G$ is given by $f \mapsto \mathcal{R}_G \cdot f$.*

Proof We define $\mathcal{R}_X : K[X] \rightarrow K[X]^G$ by $f \mapsto \mathcal{R}_G \cdot f$ and prove that it satisfies the properties of a Reynolds operator as in Definition 2.2.2. Let $\mu^* : K[X] \rightarrow K[X] \otimes K[G]$ be as in Example A.2.12. (a) If $f \in K[X]^G$, then $\mu^*(f) = f \otimes 1$ and $\mathcal{R}_X(f) = f\mathcal{R}_G(1) = f$. (b) Since $\mathcal{R}_G : K[G] \rightarrow K$ is the Reynolds operator, we have $\mathcal{R}_G(\sigma \cdot g) = \mathcal{R}_G(g)$ for all $\sigma \in G$ and all $g \in K[G]$. In other words, $\mathcal{R}_G * \epsilon_\sigma = \mathcal{R}_G$. This shows that

$$\mathcal{R}_G \cdot (\sigma \cdot f) = \mathcal{R}_G \cdot (\epsilon_\sigma \cdot f) = (\mathcal{R}_G * \epsilon_\sigma) \cdot f = \mathcal{R}_G \cdot f.$$

□

4.5.2 The Reynolds Operator for Semi-simple Groups

Suppose that G is connected and semi-simple with Lie algebra \mathfrak{g} , i.e., $[\mathfrak{g}, \mathfrak{g}] = \mathfrak{g}$. For $\delta \in \mathfrak{g}$, we define $\operatorname{ad}(\delta) : \mathfrak{g} \rightarrow \mathfrak{g}$ by $\gamma \mapsto [\delta, \gamma]$. The **Killing form** is a symmetric bilinear form $\kappa : \mathfrak{g} \times \mathfrak{g} \rightarrow K$ defined by

$$\kappa(\delta, \gamma) = \operatorname{Tr}(\operatorname{ad}(\delta) \operatorname{ad}(\gamma)),$$

where Tr is the trace. Because \mathfrak{g} is semi-simple, it follows from Humphreys [12, 5.1] that the Killing form is nondegenerate.

Definition 4.5.11 Let $\delta_1, \dots, \delta_m$ be a basis of \mathfrak{g} and let $\gamma_1, \dots, \gamma_m$ be the dual basis of \mathfrak{g} with respect to the bilinear form κ . The **Casimir operator** c is defined by

$$c = \sum_{i=1}^m \delta_i * \gamma_i \in K[G]^*.$$

The Casimir operator does not depend on the choice of the basis $\delta_1, \dots, \delta_m$. In fact, one can define the Casimir operator basis-independently as follows. The Killing form defines an element $\kappa \in S^2(\mathfrak{g})$. Because κ gives an isomorphism between \mathfrak{g} and \mathfrak{g}^* , it also induces an isomorphism between $S^2(\mathfrak{g})$ and $S^2(\mathfrak{g}^*)$. So κ determines an element in $S^2(\mathfrak{g})$ which is the Casimir operator. Here $S^2(\mathfrak{g})$ is identified with the subspace of $K[G]^*$ spanned by all $\delta * \gamma + \gamma * \delta$ with $\delta, \gamma \in \mathfrak{g}$.

Lemma 4.5.12 *If $\sigma \in G$, then $\epsilon_\sigma * c = c * \epsilon_\sigma$. This means that for every rational representation V we have*

$$\sigma \cdot (c \cdot v) = c \cdot (\sigma \cdot v), \quad v \in V.$$

Proof Let $\delta_1, \dots, \delta_m$ be a basis of \mathfrak{g} . If $\gamma \in \mathfrak{g}$, then the matrix of $\text{ad}(\text{Ad}(\sigma)\gamma)$ with respect to the basis $\text{Ad}(\sigma)\delta_1, \dots, \text{Ad}(\sigma)\delta_m$ is the same as the matrix of $\text{ad}(\gamma)$ with respect to $\delta_1, \dots, \delta_m$. This shows that $\kappa(\text{Ad}(\sigma)\gamma, \text{Ad}(\sigma)\varphi) = \kappa(\gamma, \varphi)$ for all $\gamma, \varphi \in \mathfrak{g}$. Let $\gamma_1, \dots, \gamma_m$ be the dual basis to $\delta_1, \dots, \delta_m$. Then $\text{Ad}(\sigma)\gamma_1, \dots, \text{Ad}(\sigma)\gamma_m$ is the dual basis of $\text{Ad}(\sigma)\delta_1, \dots, \text{Ad}(\sigma)\delta_m$ and

$$c = \sum_{i=1}^m (\text{Ad}(\sigma)\delta_i) * (\text{Ad}(\sigma)\gamma_i) = \text{Ad}(\sigma) \left(\sum_{i=1}^m \delta_i * \gamma_i \right) = \text{Ad}(\sigma)c.$$

□

Remark 4.5.13 As remarked in the proof, the Killing form κ is invariant under the group action of G . Since κ is nondegenerate, it defines an isomorphism between \mathfrak{g} and \mathfrak{g}^* , the dual space. If (\cdot, \cdot) is any other G -invariant bilinear form on \mathfrak{g} , then this determines a linear map $\mathfrak{g} \rightarrow \mathfrak{g}^* \cong \mathfrak{g}$ which commutes with the action of G . By Schur's Lemma, this must be a multiple of the identity. Consequently, (\cdot, \cdot) is a scalar multiple of κ . □

Example 4.5.14 Let $G = \text{SL}_n$ with Lie algebra \mathfrak{sl}_n . We can define a G -invariant bilinear form (\cdot, \cdot) on \mathfrak{sl}_n by

$$(\partial_A, \partial_B) = \text{Tr}(AB),$$

where Tr is the trace. By Remark 4.5.13 this must be a multiple of the Killing Form. It is not hard to check that $\kappa(\partial_{1,2}, \partial_{2,1}) = 2n$ and $(\partial_{1,2}, \partial_{2,1}) = 1$ so we conclude

that

$$\kappa(\cdot, \cdot) = 2n(\cdot, \cdot).$$

A basis of \mathfrak{sl}_n is given by $\partial_{i,j}$ for all $i \neq j$ and $\partial_{i,i} - \partial_{i+1,i+1}$ for $i = 0, \dots, n-1$. A dual basis with respect to (\cdot, \cdot) is $\partial_{j,i}$ for all $i \neq j$ and

$$\frac{n-i}{n}(\partial_{1,1} + \dots + \partial_{i,i}) - \frac{i}{n}(\partial_{i+1,i+1} + \dots + \partial_{n,n})$$

for $i = 1, \dots, n-1$. We divide by $2n$ to get the dual basis with respect to κ . Now the Casimir operator is defined by

$$\begin{aligned} \frac{1}{2n} \left(\sum_{i \neq j} \partial_{i,j} * \partial_{j,i} + \sum_{i=1}^{n-1} \left(\frac{n-i}{n} \sum_{j=1}^i \partial_{j,j} * (\partial_{i,i} - \partial_{i+1,i+1}) - \right. \right. \\ \left. \left. \frac{i}{n} \sum_{j=i+1}^{n-1} \partial_{j,j} * (\partial_{i,i} - \partial_{i+1,i+1}) \right) \right) = \\ = \frac{1}{2n} \sum_{i,j} \partial_{i,j} * \partial_{j,i} - \frac{1}{2n^2} \sum_{i,j} \partial_{i,i} * \partial_{j,j}. \end{aligned} \quad (4.5.1)$$

For our applications, we only need to know the Casimir operator up to a constant multiple, so we might as well work with the operator

$$\sum_{i,j} \partial_{i,j} * \partial_{j,i} - \frac{1}{n} \sum_{i,j} \partial_{i,i} * \partial_{j,j}.$$

□

Example 4.5.15 Let $G = O_n$ be the orthogonal group and let \mathfrak{o}_n be its Lie algebra. A basis of \mathfrak{o}_n is given by $\partial_{i,j} - \partial_{j,i}$ with $i < j$. The Killing form κ is a multiple of the bilinear form

$$(\partial_A, \partial_B) = \text{Tr}(AB)$$

restricted to \mathfrak{o}_n . A basis of \mathfrak{o}_n is given by $\partial_{i,j} - \partial_{j,i}$ with $i < j$. The dual basis is given by $\frac{1}{2}(\partial_{i,j} - \partial_{j,i})$ with $i < j$. The Casimir operator up to a scalar multiple is equal to

$$\sum_{i < j} (\partial_{i,j} - \partial_{j,i}) * (\partial_{i,j} - \partial_{j,i}) = \sum_{i \neq j} (\partial_{i,j} * \partial_{j,i} + \partial_{i,j} * \partial_{j,i}).$$

□

Remark 4.5.16 For every rational representation V of G , the Casimir operator $c \in K[G]^*$ commutes with the action of G on V . If V is an irreducible representation, then by Schur's Lemma, the only linear maps commuting with the action are scalar multiples of the identity map. This shows that the Casimir operator acts as a scalar on every irreducible representation. \triangleleft

Lemma 4.5.17 Suppose that V is an irreducible rational representation of G . Then c acts as the zero map $V \rightarrow V$ if and only if V is the trivial representation.

Proof This follows from Humphreys [12, §22.3]. For this we need some representation theory. Let ρ be the sum of the fundamental weights (which is equal to half the sum of the positive roots). If V is a representation with highest weight λ , then c acts as the scalar $(\lambda, \rho + \lambda)$ which is equal to 0 if and only if $\lambda = 0$. \square

Suppose that V is a rational representation of G . Let $V = V^G \oplus C$ where C is the unique G -stable complement. The action of the Reynolds operator $\mathcal{R} : K[G] \rightarrow K$ on V is the projection of V onto V^G .

Let us write $c^i = c * c * \cdots * c$ (i times) and $c^0 = \epsilon_e$. If $P(t) = \sum_{i=0}^l a_i t^i \in K[t]$ is a polynomial, we define $P(c) := \sum_{i=0}^l a_i c^i \in K[G]^*$.

Proposition 4.5.18 Suppose $v \in V$. Let P be the monic polynomial of smallest degree such that $P(c) \cdot v = 0$.

- (a) If $P(0) \neq 0$, then $\mathcal{R} \cdot v = 0$;
- (b) If $P(0) = 0$, write $P(t) = tQ(t)$. Then we have $\mathcal{R} \cdot v = Q(0)^{-1}Q(c) \cdot v$.

Proof Write $v = v_0 + v_1$ with $v_0 \in V^G$ and $v_1 \in C$. Then we have $\mathcal{R} \cdot v = v_0$. Moreover, $P(c) \cdot v = (P(c) \cdot v_0) + (P(c) \cdot v_1)$. Notice that $P(c) \cdot v_0 \in V^G$ and $P(c) \cdot v_1 \in C$. Because $P(c) \cdot v = 0$, we have $P(c) \cdot v_0 = P(c) \cdot v_1 = 0$. By Lemma 4.5.17, $c \cdot v_0 = 0$, so $P(0)v_0 = P(c) \cdot v_0 = 0$. If $P(0) \neq 0$, then $v_0 = 0$.

If $P(0) = 0$, then we have $P(c) \cdot v_1 = c(Q(c) \cdot v_1) = 0$. Because c is injective on C by Lemma 4.5.17, we have $Q(c) \cdot v_1 = 0$. We have $Q(c) \cdot v_0 = Q(0)v_0$ and $Q(c) \cdot v = Q(c)v_0 + Q(c)v_1 = Q(0)v_0$. Because of the minimality of the degree of P , we know that $Q(0) \neq 0$. \square

Algorithm 4.5.19 Suppose that V is a rational representation of a connected semisimple group G . The input of the algorithm is an element v in V , and the output will be $\mathcal{R} \cdot v$ where $\mathcal{R} : K[G] \rightarrow K$ is the Reynolds operator (if $V = K[X]$, then $\mathcal{R} \cdot v = \mathcal{R}_X v$ where $\mathcal{R}_X : K[X] \rightarrow K[X]^G$ is the Reynolds operator on $K[X]$).

- (1) Input: $v \in V$
- (2) $l := 0; v_0 := v$
- (3) If there is a linear combination $\sum_{i=0}^l a_i v_i = 0$ with $a_l \neq 0$, then
 - (4) If $a_0 \neq 0$, then
 - (5) Output: 0
 - (6) else
 - (7) Output: $a_1^{-1} \sum_{i=1}^l a_i v_{i-1}$
 - (8) $l := l + 1$

- (9) compute $v_l = c \cdot v_{l-1}$.
 (10) Go to step 3

In Step (7) we have that $a_1 \neq 0$. This follows from the proof of Proposition 4.5.18 (b), because $a_0 = P(0)$ and $a_1 = Q(0)$.

Let us explain more precisely how this works in the case where G acts on $K[V]$ with V an n -dimensional rational representation of G . Suppose we would like to compute $\mathcal{R}(f)$ for some $f \in K[V]$.

As in the algorithm we compute f_0, f_1, f_2, \dots defined by $f_0 = f$ and $f_i := c \cdot f_{i-1}$ for all $i > 0$. How to determine whether f_0, f_1, \dots, f_l are linearly dependent? Of course, for every l we can use straightforward linear algebra to test whether f_0, \dots, f_l are linearly dependent. We can do it slightly more efficient here.

For every l we define W_l as the vector space spanned by f_0, f_1, \dots, f_l (and $W_{-1} = \{0\}$). The coordinate ring $K[V]$ is isomorphic to $K[x_1, \dots, x_n]$. Choose a total ordering “ $>$ ” on the monomials. We will construct g_0, g_1, \dots with the following properties:

- (a) W_l is spanned by g_0, \dots, g_l for all l ;
- (b) If $g_l \neq 0$, then $\text{LM}(g_l) \neq \text{LM}(g_i)$ for all $i < l$;
- (c) The leading coefficient $\text{LC}(g_l)$ equals 1.

The construction is inductively. We define $g_0 = f_0$. Assume that g_0, \dots, g_{l-1} are constructed. Then we can construct g_l as follows. Start with $g_l := f_l$ and subtract multiples of the g_i 's with $i < l$ until property (b) is satisfied. Then divide by a constant to get $\text{LC}(g_l) = 1$ which is property (c). Clearly property (a) is satisfied. Algorithm 4.5.19 can be refined to

Algorithm 4.5.20 Let V be a rational representation of a connected semi-simple group G . The input of the algorithm is an element $f \in K[V]$ and the output is $\mathcal{R}f$ where \mathcal{R} is the Reynolds operator.

- (1) Input: f
- (2) $f_0 := f; l := 0$;
- (3) $g_l := f_l; b_{l,l} := 1; b_{l,i} := 0$ for $i = 0, \dots, l-1$.
- (4) $a := \text{LC}(g_l)$
- (5) If there is an $i < l$ such that $\text{LM}(g_l) = \text{LM}(g_i)$, then
 - (6) $g_l := g_l - ag_i$
 - (7) $b_{l,j} := b_{l,j} - ab_{i,j}$ for $j = 0, \dots, i$
 - (8) go to step 4
- (9) If $g_l = 0$, then
 - (10) if $b_{l,0} \neq 0$, then
 - (11) Output: 0
 - (12) else
 - (13) Output: $(\sum_{j=1}^l b_{l,j} f_{j-1}) / b_{l,1}$
 - (14) $g_l := g_l / a$
 - (15) $b_{l,j} := b_{l,j} / a$ for $j = 0, \dots, l$
 - (16) $l := l + 1$

$$(17) \quad f_l := c \cdot f_{l-1}$$

(18) go to step 3

We first note that throughout the algorithm, we will have

$$g_l = \sum_{i=0}^l b_{l,i} f_i. \quad (4.5.2)$$

This explains Step 3, 6 and 7. The loop covering the Steps 4–8 is finite because $\text{LM}(g_l)$ decreases each time because of Step 6. Once $g_l = 0$, then f_0, f_1, \dots, f_l are linearly dependent, because of (4.5.2) and the algorithm terminates.

Example 4.5.21 Let $G = \text{SL}_2$ act on V_2 . Here V_2 is the set of binary forms of degree 2, i.e.,

$$V_2 := \{a_0x^2 + a_1xy + a_2y^2\}.$$

A basis of \mathfrak{sl}_2 is $\mathbf{x} = \partial_{2,1}$, $\mathbf{y} = \partial_{1,2}$ and $\mathbf{h} = \partial_{1,1} - \partial_{2,2}$. The action of the Lie algebra of \mathfrak{sl}_2 on V_2 is given by

$$\mathbf{x} \cdot v = y \frac{\partial}{\partial x} v,$$

$$\mathbf{y} \cdot v = x \frac{\partial}{\partial y} v,$$

$$\mathbf{h} \cdot v = (x \frac{\partial}{\partial x} - y \frac{\partial}{\partial y})v.$$

The coordinate ring $K[V_2]$ can be identified with $K[a_0, a_1, a_2]$. The action of \mathfrak{sl}_2 on $K[a_0, a_1, a_2]$ is given by

$$\mathbf{x} \cdot f = (-2a_0 \frac{\partial}{\partial a_1} - a_1 \frac{\partial}{\partial a_2})f,$$

$$\mathbf{y} \cdot f = (-a_1 \frac{\partial}{\partial a_0} - 2a_2 \frac{\partial}{\partial a_1})f,$$

$$\mathbf{h} \cdot f = (-2a_0 \frac{\partial}{\partial a_0} + 2a_2 \frac{\partial}{\partial a_2})f,$$

where $f \in K[a_0, a_1, a_2]$. A dual basis of \mathbf{x} , \mathbf{y} , \mathbf{h} is $\mathbf{y}/4$, $\mathbf{x}/4$, $\mathbf{h}/8$. The Casimir operator is therefore defined by

$$c = \frac{\mathbf{x} * \mathbf{y}}{4} + \frac{\mathbf{y} * \mathbf{x}}{4} + \frac{\mathbf{h} * \mathbf{h}}{8}.$$

A straightforward calculation shows that c acts by the differential operator

$$\begin{aligned} a_0 a_1 \frac{\partial}{\partial a_0} \frac{\partial}{\partial a_1} + a_1 a_2 \frac{\partial}{\partial a_1} \frac{\partial}{\partial a_2} + 2a_0 a_2 \frac{\partial^2}{(\partial a_1)^2} + a_0 \frac{\partial}{\partial a_0} + a_1 \frac{\partial}{\partial a_1} + a_2 \frac{\partial}{\partial a_2} + \\ + \frac{1}{2} \left(a_0^2 \frac{\partial^2}{(\partial a_0)^2} + a_2^2 \frac{\partial^2}{(\partial a_2)^2} + (a_1^2 - 2a_0 a_2) \frac{\partial}{\partial a_0} \frac{\partial}{\partial a_2} \right). \end{aligned} \quad (4.5.3)$$

Let us compute $\mathcal{R}(a_1^2)$ where $\mathcal{R} : K[V_2] \rightarrow K[V_2]^{\text{SL}_2}$ is the Reynolds operator. We apply c :

$$c \cdot a_1^2 = 2a_1^2 + 4a_0 a_2, \quad c \cdot (2a_1^2 + 4a_0 a_2) = 6a_1^2 + 12a_0 a_2 = 3(2a_1^2 + 4a_0 a_2).$$

We have found the relation $c^2 \cdot a_1^2 - 3c \cdot a_1 = 0$. Therefore,

$$\mathcal{R}(a_1^2) = \frac{(c-3) \cdot a_1^2}{-3} = \frac{2a_1^2 + 4a_0 a_2 - 3a_1^2}{-3} = \frac{1}{3} (a_1^2 - 4a_0 a_2).$$

Let us compute $\mathcal{R}(a_1^4)$ following Algorithm 4.5.20. We choose the graded reverse lexicographic ordering on the monomials. We define $f_0 = g_0 = a_1^4$. Now

$$f_1 := c \cdot f_0 = c \cdot a_1^4 = 4a_1^4 + 24a_0 a_1^2 a_2.$$

The leading term of f_1 is $4a_1^4$, and the leading term of g_0 is a_1^4 . The leading term of $f_1 - 4g_0$ is $24a_0 a_1^2 a_2$ so we define $g_1 = (f_1 - 4g_0)/24$. We have $g_1 = \frac{1}{24}f_1 - \frac{1}{6}f_0$. We apply c again:

$$f_2 := c \cdot f_1 = 28a_1^4 + 264a_0 a_1^2 a_2 + 96a_0^2 a_2^2.$$

We take f_2 , subtract 28 times g_0 and 264 times g_1 . The leading term of $f_2 - 28g_0 - 264g_1$ is $96a_0^2 a_2^2$. We define $g_2 := (f_2 - 28g_0 - 264g_1)/96$. We have $g_2 = \frac{1}{96}f_2 - \frac{7}{24}f_0 - \frac{11}{4}(\frac{1}{24}f_1 - \frac{1}{6}f_0) = \frac{1}{96}f_2 - \frac{11}{96}f_1 + \frac{1}{6}f_0$. We apply c again:

$$f_3 := c \cdot f_2 = 244a_1^4 + 2712a_0 a_1^2 a_2 + 1248a_0^2 a_2^2.$$

Thus

$$f_3 = 244g_0 + 2712g_1 + 1248g_2 =$$

$$244f_0 + 2712(\frac{1}{24}f_1 - \frac{1}{6}f_0) + 1248(\frac{1}{96}f_2 - \frac{11}{96}f_1 + \frac{1}{6}f_0) = 13f_2 - 30f_1.$$

We have found the relation

$$f_3 - 13f_2 + 30f_1 = (c^3 - 13c^2 + 30c) \cdot a_1^4 = 0.$$

Therefore $\mathcal{R}(a_1^4)$ is equal to

$$\begin{aligned} \frac{(c^2 - 13c + 30\epsilon) \cdot f_0}{30} &= \frac{f_2 - 13f_1 + 30f_0}{30} = \\ &\frac{1}{5}a_1^4 - \frac{8}{5}a_0a_1^2a_2 + \frac{16}{5}a_0^2a_2^2 = \frac{1}{5}(a_1^2 - 4a_0a_2)^2. \end{aligned}$$

△

4.5.3 Cayley's Omega Process

For GL_n and SL_n there is an alternative method for computing the Reynolds operator. This is the so-called Ω process, which was already known in the nineteenth century.

Let us consider the coordinate ring of GL_n . We denote the coordinate function corresponding to the (i,j) entry by $z_{i,j}$. Let Z be the matrix

$$\begin{pmatrix} z_{1,1} & z_{1,2} & \cdots & z_{1,n} \\ z_{2,1} & z_{2,2} & & z_{2,n} \\ \vdots & & \ddots & \vdots \\ z_{n,1} & z_{n,2} & \cdots & z_{n,n} \end{pmatrix} \in K[\mathrm{GL}_n].$$

We have

$$K[\mathrm{GL}_n] = K[\{z_{i,j} \mid 1 \leq i, j \leq n\}, \det(Z)^{-1}],$$

where $\det(Z)$ is the determinant of Z . Let us write $\frac{\partial}{\partial Z}$ for the matrix

$$\left(\begin{array}{cccc} \frac{\partial}{\partial z_{1,1}} & \frac{\partial}{\partial z_{1,2}} & \cdots & \frac{\partial}{\partial z_{1,n}} \\ \frac{\partial}{\partial z_{2,1}} & \frac{\partial}{\partial z_{2,2}} & & \frac{\partial}{\partial z_{2,n}} \\ \vdots & & \ddots & \vdots \\ \frac{\partial}{\partial z_{n,1}} & \frac{\partial}{\partial z_{n,2}} & \cdots & \frac{\partial}{\partial z_{n,n}} \end{array} \right).$$

We define a differential operator $\Omega : K[GL_n] \rightarrow K[GL_n]$ by $\Omega = \det(\frac{\partial}{\partial Z})$. Let $m : GL_n \times GL_n \rightarrow GL_n$ be the group multiplication and let $m^* : K[GL_n] \rightarrow K[GL_n] \otimes K[GL_n]$ be the dual ring homomorphism. For $f \in K[GL_n]$ we denote multiplication by f as a map $K[GL_n] \rightarrow K[GL_n]$ also by f .

Lemma 4.5.22 *We have*

$$(\det(Z)^{-1} \otimes \Omega) \circ m^* = m^* \circ \Omega = (\Omega \otimes \det(Z)^{-1}) \circ m^*.$$

Proof Let $\sigma, \tau \in GL_n$ and $f \in K[GL_n]$. We get

$$\begin{aligned} (\text{id} \otimes \frac{\partial}{\partial z_{i,j}})(m^*(f))(\sigma, \tau) &= \frac{\partial}{\partial \tau_{i,j}} f(\sigma \tau) = \sum_{i,j} \sigma_{k,i} \left(\left(\frac{\partial}{\partial z_{k,j}} f \right) (\sigma \tau) \right) = \\ &= \sum_{k=1}^n \sigma_{k,i} m^* \left(\frac{\partial}{\partial z_{i,j}} f \right) (\sigma, \tau) = \sum_{k=1}^n (z_{k,i} \otimes \text{id}) \circ m^* \left(\frac{\partial}{\partial z_{k,j}} f \right) (\sigma, \tau). \end{aligned} \quad (4.5.4)$$

Or in matrix notation we have

$$(\text{id} \otimes \frac{\partial}{\partial Z})(m^*(f)) = (^t Z \otimes \text{id}) \circ m^* \left(\frac{\partial}{\partial Z} f \right).$$

Taking determinants gives us

$$(\text{id} \otimes \Omega) \circ m^* = (\det(Z) \otimes \text{id}) \circ m^* \circ \Omega.$$

This shows the first equality of the Lemma and the other equality follows by symmetry. \square

Remark 4.5.23 If $\delta \in K[GL_n]^*$, then δ is a linear function on $K[GL_n]$. The value of δ on $f \in K[GL_n]$ is denoted by δf . But GL_n acts on $K[GL_n]$, and this induces a $K[GL_n]^*$ -module structure on $K[GL_n]$:

$$(\delta, f) \in K[GL_n]^* \times K[GL_n] \mapsto \delta \cdot f \in K[GL_n].$$

The two distinct notations δf and $\delta \cdot f$ should not be confused. \triangleleft

Remark 4.5.24 The operator Ω cannot be seen as the action of an element in $K[GL_n]^*$. However, the operator $\tilde{\Omega} := \det(Z)\Omega$ can be seen as an action of an element $\omega \in K[GL_n]^*$. Notice that

$$\begin{aligned} (\text{id} \otimes \tilde{\Omega}) \circ m^* &= (\det(Z) \otimes \det(Z)) \circ (\det(Z)^{-1} \otimes \Omega) \circ m^* = \\ &= (\det(Z) \otimes \det(Z)) \circ m^* \circ \Omega = m^* \circ (\det(Z)\Omega) = m^* \circ \tilde{\Omega}. \end{aligned} \quad (4.5.5)$$

Let us define $\omega \in K[G]^*$ by $\omega f = (\tilde{\Omega}f)(e)$ for all $f \in K[G]$. We have

$$\begin{aligned}\tilde{\Omega}f &= ((\text{id} \otimes \epsilon) \circ m^* \circ \tilde{\Omega})f = ((\text{id} \otimes \epsilon) \circ (\text{id} \otimes \tilde{\Omega}) \circ m^*)(f) \\ &= ((\text{id} \otimes \omega) \circ m^*)(f) = \omega \cdot f.\end{aligned}$$

□

Remark 4.5.25 Suppose that $f \in K[\text{GL}_n]$ and $\sigma, \tau \in \text{GL}_n$. From Lemma 4.5.22 it follows that

$$\begin{aligned}(\det(\sigma)^{-1} \Omega(\sigma^{-1} \cdot f))(\tau) &= ((\det(Z)^{-1} \otimes \Omega) \circ m^*(f))(\sigma, \tau) = \\ (m^* \circ \Omega(f))(\sigma, \tau) &= (\sigma^{-1} \cdot \Omega(f))(\tau).\end{aligned}$$

So we get

$$\det(\sigma) \Omega(\sigma \cdot f) = \sigma \cdot \Omega(f).$$

□

Lemma 4.5.26 For any positive integer p , the element $c_{p,n} := \Omega^p(\det(Z)^p) \in K[\text{GL}_n]$ is a nonzero constant.

Proof Write $\det(Z)^p = \sum_i a_i m_i(Z_{1,1}, \dots, Z_{n,n})$ where all m_i are different monomials, all of degree pn . Clearly we have $\Omega^p = \sum_i a_i m_i\left(\frac{\partial}{\partial z_{1,1}}, \dots, \frac{\partial}{\partial z_{n,n}}\right)$. Notice that

$$m_i\left(\frac{\partial}{\partial z_{1,1}}, \dots, \frac{\partial}{\partial z_{n,n}}\right) m_j(Z_{1,1}, \dots, Z_{n,n})$$

is equal to 0 if $i \neq j$ and is a positive constant if $i = j$. It follows that

$$\Omega^p(\det(Z)^p) = \sum_i a_i^2 m_i\left(\frac{\partial}{\partial z_{1,1}}, \dots, \frac{\partial}{\partial z_{n,n}}\right) m_i(Z_{1,1}, \dots, Z_{n,n})$$

is a nonzero constant. □

The Reynolds operator $\mathcal{R} : K[\text{GL}_n] \rightarrow K$ can be expressed in Ω as follows.

Proposition 4.5.27 Suppose that $f \in K[\{z_{i,j} \mid 1 \leq i, j \leq n\}]$ is homogeneous. If $\deg(f) = np$, then

$$\mathcal{R}\left(\frac{f}{\det(Z)^p}\right) = \frac{\Omega^p(f)}{c_{p,n}}$$

with $c_{p,n} = \Omega^p(\det(Z)^p)$ and if $\deg(f) \neq np$, then $\mathcal{R}(f / \det(Z)^p) = 0$.

Proof We have $K[\mathrm{GL}_n]^{\mathrm{GL}_n} = K$. Let $V_{p,q} \subset K[\mathrm{GL}_n]$ be the set of all $f / \det(Z)^p$ with f homogeneous of degree q . If $q \neq np$, then $K \cap V = \{0\}$ and $V^{\mathrm{GL}_n} = 0$. It follows that $\mathcal{R}(g) = 0$ for all $g \in V_{p,q}$.

Let $V = V_{p,pn}$. Define a map $\mathcal{R}_V : V \rightarrow V^{\mathrm{GL}_n} \cong K$ by

$$\mathcal{R}_V \left(\frac{f}{\det(Z)^p} \right) = \frac{\Omega^p f}{c_{p,n}},$$

and we will show that \mathcal{R}_V is the restriction of the Reynolds operator. First of all \mathcal{R}_V is GL_n -invariant because of Lemma 4.5.22. Also, the restriction of \mathcal{R}_V to K is the identity because

$$\mathcal{R}_V(1) = \mathcal{R}_V \left(\frac{\det(Z)^p}{\det(Z)^p} \right) = \frac{\Omega^p(\det(Z)^p)}{c_{p,n}} = 1.$$

If W is the kernel of \mathcal{R}_V , then \mathcal{R}_V is the projection of $V = W \oplus K$ onto K . From Remark 2.2.6 it follows that the restriction of \mathcal{R} to V is equal to \mathcal{R}_V . \square

Proposition 4.5.28 *Let $\mathcal{R}_{\mathrm{SL}_n} : K[\mathrm{GL}_n] \rightarrow K[\mathrm{GL}_n]^{\mathrm{SL}_n}$ be the Reynolds operator, where SL_n acts on GL_n by left multiplication. Suppose that $f \in K[\{z_{i,j} \mid 1 \leq i, j \leq n\}]$ is homogeneous. If $\deg(f) = nr$, then*

$$\mathcal{R}_{\mathrm{SL}_n} \left(\frac{f}{\det(Z)^p} \right) = \det(Z)^{r-p} \frac{\Omega^r f}{c_{r,n}}.$$

If $\deg(f)$ is not divisible by n , then $\mathcal{R}_{\mathrm{SL}_n}(f / \det(Z)^p) = 0$ for every integer p .

Proof Notice that $K[\mathrm{GL}_n]^{\mathrm{SL}_n} = K[\det(Z), \det(Z)^{-1}]$. If $V_{p,q}$ is the vector space of all $f / \det(Z)^p$ with $\deg(f) = q$. If q is not divisible by n , then clearly $V_{p,q}$ cannot contain any invariants and $\mathcal{R}(f / \det(Z)^p) \in V_{p,q}^{\mathrm{SL}_n} = \{0\}$.

If $q = nr$, then a similar argument as in the proof of Proposition 4.5.27 shows that the restriction of $\mathcal{R}_{\mathrm{SL}_n}$ to $V_{p,nr}$ is given by

$$\frac{f}{\det(Z)^p} \mapsto \det(Z)^{r-p} \frac{\Omega^r f}{c_{r,n}}.$$

\square

Remark 4.5.29 The coordinate ring of SL_n is $K[\{z_{i,j} \mid 1 \leq i, j \leq n\}] / I$ where I is the principal ideal generated by $\det(Z) - 1$. The Reynolds operator $\mathcal{R}_{\mathrm{SL}_n} : K[\mathrm{SL}_n] \rightarrow K$ can be computed as follows. Suppose $g \in K[\mathrm{SL}_n]$ and suppose that it is represented by $f \in K[\{z_{i,j} \mid 1 \leq i, j \leq n\}]$. Then $\mathcal{R}_{\mathrm{SL}_n}(g) = \mathcal{R}_{\mathrm{SL}_n}(f) + I$. If we assume that f is homogeneous, then by Proposition 4.5.28

$$\mathcal{R}_{\mathrm{SL}_n}(g) = \frac{\Omega^r f}{c_{r,n}} + I$$

if $\deg(f) = rn$ and $\mathcal{R}_{\mathrm{SL}_n}(g) = 0$ if the degree of f is not divisible by n . \square

Remark 4.5.30 In Proposition 4.5.27 and Remark 4.5.29 we have described the Reynolds operators $\mathcal{R}_{\mathrm{GL}_n} : K[\mathrm{GL}_n] \rightarrow K$ and $\mathcal{R}_{\mathrm{SL}_n} : K[\mathrm{SL}_n] \rightarrow K$. Suppose that V is a rational representation of G where $G = \mathrm{GL}_n$ or $G = \mathrm{SL}_n$ and let $\mathcal{R}_V : K[V] \rightarrow K[V]^G$ be the Reynolds operator. For every $f \in K[V]$, we have $\mathcal{R}_V(f) = \mathcal{R}_G \cdot f$. Let $\mu^* : K[V] \rightarrow K[V] \otimes K[G]$ be as in Example A.2.12. If we write $\mu^*(f) = \sum_i f_i \otimes g_i$, then $\mathcal{R}_G f = \sum_i f_i \mathcal{R}_G(g_i)$ (see Proposition 4.5.10). Since we have described \mathcal{R}_G in terms of Ω , we also can describe \mathcal{R}_V in terms of Ω . \triangleleft

Example 4.5.31 Let SL_2 act on the binary forms

$$V_2 = \{a_0x^2 + a_1xy + a_2y^2\}$$

and on the coordinate ring $K[V_2] \cong K[a_0, a_1, a_2]$. Let

$$\begin{pmatrix} z_{1,1} & z_{1,2} \\ z_{2,1} & z_{2,2} \end{pmatrix} \in \mathrm{SL}_2$$

act on $a_0x^2 + a_1xy + a_2y^2$ by

$$\begin{aligned} a_0(z_{1,1}x + z_{2,1}y)^2 + a_1(z_{1,1}x + z_{2,1}y)(z_{1,2}x + z_{2,2}y) + a_2(z_{1,2}x + z_{2,2}y)^2 \\ = (a_0z_{1,1}^2 + a_1z_{1,1}z_{1,2} + a_2z_{1,2}^2)x^2 + \\ (2a_0z_{1,1}z_{2,1} + a_1z_{1,1}z_{2,2} + a_1z_{2,1}z_{1,2} + 2a_2z_{1,2}z_{2,2})xy + \\ (a_0z_{2,1}^2 + a_1z_{2,1}z_{2,2} + a_2z_{2,2}^2)y^2. \end{aligned} \quad (4.5.6)$$

Let $\mu^* : K[V_2] \rightarrow K[V_2] \otimes K[\mathrm{SL}_2]$ be as in Example A.2.12, so μ^* is given by:

$$a_0 \mapsto a_0z_{1,1}^2 + a_1z_{1,1}z_{1,2} + a_2z_{1,2}^2,$$

$$a_1 \mapsto 2a_0z_{1,1}z_{2,1} + a_1z_{1,1}z_{2,2} + a_1z_{2,1}z_{1,2} + 2a_2z_{1,2}z_{2,2},$$

$$a_2 \mapsto a_0z_{2,1}^2 + a_1z_{2,1}z_{2,2} + a_2z_{2,2}^2.$$

We will compute $\mathcal{R}(a_1^2)$. We have

$$\begin{aligned} \mu^*(a_1^2) &= (2a_0z_{1,1}z_{2,1} + a_1z_{1,1}z_{2,2} + a_1z_{2,1}z_{1,2} + 2a_2z_{1,2}z_{2,2})^2 = \\ &4z_{1,1}^2z_{2,1}^2a_0^2 + (4z_{1,1}^2z_{2,1}z_{2,2} + 4z_{1,1}z_{2,1}^2z_{1,2})a_0a_1 + 8z_{1,1}z_{2,1}z_{1,2}z_{2,2}a_0a_2 + \\ &+ (z_{1,1}^2z_{2,2}^2 + 2z_{1,1}z_{2,2}z_{2,1}z_{1,2} + z_{2,1}^2z_{1,2}^2)a_1^2 + (4z_{1,1}z_{1,2}z_{2,2}^2 + 4z_{2,1}z_{1,2}^2z_{2,2})a_1a_2 \\ &+ 4z_{1,2}^2z_{2,2}^2a_0^2. \end{aligned} \quad (4.5.7)$$

Since the coefficients of the monomials in a are homogeneous of degree 4 in the z variables, we get

$$\mathcal{R}(a_1^2) = \frac{(\text{id} \otimes \Omega^2)(m^*(a_1^2))}{c_{2,2}}.$$

Applying $\Omega^2 = \frac{\partial^2}{(\partial z_{1,1})^2} \frac{\partial^2}{(\partial z_{2,2})^2} - 2 \frac{\partial}{\partial z_{1,1}} \frac{\partial}{\partial z_{2,2}} \frac{\partial}{\partial z_{1,2}} \frac{\partial}{\partial z_{2,1}} + \frac{\partial^2}{(\partial z_{2,1})^2} \frac{\partial^2}{(\partial z_{1,2})^2}$ to (4.5.7) yields

$$4a_1^2 - 16a_0a_2.$$

We compute $c_{2,2} = \Omega^2(\det(Z))^2 = 12$, so we conclude that

$$\mathcal{R}(a_1^2) = \frac{4a_1^2 - 16a_0a_2}{12} = \frac{1}{3}(a_1^2 - 4a_0a_2).$$

△

4.6 Computing Hilbert Series

In this section we will discuss how the Hilbert series $H(K[V]^G, t)$ can be computed for a linearly reductive group G .

4.6.1 A Generalization of Molien's Formula

We assume that $\text{char}(K) = 0$. In Theorem 3.4.2 we have seen that for a finite group, the Hilbert series of the invariant ring can easily be computed in advance (without knowing the generators of the invariant ring) with Molien's Formula. If G is a finite group and V is a finite dimensional representation, then

$$H(K[V]^G, t) = \frac{1}{|G|} \sum_{\sigma \in G} \frac{1}{\det_V(1 - t \cdot \sigma)}. \quad (4.6.1)$$

This idea can be generalized to arbitrary reductive groups. Instead of averaging over a finite group, we will have to average over a reductive group. Let us assume in this section that our base field K is the complex numbers \mathbb{C} . Averaging over G does not make much sense, because an infinite reductive group is not compact. However, G always contains a maximal compact subgroup C (see Anhang II of Kraft [13] or the references there). We can choose a Haar measure $d\mu$ on C and normalize it such that $\int_C d\mu = 1$. Let V be a finite dimensional rational representation of G . The

proper generalization of (4.6.1) is

$$H(\mathbb{C}[V]^G, t) = \int_C \frac{d\mu}{\det_V(1 - t \cdot \sigma)}. \quad (4.6.2)$$

Indeed, for any representation W , let $\Phi_\sigma(W)$ be the trace of the action of $\sigma \in C$ on U . The function $I(W) := \int_C \Phi_\sigma(W) d\mu$ counts the dimension of U^C and $U^C = U^G$ since C is Zariski dense in G . Using this, (4.6.2) can be proven in a similar way as Theorem 3.4.2.

Notice that the Hilbert series $H(\mathbb{C}[V]^G, t)$ converges for $|t| < 1$ because it is a rational function with poles only at $t = 1$. Since C is compact, there exist constants $A > 0$ such that for every $\sigma \in C$ and every eigenvalue λ of σ we have $|\lambda| \leq A$. Since λ^l is an eigenvalue of σ^l , it follows that $|\lambda^l| \leq A$ for all l , so $|\lambda| \leq 1$. It is clear that the integral on the right-hand side of (4.6.2) also is defined for $|t| < 1$.

Assume that G is also connected. Let T be a maximal torus of G , and let D be a maximal compact subgroup of T . We may assume that C contains D . The torus can be identified with $(\mathbb{C}^*)^r$, where r is the rank of G , and D can be identified with the subgroup $(S^1)^r$ of $(\mathbb{C}^*)^r$, where $S^1 \subset \mathbb{C}^*$ is the unit circle. We can choose a Haar measure dv on D such that $\int_D dv = 1$. Suppose that f is a continuous class function on C . In a compact group, all elements are semi-simple and every C -conjugacy class has a representative in D . An integral like

$$\int_C f(\sigma) d\mu$$

can be viewed as an integral over D , since f is constant on conjugacy classes. More precisely, there exists a weight function $\varphi : D \rightarrow \mathbb{R}$ such that for every continuous class function f we have

$$\int_C f(\sigma) d\mu = \int_D \varphi(\sigma) f(\sigma) dv$$

(see Weyl [14, 15], Adams [16], and Zhelobenko [17]). Notice that the integrand $\det_V(1 - t \cdot \sigma)^{-1}$ in (4.6.2) only depends on the conjugacy class of σ . We get that

$$H(\mathbb{C}[V]^G, t) = \int_C \frac{d\mu}{\det_V(1 - t \cdot \sigma)} = \int_D \frac{\varphi(\sigma) dv}{\det_V(1 - t \cdot \sigma)}. \quad (4.6.3)$$

The compact torus D acts diagonally on V and its dual space V^* for a convenient choice of bases in V and V^* . So the action of $(z_1, \dots, z_r) \in D$ on V^* is given by a matrix

$$\begin{pmatrix} m_1(z) & 0 & \cdots & 0 \\ 0 & m_2(z) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & m_n(z) \end{pmatrix},$$

where m_1, m_2, \dots, m_n are Laurent monomials in z_1, \dots, z_r . With this notation, we have

$$\det_V(1 - t \cdot (z_1, \dots, z_n)) = (1 - m_1(z)t)(1 - m_2(z)t) \cdots (1 - m_n(z)t),$$

and it follows that

$$H(\mathbb{C}[V]^G, t) = \int_D \frac{\varphi(z)dv}{(1 - m_1(z)t)(1 - m_2(z)t) \cdots (1 - m_n(z)t)}. \quad (4.6.4)$$

In Sect. 4.6.3 we will give a similar, but more explicit formula.

Example 4.6.1 Let $G = \mathrm{SL}_2(\mathbb{C})$ with maximal compact subgroup $C = \mathrm{SU}_2(\mathbb{C})$. A maximal torus T of G is the set of diagonal matrices

$$\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}, \quad z \in \mathbb{C}^*.$$

A maximal compact subgroup D of T is

$$\begin{pmatrix} z & 0 \\ 0 & z^{-1} \end{pmatrix}, \quad z \in S^1.$$

We can define a diffeomorphism of the three-dimensional real sphere S^3 to $\mathrm{SU}_2(\mathbb{C})$ by

$$(x, y, v, w) \in S^3 \mapsto \begin{pmatrix} x + yi & v + wi \\ -v + wi & x - yi \end{pmatrix}.$$

It is straightforward to check that

$$d\mu = \frac{dx \wedge dy \wedge dv}{w} = -\frac{dx \wedge dy \wedge dw}{v} = \frac{dx \wedge dv \wedge dw}{y} = -\frac{dy \wedge dv \wedge dw}{x}$$

is a Haar measure on SU_2 . A normalized Haar measure is $d\mu/2\pi^2$. Under the diffeomorphism, SU_2 -conjugacy classes correspond to the 2-dimensional spheres $x = a$ with $-1 \leq a \leq 1$ and the compact torus D corresponds to $v = w = 0$.

If a function f is constant on conjugacy classes, then

$$\begin{aligned} \frac{1}{2\pi^2} \int_{S^3} f(x, y, v, w) d\mu &= \frac{1}{2\pi^2} \int_{S^3} f(x, y, v, w) \frac{dv \wedge dw \wedge dx}{y} = \\ &= \frac{1}{2\pi^2} \int_{S^3} f(x, y, v, w) \frac{\sqrt{1 - x^2} d\tilde{v} \wedge d\tilde{w} \wedge dx}{\tilde{y}} = \end{aligned}$$

$$\begin{aligned}
&= \frac{1}{2\pi^2} \int_{-1}^1 f(x, \sqrt{1-x^2}, 0, 0) \sqrt{1-x^2} dx \int_{S^2} \frac{d\tilde{v} \wedge d\tilde{w}}{\tilde{y}} = \\
&= \frac{2}{\pi} \int_{-1}^1 f(x, \sqrt{1-x^2}, 0, 0) \sqrt{1-x^2} dx,
\end{aligned}$$

where $\tilde{y} = y/\sqrt{1-x^2}$, $\tilde{v} = v/\sqrt{1-x^2}$ and $\tilde{w} = w/\sqrt{1-x^2}$. Notice that $(\tilde{y}, \tilde{v}, \tilde{w})$ lies on the two-dimensional sphere S^2 . Using a substitution $x = \cos(u)$, this is equal to

$$\begin{aligned}
&\frac{2}{\pi} \int_{\pi}^0 \sqrt{1-\cos^2(u)} f(\cos(u), \sin(u), 0, 0) (-\sin(u)) du = \\
&= \frac{1}{\pi} \int_0^{2\pi} \sin^2(u) f(\cos(u), \sin(u), 0, 0) du. \quad (4.6.5)
\end{aligned}$$

Let V_d be the binary forms of degree d . The action of $D \cong S^1$ on V_d is given by the $(d+1) \times (d+1)$ -matrix

$$\begin{pmatrix} z^d & 0 & 0 & \cdots & 0 \\ 0 & z^{d-2} & 0 & & 0 \\ 0 & 0 & z^{d-4} & & 0 \\ \vdots & & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & z^{-d} \end{pmatrix}.$$

We have

$$H(\mathbb{C}[V_d]^{\text{SL}_2}, t) = \frac{1}{\pi} \int_0^{2\pi} \frac{\sin^2(u) du}{(1 - e^{idu}t)(1 - e^{i(d-2)u}t) \cdots (1 - e^{-idu}t)}.$$

We could also view this integral as a complex contour integral by putting $z = e^{iu}$ so that $du = dz/iz$ and $\sin(u) = (z - z^{-1})/2i$:

$$\begin{aligned}
H(\mathbb{C}[V_d]^{\text{SL}_2}, t) &= \frac{-1}{4\pi i} \int_{S^1} \frac{(z - z^{-1})^2 dz}{z(1 - z^d t)(1 - z^{d-2} t) \cdots (1 - z^{-d} t)} = \\
&= \frac{1}{4\pi i} \int_{S^1} \frac{(1 - z^2) dz}{z(1 - z^d t)(1 - z^{d-2} t) \cdots (1 - z^{-d} t)} + \\
&\quad + \frac{1}{4\pi i} \int_{S^1} \frac{(1 - z^{-2}) dz}{z(1 - z^d t)(1 - z^{d-2} t) \cdots (1 - z^{-d} t)}. \quad (4.6.6)
\end{aligned}$$

By symmetry $z \leftrightarrow z^{-1}$, the latter two integrals are equal to each other. So we obtain

$$H(\mathbb{C}[V_d]^{\mathrm{SL}_2}, t) = \frac{1}{2\pi i} \int_{S^1} \frac{(1-z^2) dz}{z(1-z^d t)(1-z^{d-2} t) \cdots (1-z^{-d} t)}. \quad (4.6.7)$$

As we will see later, an integral like this can be evaluated using the Residue Theorem. An explicit treatment of Hilbert series for binary forms can be found in Springer [18]. \triangleleft

4.6.2 Hilbert Series of Invariant Rings of Tori

In this section we will derive a formula for the Hilbert series of the invariant ring of a torus group. We will work over an algebraically closed base field K of characteristic 0.

Let T be an r -dimensional torus group. Suppose that $\rho : T \rightarrow \mathrm{GL}(V)$ is a rational representation.

Definition 4.6.2 The **character** $\chi^V = \chi_T^V : T \rightarrow K^*$ of T is defined by

$$\chi^V(\sigma) = \mathrm{Tr}(\rho(\sigma)),$$

where Tr is the trace.

Let $X(T) \cong \mathbb{Z}^r$ be the group of one-dimensional characters. Choose generators z_1, \dots, z_r of $X(T)$. After a convenient basis choice, the action of T on V is diagonal. The action is given by the matrix

$$\rho = \begin{pmatrix} m_1(z) & 0 & \cdots & 0 \\ 0 & m_2(z) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & m_n(z) \end{pmatrix},$$

where m_1, \dots, m_n are Laurent monomials in z_1, \dots, z_r . The character of V is the trace of the representation:

$$\chi^V = m_1(z) + m_2(z) + \cdots + m_n(z).$$

Remark 4.6.3 Notice that $\dim V^T$ is the coefficient of $z_1^0 z_2^0 \cdots z_r^0 = 1$ in χ^V . \triangleleft

Definition 4.6.4 Suppose that $V = \bigoplus_{d=k}^{\infty} V_d$ is a graded vector space and for each d , V_d is a rational representation of T , then we define the T -Hilbert series of V by

$$H_T(V, z_1, \dots, z_r, t) = \sum_{d=k}^{\infty} \chi^{V_d} t^d.$$

Remark 4.6.5 Because of Remark 4.6.3 the Hilbert series $H(V^T, t) = \sum_{d=k}^{\infty} \dim(V_d^T) t^d$ of the invariant space V^T is obtained by taking the coefficient of $z_1^0 z_2^0 \cdots z_r^0 = 1$ in $H_T(V, z_1, \dots, z_r, t)$. \triangleleft

Suppose that V is a rational representation of T and let $\rho : T \rightarrow \mathrm{GL}(V^*)$ be the dual representation. We can choose a basis x_1, \dots, x_n of V^* such that the action of T is diagonal. Suppose that the action on V^* is given by the matrix

$$\begin{pmatrix} m_1(z) & 0 & \cdots & 0 \\ 0 & m_2(z) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & m_n(z) \end{pmatrix}.$$

Since $K[V]$ is the polynomial ring in x_1, \dots, x_n , we have

$$H_T(K[V], z_1, \dots, z_r, t) = \frac{1}{(1 - m_1(z)t)(1 - m_2(z)t) \cdots (1 - m_n(z)t)}. \quad (4.6.8)$$

From Remark 4.6.5 we get the following corollary.

Corollary 4.6.6 *With the notation as before, the Hilbert series of $K[V]^T$ is given by the coefficient of $z_1^0 z_2^0 \cdots z_r^0 = 1$ in (4.6.8).*

Example 4.6.7 Let T be a 2-dimensional torus and let z_1, z_2 are two characters such that $K[T] = k[z_1, z_2, z_1^{-1}, z_2^{-1}]$. Suppose that the representation on a vector space V is given by the matrix

$$\begin{pmatrix} z_1^{-1} & 0 & 0 \\ 0 & z_2^{-1} & 0 \\ 0 & 0 & z_1 z_2 \end{pmatrix}.$$

The action on the dual space V^* is then given by the matrix

$$\begin{pmatrix} z_1 & 0 & 0 \\ 0 & z_2 & 0 \\ 0 & 0 & z_1^{-1} z_2^{-1} \end{pmatrix}.$$

From (4.6.8) we get

$$H_T(K[V], z_1, z_2, t) = \frac{1}{(1 - z_1 t)(1 - z_2 t)(1 - z_1^{-1} z_2^{-1} t)}. \quad (4.6.9)$$

The Hilbert series $H(K[V]^T, t)$ of the invariant ring is the coefficient of $z_1^0 z_2^0$ in (4.6.9). If we expand the series in (4.6.9) we get

$$H_T(K[V], z_1, z_2, t) = (1 + z_1 t + z_1^2 t^2 + \dots)(1 + z_2 t + z_2^2 t^2 + \dots)(1 + z_1^{-1} z_2^{-1} t + z_1^{-2} z_2^{-2} t^2 + \dots).$$

It is easy to see that the constant coefficient is $1 + t^3 + t^6 + t^9 + \dots = (1 - t^3)^{-1}$. We conclude $H(K[V]^T, t) = (1 - t^3)^{-1}$. If x_1, x_2, x_3 is the basis of V^* , then it is clear that $K[V]^T = K[x_1 x_2 x_3]$. So we verify that $H(K[V]^T, t) = H(K[x_1 x_2 x_3], t) = (1 - t^3)^{-1}$. Usually it is much harder to compute the constant coefficient. \triangleleft

4.6.3 Hilbert Series of Invariant Rings of Connected Reductive Groups

Let K be again an arbitrary algebraically closed field of characteristic 0. We will assume that G is connected and reductive. We will give an algebraic derivation of a formula for the Hilbert series of the invariant ring. For details on the notation, see Sect. A.4. We fix a maximal torus $T \subseteq G$, and a Borel subgroup B of G containing T . We define the Weyl group by $W = N_G(T)/Z_G(T)$ where $N_G(T)$ is the normalizer of T in G and $Z_G(T)$ is the centralizer of T in G . The set of roots is denoted by Φ . Let $\alpha_1, \dots, \alpha_r$ be a set of simple roots. We have $\Phi = \Phi_+ \cup \Phi_-$ where Φ_+ and Φ_- are the positive and negative roots, respectively. Let $\lambda_1, \dots, \lambda_r \in X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$ be the fundamental weights, i.e., $\langle \lambda_i, \alpha_j^\vee \rangle = \delta_{i,j}$. For the group of weights $X(T)$ we will use additive notation. The character of T associated to a weight λ will be denoted by z^λ . We define $z_i = z^{\lambda_i}$. Every character of T is a Laurent monomial in z_1, \dots, z_r .

Definition 4.6.8 For a rational representation V of G we define the character χ_G^V of V by $\chi_G^V = \chi_T^V$, where T is a maximal torus of G (see Definition 4.6.2).

Let $\rho = \lambda_1 + \lambda_2 + \dots + \lambda_r$. If $V = \bigoplus_\lambda V_\lambda^{a_\lambda}$ is a rational representation, then the coefficient of $z^{\rho+\lambda}$ in $\sum_{w \in W} \text{sgn}(w) z^{w(\rho)} \chi^V$ is equal to a_λ because of Weyl's Theorem (see Theorem A.5.3). In particular, the coefficient of z^ρ in $\sum_{w \in W} \text{sgn}(w) z^{w(\rho)} \chi^V$ is equal to $a_0 = \dim V^G$.

Suppose that $V = \bigoplus_{d \geq k} V_d$ is a graded vector space and for every d , V_d is a G -module. As in Definition 4.6.4, we define the T -Hilbert series by

$$H_T(V, z_1, \dots, z_r, t) = \sum_{d=k}^{\infty} \chi^{V_d} t^d.$$

From Weyl's Theorem (Theorem A.5.3) it follows that the coefficient of z^ρ in

$$\sum_{w \in W} \operatorname{sgn}(w) z^{w(\rho)} H_T(V, z_1, \dots, z_r, t)$$

is equal to $\sum_{d=k}^{\infty} \dim V_d^G t^d = H(V^G, t)$.

Suppose that V is a rational representation of G . The action of $T \subset G$ on V^* is diagonal for some choice of basis. Suppose that the action of T on V^* is given by the matrix

$$\begin{pmatrix} m_1(z) & 0 & \cdots & 0 \\ 0 & m_2(z) & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & m_n(z) \end{pmatrix},$$

where $m_1(z), \dots, m_n(z)$ are Laurent monomials in z_1, \dots, z_r . As in (4.6.8), we have

$$H_T(K[V], z_1, \dots, z_r, t) = \frac{1}{(1 - m_1(z)t)(1 - m_2(z)t) \cdots (1 - m_n(z)t)}.$$

It follows that $H(K[V]^G, t)$ is the coefficient of z^ρ (as series in z_1, \dots, z_r with coefficients in $K(t)$) in

$$\frac{\sum_{w \in W} \operatorname{sgn}(w) z^{w(\rho)}}{(1 - m_1(z)t)(1 - m_2(z)t) \cdots (1 - m_n(z)t)}$$

or the coefficient of $z^0 = 1$ in

$$\frac{z^{-\rho} \sum_{w \in W} \operatorname{sgn}(w) z^{w(\rho)}}{(1 - m_1(z)t)(1 - m_2(z)t) \cdots (1 - m_n(z)t)}.$$

If we use the identity $\sum_{w \in W} \operatorname{sgn}(w) z^{w(\rho)} = z^\rho \prod_{\alpha \in \phi^+} (1 - z^{-\alpha})$ (Humphreys [12, 24.1 Lemma A, 24.3 Lemma]), then the next Corollary follows. This Corollary is a reformulation of Weyl's integral formula for Hilbert series (see Bröcker and tom Dieck [19]).

Corollary 4.6.9 *The Hilbert series $H(K[V]^G, t)$ is the coefficient of 1 (as series in z_1, \dots, z_r with coefficients in $K(t)$) of*

$$\frac{\prod_{\alpha \in \phi^+} (1 - z^{-\alpha})}{(1 - m_1(z)t)(1 - m_2(z)t) \cdots (1 - m_n(z)t)}. \quad (4.6.10)$$

Remark 4.6.10 In (4.6.10), if G is semisimple and we replace z_i by z_i^{-1} for all i , then $m_1(z), \dots, m_n(z)$ will just be permuted. Hence we also obtain that $H(K[V]^G, t)$

is the coefficient of 1 in

$$\frac{\prod_{\alpha \in \Phi^+} (1 - z^\alpha)}{(1 - m_1(z)t)(1 - m_2(z)t) \cdots (1 - m_n(z)t)}. \quad (4.6.11)$$

△

Example 4.6.11 Let $G = \mathrm{SL}_2$ act on the binary forms V_d . In this case $\Phi = \{\alpha_1, -\alpha_1\}$ and $\Phi^+ = \{\alpha_1\}$. We have $\alpha_1 = 2\lambda_1$. The weights appearing in V_d are $d\lambda_1, (d-2)\lambda_1, \dots, -d\lambda_1$. So we get that the Hilbert series $H(K[V_d]^{\mathrm{SL}_2}, t)$ is equal to the coefficient of $z^0 = 1$ in

$$\frac{(1 - z^2)}{(1 - z^d t)(1 - z^{d-2} t) \cdots (1 - z^{-d} t)}.$$

This is equivalent to the formula in Example 4.6.1 because $\int_{S^1} z^n dz$ is equal to 0 if $n \neq -1$ and equal to $2\pi i$ if $n = -1$. △

Example 4.6.12 Suppose that $G = \mathrm{SL}_3$ and let V be the adjoint representation. Let T be the set of diagonal matrices in SL_3 . This is a maximal torus. Let λ_1, λ_2 the two fundamental weights and let α_1, α_2 be the simple roots. Then $\alpha_1 = 2\lambda_1 - \lambda_2$ and $\alpha_2 = 2\lambda_2 - \lambda_1$. The set of roots is

$$\Phi = \{\alpha_1, \alpha_2, \alpha_1 + \alpha_2, -\alpha_1, -\alpha_2, -\alpha_1 - \alpha_2\}.$$

The weights appearing in V are all roots α (all with multiplicity 1) and 0 (which has multiplicity 2). So the weights appearing in V are

$$0, 0, 2\lambda_1 - \lambda_2, 2\lambda_2 - \lambda_1, \lambda_1 + \lambda_2, \lambda_2 - 2\lambda_1, \lambda_1 - 2\lambda_2, -\lambda_1 - \lambda_2.$$

Now $H(K[V]^{\mathrm{SL}_3}, t)$ is the coefficient of $z_1^0 z_2^0$ in

$$\frac{(1 - z_1^2 z_2^{-1})(1 - z_1^{-1} z_2^2)(1 - z_1 z_2)}{(1 - t)^2 (1 - z_1^2 z_2^{-1} t)(1 - z_1^{-1} z_2^2 t)(1 - z_1 z_2 t)(1 - z_1^{-2} z_2 t)(1 - z_1 z_2^{-2} t)(1 - z_1^{-1} z_2^{-1} t)}.$$

△

In the next section, we will show how the residue theorem can be used to compute the Hilbert series of an invariant ring. In Broer [20] an alternative method can be found.

4.6.4 Hilbert Series and the Residue Theorem

We will first briefly recall the Residue Theorem in complex function theory. This theorem can be applied to compute the Hilbert series of invariant rings.

Suppose that $f(z)$ is a meromorphic function on \mathbb{C} . If $a \in \mathbb{C}$, then f can be written as a Laurent series around $z = a$.

$$f(z) = \sum_{i=-d}^{\infty} c_i(z-a)^i.$$

If $d > 0$ and $c_{-d} \neq 0$, then f has a pole at $z = a$ and the pole order is d . The **residue** of f at $z = a$ is denoted by $\text{res}(f, a)$ and defined by

$$\text{res}(f, a) = c_{-1}.$$

If the pole order of f is 1, then the residue can be computed by

$$\text{res}(f, a) = \lim_{z \rightarrow a} (z-a)f(z).$$

Suppose D that $\gamma : [0, 1] \rightarrow \mathbb{C}$ is a smooth curve. The integral over the curve γ is defined by

$$\int_{\gamma} f(z) dz = \int_0^1 f(\gamma(t))\gamma'(t) dt.$$

Let $\gamma : [0, 1] \rightarrow \mathbb{C}$ be defined by $\gamma(t) = e^{2\pi it}$. Then $\gamma([0, 1])$ is the unit circle. For $n \in \mathbb{Z}$ we have

$$\int_{\gamma} z^n dz = \int_0^1 e^{2\pi nit} (2\pi i) e^{2\pi it} dt = 2\pi i \int_0^1 e^{2\pi(n+1)it} dt,$$

which is 0 if $n \neq -1$ and equal to $2\pi i$ if $n = -1$.

Theorem 4.6.13 (Residue Theorem) *Suppose that D is a connected, simply connected compact region in \mathbb{C} whose border is ∂D , and $\gamma : [0, 1] \rightarrow \mathbb{C}$ is a smooth curve such that $\gamma([0, 1]) = \partial D$, $\gamma(0) = \gamma(1)$ and γ circles around D exactly once in counterclockwise direction. Assume that f is a meromorphic function on \mathbb{C} with no poles in ∂D . Then we have*

$$\frac{1}{2\pi i} \int_{\gamma} f(z) dz = \sum_{a \in D} \text{res}(f, a).$$

There are only finitely many points in the compact region D such that f has nonzero residue there.

Example 4.6.14 Let $T = \mathbb{G}_m$ be the one-dimensional torus acting on a 3-dimensional space V by the matrix

$$\rho = \begin{pmatrix} z & 0 & 0 \\ 0 & z & 0 \\ 0 & 0 & z^{-2} \end{pmatrix}.$$

The action of \mathbb{G}_m on V^* is given by

$$\begin{pmatrix} z^{-1} & 0 & 0 \\ 0 & z^{-1} & 0 \\ 0 & 0 & z^2 \end{pmatrix}.$$

So we get

$$H_T(K[V], z, t) = \frac{1}{(1 - z^{-1}t)^2(1 - z^2t)}. \quad (4.6.12)$$

For the Hilbert series to converge, we need that $|z^{-1}t| < 1$ and $|z^2t| < 1$. We will assume that $|z| = 1$ and $|t| < 1$. To find the coefficient of z^0 , we divide (4.6.12) by $2\pi iz$ and integrate over the unit circle S^1 in \mathbb{C} (counterclockwise). We obtain

$$H(K[V]^{\mathbb{G}_m}, t) = \frac{1}{2\pi i} \int_{S^1} \frac{dz}{z(1 - z^{-1}t)^2(1 - z^2t)}. \quad (4.6.13)$$

By the Residue Theorem, (4.6.13) is equal to

$$\frac{1}{2\pi i} \int_{S^1} f(z) dz = \sum_{a \in D^1} \text{res}(f(z), a), \quad (4.6.14)$$

where D^1 is the unit disk and $f(z) = z^{-1}(1 - z^{-1}t)^{-2}(1 - z^2t)^{-1}$. The only poles of $f(z)$ are $z = t$ and $z = \pm t^{-1/2}$. Since $|t| < 1$, the only pole in the unit disk is $z = t$. We will compute the residue. We have

$$\frac{1}{z(1 - z^{-1}t)^2(1 - z^2t)} = \frac{1}{(z - t)^2} \frac{z}{1 - z^2t}. \quad (4.6.15)$$

The power series of $g(z) = z/(1 - z^2t)$ around $z = t$ gives

$$g(z) = g(t) + g'(t)(z - t) + \frac{g''(t)(z - t)^2}{2} + \dots = \frac{t}{1 - t^3} + \frac{1 + t^3}{(1 - t^3)^2}(z - t) + \dots \quad (4.6.16)$$

$H(K[V]^{\mathbb{G}_m}, t)$ is the residue of

$$\frac{1}{z(1-z^{-1}t)^2(1-z^2t)} = \frac{g(z)}{(z-t)^2}$$

at $z = t$ and from (4.6.16) it follows that this is equal to

$$\frac{1+t^3}{(1-t^3)^2}.$$

△

Example 4.6.15 Let again $G = \mathrm{SL}_2$ be acting on the binary forms V_d . By Example 4.6.11, the Hilbert series $H(K[V_d]^{\mathrm{SL}_2}, t)$ of the invariant ring is the constant coefficient of

$$\frac{(1-z^2)}{(1-z^dt)(1-z^{d-2}t)\cdots(1-z^{-d}t)},$$

so

$$H(K[V_d]^{\mathrm{SL}_2}, t) = \frac{1}{2\pi i} \int_{S^1} \frac{(1-z^2) dz}{z(1-z^dt)(1-z^{d-2}t)\cdots(1-z^{-d}t)}. \quad (4.6.17)$$

In this formula, we assume that $|t| < 1$.

From the Residue Theorem, it follows that (4.6.17) is equal to

$$\sum_{x \in D^1} \mathrm{res}(f_d, x),$$

where

$$f_d(t, z) = \frac{(1-z^2)}{z(1-z^dt)(1-z^{d-2}t)\cdots(1-z^{-d}t)}$$

and x runs through all the poles of f_d in the unit disk D^1 . The poles of f_d in the unit disk are exactly $\zeta_{d-2j}^k t^{1/(d-2j)}$ where $0 \leq j < d/2$, $0 \leq k < d-2j$ and ζ_p is a primitive p -th root of unity.

Let us consider $d = 1$. Then we have

$$f_1(t, z) = \frac{1-z^2}{z(1-zt)(1-z^{-1}t)} = \frac{1-z^2}{(1-zt)(z-t)}.$$

Now f_1 has a pole at $z = t$. The pole at $z = t^{-1}$ lies outside the unit disk because $|t| < 1$. Let us compute the residue.

$$\mathrm{res}(f_1, t) = \lim_{z \rightarrow t} \frac{1-z^2}{1-zt} = 1.$$

It follows that $H(K[V_1]^{\mathrm{SL}_2}, t) = 1$. This answer was to be expected, since there are no nontrivial SL_2 -invariant polynomial functions on V_1 .

Let us now take $d = 2$. Then we have

$$f_2(t, z) = \frac{1 - z^2}{z(1 - z^2t)(1 - t)(1 - z^{-2}t)}.$$

The poles of f_2 in the unit disk are $z = \sqrt{t}$ and $z = -\sqrt{t}$. We compute the residues.

$$\begin{aligned} \mathrm{res}(f_2, \sqrt{t}) &= \lim_{z \rightarrow \sqrt{t}} \frac{(1 - z^2)(z - \sqrt{t})}{z(1 - z^2t)(1 - t)z^{-2}(z + \sqrt{t})(z - \sqrt{t})} = \\ &= \frac{(1 - t)}{\sqrt{t}(1 - t^2)(1 - t)t^{-1}(2\sqrt{t})} = \frac{1}{2(1 - t^2)}. \end{aligned} \quad (4.6.18)$$

In a similar way

$$\mathrm{res}(f_2, -\sqrt{t}) = \frac{1}{2(1 - t^2)},$$

so

$$H(K[V_2]^{\mathrm{SL}_2}, t) = \frac{1}{2(1 - t^2)} + \frac{1}{2(1 - t^2)} = \frac{1}{1 - t^2}.$$

Indeed, $K[V_2]^{\mathrm{SL}_2}$ is a polynomial ring in one variable of degree 2, namely the discriminant. Below is a table of the Hilbert series of $K[V_d]^{\mathrm{SL}_2}$ for $d = 1, 2, \dots, 8$.

d	$H(K[V_d]^{\mathrm{SL}_2}, t)$
1	1
2	$\frac{1}{1 - t^2}$
3	$\frac{1}{1 - t^4}$
4	$\frac{1}{(1 - t^2)(1 - t^3)}$
5	$\frac{1}{1 + t^{18}}$
6	$\frac{(1 - t^4)(1 - t^8)(1 - t^{12})}{1 + t^{15}}$
7	$\frac{(1 - t^2)(1 - t^4)(1 - t^6)(1 - t^{10})}{f_7(t)}$
8	$\frac{(1 - t^4)(1 - t^6)(1 - t^8)(1 - t^{10})(1 - t^{12})}{1 + t^8 + t^9 + t^{10} + t^{18}}$
	$\frac{(1 - t^2)(1 - t^3)(1 - t^4)(1 - t^5)(1 - t^6)(1 - t^7)}{(1 - t^2)(1 - t^3)(1 - t^4)(1 - t^5)(1 - t^6)(1 - t^7)}$

with

$$f_7(t) = t^{32} - t^{26} + 2t^{24} - t^{22} + 5t^{20} + 2t^{18} + 6t^{16} + 2t^{14} + 5t^{12} - t^{10} + 2t^8 - t^6 + 1.$$

△

Remark 4.6.16 For degree at most 16 some explicit formulas of Hilbert series for binary forms were given in Cohen and Brouwer [21]. Some computations of Hilbert series of the invariant ring for binary forms up to a high degree were done by Littelmann and Procesi [22], who used a formula in Springer [18]. If $d = 4l$, then one can prove (see Littelmann and Procesi [22]) that

$$H(K[V_d]^{\mathrm{SL}_2}, t) = \frac{a(t)}{(1-t^2)(1-t^3)\cdots(t^{d-1}-1)},$$

where $a(t)$ is a polynomial in t with integer coefficients. It was conjectured by Dixmier [23] that $a(t)$ has nonnegative coefficients. Moreover, it was conjectured that there exists a homogeneous system of invariants f_2, \dots, f_{d-1} where f_i is of degree i . Notice that this automatically implies that $a(t)$ has nonnegative coefficients, because $K[V_d]^{\mathrm{SL}_2}$ is a free $K[f_2, \dots, f_{d-1}]$ -module. □

Remark 4.6.17 The *degree* of the invariant ring $K[V_d]^{\mathrm{SL}_2}$ is defined by (see Definition 1.4.7)

$$\deg(K[V_d]^{\mathrm{SL}_2}) = \lim_{t \rightarrow 1} (1-t)^{d-2} H(K[V_d]^{\mathrm{SL}_2}, t).$$

If f_1, \dots, f_{d-2} is a homogeneous system of parameters with $e_i := \deg(f_i)$ for all i , then the invariant ring $K[V_d]^{\mathrm{SL}_2}$ is a *free* module over $K[f_1, \dots, f_{d-2}]$ because $K[V_d]^{\mathrm{SL}_2}$ is Cohen-Macaulay (see Theorem 2.6.5 and Proposition 2.6.3). We have a Hironaka decomposition

$$K[V_d]^{\mathrm{SL}_2} = Rh_1 \oplus Rh_2 \oplus \cdots \oplus Rh_l,$$

where $R = K[f_1, \dots, f_{d-2}]$, with h_1, \dots, h_l homogeneous invariants. We have $\deg(R) = (e_1 e_2 \cdots e_{d-2})^{-1}$ (see Example 1.4.8) and

$$\deg(K[V_d]^{\mathrm{SL}_2}) = \frac{l}{e_1 e_2 \cdots e_{d-2}}.$$

If we can bound the degree of the invariant ring, then we can estimate the number of secondary invariants. There is a remarkable formula for $\deg(K[V_d]^{\mathrm{SL}_2})$ proven by Hilbert [24]. If d is odd, then

$$\deg(K[V_d]^{\mathrm{SL}_2}) = -\frac{1}{4} \frac{1}{d!} \sum_{i=0}^{\frac{d-1}{2}} (-1)^i \binom{d}{i} \left(\frac{d}{2} - i\right)^{d-3},$$

and if d is even, then

$$\deg(K[V_d]^{\mathrm{SL}_2}) = -\frac{1}{2} \frac{1}{d!} \sum_{i=0}^{\frac{d}{2}-1} (-1)^i \binom{d}{i} \left(\frac{d}{2} - i\right)^{d-3}.$$

□

The method with the Residue Theorem also works if the maximal torus of G has dimension ≥ 2 . Let us start with a rational function $f \in \mathbb{C}(z_1, \dots, z_r, t)$. We make the following assumptions.

- (a) f can be written as a power series in t with coefficients in the ring of Laurent polynomials $\mathbb{C}[z_1, \dots, z_r, z_1^{-1}, \dots, z_r^{-1}]$;
- (b) f can be written as a quotient g/h where g is a Laurent polynomial in z_1, \dots, z_r, t and $h = \prod_{i=1}^l (1 - m_i t^{d_i})$ where m_i is a Laurent monomial in z_1, \dots, z_r and d_i is a positive integer for $i = 1, \dots, r$.

If V is a representation of a torus T , then the T -Hilbert series of $K[V]$ satisfies the two conditions above.

Proposition 4.6.18 *Assume that f satisfies the two conditions above. Write f as a power series in t with coefficients in $\mathbb{C}[z_1, \dots, z_r, z_1^{-1}, \dots, z_r^{-1}]$ and let f_0 be the coefficient of z_r^0 . Then f_0 also satisfies the two conditions above.*

Proof Clearly f_0 is a power series in t with coefficients in $\mathbb{C}[z_1, \dots, z_{r-1}, z_1^{-1}, \dots, z_{r-1}^{-1}]$.

The power series of f in t converge for $|z_1| = |z_2| = \dots = |z_r| = 1$ and $|t| < 1$. The coefficient of f_0 is obtained by dividing f by $2\pi iz_r$ and integrating z_r over the unit circle (counterclockwise):

$$f_0 = \frac{1}{2\pi i} \int_{S^1} \frac{f(z_1, \dots, z_r, t)}{z_r} dz_r.$$

By the Residue Theorem this is equal to

$$\sum_{a \in D^1} \operatorname{res}(f, a),$$

where D^1 is the unit disk and f is seen as a function in z_r . All poles have the form

$$z_r = \zeta_d^i (z_1^{b_1} z_2^{b_2} \cdots z_{r-1}^{b_{r-1}} t^c)^{1/d}$$

with $b_1, \dots, b_{r-1}, c, d \in \mathbb{Z}$, ζ_d a primitive d -th root of unity. We may assume that the greatest common divisor of $b_1, \dots, b_{r-1}, c, d$ is 1 and that $0 \leq i < d$. Put

$$a_i = \zeta_d^i (z_1^{b_1} z_2^{b_2} \cdots z_{r-1}^{b_{r-1}} t^c)^{1/d}.$$

Suppose that the pole order at $z_r = a_i$ is equal to k . Then

$$\text{res}(f, a_i) = \frac{1}{(k-1)!} \left(\frac{d}{dz_r} \right)^{k-1} (z_r - a_i)^k f(z_1, \dots, z_r) \Big|_{z_r=a_i}.$$

From this, it is clear that $\text{res}(f, a_i)$ can be written as p_i/q with

$$p_i \in \mathbb{C}[z_1, \dots, z_{r-1}, z_1^{-1}, \dots, z_{r-1}^{-1}, t, t^{-1}, a_i, a_i^{-1}]$$

and $q = \prod_{j=1}^m (1 - u_j)$ with u_j a Laurent monomial in $z_1, \dots, z_{r-1}, t, a_i$ for all j . Notice that

$$\frac{1}{1 - u_j} = \frac{1 + u_j + \dots + u_j^{d-1}}{1 - u_j^d}.$$

This shows that without loss of generality we may assume that u_j is a Laurent monomial in z_1, \dots, z_{r-1}, t . It follows that u_j and $q = \prod_{j=1}^m (1 - u_j)$ do not depend on i . We have

$$\text{Res}(f, a_0) + \text{Res}(f, a_1) + \dots + \text{Res}(f, a_{d-1}) = \frac{p_0 + p_1 + \dots + p_{d-1}}{q}.$$

Now $p_0 + \dots + p_{d-1}$ is a Laurent polynomial in $z_1, z_2, \dots, z_{r-1}, t$. It follows that

$$f_0 = \sum_{a \in D^1} \text{Res}(f, a) = \frac{g'}{h'},$$

where g' is a Laurent polynomial in z_1, \dots, z_{r-1}, t and $h' = \prod_{i=1}^r (1 - m'_i t^{d'_i})$, where the m'_i are Laurent monomials in z_1, \dots, z_{r-1} and all $d'_i \in \mathbb{Z}$. We may assume that all $d'_i \geq 0$ because

$$\frac{1}{1 - m'_i t^{d'_i}} = -\frac{(m'_i)^{-1} t^{-d'_i}}{1 - (m'_i)^{-1} t^{-d'_i}}.$$

We know that for $|z_1| = |z_2| = \dots = |z_{r-1}| = 1$ and $|t| < 1$ the power series for f_0 converges. In particular f_0 has no poles. This shows that $d'_i > 0$ for all i . \square

Remark 4.6.19 From Theorem 4.6.13, Corollaries 4.6.6 and 4.6.9 follows that the Hilbert series of $K[V]^G$ can be computed using iterated applications of the Residue Theorem. \triangleleft

Example 4.6.20 Let $G = \text{SL}_3$ and suppose that V is the adjoint representation. From Example 4.6.12 it follows that the Hilbert series of the invariant ring

$H(K[V]^{\mathrm{SL}_3}, t)$ is the coefficient of $z_1^0 z_2^0$ in

$$\begin{aligned} f(z_1, z_2, t) := & (1 - z_1^2 z_2^{-1})(1 - z_1^{-1} z_2^2)(1 - z_1 z_2) / \\ & ((1-t)^2(1-z_1^2 z_2^{-1}t)(1-z_1^{-1} z_2^2t)(1-z_1 z_2 t)(1-z_1^{-2} z_2 t) \cdot \\ & (1-z_1 z_2^{-2} t)(1-z_1^{-1} z_2^{-1} t)). \end{aligned}$$

We assume that $|z_1| = 1$ and $|t| < 1$. The poles of $f z_2^{-1}$ (as a function in z_2) inside the unit disk are $z_2 = z_1^2 t$, $z_2 = \pm\sqrt{z_1 t}$ and $z_2 = z_1^{-1} t$. We will compute the residues:

$$\begin{aligned} \mathrm{res}(z_2^{-1} f, z_1^2 t) = & \\ & \frac{z_1^{-2} t^{-1} (1-t^{-1})(1-z_1^3 t^2)(1-z_1^3 t)}{(1-t)^2(z_1^2 t)^{-1}(1-z_1^3 t^3)(1-z_1^3 t^2)(1-t^2)(1-z_1^{-3} t^{-1})(1-z_1^{-3})} = \\ & = \frac{-z_1^6}{(1-t)(1-z_1^3 t^3)(1-t^2)(1-z_1^3)}, \quad (4.6.19) \end{aligned}$$

$$\begin{aligned} \mathrm{res}(z_2^{-1} f, \sqrt{z_1 t}) = & z_1^{-1/2} t^{-1/2} (1-z_1^{3/2} t^{-1/2})(1-t)(1-z_1^{3/2} t^{1/2}) / \\ & \left((1-t)^2 (1-z_1^{3/2} t^{1/2})(1-t^2)(1-z_1^{3/2} t^{3/2})(1-z_1^{-3/2} t^{3/2}) \cdot \right. \\ & \left. (2z_1^{-1/2} t^{-1/2})(1-z_1^{-3/2} t^{1/2}) \right) = \\ & = \frac{-z_1^{3/2} t^{-1/2}}{2(1-t)(1-t^2)(1-z_1^{3/2} t^{3/2})(1-z_1^{-3/2} t^{3/2})} = \\ & = \frac{-z_1^{3/2} t^{-1/2} (1+z_1^{3/2} t^{3/2})(1+z_1^{-3/2} t^{3/2})}{2(1-t)(1-t^2)(1-z_1^3 t^3)(1-z_1^{-3} t^3)} = \\ & = \frac{-z_1^{3/2} t^{-1/2} - z_1^3 t - t + z_1^{3/2} t^{5/2}}{2(1-t)(1-t^2)(1-z_1^3 t^3)(1-z_1^{-3} t^3)}. \quad (4.6.20) \end{aligned}$$

Similarly, we have

$$\mathrm{res}(z_2^{-1} f, -\sqrt{z_1 t}) = \frac{z_1^{3/2} t^{-1/2} - z_1^3 t - t + z_1^{3/2} t^{5/2}}{2(1-t)(1-t^2)(1-z_1^3 t^3)(1-z_1^{-3} t^3)}$$

and

$$\mathrm{res}(z_2^{-1} f, \sqrt{z_1 t}) + \mathrm{res}(z_2^{-1} f, -\sqrt{z_1 t}) = \frac{-z_1^3 t - t}{(1-t)(1-t^2)(1-z_1^3 t^3)(1-z_1^{-3} t^3)}.$$

Furthermore we have

$$\begin{aligned} \text{res}(z_2^{-1}f, z_1^{-1}t) &= \\ \frac{z_1 t^{-1} (1 - z_1^3 t^{-1}) (1 - z_1^{-3} t^2) (1 - t)}{(1 - t)^2 (1 - z_1^3) (1 - z_1^{-3} t^3) (1 - t^2) (1 - z_1^{-3} t^2) (1 - z_1^3 t^{-1}) (z_1 t^{-1})} &= \\ \frac{1}{(1 - t) (1 - z_1^3) (1 - z_1^{-3} t^3) (1 - t^2)}. & \end{aligned} \quad (4.6.21)$$

It follows that

$$\begin{aligned} \text{res}(z_2^{-1}f, z_1^{-1}t) + \text{res}(z_2^{-1}f, z_1^2 t) &= \\ \frac{(1 - z_1^3 t^3) - z_1^6 (1 - z_1^{-3} t^3)}{(1 - t) (1 - z_1^3) (1 - z_1^{-3} t^3) (1 - t^2) (1 - z_1^3 t^3)} &= \\ \frac{1 - z_1^6}{(1 - t) (1 - z_1^3) (1 - z_1^{-3} t^3) (1 - t^2) (1 - z_1^3 t^3)} &= \\ \frac{1 + z_1^3}{(1 - t) (1 - z_1^{-3} t^3) (1 - t^2) (1 - z_1^3 t^3)}. & \end{aligned} \quad (4.6.22)$$

So the sum of the four residues is

$$g := \frac{1 + z_1^3 - z_1^3 t - t}{(1 - t) (1 - z_1^{-3} t^3) (1 - t^2) (1 - z_1^3 t^3)}.$$

So g is the coefficient of z_2^0 in f . The coefficient of z_1^0 in g is equal to the Hilbert series $H(K[V]^{\mathrm{SL}_3}, t)$. Now g has poles at $z = \xi^j t$ where ξ is a third root of unity and $0 \leq j \leq 2$. We compute the residues

$$\text{res}(z_1^{-1}g, \xi^j t) = \frac{\xi^{-j} t^{-1} (1 + t^3 - t^4 - t)}{(1 - t) (3\xi^{-j} t^{-1}) (1 - t^2) (1 - t^6)} = \frac{1}{3(1 - t^2)(1 - t^3)}.$$

The Hilbert series of $K[V]^{\mathrm{SL}_3}$ is the sum of the residues

$$\text{res}(z_1^{-1}g, t) + \text{res}(z_1^{-1}g, \xi t) + \text{res}(z_1^{-1}g, \xi^2 t) = \frac{1}{(1 - t^2)(1 - t^3)}.$$

□

4.7 Degree Bounds for Invariants

Suppose that G is a linearly reductive group and V is a rational finite dimensional representation of G . We have defined $\beta(K[V]^G)$ to be the smallest integer N such that all invariants of degree $\leq N$ will generate $K[V]^G$. The goal of this section is to find explicit upper bounds for $\beta(K[V]^G)$. A first step in this direction was done by Hilbert [24], who gave a constructive method for finding generators of the invariant ring using a homogeneous system of parameters of the invariant ring. However, Hilbert could not give an explicit upper bound for $\beta(K[V]^G)$. By generalizing Hilbert's constructive method and combining it with the Cohen-Macaulay property (see Theorem 2.6.5) and an estimate of the degree of the Hilbert series (see Kempf [25]), Popov found an explicit upper bound for $\beta(K[V]^G)$ (see Remark 4.7.3 if G is connected, semisimple and the base field K has characteristic 0). As shown in Derksen [26], an adaption of the method of Hilbert and Popov will give a much better upper bound. We will derive that degree bound in this section.

We already showed in Corollary 2.7.3 that whenever $f_1, \dots, f_r \in K[V]^G$ is a homogeneous system of parameters, then

$$\beta(K[V]^G) \leq d_1 + d_2 + \dots + d_r - r, \quad (4.7.1)$$

where $d_i := \deg(f_i)$. Recall that $f_1, \dots, f_r \in K[V]^G$ is a homogeneous system of parameters if and only if f_1, \dots, f_r are algebraically independent and $K[V]^G$ is finite (as a module) over $K[f_1, \dots, f_r]$ (see Definition 2.5.6).

Definition 4.7.1 If $R = \bigoplus_{d \geq 0} R_d$ is a graded K -algebra, we define the constant $\gamma(R)$ as the smallest integer d such that there exist homogeneous $f_1, \dots, f_l \in R$ with $\deg(f_i) \leq d$ for all i and R is integral over $K[f_1, \dots, f_l]$.

Remark 4.7.2 In view of Lemma 2.5.5, the property that $K[V]^G$ is integral over $K[f_1, \dots, f_l]$ is equivalent to $\mathcal{V}(f_1, \dots, f_l) = \mathcal{N}_V$ where \mathcal{N}_V is Hilbert's nullcone (see Definition 2.5.1). So we may say that $\gamma(K[V]^G)$ is the smallest integer d such that there exist homogeneous $f_1, \dots, f_l \in K[V]^G$ such that $\mathcal{V}(f_1, \dots, f_l) = \mathcal{N}_V$. \triangleleft

Remark 4.7.3 Popov [27, 28] gave an explicit upper bound for $\beta(K[V]^G)$ as follows. There exist homogeneous g_1, \dots, g_l such that $K[V]^G$ is finite over $K[g_1, \dots, g_l]$ and $\deg(g_i) = d_i \leq \gamma(K[V]^G)$ for all i . Let $d = \text{lcm}(d_1, \dots, d_l)$ where lcm is the least common multiple, and define $g'_i = g_i^{d/d_i}$ for all i . $K[V]^G$ is finite over $S = K[g'_1, g'_2, \dots, g'_l]$. By the Noether Normalization Lemma, we can find linear combinations f_1, \dots, f_r of g'_1, \dots, g'_l such that f_1, \dots, f_r form a homogeneous system of parameters for S and also for $K[V]^G$. From (4.7.1) it follows that

$$\beta(K[V]^G) \leq rd - r \leq nd \leq n \text{lcm}(1, 2, \dots, \gamma(K[V]^G)).$$

Hilbert found upper bounds for $\gamma(K[V]^G)$ in the case $G = \text{SL}_n$. This bound was generalized by Popov to arbitrary connected semi-simple groups G . Explicit upper bounds for $\gamma(K[V]^G)$ can be found in Popov's cited papers. For a fixed semi-simple

group G , $\gamma(K[V]^G)$ is bounded by a polynomial in n , the dimension of V (see Sect. 4.7.1). \triangleleft

We will give another degree bound for $\beta(K[V]^G)$ in terms of $\gamma(K[V]^G)$. In Sect. 4.7.1 we will study the constant $\gamma(K[V]^G)$ and give upper bounds for it.

Theorem 4.7.4 *We have*

$$\beta(K[V]^G) \leq \max(2, \frac{3}{8}r(\gamma(K[V]^G))^2),$$

where $r = \dim(K[V]^G)$ is the Krull dimension.

By definition there exist homogeneous $f_1, \dots, f_l \in K[V]^G$ such that $K[V]^G$ is finite over $K[f_1, \dots, f_l]$ and $\mathcal{V}(f_1, \dots, f_l) = \mathcal{N}_V$. If $l = r$ where $r := \dim(K[V]^G)$, then f_1, \dots, f_r is a homogeneous system of parameters and we have a good degree bound (4.7.1). Suppose that $l > r$, i.e., the number of invariants is too large compared to $r = \dim(K[V]^G)$. In the approach of Hilbert and Popov, we would use the Noether Normalization Lemma to obtain a homogeneous system of parameters (see Remark 4.7.3). However, usually the proof of Corollary 2.5.8 would give us a homogeneous system of parameters of very high degree d because d is the least common multiple of d_1, \dots, d_l where $d_i := \deg(f_i)$. We will use a method which avoids the Noether Normalization Lemma. The idea is to construct from f_1, \dots, f_l a homogeneous system of parameters of $K[V']^G$ where V' is the direct sum of V and a number of copies of the trivial representation.

Let V be an n -dimensional rational representation of a linearly reductive group G . We identify $K[V]$ with the polynomial ring $K[x_1, \dots, x_n]$. Let us consider the representation $V \oplus K$ where K stands for the trivial representation of G . Then $K[V \oplus K] \cong K[x_1, \dots, x_n, y]$ and $K[V \oplus K]^G = K[V]^G[y]$.

Lemma 4.7.5 *Suppose that $f_1, \dots, f_l \in K[V]^G$ are homogeneous invariants with*

$$\mathcal{V}(f_1, \dots, f_l) = \mathcal{N}_V.$$

If $l > r := \dim(K[V]^G)$, then we can find homogeneous $g_1, \dots, g_l \in K[V \oplus K]^G$ such that

- (a) $g_i(x_1, \dots, x_n, 0) = f_i(x_1, \dots, x_n)$ for all i ;
- (b) $\mathcal{V}(g_1, \dots, g_l) = \mathcal{N}_V \times \{0\} \subset V \oplus K$.

Proof Consider the map $F = (f_1, \dots, f_l) : V \rightarrow K^l$. Since $l > \dim(K[V]^G)$, we know that f_1, \dots, f_l are algebraically dependent and the map F is not dominant. We can choose $\alpha = (\alpha_1, \dots, \alpha_l) \in K^l$ which does not lie in the image of F . We define $g_i(x_1, \dots, x_n, y) = f_i(x_1, \dots, x_n) - \alpha_i y^{d_i}$ with $d_i = \deg(f_i)$ for all i . Clearly $\mathcal{N} \times \{0\} \subseteq \mathcal{V}(g_1, \dots, g_l)$. Let us prove the reverse inclusion. Suppose that $(x_1, \dots, x_n, y) \in \mathcal{V}(g_1, \dots, g_l)$. If $y \neq 0$, then

$$\frac{g_i(x_1, \dots, x_n, y)}{y^{d_i}} = g_i\left(\frac{x_1}{y}, \frac{x_2}{y}, \dots, \frac{x_n}{y}, 1\right) = f_i\left(\frac{x_1}{y}, \dots, \frac{x_n}{y}\right) - \alpha_i.$$

This shows that $\alpha = F(x_1/y, \dots, x_n/y)$ which is in contradiction to our assumptions. We conclude that y must be equal to 0, so $g_i(x_1, \dots, x_n, 0) = f_i(x_1, \dots, x_n) = 0$ for all i and this shows that $(x_1, \dots, x_n) \in \mathcal{N}_V$. \square

Corollary 4.7.6 Suppose that $f_1, \dots, f_l \in K[V]^G$ are homogeneous invariants with

$$\mathcal{V}(f_1, \dots, f_l) = \mathcal{N}_V.$$

Let $V' = V \oplus K^{l-r}$ with K the trivial representation and $r = \dim(K[V]^G)$. Then there exists a homogeneous system of parameters $p_1, \dots, p_l \in K[V']^G$ such that

$$p_i(x_1, \dots, x_n, 0, \dots, 0) = f_i(x_1, \dots, x_n)$$

for all i .

Proof We will prove this statement by induction on $l - r$. If $l - r = 0$, then f_1, \dots, f_l is already a homogeneous system of parameters. Suppose that $l > r$. Let $V'' = V \oplus K$. By Lemma 4.7.5 we have $g_1, \dots, g_l \in K[V'']^G$ such that $g_i(x_1, \dots, x_n, 0) = f_i(x_1, \dots, x_n)$ for all i , and $\mathcal{V}(g_1, \dots, g_l) = \mathcal{N}_V \times \{0\} = \mathcal{N}_{V''}$. We have $K[V'']^G \cong K[V]^G[y]$, so $\dim(K[V'']^G) = r + 1$. Since $l - (r + 1) < l - r$ we can apply the induction hypothesis to find p_1, \dots, p_l such that $p_i(x_1, \dots, x_n, 0, \dots, 0) = g_i(x_1, \dots, x_n, 0) = f_i(x_1, \dots, x_n)$ for all i and $\mathcal{V}(p_1, \dots, p_l) = \mathcal{N}_{V'} = \mathcal{N}_{V''} \times \{0\} \subset V'' \oplus K^{l-r-1}$. Now $K[V']^G$ is a finite $K[p_1, \dots, p_l]$ module. We have $\dim(K[V']^G) = \dim(K[V]^G[y_1, \dots, y_{l-r}]) = r + (l - r) = l$, so p_1, \dots, p_l are algebraically independent and therefore they are a homogeneous system of parameters. \square

Corollary 4.7.7 Suppose that $f_1, \dots, f_l \in K[V]^G$ are homogeneous invariants with

$$\mathcal{V}(f_1, \dots, f_l) = \mathcal{N}_V.$$

Then we have

$$\beta(K[V]^G) \leq \max(d_1, d_2, \dots, d_l, d_1 + d_2 + \dots + d_l - l).$$

Proof By Corollary 4.7.6 there exists a homogeneous system of parameters $p_1, \dots, p_l \in K[V']^G$ with $d_i := \deg(p_i)$. It follows from Corollary 2.7.3 that

$$\beta(K[V']^G) \leq \max(d_1, \dots, d_l, d_1 + d_2 + \dots + d_l - l).$$

The inclusion $V \hookrightarrow V'$ induces a surjective ring homomorphisms $K[V'] \rightarrow K[V]$ and a surjective ring homomorphism $K[V']^G \rightarrow K[V]^G$ by Corollary 2.2.8. This shows that $\beta(K[V]^G) \leq \beta(K[V']^G)$. \square

Proof of Theorem 4.7.4 Let us put $\gamma = \gamma(K[V]^G)$. By Remark 4.7.2 there exist homogeneous $f_1, \dots, f_l \in K[V]^G$ such that $\mathcal{V}(f_1, \dots, f_l) = \mathcal{N}_V$ and $d_i \leq \gamma$ where $d_i := \deg(f_i)$. Replacing f_i by some power of itself does not change the zero set $\mathcal{V}(f_1, \dots, f_l)$. Without loss of generality we may assume that $\gamma/2 < d_i \leq \gamma$.

Suppose that $\{h_1, \dots, h_k\} \subset \{f_1, \dots, f_l\}$ is a subset of invariants which are all of the same degree d . By the Noether Normalization Lemma (Lemma 2.5.7) we obtain a homogeneous system of parameters g_1, \dots, g_j of $K[h_1, \dots, h_k]$ where g_i is a linear combination of h_1, \dots, h_k for all i and $j = \dim(K[h_1, \dots, h_k]) \leq r$, since the dimension is given by the transcendence degree. Since $K[h_1, \dots, h_k]$ is finite as a module over $K[g_1, \dots, g_j]$, we can replace h_1, \dots, h_k by g_1, \dots, g_j . This shows that without loss of generality we may assume that for every d , at most r of the invariants f_1, \dots, f_l have degree d .

We have

$$d_1 + \dots + d_l - l = \sum_{i=1}^l (d_i - 1) \leq r \sum_{i=\lceil \frac{\gamma}{2} \rceil}^{\gamma} (i - 1).$$

For even γ the right-hand side is equal to $r(\frac{3}{8}\gamma^2 - \frac{1}{4}\gamma)$ and for odd γ the right-hand side is equal to $r(\frac{3}{8}\gamma^2 - \frac{3}{8})$. In any case we have

$$d_1 + \dots + d_l - l \leq \frac{3}{8}r\gamma^2.$$

We get that

$$\beta(K[V]^G) \leq \max(d_1, \dots, d_l, d_1 + \dots + d_l - l) \leq \max\left(\gamma, \frac{3}{8}r\gamma^2\right).$$

Suppose that $\gamma > \frac{3}{8}r\gamma^2$. If $r = 0$, then $\gamma = 0$ and otherwise it follows that $\gamma < \frac{8}{3}$, so $\gamma \leq 2$. It follows that we always have

$$\beta(K[V]^G) \leq \max\left(2, \frac{3}{8}r\gamma^2\right).$$

□

4.7.1 Degree Bounds for Orbits

Popov [27, 28] gave explicit upper bounds for $\gamma(K[V]^G)$. Hiss improved Popov's bound using ideas of Knop (see Hiss [29]). We will follow Hiss' approach. Suppose that G is a linear algebraic group and V is an n -dimensional representation of G . For linearly reductive groups G we will show the relation between $\gamma(K[V]^G)$ and the degrees of orbits.

Definition 4.7.8 We can view V as a Zariski-open set in $\mathbb{P}^n = \mathbb{P}(V \oplus K)$. If all irreducible components of $X \subset V$ have the same dimension, then we define $\deg(X) = \deg(\bar{X})$ where \bar{X} is the closure of X in \mathbb{P}^n .

Remark 4.7.9 If X is a constructible set (see Hartshorne [30, Exercise II.3.18]) of dimension r , then

$$\deg(X) = \#(X \cap W_1 \cap W_2 \cap \cdots \cap W_r), \quad (4.7.2)$$

where $W_1, W_2, \dots, W_r \subset V$ are hyperplanes in general position. The set H of hyperplanes in V is an algebraic variety. By saying that (4.7.2) holds for W_1, \dots, W_r in general position, we mean that there exists a Zariski open, nonempty subset $U \subset H^r$ such that for all $(W_1, \dots, W_r) \in U$, (4.7.2) is equal to $\deg(X)$.

If W_1, \dots, W_r are not in general position, then

$$\#(X \cap W_1 \cap W_2 \cap \cdots \cap W_r) \leq \deg(X)$$

whenever the left-hand side is finite (see Fulton [31, §12.3]). \triangleleft

Proposition 4.7.10 Suppose that $X \subset V$ is Zariski closed and irreducible. Assume that $\psi : V \rightarrow W$ is a linear map between finite dimensional vector spaces, then

$$\deg(X) \geq \deg(\psi(X)).$$

Proof Let $r = \dim(X)$ and $s = \dim(\psi(X))$. We can choose W_1, \dots, W_s such that

$$\#(\psi(X) \cap W_1 \cap \cdots \cap W_s) = \deg(\psi(X)).$$

For any $y \in \psi(X) \cap W_1 \cap \cdots \cap W_s$, $\psi^{-1}(y) \cap X$ is nonempty, of dimension $r - s$. If we put $U_i := \psi^{-1}(W_i) \subset V$, then

$$X \cap U_1 \cap \cdots \cap U_s = \psi^{-1}(\psi(X) \cap W_1 \cap \cdots \cap W_s) \cap X$$

has at least $\deg(\psi(X))$ connected components.

We can take U_{s+1}, \dots, U_r such that for every connected component S of $(X \cap U_1 \cap \cdots \cap U_s)$, the intersection $S \cap U_{s+1} \cap \cdots \cap U_r$ is finite and nonempty. It follows that

$$\#(X \cap U_1 \cap \cdots \cap U_s \cap U_{s+1} \cap \cdots \cap U_r) \geq \deg(\overline{\psi(X)}).$$

On the other hand, from Remark 4.7.9 it follows that

$$\#(X \cap U_1 \cap \cdots \cap U_s \cap U_{s+1} \cap \cdots \cap U_r) \leq \deg(X).$$

\square

Definition 4.7.11 We define

$$\delta(V) = \max\{\deg(G \cdot v) \mid v \in V \setminus \mathcal{N}_V\},$$

and $\delta(V) = 0$ if $\mathcal{N}_V = V$.

It was anticipated by V. Popov that the number $\delta(V)$ may play an important role. He formulated the problem of the explicit computation of $\delta(V)$ and pointed out the connection to the formula of Kazarnovskii (see Proposition 4.7.18).

Proposition 4.7.12 *If G is linearly reductive, and V is a rational representation, then*

$$\gamma(K[V]^G) \leq \delta(V).$$

Proof We have to show that for every $v \in V \setminus \mathcal{N}_V$ there exists a homogeneous $f \in K[V]^G$ of degree $\leq \delta(V)$ such that $f(v) \neq 0$.

So let us assume that $v \in V \setminus \mathcal{N}_V$. Define $X \subseteq V$ as the Zariski closure of the cone $G \cdot Kv$ and $Y \subset X$ as the Zariski closure of $G \cdot v$. Note that $Y \subsetneq X$ since $v \in \mathcal{N}_V$, so $0 \notin Y$. Hence $\dim(Y) = \dim(X) - 1$. Let $K[X] = K[V]/I(X)$ be the graded coordinate ring of X . Since $K[X]$ is generated in degree 1, we can find linear functions $p_1, \dots, p_{r+1} \in V^*$ such that the images in $K[X]$ form a homogeneous system of parameters in $K[X]$. Define $W := K^{r+1}$ and let $\psi : V \rightarrow W$ be the linear projection defined by (p_1, \dots, p_{r+1}) . The restriction of ψ to X is a finite morphism because p_1, \dots, p_{r+1} is a homogeneous system of parameters.

Now $\psi(Y)$ defines a hypersurface in W . The vanishing ideal $I(\psi(Y)) \subset K[W]$ is generated by some polynomial g . From Proposition 4.7.10 it follows that

$$\deg(g) \leq \deg(\psi(Y)) \leq \deg(Y) \leq \delta(Y).$$

Define $f := g \circ \psi \in K[V]$. Then f is a (nonhomogeneous) polynomial of degree $\leq \delta(V)$ which vanishes on Y and $f(0) \neq 0$. Define $h = \mathcal{R}(f)$ were \mathcal{R} is the Reynolds operator. Notice that h vanishes on Y because $I(Y)$ is G -stable, therefore stable under \mathcal{R} .

Write $h = h_0 + h_1 + \dots + h_{\delta(V)}$ with h_i homogeneous of degree i . Then h_0 is a nonzero constant because $h(0) \neq 0$. Since $h(v) = 0$, we must have $h_i(v) \neq 0$ for some $i > 0$. Since $\deg(h_i) \leq \delta(V)$, we are done. \square

Definition 4.7.13 Let $\rho : G \rightarrow \text{End}(V)$ be the action of G on V . We define $\delta_{\text{gen}}(V) = \deg(\rho(G))$.

Proposition 4.7.14 *Suppose that G is a linearly reductive group and V is a rational representation. We have*

$$\delta(V) \leq \delta_{\text{gen}}(V).$$

Proof Suppose that $v \in V$. We define $\psi : \text{End}(V) \rightarrow V$, $A \mapsto Av$. Then $\overline{\psi(\rho(G))} = \overline{G \cdot v}$. From Proposition 4.7.10 it follows that

$$\deg(\overline{G \cdot v}) \leq \deg(\rho(G)) = \delta_{\text{gen}}(V).$$

\square

Example 4.7.15 If G is finite, then we obtain $\gamma(K[V]^G) \leq |\rho(G)|$. This also follows from Proposition 3.5.2. \triangleleft

We have $\gamma(K[V]^G) \leq \delta(V) \leq \delta_{\text{gen}}(V)$. Using this, we will give a concrete upper bound for $\gamma(K[V]^G)$ in terms of the degrees of the polynomials defining the group G and the representation $\rho : G \rightarrow \text{GL}(V)$. We will assume that the linearly reductive group G is given as in Sect. 4.1.2. So G is embedded in K^l for some l which gives us a surjective homomorphism $K[z_1, \dots, z_l] \rightarrow K[G]$. The representation $\rho : G \rightarrow \text{GL}(V)$ is given by a matrix

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{2,1} & a_{2,2} & \cdots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \cdots & a_{n,n} \end{pmatrix}$$

with $a_{i,j} \in K[z_1, \dots, z_l]$ for all i, j .

Proposition 4.7.16 Suppose that G is a linearly reductive group and V is a rational representation. We have an inequality

$$\gamma(K[V]^G) \leq \delta_{\text{gen}}(V) \leq CA^m,$$

where C is the degree of $G \subset K^l$, $A = \max_{i,j}(\deg(a_{i,j}))$ and $m = \dim \rho(G)$.

Proof We take m hyperplanes in general position in $\text{End}(V)$. Suppose these hyperplanes are given as the zero sets of the functions h_1, \dots, h_m , all of degree 1. If S is the intersection of $h_1 = h_2 = \dots = h_m = 0$ with $\rho(G)$, then by definition $\#S = \delta_{\text{gen}}(V)$. Define $u_i = \rho^*(h_i) = h_i \circ \rho$ for all i . The degree of u_i is at most A for all i . The intersection of $u_1 = u_2 = \dots = u_m = 0$ with $G \subseteq K^l$ has at most CA^m connected components. On the other hand this intersection is equal to $\rho^{-1}(S)$, so it must have at least $\delta_{\text{gen}}(V)$ connected components. \square

Example 4.7.17 We take $G = \text{SL}(W)$ where W is a q -dimensional vector space. Let $V_d = S_d(W)$ be the d -th symmetric power. If we choose a basis of W , we get an embedding of G into the $q \times q$ matrices, which is a q^2 -dimensional space. The coordinate ring of G is given by

$$K[G] = K[\{z_{i,j} \mid 1 \leq i, j \leq q\}] / (\det((z_{i,j})) - 1).$$

We want to apply Proposition 4.7.16. We have $m \leq q^2 - 1$ and $C = q$ is the degree of the determinant polynomial. The action of G on V is given by a matrix $(a_{i,j})$ where all $a_{i,j}$ have degree $\leq d$, therefore $A = d$. By Proposition 4.7.16 we have

$$\gamma(K[V_d]^{\text{SL}_q}) \leq qd^{q^2-1}.$$

Note that $r = \dim K[V_d]^{\mathrm{SL}_q} \leq \dim V_d = \binom{q+d-1}{q-1}$. From Theorem 4.7.4 it follows that

$$\beta(K[V_d]^{\mathrm{SL}_q}) \leq \frac{3}{8} \binom{q+d-1}{q-1} q^2 d^{2q^2-2}.$$

Note that this upper bound depends only polynomially on d . If $q = 2$, we have binary forms of degree d and $\beta(K[V_d]^{\mathrm{SL}_2}) \leq \frac{3}{2}(d+1)d^6$. This bound still seems far from sharp. For $d = 2$, for example, we have $\beta(K[V_d]^{\mathrm{SL}_2}) = 2$ and $\frac{3}{2}(d+1)d^6 = 288$. For ternary forms ($q = 3$) we get $\beta(K[V_d]^{\mathrm{SL}_3}) \leq \frac{27}{8}(d+2)(d+1)d^{18}$. \triangleleft

There also exists an exact formula for $\delta_{\mathrm{gen}}(V)$ which easily follows from a formula of Kazarnovskii which we will explain now (see Kazarnovskij [32] and Brion [33] for a generalization). We will use the notation of Sect. A.4. Suppose that G is a connected reductive group and put $m := \dim G$ and $r := \mathrm{rank } G$. Fix a Borel subgroup $B \subset G$ and $T \subset B$ a maximal torus and denote by $\alpha_1, \alpha_2, \dots, \alpha_\ell$, $\ell = \frac{m-r}{2}$, the positive roots. Let W be the Weyl group and let e_1, e_2, \dots, e_r be the Coxeter exponents, i.e., $e_1 + 1, e_2 + 1, \dots, e_r + 1$ are the degrees of the generating invariants of W . Let $X(T) \cong \mathbb{Z}^r$ be the group of characters of T . For a representation $\rho : G \rightarrow \mathrm{GL}(V)$ we denote by $\mathcal{C}_V \subset E := X(T) \otimes_{\mathbb{Z}} \mathbb{R}$ the convex hull of 0 and the weights of V . On E we use the volume form $d\mathcal{V}$ which is the standard volume form by an isomorphism $E \cong \mathbb{R}^r$ which identifies $X(T)$ with \mathbb{Z}^r . We fix a W -invariant scalar product $\langle \cdot, \cdot \rangle$ on E . We define $\tilde{\alpha}_i = 2\langle \alpha_i, \cdot \rangle / \langle \alpha_i, \alpha_i \rangle \in E^*$ for all i .

Proposition 4.7.18 *If the representation $\rho : G \rightarrow \mathrm{GL}(V)$ has finite kernel, then we have*

$$\delta_{\mathrm{gen}}(V) = \frac{m!}{|W|(e_1!e_2!\cdots e_r!)^2 |\ker(\rho)|} \int_{\mathcal{C}_V} (\tilde{\alpha}_1 \tilde{\alpha}_2 \cdots \tilde{\alpha}_\ell)^2 d\mathcal{V}.$$

Proof This follows from the formula of Kazarnovskii (see Kazarnovskij [32] and Derksen and Kraft [34]). \square

Example 4.7.19 Let V_d be the vector space of binary forms of degree d , on which SL_2 acts. With the notation of Proposition 4.7.18, we have $m = 3$, $r = 1$, $e_1 = 1$, $|W| = 2$. If d is odd, then $|\ker(\rho)| = 1$, so we get

$$\delta_{\mathrm{gen}}(V_d) = 3 \int_{-d}^d x^2 dx = 2d^3,$$

and if d is even, then $\delta_{\mathrm{gen}}(V_d) = d^3$. \triangleleft

4.7.2 Degree Bounds for Tori

In this section we discuss an upper bound for $\beta(K[V]^G)$ in case $G = T$ is a torus. This upper bound was given by Wehlau [35] and is better than the general upper bound given in Sect. 4.7.1.

We will assume that $G = T$ is a torus of dimension r . Let $\rho : T \rightarrow \mathrm{GL}(V)$ be an n -dimensional faithful representation of T . We may assume that the torus acts diagonally, i.e., the representation is given by a diagonal matrix

$$\rho = \begin{pmatrix} \chi_1 & & & 0 \\ & \chi_2 & & \\ & & \ddots & \\ 0 & & & \chi_n \end{pmatrix},$$

where $\chi_1, \chi_2, \dots, \chi_n \in X(T)$ are rational 1-dimensional characters of the torus T . The set of rational 1-dimensional characters $X(T)$ can be identified with \mathbb{Z}^r , and we will identify $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$ with \mathbb{R}^r . On \mathbb{R}^r we have the usual volume form $d\mathcal{V}$. Notice that under all identifications $X(T)$ has covolume 1 in $X(T) \otimes_{\mathbb{Z}} \mathbb{R}$. Let \mathcal{C}_V be the convex hull of χ_1, \dots, χ_n inside $X(T) \otimes \mathbb{R}$.

Theorem 4.7.20 (Wehlau [35]) *With the notation and assumptions above we have*

$$\beta(K[V]^T) \leq \max(n - r - 1, 1)r! \operatorname{vol}(\mathcal{C}_V),$$

where $\operatorname{vol}(\mathcal{C}_V)$ denotes the volume of the polytope \mathcal{C}_V .

Proof Let x_1, \dots, x_n be the coordinate functions, so $K[V] \cong K[x_1, \dots, x_n]$. We can identify a monomial $x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}$ with $(\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$. A T -invariant monomial corresponds to an n -tuple $(\alpha_1, \dots, \alpha_n)$ satisfying

$$\alpha_1 \chi_1 + \alpha_2 \chi_2 + \cdots + \alpha_n \chi_n = 0. \quad (4.7.3)$$

Let $S \subset \mathbb{N}^n$ correspond to the set of all T -invariant monomials. Let \mathbb{Q}_+ be the set of nonnegative rational numbers. Consider the cone $\mathbb{Q}_+ S \subset \mathbb{Q}_+^n$. If $\alpha \in \mathbb{Q}_+^n \setminus \{0\}$, then we call $\mathbb{Q}_+ \alpha$ a ray. A ray $\mathbb{Q}_+ \alpha \subset \mathbb{Q}_+ S$ is called an extremal ray of $\mathbb{Q}_+ S$ if $\alpha = \beta + \gamma$, $\beta, \gamma \in \mathbb{Q}_+ S$ implies that $\beta, \gamma \in \mathbb{Q}_+ \alpha$. Now $\mathbb{Q}_+ S$ is a polyhedral cone, so it has only finitely many extremal rays, say $\ell_1, \ell_2, \dots, \ell_s$. For each i there exists a unique monomial R_i such that $\ell_i \cap \mathbb{N}^n = \mathbb{N} R_i$. This monomial R_i is invariant because $R_i \in \mathbb{Q}_+ S \cap \mathbb{N}^n = S$. Suppose that M is a T -invariant monomial. Since the dimension of $\mathbb{Q}_+ S$ is $n - r$, there exist indices j_1, \dots, j_{n-r} such that M lies in the convex hull of the rays $\ell_{j_1}, \ell_{j_2}, \dots, \ell_{j_{n-r}}$. We can write

$$M = \alpha_1 R_{j_1} + \alpha_2 R_{j_2} + \cdots + \alpha_{n-r} R_{j_{n-r}}$$

with $\alpha_1, \dots, \alpha_{n-r} \in \mathbb{Q}_+$. If we write $\alpha_i = a_i + \gamma_i$ where a_i is a nonnegative integer and $0 \leq \gamma_i < 1$ for all i , then we get

$$M = R_{j_1}^{a_1} R_{j_2}^{a_2} \cdots R_{j_{n-r}}^{a_{n-r}} N,$$

where the degree of N satisfies

$$\begin{aligned} \deg(N) &= \gamma_1 \deg(R_{j_1}) + \gamma_2 \deg(R_{j_2}) + \cdots + \gamma_{n-r} \deg(R_{j_{n-r}}) \leq \\ &\leq (n-r) \max\{\deg(R_i) \mid i = 1, 2, \dots, s\}. \end{aligned}$$

By Ewald and Wessels [36, Theorem 2], N is decomposable into smaller invariant monomials if

$$\gamma_1 + \cdots + \gamma_{n-r} > n - r - 1 \geq 1.$$

It follows that

$$\beta(K[V]^T) \leq \max\{n - r - 1, 1\} \max\{\deg(R_i) \mid i = 1, 2, \dots, s\}.$$

We would like to bound $\deg(R_i)$. After a permutation of the variables we can assume that $R_i = (\mu_1, \dots, \mu_t, 0, 0, \dots, 0)$ with $\mu_1, \dots, \mu_t \in \mathbb{N} \setminus \{0\}$. We claim that the characters $\chi_1, \chi_2, \dots, \chi_t$ span a $(t-1)$ dimensional vector space. If they spanned a space of dimension $< t-1$, then there would be a solution $T = (\tau_1, \dots, \tau_t, 0, \dots, 0) \in \mathbb{Q}^n$ to (4.7.3) independent of R_i and $R_i \pm \epsilon T \in \mathbb{Q}_+ S$ for small ϵ . This contradicts the extremality of the ray ℓ_i . After another permutation of x_{t+1}, \dots, x_n we may assume that $\chi_1, \chi_2, \dots, \chi_{r+1}$ span an r -dimensional vector space. The equations

$$\alpha_1 \chi_1 + \alpha_2 \chi_2 + \cdots + \alpha_{r+1} \chi_{r+1} = \alpha_{r+2} = \cdots = \alpha_n = 0 \quad (4.7.4)$$

have a one-dimensional solution space. By Cramer's rule, we can find a nonzero solution $A = (\alpha_1, \dots, \alpha_{r+1}, 0, \dots, 0)$ to (4.7.4):

$$\begin{aligned} \alpha_i &= (-1)^i \det(\chi_1, \dots, \chi_{i-1}, \chi_{i+1}, \dots, \chi_{r+1}) = \\ &= \pm r! \operatorname{vol}(\mathcal{C}(0, \chi_1, \dots, \chi_{i-1}, \chi_{i+1}, \dots, \chi_{r+1})). \end{aligned}$$

Here \mathcal{C} denotes the convex hull and vol denotes the volume. Since A is a rational (even an integral) multiple of R_i , we obtain

$$\begin{aligned} \deg(R_i) &\leq |\alpha_1| + |\alpha_2| + \cdots + |\alpha_{r+1}| = r! \sum_{i=1}^{r+1} \operatorname{vol}(\mathcal{C}(0, \chi_1, \dots, \widehat{\chi_i}, \dots, \chi_{r+1})) = \\ &= r! \operatorname{vol}(\mathcal{C}(\chi_1, \chi_2, \dots, \chi_{r+1})) \leq r! \operatorname{vol}(\mathcal{C}_V) \end{aligned}$$

so we have

$$\beta(K[V]^T) \leq \max\{n - r - 1, 1\}r! \operatorname{vol}(\mathcal{C}_V).$$

□

4.8 Properties of Invariant Rings

Let K be a field of characteristic 0, and let V be a representation of a linearly reductive group G . Let $\pi : V \rightarrow V//G$ be the quotient map. For finite groups, the ring of invariants is a polynomial ring if and only if G is a generalized reflection group. For infinite linearly reductive groups there is not such a simple answer to the question when the invariant ring is a polynomial ring. In this section we will briefly discuss various properties of invariant rings, interactions between these properties, and some of the classifications which can be found in the literature.

We consider the following properties:

- (FA) (*Free Algebra*): $K[V]^G$ is a polynomial ring.
- (ED) (*EquiDimensional*): All fibers of π have the same dimension.
- (FO) (*Finitely many Orbits*): Each fiber of π has finitely many orbits.
- (FM) (*Free Module*): The ring $K[V]$ is a free $K[V]^G$ -module.

The following implications hold:

- (FO) \Rightarrow (ED): Let d be the dimension of a general fiber. A general orbit has dimension $\leq d$ and by semicontinuity of dimensions (see Hartshorne [30, Exercise II.3.22]) of stabilizers, every orbit has dimension $\leq d$. If we assume that every fiber has finitely many orbits, then every fiber has dimension $\leq d$. By semicontinuity of the dimension of the fiber, every fiber must have dimension d .
- (FA) and (ED) \Leftrightarrow (FM): See Popov and Vinberg [4, II.8.1] and the citations there.

Without loss of generality we may assume that G acts faithfully on V . Various classifications have been made. We mention a few.

- (i) Assume G is connected and simple, and V is irreducible.
 - (a) All (G, V) satisfying (FA) were classified by Kac et al. [37].
 - (b) All (G, V) satisfying (ED) were classified by Popov [38].
 - (c) All (G, V) satisfying (FO) were classified by Kac [39].
 - (d) Moreover, all (G, V) satisfying
 - (ST) Every point in V has a nontrivial stabilizer
 were classified by Popov [40, 41].

It turns out that for irreducible representations of connected simple groups G , the lists for all classifications coincide. In particular (FA), (ED), (FO), (FM) and (ST) are all equivalent for these examples.

- (ii) Assume G is connected and simple, and V is arbitrary.
 - (a) All (G, V) satisfying (FA) were classified by Adamovich and Golovina [42] and by Schwarz [43] independently.
 - (b) All (G, V) satisfying (ED) were classified by Adamovich [44].
- (iii) Assume G is connected and *semisimple*, and V is irreducible.
 - (a) All (G, V) satisfying (FA) were classified by Littelmann [45].
 - (b) All (G, V) satisfying (DE) also can be found by Littelmann [45].
 - (c) All (G, V) satisfying (FO) were classified by Kac [46] (see Dadoc and Kac [47] for the corrections in the tables).

Popov [38] made the following so-called *Russian Conjecture*:

Conjecture 4.8.1 If G is connected and semisimple and V is a representation, then (ED) implies (FA).

Despite all classifications, no counterexample has been found yet. For a more detailed survey on the Russian Conjecture we refer the reader to Wehlau [48].

A more complete discussion of these classifications can be found in Popov and Vinberg [4, II.8.].

4.9 Computing Invariants of Reductive Groups

In Sect. 4.1 we presented an algorithm for computing invariant rings of linearly reductive groups. But the more general class of reductive groups also has finitely generated invariant rings (see Theorem 2.2.16), so it would be desirable to have an algorithm for calculating such invariant rings. Such an algorithm, which we are going to present here, was found by Kemper [49]. The algorithm proceeds in two steps. The first step is the computation of homogeneous separating invariants. We will deal with this in Sect. 4.9.1. Since reductive groups that are not linearly reductive occur only in positive characteristic (see Theorem 2.2.13), we may assume $\text{char}(K)$ to be positive. So Theorem 2.4.6 tells us that $K[V]^G$ is the purely inseparable closure of the subalgebra generated by homogeneous separating invariants. We deal with the computation of purely inseparable closures in Sect. 4.9.2. This constitutes the second and final step of the algorithm. In Sect. 4.9.3 we present an algorithm by Derksen and Kemper [50] for computing the invariant ring $K[X]^G$ of a reductive group acting on an affine variety X .

4.9.1 Computing Separating Invariants

Let G be a reductive group and V a G -module. If we can calculate the so-called **separating variety**

$$\mathcal{S} := \{(u, v) \in V \times V \mid f(u) = f(v) \text{ for every } f \in K[V]^G\},$$

then we can also compute separating invariants by using Algorithm 4.5.1 to produce more and more homogeneous invariants f_1, f_2, \dots until reaching an r such that

$$\mathcal{S} = \{(u, v) \in V \times V \mid f_i(u) = f_i(v) \text{ for } i = 1, \dots, r\}. \quad (4.9.1)$$

It is useful to compare \mathcal{S} to the smaller set

$$\mathcal{D} := \{(u, v) \in V \times V \mid \text{there exists } \sigma \in G \text{ with } v = \sigma \cdot u\}.$$

In Sect. 4.1.1 we used the letter B for this set, and we also explained how its vanishing ideal (for which we wrote b) can be computed as an elimination ideal (see step 3 in Algorithm 4.1.9). Because of its importance in Algorithm 4.1.9, the ideal b has come to be known as the **Derksen ideal** (see, for example, [49]). For this reason we change the notation here and write the Derksen ideal as

$$D := I(\mathcal{D}) \subseteq K[x_1, \dots, x_n, y_1, \dots, y_n] =: K[\underline{x}, \underline{y}].$$

It lies in a polynomial ring in two sets of variables, where $n = \dim(V)$. One might hope that $\mathcal{S} = \overline{\mathcal{D}}$. But the following example shows that the inclusion $\overline{\mathcal{D}} \subseteq \mathcal{S}$ can be strict.

Example 4.9.1 Consider the action of the multiplicative group $G = \mathbb{G}_m$ on $V = K^2$ with weight $(1, 1)$. Then $\overline{\mathcal{D}}$ is given by the equation $x_1 y_2 = x_2 y_1$, but $\mathcal{S} = V \times V$ since there are no nonconstant invariants. \triangleleft

The key to the computation of \mathcal{S} is its characterization

$$\mathcal{S} = \{(u, v) \in V \times V \mid \text{there exists } w \in \overline{G \cdot u} \cap \overline{G \cdot v}\} \quad (4.9.2)$$

(see Corollary 2.3.8). The occurrence of a third point w prompts us to introduce a new set of indeterminates z_1, \dots, z_n . In fact, if

$$D = (f_1, \dots, f_m)$$

with $f_i \in K[\underline{x}, \underline{y}]$, we form the elimination ideal

$$J := K[\underline{x}, \underline{y}] \cap \left(f_1(\underline{x}, \underline{z}), \dots, f_m(\underline{x}, \underline{z}), f_1(\underline{y}, \underline{z}), \dots, f_m(\underline{y}, \underline{z}) \right) K[\underline{x}, \underline{y}, \underline{z}].$$

Theorem 4.9.2 *In the above situation we have $\mathcal{S} = \mathcal{V}(J)$.*

Proof First let $f \in K[V]^G$ be an invariant. Then $f(\underline{x}) - f(\underline{y}) \in D$, so $f(\underline{x}) - f(\underline{y}) = \sum_{i=1}^m g_i f_i$ with $g_i \in K[\underline{x}, \underline{y}]$. This implies

$$\begin{aligned} f(\underline{x}) - f(\underline{y}) &= f(\underline{x}) - f(\underline{z}) + f(\underline{z}) - f(\underline{y}) = \\ &\sum_{i=1}^m g_i(\underline{x}, \underline{z}) f_i(\underline{x}, \underline{z}) - \sum_{i=1}^m g_i(\underline{y}, \underline{z}) f_i(\underline{y}, \underline{z}) \in J. \end{aligned}$$

Now take $(u, v) \in \mathcal{V}(J)$. It follows from the above that $f(u) - f(v) = 0$ for every $f \in K[V]^G$, so $(u, v) \in \mathcal{S}$.

To prove the converse, we first make the following observation. If $v \in V$, then as a function of $w \in V$ every $f_i(v, w)$ vanishes on $G \cdot v$ and therefore also on $\overline{G \cdot v}$. Take $(u, v) \in \mathcal{S}$. By (4.9.2) there exists $w \in \overline{G \cdot u} \cap \overline{G \cdot v}$, so $f_i(u, w) = f_i(v, w) = 0$ for $i = 1, \dots, m$ by the above observation. Let $f \in J$. Then $f \in K[\underline{x}, \underline{y}]$ and there exist $g_i, h_i \in K[\underline{x}, \underline{y}, \underline{z}]$ with

$$f = \sum_{i=1}^m g_i f_i(\underline{x}, \underline{z}) + \sum_{i=1}^m h_i f_i(\underline{y}, \underline{z}).$$

It follows that

$$f(u, v) = \sum_{i=1}^m g_i(u, v, w) f_i(u, w) + \sum_{i=1}^m h_i(u, v, w) f_i(v, w) = 0,$$

so $(u, v) \in \mathcal{V}(J)$. □

Using Theorem 4.9.2, we can determine \mathcal{S} . To test the condition (4.9.1), which is a criterion for a set $\{f_1, \dots, f_r\}$ of invariants to be separating, we need to check whether $J \subseteq \sqrt{I}$ with $I := (f_1(\underline{x}) - f_1(\underline{y}), \dots, f_r(\underline{x}) - f_r(\underline{y}))$. Fortunately, it is not necessary for this to compute the radical ideal \sqrt{I} since there is a much easier radical membership test (see Proposition 1.5.2). In the homogeneous case there is an even easier test, based on the following lemma, which does not require any extra indeterminate.

Lemma 4.9.3 (Homogeneous radical membership test) *Let $I \subseteq K[x_1, \dots, x_n]$ be a homogeneous ideal and let $f \in K[x_1, \dots, x_n]$ be a homogeneous polynomial. Then $f \in \sqrt{I}$ if and only if $1 \in I + (1 - f)$.*

Proof If $f \in \sqrt{I}$, then $f^r \in I$ for some r , so

$$1 = (1 - f)(1 + f + \dots + f^{r-1}) + f^r \in I + (1 - f).$$

Conversely, assume $1 \in I + (1 - f)$, so

$$1 = \sum_{i=1}^m g_i f_i + g \cdot (1 - f)$$

with $g, g_i \in K[x_1, \dots, x_n]$ (not necessarily homogeneous) and $f_i \in I$ homogeneous. The idea is to homogenize this. More precisely, let y be an additional indeterminate and define $\varphi: K[x_1, \dots, x_n] \rightarrow K[x_1, \dots, x_n, y, y^{-1}]$ by $x_i \mapsto x_i/y$. We apply φ to the above equation and multiply by some y^k :

$$y^k = \sum_{i=1}^m y^{k-d_i} \varphi(g_i) f_i + y^{k-d} \varphi(g) \cdot (y^d - f)$$

where $d = \deg(f)$, $d_i = \deg(f_i)$. Choose k to be a multiple of d and large enough so that all $h_i := y^{k-d_i} \varphi(g_i)$ and $h := y^{k-d} \varphi(g)$ lie in $K[x_1, \dots, x_n, y]$. We perform division with remainder by $y^d - f$ on both sides of the above equation. Writing \tilde{t} for the unique remainder of a $t \in K[x_1, \dots, x_n, y]$, we obtain

$$f^{k/d} = \sum_{i=1}^m \tilde{h}_i f_i.$$

Setting $y = 0$ in this equation shows that $f^{k/d} \in I$, so $f \in \sqrt{I}$. \square

Putting things together, we obtain the following algorithm.

Algorithm 4.9.4 (Computing separating invariants) Let G be a reductive (but not necessarily linearly reductive) group and V a G -module. We assume that G and V are given by the same input data as in Algorithm 4.1.9. Construct a finite set $S \subset K[V]^G$ of homogeneous separating invariants by performing the following steps.

- (1) Compute homogeneous generators f_1, \dots, f_m of the Derksen ideal $D \subseteq K[\underline{x}, \underline{y}]$ as in steps 2 and 3 of Algorithm 4.1.9 (where the Derksen ideal is written as b).
- (2) With additional indeterminates z_1, \dots, z_n , form the ideal

$$\hat{J} := \left(f_1(\underline{x}, \underline{z}), \dots, f_m(\underline{x}, \underline{z}), f_1(\underline{y}, \underline{z}), \dots, f_m(\underline{y}, \underline{z}) \right) K[\underline{x}, \underline{y}, \underline{z}]$$

and compute a homogeneous generating set M of the elimination ideal

$$J := K[\underline{x}, \underline{y}] \cap \hat{J}$$

(see Algorithm 1.2.1).

- (3) Set $S := \emptyset$ and $I := (0) \subset K[\underline{x}, \underline{y}]$.
- (4) For $d := 1, 2, \dots$ perform steps 5–8.
- (5) If $M = \emptyset$, then S is a separating subset and we are done.

- (6) Use Algorithm 4.5.1 to compute a basis B of $K[V]_d^G$.
- (7) Set $S := S \cup B$ and $I := I + (f(\underline{x}) - f(\underline{y}) \mid f \in B)$.
- (8) For $g \in M$, test whether $1 \in I + (1 - g)$ (see at the end of Sect. 1.1.2). If this is the case, delete g from M .

The correctness of Algorithm 4.9.4 follows from Theorem 4.9.2, Lemma 4.9.3, and the remark before the lemma.

Remark 4.9.5

- (a) As stated, Algorithm 4.9.4 tends to produce unnecessarily large separating subsets. To avoid this, one may delete elements from the basis B until reaching a set that is linearly independent modulo the subalgebra of $K[V]^G$ generated by invariants of smaller degree. One may also test the invariants from B one by one and include only those $f \in B$ into S for which the inclusion of $f(\underline{x}) - f(\underline{y})$ into I leads to the deletion of at least one element from M in step 8.
- (b) It is not hard to generalize Algorithm 4.9.4 to the case where G acts on a G -variety X .

□

If G is reductive but not linearly reductive, then $K[V]^G$ is the purely inseparable closure of a subalgebra generated by a homogeneous separating subset (see Theorem 2.4.6). The following section deals with the computation of the purely inseparable closure (see Algorithm 4.9.9). We state the resulting algorithm for computing $K[V]^G$ already now.

Algorithm 4.9.6 (Calculating $K[V]^G$ for G reductive) Let G be a reductive (but not necessarily linearly reductive) group and V a G -module. We assume that G and V are given by the same input data as in Algorithm 4.1.9. Calculate generators of $K[V]^G$ by performing the following steps.

- (1) If G is linearly reductive, use Algorithm 4.1.9 to compute $K[V]^G$. Otherwise, perform the following steps.
- (2) Use Algorithm 4.9.4 to compute a finite, homogeneous separating subset $S \subset K[V]^G$.
- (3) With $A := K[S]$, use Algorithm 4.9.9 in the following section to compute the purely inseparable closure \hat{A} of A in $K[V]$. (Observe that $\text{char}(K) > 0$ since otherwise G would be linearly reductive.) Then $\hat{A} = K[V]^G$.

What happens if one tries to run Algorithm 4.9.6 on a nonreductive group? First, Algorithm 4.9.4 may not terminate since for nonreductive groups the inclusion $\mathcal{V}(J) \subseteq \mathcal{S}$ (which follows from the first part of the proof of Theorem 4.9.2) may be strict (for an example, see Kemper [49, Example 2.5]). If Algorithm 4.9.4 does terminate, the result will be a separating subset. However, even then $K[V]^G$ may fail to be integral over the graded separating subalgebra A (see [49, Example 1.4]), so the inclusion $\hat{A} \subseteq K[V]^G$ may be strict.

4.9.2 Computing the Purely Inseparable Closure

After having constructed a graded separating subalgebra $A \subseteq K[V]^G$, we need to calculate the purely inseparable closure \hat{A} of A in $K[V]$, which by Theorem 2.4.6 is equal to $K[V]^G$. We will present an algorithm for this in a more general setting. Let $R = K[x_1, \dots, x_n]/I$ be a reduced algebra over a perfect field of characteristic $p > 0$ (so I is a radical ideal), and let $A \subseteq R$ be a finitely generated subalgebra. We wish to compute the purely inseparable closure

$$\hat{A} := \{a \in R \mid a^{p^r} \in A \text{ for some } r \in \mathbb{N}\}$$

of A in R . We assume that \hat{A} is finitely generated. This is automatically satisfied if \hat{A} is the invariant ring of a reductive group (see Theorem 2.2.16) or if R is an integral domain (since then $\text{Quot}(R)$ is a finitely generated field extension of $\text{Quot}(A)$, and therefore the integral closure of A in $\text{Quot}(R)$, which contains \hat{A} , is finitely generated as an A -module by Eisenbud [51, Corollary 13.13]). Then there exists an r such that all generators of \hat{A} lie in

$$A_r := \sqrt[p^r]{A} := \{a \in R \mid a^{p^r} \in A\}.$$

This implies $\hat{A} = A_r$. This reduces the calculation of \hat{A} to the computation of $\sqrt[p^r]{A}$, since we can calculate the A_i by $A_i = \sqrt[p^r]{A_{i-1}}$ and stop when no new generators are required (see Algorithm 4.9.9). The following algorithm is a simplification of Algorithm 1.4 from Derksen and Kemper [50].

Algorithm 4.9.7 (Computation of a p th root of a subalgebra) Let $R = K[x_1, \dots, x_n]/I$ be a finitely generated, reduced algebra over a perfect field K of characteristic $p > 0$. Let $A := K[f_1 + I, \dots, f_m + I] \subseteq R$ be a finitely generated subalgebra given by polynomials $f_i \in K[x_1, \dots, x_n]$. The following steps produce polynomials $g_1, \dots, g_r \in K[x_1, \dots, x_n]$ such that the $g_j + I \in R$ generate $\sqrt[p^r]{A}$ as an A -module.

- (1) Form the free $K[x_1, \dots, x_n]$ -module F of dimension $p^m + 1$ with free generators e_{i_1, \dots, i_m} (with $0 \leq i_k \leq p - 1$) and e . Form the submodule $M \subseteq F$ generated by $I \cdot e$ and all

$$e_{i_1, \dots, i_m} + \prod_{k=1}^m f_k^{i_k} \cdot e.$$

- (2) With $\varphi: K[y_1, \dots, y_n] \rightarrow K[x_1, \dots, x_n]$, $y_i \mapsto x_i^p$, use Algorithm 4.9.8 below to compute the $K[y_1, \dots, y_n]$ -module

$$\tilde{M} := \varphi^{-1}(M) \subseteq K[y_1, \dots, y_n]^{p^m + 1},$$

where we write φ also for the component-wise application of φ to elements of a free module.

- (3) With $\psi: K[z_1, \dots, z_m] \rightarrow K[y_1, \dots, y_n]$, $z_i \mapsto \varphi^{-1}(f_i^p)$ and $\pi: K[y_1, \dots, y_n]^{p^m} \rightarrow K[y_1, \dots, y_n]^{p^m}$ the projection on the first p^m coordinates, use Algorithm 4.9.8 to compute elements $(s_1, t_1), \dots, (s_r, t_r) \in K[z_1, \dots, z_m]^{p^m} \times K[y_1, \dots, y_n]$ such that $\psi^{-1}(\pi(\tilde{M}))$ is generated (as a $K[z_1, \dots, z_m]$ -module) by the s_j and such that $\psi(s_j) + t_j e \in \tilde{M}$.
- (4) For $j = 1, \dots, r$ set $g_j := \sqrt[p]{\varphi(t_j)}$.

Proof of correctness of Algorithm 4.9.7 We first remark that since K is perfect and $\varphi(t_j) \in K[x_1^p, \dots, x_n^p]$, the g_j exist (and are unique). Now we show that every \bar{g}_j lies in $\sqrt[p]{A}$, where the bar indicates the residue class modulo I . Since $\psi(s_j) + t_j e \in \tilde{M}$, we can write

$$\varphi(\psi(s_j)) + g_j^p e = \sum_{i_1, \dots, i_m=0}^{p-1} u_{i_1, \dots, i_m} \cdot \left(e_{i_1, \dots, i_m} + \prod_{k=1}^m f_k^{i_k} e \right) + h e$$

with $u_{i_1, \dots, i_m} \in K[x_1, \dots, x_n]$ and $h \in I$. This implies $u_{i_1, \dots, i_m} = \varphi(\psi(s_j^{(i_1, \dots, i_m)})) = s_j^{(i_1, \dots, i_m)}(f_1^p, \dots, f_m^p)$, the e_{i_1, \dots, i_m} -component of $\varphi(\psi(s_j))$. Comparing the e -component yields

$$g_j^p = \sum_{i_1, \dots, i_m=0}^{p-1} s_j^{(i_1, \dots, i_m)}(f_1^p, \dots, f_m^p) \prod_{k=1}^m f_k^{i_k} + h.$$

This implies $\bar{g}_j^p \in A$, so $\bar{g}_j \in \sqrt[p]{A}$.

Conversely, let $g \in K[x_1, \dots, x_n]$ with $\bar{g} \in \sqrt[p]{A}$. We can write

$$g^p = \sum_{i_1, \dots, i_m=0}^{p-1} u_{i_1, \dots, i_m}(f_1^p, \dots, f_m^p) \prod_{k=1}^m f_k^{i_k} + h \tag{4.9.3}$$

with $u_{i_1, \dots, i_m} \in K[z_1, \dots, z_m]$ and $h \in I$, so

$$\sum_{i_1, \dots, i_m=0}^{p-1} u_{i_1, \dots, i_m}(f_1^p, \dots, f_m^p) e_{i_1, \dots, i_m} + g^p e \in M$$

and $\sum_{i_1, \dots, i_m=0}^{p-1} u_{i_1, \dots, i_m} e_{i_1, \dots, i_m} \in \psi^{-1}(\pi(\tilde{M}))$. Hence there exist $b_j \in K[z_1, \dots, z_m]$ such that $\sum_{i_1, \dots, i_m=0}^{p-1} u_{i_1, \dots, i_m} e_{i_1, \dots, i_m} = \sum_{j=1}^r b_j s_j$. Since $\psi(s_j) + t_j e \in \tilde{M}$, this implies

$$\sum_{i_1, \dots, i_m=0}^{p-1} \varphi(\psi(u_{i_1, \dots, i_m})) e_{i_1, \dots, i_m} + \sum_{j=1}^r \varphi(\psi(b_j)) \varphi(t_j) e \in M.$$

From the definition of M we conclude

$$\sum_{j=1}^r \varphi(\psi(b_j))\varphi(t_j) = \sum_{i_1, \dots, i_m=0}^{p-1} \varphi(\psi(u_{i_1, \dots, i_m})) \prod_{k=1}^m f_k^{i_k} + h'$$

with $h' \in I$. Since $\varphi(\psi(u_{i_1, \dots, i_m})) = u_{i_1, \dots, i_m}(f_1^p, \dots, f_m^p)$, comparing this with (4.9.3) yields

$$\sum_{j=1}^r b_j(f_1^p, \dots, f_m^p)\varphi(t_j) = g^p - h + h'.$$

Obtain $b'_j \in K[z_1, \dots, z_m]$ from b_j by substituting each coefficient by its p th root. Since $\varphi(t_j) = g_j^p$, we obtain

$$\left(g - \sum_{j=1}^r b'_j(f_1, \dots, f_m)g_j \right)^p = h - h' \in I,$$

so $\bar{g} = \sum_{j=1}^r b'_j(\bar{f}_1, \dots, \bar{f}_m)\bar{g}_j \in \sum_{j=1}^m A \cdot \bar{g}_j$, since I is a radical ideal. \square

The following algorithm was used in Algorithm 4.9.7, and it will also be used in Algorithm 4.9.9. Similar algorithms have appeared in Kreuzer and Robbiano [52, Section 3.6, Exercise 10 c], Kemper [49], and Derksen and Kemper [50].

Algorithm 4.9.8 Let $M \subseteq K[x_1, \dots, x_n]^k$ be a submodule of a free module over a polynomial ring, and let $\varphi: K[y_1, \dots, y_m] \rightarrow K[x_1, \dots, x_n]$ be a homomorphism. Let $\pi: K[x_1, \dots, x_n]^k \rightarrow K[x_1, \dots, x_n]^l$ be the projection on the first l coordinates (with $1 \leq l \leq k$). For a monomial ordering “ $>$ ”, the following steps compute $(s_1, t_1), \dots, (s_r, t_r) \in K[y_1, \dots, y_m]^l \times K[x_1, \dots, x_n]^{k-l}$ such that the s_j form a Gröbner basis of $\varphi^{-1}(\pi(M))$ with respect to “ $>$ ” and $(\varphi(s_j), t_j) \in M$. (Here we write φ also for the component-wise application of φ to elements of a free module.)

- (1) Form the submodule $\tilde{M} \subseteq K[x_1, \dots, x_n, y_1, \dots, y_m]^k$ generated by M and all $(\varphi(y_i) - y_i)e_j$ (with e_j the standard basis vectors).
- (2) Choose an extension of “ $>$ ” to a monomial ordering on $K[x_1, \dots, x_n, y_1, \dots, y_m]^k$ such that
 - (i) if $1 \leq i \leq l < j \leq k$ and $s, t \in K[x_1, \dots, x_n, y_1, \dots, y_m]$ are monomials, then $se_i > te_j$, and
 - (ii) if $1 \leq i, j \leq l$ and $s \in K[y_1, \dots, y_m]$ is a monomial, then $x_k e_i > se_j$ for every $k \in \{1, \dots, n\}$.
- (3) Compute a Gröbner basis \mathcal{G} of \tilde{M} with respect to “ $>$ ”.

- (4) For all $(s, t) \in \mathcal{G}$ with $s \in K[y_1, \dots, y_m]^l$ and $t \in K[x_1, \dots, x_n, y_1, \dots, y_m]^{k-l}$ form $(s, \varphi(t)) \in K[y_1, \dots, y_m]^l \times K[x_1, \dots, x_n]^{k-l}$. These elements $(s, \varphi(t))$ are the desired (s_j, t_j) .

Proof of correctness of Algorithm 4.9.8 Let $(s, t) \in \tilde{M}$ with $s \in K[y_1, \dots, y_m]^l$ and $t \in K[x_1, \dots, x_n, y_1, \dots, y_m]^{k-l}$. Then

$$(s, t) = \sum_{i=1}^r f_i m_i + \sum_{i=1}^m \sum_{j=1}^k g_{i,j} (\varphi(y_i) - y_i) e_j$$

with $m_i \in M$ and $f_i, g_{i,j} \in K[x_1, \dots, x_n, y_1, \dots, y_m]$. Substituting each y_i by $\varphi(y_i)$ shows that $(\varphi(s), \varphi(t)) \in M$. In particular, the $(\varphi(s_j), t_j)$ from the algorithm lie in M . This also implies $s_j \in \varphi^{-1}(\pi(M))$.

To complete the proof, we need to show that the leading monomial of an element of $\varphi^{-1}(\pi(M))$ is divisible by the leading monomial of some s_j . So take a nonzero $f \in K[y_1, \dots, y_m]^l$ such that $\varphi(f) \in \pi(M)$. There exists $g \in K[x_1, \dots, x_n]^{k-l}$ such that $(\varphi(f), g) \in M$. By the definition of \tilde{M} , this implies $(f, g) \in \tilde{M}$, so there exists $(s, t) \in \mathcal{G}$ such that $\text{LM}(s, t)$ divides $\text{LM}(f, g)$. By the property (i) of the monomial ordering, $\text{LM}(f, g) = \text{LM}(f)$, so $\text{LM}(s)$ divides $\text{LM}(f)$. Therefore $\text{LM}(s) \in K[y_1, \dots, y_m]^l$. By the property (ii) of the monomial ordering, this implies $s \in K[y_1, \dots, y_m]^l$, so there exists j with $(s, \varphi(t)) = (s_j, t_j)$. Since $\text{LM}(s_j)$ divides $\text{LM}(f)$, the proof is complete. \square

Now we state the algorithm for calculating the purely inseparable closure.

Algorithm 4.9.9 (Purely inseparable closure of a subalgebra) Let $R = K[x_1, \dots, x_n]/I$ be a finitely generated, reduced algebra over a perfect field K of characteristic $p > 0$. Let $A := K[f_1 + I, \dots, f_m + I] \subseteq R$ be a finitely generated subalgebra given by polynomials $f_i \in K[x_1, \dots, x_n]$, and assume that the purely inseparable closure \hat{A} of A in R is finitely generated (see at the beginning of Sect. 4.9.2). Perform the following steps to calculate \hat{A} .

- (1) Set $B := A$.
- (2) Use Algorithm 4.9.7 to compute $g_1, \dots, g_r \in R$ which generate $\sqrt[p]{B}$ as a B -module.
- (3) For $j = 1, \dots, r$ perform steps 4–6.
- (4) With $B = K[f_1 + I, \dots, f_m + I]$, form the map $\varphi: K[y_0, \dots, y_m] \rightarrow K[x_1, \dots, x_n]$, $y_0 \mapsto g_j$, $y_i \mapsto f_i$ ($i > 0$).
- (5) Use Algorithm 4.9.8 to compute a Gröbner basis \mathcal{G} of $\varphi^{-1}(I)$ with respect to a monomial ordering " $>$ " such that $y_0 > t$ for every monomial $t \in K[y_1, \dots, y_m]$.
- (6) If \mathcal{G} contains no polynomial whose leading monomial is y_0 , set $B := K[f_1 + I, \dots, f_m + I, g_j + I]$.
- (7) If no new generator was added to B during the loop in steps 4–6, then $B = \hat{A}$ and the algorithm is finished. Otherwise, go to step 2.

Proof of correctness of Algorithm 4.9.9 The loop in steps 4–6 test if $g_j + I \in B$. Indeed, if this is the case, than there exists a polynomial in $\varphi^{-1}(I)$ whose leading monomial is y_0 , and therefore there also exists such a polynomial in \mathcal{G} . The converse is clear. There is nothing else to show. \square

4.9.3 Actions on Varieties

In this section we consider a reductive group G acting on an affine variety X by a morphism $G \times X \rightarrow X$. Explicitly, G is given as an algebraic subset $G \subseteq K^m$ by a radical ideal $I_G \subset K[z_1, \dots, z_m]$, $X \subseteq K^n$ is given by a radical ideal $I_X \subseteq K[x_1, \dots, x_n]$, and the action is given by polynomials $g_1, \dots, g_n \in K[x_1, \dots, x_n, z_1, \dots, z_m]$ such that for a point $(\xi_1, \dots, \xi_n) \in X$ and $\sigma \in G$ we have

$$\sigma \cdot (\xi_1, \dots, \xi_n) = (g_1(\xi_1, \dots, \xi_n, \sigma), \dots, g_n(\xi_1, \dots, \xi_n, \sigma)),$$

where the z_j in g_i are substituted by the coordinates of σ . For $f \in K[x_1, \dots, x_n]$ we write $\bar{f} = f + I_X \in K[X] =: R$. Since

$$(\sigma^{-1} \cdot \bar{x}_i)(\xi_1, \dots, \xi_n) = \bar{x}_i(\sigma \cdot (\xi_1, \dots, \xi_n)) = g_i(\xi_1, \dots, \xi_n, \sigma),$$

the action of G on R is given by

$$\sigma^{-1} \cdot \bar{x}_i = \overline{g_i(\sigma)}. \quad (4.9.4)$$

(Again, on the right hand side the z_j are substituted by the coordinates of σ .) We wish to calculate generators of $R^G = K[X]^G$. The first step is to embed X equivariantly into a G -module V , or, equivalently, to construct a G -equivariant epimorphism $K[V] \rightarrow R$. (We will also call such an epimorphism a G -epimorphism.) The idea for this is quite simple. Since the action of G on R is locally finite (see Lemma A.1.8), there exists a G -module $W \subseteq R$ containing a generating set of R . This provides a G -epimorphism $K[W^*] = S(W) \rightarrow R$ from the symmetric algebra of W onto R . This idea is made explicit in the following algorithm. In the algorithm we drop the assumptions that G is reductive and I_X is a radical ideal.

Algorithm 4.9.10 (Embedding a G -variety into a G -module) Let G be a linear algebraic group, given as a subset of K^m by a radical ideal $I_G \subset K[z_1, \dots, z_m]$, and let $R = K[x_1, \dots, x_n]/I_X$ be a finitely generated K -algebra. Assume that a G -action on R is given by polynomials $g_1, \dots, g_n \in K[x_1, \dots, x_n, z_1, \dots, z_m]$ as in (4.9.4). The following steps construct a G -module V together with a G -epimorphism $K[V] \rightarrow R$.

- (1) Compute Gröbner bases \mathcal{G}_G and \mathcal{G}_X of I_G and I_X with respect to arbitrary monomial orderings.
- (2) Substitute each g_i by its normal form with respect to \mathcal{G}_G and \mathcal{G}_X .

- (3) Regarding the g_i as polynomials in z_1, \dots, z_m with coefficients in $K[x_1, \dots, x_n]$, form the subspace $W \subseteq K[x_1, \dots, x_n]$ generated by the coefficients of all g_i , and choose a basis $\{h_1, \dots, h_r\}$ of W .
- (4) For $i = 1, \dots, r$ let $H_i \in K[x_1, \dots, x_n, z_1, \dots, z_m]$ be the normal form of $h_i(g_1, \dots, g_n)$ with respect to \mathcal{G}_G and \mathcal{G}_X .
- (5) For $i = 1, \dots, r$ find $a_{i,1}, \dots, a_{i,r} \in K[z_1, \dots, z_m]$ with

$$H_i = \sum_{j=1}^r a_{i,j} h_j. \quad (4.9.5)$$

This can be done by regarding both sides of (4.9.5) as polynomials in x_1, \dots, x_n and comparing coefficients. This leads to a system of linear equations for the $a_{i,j}$ with coefficients in $K(z_1, \dots, z_m)$. It turns out that this system is uniquely solvable and the solution lies in $K[z_1, \dots, z_m]^r$.

- (6) The $a_{i,j}$ define a G -module structure on $V = K^r$ as explained at the beginning of Sect. 4.1.2. With $K[V] = K[y_1, \dots, y_r]$, the map $\varphi: K[V] \rightarrow R$, $y_i \mapsto \bar{h}_i$ (the residue class of h_i modulo I_X) is a G -epimorphism.

Proof of correctness of Algorithm 4.9.10 Set $\overline{W} := \{\bar{h} \mid h \in W\}$. We claim that

$$\overline{W} = \langle \sigma \cdot \bar{x}_i \mid \sigma \in G, i = 1, \dots, n \rangle_K. \quad (4.9.6)$$

If we write $g_i = \sum_{j=1}^l g_{i,j} t_j$ with $g_{i,j} \in K[x_1, \dots, x_n]$ and t_j pairwise distinct monomials in z_1, \dots, z_m , then by definition \overline{W} is generated by the $\bar{g}_{i,j}$. For every $\sigma \in G$ and $i \in \{1, \dots, n\}$, (4.9.4) implies

$$\sigma^{-1} \cdot \bar{x}_i = \sum_{j=1}^l \bar{g}_{i,j} t_j(\sigma) \in \overline{W},$$

which shows that the right hand side of (4.9.6) is contained in the left hand side. To prove the reverse inclusion, observe that all t_j are in normal form with respect to \mathcal{G}_G (since the g_i are in normal form), so they are linearly independent as functions $G \rightarrow K$. It follows that there exist $\sigma_1, \dots, \sigma_l \in G$ such that the matrix $(t_j(\sigma_k))_{j,k} \in K^{l \times l}$ is invertible. Since $\sum_{j=1}^l \bar{g}_{i,j} t_j(\sigma_k) = \sigma_k^{-1} \cdot \bar{x}_i$, this implies

$$\bar{g}_{i,j} \in \langle \sigma_1^{-1} \cdot \bar{x}_i, \dots, \sigma_l^{-1} \cdot \bar{x}_i \rangle_K.$$

This completes the proof of (4.9.6). From (4.9.4) we get

$$\sigma^{-1} \cdot \bar{h}_i = \overline{H_i(\sigma)} \quad (4.9.7)$$

for $\sigma \in G, i = 1, \dots, n$. We now show that step 5 works as claimed. Since the h_i are linearly independent elements of the vector space of all polynomials in $K[x_1, \dots, x_n]$

that are in normal form with respect to \mathcal{G}_X , we can choose a set B that together with the h_i forms a basis of that vector space. We can write

$$H_i = \sum_{j=1}^r a_{i,j} h_j + \sum_{j=1}^s c_{i,j} b_j \quad (4.9.8)$$

with $b_j \in B$ and $a_{i,j}, c_{i,j} \in K[z_1, \dots, z_m]$. Since the H_i are in normal form with respect to \mathcal{G}_G , the same is true for the $a_{i,j}$ and $c_{i,j}$. For $\sigma \in G$ we have

$$\sum_{i=1}^r a_{i,j}(\sigma) \bar{h}_j + \sum_{j=1}^s c_{i,j}(\sigma) \bar{b}_j = \overline{H_i(\sigma)} = \sigma^{-1} \cdot \bar{h}_i \in \overline{W} = \langle \bar{h}_1, \dots, \bar{h}_r \rangle_K,$$

where we use (4.9.7) and the fact that \overline{W} is G -stable by (4.9.6). Since the h_j and b_j are in normal form with respect to \mathcal{G}_X , we actually have $\sum_{i=1}^r a_{i,j}(\sigma) h_j + \sum_{j=1}^s c_{i,j}(\sigma) b_j \in \langle h_1, \dots, h_r \rangle_K$, so $c_{i,j}(\sigma) = 0$. This holds for all $\sigma \in G$, and therefore $c_{i,j} \in I_G$. Since the $c_{i,j}$ are in normal form with respect to \mathcal{G}_G , this implies $c_{i,j} = 0$. Now (4.9.8) implies the existence of the $a_{i,j}$ in step 5. Their uniqueness follows from the fact that the h_j are linearly independent over K , hence also over $K(z_1, \dots, z_m)$ when regarded as polynomials in $K(z_1, \dots, z_m)[x_1, \dots, x_n]$.

From (4.9.7) we get

$$\sigma^{-1} \cdot \bar{h}_i = \sum_{j=1}^r a_{i,j}(\sigma) \bar{h}_j.$$

This implies that $\sigma \mapsto (a_{i,j}(\sigma))_{i,j}$ defines a G -module structure on $V = K^r$. It is a routine computation to check that the action on the dual basis y_1, \dots, y_r of the standard basis of V is the same as on the \bar{h}_i , so φ is G -equivariant. Finally, the surjectivity of φ follows since all generators \bar{x}_i of R lie in $\langle \bar{h}_1, \dots, \bar{h}_r \rangle_K$ by (4.9.6).

□

If G is a linearly reductive group and R is the coordinate ring of a G -variety (or, more generally, R is a finitely generated algebra with a G -action given as in (4.9.4)), then the G -epimorphism $\varphi: K[V] \rightarrow R$ from Algorithm 4.9.10 restricts to an epimorphism $K[V]^G \rightarrow R^G$. If generators f_1, \dots, f_m of $K[V]^G$ have been calculated (e.g., by Algorithm 4.1.9), then the $\varphi(f_i)$ generate R^G . So we have an algorithm for computing invariants of linearly reductive groups acting on affine varieties.

However, if G is reductive but not linearly reductive, then φ does not necessarily restrict to an epimorphism of the invariants. But the following weaker result is well-known (see Mumford et al. [53, Lemma A.1.2]): If R is reduced (i.e., R is the coordinate ring of a G -variety), then R^G is the purely inseparable closure of $\varphi(K[V]^G)$ in R . We will provide a proof of this result (in the slightly more general version given in Proposition 4.9.12 that is needed for our final algorithm), since it fits seamlessly into our framework of separating invariants.

Lemma 4.9.11 *Let G be a reductive group over a field K acting on two finitely generated K -algebras A and B with actions given as in (4.9.4). Let $\varphi: A \rightarrow B$ be G -epimorphism. Then for every $b \in B^G$ there exists a positive integer d with $b^d \in \varphi(A^G)$.*

Proof We may assume $b \neq 0$. Choose $a \in \varphi^{-1}(\{b\})$. By Lemma A.1.8 there exists a G -module $W \subseteq A$ with $a \in W$. It is easy to see that $V := Ka \oplus (W \cap \ker(\varphi)) \subseteq A$ is also a G -module. Consider the linear form $x \in V^*$ with $x(a) = 1$ and $x(w) = 0$ for $w \in W \cap \ker(\varphi)$. A short computation shows that $x \in (V^*)^G$, so by the reductivity of G there exists a homogeneous invariant $f \in K[V^*]^G = S(V)^G$ of positive degree d such that $f(x) = 1$. The embedding $V \subseteq A$ induces a G -equivariant map $\psi: S(V) \rightarrow A$. It is easy to see that $\psi(f) = a^d + g$ with $g \in \ker(\varphi)$, so $\varphi(\psi(f)) = b^d$. \square

The next proposition shows that the integer d from Lemma 4.9.11 can be assumed to be a power of $p = \text{char}(K)$.

Proposition 4.9.12 *Let G be a reductive group over a field K of characteristic $p > 0$. Let X be a G -variety with a closed, G -stable subvariety $Y \subseteq X$. If $A \subseteq K[X]^G$ is a separating subset such that $K[X]^G$ is integral over A , then $K[Y]^G$ is the purely inseparable closure (in $K[Y]$) of the image of A under the restriction map $K[X] \rightarrow K[Y]$.*

Proof Write $\varphi: K[X] \rightarrow K[Y]$ for the restriction map. It follows by Lemma 4.9.11 that $K[Y]^G$ is integral over $\varphi(K[X]^G)$ and therefore also over $\varphi(A)$. By Theorem 2.4.9 the image $\varphi(A) \subseteq K[Y]^G$ is a separating subalgebra. So the map of varieties induced by the embedding is injective, and Proposition 2.4.5 shows that for every element of $f \in K[Y]^G$ some f^{p^r} lies in $\varphi(A)$. Conversely, if $f \in K[Y]$ such that $f^{p^r} \in \varphi(A)$, then $f \in K[Y]^G$ since $K[Y]$ is reduced. \square

Putting things together, we arrive at the following algorithm, which appeared in Derksen and Kemper [50].

Algorithm 4.9.13 (Invariants of a reductive group acting on a variety) Let G be a reductive group and X a G -variety. Assume that G and the action are given as in Algorithm 4.9.10. The following steps calculate a generating set of R^G , where $R = K[X]$.

- (1) Use Algorithm 4.9.10 to construct a G -module V with a G -epimorphism $\varphi: K[V] \rightarrow R$.
- (2) If G is linearly reductive, use Algorithm 4.1.9 to compute generators f_1, \dots, f_m of $K[V]^G$. Then $R = K[\varphi(f_1), \dots, \varphi(f_m)]$, and we are done. In this case, we need not require that R be reduced. If G is reductive but not linearly reductive, perform the following steps.
- (3) Use Algorithm 4.9.4 to compute a finite, homogeneous separating subset $S \subset K[V]^G$.
- (4) Let $A \subseteq R^G$ be the subalgebra generated by the $\varphi(f)$, $f \in S$. Use Algorithm 4.9.9 to compute the purely inseparable closure \hat{A} of A in R . (Observe that $\text{char}(K) > 0$ since otherwise G would be linearly reductive.) Then $\hat{A} = R^G$.

With Algorithm 4.9.13, the finiteness results of Hilbert and Nagata have been made almost entirely constructive. What remains to be covered is the case where a reductive group G (over a field K) acts on a finitely generated, nonreduced K -algebra R with an action as in (4.9.4). (This is equivalent to the very natural hypothesis that the action is given by a map $R \rightarrow K[G] \otimes_K R$.) In this case we know from Nagata [54] that R^G is finitely generated. The case of finite groups was treated in Sect. 3.13. At first sight one might think that it might not too hard to generalize Algorithm 4.9.13 to the case where R is not reduced. But the following example, which is taken from Kamke [55], shows that the approach from Algorithm 4.9.13 is irreparably flawed for nonreduced algebras.

Example 4.9.14 Assume that K has characteristic 2 and consider the action of the multiplicative group $G = \mathbb{G}_m$ on $R := K[x_1, x_2]/(x_1^2)$ with weight $(1, 1)$. We can take $K[V] = K[x_1, x_2]$, so $K[V]^G = K$. Writing \bar{x}_i for the class of x_i in R , we obtain

$$\sqrt[2]{K} = K \oplus (\bar{x}_1)R = K[\bar{x}_1, \bar{x}_1\bar{x}_2, \bar{x}_1\bar{x}_2^2, \dots],$$

which is not finitely generated as a K -algebra. Moreover, $\sqrt[2]{K}$ and therefore also the purely inseparable closure \hat{K} are strictly bigger than R^G . In fact, $R^G = K$. This can be derived from elementary calculations but also from the fact that G is linearly reductive. \triangleleft

4.10 Invariant Fields and Localizations of Invariant Rings

In this section we go beyond reductive groups. Invariant rings of nonreductive groups often turn out to be finitely generated, although there is no guarantee for that. We will present an algorithm for computing the invariant field of a linear algebraic group (without any reductivity hypothesis). If the invariant field equals the field of fractions of the invariant ring, then the algorithm also computes a localization $K[X]^G_a$ of the invariant ring, where $a \in K[X]^G$ is a nonzero invariant. From this the invariant ring $K[X]^G$ can be extracted if it is finitely generated.

The main tool is a modified and generalized version of an ideal that we have already come across in Sects. 4.1 and 4.9.1: the Derksen ideal. In this section we will define so-called extended Derksen ideals and deal with their geometric and computational aspects. The algorithms turn out to be particularly well suited for computing a localization of an invariant ring of the additive group. At the end of the section we discuss the problem of representing an invariant ring (of a nonreductive group) as the ring of regular functions on a quasi-affine variety. The section also has an interlude on the Italian problem, i.e., the question whether the invariant field and the field of fractions of the invariant ring coincide. Most of the material from this section is drawn from Müller-Quade and Beth [56], Hubert and Kogan [57], Kamke and Kemper [58], and Kemper [59].

4.10.1 Extendend Derksen Ideals and CAGEs

We start by introducing a generalized notion of a Derksen ideal. We also introduce extended and tamely extended Derksen ideals, which, as we will see, are useful for computations and have interesting geometric interpretations. We assume we are in the same situation as in Sect. 4.9.3, but we drop the assumption that G is reductive.

Definition 4.10.1 Suppose that G is a linear algebraic group over an algebraically closed field K and that X is an irreducible G -variety (i.e., X is irreducible as a variety). Assume that X is given as a closed subset of K^n defined by a prime ideal $I_X \subseteq K[x_1, \dots, x_n]$, and write $\bar{x}_i := x_i + I_X \in K[X]$. Also write $K(X) = \text{Quot}(K[X])$ for the function field and let y_1, \dots, y_n be indeterminates, on which G acts trivially.

- (a) The **Derksen ideal** is the intersection

$$D := \bigcap_{\sigma \in G} (y_1 - \sigma \cdot \bar{x}_1, \dots, y_n - \sigma \cdot \bar{x}_n) \subseteq K(X)[y_1, \dots, y_n].$$

(The ideals are understood to be ideals in $K(X)[y_1, \dots, y_n]$.) Of course, D depends not only on G and X but also on the embedding $X \subseteq K^n$.

- (b) A proper, G -stable ideal $E \subsetneq K(X)[y_1, \dots, y_n]$ is called an **extended Derksen ideal** if it contains D .
- (c) For an extended Derksen ideal E , consider the ideal

$$I := \{f(\bar{x}_1, \dots, \bar{x}_n) \mid f \in K[y_1, \dots, y_n] \cap E\} \subseteq K[X].$$

Then E is called **tamely extended** if

$$\bigcap_{\sigma \in G} \sigma \cdot I = \{0\}.$$

Clearly D itself is a tamely extended Derksen ideal (in this case $I = \{0\}$). Before addressing geometric and computational aspects of (extended) Derksen ideals, we show how they can be used. The applications are linked to a monic reduced Gröbner basis, which makes the language introduced in the following definition convenient.

Definition 4.10.2 In the situation of Definition 4.10.1, let E be an extended Derksen ideal, and let \mathcal{G} be a monic reduced Gröbner basis of E with respect to an arbitrary monomial ordering. Then the K -subalgebra $A \subseteq K(X)$ generated by the coefficients of all polynomials from \mathcal{G} is called a **CAGE** (the acronym standing for Coefficient Algebra of a Gröbner basis of an Extended Derksen ideal). If E is tamely extended, A is called a **tame CAGE**.

Our first result generalizes results of Müller-Quade and Beth [56], Hubert and Kogan [57], Kemper [60], and Kamke and Kemper [58].

Theorem 4.10.3 (Invariant field) *In the situation of Definition 4.10.1, let A be a tame CAGE. Then*

$$K(X)^G = \text{Quot}(A).$$

We will prove the above theorem together with Theorems 4.10.4 and 4.10.5. Notice that Theorem 4.10.3, just as the other results from this section, does not require any hypothesis on properties of the group action (such as reductivity).

The following result allows the computation of a localization of the invariant ring.

Theorem 4.10.4 (Localized invariant ring) *In the situation of Definition 4.10.1, let A be a CAGE. Then $K[X]^G \subseteq A \subseteq K(X)^G$. If there exists a nonzero invariant $a \in K[X]^G$ with $A \subseteq K[X]_a$ ($=$ the $K[X]$ -algebra generated by a^{-1}), then*

$$K[X]_a^G = A_a. \quad (4.10.1)$$

We will discuss the existence of an $a \in K[X]^G$ as in the theorem in Sect. 4.10.2. Since G is not assumed to be reductive, the above theorem can be used to produce finitely generated localizations of nonfinitely generated invariant rings. This is an instance of the following interesting result (see Giral [61, Proposition 2.1(b)] or Kemper [62, Exercise 10.3]): For every subalgebra $B \subseteq A$ of a finitely generated domain A over a ring there exists a nonzero $a \in B$ such that B_a is finitely generated.

In the situation of Definition 4.10.1, let \mathcal{G} be a monic reduced Gröbner basis of an extended Derksen ideal E and let A be the corresponding CAGE. Using the normal form map given by \mathcal{G} , we define a new map as follows: An element $b \in K[X]$ can be written as $b = f(\bar{x}_1, \dots, \bar{x}_n)$ with $f \in K[y_1, \dots, y_n]$. Define

$$\varphi_{\mathcal{G}}: K[X] \rightarrow A, \quad b \mapsto (\text{NF}_{\mathcal{G}}(f))(0, \dots, 0)$$

(i.e., set all y_i equal to zero in the normal form of f). We call $\varphi_{\mathcal{G}}$ the **invariantization** map.

Theorem 4.10.5 (Invariantization) *The invariantization map $\varphi_{\mathcal{G}}$ is a well-defined homomorphism of $K[X]^G$ -modules. It restricts to the identity on $K[X]^G$. If (4.10.1) is satisfied, then $\varphi_{\mathcal{G}}$ uniquely extends to a $K[X]_a^G$ -linear projection $K[X]_a \twoheadrightarrow K[X]_a^G$, and in particular $K[X]_a^G$ is a direct summand of $K[X]_a$.*

The concept of invariantization was originally introduced by Fels and Olver [63], who used the term for a projection from the set of smooth functions on an open subset of a manifold to the set of local invariants under a group action. A (different) algebraic version of invariantization was introduced by Hubert and Kogan [64].

Proof of Theorems 4.10.3, 4.10.4 and 4.10.5 We assume that E is a (tamely) extended Derksen ideal and that \mathcal{G} is a monic reduced Gröbner basis of E . G acts on $K(X)[y_1, \dots, y_n]$ coefficient-wise. Hence for $\sigma \in G$ the set $\sigma \cdot \mathcal{G}$ is a monic reduced Gröbner basis of $\sigma \cdot E = E$. It follows from the uniqueness of

monic reduced Gröbner bases that $\sigma \cdot \mathcal{G} = \mathcal{G}$. Since the polynomials from \mathcal{G} have pairwise distinct leading monomials, this implies that σ fixes every polynomial in \mathcal{G} , so $\mathcal{G} \subseteq K(X)^G[y_1, \dots, y_n]$. Hence $A \subseteq K(X)^G$ and $\text{Quot}(A) \subseteq K(X)^G$, which establishes two of the claimed inclusions in Theorems 4.10.3 and 4.10.4.

Now let $b \in K(X)^G$ and suppose that E is tamely extended. The set $J := \{d \in K[X] \mid bd \in K[X]\} \subseteq K[X]$ is a nonzero, G -stable ideal. Therefore $J \not\subseteq I$ (with I the ideal from Definition 4.10.1(c)), since otherwise $J \subseteq \bigcap_{\sigma \in G} \sigma \cdot I = \{0\}$. So there exists $g \in K[y_1, \dots, y_n] \setminus E$ such that $g(\bar{x}_1, \dots, \bar{x}_n) \in J$. By the definition of J , this implies the existence of $f \in K[y_1, \dots, y_n]$ with

$$bg(\bar{x}_1, \dots, \bar{x}_n) = f(\bar{x}_1, \dots, \bar{x}_n). \quad (4.10.2)$$

Set $h := f - bg \in K(X)[y_1, \dots, y_n]$. For $\sigma \in G$, the G -invariance of b implies

$$h(\sigma \cdot \bar{x}_1, \dots, \sigma \cdot \bar{x}_n) = \sigma \cdot (f(\bar{x}_1, \dots, \bar{x}_n) - bg(\bar{x}_1, \dots, \bar{x}_n)) = 0.$$

Therefore $h \in D \subseteq E$ and, using the $K(X)$ -linearity of the normal form map, we conclude

$$0 = \text{NF}_{\mathcal{G}}(h) = \text{NF}_{\mathcal{G}}(f) - b \text{NF}_{\mathcal{G}}(g). \quad (4.10.3)$$

Since $g \notin E$ we have $\text{NF}_{\mathcal{G}}(g) \neq 0$, so (4.10.3) implies

$$b = \frac{\text{NF}_{\mathcal{G}}(f)}{\text{NF}_{\mathcal{G}}(g)}.$$

Since f , g , and \mathcal{G} are contained in $A[y_1, \dots, y_n]$, we can see from Algorithm 1.1.6 that also $\text{NF}_{\mathcal{G}}(f), \text{NF}_{\mathcal{G}}(g) \in A[y_1, \dots, y_n]$, so the above equation tells us

$$b \in \text{Quot}(A[y_1, \dots, y_n]) \cap K(X) = \text{Quot}(A).$$

This completes the proof of Theorem 4.10.3.

For the proof of Theorem 4.10.4 let $b \in K[X]^G$, so (4.10.2) holds with $g = 1$. Since E is a proper ideal, we have $\text{NF}_{\mathcal{G}}(1) = 1$ and (4.10.3) yields

$$b = \text{NF}_{\mathcal{G}}(f) \in A[y_1, \dots, y_n] \cap K(X) = A. \quad (4.10.4)$$

Now both inclusions $K[X]^G \subseteq A \subseteq K(X)^G$ are established. Assume $A \subseteq K[X]_a$ with $a \in K[X]^G$ nonzero. Then

$$K[X]_a^G \subseteq A_a \subseteq K[X]_a \cap K(X)^G = K[X]_a^G,$$

so Theorem 4.10.4 is proved.

We now turn our attention to Theorem 4.10.5. Let $f \in K[y_1, \dots, y_n]$ be a polynomial and $b := f(\bar{x}_1, \dots, \bar{x}_n) \in K[X]$. If $b = 0$, then $\text{NF}_{\mathcal{G}}(f) = 0$

by (4.10.4). This implies that φ_G does not depend on the choice of the polynomial in $K[y_1, \dots, y_n]$ that is used for its definition. If $b \in K[X]^G$, it follows from (4.10.4) that $\varphi_G(b) = b$. For $b \in K[X]$ not necessarily an invariant, we have already seen that $\text{NF}_G(f) \in A[y_1, \dots, y_n]$, so $\varphi_G(b) \in A$.

To prove that φ_G is a homomorphism of $K[X]^G$ -modules, take a further element $c = g(\bar{x}_1, \dots, \bar{x}_n) \in K[X] \setminus \{0\}$ such that $\frac{b}{c} \in K(X)^G$. By (4.10.3), this implies $\text{NF}_G(f) = \frac{b}{c} \text{NF}_G(g)$, and therefore $\varphi_G(b) = \frac{b}{c} \varphi_G(c)$. In particular, $\varphi_G(rc) = r\varphi_G(c)$ for $r \in K[X]^G$, and this also holds if $c = 0$. The additivity of φ_G follows from the additivity of the normal form. Finally, if (4.10.1) holds, then it is clear that $a^{-k}b \mapsto a^{-k}\varphi_G(b)$ gives a well-defined map that uniquely extends φ_G to a $K[X]_a^G$ -linear map. It also follows that this extension is the identity on $K[X]_a^G$ and that its image is $K[X]^G_a$. \square

See Kemper [59] for examples that show that the invariantization map need not be a ring homomorphism or G -equivariant, that it need not coincide with the Reynolds operator (if there is one), and that in general it depends on the choice of the extended Derksen ideal and the monomial ordering. If in the situation of Theorem 4.10.4 the equality (4.10.1) holds, then by Theorem 4.10.5, $K[X]_a^G$ is a direct summand of $K[X]_a$. This has beneficial consequences, which in the finite group case were studied by Broer [65]. In particular, the existence of the invariantization map $K[X]_a \rightarrow K[X]_a^G$ has the following consequence: For an ideal $I \subseteq K[X]_a^G$, forming the ideal in $K[X]_a$ generated by I and then intersecting it with $K[X]_a^G$ yields the original ideal I . This implies that the map $\text{Spec}(K[X]_a) \rightarrow \text{Spec}(K[X]_a^G)$ induced from the embedding is surjective. Moreover, we can use a result by Hochster and Huneke [66], which tells us that if $K[X]_a$ is a regular ring, then $K[X]_a^G$ is Cohen–Macaulay.

We now come back to Theorem 4.10.4 and ask how it can be used to calculate $K[X]^G$. If (4.10.1) holds, we can assume a to be one of the generators of A and then multiply the generators of A by powers of a to obtain elements of $K[X]^G$. This produces a subalgebra $B \subseteq K[X]^G$ that still satisfies $K[X]_a^G = B_a$. The following theorem deals with how to extract the invariant ring $K[X]^G$ in this situation.

Theorem 4.10.6 (Invariant ring) *In the situation of Definition 4.10.1, assume that $B \subseteq K[X]^G$ is a finitely generated K -subalgebra such that $K[X]_a^G = B_a$ with $a \in B$ nonzero. Define an ascending chain of subalgebras $B_0, B_1, B_2, \dots \subseteq K[X]$ by setting $B_0 := B$ and taking B_{k+1} to be the subalgebra generated by $a^{-1}B_k \cap K[X]$. Then*

$$K[X]^G = \bigcup_{k=0}^{\infty} B_k.$$

Moreover, all B_k are finitely generated. If $B_k = B_{k+1}$ for some k , then $K[X]^G = B_k$. If $K[X]^G$ is finitely generated then such a k exists.

The proof is quite straightforward and can be found in Kemper [59].

Remark 4.10.7 In Definition 4.10.1 the algebra $R = K[X]$ can be replaced by any finitely generated K -domain, with K any commutative ring. Then all the results from this section continue to hold. This generalization is quite fruitful in the case that G is a finite group. Then the Derksen ideal can be computed (see Sect. 1.2.3), and there exists $a \in R^G$ such that the CAGE A is contained in R_a . Moreover, if K is Noetherian, then R^G is finitely generated by Proposition 3.0.1, so the sequence B_k from Theorem 4.10.6 stops. We will present a procedure for computing this sequence (see Semi-algorithm 4.10.16). It turns out that this procedure generalizes to the case in which R is a finitely generated domain over a Zacharias ring K . In summary, we obtain an algorithm for computing invariant rings of finite groups acting on finitely generated domains over Zacharias rings. We refer to Kemper [59] for details. For an example, see Example 3.13.3. \triangleleft

4.10.2 The Italian Problem

Computing a localization of an invariant ring by means of Theorem 4.10.4 only works if there exists $a \in K[X]^G$ such that the CAGE A is contained in $K[X]_a$. We discuss this condition now.

Proposition 4.10.8 *In the situation of Definition 4.10.1, let A be a CAGE. If*

$$K(X)^G = \text{Quot}(K[X]^G),$$

then there exists a nonzero invariant $a \in R^G$ such that $A \subseteq K[X]_a$. If $K(X)^G = \text{Quot}(A)$ (which by Theorem 4.10.3 is guaranteed to hold if A is a tame CAGE), then the converse holds.

Proof Suppose $K(X)^G = \text{Quot}(K[X]^G)$. Since A is a finitely generated subalgebra of $K(X)^G$, we can choose $a \in K[X]^G \setminus \{0\}$ as a common denominator of the generators. Then $A \subseteq K[X]_a$. Conversely, $A \subseteq K[X]_a$ with $a \in K[X]^G$ nonzero implies

$$A \subseteq K[X]_a \cap K(X)^G = (K[X]_a)^G = (K[X]^G)_a \subseteq \text{Quot}(K[X]^G),$$

so $K(X)^G = \text{Quot}(A) \subseteq \text{Quot}(K[X]^G) \subseteq K(X)^G$. \square

The question whether the invariant field coincides with the field of fractions of the invariant ring is sometimes referred to as the *Italian problem* (see Mukai [67, page 183]). A typical example where $K(X)^G$ and $\text{Quot}(K[X]^G)$ fall apart is the action of the multiplicative group \mathbb{G}_m on K^2 with weight $(1, 1)$. This is treated in Example 4.10.11, which shows that nontamely extended Derksen ideals can serve to compute (a localization of) $K[X]^G$ even if the Italian problem has a negative answer.

The following theorem gives a positive answer to the Italian problem in some important cases.

Theorem 4.10.9 (Popov and Vinberg [4, Theorem 3.3]) *In the situation of Definition 4.10.1, the equality $K(X)^G = \text{Quot}(K[X]^G)$ holds if*

- (a) *the identity component G^0 is unipotent, or*
- (b) *$K[X]$ is a unique factorization domain and every homomorphism $G^0 \rightarrow \mathbb{G}_m$ to the multiplicative group is trivial.*

4.10.3 Geometric Aspects of Extended Derksen Ideals

In Sect. 4.1.1 the Derksen ideal (denoted by the letter b there) was defined as the vanishing ideal of the graph of the action, and it was an ideal in the polynomial ring $K[V \times V]$. In this section, the Derksen ideal D , defined in Definition 4.10.1, is an ideal in $K(X)[y_1, \dots, y_n]$, so geometric meaning (in terms of varieties over the algebraically closed field K) can only be assigned to the intersection $D' := K[X][y_1, \dots, y_n] \cap D$. It is easy to see that

$$D' = \bigcap_{\sigma \in G} (y_1 - \sigma \cdot \bar{x}_1, \dots, y_n - \sigma \cdot \bar{x}_n),$$

where the ideals on the right hand side are understood to be ideals in $K[X][y_1, \dots, y_n]$. From this it is clear that D' is the vanishing ideal of the set

$$\mathcal{D} := \{(\sigma \cdot x, x) \mid x \in X, \sigma \in G\} \subseteq X \times X \subseteq X \times K^n,$$

which is also the graph of the action. Moreover $D = D' \cdot K(X)[y_1, \dots, y_n]$ (the ideal in $K(X)[y_1, \dots, y_n]$ generated by D'), so we have a geometric description of D .

Let us now turn our attention to extended Derksen ideals. Given any ideal $E \subseteq K(X)[y_1, \dots, y_n]$, let $\mathcal{E} \subseteq X \times K^n$ be the closed subset defined by $E' := K[X][y_1, \dots, y_n] \cap E$. Provided that E is a radical ideal, E is G -stable if and only if the same holds for \mathcal{E} , and the Derksen ideal D is contained in E if and only if $\mathcal{E} \subseteq \overline{D}$. Moreover, since E' comes from an ideal in $K(X)[y_1, \dots, y_n]$, it follows that for every irreducible component \mathcal{E}_i of \mathcal{E} the first projection $\pi_X(\mathcal{E}_i)$ is dense in X . Conversely, for a nonempty closed subset $\mathcal{E} \subseteq X \times K^n$ whose irreducible components have this property, the vanishing ideal E' satisfies $E' \cdot K(X)[y_1, \dots, y_n] \subsetneq K(X)[y_1, \dots, y_n]$. In summary, we have seen that radical extended Derksen ideals correspond to nonempty G -stable closed subsets $\mathcal{E} \subseteq X \times K^n$ contained in \overline{D} such that for every irreducible component \mathcal{E}_i the first projection $\pi_X(\mathcal{E}_i) \subseteq X$ is dense.

The following result provides a more practical way of constructing extended Derksen ideals.

Proposition 4.10.10 *In the situation of Definition 4.10.1, let $(f_1, \dots, f_s) \subseteq K[y_1, \dots, y_n]$ be an ideal and consider the subvariety $Z \subseteq X$ of points vanishing at all $f_i(\bar{x}_1, \dots, \bar{x}_n)$. Suppose that the set*

$$\mathcal{M} := \{x \in X \mid \overline{G \cdot x} \cap Z \neq \emptyset\}$$

of points whose orbit closure passes through Z is dense in X . Then $E := D + (f_1, \dots, f_s) \subseteq K(X)[y_1, \dots, y_n]$ is an extended Derksen ideal.

Proof It is clear that E is G -stable and contains D , so we only need to show that E is a proper ideal. If $1 \in E$, then there would exist a nonzero $h \in K[X]$ with $h \in D' + (f_1, \dots, f_s) \subseteq K[X][y_1, \dots, y_n]$. We will show that this is not the case.

Let $x \in \mathcal{M}$. Then there exists $z \in \overline{G \cdot x} \cap Z$, so all f_i vanish at $(x, z) \in X \times K^n$. Take $h \in D'$. Then $h(x, \sigma \cdot x) = 0$ for all $\sigma \in G$, so the function $X \rightarrow K$, $y \mapsto h(x, y)$ vanishes on $G \cdot x$. Since it is continuous, it also vanishes on $\overline{G \cdot x}$. In particular, $h(x, z) = 0$. We conclude that $g(x, z) = 0$ for all $g \in D' + (f_1, \dots, f_s)$. If also $g \in K[X]$, then $g(x) = 0$. Since x was taken as an arbitrary element of \mathcal{M} , this implies $g = 0$. \square

The following simple example shows that (1) not all extended Derksen ideals are tamely extended, (2) the tameness hypothesis in Theorem 4.10.3 cannot be dropped, and (3) the converse of Proposition 4.10.8 may fail. In other words, nontamely extended Derksen ideals can help to achieve that $a \in K[X]^G$ exists with $A \subseteq K[X]_a$ (using the notation of Theorem 4.10.4), even if the Italian problem has a negative answer.

Example 4.10.11 Consider the action of the multiplicative group \mathbb{G}_m on $X = K^2$ with weight $(1, 1)$. The Derksen ideal is $D = (x_1 y_2 - x_2 y_1)$. Since all orbit closures contain the origin, Proposition 4.10.10 yields that $E = (y_1, y_2)$ is an extended Derksen ideal. The given basis is a monic reduced Gröbner basis, and Theorem 4.10.4 tells us that $K[X]^G = K$. This argument always applies when all orbit closures meet in one point, and yields the well-known result that in such a situation no nonconstant invariants exist.

Trying to apply Theorem 4.10.3 would yield $K(X)^G = K$, which is incorrect. This implies that E is not tamely extended. \triangleleft

Finally, let us consider a tamely extended Derksen ideal $E \subseteq K(X)[y_1, \dots, y_n]$. With $\mathcal{E} \subseteq X \times K^n$ the closed subset given by $K[X][y_1, \dots, y_n] \cap E$ and $\pi_{K^n}: X \times K^n \rightarrow K^n$ the second projection, the ideal $I \subseteq K[X]$ from Definition 4.10.1(c) defines the closed subset

$$Z := \overline{\pi_{K^n}(\mathcal{E})} \subseteq X.$$

The condition $\bigcap_{\sigma \in G} \sigma \cdot I = \{0\}$ is equivalent to the condition that the set $G \cdot Z$ of points from X whose orbit meets Z is dense in X . Notice the subtle difference between the set $G \cdot Z$ and the set \mathcal{M} from Proposition 4.10.10.

Conversely, let $Z \subseteq X$ be a closed subset such that $G \cdot Z$ is dense in X , and consider the set

$$\mathcal{E}_Z := \{(\sigma \cdot z, z) \mid z \in Z, \sigma \in G\} \subseteq X \times K^n,$$

which need not be closed. With $E'_Z \subseteq K[X][y_1, \dots, y_n]$ the vanishing ideal of \mathcal{E}_Z , it turns out that $E_Z := E'_Z \cdot K(X)[y_1, \dots, y_n]$ is a tamely extended Derksen ideal. Theorem 4.10.13 in this book contains a computational version of this statement.

In summary, tamely extended Derksen ideals E are intimately related to closed subsets $Z \subseteq X$ such that $G \cdot Z$ (the set of points whose orbit meets Z) is dense in X . It is not hard to work out what happens when one starts with a subset Z , passes to the corresponding E_Z and then back to a closed subset of X . However, it is not so clear what happens if one starts with E , forms Z and then E_Z .

Our condition on Z is related to the concept of a cross-section from Hubert and Kogan [57, Section 3.1], which in fact motivated the first definition, made in Kamke and Kemper [58], of extended Derksen ideals. However, cross-sections in the sense of Hubert and Kogan are more restrictive, since they require that a generic orbit meets the cross-section in only finitely many points.

We finish the section with a result on the dimension of the Derksen ideal. Recall from the remarks on geometric quotients on page 47 that X has an open subset where the maximal dimension of a G -orbit is attained.

Proposition 4.10.12 *In the situation of Definition 4.10.1 let d be the maximal dimension of a G -orbit in X . Then $K(X)[y_1, \dots, y_n]/D$ is equidimensional of dimension d (i.e., we get the same dimension whenever we replace D by a prime ideal lying minimally over D).*

The proof can be found in Kemper [68].

4.10.4 Computational Aspects of Extended Derksen Ideals

In this section we deal with the computation of extended Derksen ideals. Recall from Sect. 4.1.3 that the computation of the “classical” Derksen ideal comes down to calculating an elimination ideal. As we will see, the same is true for our generalized notions. But the computation can be made easier by using (tamely) extended Derksen ideals. We assume the situation of Definition 4.10.1. So we have $g_1, \dots, g_n \in K[G \times X] = K[G] \otimes K[X]$ such that

$$\sigma^{-1} \cdot \bar{x}_i = g_i(\sigma)$$

for $\sigma \in G$, $i = 1, \dots, n$ (see (4.9.4)).

Theorem 4.10.13 *Assume the above notation and hypotheses.*

(a) *Let*

$$\hat{D} := (y_1 - g_1, \dots, y_n - g_n) \subseteq K[G] \otimes K(X)[y_1, \dots, y_n].$$

Then the Derksen ideal is the elimination ideal

$$D = K(X)[y_1, \dots, y_n] \cap \hat{D}.$$

(b) Let $f_1, \dots, f_s \in K[y_1, \dots, y_n]$ be polynomials and set

$$\hat{E} := \hat{D} + (f_1, \dots, f_s) \subseteq K[G] \otimes K(X)[y_1, \dots, y_n].$$

If

$$K[X] \cap (f_1(g_1, \dots, g_n), \dots, f_s(g_1, \dots, g_n)) = \{0\} \quad (4.10.5)$$

(where the ideal $(f_1(g_1, \dots, g_n), \dots, f_s(g_1, \dots, g_n))$ is formed in $K[G] \otimes K[X]$), then the elimination ideal

$$E := K(X)[y_1, \dots, y_n] \cap \hat{E}$$

is a tamely extended Derksen ideal.

Remark With $Z \subseteq X$ the closed subset defined by the $f_i(\bar{x}_1, \dots, \bar{x}_n)$, the ideal $(f_1(g_1, \dots, g_n), \dots, f_s(g_1, \dots, g_n))$ corresponds to the set

$$\{(\sigma, x) \in G \times X \mid \sigma \cdot x \in Z\} \subseteq G \times X.$$

So the condition (4.10.5) is equivalent to $\overline{G \cdot Z} = X$. \triangleleft

Proof of Theorem 4.10.13

- (a) If $f \in D$, then for every $\sigma \in G$ we have $f(g_1(\sigma), \dots, g_n(\sigma)) = 0$, so $f \in \hat{D}$. Conversely, if $f \in K(X)[y_1, \dots, y_n] \cap \hat{D}$, then $f = \sum_{i=1}^n h_i(y_i - g_i)$ with $h_i \in K[G] \otimes K(X)[y_1, \dots, y_n]$, so for $\sigma \in G$ we obtain $f = \sum_{i=1}^n h_i(\sigma)(y_i - \sigma^{-1} \cdot \bar{x}_i)$, and then $f(\sigma^{-1} \cdot \bar{x}_1, \dots, \sigma^{-1} \cdot \bar{x}_n) = 0$. This implies $f \in D$.
- (b) Let G act on $G \times X$ by $\tau \cdot (\sigma, x) := (\sigma \tau^{-1}, \tau \cdot x)$. It is easy to check that the $g_i \in K[G \times X]$ are G -invariant under the induced action. The f_i are also invariant. It follows that \hat{E} is G -stable, hence the same is true for E . It follows from (a) that $D \subseteq E$. Consider the ideal

$$I := \{h(\bar{x}_1, \dots, \bar{x}_n) \mid h \in K[y_1, \dots, y_n] \cap E\} \subseteq K[X].$$

from Definition 4.10.1(c) and assume that there exists a nonzero element $d \in \bigcap_{\sigma \in G} \sigma \cdot I =: J$. Since the G -action on $K[X]$ is locally finite (see Lemma A.1.8) and J is G -stable, it contains a G -module V with $d \in V$. Choose a basis $d = d_1, d_2, \dots, d_m$ of V . There exists a matrix $(c_{j,i}) \in K[G]^{m \times m}$ such that $\sigma \cdot d_i = \sum_{j=1}^m c_{j,i}(\sigma) d_j$ for $1 \leq i \leq m$ and $\sigma \in G$. Since $d_j \in J \subseteq I$ we can write

$d_j = h_j(\bar{x}_1, \dots, \bar{x}_n)$ with $h_j \in K[y_1, \dots, y_n] \cap E$. We obtain

$$d_i = \sum_{j=1}^m c_{j,i}(\sigma)(\sigma^{-1} \cdot d_j) = \sum_{j=1}^m c_{j,i}(\sigma)h_j(g_1(\sigma), \dots, g_n(\sigma)),$$

which implies

$$d_i = \sum_{j=1}^m c_{j,i}h_j(g_1, \dots, g_n).$$

From $h_j \in E$ we obtain $h_j(g_1, \dots, g_n) \in \hat{E}$, so $d_i \in K[X] \cap \hat{E}$. In particular, this holds for $d = d_1$. So if we can show that $K[X] \cap \hat{E} = \{0\}$, we are done. An element $a \in K[X] \cap \hat{E}$ can be written as a linear combination of the $f_i(g_1, \dots, g_n)$ with coefficients in $K[G] \otimes K(X)$. There exists a nonzero $b \in K[X]$ such that ab is a linear combination of the same element with coefficients in $K[G] \otimes K[X]$. So $ab = 0$ by (4.10.5), and $a = 0$ follows. \square

Theorem 4.10.13 raises the question how we can find polynomials f_1, \dots, f_s satisfying (4.10.5), and whether they can be chosen such that the computation of the elimination ideal E becomes easier. The upshot of the following result is that the f_i can be chosen in such a way that the number of indeterminates involved in the computation of E is effectively reduced by d , the maximal dimension of a G -orbit. The theorem generalizes Theorem 3.3 from Hubert and Kogan [57].

Theorem 4.10.14 *In the situation of Theorem 4.10.13 let d be the maximal dimension of a G -orbit in X . There exist indices $1 \leq i_1 < \dots < i_d \leq n$ such that the classes of the y_{i_j} in $(K[G] \otimes K(X)[y_1, \dots, y_n])/\hat{D}$ are algebraically independent over L (with \hat{D} as in Theorem 4.10.13). Given such a choice of indices i_j , there exists an open, dense subset $U \subseteq K^d$ such that for $(\beta_1, \dots, \beta_d) \in U$ the polynomials*

$$f_j := y_{i_j} - \beta_j \in K[y_1, \dots, y_n] \quad (j = 1, \dots, d)$$

satisfy the condition (4.10.5) from Theorem 4.10.13. Moreover, the tamely extended Derksen ideal E formed as in Theorem 4.10.13 using such f_j satisfies

$$\dim(K(X)[y_1, \dots, y_n]/E) = 0.$$

Proof sketch Since $K(X)[y_1, \dots, y_n]/D$ has dimension d by Proposition 4.10.12 we can find y_{i_1}, \dots, y_{i_d} that are algebraically independent modulo D . With $A := K(X)[y_{i_1}, \dots, y_{i_d}]$ we obtain injective maps

$$A \rightarrow K(X)[y_1, \dots, y_n]/D \rightarrow (K[G] \otimes K(X)[y_1, \dots, y_n])/\hat{D}.$$

The ring on the right hand side is isomorphic to $K[G] \otimes K(X)$ and therefore equidimensional. By a standard result on fibers of morphisms (see Kemper [62, Theorem 10.5]), there exists a nonzero $a \in A$ such that for every maximal ideal $\mathfrak{m} \subset A$ with $a \notin \mathfrak{m}$ the fibers of \mathfrak{m} in the spectra of the above rings are nonempty. We also have the usual formula for the fiber dimensions, so in particular the fiber in $\text{Spec}(K(X)[y_1, \dots, y_n]/D)$ is zero-dimensional. Applying this to $\mathfrak{m} = (y_{i_1} - \beta_1, \dots, y_{i_d} - \beta_d) \subset A$ with $\beta_1, \dots, \beta_d \in K$ such that $a(\beta_1, \dots, \beta_d) \neq 0$ yields the desired results. \square

With Theorems 4.10.13 and 4.10.14, the construction of tamely extended Derksen ideals has become an algorithmic task. First, to find the number d and indices i_1, \dots, i_d as in Theorem 4.10.14, one can test algebraic independence of some y_{i_j} as elements of $(K[G] \otimes K(X)[y_1, \dots, y_n])/\hat{D}$ by using the isomorphism with $K[G] \otimes K(X)$. This means that the classes of the y_{i_j} are algebraically independent if and only if the $g_{i_j} \in K[G] \otimes K(X)$ are algebraically independent. This can be tested by using an elimination ideal (see Sect. 1.2.1). It may be useful to first obtain a good lower bound for d by picking random points from X and using the methods from Sect. 1.2.1 to compute their orbit closure.

Once suitable indices i_1, \dots, i_d are found, a vector $(\beta_1, \dots, \beta_d) \in K^d$ as in Theorem 4.10.14 can be found as follows: Fix an injective map $\eta: \mathbb{N}_0 \rightarrow K$. Then for $e = 0, 1, 2, \dots$, test for all $(a_1, \dots, a_d) \in \mathbb{N}_0^d$ with $\sum_{i=1}^d a_i = e$ whether $(\beta_1, \dots, \beta_d) := (\eta(a_1), \dots, \eta(a_d))$ qualifies. This will be successful for the following reason: By Theorem 4.10.14 there exists a nonzero polynomial $F \in K[t_1, \dots, t_d]$ such that if $F(\beta_1, \dots, \beta_d) \neq 0$, then the $f_j = y_{i_j} - \beta_j$ satisfy (4.10.5) from Theorem 4.10.13. But there exist $a_1, \dots, a_d \in \mathbb{N}_0$ such that $F(\eta(a_1), \dots, \eta(a_d)) \neq 0$, and the search will eventually find such a_j .

By putting together Theorems 4.10.3, 4.10.4, 4.10.13 and 4.10.14, we obtain the following algorithm.

Algorithm 4.10.15 (Computation of a localization of an invariant ring)

Input: A linear algebraic group G given as a subset of K^m by a radical ideal $I_G \subseteq K[z_1, \dots, z_m]$, and an irreducible G -variety X given by a prime ideal $I_X \subseteq K[x_1, \dots, x_n]$, with the action given by

$$\sigma \cdot v = (g_1(v, \sigma), \dots, g_n(v, \sigma))$$

for $v \in X$ and $\sigma \in G$, where $g_i \in K[x_1, \dots, x_n, z_1, \dots, z_m]$.

Output: Generators of the invariant field $K(X)^G$ and invariants $a, b_1, \dots, b_k \in K[X]^G$ such that

$$K[X]_a^G = K[a^{-1}, a, b_1, \dots, b_k].$$

The latter is only possible if $K(X)^G = \text{Quot}(K[X]^G)$ (see Theorem 4.10.9 for conditions which guarantee this).

- (1) With d equal to (or less than) the maximal dimension of a G -orbit in X , proceed as described above to find indices $i_1, \dots, i_d \in \{1, \dots, n\}$ and $\beta_1, \dots, \beta_d \in K$ such that the $f_j := y_{i_j} - \beta_j$ satisfy (4.10.5) from Theorem 4.10.13.
- (2) With y_1, \dots, y_n additional indeterminates, form the ideal $\hat{E} \subseteq K(X)[y_1, \dots, y_n, z_1, \dots, z_m]$ generated by $I_G, y_1 - g_1, \dots, y_n - g_n$, and f_1, \dots, f_d .
- (3) Compute a monic reduced Gröbner basis \mathcal{G} (with respect to an arbitrary monomial ordering) of the elimination ideal $E := K(X)[y_1, \dots, y_n] \cap \hat{E}$ (see Sect. 1.2).
- (4) Let $\frac{f_j}{h_j}$ ($j = 1, \dots, k$, $f_j, h_j \in K[X]$) be the coefficients appearing in the polynomials of \mathcal{G} . Then

$$K(X)^G = K\left(\frac{f_1}{h_1}, \dots, \frac{f_k}{h_k}\right).$$

- (5) Find $a \in K[X]^G \setminus \{0\}$ and $b_1, \dots, b_k \in K[X]$ such that $af_j = b_j h_j$ holds for all j . This can be done by allowing a and the b_j to be represented by (nonhomogeneous) polynomials in $K[x_1, \dots, x_n]$ of increasing maximal degree with unknown coefficients and testing the above equations and the G -invariance of a by using the normal form map. Then

$$K[X]_a^G = K[a^{-1}, a, b_1, \dots, b_k].$$

The search terminates only if a and the b_j exist, which is equivalent to $K(X)^G = \text{Quot}(K[X]^G)$.

Remark

- (a) For two reasons, it is impractical to compute the Gröbner basis \mathcal{G} directly in $K(X)[y_1, \dots, y_n]$: Computer algebra systems do not support coefficient fields as complicated as $K(X)$, and even if $K(X)$ is a rational function field, using it as a coefficient field for Gröbner basis computations is very inefficient, as experience shows. Instead, one can compute in the polynomial ring $K[x_1, \dots, x_n, y_1, \dots, y_n, z_1, \dots, z_m]$ and choose a block ordering which “emulates” computing a Gröbner basis in $K(X)[y_1, \dots, y_n]$.
- (b) If $K(X)^G \neq \text{Quot}(K[X]^G)$, it may be possible to enlarge the elimination ideal E by adding in suitable polynomials from $K[y_1, \dots, y_n]$ such that the resulting ideal is still proper. Doing so will open a chance that step 5 terminates. However, in this case the computation of the invariant field will not be correct. \triangleleft

Next we turn Theorem 4.10.6 into a procedure. Since the sequence of subalgebras B_k in the theorem becomes stationary only if the invariant ring is finitely generated, the procedure is a semi-algorithm in the sense that it need not terminate after finitely many steps. After running Algorithm 4.10.15, its output can be passed directly into Semi-algorithm 4.10.16, which will then compute generators of the invariant ring. Semi-algorithm 4.10.16 has appeared in a less explicit form in van den Essen [69].

Semi-algorithm 4.10.16 (Unlocalizing the invariant ring)

Input: A finitely generated algebra $R = K[x_1, \dots, x_n]/I$ over a field K , a finitely generated subalgebra $A = K[f_1 + I, \dots, f_k + I] \subseteq R$, and an element $a \in A$ such that multiplication by a is injective on R .

Output: Generators of the K -algebra $R \cap A_a$. The procedure terminates after finitely many steps if and only if $R \cap A_a$ is finitely generated.

- (1) Set $m := k$.
- (2) This step is optional. Substitute $f_1 + I, \dots, f_m + I$ by a smaller set of generators of the subalgebra generated by the $f_i + I$.
- (3) With additional indeterminates y_1, \dots, y_m , let $\hat{L} \subseteq K[x_1, \dots, x_n, y_1, \dots, y_m]$ be the ideal generated by I and $y_i - f_i$ ($i = 1, \dots, m$). Moreover, let $\hat{M} \subseteq K[x_1, \dots, x_n, y_1, \dots, y_m]$ be the ideal generated by \hat{L} and a polynomial $g \in K[y_1, \dots, y_m]$ with $g(f_1, \dots, f_m) + I = a$.
- (4) Compute the elimination ideal $M := K[y_1, \dots, y_m] \cap \hat{M}$. Let $L \subseteq K[y_1, \dots, y_m]$ be the ideal generated by the elimination ideal $K[y_1, \dots, y_m] \cap \hat{L}$ and by g .
- (5) If $M \subseteq L$, return $f_1 + I, \dots, f_m + I$ as the desired generators for $R \cap A_a$.
- (6) Choose $h_1, \dots, h_r \in M$ such that L together with the h_i generates M .
- (7) For $i = 1, \dots, r$ find $f_{m+i} \in K[x_1, \dots, x_n]$ such that

$$g(f_1, \dots, f_m)f_{m+i} - h_i(f_1, \dots, f_m) \in I$$

This can be done by allowing the f_{m+i} to be given by (nonhomogeneous) polynomials in $K[x_1, \dots, x_n]$ of increasing maximal degree with unknown coefficients and imposing the above ideal membership relation by using the normal form map.

- (8) Set $m := m + r$ and go to step 2.

Proof of correctness of Semi-algorithm 4.10.16 Let $B = K[f_1 + I, \dots, f_m + I]$, with f_1, \dots, f_m as in step 3, possibly after having performed steps 2, 3, 4, 5, 6, 7 and 8 several times. It is easy to see that for $h \in K[y_1, \dots, y_m]$ we have the equivalences

$$h(f_1, \dots, f_m) + I \in B \cap aR \iff h \in M$$

and

$$h(f_1, \dots, f_m) + I \in aB \iff h \in L.$$

The first equivalence implies the existence of f_{m+i} in step 7. We obtain $M/L \cong (B \cap aR)/aB \cong (a^{-1}B \cap R)/B$, so step 5 tests $a^{-1}B \cap R \subseteq B$. If this is not the case, the algorithm goes back to step 2 with B replaced by the algebra generated by $a^{-1}B \cap R$. So the algorithm produces the same ascending chain of subalgebras of R that is dealt with in Theorem 4.10.6, and the correctness and termination condition follow from that theorem. \square

4.10.5 The Additive Group

As we will explain here, computing a localization of the invariant ring of the additive group \mathbb{G}_a is particularly easy. The methods we present are based on ideas from van den Essen [69], Miyanishi [70], Freudenburg [71], and Tanimoto [72]. Suppose that the additive group \mathbb{G}_a acts nontrivially and morphically on an affine variety X . For the sake of simplicity we assume that X is irreducible, although the following material carries over, with slight modifications, to the case of reducible varieties. Writing $R := K[X]$ and identifying $K[\mathbb{G}_a] \otimes R$ with the polynomial ring $R[z]$, we see that the action induces a homomorphism $\varphi: R \rightarrow R[z]$ with the following property: If $s \in R$ and $\varphi(s) =: g(z)$, then

$$g(0) = s \quad \text{and} \quad \varphi(g(w)) = g(w + z), \quad (4.10.6)$$

where in the second equality φ is applied to polynomials in $R[w]$ coefficient-wise. The invariant ring is $R^{\mathbb{G}_a} := \ker(\varphi - \text{id})$. If $g(z) = \sum_{i=0}^d c_i z^i$ (with $c_i \in R$, $c_d \neq 0$), it follows that

$$\varphi(c_i) = \sum_{j=0}^{d-i} \binom{i+j}{i} c_{i+j} z^j. \quad (4.10.7)$$

In particular, $c := c_d \in R^{\mathbb{G}_a}$. Let $a \in R$ be another element and write $f(z) := \varphi(a)$. Then division with remainder yields

$$c^m f(z) = q(z)g(z) + r(z) \quad (4.10.8)$$

with $m \in \mathbb{N}_0$, $q(z), r(z) \in R[z]$ and $\deg_z(r(z)) < d$. Using (4.10.6), we get

$$\begin{aligned} q(w+z)g(w+z) + r(w+z) &= c^m f(w+z) = c^m \varphi(f(w)) = \\ \varphi(c^m f(w)) &= \varphi(q(w))\varphi(g(w)) + \varphi(r(w)) = \varphi(q(w))g(w+z) + \varphi(r(w)), \end{aligned}$$

so

$$g(w+z)(q(w+z) - \varphi(q(w))) + (r(w+z) - \varphi(r(w))) = 0.$$

Considering this as an equality of polynomials in w and using the w -degree, we conclude that $q(w+z) = \varphi(q(w))$ and $r(w+z) = \varphi(r(w))$. Substituting $w = 0$ yields

$$\varphi(q(0)) = q(z) \quad \text{and} \quad \varphi(r(0)) = r(z). \quad (4.10.9)$$

Write $\deg(s) := d$ and assume that s is chosen of minimal positive degree. Following Freudenburg [71] and Tanimoto [72], we express this by saying that s

is a *local slice*. We will treat the computation of a local slice later. It is not hard to see from (4.10.7) that the degree d of a local slice is a power of the characteristic of K , so it is 1 if $\text{char}(K) = 0$.

Example 4.10.17 This example shows that a local slice can have degree $d > 1$. Let $R = K[x, y]$ be a polynomial ring over a field of characteristic $p > 0$ and define $\varphi: R \rightarrow R[z]$ by

$$\varphi(x) = x + zy + z^p, \quad \varphi(y) = y.$$

Then $s = x$ is a local slice and its degree is p . \triangleleft

It follows from (4.10.9) that the degree of $r(0)$ equals the z -degree of $r(z)$, which is less than d . By the minimality of d , $r(0)$ must have degree 0, so $r(z) = r \in R_c^{\mathbb{G}_a}$.

Now we take the localization R_c with respect to the multiplicative set $\{1, c, c^2, \dots\}$. The map $R_c \rightarrow R_c[z]$ induced by φ also satisfies (4.10.6). (It corresponds to the \mathbb{G}_a -action on the subset $U \subseteq X$ where c does not vanish.) By abuse of notation we write φ for this map as well. By dividing (4.10.8) by c^m , replacing r and $q(z)$ by their products with c^{-m} and taking into account that the original r is an invariant, we obtain

$$f(z) = q(z)g(z) + r \tag{4.10.10}$$

with $r \in R_c^{\mathbb{G}_a}$. Since the remainder r has z -degree 0, it follows that the remainder for a product of elements of R_c is the product of the remainders. So we obtain a ring-homomorphism

$$\pi = \pi_s: R_c \rightarrow R_c^{\mathbb{G}_a}, \quad a \mapsto r,$$

which some authors (as Freudenburg [71], Tanimoto [72]) call the *Dixmier map*. It is clear that π fixes $R_c^{\mathbb{G}_a}$ element-wise, so it is a homomorphism of $R_c^{\mathbb{G}_a}$ -algebras. Of course, if the degree d of s is 1 and so $g(z)$ has the form $cz - b$, then $\pi(a)$ is formed by substituting $z = b/c$ in $\varphi(a)$. It may be interesting to note that the ideas so far can be developed within the framework of extended Derksen ideals, and then the Dixmier map turns out to be precisely the invariantization map from Theorem 4.10.5.

We are now ready to formulate an algorithm for computing a localization of the invariant ring, which includes the construction of a local slice. The algorithm specializes to the algorithm found by van den Essen [69] in the case $d = 1$.

Algorithm 4.10.18 (A localization of the invariant ring of a \mathbb{G}_a -action)

Input: An irreducible affine variety X with coordinate ring $R = K[X] = K[a_1, \dots, a_n]$, together with a \mathbb{G}_a -action given by the induced homomorphism $\varphi: R \rightarrow R[z]$, $a_i \mapsto g_i(z)$.

Output: A local slice $s \in R$, the leading coefficient $c \in R^{\mathbb{G}_a}$ of $\varphi(s)$, invariants $b_1, \dots, b_n \in R^{\mathbb{G}_a}$, and nonnegative integers m_i such that the homomorphism $\pi: R_c \rightarrow R_c^{\mathbb{G}_a}$ of K -algebras given by $a_i \mapsto c^{-m_i}b_i$, $c^{-1} \mapsto c^{-1}$ fixes $R_c^{\mathbb{G}_a}$. In

particular,

$$R_c^{\mathbb{G}_a} = K[b_1, \dots, b_n]_c.$$

- (1) For $i = 1, \dots, n$, set $b_i(z) := g_i(z)$. Set $s := c := 1$.
- (2) While not all $b_i(z)$ are constant polynomials, perform steps 3 and 4.
- (3) Choose $s \in R$ as a noninvariant coefficient of minimal degree d of one of the $b_i(z)$. One can use (4.10.7) for this. If $\text{char}(K) = 0$ then automatically $d = 1$.
- (4) With $c \in R^{\mathbb{G}_a}$ the leading coefficient of $g(z) := \varphi(s)$, perform division with remainder of the $g_i(z)$ by $g(z)$. This yields $q_i(z)$ and $b_i(z) \in R[z]$ such that

$$c^{m_i} g_i(z) = q_i(z)g(z) + b_i(z)$$

with $m_i \in \mathbb{N}_0$ and $\deg_z(b_i(z)) < d$.

- (5) This step is reached when all $b_i(z) = b_i$ are constant. Then the algorithm terminates.

Proof (Proof of correctness of Algorithm 4.10.18) After the algorithm has passed steps 3 and 4, it follows from (4.10.9) that

$$\deg(b_i(0)) = \deg_z(b_i(z)) < d.$$

Since $b_i(0)$ is one of the coefficients among which the new s is chosen when returning to step 3, this implies that the number d strictly decreases with each passage through the loop, guaranteeing termination. When step 5 is reached, the above formula shows that $\deg(b_i) = 0$, so $b_i \in R^{\mathbb{G}_a}$. Moreover, we have $\varphi(a_i) = c^{-m_i} q_i(z)g(z) + c^{-m_i} b_i$, so for all polynomials $F \in K[x_1, \dots, x_n]$ it follows that $\varphi(F(a_1, \dots, a_n)) - F(c^{-m_1} b_1, \dots, c^{-m_n} b_n) \in R_c[z] \cdot g(z)$. Since all elements from R are of the form $F(a_1, \dots, a_n)$, this implies that s is a local slice and that the Dixmier map π sends each a_i to $c^{-m_i} b_i$. Therefore

$$R_c^{\mathbb{G}_a} = \pi(R_c) = \pi(K[a_1, \dots, a_n]_c) \subseteq K[b_1, \dots, b_n]_c \subseteq R_c^{\mathbb{G}_a},$$

so the algorithm is correct. \square

The output of Algorithm 4.10.18 can be passed into Semi-algorithm 4.10.16.

Let us look at an example. The (in some sense) smallest example known to date of a nonfinitely generated invariant ring was given by Daigle and Freudenburg [73]. So it will be interesting to run Algorithm 4.10.18 on this example.

Example 4.10.19 Daigle and Freudenburg's example is an action of the additive group \mathbb{G}_a on the polynomial ring $R = \mathbb{C}[x_1, \dots, x_5]$, which is best defined in terms of the locally nilpotent derivation

$$\delta = x_1^3 \frac{\partial}{\partial x_2} + x_2 \frac{\partial}{\partial x_3} + x_3 \frac{\partial}{\partial x_4} + x_1^2 \frac{\partial}{\partial x_5},$$

so

$$\mathbb{C}[x_1, \dots, x_5]^{\mathbb{G}_a} = \ker(\delta).$$

Converting the action to our setting yields an action given by $\varphi: R \rightarrow R[z]$, $x_i \mapsto g_i$ with

$$\begin{aligned} g_1 &= x_1, & g_2 &= x_2 + zx_1^3, & g_3 &= x_3 + zx_2 + \frac{z^2}{2}x_1^3, \\ g_4 &= x_4 + zx_3 + \frac{z^2}{2}x_2 + \frac{z^3}{6}x_1^3, & \text{and} & & g_5 &= x_5 + zx_1^2. \end{aligned}$$

As a polynomial in z , g_2 has degree 1, so $s = x_2$ is a local slice with $c = x_1^3$. To obtain the b_i from the algorithm, we need to substitute $z = -x_2/x_1^3$ in the g_j and take numerators. We obtain

$$\mathbb{C}[x_1, \dots, x_5]_{x_1}^{\mathbb{G}_a} = \mathbb{C}[x_1^{-1}, x_1, b_1, b_2, b_3]$$

with

$$b_1 = 2x_1^3x_3 - x_2^2, \quad b_2 = 3x_1^6x_4 - 3x_1^3x_2x_3 + x_2^3, \quad \text{and} \quad b_3 = x_1x_5 - x_2.$$

So the localized invariant ring is isomorphic to a localized polynomial ring, the simplest possible structure. In particular, the invariant field is $\mathbb{C}(x_1, \dots, x_5)^{\mathbb{G}_a} = \mathbb{C}(x_1, b_1, b_2, b_3)$, so it is a purely transcendental field extension of \mathbb{C} . It seems odd that despite all this simplicity, the invariant ring itself is not finitely generated.

The Dixmier map π is given by

$$\pi(x_1) = x_1, \quad \pi(x_2) = 0, \quad \pi(x_3) = \frac{b_1}{2x_1^3}, \quad \pi(x_4) = \frac{b_2}{3x_1^6}, \quad \text{and} \quad \pi(x_5) = \frac{b_3}{x_1}.$$

This is not \mathbb{G}_a -equivariant. (In fact, there cannot exist a \mathbb{G}_a -equivariant projection $\mathbb{C}[x_1^{-1}, x_1, \dots, x_5] \rightarrow \mathbb{C}[x_1, \dots, x_5]_{x_1}^{\mathbb{G}_a}$ since such a map would produce a \mathbb{G}_a -complement of the invariant ring, which would then contain nonzero invariants by the unipotency of \mathbb{G}_a .)

In this example, \mathbb{C} may be replaced by any field K in which 2 and 3 are invertible. The localized invariant ring $R_c^{\mathbb{G}_a}$ will then be “the same” as over \mathbb{C} . But for K a field of characteristic p with $5 \leq p \leq 17$, running Semi-algorithm 4.10.16 shows that $K[x_1, \dots, x_5]^{\mathbb{G}_a}$ is finitely generated in these cases. These computations were done in MAGMA. So it appears that the infinite generation in this example occurs only in characteristic 0. \triangleleft

It can also be shown that the quotient $X_c := \text{Spec}(R_c) \rightarrow Y := \text{Spec}(R_c^{\mathbb{G}_a})$ computed by Algorithm 4.10.18 has very good geometric properties. In fact, it is a

universal geometric quotient, and there is an isomorphism $X_c \cong \mathbb{A}^1 \times Y$ of schemes over Y .

All of this can be carried further: first from the additive group to connected unipotent groups (see Greuel and Pfister [74], Sancho de Salas [75], Kemper [76]), and then to connected solvable groups. The following result emerges from this:

Theorem 4.10.20 (Kemper [76]) *Let G be a connected solvable linear algebraic group acting morphically on an irreducible affine variety X .*

- (a) *There is an algorithm that computes a nonzero semi-invariant $c \in R := K[X]$ and the invariant ring $(R_c)^G$. The algorithm also computes a homomorphism $R_c \rightarrow (R_c)^G$ of $(R_c)^G$ -algebras and its kernel. So the invariant ring requires no more generators than R_c . The algorithm involves no Gröbner basis computations, except perhaps for zero testing of elements of R .*
- (b) *The morphism $X_c := \text{Spec}(R_c) \rightarrow Y := \text{Spec}((R_c)^G)$ induced by the inclusion is a universal geometric quotient. Moreover, there is an isomorphism $X_c \cong \mathbb{A}^k \times T \times Y$ of Y -schemes, where T is a torus. In particular, all G -orbits in X_c are isomorphic to $\mathbb{A}^k \times T$ (but there is no “uniform” G -action on $\mathbb{A}^k \times T$). If G is unipotent, then $T = \{1\}$.*
- (c) *If R or R_c is a complete intersection, so is $(R_c)^G$.*
- (d) *The invariant field is $K(X)^G = \text{Quot}((R_c)^G)$, so the algorithm mentioned above also computes $K(X)^G$.*

4.10.6 Invariant Rings and Quasi-affine Varieties

Even if an invariant ring is not finitely generated and therefore does not correspond to an affine variety, there is a way to give it a “finite description”. In fact, if a linear algebraic group G acts on a normal variety X , then by Nagata [77, Chapter V, Proposition 4] the invariant ring $K[X]^G$ is isomorphic to the ring of regular functions on a quasi-affine variety, i.e., an open subvariety of an affine variety. A modern proof was given by Winkelmann [78], who also added a very interesting converse: If a quasi-affine variety has a normal ring of regular functions, then this is isomorphic to an invariant ring $K[X]^G$, where the group G can even be chosen to be the additive group. The ring of regular functions on a quasi-affine variety can be described explicitly as follows. Let Y be an irreducible affine variety and A its ring of regular functions, which is finitely generated. If a closed subset $Z \subseteq Y$ is given by an ideal $I \subseteq A$, then the ring of regular functions on the quasi-affine variety $U := Y \setminus Z$ is

$$K[U] = \{f \in \text{Quot}(A) \mid I^k \cdot f \subseteq A \text{ for some } k \in \mathbb{N}\} =: (A : I^\infty)_{\text{Quot}(A)}$$

(see [50, Lemma 2.3]). So the above result tells us that if $K[X]$ is normal, then there exists a finitely generated subalgebra $A \subseteq K[X]^G$ and an ideal $I \subseteq A$ such that

$$K[X]^G = (A : I^\infty)_{\text{Quot}(A)} . \quad (4.10.11)$$

This raises the question how A and I can be found constructively. Observe that if $K[X]_a^G = A_a$ with $A \subseteq K[X]$ a finitely generated algebra and $a \in A$ nonzero, then

$$K[X]^G = \{f \in K[X] \mid a^k f \in A \text{ for some } k \in \mathbb{N}\} =: (A : (a)^\infty)_{K[X]},$$

which looks deceptfully similar to (4.10.11). In fact, the following result shows that (4.10.11) can be achieved if there are enough representations of $K[X]^G$ as $(A : (a)^\infty)_{K[X]}$.

Proposition 4.10.21 (Dufresne [79]) *Let G be a linear algebraic group and X a normal G -variety. Let $A \subseteq K[X]^G$ be a subalgebra and $a_1, a_2 \in A$ such that*

$$A_{a_i} = K[X]_{a_i}^G \quad \text{for } i = 1, 2.$$

If the ideal $(a_1, a_2) \subseteq K[X]$ has height at least 2, then

$$K[X]^G = (A : (a_1, a_2)^\infty)_{\text{Quot}(A)}.$$

Proof Let $f \in K[X]^G$. Then there exist $k_i \in \mathbb{N}$ such that $a_i^{k_i} f \in A$. Setting $k := k_1 + k_2 - 1$, we see that $(a_1, a_2)^k \cdot f \subseteq A$, so $f \in (A : (a_1, a_2)^\infty)_{\text{Quot}(A)}$.

To prove the converse, we first remark that for every height one prime ideal $P \in \text{Spec}(K[X])$ there exists $i \in \{1, 2\}$ such that $a_i \notin P$. Therefore

$$K[X]_{a_1} \cap K[X]_{a_2} \subseteq \bigcap_{\substack{P \in \text{Spec}(K[X]) \\ \text{with } \text{ht}(P)=1}} K[X]_P = K[X],$$

where the last equation holds since X is normal (see Eisenbud [51, Corollary 11.4]). Now let $f \in (A : (a_1, a_2)^\infty)_{\text{Quot}(A)}$. Then there exists $k \in \mathbb{N}$ such that $a_i^k f \in A \subseteq K[X]$ for $i = 1, 2$, so $f \in K[X]_{a_1} \cap K[X]_{a_2} = K[X]$. Moreover, $f \in \text{Quot}(A) \subseteq K(X)^G$, so $f \in K[X]^G$. \square

Of course Proposition 4.10.21 only produces a representation of $K[X]^G$ as the ring of regular functions on a quasi-affine variety if A is finitely generated. This motivates the study of the set

$$F_R := \{a \in R \mid R_a \text{ is finitely generated as a } K\text{-algebra}\},$$

where R stands for any K -algebra. It turns out that F_R is always a radical ideal in R (see Onoda and Yoshida [80] or [50, Proposition 2.9]). Following [50], we call F_R the **finite generation ideal** of R . In our situation, the question is whether the ideal $(F_{K[X]^G}) \subseteq K[X]$ generated by the finite generation ideal of $K[X]^G$ has height at least 2. Then there exist a_1, a_2 and a finitely generated subalgebra $A \subseteq K[X]^G$ satisfying the hypotheses of Proposition 4.10.21. In general, this question seems to be open. But Derksen and Kemper [50] showed that if $K[X]$ is a factorial ring

and G is connected and unipotent, then $(F_{K[X]^G}) \subseteq K[X]$ has height at least 2 or $(F_{K[X]^G}) = K[X]$.

The paper [50] also contains an algorithm (Algorithm 3.9) for computing $K[X]^G$ as a ring of regular functions on a quasi-affine variety in this situation. However, this algorithm seems to be rather impractical: when applying it to the example of Daigle and Freudenburg [73] (see Example 4.10.19), the Gröbner basis computations quickly become too hard to perform.

Using Proposition 4.10.21 and choosing the a_i in an ad hoc fashion is a more promising approach, as the following continuation of Example 4.10.19 shows.

Example 4.10.22 We use the notation of Example 4.10.19. In that example we computed the following finitely generated localization of the invariant ring:

$$\mathbb{C}[x_1, \dots, x_5]_{x_1}^{\mathbb{G}_a} = \mathbb{C}[x_1, f_1, f_2, f_3]_{x_1}$$

with

$$f_1 = 2x_1^3x_3 - x_2^2, \quad f_2 = 3x_1^6x_4 - 3x_1^3x_2x_3 + x_2^3, \quad \text{and} \quad f_3 = x_1x_5 - x_2.$$

The localization by the invariant x_1 comes from the fact that x_2 is a local slice with $\varphi(x_2) = g_2 = x_2 + zx_1^3$. In order to apply Proposition 4.10.21 we need to compute the localization with respect to another invariant. For producing another local slice, we may use division with remainder according to (4.10.8). In fact, applying this to $\varphi(x_4) = g_4$ (as dividend) and $\varphi(x_3) = g_3$ (as divisor) yields

$$3x_1^3g_4 = g_2g_3 + (3x_1^3x_4 - x_2x_3 + f_1z).$$

By (4.10.9), this implies that $f := 3x_1^3x_4 - x_2x_3$ satisfies

$$\varphi(f) = f + zf_1,$$

so f is another local slice. Using this, we run Algorithm 4.10.18. So we need to substitute $z = -f/f_1$ in the polynomials g_1, \dots, g_5 defining the \mathbb{G}_a -action on the x_i , and then form the subalgebra generated by the numerators of these polynomials. These numerators are quite large, but using MAPLE, it can be verified that they all lie in the subalgebra generated by the invariants

$$x_1, \quad f_1, \quad f_3, \quad f_4 := \frac{f_1f_3 - f_2}{x_1}, \quad \text{and} \quad f_5 := \frac{f_1^3 + (f_1f_3 - x_1f_4)^2}{x_1^6},$$

where f_4 and f_5 turn out to be polynomials. The definition of f_4 implies that $f_2 \in A := \mathbb{C}[x_1, f_1, f_3, f_4, f_5]$, so

$$\mathbb{C}[x_1, \dots, x_5]_a^{\mathbb{G}_a} = A_a$$

holds for $a = x_1$ and $a = f_1$. Clearly $(x_1, f_1) \subseteq \mathbb{C}[x_1, \dots, x_5]$ has height 2, so

$$\mathbb{C}[x_1, \dots, x_5]^{\mathbb{G}_a} = (A : (x_1, f_1)^\infty)_{\text{Quot}(A)}$$

by Proposition 4.10.21. To write this as the ring of regular functions on a quasi-affine variety, we need the relations between the generators of A . It is obvious that the relation $x_1^6 f_5 - f_1^3 - (f_1 f_3 - x_1 f_4)^2 = 0$ (derived from the definition of f_5) generates the ideal of relations. It follows that $\mathbb{C}[x_1, \dots, x_5]^{\mathbb{G}_a}$ is isomorphic to the ring of regular functions on the quasi-affine variety

$$U = \{(\xi_1, \dots, \xi_5) \in \mathbb{C}^5 \mid \xi_1^6 \xi_5 - \xi_2^3 - (\xi_2 \xi_3 - \xi_1 \xi_4)^2 = 0, (\xi_1, \xi_2) \neq (0, 0)\}.$$

Notice that Winkelmann [78, Section 4] obtained the same generators f_i and the same quasi-affine variety U . Dufresne [79] presented this example from a slightly different point of view. \triangleleft

Further examples where a nonfinitely generated invariant ring is represented as the ring of regular functions on a quasi-affine variety can be found in Dufresne [79].

References

1. Harm Derksen, *Computation of invariants for reductive groups*, Adv. in Math. **141** (1999), 366–384.
2. Bernd Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, Wien, New York 1993.
3. Domingo Luna, *Slices étales*, Bull. Soc. Math. France **33** (1973), 81–105.
4. Vladimir L. Popov, Ernest B. Vinberg, *Invariant theory*, in: N. N. Parshin, I. R. Shafarevich, eds., *Algebraic Geometry IV*, Encyclopaedia of Mathematical Sciences **55**, Springer-Verlag, Berlin, Heidelberg 1994.
5. D. Khadzhiev, *Some questions in the theory of vector invariants*, Mat. Sb., Nov. Ser. **72** (3) (1967), 420–435, English Translation: Math. USSR, Sb. 1, 383–396..
6. Frank Grosshans, *Observable groups and Hilbert's fourteenth problem*, Am. J. Math. **95** (1) (1973), 229–253.
7. Lorenzo Robbiano, Moss Sweedler, *Subalgebra bases*, in: W. Bruns, A. Simis, eds., *Commutative Algebra*, Lecture Notes in Math. **1430**, pp. 61–87, Springer-Verlag, New York 1990.
8. Jozsef Beck, Vera T. Sós, *Discrepancy theory*, in: R. L. Graham, Martin Grötschel, Laszlo Lovász, eds., *Handbook of Combinatorics*, vol. 2, pp. 1405–1488, North-Holland, 1995.
9. Bernd Sturmfels, Neil White, *Gröbner bases and Invariant Theory*, Adv. Math. **76** (1989), 245–259.
10. Alfred Young, *On quantitative substitutional analysis (3rd paper)*, Proc. London Math. Soc. **28** (1928), 255–292.
11. W. V. D. Hodge, D. Pedoe, *Methods of Algebraic Geometry*, Cambridge University Press, Cambridge 1947.
12. James E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer-Verlag, Berlin, Heidelberg, New York 1980.
13. Hanspeter Kraft, *Geometrische Methoden in der Invariantentheorie*, Aspects of Mathematics **D1**, Vieweg, Braunschweig/Wiesbaden 1985.
14. Hermann Weyl, *Theorie der Darstellung kontinuierlicher halbeinfacher Gruppen durch lineare Transformationen I*, Math. Z. **23** (1925), 271–309.

15. Hermann Weyl, *Theorie der Darstellung kontinuierlicher halbeinfacher Gruppen durch lineare Transformationen II, III, IV*, Math. Z. **24** (1926), 328–376, 377–395, 789–791.
16. F. Adams, *Lectures on Lie Groups*, W.A. Benjamin, New York, Amsterdam 1969.
17. D. P. Zhelobenko, *Compact Lie Groups and Their Representations*, Transl. Math. Monogr. **40**, American Mathematical Society, Providence 1973.
18. Tonny A. Springer, *On the Invariant Theory of SU_2* , Nederl. Akad. Wetensch. Indag. Math. **42** (3) (1980), 339–345.
19. Theodor Bröcker, Tammo tom Dieck, *Representations of Compact Lie Groups*, vol. 98 of *Graduate Texts in Mathematics*, Springer-Verlag, New York–Berlin 1985.
20. Abraham Broer, *A new method for calculating Hilbert series*, J. of Algebra **168** (1994), 43–70.
21. A. M. Cohen, A. E. Brouwer, *The Poincaré series of the polynomials invariant under SU_2 in its irreducible representation of degree ≤ 17* , Math. Centrum Amsterdam Afd. Zuivere Wiskunde **ZW 134/79** (1979), 1–20.
22. Peter Littelmann, Claudio Procesi, *On the Poincaré series of the invariants of binary forms*, J. of Algebra **133** (1990), 490–499.
23. Jacques Dixmier, *Quelques résultats et conjectures concernant les séries de Poincaré des invariants des formes binaires*, in: *Sém. d’Algèbre P. Dubreil and M. P. Malliavin*, vol. 1146 of *Lecture Notes in Mathematics*, pp. 127–160, Springer-Verlag, Berlin 1985.
24. David Hilbert, *Über die vollen Invariantensysteme*, Math. Ann. **42** (1893), 313–370.
25. George Kempf, *The Hochster-Roberts theorem of invariant theory*, Michigan Math. J. **26** (1979), 19–32.
26. Harm Derksen, *Polynomial bounds for rings of invariants*, Proc. Amer. Math. Soc. **129** (2001), 955–963.
27. Vladimir L. Popov, *Constructive invariant theory*, Astérisque **87–88** (1981), 303–334.
28. Vladimir L. Popov, *The constructive theory of invariants*, Math. USSR Izvest. **10** (1982), 359–376.
29. Karin Hiss, *Constructive invariant theory for reductive algebraic groups*, preprint, 1993.
30. Robin Hartshorne, *Algebraic Geometry*, Springer-Verlag, New York, Heidelberg, Berlin 1977.
31. William Fulton, *Intersection Theory*, Springer-Verlag, Berlin, Heidelberg, New York 1984.
32. B. Kazarnovskij, *Newton polyhedra and the Bezout formula for matrix-valued functions of finite-dimensional representations*, Functional Analysis and its Applications **21(4)** (1987), 73–74.
33. Michel Brion, *Groupe de Picard et nombres caractéristiques des variétés sphériques*, Duke Math. J. **58** (1989), 397–424.
34. Harm Derksen, Hanspeter Kraft, *Constructive Invariant Theory*, in: *Algèbre non commutative, groupes quantiques et invariants (Reims, 1995)*, vol. 36 of *Sémin. Congr.*, pp. 221–244, Soc. Math. France, Paris 1997.
35. David Wehlau, *Constructive invariant theory for tori*, Ann. Inst. Fourier **43**, 4 (1993).
36. Guenter Ewald, Uwe Wessels, *On the ampleness of invertible sheaves in complete projective toric varieties*, Result. Math. **19** (1991), 275–278.
37. Victor G. Kac, Vladimir L. Popov, Ernest B. Vinberg, *Sur les groupes linéaires algébriques dont l’algèbre des invariants est libre*, C. R. Acad. Sci., Paris, Ser. A **283** (1976), 875–878.
38. Vladimir L. Popov, *Representations with a free module of covariants*, Funkts. Anal. Prilozh. **10** (1976), 91–92, English transl.: Funct. Anal. Appl. **10** (1997), 242–244.
39. Victor G. Kac, *On the question of describing the orbit space of linear algebraic groups*, Usp. Mat. Nauk **30** (6) (1975), 173–174, (Russian).
40. A. M. Popov, *Finite isotropy subgroups in general position in simple linear Lie groups*, Tr. Mosk. Math. O.-va **48** (1985), 7–59, English transl.: Trans. Mosc. Math. Soc. 1986 (1988), 3–63.
41. A. M. Popov, *Finite isotropy subgroups in general position in irreducible semisimple linear Lie groups*, Tr. Mosk. Math. O.-va **50** (1985), 209–248, English transl.: Trans. Mosc. Math. Soc. 1988 (1988), 205–249.

42. O. M. Adamovich, E. .O. Golovina, *Simple linear Lie groups having a free algebra of invariants*, in: *Vopr. Teor. Grupp. Gomologicheskoy Algebry*, vol. 2, pp. 3–41, 1979, English transl.: Sel. Math. Sov. **3** (2) (1984), 183–220.
43. Gerald Schwarz, *Representations of simple Lie groups with regular rings of invariants*, Invent. Math. **49** (1978), 167–197.
44. O. M. Adamovich, *Equidimensional representations of simple algebraic groups*, in: *Geom. Metod. Zadach. Algebry Anal.*, vol. 2, pp. 120–125, 1980, English transl.: Transl., II. Ser., Ann. Math. Soc. **128** (1986), 25–29.
45. Peter Littelmann, *Koreguläre und äquidimensionale Darstellungen*, J. of Algebra **123** (1) (1989), 193–222.
46. Victor G. Kac, *Some remarks on nilpotent orbits*, J. Algebra **64** (1980), 190–213.
47. Jiri Dadoc, Victor G. Kac, *Polar representations*, J. Algebra **92** (2) (1985), 504–524.
48. David Wehlau, *Equidimensional representations of 2-simple groups*, J. Algebra **154** (1993), 437–489.
49. Gregor Kemper, *Computing invariants of reductive groups in positive characteristic*, Transformation Groups **8** (2003), 159–176.
50. Harm Derksen, Gregor Kemper, *Computing invariants of algebraic group actions in arbitrary characteristic*, Adv. Math. **217** (2008), 2089–2129.
51. David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, New York 1995.
52. Martin Kreuzer, Lorenzo Robbiano, *Computational Commutative Algebra 1*, Springer-Verlag, Berlin 2000.
53. David Mumford, John Fogarty, Frances Kirwan, *Geometric Invariant Theory*, Ergebnisse der Math. und ihrer Grenzgebiete **34**, third edn., Springer-Verlag, Berlin, Heidelberg, New York 1994.
54. Masayoshi Nagata, *Invariants of a group in an affine ring*, J. Math. Kyoto Univ. **3** (1963/1964), 369–377.
55. Tobias Kamke, *Algorithms for the computation of invariant rings*, Dissertation, Technische Universität München, 2009.
56. Jörn Müller-Quade, Thomas Beth, *Calculating generators for invariant fields of linear algebraic groups*, in: *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (Honolulu, HI, 1999)*, Lecture Notes in Comput. Sci. **1719**, pp. 392–403, Springer, Berlin 1999.
57. Evelyne Hubert, Irina A. Kogan, *Rational invariants of an algebraic groups action. Constructing and rewriting*, J. Symb. Comput. **42** (2007), 203–217.
58. Tobias Kamke, Gregor Kemper, *Algorithmic invariant theory of nonreductive groups*, Qualitative Theory of Dynamical Systems **11** (2012), 79–110.
59. Gregor Kemper, *Using extended Derksen ideals in computational invariant theory*, J. Symbolic Comput. **72** (2016), 161–181.
60. Gregor Kemper, *The computation of invariant fields and a constructive version of a theorem by Rosenlicht*, Transformation Groups **12** (2007), 657–670.
61. José M. Giral, *Krull dimension, transcendence degree and subalgebras of finitely generated algebras*, Arch. Math. (Basel) **36** (1981), 305–312.
62. Gregor Kemper, *A Course in Commutative Algebra*, Graduate Texts in Mathematics **256**, Springer-Verlag, Berlin, Heidelberg 2011.
63. Mark Fels, Peter J. Olver, *Moving coframes. II. Regularization and theoretical foundations*, Acta Appl. Math. **55** (1999), 127–208.
64. Evelyne Hubert, Irina A. Kogan, *Smooth and algebraic invariants of a group action: local and global constructions*, Found. Comput. Math. **7** (2007), 455–493.
65. Abraham Broer, *The direct summand property in modular invariant theory*, Transform. Groups **10** (2005), 5–27.
66. Melvin Hochster, Craig Huneke, *Applications of the existence of big Cohen-Macaulay algebras*, Adv. Math. **113** (1995), 45–117.

67. Shigeru Mukai, *An introduction to invariants and moduli*, vol. 81 of *Cambridge Studies in Advanced Mathematics*, Cambridge University Press, Cambridge 2003, Translated from the 1998 and 2000 Japanese editions by W. M. Oxbury.
68. Gregor Kemper, *Using extended Derksen ideals in computational invariant theory*, preprint, Technische Universität München, 2014, <http://arxiv.org/abs/1310.6851v2>.
69. Arno van den Essen, *An algorithm to compute the invariant ring of a G_a -action on an affine variety*, J. Symbolic Comput. **16** (1993), 551–555.
70. Masayoshi Miyanishi, *Curves on rational and unirational surfaces*, vol. 60 of *Tata Institute of Fundamental Research Lectures on Mathematics and Physics*, Tata Institute of Fundamental Research, Bombay; Narosa Publishing House, New Delhi 1978.
71. Gene Freudenburg, *Algebraic theory of locally nilpotent derivations*, Encyclopaedia of Mathematical Sciences **136**, Springer-Verlag, Berlin 2006.
72. Ryuji Tanimoto, *An algorithm for computing the kernel of a locally finite iterative higher derivation*, J. Pure Appl. Algebra **212** (2008), 2284–2297.
73. Daniel Daigle, Gene Freudenburg, *A counterexample to Hilbert’s fourteenth problem in dimension 5*, J. Algebra **221** (1999), 528–535.
74. Gert-Martin Greuel, Gerhard Pfister, *Geometric quotients of unipotent group actions*, Proc. London Math. Soc. (3) **67** (1993), 75–105.
75. Carlos Sancho de Salas, *Invariant theory for unipotent groups and an algorithm for computing invariants*, Proc. London Math. Soc. (3) **81** (2000), 387–404.
76. Gregor Kemper, *Quotients by connected solvable groups*, in preparation, 2015.
77. Masayoshi Nagata, *Lectures on the Fourteenth Problem of Hilbert*, Tata Institute of Fundamental Research, Bombay 1965.
78. Jörg Winkelmann, *Invariant rings and quasiaffine quotients*, Math. Zeitschrift **244** (2003), 163–174.
79. Emilie Dufresne, *Finite separating sets and quasi-affine quotients*, J. Pure Appl. Algebra **217** (2013), 247–253.
80. Nobuharu Onoda, Ken-ichi Yoshida, *On Noetherian subrings of an affine domain*, Hiroshima Math. J. **12** (1982), 377–384.

Chapter 5

Applications of Invariant Theory

In this chapter we give a survey of some applications of invariant theory. The selection of topics is very incomplete, and so are certainly the references given for each topic. For example, we omit applications to projective geometry, which are very well explained in Sturmfels [1, Chap. 3]. We try to present a wide range of applications from different fields, and exemplify the use of invariant theory in each case.

5.1 Cohomology of Finite Groups

The cohomology of finite groups has been a very active field of research in recent years, and it has used invariant theory as a tool for computing cohomology rings (see Adem and Milgram [2]). The most important way invariant theory comes in is the following. Suppose that G is a finite group and V is a KG -module, and we want to determine the cohomology $H^*(G, V)$. Furthermore, suppose that we have an exact sequence of groups

$$1 \longrightarrow N \longrightarrow G \longrightarrow H \longrightarrow 1$$

such that the characteristic of K does not divide the order of H . Then there is a natural action of H on $H^*(N, V)$ (see Evens [3, p. 35]), and the restriction $\text{res}_{G,N}$ provides an isomorphism

$$H^*(G, V) \xrightarrow{\sim} H^*(N, V)^H. \quad (5.1.1)$$

This is well known and follows from the fact that $\text{cores}_{N,G} \circ \text{res}_{G,N}$ is multiplication by $|H|$ (see Evens [3, Proposition 4.2.2]) and that $\text{res}_{G,N} \circ \text{cores}_{N,G} = \sum_{\sigma \in H} \sigma$ by the Mackey formula (see Evens [3, Theorem 4.2.6]). A particularly interesting case

is $V = K$, the trivial module. The cup product gives $H^*(G, K)$ the structure of a (not quite commutative) K -algebra which is respected by the H -action, so the right-hand side of the isomorphism (5.1.1) is an invariant ring. The isomorphism does not hold if we drop the assumption that $\text{char}(K) \nmid |H|$, but then there is still a strong relation between $H^*(G, K)$ and $H^*(N, K)^H$ (see Adem and Milgram [4]).

There are two difficulties in applying the standard techniques of invariant theory to obtain $H^*(N, K)^H$. The first is that $H^*(N, K)$ is not commutative but instead $\alpha\beta = (-1)^{de}\beta\alpha$ for α and β homogeneous of degree d and e , respectively. This difficulty vanishes in characteristic 2, or if we consider only the even part of the cohomology. The second difficulty is that $H^*(N, K)$ is in general not a standard graded algebra, i.e., not generated in degree 1. Nevertheless, techniques from the above sections can be used in many examples to facilitate the computation of cohomology rings.

Example 5.1.1 (cf. Adem and Milgram [2]) We want to compute the mod 2 cohomology $H^*(A_4, \mathbb{F}_2)$ of the alternating group on four symbols. Let $N = \langle (1 2)(3 4), (1 3)(2 4) \rangle$ be the Sylow 2-subgroup. By Evens [3, p. 33] we have $H^*(N, \mathbb{F}_2) = \mathbb{F}_2[\alpha, \beta]$ with α, β algebraically independent of degree 1. A generator of G/N acts on $H^*(N, \mathbb{F}_2)$ by $\alpha \mapsto \beta$ and $\beta \mapsto \alpha + \beta$. In this situation we can use the standard algorithms from Sects. 3.5 and 3.7 and obtain

$$H^*(A_4, \mathbb{F}_2) = \mathbb{F}_2[A, B, C]$$

with

$$\begin{aligned} A &= \alpha^2\beta + \alpha\beta^2, \\ B &= \alpha^3 + \alpha\beta^2 + \beta^3, \\ C &= \alpha^2 + \alpha\beta + \beta^2, \end{aligned}$$

and, using the methods of Sect. 3.8, the relation

$$C^3 + A^2 + AB + B^2 = 0.$$

5.2 Galois Group Computation

If $f \in K[X]$ is a separable polynomial over a field K , then the Galois group $\text{Gal}(N/K)$ of the splitting field N of f over K acts on the zeros $\alpha_1, \dots, \alpha_n \in N$ of f . This yields a faithful permutation representation $\text{Gal}(N/K) \rightarrow S_n$, whose image is denoted by $\text{Gal}(f)$, the Galois group of f . Of course $\text{Gal}(f)$ is only determined up to conjugacy in S_n . In this section we look at methods for computing the Galois group. We will discuss the basic ideas of Stauduhar's algorithm [5], which is the one that is most

widely used. Our presentation is strongly influenced by the article of Geißler and Klünners [6].

Suppose we know already that $\text{Gal}(f) \leq G$ for a subgroup $G \leq S_n$ (this is always true for $G = S_n$). Given a smaller group $H \leq G$ (often a maximal subgroup of G), we would like to check whether $\text{Gal}(f) \leq H$. The basic idea is to use a polynomial $F \in K[x_1, \dots, x_n]^H$ such that $\sigma \cdot F \neq F$ for all $\sigma \in G \setminus H$. Such a polynomial is called a **G -relative H -invariant**. In other words, we are looking for a polynomial $F \in K[x_1, \dots, x_n]$ with $\text{Stab}_G(F) = H$. G -relative H -invariants always exist, one (standard) example being provided by

$$F := \sum_{\sigma \in H} \left(\sigma \cdot \prod_{i=1}^{n-1} x_i^i \right).$$

Since it is important for the efficiency of Stauduhar's algorithm to obtain "simple" G -relative H -invariants, Geißler and Klünners [6] propose to compare the Hilbert series of $K[x_1, \dots, x_n]^G$ and $K[x_1, \dots, x_n]^H$, which can be computed by Molien's formula (see Theorem 3.4.2 and (3.4.5)). If H is maximal in G , the minimal degree of a G -relative H -invariant can be read off from this comparison, and then the actual construction of F can be done by forming H -orbit sums of monomials. In some special situations it is also possible to obtain G -relative H -invariants whose evaluation requires a fairly small number of arithmetic operations (see Eichenlaub [7] or Geißler and Klünners [6]). Geißler's master thesis [8, Section 5.2] has some examples where a good choice of invariants dramatically reduces the number of arithmetic operations. The following proposition explains why G -relative H -invariants are useful for Galois group computation.

Proposition 5.2.1 *Suppose that in the above situation F is a G -relative H -invariant and*

$$F(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)}) \neq F(\alpha_1, \dots, \alpha_n) \quad \text{for all } \sigma \in G \setminus H, \quad (5.2.1)$$

where $\alpha_1, \dots, \alpha_n$ are the roots of f , and $\text{Gal}(f) \leq G$. Then

$$\text{Gal}(f) \leq H \iff F(\alpha_1, \dots, \alpha_n) \in K.$$

Proof Write $\gamma := F(\alpha_1, \dots, \alpha_n)$. If $\text{Gal}(f) \leq H$, then for every $\sigma \in \text{Gal}(f)$ we have $\sigma \cdot F = F$ and therefore $\sigma \cdot \gamma = \gamma$ for every $\sigma \in \text{Gal}(N/K)$, since the Galois action on the α_i is the same as the permutation action on the x_i . Thus $\gamma \in N^{\text{Gal}(N/K)} = K$. On the other hand, if $\text{Gal}(f) \not\leq H$, there exists $\sigma \in \text{Gal}(N/K)$ whose action on the α_i lies in $G \setminus H$. Hence by (5.2.1) we have $\sigma \cdot \gamma \neq \gamma$, so $\gamma \notin K$.

We will explain later how the condition $F(\alpha_1, \dots, \alpha_n) \in K$ can be tested. First we discuss how the hypothesis (5.2.1) can be achieved. Fortunately, one does not have to change F for this, but can use Tschirnhaus transformations.

Lemma 5.2.2 (Girstmair [9]) Suppose that K is an infinite field. Then in the situation of Proposition 5.2.1 there exist $c_0, \dots, c_{n-1} \in K$ such that for $\beta_i := \sum_{j=0}^{n-1} c_j \alpha_i^j$ we have

$$F(\beta_{\sigma(1)}, \dots, \beta_{\sigma(n)}) \neq F(\beta_1, \dots, \beta_n) \quad \text{for all } \sigma \in G \setminus H$$

and $\beta_i \neq \beta_j$ for $i \neq j$. In fact, if $S \subset K$ is any set with $|S| > \deg(F) \cdot \binom{[G:H]}{2} + \binom{n}{2}$, the c_i can be chosen from S .

Proof Let C_0, \dots, C_{n-1} be indeterminates over N . Then the $B_i := \sum_{j=0}^{n-1} C_j \alpha_i^j$ are algebraically independent over N (Vandermonde determinant). Set

$$D(C_0, \dots, C_{n-1}) :=$$

$$\prod_{1 \leq i < j \leq n} (B_i - B_j) \prod_{1 \leq i < j \leq m} (F(B_{\sigma_i(1)}, \dots, B_{\sigma_i(n)}) - F(B_{\sigma_j(1)}, \dots, B_{\sigma_j(n)})),$$

where $\sigma_1, \dots, \sigma_m$ is a set of left coset representatives of H in G . Since $\sigma \cdot F \neq \tau \cdot F$ for $\sigma H \neq \tau H$, it follows that $D(C_0, \dots, C_{n-1}) \neq 0$. Since $|S| > \deg(D)$, there exists $c_0 \in S$ with $D(c_0, C_1, \dots, C_{n-1}) \neq 0$. Continuing this way, we find $c_0, \dots, c_{n-1} \in K$ such that $D(c_0, \dots, c_{n-1}) \neq 0$. But this means that $F(\beta_{\sigma(1)}, \dots, \beta_{\sigma(n)}) \neq F(\beta_1, \dots, \beta_n)$ for $\sigma \in G \setminus H$, and $\beta_i \neq \beta_j$ for $i \neq j$.

If $\hat{f} := \prod_{i=1}^n (X - \beta_i) \in K[X]$ with the β_i as in Lemma 5.2.2, then of course $\text{Gal}(\hat{f}) = \text{Gal}(f)$. The rough algorithm for computing $\text{Gal}(f)$ is now clear: First (pre-)compute the subgroup lattice of S_n , and for each pair $H \leq G$ of subgroups with H maximal in G find a G -relative H -invariant. Then start with S_n and use Proposition 5.2.1 and if necessary Tschirnhaus transformations to walk down the subgroup lattice until a group $G \leq S_n$ is reached such that $\text{Gal}(f) \leq G$ but $\text{Gal}(f) \not\leq H$ for every maximal subgroup $H \leq G$. Then $\text{Gal}(f) = G$. Apart from a number of implementation issues, there is still one fundamental problem with this idea: We do not usually know (the exact values of) the roots α_i of f . We will discuss two basic approaches to handle this problem, both of which involve the resolvent, defined as follows: For $F \in K[x_1, \dots, x_n]$ a G -relative H -invariant polynomial, define the “**resolvent form**” as

$$R_{G,H,F}(X) := \prod_{\sigma \in G/H} (X - \sigma \cdot F) \in K[x_1, \dots, x_n]^G[X],$$

where the σ run through a set of left coset representatives. The **resolvent** is then defined by

$$\bar{R}_{G,H,F}(X) := \prod_{\sigma \in G/H} (X - F(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})) \in K[X],$$

i.e., by substituting $x_i = \alpha_i$ in $R_{G,H,F}(X)$. Proposition 5.2.1 now translates to:

Theorem 5.2.3 *Let $f \in K[x]$ be a separable polynomial of degree n and $G \leq S_n$ a subgroup with $\text{Gal}(f) \leq G$. Moreover, let $H < G$ be a proper subgroup and $F \in K[x_1, \dots, x_n]$ a G -relative H -invariant. Suppose that the resolvent $\bar{R}_{G,H,F}(X) \in K[X]$ has nonzero discriminant. Then the following statements are equivalent:*

- (a) *There exists $\sigma \in G$ such that $\text{Gal}(f) \leq \sigma H \sigma^{-1}$.*
- (b) *$\bar{R}_{G,H,F}(X)$ has a zero in K .*

In this case, after a suitable renumbering of the zeros of f we may assume that $\text{Gal}(f) \leq H$.

Example 5.2.4 Suppose that $\text{char}(K) \neq 2$. Then

$$F := \prod_{1 \leq i < j \leq n} (x_i - x_j)$$

is an S_n -relative A_n -invariant. The resolvent is

$$\bar{R}_{S_n, A_n, F}(X) = X^2 - D(f),$$

where $D(f)$ is the discriminant. In this case, Theorem 5.2.3 yields the well-known criterion that $\text{Gal}(f) \leq A_n$ if and only if $D(f)$ is a square in K . \triangleleft

We now present two approaches how to handle the fact that the zeros α_i of f are not known.

5.2.1 Approximating Zeros

The most obvious and most practical approach is to approximate the α_i and work with approximations instead of exact values. Of course it depends on the ground field K whether and in what sense we can talk about “approximation” at all. Fields like \mathbb{Q} or rational function fields $k(t)$ lend themselves for approximating zeros. Moreover, we need to be able to detect whether for a G -relative H -invariant $F \in K[x_1, \dots, x_n]$ we have $F(\alpha_1, \dots, \alpha_n) \in K$ by evaluating F at the approximations of the α_i . The most important case is $K = \mathbb{Q}$. For this case a p -adic approximation of the α_i , using a suitable prime p , turns out to be practical (see Geißler and Klüners [6]). Of course numeric approximations also work. Moreover, the α_i can be assumed to be integral over \mathbb{Z} (simply by multiplying them with a suitable integer). If the G -relative H -invariant polynomials F are chosen to lie in $\mathbb{Z}[x_1, \dots, x_n]$, then it only has to be tested whether $F(\alpha_1, \dots, \alpha_n) \in \mathbb{Z}$. This makes it possible for Geißler and Klüners to derive criteria for the accuracy of the approximation of the α_i . If the accuracy meets these criteria, then it is possible to decide whether $F(\alpha_1, \dots, \alpha_n)$ lies in \mathbb{Z} . It can also be decided from the approximation whether $\bar{R}_{G,H,F}(X)$ is separable.

These remarks should give the reader a general idea how algorithms for computing $\text{Gal}(f)$ by approximating zeros can be set up. There are many details and implementation issues that we omit. For these, we refer the reader to Geißler and Klünner [6]. A fairly recent implementation of algorithms for Galois group computation was provided by Fieker and Klünner [10]. In this implementation, G -relative H -invariants are not precomputed but are generated “dynamically.” Therefore the implementation has no built-in degree limit. Indeed, the authors have managed to determine Galois groups of polynomials of degrees exceeding 100 with this implementation.

5.2.2 The Symbolic Approach

A different approach which avoids approximations was proposed by Colin [11]. The idea uses the fact that the resolvent form $R_{G,H,F}(X)$ has coefficients in $K[x_1, \dots, x_n]^G$. Therefore these coefficients can be expressed as a polynomial in generating invariants for $K[x_1, \dots, x_n]^G$. This can be applied most readily in the case $G = S_n$, i.e., if we are dealing with absolute resolvents. Then

$$R_{S_n,H,F}(X) = X^n + \sum_{i=1}^n H_i(s_1, \dots, s_n) X^{n-i}$$

with s_i the i -th elementary symmetric polynomial and $H_i \in K[x_1, \dots, x_n]$. The H_i can be found by Algorithm 3.10.2. If

$$f = X^n + \sum_{i=1}^n (-1)^i a_i X^{n-i},$$

then $a_i = s_i(\alpha_1, \dots, \alpha_n)$, and therefore the resolvent can be expressed as

$$\bar{R}_{S_n,H,F}(X) = X^n + \sum_{i=1}^n H_i(a_1, \dots, a_n) X^{n-i}.$$

Thus it is not necessary to know the zeros α_i in order to find the resolvent. It is also easy to apply Tschirnhaus transformations to arrange that $\bar{R}_{S_n,H,F}(X)$ is separable (using Lemma 5.2.2). In fact, if $\beta_i = g(\alpha_i)$ with $g \in K[X]$ a polynomial whose coefficients were chosen randomly, then

$$\prod_{i=1}^n (X - g(\alpha_i)) = X^n + \sum_{i=1}^n h_i(s_1, \dots, s_n) X^{n-i},$$

where the $h_i \in K[x_1, \dots, x_n]$ can again be computed by Algorithm 3.10.2. Then for $\hat{f} := \prod_{i=1}^n (X - \beta_i)$ we have

$$\hat{f} = X^n + \sum_{i=1}^n h_i(a_1, \dots, a_n) X^{n-i},$$

where the a_i are again the coefficients of the original polynomial f .

Things become much more delicate if we are dealing with the relative case, i.e., $G \not\leq S_n$. Again the task is to find the (relative) resolvent $\bar{R}_{G,H,F}(X)$ without knowing the α_i . Suppose that we have descended along a chain of subgroups $S_n = G_0 \not\geq G_1 \not\geq \dots \not\geq G_k = G$ and proved, using Theorem 5.2.3, that $\text{Gal}(f) \leq G$. If F_i is a G_{i-1} -relative G_i -invariant, this amounts to having found the values $b_i := F_i(\alpha_1, \dots, \alpha_n) \in K$ (after a suitable renumbering of the unknown zeros). By Galois theory we know that $K(x_1, \dots, x_n)^{G_i} = K(x_1, \dots, x_n)^{G_{i-1}}(F_i)$. Thus $K(x_1, \dots, x_n)^G = K(s_1, \dots, s_n, F_1, \dots, F_k)$. In order to find $\bar{R}_{G,H,F}(X)$, we want to write the resolvent form $R_{G,H,F}(X)$ in terms of the s_i and F_i . Each coefficient of $R_{G,H,F}(X)$ lies in $K(x_1, \dots, x_n)^G = K(s_1, \dots, s_n, F_1, \dots, F_k)$, hence we can write

$$R_{G,H,F}(X) = X^n + \sum_{i=1}^n H_i(s_1, \dots, s_n, F_1, \dots, F_k) X^{n-i} \quad (5.2.2)$$

with H_i rational functions in $n+k$ arguments. In this case Algorithm 3.10.2 or any other standard algorithm using linear algebra does not help to find the H_i . Instead an algorithm of Sweedler [12], which involves Gröbner bases, can be used. Substituting the α_i into (5.2.2) yields

$$\bar{R}_{G,H,F}(X) = X^n + \sum_{i=1}^n H_i(a_1, \dots, a_n, b_1, \dots, b_k) X^{n-i},$$

but only if no zero-division occurs on the right hand side. Such a zero-division can be avoided by using Tschirnhaus transformations again, in the spirit of Lemma 5.2.2. Then of course applying a Tschirnhaus transformation changes the values of the a_i and b_i . All the questions arising here can be solved, but at this point we prefer to stop and refer the reader to Colin [11] for further details.

Vectorial Polynomials.

Suppose that we have a Galois field extension N/K with $\mathbb{F}_q \subseteq K$. Let $\mathcal{M} \subset N$ be a finite set such that $N = K(\mathcal{M})$ and $\text{Gal}(N/K)$ maps \mathcal{M} to itself. Then $\text{Gal}(N/K)$ also acts on the \mathbb{F}_q -span V of \mathcal{M} , and $N = K(V)$, so the action is faithful. The polynomial $f := \prod_{\alpha \in V} (X - \alpha) \in K[X]$ has the form

$$f = X^{q^n} + a_1 X^{q^{n-1}} + \dots + a_{n-1} X^q + a_n X$$

(see Wilkerson [13]). Polynomials of this form are called **vectorial** (see Abhyankar [14]). Obviously the set of zeros of *any* vectorial polynomial is a vector space over \mathbb{F}_q . In the same way as $\text{Gal}(f)$ is the image of $\text{Gal}(N/K)$ under the permutation representation on the roots of f , we define $\text{Gal}_{\text{vect}}(f)$ to be the image of $\text{Gal}(N/K)$ under the representation $\text{Gal}(N/K) \rightarrow \text{GL}(V)$. So $\text{Gal}_{\text{vect}}(f) \leq \text{GL}(V)$ is a finite linear group, and we can try to formulate an analogue of Stauduhar's method for the determination of $\text{Gal}_{\text{vect}}(f)$. This method will use invariants in $\mathbb{F}_q[V]^G$ for subgroups $G \leq \text{GL}(V)$ to test whether $\text{Gal}_{\text{vect}}(f) \leq G$.

5.3 Noether's Problem and Generic Polynomials

In inverse Galois theory (see Malle and Matzat [15]) one is interested in obtaining polynomials which have a given group as Galois group. It is even more desirable to have a polynomial which parametrizes all polynomials with a given group, or at least all Galois field extensions having this group. A typical example is the polynomial $X^2 - t$, which parametrizes all C_2 -extensions over a field of characteristic not 2. Such polynomials are called generic. More precisely, we define:

Definition 5.3.1 Let K be a field and G a finite group. A separable polynomial $g(t_1, \dots, t_m; X) \in K(t_1, \dots, t_m)[X]$ with coefficients in the rational function field $K(t_1, \dots, t_m)$ is called **generic** for G over K if the following two properties hold:

- (a) The Galois group of g (as a polynomial in X) is G ;
- (b) if L is an infinite field containing K and N/L is a Galois field extension with group G , then there exist $\lambda_1, \dots, \lambda_m \in L$ such that N is the splitting field of $g(\lambda_1, \dots, \lambda_m; X)$ over L .

A connection between generic polynomials and invariant theory was discovered by Emmy Noether [16], who proved that if the invariant field $K(x_1, \dots, x_n)^G$ of a permutation group $G \leq S_n$ is purely transcendental as a field extension of K , then a generic polynomial for G exists and has n parameters. A generic polynomial constructed in this way even parametrizes (almost) all polynomials with Galois group G . Because of this result, the question whether the invariant field of a finite linear group is purely transcendental is known as **Noether's problem**. Apart from a complete answer in the case of abelian groups given by Lenstra [17] and a few examples and counterexamples (see Swan [18] and Saltman [19]), not much is known about Noether's problem. In particular, we have no algorithm for deciding whether the invariant field of a given finite linear group is purely transcendental or not. For a survey on Noether's problem we refer the reader to Saltman [20] or Kemper [21].

The following theorem gives a somewhat more general construction method for generic polynomials, which is not restricted to permutation representations.

Theorem 5.3.2 (see Kemper and Mattig [22]) *Let G be a finite group and V an m -dimensional, faithful linear representation of G over a field K . If the invariant field $K(V)^G$ is purely transcendental over K , then there exists a generic polynomial with m parameters for G over K .*

The generic polynomial whose existence is guaranteed by Theorem 5.3.2 can be constructed as follows: Assume that $K(V)^G = K(\varphi_1, \dots, \varphi_m)$ (which implies that the φ_i are algebraically independent). Choose a finite, G -stable subset $\mathcal{Y} \subset K(V)$ on which G acts faithfully, and set

$$f(X) := \prod_{y \in \mathcal{Y}} (X - y) \in K(V)[X].$$

The coefficients of f are G -invariant, so f can be written as $f(X) = g(\varphi_1, \dots, \varphi_m; X)$ with $g \in K(t_1, \dots, t_m)[X]$. Then $g(t_1, \dots, t_m; X)$ is the desired generic polynomial for G over K . We say that $\varphi_1, \dots, \varphi_m$ form a **minimal basis** of the invariant field. Thus the knowledge of a minimal basis leads directly to the construction of a generic polynomial. The advantage of working with linear representations instead of permutation representations is that they usually lead to simpler generic polynomials. Moreover, considering a representation of small degree often makes it easier to give a positive answer to Noether's problem and to find a minimal basis.

Example 5.3.3 ([22]) We would like to construct a generic polynomial for the cyclic group $G = C_4$ over $K = \mathbb{Q}$. The smallest faithful representation is given by sending a generator of G to $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. It is easy to compute generating invariants using the methods of Chap. 3. We obtain

$$f_1 = x_1^2 + x_2^2, \quad f_2 = x_1^2 x_2^2, \quad \text{and} \quad f_3 = x_1 x_2 (x_1^2 - x_2^2)$$

as generating invariants, subject to the relation

$$f_3^2 = f_1^2 f_2 - 4f_2^2. \tag{5.3.1}$$

The invariant ring is not a polynomial ring, but dividing (5.3.1) by f_2^2 tells us that $\varphi_1 := f_1$ and $\varphi_2 := f_3/f_2$ form a minimal basis:

$$K(V)^G = K(f_1, f_2, f_3) = K(\varphi_1, \varphi_2).$$

We choose $\mathcal{Y} = \{\pm x_1, \pm x_2\}$ and obtain

$$f(X) = \prod_{y \in \mathcal{Y}} (X - y) = X^4 - f_1 X^2 + f_2 = X^4 - \varphi_1 X^2 + \frac{\varphi_1^2}{\varphi_2^2 + 4}.$$

This yields the generic polynomial $g(t_1, t_2; X) = X^4 - t_1 X^2 + t_1^2/(t_2^2 + 4)$. Alternatively, taking $\mathcal{Y} = \{\pm \varphi_1/x_1, \pm \varphi_1/x_2\}$ and replacing φ_1 and φ_2 by $-\varphi_1/2$

and $2\varphi_2$, respectively, yields the nicer generic polynomial

$$g(t_1, t_2; X) = X^4 + 2t_1(t_2^2 + 1)X^2 + t_1^2(t_2^2 + 1).$$

This is much simpler than the “classical” generic polynomial given by Seidelmann [23]. \triangleleft

Similarly, one gets nice generic polynomials over $K = \mathbb{Q}$ for groups like C_3 , the Klein 4-group, the dihedral group D_4 of order 8, and many more, in particular for groups which become reflection groups after adding some scalar matrices (see Kemper and Mattig [22]). The approach given by Theorem 5.3.2 turns out to be particularly successful in positive characteristic. For example, the fact that the invariant ring $\mathbb{F}_q[V]^{\mathrm{GL}(V)}$ is generated by the Dickson invariants (see Wilkerson [13]) leads to the generic polynomial

$$g(t_1, \dots, t_m; X) = X^{q^m-1} + t_1 X^{q^{m-1}-1} + \dots + t_{m-1} X^{q-1} + t_m.$$

for $G = \mathrm{GL}_m(\mathbb{F}_q)$ over $K = \mathbb{F}_q$.

Example 5.3.4 (Artin-Schreier polynomials) Let $G = C_p$ be the cyclic group of prime order p and $K = \mathbb{F}_p$. A faithful representation of G over K is given by sending a generator of G to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. The invariant ring is a polynomial ring generated by

$$f_1 = x_1 \quad \text{and} \quad f_2 = x_2^p - x_1^{p-1}x_2,$$

which follows by Theorem 3.9.4. Hence f_1 and f_2 also form a minimal basis of $K(V)^G$. A more convenient minimal basis is given by $\varphi_1 = x_1$ and $\varphi_2 = f_2/x_1^p$. We choose $\mathcal{Y} = \{(ax_1 + x_2)/x_1 \mid a \in \mathbb{F}_p\}$. Then

$$\begin{aligned} f(X) &= \prod_{a \in \mathbb{F}_p} \left(X - \frac{x_2}{x_1} - a \right) = \left(X - \frac{x_2}{x_1} \right)^p - \left(X - \frac{x_2}{x_1} \right) = \\ &= X^p - X - \frac{x_2^p - x_1^{p-1}x_2}{x_1^p} = X^p - X - \varphi_2. \end{aligned}$$

Thus we get $g(t, X) = X^p - X - t$ as a generic polynomial for C_p over \mathbb{F}_p . This is the well-known Artin-Schreier polynomial (see Lang [24, Chap. VIII, Theorem 6.4]). \triangleleft

Many more examples of generic polynomials in positive characteristic (for example for classical groups) can be obtained from the fact that for every finite, irreducible reflection group the invariant field is purely transcendental (Kemper and Malle [25]).

5.4 Systems of Algebraic Equations with Symmetries

We already mentioned in Sect. 1.2 that Gröbner bases can be used to solve systems of algebraic equations. In practice, such systems very often have symmetries, i.e., the solution set or the given equations are invariant under the action of a linear group (which may be finite or infinite). The disadvantage of Gröbner bases is that they destroy the symmetries of the system, instead of using them. For example, a lexicographic Gröbner basis of the ideal $(x + y - 1, xy)$ (invariant under $x \leftrightarrow y$) is $\{x+y-1, y^2-y\}$. In this section we will explain how invariants (in combination with Gröbner bases) can be used to rectify this shortcoming of Gröbner bases. The goal of these techniques is to facilitate (or make possible at all) practical computations. The ideas of this exposition are drawn from Sturmfels [1, Section 2.6].

Let $G \leq \mathrm{GL}(V)$ be a finite group acting on a finite dimensional vector space V over an algebraically closed field K . From the finiteness of G it follows that the categorical quotient $\pi_G: V \rightarrow V//G$ is in fact a geometric quotient (see Sect. 2.3). This implies that

$$\pi_G^{-1}(\pi_G(X)) = G \cdot X \quad (5.4.1)$$

for any affine variety $X \subseteq V$. We are interested in the situation in which X is G -stable, so we have $X = \pi_G^{-1}(\pi_G(X))$. The idea of using π_G is that it shrinks a G -orbit of points in V into a single point in $V//G$. For this reason the image $\pi_G(X)$ is also called the **orbit variety** of X . Suppose X is given by an ideal $I = (f_1, \dots, f_m)$. How can we use (5.4.1) for the computation of X ? We first have to calculate the orbit variety $\pi_G(X)$, which is equal to $\pi_G(G \cdot X)$ and hence closed by Corollary 2.3.4. Therefore we can use the method of Sect. 1.2.1 to compute $\pi_G(X)$. Let $g_1, \dots, g_r \in K[V]^G$ be generators for $K[V]^G$ as a K -algebra. Then π_G is given by $\pi_G(v) = (g_1(v), \dots, g_r(v))$. Thus we obtain the following algorithm.

Algorithm 5.4.1 (Orbit variety) Given polynomials $f_1, \dots, f_m \in K[V] = K[x_1, \dots, x_n]$ defining a variety $X \subseteq V$ and generating invariants g_1, \dots, g_r for the invariant ring $K[V]^G$ of a finite group $G \leq \mathrm{GL}(V)$, perform the following steps to compute an ideal $J \subseteq K[y_1, \dots, y_r]$ such that $\mathcal{V}(J) = \pi_G(X)$.

(1) Form the ideal

$$\bar{J} := (f_1, \dots, f_m, g_1 - y_1, \dots, g_r - y_r) \subseteq K[x_1, \dots, x_n, y_1, \dots, y_r].$$

(2) Use Algorithm 1.2.1 to compute J as the elimination ideal

$$J := \bar{J} \cap K[y_1, \dots, y_r].$$

If $J = (h_1, \dots, h_k)$ is the result of Algorithm 5.4.1, then

$$G \cdot X = \pi_G^{-1}(\pi_G(X)) = \mathcal{V}_V(h_1(g_1, \dots, g_r), \dots, h_k(g_1, \dots, g_r)).$$

Therefore we have a way to compute the G -orbit of a variety. If I is a zero-dimensional G -invariant ideal, we are interested in explicitly calculating the points of $X = \pi_G^{-1}(\pi_G(X))$. Thus for $(\eta_1, \dots, \eta_r) \in \pi_G(X)$ we want to compute the preimage

$$\pi_G^{-1}(\eta_1, \dots, \eta_r) = \{v \in V \mid g_i(v) = \eta_i \forall i\}.$$

This can be done by calculating a lexicographic Gröbner basis of the ideal

$$(g_1 - \eta_1, \dots, g_r - \eta_r) \subseteq K[x_1, \dots, x_n].$$

Thus we have split the process of finding X into two parts, both of which involve Gröbner basis calculations: the finding of $\pi_G(X)$ by Algorithm 5.4.1 and the computation of $\pi_G^{-1}(\eta_1, \dots, \eta_r)$ for a point $(\eta_1, \dots, \eta_r) \in \pi_G(X)$. Apart from this, we need generators for the invariant ring, which only have to be calculated once for the group G . In many practical examples this divide and conquer approach leads to much better running times, or makes computations possible which would otherwise be out of reach (see Worfolk [26]).

5.5 Graph Theory

Let K be a field and g a graph with vertices $\{1, \dots, n\}$ and edges which are weighted by values of K . We say that g is a **K -weighted graph** with n vertices. Thus g is given by the function m_g associating to each subset $\{i, j\} \subseteq \{1, \dots, n\}$ of size two the weight of the edge between the vertices i and j . The set of all K -weighted graphs with n vertices may be identified with the vector space $V = K^{\binom{n}{2}}$. If g' is another K -weighted graph with n vertices, we say that g and g' are isomorphic if there exists a permutation $\sigma \in S_n$ such that $m_g(\{\sigma(i), \sigma(j)\}) = m_{g'}(\{i, j\})$ for all $i \neq j$. This means that m_g and $m_{g'}$ lie in the same orbit under the action of $G = S_n$ on the two-sets $\{i, j\}$. Assume for the moment that K is algebraically closed. Then the G -orbits in V are in bijective correspondence to points in the categorical quotient $V//G$, since G is finite (see Sect. 2.3). Thus we have a bijection

$$\{\text{isomorphism classes of } K\text{-weighted graphs with } n \text{ vertices}\} \leftrightarrow V//G,$$

which endows the set of isomorphism classes of graphs with the structure of an algebraic variety. If we drop the assumption that K be algebraically closed, then

we still have an injective map from the set of isomorphism classes of K -weighted graphs with n vertices into $V//G$.

Let us put this injection into more explicit terms. Consider the polynomial ring $R := K[x_{\{i,j\}} \mid 1 \leq i, j \leq n, i \neq j]$ in $\binom{n}{2}$ variables. For a polynomial $f \in R$ and a K -weighted graph g with n vertices, define $f(g)$ by sending $x_{\{i,j\}}$ to $m_g(\{i,j\})$. The symmetric group $G = S_n$ acts on R by $\sigma \cdot x_{\{i,j\}} = x_{\{\sigma(i),\sigma(j)\}}$. Suppose we have invariants $f_1, \dots, f_m \in R^{S_n}$ which generate the invariant ring or a separating subalgebra. Then we have the following simple test whether two graphs are isomorphic.

Lemma 5.5.1 *With the above notation, two K -weighted graphs g and g' with n vertices are isomorphic if and only if*

$$f_i(g) = f_i(g') \quad \text{for } i = 1, \dots, m. \quad (5.5.1)$$

This approach requires the pre-computation of R^{S_n} for given values of n . The action of S_n on the indeterminates of R is the permutation action on subsets of size two of $\{1, \dots, n\}$. Unfortunately, the computation of these invariant rings turns out to be harder than one might expect. The computation is easy for $n \leq 3$, and was done for $n = 4$ by Aslaksen et al. [27] (see Example 3.7.4(b)). In [27] the authors also considered the corresponding permutation representation of S_5 , which is 10-dimensional. This representation has long been resistant against all existing algorithms for the computation of generating invariants. Using his library PerMuVAR [28] and Thiéry [29] studied the case $n = 5$. He was able to find (optimal) primary invariants of degrees 1, 2, 2, 3, 3, 4, 4, 5, 5, 6, and to check that the invariants of degree up to 17 are generated by invariants of degree at most 9. He used algorithms which are based on the concept of SAGBI-Gröbner bases (see Thiéry [30]). It was later confirmed by the second author of this book that the invariants for $n = 5$ are indeed generated in degrees at most 9. The computations for this confirmation are very demanding and were done in MAGMA. Thiéry conducted some experiments for $n = 6$ and thinks that the degree bound should be 11.

Let us remark that graphs with discretely weighted edges inject into the space V of K -weighted graphs, provided that K is large enough to permit an (arbitrary) injection of the weights into K . Thus Lemma 5.5.1 can also be used to test discretely weighted graphs for isomorphism. Moreover, if the vertices are also weighted, this translates into an action of S_n on $K^{\binom{n}{2}+n}$, so in this situation invariants can be used as well. This is also possible for directed graphs. In that case we will get an action of S_n by permutations combined with changes of signs.

Ulam's Conjecture.

We return to applications of invariant theory in graph theory itself. Let g be a **multigraph**, i.e., an undirected graph with vertices $\{1, \dots, n\}$ and (possibly) multiple edges. We might say that g is an \mathbb{N}_0 -weighted graph, and therefore the set of these graphs is a subset of the \mathbb{Q} -weighted graphs. So again Lemma 5.5.1 applies and gives a test whether two multigraphs are isomorphic.

A multigraph is called **simple** if there is at most one edge between two vertices. An interesting conjecture about simple graphs was formulated by Ulam [31]. Let \mathcal{G}_n be the set of isomorphism classes of simple graphs with n vertices. For a simple graph g with vertices $\{1, \dots, n\}$, consider the function $S_g: \mathcal{G}_{n-1} \rightarrow \mathbb{N}_0$ which assigns to each isomorphism class C of graphs with $n-1$ vertices the number of indices $i \in \{1, \dots, n\}$ such that the graph obtained by deleting the vertex i from g lies in the class C . Clearly if g and g' are isomorphic, then $S_g = S_{g'}$. With this notation Ulam's conjecture reads as follows.

Conjecture 5.5.2 *Let g and g' be two simple graphs with vertices $\{1, \dots, n\}$ with $n \geq 3$. Then $S_g = S_{g'}$ implies that g and g' are isomorphic.*

A stronger version of this conjecture can be translated into algebraic terms and leads to the following conjecture about the invariant rings R^{S_n} .

Conjecture 5.5.3 (Pouzet [32]) *Let R^{S_n} be the invariant ring of the symmetric group acting on $R = \mathbb{Q}[x_{\{i,j\}} \mid 1 \leq i < j \leq n]$ by $\sigma \cdot x_{\{i,j\}} = x_{\{\sigma(i),\sigma(j)\}}$. Then for $n \geq 3$, R^{S_n} is generated as a \mathbb{Q} -algebra by sums over S_n -orbits of monomials in the $x_{\{i,j\}}$ with $1 \leq i < j < n$ (i.e., by orbit-sums over monomials not involving the indeterminates $x_{\{i,n\}}$).*

This conjecture would imply Conjecture 5.5.2, even without the hypothesis that the graphs be simple. Unfortunately, however, Conjecture 5.5.3 was recently disproved by Thiéry [29], who used Hilbert series and counting arguments to show that the conjecture is false for $11 \leq n \leq 18$ (and probably for larger values of n as well). See also Thiéry [33] for some experimental results, and Pouzet and Thiéry [34] for more background and some related questions.

5.6 Combinatorics

Invariant theory has also been applied to combinatorics. Quite a few interesting examples can be found in Stanley's survey article [35] or in Stanley [36]. In some of these, combinatorial quantities are in some way encoded into a power series, which is then recognized as the Hilbert series of some invariant ring (e.g. by comparing with Molien's formula). Any knowledge about the invariant rings in question then leads to results about combinatorics.

Example 5.6.1 (Stanley [35]) Suppose we want to evaluate the sum

$$S(k) := \sum_{j=1}^k |1 - \zeta^j|^{-2},$$

where $\zeta = e^{\frac{2\pi i}{k}} \in \mathbb{C}$. In order to write $S(k)$ as a limit, define

$$F_k(t) := \sum_{j=0}^k \frac{1}{(1 - \zeta^j t)(1 - \zeta^{-j} t)}. \quad (5.6.1)$$

Then

$$S(k) = \lim_{t \rightarrow 1} \left(F_k(t) - \frac{1}{(1-t)^2} \right). \quad (5.6.2)$$

By comparing Eq. (5.6.1) with Molien's formula (Theorem 3.4.2), we see that $\frac{1}{k} F_k(t)$ is the Hilbert series of the invariant ring $\mathbb{C}[x, y]^G$ of the cyclic group

$$G = \langle \begin{pmatrix} \zeta & 0 \\ 0 & \zeta^{-1} \end{pmatrix} \rangle.$$

But the invariants of G are easily determined: They are \mathbb{C} -linear combinations of invariant monomials, and a monomial $x^i y^j$ is invariant if and only if $i \equiv j \pmod{k}$. Thus $\mathbb{C}[x, y]^G$ is generated by x^k, y^k , and xy with the sole relation $(xy)^k = x^k y^k$. This yields

$$H(\mathbb{C}[x, y]^G, t) = \frac{1 - t^{2k}}{(1 - t^2)(1 - t^k)^2}.$$

Equating this to $\frac{1}{k} F_k(t)$ and using Eq. (5.6.2), we obtain

$$S(k) = \lim_{t \rightarrow 1} \left(k \frac{1 - t^{2k}}{(1 - t^2)(1 - t^k)^2} - \frac{1}{(1-t)^2} \right) = \frac{k^2 - 1}{12},$$

where the last step is performed by l'Hôpital's rule, or by forming the limit with MAPLE (Char et al. [37]). \triangleleft

Example 5.6.2 This example is due to Solomon [38], and our account here is largely drawn from Stanley [35]. Given nonnegative integers $d_1, \dots, d_r \in \mathbb{N}_0$, we are interested in the number $P_n(\mathbf{d})$ of ways to write $\mathbf{d} := (d_1, \dots, d_r)$ as a sum of n vectors from \mathbb{N}_0^r , where the order of the summation is disregarded. One says that $P_n(\mathbf{d})$ is the number of **multipartite partitions** of \mathbf{d} . Introduce the polynomial ring $R := K[x_{i,j} \mid 1 \leq i \leq r, 1 \leq j \leq n]$ in $r \cdot n$ variables over a field K of characteristic 0. We give R an \mathbb{N}_0^r -grading by defining the homogeneous component $R_{\mathbf{d}}$ of multi-degree $\mathbf{d} = (d_1, \dots, d_r)$ as the K -span of the monomials $\prod_{i=1}^r \prod_{j=1}^n x_{i,j}^{e_{ij}}$ with $\sum_{j=1}^n e_{ij} = d_i$ for all i . Obviously the number of monomials of degree \mathbf{d} is equal to the number of ways how \mathbf{d} can be written as a sum of n vectors in \mathbb{N}_0^r , but now the order of the summation matters. More precisely, two summations having the same summands but in a different order correspond to two monomials lying

in the same orbit under the action of the symmetric group S_n by $\sigma \cdot x_{i,j} := x_{i,\sigma(j)}$. Therefore $P_n(\mathbf{d})$ is equal to the number of S_n -orbits of monomials of multi-degree \mathbf{d} . But this is the same as the dimension of $R_{\mathbf{d}}^{S_n}$, the homogeneous part of the invariant ring of multi-degree \mathbf{d} . Thus $P_n(\mathbf{d}) = \dim_K(R_{\mathbf{d}}^{S_n})$, and assembling this into a formal power series yields

$$\sum_{\mathbf{d} \in \mathbb{N}_0^r} P_n(\mathbf{d}) \cdot t_1^{d_1} \cdots t_r^{d_r} = \sum_{\mathbf{d} \in \mathbb{N}_0^r} \dim_K(R_{\mathbf{d}}^{S_n}) \cdot t_1^{d_1} \cdots t_r^{d_r} =: H(R^{S_n}; t_1, \dots, t_r), \quad (5.6.3)$$

where the right-hand side is the multi-graded Hilbert series of R^{S_n} . Thus our interest lies with R^{S_n} , the ring of vector invariants of the symmetric group. Quite a bit is known about this invariant ring. In particular, it is a result of Hermann Weyl that R^{S_n} is generated by the polarized elementary symmetric polynomials (see Smith [39, Theorem 3.4.1]). However, this is not enough information to derive a nice expression for the Hilbert series $H(R^{S_n}; t_1, \dots, t_r)$. Something can nevertheless be said about its structure. In fact, the elementary symmetric polynomials $s_{i,j}$ ($1 \leq i \leq r$, $1 \leq j \leq n$), as defined in Eq. (3.10.2), form a system of primary invariants (see Theorem 3.10.1). Moreover, $s_{i,j}$ is multi-homogeneous of degree $(0, \dots, 0, j, 0, \dots, 0)$, where the j appears in the i -th position. Therefore the subalgebra $A := K[s_{i,j} \mid 1 \leq i \leq r, 1 \leq j \leq n]$ has the multi-graded Hilbert series $\prod_{i=1}^r \prod_{j=1}^n (1 - t_i^j)^{-1}$. Since R^{S_n} is Cohen-Macaulay (Theorem 3.6.1), it is a free module over A . By the homogeneous Nakayama Lemma (Lemma 3.7.1), free generators can be chosen as a subset of any set of homogeneous generators. But there exist multi-homogeneous generators for R^{S_n} , and therefore

$$H(R^{S_n}; t_1, \dots, t_r) = \frac{\mathbf{t}^{\mathbf{e}_1} + \cdots + \mathbf{t}^{\mathbf{e}_m}}{\prod_{i=1}^r \prod_{j=1}^n (1 - t_i^j)},$$

where the \mathbf{e}_i are the multi-degrees of multi-homogeneous free generators. Putting this together with Eq. (5.6.3), we see that

$$\sum_{d_1, \dots, d_r \in \mathbb{N}_0} P_n(\mathbf{d}) \cdot t_1^{d_1} \cdots t_r^{d_r} = \frac{f(t_1, \dots, t_r)}{\prod_{i=1}^r \prod_{j=1}^n (1 - t_i^j)},$$

where f is a polynomial in t_1, \dots, t_r with nonnegative integers as coefficients. \triangleleft

A more recent connection between combinatorics and invariant theory was discovered by Elashvili and Jibladze [40]. The authors consider the invariants of the cyclic group $G = C_n$ acting by the regular representation. Let $a(n, m)$ be the dimension of the subspace of invariants in $K[V_{\text{reg}}]^G$ of degree m , so

$$H(K[V_{\text{reg}}]^G, t) = \sum_{m=0}^{\infty} a(n, m) t^m.$$

Since G acts by permutations of the monomials, the Hilbert series $H(K[V_{\text{reg}}]^G, t)$ is independent of the choice of the field K . Thus K can be chosen as \mathbb{C} . Then the regular representation is isomorphic to the diagonal representation where a generator of G acts by $\text{diag}(\zeta^0, \dots, \zeta^{n-1})$ with $\zeta = e^{\frac{2\pi i}{n}}$. In this representation, the invariants are precisely the \mathbb{C} -linear combination of invariant monomials, and a monomial $x_1^{e_1} \cdots x_n^{e_n}$ is invariant if and only if $\sum_{i=0}^{n-1} ie_i \equiv 0 \pmod{n}$. Thus $a(n, m)$ counts the number of solutions of

$$\sum_{i=0}^{n-1} ie_i \equiv 0 \pmod{n}, \quad \sum_{i=0}^{n-1} e_i = m. \quad (5.6.4)$$

But this is the same as the number of partitions of multiples of n into m summands which do not exceed $n - 1$, thereby providing a combinatorial interpretation of the numbers $a(n, m)$. In Elashvili et al. [41], another combinatorial interpretation in terms of so-called “necklaces” was given to the $a(n, m)$. On the other hand, $H(K[V_{\text{reg}}]^G, t)$ can be evaluated by Molien’s formula. The result is

$$H(K[V_{\text{reg}}]^G, t) = \frac{1}{n} \sum_{d|n} \varphi(d) (1 - t^d)^{-\frac{n}{d}},$$

where $\varphi(d)$ is the Euler totient function (see [40]). From this, the authors of [40] proceeded to derive a more explicit formula for $a(n, m)$, from which the interesting reciprocity law

$$a(n, m) = a(m, n)$$

can be read off.

5.7 Coding Theory

An interesting application of invariant theory to coding theory can be found in the very nice survey article by Sloane [42]. Let $C \subseteq \mathbb{F}_q^n$ be a code of length n defined over the finite field \mathbb{F}_q . If a_i is the number of codewords in C of weight i (i.e., codewords having exactly i nonzero coordinates), then the **weight enumerator** of C is defined as

$$W_C(x, y) := \sum_{i=0}^n a_i x^{n-i} y^i \in \mathbb{C}[x, y].$$

Suppose C is linear (i.e., a linear subspace of \mathbb{F}_q^n), and C^\perp is the dual code, which by definition consists of all vectors in \mathbb{F}_q^n whose standard scalar product with all codewords from C is zero. Then a celebrated theorem of MacWilliams [43] says

that

$$q^k W_{C^\perp}(x, y) = W_C(x + (q - 1)y, x - y), \quad (5.7.1)$$

where k is the dimension of C . An area of great interest in coding theory is the study of self-dual codes, i.e., linear codes C with $C^\perp = C$. This condition implies that $k = \dim(C) = n/2$. Since $W_C(x, y)$ is homogeneous of degree n , we obtain

$$W_C(\sqrt{q} \cdot x, \sqrt{q} \cdot y) = q^k W_C(x, y) = q^k W_{C^\perp}(x, y).$$

Thus for a self-dual code C , Eq. (5.7.1) becomes

$$W_C\left(\frac{x + (q - 1)y}{\sqrt{q}}, \frac{x - y}{\sqrt{q}}\right) = W_C(x, y).$$

This can be expressed by saying that W_C is invariant under the group G generated by the linear transformation

$$\sigma = \frac{1}{\sqrt{q}} \begin{pmatrix} 1 & 1 \\ q - 1 & -1 \end{pmatrix}$$

occurring above. The invariant ring of G is a polynomial ring generated by $f = x + (\sqrt{q} - 1)y$ and $g = y(x - y)$. Therefore $W_C(x, y)$ must be a polynomial in f and g . But since the degree n of W_C is even, it must in fact be a polynomial in f^2 and g , or, somewhat simpler, in $f^2 + 2(1 - \sqrt{q})g = x^2 + (q - 1)y^2$ and $g = y(x - y)$. Thus invariant theory gives strong restrictions on possible weight enumerators of self-dual codes.

Assume that we have the additional restriction that the code is binary ($q = 2$), and all occurring weights are divisible by 4. This means that $W_C(x, y)$ is also invariant under the transformation given by $\tau = \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}$. Let \hat{G} be the group generated by the above transformation σ (for $q = 2$) and by τ . It is found that \hat{G} is a complex reflection group of order 192 (G_9 in the classification of Shephard and Todd [44]). The invariant ring $\mathbb{C}[x, y]^{\hat{G}}$ is a polynomial ring generated by the invariants

$$\begin{aligned} \theta &= x^8 + 14x^4y^4 + y^8, \\ \varphi &= x^4y^4(x^4 - y^4)^4 \end{aligned}$$

of degrees 8 and 24. (The generators can either be taken from Sloane [42] or computed with MAGMA, which takes about half a second.) Thus every weight enumerator of a self-dual binary code whose weights are all divisible by 4 must be a polynomial in θ and φ . This result goes back to Gleason [45]. Moreover, the coefficients of W_C must be nonnegative integers, and the coefficient of x^n must be 1. All this imposes strong restrictions on the possible weight enumerators. These restrictions can be used to determine the weight enumerator of specific codes using

only very little further knowledge (see Sloane [42, Section I.F]), or to rule out the existence of certain codes. For example, it can be proved that the minimum distance of a self-dual binary code of length n with all weights divisible by 4 cannot exceed $4[n/24] + 4$, and only a finite number of codes exist where this upper bound is attained (see Sloane [42, Section IV.B]).

A huge number of other, more recent examples where invariant theory is used for coding theory can be found in Rains and Sloane [46] and Bannai et al. [47]. The applications are all in the same spirit as the one explained above, but the invariant rings that emerge are considerably more complicated. A novel and systematic treatment of the whole area can be found in the book by Nebe et al. [48].

5.8 Equivariant Dynamical Systems

In the theory of dynamical systems one studies differential equations of the type

$$\frac{d}{dt}\mathbf{x} = \mathbf{f}(\mathbf{x}), \quad (5.8.1)$$

where $\mathbf{f}: \mathbb{R}^n \rightarrow \mathbb{R}^n$ is a function (“vector field”), and solutions \mathbf{x} are functions $\mathbb{R} \rightarrow \mathbb{R}^n$ of t . Often the vector field \mathbf{f} also depends on a tuple $\lambda \in \mathbb{R}^l$, so we have the equation $\frac{d}{dt}\mathbf{x} = \mathbf{f}(\mathbf{x}, \lambda)$. It is quite common that a dynamical system has symmetries, such as rotational symmetries when the flow of some liquid through a (motionless) cylinder is considered. Such symmetries translate into the condition that the vector field \mathbf{f} is equivariant under the action of some group $G \leq \mathrm{GL}_n(\mathbb{R})$, i.e.,

$$\mathbf{f} \circ \sigma = \sigma \circ \mathbf{f} \quad \text{for all } \sigma \in G.$$

In this context G may or may not be finite. In bifurcation theory one studies the question of how the behavior of the system changes under small perturbations of the parameter λ . If \mathbf{f} is equivariant with respect to some group, we speak of equivariant bifurcation theory. Of particular interest is the study of stationary states, i.e., solutions with constant \mathbf{x} , which are given by

$$\mathbf{f}(\mathbf{x}, \lambda) = 0. \quad (5.8.2)$$

Again the solutions \mathbf{x} depend on λ , and (equivariant) bifurcation theory studies those values of λ where branches of solutions meet. For a detailed introduction into equivariant bifurcation theory we refer the reader to the books by Sattinger [49], Golubitsky and Schaeffer [50], and Golubitsky et al. [51]. Information on equivariant dynamical systems and many more references can be found in Gatermann [52], Gatermann and Guyard [53], and Gaeta et al. [54].

If \mathbf{f} is G -equivariant (for every λ), then the solution set of Eq. (5.8.2) is G -stable, hence the methods of Sect. 5.4 apply if \mathbf{f} consists of (or can be approximated by) polynomials and G is finite. On the other hand, if \mathbf{f} is G -equivariant and $G \subseteq \mathrm{O}_n(\mathbb{R})$ is infinite, suppose that $\pi_1, \dots, \pi_k: \mathbb{R}^n \rightarrow \mathbb{R}^n$ are equivariants generating the module of equivariants over the invariant ring. Then the scalar products $\pi_i \cdot \mathbf{f}$ are G -invariant functions $\mathbb{R}^n \rightarrow \mathbb{R}$. It is easy to see that

$$\mathcal{V}_{\mathbb{R}^n}(\mathbf{f}) = \mathcal{V}_{\mathbb{R}^n}(\pi_1 \cdot \mathbf{f}, \dots, \pi_k \cdot \mathbf{f})$$

(Jarić et al. [55]). Hence in this situation the methods of Sect. 5.4 can also be used to try to facilitate the solution of Eq. (5.8.2). This approach was carried out successfully by Worfolk [26], for example.

A closely related technique used in the study of equivariant dynamical systems is called orbit space reduction, and is based on the following observation. Let $g_1, \dots, g_r \in K[x_1, \dots, x_n]^G$ be generators for the invariant ring. We view the g_i as functions $\mathbb{R}^n \rightarrow \mathbb{R}$. For $\sigma \in G$ we have

$$\mathrm{grad} \, g_i = \mathrm{grad}(g_i \circ \sigma) = (\mathrm{grad} \, g_i \circ \sigma) \cdot \sigma$$

by the invariance and by the chain rule. Since \mathbf{f} is G -equivariant, it follows that the product $(\mathrm{grad} \, g_i) \cdot \mathbf{f}$ (with the gradient written as a row and \mathbf{f} as a column) is G -invariant as a function $\mathbb{R}^n \rightarrow \mathbb{R}$. Let us assume for simplicity that \mathbf{f} consists of polynomials. Then $(\mathrm{grad} \, g_i) \cdot \mathbf{f} = h_i(g_1, \dots, g_r)$ with $h_i \in \mathbb{R}[y_1, \dots, y_r]$ a polynomial in new variables y_j . Now if $\mathbf{x}: \mathbb{R} \rightarrow \mathbb{R}^n$ is a solution of Eq. (5.8.1), then by the chain rule

$$\frac{d}{dt}(g_i \circ \mathbf{x}) = (\mathrm{grad} \, g_i \circ \mathbf{x}) \cdot \frac{d}{dt}\mathbf{x} = (\mathrm{grad} \, g_i \circ \mathbf{x}) \cdot \mathbf{f}(\mathbf{x}) = h_i(g_1 \circ \mathbf{x}, \dots, g_r \circ \mathbf{x}).$$

Summarizing the $g_i \circ \mathbf{x}$ into a function $\mathbf{g}: \mathbb{R} \rightarrow \mathbb{R}^r$ and the h_i into a vector field $\mathbf{h}: \mathbb{R}^r \rightarrow \mathbb{R}^r$, we can write this as

$$\frac{d}{dt}\mathbf{g} = \mathbf{h}(\mathbf{g}). \quad (5.8.3)$$

The process of obtaining (5.8.3) from (5.8.1) is called orbit space reduction since this method contracts orbits into points. For example, a periodic solution which moves along a G -orbit is contracted into a stationary solution. For any solution \mathbf{x} of (5.8.1), the corresponding \mathbf{g} satisfies (5.8.3), and it also satisfies the algebraic relations between the g_i (see Sect. 3.8). Thus we have a differential equation with algebraic side conditions, or, equivalently, a differential equation on the quotient variety $\mathbb{R}^n // G$. The relation between solutions of (5.8.3) and (5.8.1) is quite intricate, since a point $\mathbf{g}(t)$ has many preimages $\mathbf{x}(t)$ in \mathbb{R}^n , and it is not clear how they can be put together for different t to obtain a solution of (5.8.1). But the advantage of (5.8.3) is that its investigation is much easier.

Example 5.8.1 Consider the dynamical system given by

$$\frac{d}{dt} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} y \\ -x \end{pmatrix} + (1 - \lambda(x^2 + y^2)) \begin{pmatrix} x \\ y \end{pmatrix}.$$

The vector field is equivariant under $G = \text{SO}_2(\mathbb{R})$. It is easily seen that the invariant ring $\mathbb{R}[x, y]^G$ is generated by the single invariant $g = x^2 + y^2$. We perform orbit space reduction and obtain

$$\begin{aligned} \frac{d}{dt} g &= 2x(y + (1 - \lambda(x^2 + y^2))x) + \\ &\quad 2y(-x + (1 - \lambda(x^2 + y^2))y) = 2g(1 - \lambda g). \end{aligned}$$

This equation is much more tractable than the original one, and has the general solution

$$g(t) = \frac{c}{\lambda c + (1 - \lambda c)e^{-2t}}$$

with $c = g(0) \in \mathbb{R}$ nonnegative. (For $\lambda < 0$ and $c > 0$, $g(t)$ is only defined for $0 \leq t < \ln(1 - 1/(\lambda c))/2$.) However, this solution does not capture the angular movement of (x, y) , for example the circular movement in the case of the stationary solution $g(t) = 1/\lambda$ (for $\lambda > 0$). \triangleleft

Orbit space reduction has been studied and used by many authors. We content ourselves in giving the references Gatermann and Lauterbach [56] and Lari-Lavassani et al. [57] here, where the symbolic computation of invariants is used. It is clear that the methods discussed here find applications in physics, chemistry, and engineering. Three examples are given by the references Jarić et al. [55], Campbell and Holmes [58], and Collins and Thompson [59].

5.9 Material Science

For fuel or water tanks in aircrafts and rockets one frequently uses textile reinforced composites to achieve high durability at a low weight. It is important to find failure conditions for such materials, i.e., functions in terms of the stresses (usually given by a symmetric tensor with components $\sigma_x, \sigma_y, \sigma_z, \tau_{yz}, \tau_{zx}, \tau_{yx}$) which describe under what stress the material will break. Since at present there is no valid theory to compute such failure conditions from the geometry and basic ingredients of the material, experiments are necessary for their determination. More precisely, one writes (approximate) failure conditions as polynomials (or other simple functions) in the stresses and then performs a few experiments to determine the coefficients of these polynomials. In this process it is important to incorporate any additional

information on the material into the initial polynomials. In particular, failure conditions are invariant under any orthogonal transformation of coordinates which respects the symmetries of the material. Therefore the failure conditions should be chosen as invariants under the symmetry group of the material. This drastically reduces the number of coefficients to be determined by experiments, and thus the number of experiments that are necessary. An invariant theoretic approach has been taken by materials researchers for quite a while (see, for example, Hashin [60] and Helisch [61]).

The symmetry group is given as a subgroup of $O_3(\mathbb{R})$. Since we are considering polynomials in the stresses, we have to determine the action of a matrix $A \in O_3(\mathbb{R})$ on the tensor of stresses. This is given by

$$A \cdot \begin{pmatrix} \sigma_x & \tau_{yx} & \tau_{zx} \\ \tau_{yx} & \sigma_y & \tau_{yz} \\ \tau_{zx} & \tau_{yz} & \sigma_z \end{pmatrix} = A^{-1} \begin{pmatrix} \sigma_x & \tau_{yx} & \tau_{zx} \\ \tau_{yx} & \sigma_y & \tau_{yz} \\ \tau_{zx} & \tau_{yz} & \sigma_z \end{pmatrix} A.$$

Observe that $-1 \in O_3(\mathbb{R})$ lies in the kernel of the action. Let us consider a few examples of material symmetries.

Example 5.9.1 Let us consider the case of a “unidirectional reinforced composite”, where the fibers all lie parallel to each other, say along the x -coordinate axis. The symmetry group is $O_2(\mathbb{R}) \times \{\pm 1\}$, with $O_2(\mathbb{R})$ acting on the y - z -plane and $\{\pm 1\}$ acting as a reflection at this plane. Hence

$$G = \left\{ \begin{pmatrix} z_1 & 0 & 0 \\ 0 & z_2 z_3 & -z_4 \\ 0 & z_2 z_4 & z_3 \end{pmatrix} \mid z_1^2 = z_2^2 = z_3^2 + z_4^2 = 1 \right\}. \quad (5.9.1)$$

An element $g \in G$ acts on the σ 's and τ 's by

$$g \cdot \begin{pmatrix} \sigma_x \\ \sigma_y \\ \sigma_z \\ \tau_{yx} \\ \tau_{zx} \\ \tau_{yz} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & z_3^2 & z_4^2 & 0 & 0 & 2z_3 z_4 \\ 0 & z_4^2 & z_3^2 & 0 & 0 & -2z_3 z_4 \\ 0 & 0 & 0 & z_1 z_2 z_3 & z_1 z_2 z_4 & 0 \\ 0 & 0 & 0 & -z_1 z_4 & z_1 z_3 & 0 \\ 0 & -z_2 z_3 z_4 & z_2 z_3 z_4 & 0 & 0 & z_2 - 2z_2 z_4^2 \end{pmatrix} \begin{pmatrix} \sigma_x \\ \sigma_y \\ \sigma_z \\ \tau_{yx} \\ \tau_{zx} \\ \tau_{yz} \end{pmatrix}. \quad (5.9.2)$$

G is an infinite, reductive group, so we can use the methods of Sect. 4.1 to compute generators of the invariant ring. The ideal $I(G)$ defining the group and the matrix A defining the action are given by Eqs. (5.9.1) and (5.9.2), respectively. We form the ideal in step (2) of Algorithm 4.1.9, compute the elimination ideal b as in step (3), and set the second set of variables equal to zero. The resulting ideal is

$$I = (\underbrace{\sigma_x}_{=:f_{11}}, \underbrace{\sigma_y + \sigma_z}_{=:f_{12}}, \underbrace{\tau_{yx}^2 + \tau_{zx}^2}_{=:f_{21}}, \underbrace{\sigma_z^2 + \tau_{yz}^2}_{=:f_{22}}, \underbrace{\sigma_z \tau_{zx}^2 + \tau_{yx} \tau_{zx} \tau_{yz}}_{=:f_3}), \quad (5.9.3)$$

which is equal to the ideal generated by all invariants of positive degree. It is easy to check that the generators f_{11} , f_{12} , and f_{21} are already invariants. We have to replace the generators f_{22} and f_3 by invariants. In Algorithm 4.1.9, this is done by applying the Reynolds operator. Here we choose a different approach. First we substitute the f_{22} by

$$\tilde{f}_{22} := f_{22} - \sigma_z f_{12} = \tau_{yz}^2 - \sigma_y \sigma_z,$$

which is seen to be an invariant. It remains to find an irreducible invariant of degree 3 in I . To this end, we write down a basis of the space of elements of I of degree 3, modulo the space generated by products of invariants of degree less than 3. This basis has 37 elements. We apply a general element of G , given by the matrix in (5.9.2), to a linear combination with unknown coefficients of these 37 polynomials. From this we subtract the original linear combination, and then form the normal form of the result with respect to $I(G) = (z_1^2 - 1, z_2^2 - 1, z_3^2 + z_4^2 - 1)$. A necessary and sufficient condition for the linear combination to be G -invariant is that this normal form is zero. Setting all coefficients of the normal form equal to zero yields a system of 148 linear equations in 37 unknowns. The solution space is one-dimensional, as expected, and we obtain the invariant

$$\tilde{f}_3 = 2f_3 - \tau_{zx}^2 f_{12} - \sigma_z f_{21} = 2\tau_{yx}\tau_{zx}\tau_{yz} - \sigma_y \tau_{zx}^2 + \sigma_z \tau_{yx}^2.$$

Thus we have found that the invariant ring is generated by f_{11} , f_{12} , f_{21} , \tilde{f}_{22} , and \tilde{f}_3 . This confirms a result of Hashin [60]. The computation in this example was done in MAGMA and took about 5 s. \triangleleft

In the following example we consider material structures which have a finite symmetry group.

Example 5.9.2

- (a) A very common case is a woven textile reinforcement with warp and weft inclined at 90° , but made of different materials. Then the symmetry group is generated by reflections at the coordinate planes. Since $-1 \in O_3(\mathbb{R})$ acts trivially, the symmetry group acts as a Klein 4-group. The invariant ring is a hypersurface generated by invariants of degree at most 3 (see Boehler [62]). It can easily be calculated with the methods from Chap. 3.
- (b) Almost as common is the case of a woven textile with identical fibers in warp and weft, inclined at 90° . Here the symmetry group is generated by a rotation by 90° about an axis orthogonal to the textile layer and reflections at the coordinate planes. The resulting group is a dihedral group of order 8. The invariant ring is a complete intersection generated by invariants of maximal degree 4 (see Smith et al. [63]).
- (c) A more exotic structure is a textile layer with a 45° -symmetry. Here the symmetry group is a dihedral group of order 16. The invariant ring was calculated by Meckbach and Kemper [64] using the methods of Chap. 3. It is a

Gorenstein ring but considerably more complicated than the ones in the previous examples. There are 10 generators of maximal degree 8.

△

5.10 Computer Vision

A very rich field of applications of invariant theory is computer vision. Philosophically, this comes from the fact that the camera image of an object (two or three dimensional) depends very much on the angle from which it is viewed, as well as many other factors. Therefore the immediate parameters that can be measured from the image are almost never inherent object characteristics. It is therefore an obvious approach to use invariant theory in order to extract inherent characteristics from the image parameters, i.e., characteristics that remain unchanged if the camera angle or other factors are changed. It is not surprising that there is a multitude of ways in which invariant theory is used in computer vision. We found a rich source of information in the book by Mundy and Zisserman [65], which has a nice introductory chapter written by the editors. The relevant literature on this field is vast, as can be seen from the references given in [65]. Let us also direct the reader to the references Reiss [66], Kanatani [67], and Florack [68]. In keeping with the general style of this chapter, we will only give a very limited number of applications to computer vision in this section.

5.10.1 View Invariants of 3D Objects

A very important and difficult issue in computer vision is the recognition of three-dimensional objects or scenes from their two-dimensional images given by camera views. Quite a number of sophisticated techniques are applied to interpret 2D projections, such as reconstruction from multiple or stereo views, shape from motion, shape from shading, or shape from texture. Most of these techniques use image features as an input, which are produced by preprocessing the camera data with some standard tools, such as edge detectors or detectors of points with maximal brightness or highest curvature. Once an edge is detected in an image, it can be classified as being a straight line, a conic, etc., and for each such category of curves the defining parameters can be determined. No classification is necessary for points, where the defining parameters are just the two coordinates of the measured 2D projection of the point. This second step is also referred to as the extraction of geometric primitives, where points, straight lines, conics etc. are regarded as geometric primitives.

The problem is that the position and therefore also the defining parameters of the detected geometric primitives change when the same 3D object or scene is rotated

or viewed from a different angle or distance. This is where invariant theory comes in as a helpful tool. The idea is to form expressions from the feature parameters which remain invariant under changes of viewing angle or distance. The question how many such invariants exist and what discriminatory power they have cannot be answered in complete generality. One has to restrict to certain configurations of geometric primitives which either have been detected or are a priori known to be present in the image. Thus one can talk, for instance, of invariants of a configuration of two straight lines and two conics. This configuration would be detected when viewing a cylindrical object (with one conic partially occluded). Rothwell et al. [69] report on an experimental recognition system which uses such invariants. The system receives a 2D view of several objects, typically metallic plates and other workpieces, and compares these objects to models from a database.

Let us consider a simple example of single view invariants. Suppose that we have detected n points in a 3D scene, and suppose we know for some reason that these points are coplanar. What we have measured are the $2n$ coordinates of the projections of the points onto the camera plane, which is in general different from the plane containing the points. Changes in camera position and orientation are adequately represented by the action of the group $G = \mathbb{R}^3 \rtimes (\mathbb{R}^* \times \text{SO}_3(\mathbb{R}))$ generated by all translations, rotations, and scalars. If we exclude the possibility that the n points lie on a plane perpendicular to the camera plane, then it is easy to see that the 2D projection of the G -orbit of the original points coincides with the orbit of the projected points under the two-dimensional affine linear group $H = \text{AGL}_2(\mathbb{R}) = \mathbb{R}^2 \rtimes \text{GL}_2(\mathbb{R})$. If we also assume that no three points are collinear, then Theorem 4.4.4 provides the rational invariants

$$f_{i,j} = \frac{\det \begin{pmatrix} x_i & x_j \\ y_i & y_j \end{pmatrix}}{\det \begin{pmatrix} x_1 & x_2 \\ y_1 & y_2 \end{pmatrix}}, \quad (1 \leq i \leq 2, 3 \leq j \leq n-1),$$

where (x_i, y_i) is the vector connecting the camera images of the i -th and the n -th point. It would be interesting to obtain invariants which also ignore the action of the symmetric group S_n by permuting the n points. This is our next topic, but we will restrict ourselves to the 2D case, i.e., all points lie on the camera plane.

5.10.2 Invariants of n Points on a Plane

Suppose we have measured the $\binom{n}{2}$ mutual distances of a configuration of n points on a plane which coincides with the camera plane (one could also think of the angular distances of n stars). In order to recognize the object we have measured, we wish to compare the measured distances with the distances of configurations of points stored in a database (such as a database of constellations). But we do not know how

the order in which the measured points appear in our measurement corresponds to the order of points chosen for an item in the database. So what we wish to do is to determine if two n -point configurations in $(\mathbb{R}^2)^n$ lie in the same orbit under the group $G = S_n \times \text{AO}_2(\mathbb{R})$, where the Euclidean group $\text{AO}_2(\mathbb{R}) = \mathbb{R}^2 \rtimes \text{O}_2(\mathbb{R})$ generated by translations and orthogonal transformations acts diagonally. The mutual distances form invariants of $\text{AO}_2(\mathbb{R})$, and they separate orbits (since we are working over the reals). The difficulty arises from the action of S_n .

This brings us back to the situation discussed in Sect. 5.5. In fact, we are given an \mathbb{R} -weighted graph g with n vertices (the weights being the measured distances), and we want to find a graph in the database that is isomorphic to g . Thus Lemma 5.5.1 can be used to obtain a relatively easy recognition procedure for objects made of n points. Unfortunately the computational problems mentioned in Sect. 5.5 severely limit the scope of this approach. So taking graph invariants and evaluating them at mutual distances would be “right thing” for recognizing point configurations up the G -action. But since the “right thing” is impractical even for quite small values of n , maybe one should do the “easy thing” instead. An idea would be to use the distribution of the $\binom{n}{2}$ distances. This raises the question whether one can reconstruct a plane n -point configuration (up to the G -action) from the distribution of its $\binom{n}{2}$ distances. Unfortunately, the answer is no in general. Figure 5.1 shows a counterexample. We have put the distances next to the lines connecting pairs of points. Notice that the upper point in the first configuration is moved diagonally downward to obtain the second configuration, while the other three points remain inert.

From an invariant theoretic point of view, considering the distribution of distances amounts to taking the invariants of the symmetric group $S_{\binom{n}{2}}$ acting on the vector space $\mathbb{R}^{\binom{n}{2}}$ of weighted graphs with n vertices and evaluating them at the mutual distances. So we have taken invariants of the wrong group: $S_{\binom{n}{2}}$ instead of S_n . This makes it clear that we could not expect that the distribution of distances characterizes point configurations up to the action of G .

However, there are relations between the mutual distances. In fact, let (x_i, y_i) be the measured coordinates of the points $P_i \in \mathbb{R}^2$ and consider the squared distances $d_{i,j} = (x_i - x_j)^2 + (y_i - y_j)^2$. Relations between the $d_{i,j}$ come from the fact that the Gram matrix of any number of vectors in \mathbb{R}^2 has rank at most 2. Fix the point P_n , for example, and consider the connecting vectors $v_i := (x_i - x_n, y_i - y_n)$ for

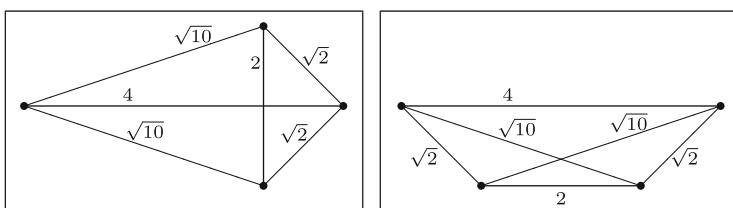


Fig. 5.1 Two 4-point configurations with the same distribution of distances

$1 \leq i \leq n - 1$. Then the (3×3) -minors of the Gram matrix $(\langle v_i, v_j \rangle)_{i,j=1,\dots,n-1}$ (with scalar products as entries) are zero. But $\langle v_i, v_j \rangle = (d_{i,n} + d_{j,n} - d_{i,j})/2$. For $n = 4$, for example, we get the relation

$$\det(d_{i,4} + d_{j,4} - d_{i,j})_{i,j=1,\dots,3} = 0.$$

Thus the $d_{i,j}$ lie on a subvariety $X \subseteq \mathbb{R}^{\binom{n}{2}}$, on which S_n acts. Now it can be shown that only those permutations from $S_{\binom{n}{2}}$ that come from elements of S_n map X into itself. But if the vector of squared distances of a point configuration lies in none of the $\sigma \cdot X$ for $\sigma \in S_{\binom{n}{2}} \setminus S_n$, then every other point configuration sharing the same distribution of distances is in fact in the same G -orbit. We obtain the following result:

Theorem 5.10.1 (Boutin and Kemper [70]) *There is a nonempty Zariski-open subset $U \subseteq (\mathbb{R}^2)^n$ such that every point configuration $(P_1, \dots, P_n) \in U$ is reconstructible from its distribution of distances, i.e., every point configuration (Q_1, \dots, Q_n) sharing the same distribution of distances as (P_1, \dots, P_n) lies in the same orbit as (P_1, \dots, P_n) under the group $G = S_n \times \text{AO}_2(\mathbb{R})$.*

In fact, the theorem generalizes from the plane \mathbb{R}^2 to any \mathbb{R}^m with $m \leq \max\{2, n - 2\}$ and from \mathbb{R} to any field of characteristic $\neq 2$.

5.10.3 Moment Invariants

Let us look at a third way of applying invariant theory to computer vision. Our presentation is motivated by the article of Taubin and Cooper [71]. Suppose we have a 2D gray scale image given by a function $f: \mathbb{R}^2 \rightarrow \mathbb{R}$ with compact support. One could think of an image obtained by scanning a post stamp, for example. The goal would then be to identify this post stamp (by comparing with a database representing the currently valid post stamps). An approach that does not require any edge detection or extraction of geometric primitives is provided by moments, i.e., integrals of the form

$$\langle f, g \rangle = \int_{\mathbb{R}^2} g(x, y) f(x, y) dx dy$$

where $g \in \mathbb{R}[x, y]$ is a polynomial. It suffices to do this for monomials. For nonnegative integers i and j , write

$$a_{i,j} = \int_{\mathbb{R}^2} x^i y^j f(x, y) dx dy.$$

The idea is to compute these $a_{i,j}$ for a limited range of i 's and j 's until enough data is collected to efficiently discriminate between different post stamps, for example.

Again, the problem is that the values $a_{i,j}$ change drastically when the image is rotated or shifted by a vector in \mathbb{R}^2 . It is easy to see that any affine linear map applied to the gray-scale image results in a linear transformation of the $a_{i,j}$. Thus the idea to form invariant polynomials from the $a_{i,j}$ is very natural. Such invariants are called **moment invariants**. As a first step we want to form invariants under translations by vectors from \mathbb{R}^2 . The idea is to shift the image in such a way that its center of mass is sent to the coordinate origin, and then to compute the moments. Explicitly, set $\bar{x} := a_{1,0}/a_{0,0}$ and $\bar{y} := a_{0,1}/a_{0,0}$. Then the **normalized moments** may be defined by

$$\bar{a}_{i,j} := a_{0,0}^{i+j-1} \cdot \int_{\mathbb{R}^2} (x - \bar{x})^i (y - \bar{y})^j f(x, y) dx dy.$$

It is clear that $\bar{a}_{i,j}$ is translation-invariant. It is also clear from the construction that the normalized moments generate a separating algebra (in the sense of Definition 2.4) for the action of the translation group. We have inserted the factor $a_{0,0}^{i+j-1}$ to make sure that $\bar{a}_{i,j}$ is a polynomial in the nonnormalized moments $a_{v,\mu}$. For example, we obtain

$$\begin{aligned}\bar{a}_{1,0} &= \bar{a}_{0,1} = 0, \\ \bar{a}_{2,0} &= a_{0,0}a_{2,0} - a_{1,0}^2, \\ \bar{a}_{1,1} &= a_{0,0}a_{1,1} - a_{1,0}a_{0,1}, \\ \bar{a}_{0,2} &= a_{0,0}a_{0,2} - a_{0,1}^2,\end{aligned}\tag{5.10.1}$$

and so on. After normalizing the moments we are left with linear actions. A matrix $\sigma = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ acts on the $\bar{a}_{i,j}$ in the same way as on the $a_{i,j}$. The action is closely related to the action on binary forms (see Example 2.1.2). For the $\bar{a}_{i,j}$ with $i + j = 2$ we obtain

$$\sigma : \begin{pmatrix} \bar{a}_{2,0} \\ \bar{a}_{1,1} \\ \bar{a}_{0,2} \end{pmatrix} \mapsto \det(\sigma)^2 \begin{pmatrix} \alpha^2 & 2\alpha\beta & \beta^2 \\ \alpha\gamma & \alpha\delta + \beta\gamma & \beta\delta \\ \gamma^2 & 2\gamma\delta & \delta^2 \end{pmatrix} \begin{pmatrix} \bar{a}_{2,0} \\ \bar{a}_{1,1} \\ \bar{a}_{0,2} \end{pmatrix}.$$

We can now use Algorithm 4.1.9 to compute generating invariants in $\mathbb{R}[\bar{a}_{2,0}, \bar{a}_{1,1}, \bar{a}_{0,2}]$ under the special orthogonal group $\mathrm{SO}_2(\mathbb{R})$ (regarding the $\bar{a}_{i,j}$ as indeterminates). We find two generators:

$$g_1 = \bar{a}_{2,0} + \bar{a}_{0,2} \quad \text{and} \quad g_2 = \bar{a}_{2,0}\bar{a}_{0,2} - \bar{a}_{1,1}^2.$$

Using (5.10.1) to express the g_i in terms of the nonnormalized moments yields

$$\begin{aligned}g_1 &= a_{0,0}(a_{2,0} + a_{0,2}) - a_{1,0}^2 - a_{0,1}^2, \\ g_2/a_{0,0} &= a_{0,0} (a_{2,0}a_{0,2} - a_{1,1}^2) + 2a_{1,1}a_{1,0}a_{0,1} - a_{1,0}^2a_{0,2} - a_{0,1}^2a_{2,0}.\end{aligned}$$

It may be surprising that g_2 turns out to be divisible by $a_{0,0}$. This shows that although the normalized moments are separating invariants for the translation action, they are not generating invariants. In addition to the above invariants, we have $a_{0,0}$ as an invariant under translations and rotations. It is clear that if we compute more moments $a_{i,j}$ we can also expect a larger number of moment invariants that can be formed from them.

Of course the group $(\mathbb{R}^2 \rtimes \mathrm{SO}_2(\mathbb{R}))$ that we used above is not the only group relevant for the identification of 2D images. Depending on the situation, other groups such as the group $\mathbb{R}^2 \rtimes (\mathbb{R}^* \times \mathrm{SO}_2(\mathbb{R}))$ generated by translations, rotations, and scalings may be appropriate. In that case, we will get fewer moment invariants.

References

1. Bernd Sturmfels, *Algorithms in Invariant Theory*, Springer-Verlag, Wien, New York 1993.
2. Alejandro Adem, R. James Milgram, *Cohomology of Finite Groups*, Springer-Verlag, Berlin, Heidelberg, New York 1994.
3. Leonard Evens, *The Cohomology of Groups*, Oxford University Press, Oxford 1991.
4. Alejandro Adem, R. James Milgram, *Invariants and cohomology of groups*, Bol. Soc. Mat. Mex. **37** (1992), 1–25.
5. Richard P. Stauduhar, *The determination of Galois groups*, Math. Comput. **27** (1973), 981–996.
6. Katharina Geißler, Jürgen Klünners, *Galois group computation for rational polynomials*, J. Symb. Comput. **30** (2000), 653–674.
7. Yves Eichenlaub, *Problèmes effectifs de la théorie de Galois en degrés 8 à 11*, Dissertation, Université Bordeaux 1, 1996.
8. Katharina Geißler, *Zur Berechnung von Galoisgruppen*, Diplomarbeit, Technische Universität Berlin, 1997.
9. Kurt Girstmair, *On the computation of resolvents and Galois groups*, Manuscr. Math. **43** (1983), 289–307.
10. Claus Fieker, Jürgen Klünners, *Galoisgruppen in Magma*, Computeralgebra-Rundbrief **43** (2008), 19–20.
11. Antoine Colin, *Formal computation of Galois groups with relative resolvents*, in: Gérard Cohen, Marc Giusti, Teo Mora, eds., *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes (AAECC-11)*, Lecture Notes in Computer Science **948**, pp. 169–182, Springer-Verlag, Berlin 1995.
12. Moss Sweedler, *Using Gröbner bases to determine the algebraic and transcendental nature of field extensions: Return of the killer tag variables*, in: Gérard Cohen, Teo Mora, Oscar Moreno, eds., *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, Springer-Verlag, Berlin, Heidelberg, New York 1993.
13. Clarence Wilkerson, *A primer on the Dickson invariants*, Amer. Math. Soc. Contemp. Math. Series **19** (1983), 421–434.
14. Shreeram S. Abhyankar, *Galois embeddings for linear groups*, Trans. Amer. Math. Soc. **352** (2000), 3881–3912.
15. Gunter Malle, B. Heinrich Matzat, *Inverse Galois Theory*, Springer-Verlag, Berlin, Heidelberg 1999.
16. Emmy Noether, *Gleichungen mit vorgeschrriebener Gruppe*, Math. Ann. **78** (1918), 221–229.
17. H. W. Lenstra, *Rational functions invariant under a finite abelian group*, Invent. Math. **25** (1974), 299–325.

18. Richard G. Swan, *Invariant rational functions and a problem of Steenrod*, Invent. Math. **7** (1969), 148–158.
19. David J. Saltman, *Noether's problem over an algebraically closed field*, Invent. Math. **77** (1984), 71–84.
20. David J. Saltman, *Groups acting on fields: Noether's problem*, Contemp. Mathematics **43** (1985), 267–277.
21. Gregor Kemper, *Das Noethersche Problem und generische Polynome*, Dissertation, Universität Heidelberg, 1994a, also available as: Preprint **94-49**, IWR, Heidelberg, 1994.
22. Gregor Kemper, Elena Mattig, *Generic polynomials with few parameters*, J. Symb. Comput. **30** (2000), 843–857.
23. F. Seidelmann, *Die Gesamtheit der kubischen und biquadratischen Gleichungen mit Affekt bei beliebigem Rationalitätsbereich*, Math. Ann. **78** (1918), 230–233.
24. Serge Lang, *Algebra*, Addison-Wesley Publishing Co., Reading, Mass. 1985.
25. Gregor Kemper, Gunter Malle, *Invariant fields of finite irreducible reflection groups*, Math. Ann. **315** (1999), 569–586.
26. Patrick A. Worfolk, *Zeros of equivariant vector fields: Algorithms for an invariant approach*, J. Symb. Comput. **17** (1994), 487–511.
27. Helmer Aslaksen, Shih-Ping Chan, Tor Gulliksen, *Invariants of S_4 and the shape of sets of vectors*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), 53–57.
28. Nicolas M. Thiéry, *PerMuVAR, a library for mupad for computing in invariant rings of permutation groups*, <http://permuvvar.sf.net/>.
29. Nicolas M. Thiéry, *Algebraic invariants of graphs; a study based on computer exploration*, SIGSAM Bulletin **34** (2000), 9–20.
30. Nicolas M. Thiéry, *Computing minimal generating sets of invariant rings of permutation groups with SAGBI-Gröbner basis*, in: *International Conference DM-CCG, Discrete Models - Combinatorics, Computation and Geometry*, Paris, July 2–5 2001, 2001, to appear.
31. S. M. Ulam, *A Collection of Mathematical Problems*, Interscience Publishers, New York, London 1960.
32. Maurice Pouzet, *Quelques remarques sur les résultats de Tutte concernant le problème de Ulam*, Publ. Dép. Math. (Lyon) **14** (1977), 1–8.
33. Nicolas M. Thiéry, *Invariants algébriques de graphes et reconstruction; une étude expérimentale*, Dissertation, Université Lyon I, Lyon 1999.
34. Maurice Pouzet, Nicolas M. Thiéry, *Invariants algébriques de graphes et reconstruction*, Comptes Rendus de l'Académie des Sciences **333** (2001), 821–826.
35. Richard P. Stanley, *Invariants of finite groups and their applications to combinatorics*, Bull. Amer. Math. Soc. **1(3)** (1979), 475–511.
36. Richard P. Stanley, *Combinatorics and invariant theory*, in: *Relations Between Combinatorics and Other Parts of Mathematics (Columbus, Ohio 1978)*, Proc. Symp. Pure Math. **34**, pp. 345–355, Am. Math. Soc., Providence, RI 1979.
37. B. Char, K. Geddes, G. Gonnet, M. Monagan, S. Watt, *Maple Reference Manual*, Waterloo Maple Publishing, Waterloo, Ontario 1990.
38. Louis Solomon, *Partition identities and invariants of finite groups*, J. Comb. Theory, Ser. A **23** (1977), 148–175.
39. Larry Smith, *Polynomial Invariants of Finite Groups*, A. K. Peters, Wellesley, Mass. 1995.
40. A. Elashvili, M. Jibladze, *Hermite reciprocity for the regular representations of cyclic groups*, Indag. Math., New Ser. **9** (1998), 233–238.
41. A. Elashvili, M. Jibladze, D. Pataraia, *Combinatorics of necklaces and “Hermite reciprocity”*, J. Algebr. Comb. **10** (1999), 173–188.
42. N.J.A. Sloane, *Error-correcting codes and invariant theory: New applications of a nineteenth-century technique*, Amer. Math. Monthly **84** (1977), 82–107.
43. F. Jessie MacWilliams, *A theorem on the distribution of weights in a systematic code*, Bell Syst. Tech. J. **42** (1963), 79–84.
44. G. C. Shephard, J. A. Todd, *Finite unitary reflection groups*, Canad. J. Math. **6** (1954), 274–304.

45. Andrew M. Gleason, *Weight polynomials of self-dual codes and the MacWilliams identities*, in: *Actes Congr. internat. Math.*, 3, 1970, pp. 211–215, Gauthier-Villars, Paris 1971.
46. Eric M. Rains, N.J.A. Sloane, *Self-dual codes*, in: Vera S. Pless, ed., *Handbook of Coding Theory*, vol. 1, pp. 177–294, Elsevier, Amsterdam 1998.
47. Eiichi Bannai, Steven T. Dougherty, Masaaki Harada, Manabu Oura, *Type II codes, even unimodular lattices, and invariant rings*, IEEE Trans. Inf. Theory **45** (1999), 1194–1205.
48. Gabriele Nebe, Eric M. Rains, Neil J. A. Sloane, *Self-dual Codes and Invariant Theory*, vol. 17 of *Algorithms and Computation in Mathematics*, Springer-Verlag, Berlin 2006.
49. D. H. Sattinger, *Group Theoretic Methods in Bifurcation Theory*, Lecture Notes in Math. **762**, Springer-Verlag, Berlin, Heidelberg, New York 1979.
50. Martin Golubitsky, David G. Schaeffer, *Singularities and Groups in Bifurcation Theory I*, Applied Mathematical Sciences **51**, Springer-Verlag, New York 1985.
51. Martin Golubitsky, Ian Stewart, David G. Schaeffer, *Singularities and Groups in Bifurcation Theory II*, Applied Mathematical Sciences **69**, Springer, New York 1988.
52. Karin Gatermann, *Computer Algebra Methods for Equivariant Dynamical Systems*, Lecture Notes in Mathematics **1728**, Springer-Verlag, Berlin, Heidelberg 2000.
53. Karin Gatermann, F. Guyard, *Gröbner bases, invariant theory and equivariant dynamics*, J. Symb. Comput. **28** (1999), 275–302.
54. Giuseppe Gaeta, Frank D. Grosshans, Jürgen Scheurle, Sebastian Walcher, *Reduction and reconstruction for symmetric ordinary differential equations*, J. Differential Equations **244** (2008), 1810–1839.
55. M. V. Jarić, L. Michel, R. T. Sharp, *Zeros of covariant vector fields for the point groups: Invariant formulation*, J. Physique **45** (1984), 1–27.
56. Karin Gatermann, Reiner Lauterbach, *Automatic classification of normal forms*, Nonlinear Analysis, Theory, Methods, and Applications **34** (1998), 157–190.
57. Ali Lari-Lavassani, William F. Langford, Koncay Huseyin, Karin Gatermann, *Steady-state mode interactions for D_3 and D_4 -symmetric systems*, Dynamics of Continuous, Discrete and Impulsive Systems **6** (1999), 169–209.
58. Sue Ann Campbell, Philip Holmes, *Heteroclinic cycles and modulated travelling waves in a system with D_4 symmetry*, Physica D **59** (1992), 52–78.
59. Michael A. Collins, Keiran C. Thompson, *Group theory and the global functional shapes for molecular potential energy surfaces*, in: Danail Bonchev, Dennis H. Rouvray, eds., *Chemical Group Theory: Techniques and Applications*, pp. 191–234, Gordon and Breach Publishers, Reading 1995.
60. Z. Hashin, *Failure criteria for unidirectional fiber composites*, J. Appl. Mech. **47** (1980), 329–334.
61. W. Helisch, *Invariante Systeme und Tensorgeneratoren bei Materialtensoren zweiter und vierter Stufe*, Dissertation, RWTH Aachen, Aachen 1993.
62. J. P. Boehler, ed., *Applications of Tensor Functions in Solid Mechanics*, CISM Courses and Lectures **292**, Springer-Verlag, Wien, New York 1987.
63. G.F. Smith, M.M. Smith, R.S. Rivlin, *Integrity bases for a symmetric tensor and a vector. The crystal classes*, Arch. Ration. Mech. Anal. **12** (1963), 93–133.
64. Sabine Meckbach, Gregor Kemper, *Invariants of textile reinforced composites*, preprint, Universität Gh Kassel, Kassel, 1999.
65. Joseph L. Mundy, Andrew Zisserman, eds., *Geometric Invariance in Computer Vision*, Artificial Intelligence, MIT Press, Cambridge, MA 1992.
66. Thomas H. Reiss, *Recognizing Planar Objects Using Invariant Image Features*, Lecture Notes in Computer Science **676**, Springer-Verlag, Berlin 1993.
67. Kenichi Kanatani, *Group-Theoretical Methods in Image Understanding*, Springer-Verlag, Berlin, Heidelberg, New York 1990.
68. Luc Florack, *Image Structure*, Computational Imaging and Vision **10**, Kluwer, Dordrecht, Boston, London 1997.

69. Charles A. Rothwell, Andrew Zisserman, David A. Forsyth, Joseph L. Mundy, *Fast recognition using algebraic invariants*, in: Joseph L. Mundy, Andrew Zisserman, eds., *Geometric Invariance in Computer Vision*, pp. 398–407, MIT Press, Cambridge, Mass. 1992.
70. Mireille Boutin, Gregor Kemper, *On reconstructing n -point configurations from the distribution of distances or areas*, Adv. Applied Math. **32** (2004), 709–735.
71. Gabriel Taubin, David B. Cooper, *Object recognition based on moment (or algebraic) invariants*, in: Joseph L. Mundy, Andrew Zisserman, eds., *Geometric Invariance in Computer Vision*, pp. 375–397, MIT Press, Cambridge, Mass. 1992.

Appendix A

Linear Algebraic Groups

A.1 Linear Algebraic Groups

Let us fix an algebraically closed field K . We work in the category of affine varieties over K . The purpose of this section is to give a brief exposition on the basic facts of algebraic groups.

Definition A.1.1 A **linear algebraic group** is an affine algebraic variety G together with a unit element $e \in G$ and morphisms $m : G \times G \rightarrow G$ and $i : G \rightarrow G$ satisfying the group axioms

- (a) $m(\sigma, e) = m(e, \sigma) = \sigma$ for all $\sigma \in G$;
- (b) $m(\sigma, i(\sigma)) = m(i(\sigma), \sigma) = e$ for all $\sigma \in G$;
- (c) $m(\sigma, m(\tau, \gamma)) = m(m(\sigma, \tau), \gamma)$ (associativity) for all $\sigma, \tau, \gamma \in G$.

Often we will just write $\sigma\tau$ and σ^{-1} instead of $m(\sigma, \tau)$ and $i(\sigma)$, respectively.

Example A.1.2 The group GL_n , the set of invertible $n \times n$ matrices over K , is a linear algebraic group. Any Zariski closed subgroup $G \subset \mathrm{GL}_n$ is a linear algebraic group. In fact, every linear algebraic group is isomorphic to a Zariski closed subgroup of GL_n (see Borel [1, Proposition I.1.10]). This justifies calling it a *linear* algebraic group. \triangleleft

The axioms for a linear algebraic group can also be stated in terms of the coordinate ring. The maps $m : G \times G \rightarrow G$ and $i : G \rightarrow G$ correspond to ring homomorphisms $m^* : K[G] \rightarrow K[G] \otimes K[G]$ and $i^* : K[G] \rightarrow K[G]$. The unit element $e \in G$ corresponds to a ring homomorphism $\epsilon : K[G] \rightarrow K$ defined by $f \mapsto f(e)$. The axioms for a linear algebraic group translate to

- (a) $(\mathrm{id} \otimes \epsilon) \circ m^* = (\epsilon \otimes \mathrm{id}) \circ m^* = \mathrm{id}$;
- (b) $(i^* \otimes \mathrm{id}) \circ m^* = (\mathrm{id} \otimes i^*) \circ m^* = \epsilon$ (using the inclusion $K \subset K[G]$ we can view $\epsilon : K[G] \rightarrow K$ as a map $K[G] \rightarrow K[G]$);
- (c) $(\mathrm{id} \otimes m^*) \circ m^* = (m^* \otimes \mathrm{id}) \circ m^*$.

Example A.1.3 The additive group \mathbb{G}_a is defined as the additive group of K . We define $m(x, y) = x + y$, $i(x) = -x$ for all $x, y \in K$ and $e = 0 \in K$. The coordinate ring $K[\mathbb{G}_a]$ is equal to the polynomial ring $K[t]$. The homomorphism $m^* : K[t] \rightarrow K[t] \otimes K[t]$ is defined by $m^*(t) = t \otimes 1 + 1 \otimes t$, $i^* : K[t] \rightarrow K[t]$ is defined by $t \mapsto -t$ and $\epsilon : K[t] \rightarrow K$ is defined by $f \mapsto f(0)$.

Example A.1.4 The group GL_n is an algebraic group. The coordinate ring $K[\mathrm{GL}_n]$ is isomorphic to

$$K[\{z_{ij} \mid 1 \leq i, j \leq n\}, T]/(f),$$

where $f = T \det(Z) - 1$ with Z the matrix $(z_{ij})_{i,j=1}^n$. Now $m^* : K[\mathrm{GL}_n] \rightarrow K[\mathrm{GL}_n] \otimes K[\mathrm{GL}_n]$ is defined by $z_{ij} \mapsto \sum_{k=1}^n z_{i,k} \otimes z_{k,j}$ for all i, j . Notice that $m^*(\det(Z)) = \det(Z) \otimes \det(Z)$.

Example A.1.5 Let $T = (K^*)^r$. The coordinate ring $K[T]$ is isomorphic to

$$K[z_1, \dots, z_r, z_1^{-1}, \dots, z_r^{-1}].$$

The ring homomorphisms $m^* : K[T] \rightarrow K[T] \otimes K[T]$, $i^* : K[T] \rightarrow K[T]$ and $\epsilon : K[T] \rightarrow K$ are given by $m^*(z_i) = z_i \otimes z_i$, $i^*(z_i) = z_i^{-1}$ and $\epsilon(z_i) = 1$ for all i . \triangleleft

Definition A.1.6 Suppose that X is an affine variety. A regular action of G on X is a morphism $\mu : G \times X \rightarrow X$ satisfying the axioms for an action

- (a) $\mu(e, x) = x$ for all $x \in X$;
- (b) $\mu(\sigma, \mu(\tau, x)) = \mu(m(\sigma, \tau), x)$ for all $\sigma, \tau \in G$ and all $x \in X$.

We will often just write $\sigma \cdot x$ instead of $\mu(\sigma, x)$. Instead of saying that G acts regularly on X , we often just say that X is a G -variety.

Definition A.1.7 Suppose that V is a (possibly infinite dimensional) vector space over K . A linear action $\mu : G \times V \rightarrow V$ of G on a vector space is called **rational** if there is a map $\mu^* : V \rightarrow V \otimes K[G]$ satisfying $\mu(\sigma, v) = \sum_{i=1}^l v_i f_i(\sigma)$ whenever $\mu^*(v) = \sum_{i=1}^l v_i \otimes f_i$

Lemma A.1.8 Suppose that a linear action of a linear algebraic group G on a vector space V is rational. For every $v \in V$ there exists a finite dimensional G -stable subspace $W \subseteq V$ containing v . The restriction of the G -action to W is also rational.

Proof Write $\mu^*(v) = \sum_{i=1}^l v_i \otimes f_i$ with f_1, \dots, f_l linearly independent over K . Let $W = K(G \cdot v)$, the linear span of the orbit $G \cdot v$. It is not hard to see that W is a subspace of the space spanned by v_1, \dots, v_l . This shows that $\dim W < \infty$.

We can restrict μ^* to W to obtain a map $W \rightarrow W \otimes K[G]$. Therefore the G -action on W is rational. \square

The content of Lemma A.1.8 can be expressed by saying that a rational action is “locally finite”. If G acts regularly on an affine variety X , then G also acts on the coordinate ring $K[X]$. For $\sigma \in G$ and $f \in K[X]$ we define $\sigma \cdot f \in K[X]$ by

$$(\sigma \cdot f)(x) = f(\sigma^{-1} \cdot x)$$

for all $x \in X$.

A map $X \rightarrow Y$ between two sets on which G acts is called G -equivariant if $\varphi(\sigma \cdot x) = \sigma \cdot \varphi(x)$ for all $x \in X$ and all $\sigma \in G$.

Lemma A.1.9 *Suppose that X is a G -variety. Then there exists a finite dimensional rational representation V and a G -equivariant closed embedding $X \hookrightarrow V$.*

Proof Choose generators f_1, \dots, f_r of $K[X]$ and let W be a finite dimensional G -stable subspace of $K[X]$ containing f_1, \dots, f_r . The inclusion $W \rightarrow K[X]$ extends to a surjective G -equivariant ring homomorphism $S(W) \twoheadrightarrow K[X]$, where $S(W)$ is the symmetric algebra. This ring homomorphism corresponds to a G -equivariant closed embedding $X \hookrightarrow W^*$ where W^* is the dual space of W . \square

The following two propositions can be found in Borel [1, Proposition I.1.2].

Proposition A.1.10 *A linear algebraic group G is smooth.*

Proposition A.1.11 *Let G° be the connected component of $e \in G$. Then G° is a normal subgroup of G of finite index.*

A.2 The Lie Algebra of a Linear Algebraic Group

We will first study the dual vector space $K[G]^*$ of $K[G]$. As we will see, $K[G]^*$ contains the Lie algebra \mathfrak{g} as a finite dimensional subspace. For every $\sigma \in G$ we can define $\epsilon_\sigma : K[G] \rightarrow K$ by $f \mapsto f(\sigma)$. In this way we can view G as a subset of $K[G]^*$. By Definition A.2.1 below, the group structure of G equips $K[G]^*$ with an associative algebra structure with identity element $\epsilon = \epsilon_e$. This even allows us to see $K[G]^*$ as an enveloping algebra of \mathfrak{g} (containing the universal enveloping algebra of \mathfrak{g}). Our approach is similar to Borel [1, §I.3].

Definition A.2.1 Suppose that $\delta, \gamma \in K[G]^*$. Then we define the convolution $\gamma * \delta \in K[G]^*$ as the composition of $\gamma \otimes \delta : K[G] \otimes K[G] \rightarrow K \otimes K = K$ and $m^* : K[G] \rightarrow K[G] \otimes K[G]$. In other words, suppose $f \in K[G]$ and $m^*(f) = \sum_i g_i \otimes h_i$, then

$$(\gamma * \delta)(f) = \sum_i \gamma(g_i) \delta(h_i).$$

Proposition A.2.2 *The space $K[G]^*$ is an associative algebra with the multiplication $*$ and unit element $\epsilon = \epsilon_e$.*

Proof From the axiom

$$m(m(\sigma, \tau), \mu) = m(\sigma, m(\tau, \mu)),$$

it follows that

$$(m^* \otimes \text{id}) \circ m^* = (\text{id} \otimes m^*) \circ m^*.$$

This multiplication is associative, because

$$\begin{aligned} (\delta * \gamma) * \varphi &= (((\delta \otimes \gamma) \circ m^*) \otimes \varphi) \circ m^* = (\delta \otimes \gamma \otimes \varphi) \circ (m^* \otimes \text{id}) \circ m^* = \\ &= (\delta \otimes \gamma \otimes \varphi) \circ (\text{id} \otimes m^*) \circ m^* = (\delta \otimes ((\gamma \otimes \varphi) \circ m^*)) \circ m^* = \delta * (\gamma * \varphi). \end{aligned} \quad (\text{A.2.1})$$

Notice that from $m(e, \sigma) = \sigma$ it follows that $(\epsilon \otimes \text{id}) \circ m^* = \text{id}$. We get

$$\delta * \epsilon = (\delta \otimes \epsilon) \circ m^* = \delta \circ (\text{id} \otimes \epsilon) \circ m^* = \delta \circ \text{id} = \delta,$$

and similarly $\epsilon * \delta = \delta$. □

Example A.2.3 If $f \in K[G]$ and $\sigma \in G$, we define $L_\sigma(f)$ and $R_\sigma(f)$ by $L_\sigma(f)(\tau) = f(\sigma\tau)$ and $R_\sigma(f)(\tau) = f(\tau\sigma)$. Notice that $(\text{id} \otimes \epsilon_\sigma) \circ m^* = R_\sigma$ and $(\epsilon_\sigma \otimes \text{id}) \circ m^* = L_\sigma$. From this it follows that

$$\delta * \epsilon_\sigma = \delta \circ (\text{id} \otimes \epsilon_\sigma) \circ m^* = \delta \circ R_\sigma$$

and

$$\epsilon_\sigma * \delta = \delta \circ (\epsilon_\sigma \otimes \text{id}) \circ m^* = \delta \circ L_\sigma.$$

△

Definition A.2.4 We define the **Lie algebra** \mathfrak{g} of G as the set of all $\delta \in K[G]^*$ satisfying

$$\delta(fg) = \delta(f)g(e) + f(e)\delta(g). \quad (\text{A.2.2})$$

for all $f, g \in K[G]$.

An element $\delta \in K[G]$ satisfying (A.2.2) is called a point derivation of $K[G]$ at e . Let \mathfrak{m}_e be the maximal ideal of $K[G]$ vanishing at $e \in G$. The Zariski tangent space $T_e(G)$ of G at e is defined as $(\mathfrak{m}_e/\mathfrak{m}_e^2)^*$ which is the dual space of $\mathfrak{m}_e/\mathfrak{m}_e^2$. If

$\delta \in (\mathfrak{m}_e/\mathfrak{m}_e^2)^*$, we can define $\rho(\delta) \in K[G]^*$ by

$$\rho(\delta)f = \delta(f - f(e) + \mathfrak{m}_e^2).$$

It is not hard to show that $\rho(\delta)$ is a point derivation at e and that $\delta \mapsto \rho(\delta)$ is an isomorphism between $T_e(G)$ and \mathfrak{g} . Because G is smooth (Proposition A.1.10) we have $\dim(\mathfrak{g}) = \dim(T_e(G)) = \dim(G)$.

Proposition A.2.5 *The space \mathfrak{g} is a Lie algebra with the Lie bracket*

$$[\delta, \gamma] := \delta * \gamma - \gamma * \delta.$$

Proof The only thing we have to show is that $[\delta, \gamma] \in \mathfrak{g}$ if $\delta, \gamma \in \mathfrak{g}$. But this is checked by a straightforward calculation. \square

Definition A.2.6 For $\delta \in K[G]^*$, we define $\bar{\delta} \in K[G]^*$ to be the composition $\delta \circ i^* : K[G] \rightarrow K[G] \rightarrow K$.

Lemma A.2.7 *The map $\delta \mapsto \bar{\delta}$ is an involution, and a skew algebra homomorphism $K[G]^* \rightarrow K[G]^*$, i.e., $\bar{\delta} * \gamma = \bar{\gamma} * \bar{\delta}$ for all $\delta, \gamma \in K[G]^*$ and $\bar{\epsilon} = \epsilon$.*

Proof The map $\delta \rightarrow \bar{\delta}$ is an involution because i and i^* are involutions.

Let $S : G \times G \rightarrow G \times G$ be defined by $S(\sigma, \tau) \rightarrow (\tau, \sigma)$ and let $S^* : K[G] \otimes K[G] \rightarrow K[G] \otimes K[G]$ be the dual ring homomorphism. From $i(m(\sigma, \tau)) = m(i(\tau), i(\sigma))$ it follows that

$$(i^* \otimes i^*) \circ m^* = S^* \circ m^* \circ i^*.$$

We can deduce from this that

$$\begin{aligned} \bar{\delta} * \bar{\gamma} &= (\delta \otimes \gamma) \circ (i^* \otimes i^*) \circ m^* = (\delta \otimes \gamma) \circ S^* \circ m^* \circ i^* = \\ &= (\gamma \otimes \delta) \circ m^* \circ i^* = (\gamma * \delta) \circ i^* = \bar{\gamma} * \bar{\delta}. \end{aligned} \quad (\text{A.2.3})$$

From $e^{-1} = e$ it follows that $\epsilon \circ i^* = \epsilon$ so $\bar{\epsilon} = \epsilon$. \square

Remark A.2.8 An action $\mu : G \times V \rightarrow V$ of G on a vector space is a rational representation if there is a map $\mu^* : V \rightarrow V \otimes K[G]$ with $\mu(\sigma, v) = ((\text{id} \otimes \epsilon_\sigma) \circ \mu^*)v$. \triangleleft

Definition A.2.9 For $\delta \in K[G]^*$ and $v \in V$ we define $\delta \cdot v$ by $((\text{id} \otimes \delta) \circ \mu^*)v$. In other words, if $\mu^*(v) = \sum_i v_i \otimes h_i$, then

$$\delta \cdot v = \sum_i v_i \delta(h_i).$$

In particular, we have $\sigma \cdot v = \epsilon_\sigma \cdot v$ for all $\sigma \in G$ and $v \in V$.

Proposition A.2.10 *The map $(\delta, v) \mapsto \delta \cdot v$ gives V the structure of a $K[G]^*$ -module.*

Proof From the axiom

$$\mu(\sigma, \mu(\tau, v)) = \mu(m(\sigma, \tau), v)$$

for all $\sigma, \tau \in G$ and $v \in V$, it follows that

$$(\text{id} \otimes m^*) \circ \mu^* = (\mu^* \otimes \text{id}) \circ \mu^*.$$

We have

$$\begin{aligned} \gamma \cdot (\delta \cdot v) &= ((\text{id} \otimes \gamma) \circ \mu^* \circ (\text{id} \otimes \delta) \circ \mu^*)v = \\ &= ((\text{id} \otimes \gamma) \circ (\text{id} \otimes \text{id} \otimes \delta) \circ (\mu^* \otimes \text{id}) \circ \mu^*)v = ((\text{id} \otimes \gamma \otimes \delta) \circ (\text{id} \otimes m^*) \circ \mu^*)v \\ &= ((\text{id} \otimes ((\gamma \otimes \delta) \circ m^*)) \circ \mu^*)v = (\gamma * \delta) \cdot v. \end{aligned} \quad (\text{A.2.4})$$

From $\mu(e, x) = x$ it follows that

$$(\text{id} \otimes \epsilon) \circ \mu^* = \text{id},$$

so

$$\epsilon \cdot v = ((\text{id} \otimes \epsilon) \circ \mu^*)v = \text{id } v = v.$$

□

Example A.2.11 The group G acts on $K[G]$ as follows: Let $\tilde{\mu} : G \times G \rightarrow G$ defined by $(\tau, \sigma) \mapsto (\sigma^{-1}\tau)$ and let $\mu^* : K[G] \rightarrow K[G] \otimes K[G]$ be the dual homomorphism. The maps m and m^* are as usual, the multiplication map $G \times G \rightarrow G$ and its dual homomorphism respectively. We have

$$(\delta \cdot f)(e) = ((\epsilon \otimes \delta) \circ \mu^*)f = ((\epsilon \otimes (\delta \circ i^*)) \circ m^*)f = (\epsilon * \bar{\delta})f = \bar{\delta}f.$$

△

Example A.2.12 Let X be an affine G -variety. Suppose that $\mu^* : K[X] \rightarrow K[X] \otimes K[G]$ is the dual homomorphism of $\tilde{\mu} : X \times G \rightarrow X$ defined by $(x, \sigma) \mapsto \sigma^{-1} \cdot x$. For $f \in K[X]$ we already defined

$$(\sigma \cdot f)(x) = f(\sigma^{-1} \cdot x) = f(\tilde{\mu}(x, \sigma)) = \mu^*(f)(x, \sigma) = ((\text{id} \otimes \epsilon_\sigma) \circ \mu^*)(f)(x)$$

for all $f \in K[X]$, $x \in X$, $\sigma \in G$. This shows that $K[X]$ is a rational representation of G . Now also $K[G]^*$ acts on $K[X]$ and in particular \mathfrak{g} acts on $K[X]$. □

Lemma A.2.13 *The Lie algebra \mathfrak{g} acts on $K[X]$ by derivations.*

Proof Let $f, u \in K[X]$, and write $\mu^*(f) = \sum_i g_i \otimes h_i$ and $\mu^*(u) = \sum_j v_j \otimes w_j$. Then we have

$$\begin{aligned} \delta \cdot fu &= \sum_{i,j} g_i v_j \delta(h_i w_j) = \sum_{i,j} (g_i v_j \delta(h_i) w_j(e) + g_i v_j h_i(e) \delta(w_j)) = \\ &= (\delta \cdot f)(\epsilon \cdot u) + (\epsilon \cdot f)(\delta \cdot u) = (\delta \cdot f)u + f(\delta \cdot u). \end{aligned} \quad (\text{A.2.5})$$

□

Definition A.2.14 For $\sigma \in G$ and $\delta \in K[G]^*$, we define

$$\text{Ad}(\sigma)\delta := \epsilon_\sigma * \delta * \epsilon_{\sigma^{-1}}.$$

Notice that $\epsilon_{\sigma^{-1}}$ is the inverse of ϵ_σ in the algebra $K[G]^*$. This shows that $\text{Ad}(\sigma)$ is an algebra automorphisms of $K[G]^*$ for every $\sigma \in G$.

Lemma A.2.15 *The map Ad defines a rational action of G on \mathfrak{g} .*

Proof If $f \in K[G]$, $\sigma \in G$ and $\delta \in K[G]^*$, then from Example A.2.3 it follows that

$$(\text{Ad}(\sigma)\delta)f = (\epsilon_\sigma * \delta * \epsilon_{\sigma^{-1}})f = L_\sigma R_{\sigma^{-1}}f.$$

Now \mathfrak{g} can be characterized as the set of all $\delta \in K[G]^*$ such that $\delta(\mathfrak{m}_e^2) = \{0\}$ and $\delta(1) = 0$ where \mathfrak{m}_e is the maximal ideal in $K[G]$ corresponding to $e \in G$. Since both \mathfrak{m}_e^2 and 1 are stable under $L_\sigma R_{\sigma^{-1}}$, it follows that $\text{Ad}(\sigma)\mathfrak{g} \subseteq \mathfrak{g}$. We can let G act on $K[G]$ by

$$(\sigma \cdot f)(\tau) = f(\sigma^{-1}\tau\sigma) = (L_{\sigma^{-1}}R_\sigma f)(\tau).$$

This action of G on $K[G]^*$ via Ad is dual to this action. In particular the action of G via Ad on \mathfrak{g} is dual to the action of G on $\mathfrak{m}_e/\mathfrak{m}_e^2$ and therefore defines a rational representation. □

A.3 Reductive and Semi-simple Groups

We now introduce some structure theory of linear algebraic groups. Let G be a linear algebraic group.

Definition A.3.1 A **Borel subgroup** B of G is a maximal connected solvable subgroup.

We also often will need a maximal torus T of G . Since tori are connected and solvable, clearly T is contained in some Borel subgroup B and it is a maximal torus of B as well.

Theorem A.3.2 *All Borel subgroups of G are conjugate.*

Proof See Borel [1, IV.11.1]. □

Definition A.3.3 An endomorphism $A \in \mathrm{GL}(V)$ is called **unipotent** if $A - I$ is nilpotent, i.e., $(A - I)^N = 0$ for some positive integer N where I is the identity of $\mathrm{GL}(V)$. An algebraic group U is called **unipotent** if for every finite dimensional representation $\rho : U \rightarrow \mathrm{GL}(V)$ and every $\sigma \in U$ we have that $\rho(\sigma)$ is a unipotent endomorphism.

Proposition A.3.4 *Suppose that B is a solvable connected linear algebraic group. Let T be a maximal torus of B . Then there exists a unique connected unipotent normal subgroup B_u such that B is a semidirect product of T and B_u .*

Proof See Borel [1, III.10.6]. □

Definition A.3.5 Suppose that G is a linear algebraic group and let \mathcal{B} be the set of all Borel subgroups of G . The **radical** $R(G)$ of G is defined as the connected component of the intersection of all Borel subgroups, i.e.,

$$R(G) = \left(\bigcap_{B \in \mathcal{B}} B \right)^\circ.$$

The unipotent part $R(G)_u$ of $R(G)$ is called the **unipotent radical** of G .

Definition A.3.6 A linear algebraic group G is called **reductive** if the unipotent radical $R(G)_u$ is trivial, or equivalently, if $R(G)$ is a torus. If $R(G)$ is trivial, then G is called **semi-simple**.

A.4 Roots

Suppose that G is a connected reductive group, $T \subseteq G$ is a maximal torus and $B \subseteq G$ is a Borel subgroup containing T . Let $m = \dim G$ and $r = \dim T$. Let $X(T) \cong \mathbb{Z}^r$ be the set of 1-dimensional characters, i.e., the set of algebraic group homomorphisms $T \rightarrow \mathbb{G}_m$, where \mathbb{G}_m is the multiplicative group. Usually, we use additive notation for the group $X(T)$. We let $X^\vee(T) \cong \mathbb{Z}^r$ be the set of algebraic group homomorphisms $\mathbb{G}_m \rightarrow T$. We have a pairing $\langle \cdot, \cdot \rangle : X(T) \times X^\vee(T) \rightarrow \mathbb{Z}$ which is defined as follows. If $\chi : T \rightarrow \mathbb{G}_m$ and $\lambda : \mathbb{G}_m \rightarrow T$ are algebraic group homomorphisms, then $\chi(\lambda(\sigma)) = \sigma^a$ for some $a \in \mathbb{Z}$ and all $\sigma \in \mathbb{G}_m$. We define $\langle \chi, \lambda \rangle = a$.

The Weyl group W is the group $N_G(T)/Z_G(T)$ where $N_G(T)$ is the normalizer of T in G and $Z_G(T)$ is the centralizer of T in G . The Weyl groups acts in a natural way on $X(T)$ and $X^\vee(T)$.

Consider the adjoint representation of G on \mathfrak{g} . For an element $\alpha \in X(T)$ we define

$$\mathfrak{g}_\alpha = \{v \in \mathfrak{g} \mid \text{Ad}(\sigma)v = \alpha(\sigma)v \text{ for all } \sigma \in T\}.$$

A nonzero element $\alpha \in X(T)$ is called a **root** if $\mathfrak{g}_\alpha \neq 0$. We write Φ for the set of all roots. Since the action of the torus is diagonalizable (see Borel [1, Proposition III.8.4]), we have a decomposition

$$\mathfrak{g} = \mathfrak{g}^T \oplus \bigoplus_{\alpha \in \Phi} \mathfrak{g}_\alpha$$

where $\mathfrak{g}^T = \mathfrak{g}_0$ is the T -invariant subspace. For each root α , the space \mathfrak{g}_α is 1-dimensional (this follows from Humphreys [2][8.4.]).

Let α be a root. The kernel T_α of α is a torus of dimension $r - 1$. There is a unique nontrivial element $s_\alpha \in W$ which fixes T_α . The group W is generated by all reflections $s_\alpha, \alpha \in \Phi$.

We define $\alpha^\vee \in X^\vee(T)$ by

$$s_\alpha(\beta) = \beta - \langle \beta, \alpha^\vee \rangle \alpha.$$

Let $\mathfrak{t} \subset \mathfrak{g}$ be the Lie algebra of the torus T and let $\mathfrak{u} \subset \mathfrak{g}$ be the Lie algebra of the unipotent complement U of T in B . We have $\mathfrak{t} = \mathfrak{g}^T$, and \mathfrak{u} is a direct sum of weight spaces \mathfrak{g}_α . Let us define the set of positive roots Φ_+ by

$$\mathfrak{u} = \bigoplus_{\alpha \in \Phi_+} \mathfrak{g}_\alpha.$$

We define $\Phi_- := -\Phi_+$. It is known that Φ is the disjoint union of Φ_+ and Φ_- .

We can uniquely choose a subset $\Delta = \{\alpha_1, \dots, \alpha_l\}$ of Φ_+ with the following properties:

- (a) $\alpha_1, \dots, \alpha_l$ is an \mathbb{R} -basis of $E = X(T) \otimes_{\mathbb{Z}} \mathbb{R}$;
- (b) $\langle \alpha_i, \alpha_j^\vee \rangle \leq 0$ for all $i \neq j$.

Elements of Δ are called **simple roots**. Every $\alpha \in \Phi_+$ can uniquely be written as a sum

$$m_1\alpha_1 + m_2\alpha_2 + \cdots + m_l\alpha_l$$

for some nonnegative integers m_1, \dots, m_l .

A.5 Representation Theory

Let G be a connected reductive linear algebraic group over an algebraically closed field K . Let $\Delta = \{\alpha_1, \dots, \alpha_l\}$ be the set of simple roots. A weight $\lambda \in X(T)$ is called **dominant** if $\langle \lambda, \alpha_i^\vee \rangle \geq 0$ for all simple roots α_i . There exist unique so-called **fundamental weights** $\lambda_1, \dots, \lambda_l \in X(T) \otimes_{\mathbb{Z}} \mathbb{Q}$ such that $\langle \lambda_i, \alpha_j^\vee \rangle = \delta_{ij}$ where δ_{ij} is the Kronecker delta symbol.

Theorem A.5.1 Choose a Borel subgroup $B \subset G$, a maximal torus $T \subset G$ and a unipotent subgroup $U \subset B$ such that $B = T \ltimes U$. If V is an irreducible representation of G , then $V^U = Kv$ for some nonzero vector $v \in V$. We have $\sigma \cdot v = \lambda(\sigma)v$ for all $\sigma \in T$ for some dominant weight $\lambda \in X(T)$ called the **highest weight** of V . For each dominant weight $\lambda \in X(T)$ there exists a unique irreducible representation V_λ with highest weight λ .

Proof See Humphreys [3, Chap. IX]. □

A vector $v_\lambda \in V_\lambda$ with $V_\lambda^U = Kv_\lambda$ and $\sigma \cdot v_\lambda = \lambda(\sigma)v_\lambda$ for all $\sigma \in T$ is called a **highest weight vector** of V_λ .

Definition A.5.2 Suppose $\mu : G \rightarrow \mathrm{GL}(V)$ is a rational representation of G . Then the character $\chi^V : T \rightarrow K$ is defined by

$$\chi^V(\sigma) = \mathrm{Tr}(\mu(\sigma))$$

for all $\sigma \in T$.

In the sequel, we would rather use multiplicative notation in $X(T)$. To each fundamental weight λ_i ($1 \leq i \leq l$) in the additive notation we associate an indeterminate z_i (i.e., a character in the multiplicative notation). If $\lambda = \sum_{i=1}^l a_i \lambda_i$ is a weight, we define $z^\lambda := z_1^{\lambda_1} z_2^{\lambda_2} \cdots z_l^{\lambda_l}$. The action of the torus T is diagonalizable, so after a convenient choice of basis, the action is given by a matrix

$$\mu = \begin{pmatrix} m_1(z) & 0 & \cdots & 0 \\ 0 & m_2(z) & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & m_n(z) \end{pmatrix}.$$

where m_1, \dots, m_n are monomials in z_1, \dots, z_l . The character χ^V is then given by the formal sum

$$m_1(z) + m_2(z) + \cdots + m_n(z).$$

Let us write $\rho = \lambda_1 + \cdots + \lambda_l$.

Theorem A.5.3 (Weyl's Theorem, see Humphreys [2, 24.3])

$$\chi^{V_\lambda} \sum_{w \in W} \text{sgn}(w) z^{w(\rho)} = \sum_{w \in W} \text{sgn}(w) z^{w(\rho + \lambda)}.$$

References

1. Armand Borel, *Linear Algebraic Groups*, Graduate Texts in Mathematics **126**, Springer Verlag, New York 1991.
2. James E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Springer-Verlag, Berlin, Heidelberg, New York 1980.
3. James E. Humphreys, *Linear Algebraic Groups*, Springer-Verlag, Berlin, Heidelberg, New York 1981.

Appendix B

Is One of the Two Orbits in the Closure of the Other?

Vladimir L. Popov

B.1 Introduction

B.1.1 In this appendix we expound two solutions, suggested in [1], to the following Problem B.1.1 permanently arising in algebraic transformation group theory and its applications.

Let G be a connected affine algebraic group and let V be a finite dimensional algebraic G -module, all are taken over an algebraically closed ground field k of arbitrary characteristic. Given a subset X of V , we denote by \overline{X} the Zariski closure of X in V . Consider two points a and $b \in V$ and their G -orbits $G \cdot a$ and $G \cdot b$.

Problem B.1.1 *How can one constructively verify whether or not $G \cdot a \subseteq \overline{G \cdot b}$?*

B.1.2 We shall give two solutions to Problem B.1.1. Both are based on the possibility to rationally parametrize an open subset of G by means of a variety $\mathbb{A}^{r,s}$ of a special type (see below formula (B.3.1)).

Namely, in Sect. B.3 we expound an algorithm that yields, by means of a finite number of effectively feasible operations, a finite system of linear equations in finitely many variables over the field k such that the inclusion $G \cdot a \subseteq \overline{G \cdot b}$ is equivalent to its inconsistency (the precise formulation is contained in Theorem B.3.5).

Steklov Mathematical Institute, Russian Academy of Sciences, Gubkina 8, Moscow 119991, Russia. *E-mail address:* popovvl@mi.ras.ru

Supported by the program *Geometry of Algebraic Varieties* of the Russian Federal Agency of Scientific Organizations.

By Kronecker–Capelli’s theorem this reduces solving Problem B.1.1 to comparing the ranks of two explicitly given matrices with coefficients in k that can be executed constructively.

In Sect. B.4 we expound another algorithm for solving Problem B.1.1. It is a straightforward reduction to elimination using Gröbner bases. Being less effective, it concerns a more general problem.

The survey [2] illustrates these algorithms by examples.

B.1.3 Since any orbit of algebraic transformation group is open in its closure (see [3]), we have

$$G \cdot a = G \cdot b \iff G \cdot a \subseteq \overline{G \cdot b} \text{ and } G \cdot b \subseteq \overline{G \cdot a}.$$

Therefore, a constructive solution to Problem B.1.1 provides a constructive solution to the following problem:

Problem B.1.2 *How can one constructively verify whether or not two given points of V lie in the same G -orbit?*

This means that our result yields a constructive solution to the classification problem for some types of mathematical objects: for instance, for k -algebras of a fixed dimension up to isomorphisms; for A -modules of a fixed dimension over a fixed k -algebra A up to isomorphism; for k -representations of a fixed dimension of a given quiver; for some types of algebraic varieties (see below Examples B.2.6, B.2.7, B.2.9).

B.1.4 As every normal quasiprojective variety endowed with an algebraic action of G can be equivariantly embedded in a projective space (see, e.g., [4, Thm. 1.7]), a problem analogous to Problem B.1.1 but for the action of G on a projective space continually arises in algebraic transformation group theory and its applications. However, this problem is reduced to Problem B.1.1 for actions on vector spaces, see Sect. B.3.4.

B.1.5 Before proceeding to the description of the algorithm, we shall give several examples of the cases, in which Problems B.1.1 and B.1.2 arise.

B.2 Examples

Example B.2.1 If G is reductive and $a = 0$, then Problem B.1.1 means constructively finding out whether or not b is unstable point in the sense of Geometric Invariant Theory [5]. A description of the cone of all unstable points is provided by the Hilbert–Mumford theory (see below Appendix C).

Example B.2.2 Let G be a torus and let $X(G)$ be the group of its characters in additive notation. For every $\lambda \in X(G)$, $g \in G$, and $v \in V$ denote by g^λ and v_λ , respectively, the value of λ at g and the projection of v to the λ -weight subspace of the G -module V parallel to the sum of the other weight subspaces. Let

$\text{supp } v := \{\lambda \in X(G) \mid v_\lambda \neq 0\}$. Then by the elementary properties of toric varieties Problem B.1.1 means constructively finding out whether or not

- (i) the cone generated by $\text{supp } a$ in $X(G) \otimes_{\mathbb{Z}} \mathbb{R}$ is a face of the cone generated by $\text{supp } b$, and
- (ii) there is an element $g \in G$ such that $g^\lambda a_\lambda = b_\lambda$ for every $\lambda \in \text{supp } a$.

Example B.2.3 If the group G is unipotent, then every G -orbit is closed in V , see [6]. Therefore, in this case Problem B.1.1 means constructively finding out whether or not the points a and b lie in the same G -orbit, i.e., Problem B.1.1 is equivalent to Problem B.1.2.

Example B.2.4 Let $\text{char } k = 0$. Assume that G is a simple group, V is its Lie algebra endowed with the adjoint action of G , and the elements a and b are nilpotent. If G is a classical group (i.e., of type A_l , B_l , C_l , or D_l), then the constructive solution to Problem B.1.1 is given by the known rule formulated in terms of the sizes of Jordan blocks of the Jordan normal forms of a and b , see, e.g., [7]. If the group G is exceptional (i.e., of type E_6 , E_7 , E_8 , F_4 , or G_2), such a solution, obtained by means of ad hoc methods, is known as well; in this case the answer is given by the explicit Hasse diagrams of the set of nilpotent orbits endowed with the *Bruhat order*, i.e., partially ordered according to the rule $\mathcal{O}_1 \leqslant \mathcal{O}_2 \iff \mathcal{O}_1 \subseteq \overline{\mathcal{O}_2}$, see [8, 9].

More generally, for nilpotent elements of the so-called θ -groups (see below Section C.4.7. of Appendix C) a solution to Problem B.1.1 is given, in view of Propositions 2 and 4 of Appendix C (see Sect. C.2.12), by the algorithms expounded in the present appendix; another algorithm is obtained in [10] (see also the survey [2]).

Example B.2.5 Apart from the classical case of orbits of a Borel subgroup of a reductive group G on the generalized flag variety G/P and the case of Example B.2.4, the Hasse diagrams of the sets of orbits endowed with the Bruhat order are found utilizing the ad hoc methods in some other special cases (see, e.g., [11–15], and Examples B.2.6, B.2.7 below). On the other hand, in a number of cases the orbits are classified, but the Hasse diagrams are not found: for instance, this is so for nilpotent 3-vectors of the n -dimensional spaces where $n \leqslant 9$, for 4-vectors of an 8-dimensional space, for spinors of the m -dimensional spaces where $m \leqslant 14$ and 16 (see the relevant references in [4]).

Example B.2.6 Let L be a finite dimensional vector space over k . Let $G = \text{GL}(L)$ and $V = L^* \otimes L^* \otimes L$. The points of V are structures of (not necessarily associative) k -algebras on the vector space L . The algebras defined by structures a and b are isomorphic if and only if $G \cdot a = G \cdot b$. In the language of the theory of algebras, Problem B.1.1 is formulated as follows: How can one constructively find out whether or not the algebra defined by the structure a is a *degeneration* of the algebra defined by the structure b ? In general case it is considered to be a difficult problem. There is a number of papers where a classification of degenerations in various special cases is obtained by means of ad hoc methods (see, e.g., [16–18], and the survey [19, Chap. 7]).

Example B.2.7 Consider the conjugation action of the group $G = \mathrm{GL}_d(k)$ on $\mathrm{Mat}_{d,d}(k)$. Let A be a finite dimensional associative k -algebra and let L be a d -dimensional vector space over k . If a basis in A and a basis in L are fixed, then the set of structures of left A -modules on L is naturally identified with a Zariski closed G -stable subset Mod_A^d of $V := \mathrm{Mat}_{d,d}(k)^{\oplus \dim_k A}$ (the direct sum of $\dim_k A$ copies of the G -module $\mathrm{Mat}_{d,d}(k)$). Denote by M_x the A -module corresponding to a point $x \in \mathrm{Mod}_A^d$. Then the A -modules M_a and M_b are isomorphic if and only if $G \cdot a = G \cdot b$, and in this theory the condition $G \cdot a \subseteq \overline{G \cdot b}$ is expressed by saying that M_a is a *degeneration* of M_b . In the case when A is the path algebra of a quiver obtained by fixing an orientation of the extended Dynkin graph of a root system of type A_l , D_l , E_6 , E_7 , or E_8 , a characterization of the degeneration relation in terms of the A -module structures of M_a and M_b and an algorithm for finding out whether or not M_a is a degeneration of M_b are obtained in [20].

Example B.2.8 In the case of the natural action of the group $G = \mathrm{GL}_n(k)$ on the space of n -ary forms of degree d with coefficients in k , Problem B.1.1 (under the name *The orbit closure problem*) is of fundamental importance in the application of geometric invariant theory to complexity theory: Valiant's conjecture links Cook's celebrated $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$ problem with finding out whether or not the padded permanent lies in the G -orbit closure of the determinant (see [21, 22, 23]).

Example B.2.9 Let f_1 and f_2 be two irreducible forms of the same degree $d > 2$ in the homogeneous coordinates of the projective space \mathbb{P}^n with coefficients in k . Assume that, for every $i = 1, 2$, the hypersurface H_i in \mathbb{P}^n defined by the equation $f_i = 0$ is smooth. Let $n \geq 4$. Then by a theorem of Severi–Lefschetz–Andreotti every positive divisor on the hypersurface H_i is cut out by a hypersurface in \mathbb{P}^n (see [24, Thm. 2]). It is not difficult to deduce from this that the algebraic varieties H_1 and H_2 are isomorphic if and only if H_1 is the image of H_2 under a projective transformation of \mathbb{P}^n , i.e., if and only if f_1 is in the $\mathrm{GL}_{n+1}(k)$ -orbit of f_2 .

There are other types of algebraic varieties for which the isomorphism problem is reduced to finding out whether or not some forms lie in the same orbit of the corresponding affine algebraic group. For instance, smooth irreducible projective curves of a genus $g \geq 2$ are embedded in \mathbb{P}^{5g-6} by means of the tripled canonical class, and two curves are isomorphic if and only if the image of one of them is transformed to the image of the other by a projective transformation of \mathbb{P}^{5g-6} . In turn, the latter condition is equivalent to the property that the Chow forms (also known as Cayley forms) of these images lie in one and the same orbit of the corresponding affine algebraic group.

B.3 Algorithm

B.3.1 We denote by \mathbb{N} the set of all nonnegative integers. Given two numbers $r, s \in \mathbb{N}$, we put

$$\mathbb{A}^{r,s} := \{(\varepsilon_1, \dots, \varepsilon_{r+s}) \in \mathbb{A}^{r+s} \mid \varepsilon_1 \cdots \varepsilon_r \neq 0\}. \quad (\text{B.3.1})$$

Our considerations are based on the following fact.

Lemma B.3.1 *For some $r, s \in \mathbb{N}$, there is a dominant morphism*

$$\iota: \mathbb{A}^{r,s} \rightarrow G. \quad (\text{B.3.2})$$

Moreover, for $r = \text{rk } G$, there is an open embedding (B.3.2).

Proof Let $R_u(G)$ be the unipotent radical of the group G . In view of [25, Props. 1, 2], [26, Thm. 10], the underlying variety of G is isomorphic to the product of that of $G/R_u(G)$ and $R_u(G)$, and the latter is isomorphic to the affine space $\mathbb{A}^{\dim R_u(G)}$. On the other hand, the big Bruhat cell of the reductive group $G/R_u(G)$ is isomorphic to $\mathbb{A}^{r, \dim G/R_u(G) - r}$, where $r = \text{rk } G/R_u(G) = \text{rk } G$ (see [3]). As the variety $\mathbb{A}^{r, \dim G - r}$ is isomorphic to $\mathbb{A}^{\dim R_u(G)} \times \mathbb{A}^{r, \dim G/R_u(G) - r}$, this shows that there is its open embedding in G . \square

B.3.2 Functions $\rho_{i,j}$ and x_i

Fix a basis e_1, \dots, e_n in V . As the case $n = 1$ is clear, below we assume that $n > 1$. There are the regular functions $\rho_{i,j}: G \rightarrow k$, $1 \leq i, j \leq n$, such that the G -module structure on V is determined by the matrix representation

$$\rho: G \rightarrow \text{Mat}_{n,n}(k), \quad \rho(g) = \begin{bmatrix} \rho_{1,1}(g) & \cdots & \rho_{1,n}(g) \\ \vdots & \ddots & \vdots \\ \rho_{n,1}(g) & \cdots & \rho_{n,n}(g) \end{bmatrix}, \quad g \in G, \quad (\text{B.3.3})$$

i.e., $\rho(g)$ is the matrix of the linear $V \rightarrow V$, $v \mapsto g \cdot v$ in the basis e_1, \dots, e_n , so that

$$g \cdot \left(\sum_{i=1}^n \gamma_i e_i \right) = \sum_{i=1}^n \left(\sum_{j=1}^n \rho_{i,j}(g) \gamma_j \right) e_i \quad \text{for any } g \in G \text{ and } \gamma_1, \dots, \gamma_n \in k. \quad (\text{B.3.4})$$

Applying Lemma B.3.1, fix a dominant morphism (B.3.2). Let x_1, \dots, x_{r+s} the standard coordinate functions on $\mathbb{A}^{r,s}$:

$$x_i(a) = \varepsilon_i \quad \text{for } a = (\varepsilon_1, \dots, \varepsilon_{r+s}) \in \mathbb{A}^{r,s}. \quad (\text{B.3.5})$$

As $x_1, \dots, x_{r+s}, x_1^{-1}, \dots, x_r^{-1}$ generate the k -algebra $k[\mathbb{A}^{r,s}]$ of regular functions on $\mathbb{A}^{r,s}$ and x_1, \dots, x_{r+s} are algebraically independent over k , all monomials of the form

$$x_1^{i_1} \cdots x_{r+s}^{i_{r+s}}, \quad \text{where } i_1, \dots, i_{r+s} \in \mathbb{Z} \quad \text{and } i_{r+1}, \dots, i_{r+s} \in \mathbb{N}, \quad (\text{B.3.6})$$

constitute a basis of the vector space $k[\mathbb{A}^{r,s}]$ over k .

B.3.3 The degree of the variety $\rho(G)$

Recall [27] that the degree of a locally closed subset Y of \mathbb{A}^l is the cardinality $\deg Y$ of the intersection of Y with an $(l - \dim Y)$ -dimensional linear subvariety of

\mathbb{A}^l in general position. For us, the degree $\deg \rho(G)$ of the subvariety $\rho(G)$ of the space of matrices $\text{Mat}_{n,n}(k)$ is of the special interest. Recall from Sect. 4.7.1 that if $\text{char } k = 0$, G is a reductive group, and the kernel of ρ is finite, then $\deg \rho(G)$ is given by Kazarnovskii's formula (see Definition 4.7.13 and Proposition 4.7.18). The number $\deg \rho(G)$ is used in our algorithm and considered to be known to us.

Example B.3.2 Let $\text{char } k = 0$. Consider the main object of pre-Hilbertian classical invariant theory: $G = \text{SL}_2(k)$ and $V = V_h$ is the space of binary forms of degree h in variables z_1, z_2 over the field k , on which G acts by linear substitutions of variables:

$$g \cdot z_1 = \alpha z_1 + \gamma z_2, \quad g \cdot z_2 = \beta z_1 + \delta z_2, \quad \text{if } g = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in G. \quad (\text{B.3.7})$$

Take as the basis e_1, \dots, e_{h+1} of V the sequence $z_1^h, z_1^{h-1}z_2, \dots, z_1 z_2^{h-1}, z_2^h$, and let ρ_h be the matrix representation given by formula (B.3.3). Its kernel is finite, and Kazarnovskii's formula yields (see Example 4.7.19)

$$\deg \rho_h(\text{SL}_2) = \begin{cases} 2h^3 & \text{if } h \text{ is odd,} \\ h^3 & \text{if } h \text{ is even.} \end{cases} \quad (\text{B.3.8})$$

B.3.4 Reduction to the conical case

Let L be a finite dimensional vector space over k . Let H be an algebraic group (algebraically) acting on a projective space $\mathbb{P}(L)$ of all one-dimensional linear subspaces of L . Keeping H -orbits in $\mathbb{P}(L)$, we may replace the group H by its quotient group by the kernel of the action and assume that H is a subgroup of $\text{Aut}(\mathbb{P}(L))$. Let \tilde{H} be the inverse image of H with respect to the natural homomorphism $\text{GL}(L) \rightarrow \text{Aut}(\mathbb{P}(L))$ (note that H is reductive if and only if \tilde{H} shares this property). Let $\pi: L \setminus \{0\} \rightarrow \mathbb{P}(L)$ be the natural projection. We call a subset in L *conical* if it is stable with respect to scalar multiplication by every nonzero element of k .

Lemma B.3.3 *Let U be a nonempty open H -stable subset of $\mathbb{P}(L)$ and let $p, q \in U$ be two its points. Take any points $\tilde{p} \in \pi^{-1}(p)$ and $\tilde{q} \in \pi^{-1}(q)$. Then the following properties are equivalent:*

- (i) *the orbit $H \cdot p$ lies in the Zariski closure of the orbit $H \cdot q$ in $\mathbb{P}(L)$;*
- (ii) *the orbit $H \cdot p$ lies in the Zariski closure of the orbit $H \cdot q$ in U ;*
- (iii) *the orbit $\tilde{H} \cdot \tilde{p}$ lies in the Zariski closure of the orbit $\tilde{H} \cdot \tilde{q}$ in L .*

The orbits $\tilde{H} \cdot \tilde{p}$ and $\tilde{H} \cdot \tilde{q}$ are conical.

Proof As \tilde{H} contains all scalar multiplications of the space L by nonzero scalars, $\tilde{H} \cdot \tilde{p} = \pi^{-1}(H \cdot p)$ and $\tilde{H} \cdot \tilde{q} = \pi^{-1}(H \cdot q)$. The statement follows from this and the definitions. \square

We will need the following application of Lemma B.3.3. Let L be the coordinate space k^{n+1} and let H be the group G from Sect. B.1.1 that acts on $\mathbb{P}(L)$ according to the rule (see (B.3.3))

$$g \cdot (\alpha_0 : \alpha_1 : \dots : \alpha_n) := \left(\alpha_0 : \sum_{i=1}^n \rho_{1,i}(g)\alpha_i : \dots : \sum_{i=1}^n \rho_{n,i}(g)\alpha_i \right).$$

The standard principal open subset $\{(\alpha_0 : \alpha_1 : \dots : \alpha_n) \mid \alpha_0 \neq 0\}$ of $\mathbb{P}(\tilde{L})$ is G -stable and is equivariantly isomorphic to the G -module V . Hence, by Lemma B.3.3, solving Problem B.1.1 is equivalent to its solving for G, V, a, b replaced respectively by $\tilde{G}, L, \tilde{a}, \tilde{b}$. This reduces solving Problem B.1.1 to the case where both orbits $G \cdot a$ and $G \cdot b$ are nonzero and conical. Given this,

searching for an answer to Problem B.1.1, we may (and shall)
assume that $G \cdot a$ and $G \cdot b$ are nonzero conical orbits. (B.3.9)

Note also that by Lemma B.3.3 the problem analogous to Problem (B.1.1), but for an action on a projective space is reduced to Problem B.1.1 for an action on a linear space.

B.3.5 The input of the algorithm

We assume that the following data are known (cf. [28]):

- The degree of the variety $\rho(G)$,

$$d := \deg \rho(G). \quad (\text{B.3.10})$$

- The functions (see (B.3.2), (B.3.3), (B.3.5))

$$\iota^*(\rho_{p,q}) \in k[\mathbb{A}^{r,s}] = k[x_1, \dots, x_{r+s}, x_1^{-1}, \dots, x_r^{-1}], \quad 1 \leq p, q \leq n.$$

Example B.3.4 Consider the same situation as in Example B.3.2. Number (B.3.10) is given by formula (B.3.8). It follows from (B.3.7) that the functions $\rho_{p,q}$ in (B.3.3) are defined by the equality

$$(\alpha z_1 + \gamma z_2)^{h-j} (\beta z_1 + \delta z_2)^j = \sum_{i=0}^h \rho_{i+1,j+1}(g) z_1^{h-i} z_2^i, \quad g = \begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in G. \quad (\text{B.3.11})$$

Take ι to be the morphism

$$\begin{aligned} \iota: \mathbb{A}^{1,2} &\hookrightarrow \mathrm{SL}_2(k), \\ (\varepsilon_1, \varepsilon_2, \varepsilon_3) &\mapsto \begin{bmatrix} 1 & \varepsilon_2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \varepsilon_1 & 0 \\ 0 & \varepsilon_1^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ \varepsilon_3 & 1 \end{bmatrix} = \begin{bmatrix} \varepsilon_1^{-1} \varepsilon_2 \varepsilon_3 + \varepsilon_1 & \varepsilon_1^{-1} \varepsilon_2 \\ \varepsilon_1^{-1} \varepsilon_3 & \varepsilon_1^{-1} \end{bmatrix}. \end{aligned} \quad (\text{B.3.12})$$

Then it follows from (B.3.5), (B.3.11), (B.3.12) that the function $\iota^*(\rho_{i+1,j+1})$ is equal to the coefficient of $z_1^{h-i}z_2^j$ in the decomposition of the binary form

$$((x_1 + x_1^{-1}x_2x_3)z_1 + (x_1^{-1}x_3)z_2)^{h-j}((x_1^{-1}x_2)z_1 + (x_1^{-1})z_2)^j$$

in the variables z_1, z_2 with coefficients in the field $k(x_1, x_2, x_3)$ as a sum of monomials in z_1, z_2 . For instance, if $h = 2$, then $\iota^*(\rho_{2,2}) = 1 + 2x_1^{-2}x_2x_3$.

B.3.6 The algorithm

We utilize the notation and conventions introduced above and exclude the trivial case $\overline{G \cdot b} = V$, i.e., assume that

$$\dim G \cdot b < \dim V \quad (\text{B.3.13})$$

(as the number $\dim G \cdot b$ is equal to the rank of the system of vectors $\{d\rho(Y_i) \cdot b\}_{i \in I}$ where $\{Y_i\}_{i \in I}$ is a basis of the vector space $\text{Lie}(G)$, condition (B.3.13) can be verified constructively if the operators $d\rho(Y_i)$ are known).

The following sequence of steps together with Theorem B.3.5 formulated below provide a constructive method for solving Problem (*):

1. Find the coordinates of the vectors a and b in the basis e_1, \dots, e_n :

$$a = \alpha_1 e_1 + \dots + \alpha_n e_n, \quad b = \beta_1 e_1 + \dots + \beta_n e_n,$$

and, changing the basis e_1, \dots, e_n if necessary, achieve that the following condition holds:

$$\beta_1 \cdots \beta_n \neq 0.$$

2. Consider n “generic” polynomials F_1, \dots, F_n of degree $2d - 2$ (where d is defined by formula (B.3.10)) in the variables y_1, \dots, y_n ,

$$F_p := \sum_{\substack{q_1, \dots, q_n \in \mathbb{N} \\ q_1 + \dots + q_n \leq 2d-2}} c_{p,q_1, \dots, q_n} y_1^{q_1} \cdots y_n^{q_n}, \quad p = 1, \dots, n, \quad (\text{B.3.14})$$

i.e., such that, apart from y_1, \dots, y_n , all the coefficients c_{p,q_1, \dots, q_n} are the indeterminates over k as well, and put

$$H(y_1, \dots, y_n) := (y_1 - \alpha_1)F_1 + \dots + (y_n - \alpha_n)F_n - 1. \quad (\text{B.3.15})$$

3. Replacing every variable y_i in $H(y_1, \dots, y_n)$ by $\sum_{j=1}^n \beta_j \iota^*(\rho_{i,j})$, obtain a linear combination of monomials of the form (B.3.6) with coefficients in the ring $k[\dots, c_{p,q_1, \dots, q_n}, \dots]$ of polynomials in variables c_{p,q_1, \dots, q_n} over the field k :

$$\begin{aligned} H\left(\sum_{j=1}^n \beta_j \iota^*(\rho_{1,j}), \dots, \sum_{j=1}^n \beta_j \iota^*(\rho_{n,j})\right) \\ = \sum_{(i_1, \dots, i_{r+s}) \in M} \ell_{i_1, \dots, i_{r+s}} x_1^{i_1} \cdots x_{r+s}^{i_{r+s}}, \end{aligned} \quad (\text{B.3.16})$$

where $\ell_{i_1, \dots, i_{r+s}} \in k[\dots, c_{p,q_1, \dots, q_n}, \dots]$ and M is a finite subset in $\mathbb{Z}^r \times \mathbb{N}^s$. By (B.3.14) and (B.3.15), every coefficient $\ell_{i_1, \dots, i_{r+s}}$ in (B.3.16) is a *linear* function in the variables c_{p,q_1, \dots, q_n} with coefficients in the field k .

4. Consider the following finite system of *linear* equations in the variables c_{p,q_1, \dots, q_n} with coefficients in the field k :

$$\ell_{i_1, \dots, i_{r+s}} = 0, \quad \text{where } (i_1, \dots, i_{r+s}) \in M. \quad (\text{B.3.17})$$

Theorem B.3.5 *Let $G \cdot b$ be a nonzero conical orbit (see (B.3.9)). The following properties are equivalent:*

- (i) *the closure of the orbit $G \cdot b$ in V contains the orbit $G \cdot a$;*
- (ii) *system of linear equations (B.3.17) is inconsistent.*

Proof See [1]. □

Remark B.3.6 The proof shows that the claim of Theorem B.3.5 remains true if the constant d in the definition of the “generic” polynomials F_1, \dots, F_n is replaced by $\deg \overline{G \cdot b} = \deg G \cdot b$. If, for some reasons, the number $\deg G \cdot b$ is known, this permits one to decrease the number of variables and equations in system of linear equations (B.3.17). In some cases the degrees of orbits indeed have been computed.

Example B.3.7 Consider the same situation as in Examples B.3.2 and B.3.4. Take a nonzero binary form $v \in V_h$ and decompose it as a product $v = v_1^{n_1} \cdots v_p^{n_p}$, where v_1, \dots, v_p are pairwise nonproportional forms from V_1 . Assume that $p \geq 3$ and $s/n_i \geq 2$ for every i . Then the G -stabilizer G_v of the form v is finite [29] and $|G_v| \deg G \cdot v = -2(p-1)h^3 - 4 \sum_{i=1}^p (h-n_i)^3 + 3h^2 \sum_{i=1}^p (h-n_i) + 3h \sum_{i=1}^p (h-n_i)(h-2n_i)$ (see the proof in [30, Sect. 8]). In particular, if all the roots of the form v are simple, i.e., $p = h$, $n_1 = \dots = n_h = 1$, then

$$|G_v| \deg(G \cdot v) = 2h(h-1)(h-2). \quad (\text{B.3.18})$$

Formula (B.3.18) can also be deduced from a calculation of 1897 by Enriques and Fano; this has been done in 1983 by Mukai and Umemura (with a gap fixed in [30, Sect. 8, Remark] where one can find the relevant references).

B.4 Defining the Set $\overline{G \cdot L}$ by Equations

B.4.1 In this section we suggest another algorithm for solving Problem B.1.1. It is less effective than the algorithm from Sect. B.3, but it provides more information and concerns a more general problem.

To wit, let L be a linear subvariety of V and let $G \cdot L = \bigcup_{v \in L} G \cdot v$. We show how one can constructively find a finite system of polynomial functions q_1, \dots, q_m on V such that

$$\overline{G \cdot L} = \{x \in V \mid q_1(x) = \dots = q_m(x) = 0\}. \quad (\text{B.4.1})$$

For $L = b$ this provides the following constructive solution to Problem B.1.1:

$$G \cdot a \subseteq \overline{G \cdot b} \iff q_1(a) = \dots = q_m(a) = 0.$$

Note that varieties of the form $\overline{G \cdot L}$ are ubiquitous in algebraic transformation group theory: apart from orbit closures, to them also belong irreducible components of Hilbert null-cones and, more generally, closures of Hesselink strata [31] (see also below Appendix C), closures of sheets [4], and closures of Jordan (also known as decomposition) classes [32]. Also note that if a system of polynomials q_1, \dots, q_m satisfying (B.4.1) is given, modern commutative algebra provides algorithms to constructively find a system of generators of the ideal of all polynomials vanishing on $\overline{G \cdot L}$, see, e.g., [33, Chap. 4, §2]. In particular, this provides methods for constructively finding generators of the ideal of polynomials vanishing on the closure of an orbit. In some special cases (for instance, for nilpotent orbits of the adjoint action of the group $\mathrm{SL}_n(k)$ and for “rank varieties”) such generators have been found, see [34].

B.4.2 Fix a morphism

$$\tau: \mathbb{A}^l \rightarrow V,$$

whose image is dense in L : for instance, one can take τ to be an affine embedding of \mathbb{A}^l into V whose image is L . In addition, as in Sect. B.3.2, we assume that a dominant morphism (B.3.2) is fixed.

We maintain the notation from Sect. B.3.2. We denote by z_1, \dots, z_n the basis of V^* dual to e_1, \dots, e_n . In addition, we denote by y_1, \dots, y_l the standard coordinate functions on \mathbb{A}^l :

$$y_i(a) = \delta_i \quad \text{for } a = (\delta_1, \dots, \delta_l) \in \mathbb{A}^l.$$

Then

$$\tau(v) = \sum_{i=1}^n \tau^*(z_i)(v) e_i \quad \text{for every } v \in \mathbb{A}^l. \quad (\text{B.4.2})$$

B.4.3 The functions $x_1, \dots, x_{r+s}, y_1, \dots, y_l$ can be naturally extended to the functions on $\mathbb{A}^{r,s} \times \mathbb{A}^l$; we denote these extensions by the same letters. Consider the morphism

$$\not\preceq: A^{r,s} \times \mathbb{A}^l \rightarrow V, \quad \mu(u, v) = \iota(u) \cdot \tau(v) \quad (\text{B.4.3})$$

Then (B.3.4) and (B.4.2) imply that

$$f_p := \mu^*(z_p) = \sum_{q=1}^n \iota^*(\rho_{pq}) \tau^*(z_q), \quad 1 \leq p, q \leq n. \quad (\text{B.4.4})$$

We identify $\mathbb{A}^{r,s} \times \mathbb{A}^l$ with the open subset of \mathbb{A}^{r+s+l} by means of the embedding

$$\mathbb{A}^{r,s} \times \mathbb{A}^l \hookrightarrow \mathbb{A}^{r+s+l}, \quad ((\varepsilon_1, \dots, \varepsilon_{r+s}), (\delta_1, \dots, \delta_l)) \mapsto (\varepsilon_1, \dots, \varepsilon_{r+s}, \delta_1, \dots, \delta_l),$$

then $x_1, \dots, x_{r+s}, y_1, \dots, y_l$ become the standard coordinate functions on \mathbb{A}^{r+s+l} . We also identify V with \mathbb{A}^n by means of the isomorphism

$$V \rightarrow \mathbb{A}^n, \quad \sum_{i=1}^n \gamma_i e_i \mapsto (\gamma_1, \dots, \gamma_n).$$

Then morphism (B.4.3) becomes the rational map ϱ of the affine space \mathbb{A}^{r+s+l} to the affine space \mathbb{A}^n :

$$\varrho: \mathbb{A}^{r+s+l} \dashrightarrow \mathbb{A}^n, \quad a \mapsto (f_1(a), \dots, f_n(a)).$$

As $\overline{\iota(\mathbb{A}^{r,s}) \cdot L} = \overline{G \cdot L}$, we have the equality

$$\overline{\varrho(\mathbb{A}^{r+s+l})} = \overline{G \cdot L}. \quad (\text{B.4.5})$$

This makes it possible to apply elimination theory to finding the equations that cut out $\overline{G \cdot L}$ in V . An algorithmic solution to this problem is obtained by means of Gröbner bases as follows.

B.4.4 The input of the algorithm

We assume that the following data are known:

— The functions

$$\iota^*(\rho_{p,q}) \in k[x_1, \dots, x_{r+s}, x_1^{-1}, \dots, x_r^{-1}] \subset k(\mathbb{A}^{r+s+l}), \quad 1 \leq p, q \leq n. \quad (\text{B.4.6})$$

— The functions

$$\tau^*(z_i) \in k[y_1, \dots, y_l] \subset k(\mathbb{A}^{r+s+l}), \quad 1 \leq i \leq n. \quad (\text{B.4.7})$$

Example B.4.1 Fix a point $v \in L$ and a sequence f_1, \dots, f_m of linear independent vectors defining a parametric presentation $L = \{v + \sum_{i=1}^m \lambda_i f_i \mid \lambda_d, \dots, \lambda_m \in k\}$. Take τ to be the embedding $\tau: \mathbb{A}^m \hookrightarrow \mathbb{A}^n$, $\tau(\lambda_1, \dots, \lambda_m) = v + \sum_{i=m}^l \lambda_i f_i$. Let $v = \sum_{j=1}^n \gamma_j e_j$ and $f_i = \sum_{j=1}^n v_{ji} e_j$. Then

$$\tau^*(z_i) = \sum_{i=1}^n v_{ij} y_j + \gamma_i, \quad 1 \leq i \leq n.$$

See Example B.3.4 regarding the functions $\iota^*(\rho_{p,q})$.

B.4.5 The algorithm

The following sequence of steps, together with Theorem B.4.2 provide a constructive method to obtain the equations defining $\overline{G \cdot L}$ in V :

- (1) Compute the rational functions f_p using formula (B.4.4) and write down each of them as a fraction of polynomials:

$$f_p = \frac{g_p}{h_p}, \quad g_p \in k[x_1, \dots, x_{r+s}, y_1, \dots, y_t], \quad h_p \in k[x_1, \dots, x_r]$$

(see (B.4.6) and (B.4.7)).

- (2) Consider the polynomial ring $k[t, x_1, \dots, x_{r+s}, y_1, \dots, y_t, z_1, \dots, z_n]$, where t is a new variable, and find for its ideal generated by the polynomials

$$h_1 z_1 - g_1, \dots, h_n z_n - g_n, 1 - h_1 \cdots h_n t.$$

a Gröbner basis with respect to an order of monomials such that every variable t , x_i , and y_j is greater than every variable z_p .

Theorem B.4.2 *Let q_1, \dots, q_m be all the elements of this Gröbner basis that lie in $k[z_1, \dots, z_n]$. Then*

$$\overline{G \cdot L} = \{v \in \mathbb{A}^n \mid q_1(v) = \dots = q_m(v) = 0\}.$$

Proof We have $\overline{\varrho(\mathbb{A}^{r+s+l})} = \{v \in \mathbb{A}^n \mid q_1(v) = \dots = q_m(v) = 0\}$; this is a general fact about the closure of the image of every rational map of one affine space to another, see, e.g., [33, Chap. 3, § 3, Thm. 2]. Now the claim that we wish to prove follows from equality (B.4.5). \square

Remark B.4.3 Although the elements q_1, \dots, q_m , interesting for us, constitute a part of the Gröbner basis, for finding them by means of the described algorithm, we should find the whole this basis.

References

1. V. L. Popov, *Two orbits: When is one in the closure of the other?*, Proc. Steklov Inst. Math. **264** (2009), 146–158, arXiv:0808.2735.
2. W. de Graaf, *Orbit closures of linear algebraic groups*, in: *Computer Algebra and Polynomials*, Lecture Notes in Computer Science, Vol. 8942, 2015, pp. Springer, 76–93.
3. A. Borel, *Linear Algebraic Groups*, 2nd ed., Springer-Verlag, New York, 1991.
4. V. L. Popov, E. B. Vinberg, *Invariant Theory*, in: *Algebraic Geometry IV*, Enc. Math. Sci., Vol. 55, Springer, Berlin, 1994, pp. 123–284.
5. D. Mumford, *Geometric Invariant Theory*, Ergeb. Math., Bd. 34, Springer-Verlag, Berlin, 1965.
6. M. Rosenlicht, *On quotient varieties and the affine embedding of certain homogeneous spaces*, Trans. Amer. Math. Soc. **101** (1961), 211–223.
7. D. H. Collingwood, W. M. McGovern, *Nilpotent Orbits in Semisimple Lie Algebras*, Van Nostrand Reinhold, New York, 1993.
8. N. Spaltenstein, *Classes Unipotentes et Sous-Groupes de Borel*, Lecture Notes in Mathematics, Vol. 946, Springer-Verlag, New York, 1982.
9. R. Carter, *Finite Groups of Lie Type: Conjugacy Classes and Complex Characters*, John Wiley & Sons, London, 1985.
10. W. A. de Graaf, E. B. Vinberg, O. S. Yakimova, *An effective method to compute closure ordering for nilpotent orbits of θ -representations*, J. Algebra **371** (2012), 38–62.
11. V. V. Kashin, *Orbits of adjoint and coadjoint actions of Borel subgroups of semisimple algebraic groups*, in: *Problems in Group Theory and Homological Algebra*, Yaroslavl', 1990, pp. 141–159 (Russian).
12. D. D. Pervouchine, *Hierarchy of closures of matrix pencils*, J. Lie Theory **14** (2004), 443–479.
13. T. Brustle, L. Hille, G. Röhrle, G. Zwara, *The Bruhat–Chevalley order of parabolic group actions in general linear groups and degeneration for Δ -filtered modules*, Adv. in Math. **148** (1999), no. 2, 203–242.
14. S. Goodwin, L. Hille, G. Röhrle, *Orbits of parabolic subgroups on metabelian ideals*, 2007, arXiv:0711.3711.
15. P. Magyar, J. Weyman, A. Zelevinsky, *Multiple flag varieties of finite type*, Adv. Math. **141** (1999), no. 1, 97–118.
16. D. Burde, *Degenerations of 7-dimensional nilpotent Lie algebras*, Commun. Algebra **33** (2005), no. 4, 1259–1277.
17. D. Burde, C. Steinhoff, *Classification of orbit closures of 4-dimensional complex Lie algebras*, J. Algebra **214** (1999), 729–739.
18. C. Seeley, *Degenerations of 6-dimensional nilpotent Lie algebras over \mathbb{C}* , Comm. in Algebra **18** (1990), 3493–3505.
19. A. L. Onishchik, E. B. Vinberg, V. V. Gorbatsevich, *Structure of Lie groups and Lie algebras*, in: *Lie Groups and Lie Algebras III*, Encyclopaedia of Mathematical Sciences, Vol. 41, Springer-Verlag, Berlin, 1994, pp. 1–248.
20. K. Bongartz, *Degenerations for representations of tame quivers*, Ann. Sci. ÉNS **28** (1995), no. 5, 647–668.
21. K. Mulmuley, M. Sohoni, *Geometric complexity theory I: An approach to the P vs. NP and related problems*, SIAM J. Comput. **31** (2001), no. 2, 496–526.
22. P. Bürgisser, J. Landsberg, L. Manivel, J. Weyman, *An overview of mathematical issues arising in the geometric complexity theory approach to $VP \neq VNP$* , SIAM J. Comput. **40** (2011), no. 4, 1179–1209.
23. L. M. Landsberg, *Geometric complexity theory: an introduction for geometers*, Ann. Univ. Ferrara Sez. VII Sci. Mat. **61** (2015), no. 1, 65–117.
24. H. Matsumura, P. Monsky, *On the automorphisms of hypersurfaces*, J. Math. Kyoto Univ. **3** (1964), 347–361.

25. A. Grothendieck, *Torsion homologique et sections rationnelles*, in: *Anneaux de Chow et Applications*, Séminaire C. Chevalley ENS 1958, Sec. math. 11 rue Pierre Cirue, Paris, 1958, pp. 5-10–5-29.
26. M. Rosenlicht, *Some basic theorems on algebraic groups*, Amer. J. Math. **78** (1956), 401–443.
27. D. Mumford, *Algebraic Geometry I. Complex Projective Varieties*, Grundlehren der mathematischen Wissenschaften, Vol. 221, Springer-Verlag, Berlin, 1976.
28. V. L. Popov, *Constructive invariant theory*, Astérisque **87–88** (1981), 303–334.
29. V. L. Popov, *Structure of the closure of orbits in spaces of finite-dimensional linear $\mathrm{SL}(2)$ representations*, Math. Notes 16 (1974), 1159–1162.
30. L. Moser-Jauslin, *The Chow rings of smooth complete SL_2 -embeddings*, Compositio Math. **82** (1992), 67–106.
31. V. L. Popov, *The cone of Hilbert nullforms*, Proc. Steklov Inst. of Math. **241** (2003), 177–194.
32. P. Tauvel, R. W. T. Yu, *Lie Algebras and Algebraic Groups*, Springer Monographs in Mathematics, Springer, Berlin, 2005.
33. D. Cox, J. Little, D. O’Shea, *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*, 2nd ed., Undergraduate Texts in Mathematics, Springer, New York, 1998.
34. J. Weyman, *The equations of conjugacy classes of nilpotent matrices*, Invent. Math. **98** (1989), 229–245.

Appendix C

Stratification of the Nullcone

Vladimir L. Popov

C.1 Introduction

C.1.1 Let G be a connected reductive algebraic group and let V be a nonzero finite dimensional algebraic G -module, all are taken over an algebraically closed ground field k of characteristic zero.

A vector $v \in V$ is called a *Hilbert nullform* (cf. [1]; other terms are *unstable* vector [2], *nilpotent* vector [3]), if any G -invariant polynomial function on V that vanishes at 0 also vanishes at v . Therefore, the set of all Hilbert nullforms is the nullcone $\mathcal{N}_{G,V}$ in V (see Definition 2.5.1). Hilbert was the first who found that the nullcones play a fundamental role in the theory of invariants and its applications, see [4]. In the general case, the nullcone has a complicated structure; it may be nonreduced, reducible, nonequidimensional, and may have complicated singularities.

C.1.2 According to the Hilbert–Mumford criterion (see Theorem 2.5.3), a vector $v \in V$ is a nullform if and only if there is a one-parameter subgroup $\lambda : k^* \rightarrow G$ that steers v to 0 (i.e., such that $\lim_{t \rightarrow 0} \lambda(t) \cdot v = 0$). In 1978, when solving

Steklov Mathematical Institute, Russian Academy of Sciences, Gubkina 8, Moscow 119991, Russia. National Research University Higher School of Economics, Myasnitskaya 20, Moscow 101000, Russia. *E-mail address:* popovvl@mi.ras.ru

Supported by the program *Contemporary Problems of Theoretical Mathematics* of the Russian Academy of Sciences, Branch of Mathematics.

different problems, several authors simultaneously revealed the key role of those λ that do it “most optimally”, see [1, 5–8] (however, for $V = \text{Lie}(G)$, where the nullcone coincides with the cone of nilpotent elements, this fact was revealed in a different form already in [9]: indeed, it was found out later (see [1, 7, 10]) that the “characteristics” of nilpotent elements introduced in [9] can be equivalently defined in terms of the optimality property). The formalization of this property is performed by introducing an $\text{Ad}(G)$ -invariant norm on the set of all one-parameter subgroups: optimal subgroups are those that have the minimal norm. Technically, it is more convenient to consider a wider class of virtual one-parameter subgroups [1, 7], which is actually the set of rational semisimple elements in $\text{Lie}(G)$. The norm is defined by the choice of an $\text{Ad}(G)$ -invariant inner product on $\text{Lie}(G)$ that is rational-valued and positive definite on the \mathbb{Q} -vector space of rational elements of the Lie algebra of a certain (and thereby any) maximal torus in G . If $\Lambda(v)$ is a family of all optimal virtual one-parameter subgroups corresponding to a nullform v , then, following [1], we can consider the following equivalence relations on the set of all nullforms:

$$x \sim y \iff \Lambda(g \cdot x) = \Lambda(y) \text{ for a certain } g \in G.$$

C.1.3 The equivalence classes form a finite partition of $\mathcal{N}_{G,V}$ and are called *strata*. They coincide with the sets $\mathcal{H}[l]$ described below in Sect. C.2.6. Note that, in general, the strata depend on the choice of the norm. It is remarkable that, although $\mathcal{N}_{G,V}$ itself has a complicated structure, the structure of the strata turns out to be simple: Hesselink [1] proved that each stratum S is an irreducible subvariety of $\mathcal{N}_{G,V}$, open in its closure \bar{S} , and there exists an isomorphism φ of the stratum S onto an invariant open subset of a homogeneous vector bundle E over G/P , where P is a parabolic subgroup in G (all these objects depend on S); in particular, S is a smooth rational variety. Moreover, there exists a morphism $\pi : E \rightarrow \bar{S}$, which is a resolution of singularities of the variety \bar{S} and is such that $\pi|_{\pi^{-1}(S)} = \varphi^{-1}$. In particular, this gives a resolution of singularities for each irreducible component of $\mathcal{N}_{G,V}$ and shows that, using Kempf’s terminology, [6], the latter is obtained by collapsing of a homogeneous vector bundle over a generalized flag variety of the group G . In particular, for the adjoint G -module $V = \text{Lie}(G)$, this yields the celebrated resolution of singularities of the cone of nilpotent elements of $\text{Lie}(G)$.

Note that, in general, the closure of a stratum is not a union of strata.

C.1.4 In this appendix we describe a geometric-combinatorial algorithm, suggested in [11], that allows one, using solely the system of weights of V and roots of G , to constructively find the strata of $\mathcal{N}_{G,V}$ and calculate their dimensions. In particular, it provides a constructive approach to calculating $\dim \mathcal{N}_{G,V}$ and determining all irreducible components of $\mathcal{N}_{G,V}$ of maximal dimension. Note that calculating $\dim \mathcal{N}_{G,V}$ is a nontrivial problem. For example (see below Subsection 4.8 and [3, §8]), the problem of classifying equidimensional representations and that of classifying representations with a free module of covariants (see [12–15]) are

reduced to it; their solutions are actually based on developing various ad hoc methods for estimating $\dim \mathcal{N}_{G,V}$.

In the case of the adjoint G -module $V = \text{Lie}(G)$ (and, more generally, V determined by a so-called θ -representation, see below Sect. C.4.7), the algorithm turns into the classification algorithm for the conjugacy classes of nilpotent elements in a semisimple Lie algebra (respectively, homogeneous nilpotent elements in a cyclically graded semisimple Lie algebra). These classifications were obtained in [9] (respectively, [16–18]) by a different method based on the use of specific properties of these G -modules.

C.1.5 For semisimple G , the algorithm is implemented in `pari-gp` and `LiE` framework by N. A'Campo and the author [19]. This computer algebra package, named **HNC**, yields the constructive description of all strata, calculates their dimensions, and describes all irreducible components of $\mathcal{N}_{G,V}$ of maximal dimension. The source code `hnc.gp` of **HNC** (its electronic version is available at <http://www.geometrie.ch/>) is contained in Addendum.

C.2 The Stratification

C.2.1 First, we shall introduce some notation and conventions.

- Given a subset X of V , we denote the set $\{g \cdot x \mid g \in G, x \in X\}$ by $G \cdot X$.
- If H is an algebraic subgroup of G , and F an algebraic variety endowed with a regular action of H , we denote by $G \times^H F$ the homogeneous fiber space over G/H with the fiber F . Under broad assumptions, $G \times^H F$ is an algebraic variety and the natural projection $G \times^H F \rightarrow G/H$ is a morphism (e.g., this is so if F is quasiprojective); see [3, 4.8]. By $[g, x]$ we denote the image of the point $g \times x$ under the natural map $G \times F \rightarrow G \times^H F$.
- Let T be an algebraic torus. The group $X(T)$ of its rational characters (i.e., homomorphisms $T \rightarrow k^*$ of algebraic groups) is a free abelian group of rank $\dim T$. We consider it in additive notation and denote by t^μ the value of the character $\mu \in X(T)$ at point $t \in T$. We put

$$X(T)_\mathbb{Q} := X(T) \otimes_{\mathbb{Z}} \mathbb{Q};$$

it is a vector space over \mathbb{Q} containing the lattice $X(T)$.

Let $\mathfrak{t} := \text{Lie}(T)$. Taking the differential at the identity element e , we obtain the group embedding $X(T) \hookrightarrow \mathfrak{t}^*$, $\mu \mapsto d_e \mu$, which naturally extends to the embedding $X(T)_\mathbb{Q} \hookrightarrow \mathfrak{t}^*$. We identify $X(T)_\mathbb{Q}$ with its image; thus $X(T)_\mathbb{Q}$ becomes a \mathbb{Q} -form of the vector space \mathfrak{t}^* over k . Then

$$\mathfrak{t}_\mathbb{Q} := \{x \in \mathfrak{t} \mid l(x) \in \mathbb{Q} \text{ for every } l \in X(T)_\mathbb{Q}\}$$

is a \mathbb{Q} -form of \mathfrak{t} , and $X(T)_\mathbb{Q}$ is its dual.

For any character $\mu \in X(T)$ and algebraic T -module L we set

$$L_\mu := \{l \in L \mid t \cdot l = t^\mu l \text{ for every } t \in T\}$$

and denote by $\Delta(L, T)$ the system of weights of T in L ,

$$\Delta(L, T) := \{\mu \in X(T) \mid L_\mu \neq 0\}.$$

Then, $L = \bigoplus_{\mu \in \Delta(L, T)} L_\mu$. The *multiplicity of the weight* μ in the T -module L is the number $\dim_k L_\mu$.

C.2.2 Now let T be a maximal torus in G . The natural action of the Weyl group $W_{G,T}$ of T on \mathfrak{t} and \mathfrak{t}^* stabilizes $\mathfrak{t}_\mathbb{Q}$, $X(T)_\mathbb{Q}$, and $X(T)$.

There is an $\mathrm{Ad}(G)$ -invariant inner product $(\ , \)$ on $\mathfrak{g} := \mathrm{Lie}(G)$ whose restriction to $\mathfrak{t}_\mathbb{Q}$ is rational-valued and positive definite (see, e.g., [3, 5.5]). It yields the $W_{G,T}$ -equivariant isomorphism $\iota: \mathfrak{t}^* \rightarrow \mathfrak{t}$ defined by the condition $(\iota(l), x) = l(x)$ for all $l \in \mathfrak{t}^*$, $x \in \mathfrak{t}$. We have $\iota(X(T)_\mathbb{Q}) = \mathfrak{t}_\mathbb{Q}$. Let $\langle \ , \ \rangle$ be the inner product on \mathfrak{t}^* uniquely defined by the condition $\langle l_1, l_2 \rangle = (\iota(l_1), \iota(l_2))$ for all $l_1, l_2 \in \mathfrak{t}^*$. It is $W_{G,T}$ -invariant and its restriction to $X(T)_\mathbb{Q}$ is rational-valued and positive definite.

In what follows, we assume that the strata of $\mathcal{N}_{G,V}$ are defined by the norm determined by $(\ , \)$.

C.2.3 We have the following decomposition:

$$V = \bigoplus_{\mu \in \Delta(V, T)} V_\mu. \quad (\text{C.2.1})$$

Since maximal tori are conjugate and their union is dense in G , the action of G on V is trivial if and only if $\Delta(V, T) = \{0\}$.

For the adjoint G -module $\mathfrak{g} := \mathrm{Lie} G$, we have $\Delta(\mathfrak{g}, T) = \Phi(\mathfrak{g}, T) \sqcup \{0\}$, where $\Phi(\mathfrak{g}, T)$ is the system of roots of \mathfrak{g} with respect to T . We have $\mathfrak{g}_0 = \mathfrak{t}$, $\dim \mathfrak{g}_\alpha = 1$ for every $\alpha \in \Phi(\mathfrak{g}, T)$, and

$$\mathfrak{g} = \mathfrak{t} \oplus \bigoplus_{\alpha \in \Phi(\mathfrak{g}, T)} \mathfrak{g}_\alpha. \quad (\text{C.2.2})$$

C.2.4 Take a nonzero element $l \in X(T)_\mathbb{Q}$. For any number $\gamma \in \mathbb{Q}$ we set

$$\{l = \gamma\} := \{t \in X(T)_\mathbb{Q} \mid \langle l, t \rangle = \gamma\};$$

$\{l \geq \gamma\}$, etc. are defined similarly.

We denote

$$\mathfrak{t}[l] := \{t \in \mathfrak{t} \mid l(t) = 0\}, \quad \mathfrak{g}[l] := \mathfrak{t}[l] \oplus \bigoplus_{\alpha \in \{l=0\}} \mathfrak{g}_\alpha, \quad \mathfrak{p}[l] := \mathfrak{t} \oplus \bigoplus_{\alpha \in \{l \geq 0\}} \mathfrak{g}_\alpha. \quad (\text{C.2.3})$$

Clearly $t[l]$ is a torus and $\mathfrak{p}[l]$ is a parabolic subalgebra of \mathfrak{g} . One can show that $\mathfrak{g}[l]$ is a reductive subalgebra of \mathfrak{g} and $t[l]$ is its maximal torus (see [3, 5.5]). Let $T[l]$, $G[l]$, and $P[l]$ be connected algebraic subgroups of G with the Lie algebras $t[l]$, $\mathfrak{g}[l]$, and $\mathfrak{p}[l]$, respectively. The group $G[l]$ is reductive, $T[l]$ is its maximal torus, $P[l]$ is a parabolic subgroup in G , and we have

$$\begin{aligned} X(T[l])_{\mathbb{Q}} &= \{f \in X(T)_{\mathbb{Q}} \mid \langle f, l \rangle = 0\}, \\ \Phi(\mathfrak{g}[l], T[l]) &= \Phi(\mathfrak{g}, T) \cap \{l = 0\}, \\ \mathfrak{g}[l]_{\alpha} &= \mathfrak{g}_{\alpha} \text{ for every } \alpha \in \Phi(\mathfrak{g}[l], T[l]). \end{aligned} \quad (\text{C.2.4})$$

The element l also determines the following linear subspaces in V :

$$V[l] := \bigoplus_{\mu \in \{l=1\}} V_{\mu}, \quad V[l^+] := \bigoplus_{\mu \in \{l>1\}} V_{\mu}, \quad (\text{C.2.5})$$

Relations (C.2.3) and (C.2.5) imply the $G[l]$ -invariance of $V[l]$ and the $P[l]$ -invariance of $V[l^+]$. Thus $V[l]$ is a $G[l]$ -module, and $V[l^+]$ is a $P[l]$ -module.

C.2.5 Consider the projection

$$V[l^+] \rightarrow V[l], \quad v \mapsto v',$$

parallel to $\bigoplus_{\mu \in \{l>1\}} V_{\mu}$, the nullcone $\mathcal{N}_{G[l], V[l]}$ of the $G[l]$ -module $V[l]$, and the open $P[l]$ -invariant subset

$$V[l^+]^0 := \{v \in V[l^+] \mid v' \notin \mathcal{N}_{G[l], V[l]}\} \quad (\text{C.2.6})$$

in $V[l^+]$. In general, $V[l^+]^0$ may be empty. By (C.2.6), its nonemptiness is equivalent to the inequality

$$\mathcal{N}_{G[l], V[l]} \neq V[l]. \quad (\text{C.2.7})$$

Definition A nonzero element $l \in X(T)_{\mathbb{Q}}$ is called a *stratifying* element if condition (C.2.7) holds.

The set of all stratifying elements of $X(T)_{\mathbb{Q}}$ is denoted by \mathcal{S} .

C.2.6 Let l be an element of \mathcal{S} . Then $V[l^+]^0 \neq \emptyset$. Consider the following morphism of the homogeneous fiber space over $G/P[l]$ with the fiber $V[l^+]^0$:

$$G \times^{P[l]} V[l^+]^0 \rightarrow V, \quad [g, v] \mapsto g \cdot v. \quad (\text{C.2.8})$$

Let $\mathcal{H}[l]$ be the image of morphism (C.2.8),

$$\mathcal{H}[l] := G \cdot V[l^+]^0. \quad (\text{C.2.9})$$

Theorem C.2.1 (stratification of the nullcone)

- (i) *The set \mathcal{S} is finite and $W_{G,T}$ -invariant.*
- (ii) *For every elements $l_1, l_2 \in \mathcal{S}$, the following are equivalent:*
 - (a) $\mathcal{H}[l_1] \cap \mathcal{H}[l_2] \neq \emptyset$;
 - (b) $\mathcal{H}[l_1] = \mathcal{H}[l_2]$;
 - (c) l_1 and l_2 lie in the same $W_{G,T}$ -orbit.
- (iii) *For every element $l \in \mathcal{S}$,*
 - (a) *morphism (C.2.8) isomorphically maps $G \times^{P[l]} V[l^+]^0$ onto $\mathcal{H}[l]$;*
 - (b) *$G \cdot V[l^+]$ is the closure of $\mathcal{H}[l]$;*
 - (c) *$\mathcal{H}[l]$ is open in $G \cdot V[l^+]$.*
- (iv) *If \mathcal{R} is a subset of \mathcal{S} intersecting every $W_{G,T}$ -orbit in \mathcal{S} at a single point, then*

$$\mathcal{N}_{G,V} \setminus \{0\} = \bigsqcup_{l \in \mathcal{R}} \mathcal{H}[l]. \quad (\text{C.2.10})$$

Proof See [3, Thm. 5.6] (see also [10, Prop. 1], [20, Proof of Thm. 9.2], [21, Rem. 12.21]). \square

C.2.7 Theorem C.2.1 implies that, for every irreducible component Z of the nullcone $\mathcal{N}_{G,V}$, there exists an element $l \in \mathcal{S}$ such that Z is the closure of $\mathcal{H}[l]$. Therefore, by Theorem C.2.1(iii),

$$G \times^{P[l]} V[l^+] \rightarrow Z, \quad [g, v] \mapsto g \cdot v,$$

is a resolution of singularities of Z .

C.2.8 Since $\dim G \times^{P[l]} V[l^+]^0 = \dim G/P[l] + \dim V[l^+]^0$, formulas (C.2.1), (C.2.2), (C.2.3), (C.2.5), (C.2.6), Theorem C.2.1(iii)(a), and the one-dimensionality of the root subspaces \mathfrak{g}_α imply the following corollary.

Corollary C.2.2 (formula for the dimension of a stratum)

$$\dim \mathcal{H}[l] = |\{l < 0\} \cap \Phi(\mathfrak{g}, T)| + \sum_{\mu \in \{l \geq 1\}} \dim V_\mu. \quad (\text{C.2.11})$$

In turn, since the strata are open in their closures and the number of strata is finite, we obtain the following corollary from (C.2.1) and (C.2.11).

Corollary C.2.3 (numerical criterion for the openness of a stratum in V) *The following properties of an $l \in \mathcal{S}$ are equivalent:*

- (a) $\mathcal{H}[l]$ is open in V ;
- (b) $\dim \mathcal{H}[l] = \dim V$,
- (c) $|\{l < 0\} \cap \Phi(\mathfrak{g}, T)| = \sum_{\mu \in \{l < 1\}} \dim V_\mu$.

An element l with these properties exists if and only if $\mathcal{N}_{G,V} = V$.

Finally, the inclusion $\mathcal{H}(l) \subseteq V$ yields the following corollary.

Corollary C.2.4 *For every element $l \in \mathcal{S}$,*

$$|\{l < 0\} \cap \Phi(\mathfrak{g}, T)| \leq \sum_{\mu \in \{l < 1\}} \dim V_\mu. \quad (\text{C.2.12})$$

C.2.9 In Sect. C.3 we will show that the subset \mathcal{S} of the Euclidean space $X(T)_\mathbb{Q}$ is completely determined only by the geometric configuration of the system of weights $\Delta(V, T)$ (endowed with their multiplicities) and the system of roots $\Phi(\mathfrak{g}, T)$, and obtain a simple geometric-combinatorial algorithm for constructively describing \mathcal{S} .

Namely, this algorithm allows one to describe constructively a set \mathcal{R} of representatives of all $W_{G,T}$ -orbits in \mathcal{S} . By Theorem C.2.1 this yields the decomposition (C.2.10) and the following description for the nullcone:

$$\mathcal{N}_{G,V} = \bigcup_{l \in \mathcal{R}} G \cdot V[l^+]. \quad (\text{C.2.13})$$

This description is constructive in the sense that our algorithm constructively describes all linear subspaces $V[l^+]$ from (C.2.13). Since the application of this algorithm to the $G[l]$ -module $V[l]$ for $l \in \mathcal{R}$ yields a constructive description, analogous to (C.2.13), of the nullcone $\mathcal{N}_{G[l],V[l]}$, we obtain from (C.2.6) a constructive description of every stratum $G \cdot V[l^+]^0$.

C.2.10 In view of Corollary C.2.2 to Theorem C.2.1, the constructive description of \mathcal{R} also yields the following constructive method for calculating $\dim \mathcal{N}_{G,V}$ by means of calculating the number of roots and weights (with multiplicities) in appropriate half-spaces of $X(T)_\mathbb{Q}$:

Proposition C.2.5

$$\dim \mathcal{N}_{G,V} = \max_{l \in \mathcal{R}} \left\{ |\{l < 0\} \cap \Phi(\mathfrak{g}, T)| + \sum_{\mu \in \{l \geq 1\}} \dim V_\mu \right\}.$$

In addition, Corollary C.2.2 to Theorem C.2.1 yields a constructive method for describing all irreducible components of maximal dimension of $\mathcal{N}_{G,V}$: they are exhausted, without repetition, by the varieties $G \cdot V[l^+]$, where $l \in \mathcal{R}$ is an element for which the sum $|\{l < 0\} \cap \Phi(\mathfrak{g}, T)| + \sum_{\mu \in \{l \geq 1\}} \dim V_\mu$ attains its maximum.

C.2.11 The following proposition can be used for constructive finding the representatives of strata.

Proposition C.2.6 *Consider a T -weight basis $\{v_i\}_{i \in I}$ in V and a set $\{X_\alpha \in \mathfrak{g}_\alpha \mid X_\alpha \neq 0, \alpha \in \Phi(\mathfrak{g}, T)\}$ such that, for any i and α , the coordinates of the vector $X_\alpha \cdot v_i$ in the basis $\{v_i\}_{i \in I}$ lie in \mathbb{Q} . Take an element $l \in \mathcal{S}$ and let $J := \{i \in I \mid v_i \in V[l]\}$.*

Then, for any family of constants $\{c_j \in k \mid j \in J\}$ that are algebraically independent over \mathbb{Q} ,

$$\sum_{j \in J} c_j v_j \in \mathcal{H}[l].$$

Proof See [11, Prop. 2]. \square

Note that the basis and the set mentioned in Proposition C.2.6 always exist because there exists a \mathbb{Z} -form of \mathfrak{g} defined by the Chevalley basis and an admissible \mathbb{Z} -form of V (see, e.g., [22]). For the adjoint representation, these basis and set are given by the \mathbb{Z} -form of \mathfrak{g} .

C.2.12 In some important cases, it is a priori known that every $\mathcal{H}(l)$ is a G -orbit. For example, this is so for the adjoint G -module $V = \mathfrak{g}$ and, more generally, for every G -module determined by a θ -representation (see Sect. C.4.7 below). In these cases, our algorithm turns into the classification algorithm for G -orbits in $\mathcal{N}_{G,V}$ and Proposition C.2.6 yields the representatives of these orbits (see below Example C.4.6).

C.2.13 If the number of G -orbits in $\mathcal{N}_{G,V}$ is finite, then the strata do not necessarily coincide with G -orbits (see below Example C.4.4). It would be interesting to find out whether it is always possible turn strata into orbits in such cases by changing the inner product $\langle \cdot, \cdot \rangle$. If this is so, then our algorithm yields a classification algorithm for the nullforms of the so-called *visible* G -modules (see [3, 8.1], [23, 24]).

C.3 The Algorithm

First, we present some notation concerning geometry.

C.3.1 Let E be a finite-dimensional linear Euclidean space over \mathbb{Q} and let M be its nonempty subset. We use the following notation (Fig. C.1):

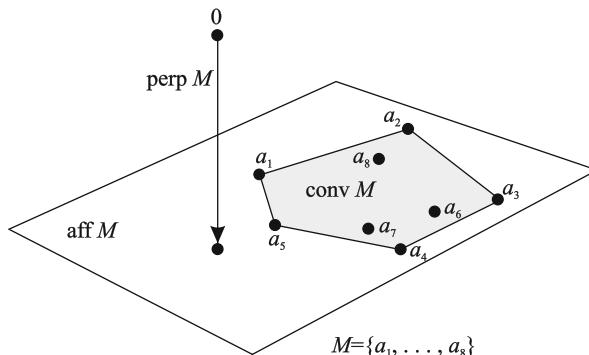


Fig. C.1 $\text{aff } M$, $\text{conv } M$, and $\text{perp } M$

- $\text{aff } M$ is the affine hull of M in E (i.e., the minimal linear variety in E that contains M);
- $\text{conv } M$ is the convex hull of M in E ,
- $\text{perp } M$ is the perpendicular dropped from zero onto $\text{aff } M$ (i.e., the unique vector from E that is orthogonal to the difference of any two vectors from $\text{aff } M$).

C.3.2 Passing to the construction of the algorithm, consider a nonzero element $l \in X(T)_{\mathbb{Q}}$. Suppose that the set of weights

$$\Delta(V, T)[l] := \Delta(V, T) \cap \{l = 1\} \quad (\text{C.3.1})$$

is nonempty. By (C.2.5), this is equivalent to the condition $V[l] \neq \{0\}$.

Consider the orthogonal projection

$$\text{pr}_l : X(T)_{\mathbb{Q}} \rightarrow X(T[l])_{\mathbb{Q}}.$$

By (C.2.4) and (C.2.5), the system of weights $\Delta(V[l], T[l])$ of $T[l]$ in $V[l]$ has the form

$$\Delta(V[l], T[l]) = \text{pr}_l(\Delta(V, T)[l]) \quad (\text{C.3.2})$$

and (C.3.2) holds with the mutiplicities of the weights taken into account if we assume that the latter are preserved under pr_l .

Proposition C.3.1 *Let $M := \Delta(V, T)[l]$. If $l \in \mathcal{S}$, then (see Fig. C.2)*

$$\text{perp } M \in \text{conv } M, \quad (\text{C.3.3})$$

$$\text{perp } M = \text{perp } \{l = 1\}. \quad (\text{C.3.4})$$

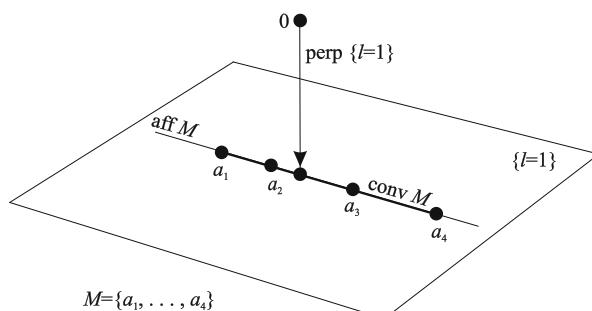


Fig. C.2 $\text{perp } M \in \text{conv } M$ and $\text{perp } M = \text{perp } \{l = 1\}$

Proof If $l \in \mathcal{S}$, then

$$0 \in \text{conv} \text{pr}_l M. \quad (\text{C.3.5})$$

Indeed, if (C.3.5) did not hold, then, by (C.3.2), each $T[l]$ -orbit in $V[l]$ would contain zero in its closure (see, for example, [3, 5.4]), and, hence, $\mathcal{N}_{G[l], V[l]} = V[l]$ in spite of the fact that $l \in \mathcal{S}$.

Since pr_l commutes with taking convex hull and the only vector of $\{l = 1\}$ that is mapped by pr_l to zero is $\text{perp} \{l = 1\}$, inclusion (C.3.5) is equivalent to the inclusion

$$\text{perp} \{l = 1\} \in \text{conv} M. \quad (\text{C.3.6})$$

Since $\text{aff } M \subseteq \{l = 1\}$, the vector $\text{perp} \{l = 1\}$ is orthogonal to the difference of any two vectors from $\text{aff } M$. By the inclusion $\text{conv} M \subset \text{aff } M$ and the uniqueness of the perpendicular dropped from zero onto a linear variety, (C.3.6) implies (C.3.4). In turn, (C.3.4) and (C.3.6) imply (C.3.3). \square

C.3.3 We now introduce certain finite subsets in $X(T)_{\mathbb{Q}}$ determined by the G -module V . Namely, consider the orbits of $W_{G,T}$ under its natural action on the set of all nonempty subsets of the system of weights $\Delta(V, T)$ and fix a representative in each such orbit. Among these representatives, we choose those representatives M , that share the following properties:

- (i) $\text{perp} M \neq 0$,
- (ii) $\text{perp} M \in \text{conv} M$,
- (iii) M is the intersection of $\Delta(V, T)$ with the hyperplane in $X(T)_{\mathbb{Q}}$ passing through the end of the vector $\text{perp} M$ and orthogonal to this vector:

$$M = \Delta(V, T) \cap \{l_M = 1\}, \quad \text{where } l_M := \frac{\text{perp} M}{\|\text{perp} M\|^2},$$

- (iv) for $l = l_M$, inequality (C.2.12) holds.

When M runs over the whole family of representatives possessing properties (i)–(iv), the vector l_M runs over a certain finite subset $\mathcal{L}_{G,T,V}$ of $X(T)_{\mathbb{Q}}$.

If the G -module V is trivial (i.e., $\Delta(V, T) = \{0\}$), then $\mathcal{L}_{G,T,V} = \emptyset$ by (i). In particular, this is so if G is the identity group $\{e\}$. If the G -module V is nontrivial, then there exist nonzero nullforms in V (for example, vectors from V_{μ} for nonzero $\mu \in \Delta(V, T)$); hence, there are strata in $\mathcal{N}_{G,V} \setminus \{0\}$. According to the previous discussion, these strata are exhausted, without repetition, by varieties of the form $\mathcal{H}[l]$, where $l \in \mathcal{L}_{G,T,V} \cap \mathcal{S}$. In particular, $\mathcal{L}_{G,T,V} \neq \emptyset$ in this case.

Thus the algorithm for describing all strata of $\mathcal{N}_{G,V}$ for any nontrivial G -module V will be obtained if we find an algorithm for verifying whether or not $l \in \mathcal{L}_{G,T,V}$ is a stratifying element. That is what we shall now do.

C.3.4 To this end, we consider the following subset in $\mathcal{L}_{G,T,V}$:

$$\mathcal{M}_{G,T,V} := \left\{ l \in \mathcal{L}_{G,T,V} \mid \#(\{l < 0\} \cap \Phi(\mathfrak{g}, T)) = \sum_{\mu \in \{\langle -1 \rangle\}} \dim V_\mu \right\}. \quad (\text{C.3.7})$$

This subset “governs” the coincidence of $\mathcal{N}_{G,V}$ with V . Namely, if the G -module V is nontrivial, then (C.3.7) and Corollary C.2.3 of Theorem C.2.1 imply that the existence of a stratifying vector l in $\mathcal{M}_{G,T,V}$ is equivalent to the equality $\mathcal{N}_{G,V} = V$, and that, for such l , the stratum $\mathcal{H}[l]$ is open in V . Since different elements from $\mathcal{M}_{G,T,V}$ lie in different $W_{G,T}$ -orbits, the openness of $\mathcal{H}[l]$ in V and Theorem C.2.1(ii) imply that *only one* such an element l may exist. Note the particular case:

$$\mathcal{M}_{G,T,V} = \emptyset \implies \mathcal{N}_{G,V} \neq V. \quad (\text{C.3.8})$$

Implication (C.3.8) also holds for trivial G -modules V , since, for these modules, $\mathcal{N}_{G,V} = \{0\} \neq V$ and $\mathcal{M}_{G,T,V} = \emptyset$ by virtue of $\mathcal{L}_{G,T,V} = \emptyset$.

C.3.5 Henceforth, we assume that the G -module V is nontrivial and pass to the algorithm for verifying whether or not $l \in \mathcal{L}_{G,T,V}$ is a stratifying element. Since $\mathcal{N}_{G[l],V[l]}$ is closed in $V[l]$, condition (C.2.7) is equivalent to the fact that l satisfies the inequality

$$\dim \mathcal{N}_{G[l],V[l]} < \dim V[l]. \quad (\text{C.3.9})$$

In turn, because the number of strata is finite and the strata are open in their closures, (C.3.9) is equivalent to the fact that the dimension of all strata of $\mathcal{N}_{G[l],V[l]}$ is strictly less than $\dim V[l]$. As is shown above, the latter is equivalent to the fact that not a single element of $\mathcal{M}_{G[l],T[l],V[l]}$ determines the stratum of $\mathcal{N}_{G[l],V[l]}$, i.e., *no element* $l' \in \mathcal{M}_{G[l],T[l],V[l]}$ *satisfies* the following inequality:

$$\dim \mathcal{N}_{G[l][l'],V[l][l']} < \dim V[l][l']. \quad (\text{C.3.10})$$

Applying these arguments to the $G[l][l']$ -module $V[l][l']$, we obtain that (C.3.10) is *not fulfilled* precisely when $\mathcal{M}_{G[l][l'],T[l][l'],V[l][l']}$ contains an element l'' that determines the stratum of $\mathcal{N}_{G[l][l'],V[l][l']}$, i.e., such stratum that the following inequality is *fulfilled*:

$$\dim \mathcal{N}_{G[l][l'][l''],V[l][l'][l'']} < \dim V[l][l'][l''].$$

An so on.

C.3.6 This brings us to the consideration of all possible sequences of the form

$$l_1, \dots, l_d, \text{ where } l_1 = l \text{ and } l_{i+1} \in \mathcal{M}_{G[l_1] \dots [l_i], T[l_1] \dots [l_i], V[l_1] \dots [l_i]} \text{ for } i = 1, \dots, d-1. \quad (\text{C.3.11})$$

By (C.2.3) and (C.2.5), for each of these sequences, $V[l_1] \dots [l_d] \neq \{0\}$ and $G[l_1] \dots [l_d]$ is a connected reductive group of rank $\mathrm{rk} G - d$. Thus, $d \leq \mathrm{rk} G$.

The sequence (C.3.11) is maximal (i.e., nonextendable to the right) if and only if $\mathcal{M}_{G[l_1] \dots [l_d], T[l_1] \dots [l_d], V[l_1] \dots [l_d]} = \emptyset$; in this case, it follows from (C.3.8) that

$$\mathcal{N}_{G[l_1] \dots [l_d], V[l_1] \dots [l_d]} \neq V[l_1] \dots [l_d].$$

C.3.7 Let us associate with vector $l \in \mathcal{L}_{G,T,V}$ a rooted tree Γ_l (i.e., a connected graph without cycles and with a selected vertex called a *root*), whose edges are equipped with an orientation “from” the root, i.e., so that any vertex different from the root is the end of exactly one edge (this requirement uniquely determines the orientation of edges). This tree is successively constructed by the following procedure (see Fig. C.3):

- l is the root of Γ_l .
- If the set $\mathcal{M}_{G[l], T[l], V[l]}$ is empty, then Γ_l consists only of the root.
- If this set is nonempty and, say, consists of elements a_1, \dots, a_s , then these elements are vertices of Γ_l , and exactly s edges emanate from the root that have the ends a_1, \dots, a_s .
- Similarly, if the set $\mathcal{M}_{G[l][a_i], T[l][a_i], V[l][a_i]}$ is empty, then there are no edges emanating from vertex a_i .
- If this set is nonempty and, say, consists of elements b_1, \dots, b_t , then these elements are vertices of Γ_l , and exactly t edges emanate from a_i that have the ends b_1, \dots, b_t .
- And so on.
- There are no other vertices and edges in the tree Γ_l .

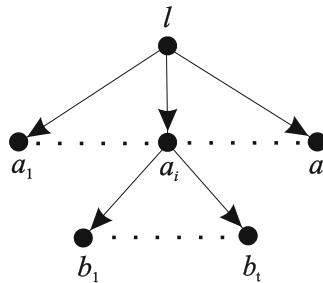


Fig. C.3 Rooted tree Γ_l

C.3.8 The decision rule can be now formulated as follows.

Theorem C.3.2 *Let l be an element of the set $\mathcal{L}_{G,T,V}$. We assign plus or minus signs to the vertices of the tree Γ_l (see Fig. C.4) by the following rule (which uniquely determines this sign allocation):*

A minus sign is assigned to a vertex if and only if there exists an edge emanating from this vertex whose end has a plus sign (in particular, all end vertices have a plus sign).

Then, l is a stratifying element if and only if the root of the graph Γ_l has a plus sign.

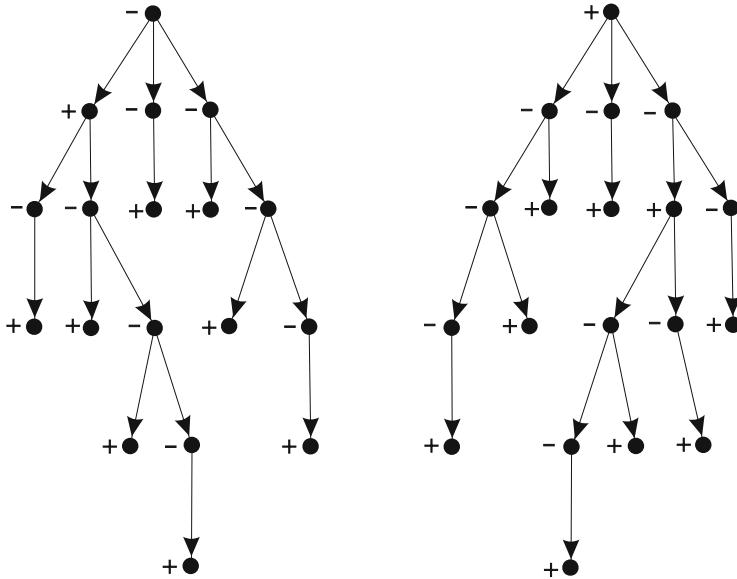


Fig. C.4 The sign allocation of the vertices of Γ_l

Proof See [11, Thm. 2]. □

Remark C.3.3 In fact, the proof and what has been said in Sect. C.3.4 imply that Γ_l automatically possesses the following special property: *at most one* edge emanates from any vertex of Γ_l whose other end has a plus sign. In particular, at most one edge leading to an end vertex emanates from any vertex. △

Corollary C.3.4 Suppose that an element $l \in \mathcal{L}_{G,T,V}$ is not orthogonal to any root. Then l is a stratifying element.

Proof By (C.3.1) and (C.3.2) and conditions (ii) and (iii) in the definition of $\mathcal{L}_{G,T,V}$ (see Sect. C.3.3), $0 \in \text{conv } \Delta(V[l], G[l])$. Therefore, for any nonzero element $l' \in X(T[l])_{\mathbb{Q}}$, the half-space $\{l' < 1\}$ contains at least one weight. Since, by the hypothesis, there are no roots in $X(T[l])_{\mathbb{Q}}$, condition (C.3.7) implies that $\mathcal{M}_{G[l], G[l], V[l]} = \emptyset$. Thus the tree Γ_l with the allocation of signs defined in Theorem C.3.2 has the form shown in Fig. C.5.



Fig. C.5 The tree Γ_l when l is not orthogonal to any root

Hence, l is a stratifying element. □

Since $\Phi(\mathfrak{g}, T) = \emptyset$ for $G = T$, this and (C.2.9) imply the following corollary.

Corollary C.3.5 (the case of a torus) *If G is a torus, $G = T$, then*

- (a) *all elements of the set $\mathcal{L}_{G,T,V}$ are stratifying elements;*
- (b) *the closures of the strata are linear subspaces of the form $\bigoplus_{\mu \in \text{conv}_M} V_\mu$, where M runs over those subsets in $\Delta(V, T)$ that possess properties (i), (ii), and (iii) pointed out in Sect. C.3.3. The strata themselves are complements, in these subspaces, to unions of finite sets of linear spaces of a similar form.*

C.4 Examples

C.4.1 Denote by $F_{d,n}$ the space of forms of degree $d \geq 0$ in variables x_1, \dots, x_n over k . We consider this space as the G -module for $G = \text{GL}_n$ or SL_n with respect to the natural action by linear transformations of variables.

We put $\mathbb{N} := \{0, 1, 2, \dots\}$ and $\mathbb{Z}_+ := \{1, 2, 3, \dots\}$.

C.4.2 Example (the case of rank 1) If $\dim T = 1$, then, by Corollary C.3.4 to Theorem C.3.2, all elements of $\mathcal{L}_{G,T,V}$ are stratifying elements.

Suppose that, in view of Corollary C.3.5 to Theorem C.3.2, the group G is not a torus. Then, passing to the universal covering, we can assume that $G = \text{SL}_2$ and T is the diagonal maximal torus in G . The group $X(T)$ is generated by the character $\text{diag}(a, a^{-1}) \mapsto a$. Denote it by ε . Then $\Phi(\mathfrak{g}, T) = \{2\varepsilon, -2\varepsilon\}$, and, since $W_{G,T} = \{1, -1\}$, we can assume that

$$\mathcal{L}_{G,T,V} = \left\{ \frac{\varepsilon}{\langle \mu, \varepsilon \rangle} \varepsilon \mid \mu \in \Delta(V, T) \cap \mathbb{Z}_+ \varepsilon \right\}.$$

Since $\text{char } k = 0$, we have, up to an isomorphism, $V = F_{d_{1,2}} \oplus \dots \oplus F_{d_{s,2}}$. Let d_{odd} (respectively, d_{even}) be the greatest positive odd (respectively, even) number among d_1, \dots, d_s , if such numbers exist, and 0 otherwise. Since

$$\Delta(F_{d,2}, T) = \{d\varepsilon, (d-2)\varepsilon, \dots, (2-d)\varepsilon, -d\varepsilon\}$$

and all the weights in $\Delta(F_{d,2}, T)$ have multiplicity 1, we obtain that the number of strata in $\mathcal{N}_{G,V} \setminus \{0\}$ is equal to $[(d_{\text{odd}} + 1)/2] + d_{\text{even}}/2$, and the dimension of the stratum $\mathcal{N}[l]$ defined by $l = \varepsilon/\langle m\varepsilon, \varepsilon \rangle \in \mathcal{L}_{G,T,V}$ is equal to $1 + \sum_{d_i \geq m} \lceil m, d_i \rceil$, where $\lceil a, b \rceil$ for $a, b \in \mathbb{Z}_+$, $a \leq b$, denotes the number of integers in the interval $[a, b]$ that have the same parity as b .

For example, when $s = 5$ and $(d_1, d_2, d_3, d_4, d_5) = (2, 3, 3, 4, 5)$, we have $d_{\text{odd}} = 5$, $d_{\text{even}} = 4$ and $\mathcal{L}_{G,T,V}$ consists of $[(d_{\text{odd}} + 1)/2] + d_{\text{even}}/2 = 5$ elements l_1, \dots, l_5 . Thus, there are exactly five strata in $\mathcal{N}_{G,V} \setminus \{0\}$. The weights from $\Delta(V, T)$ are depicted by circles in Fig. C.6; the numbers at these circles are the multiplicities of these weights. The roots are marked by arrows. One can choose l_i so that the point $\{l_i = 1\}$ is such as shown in Fig. C.6. The dimension of the stratum $\mathcal{H}[l_i]$ is

greater by 1 than the sum of multiplicities of the circles lying to the left of the circle $\{l_i = 1\}$ (including the latter); i.e., it is equal to 11, 8, 6, 3, and 2 for $i = 1, \dots, 5$, respectively. This, in particular, yields $\dim \mathcal{N}_{G,V} = 11$.

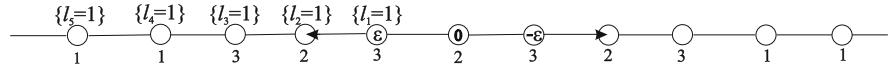


Fig. C.6 The case of $G = \mathrm{SL}_2$

C.4.3 Example (the case of rank 2) Let $\dim T = 2$. By Corollary C.3.5 to Theorem C.3.2, we assume that G is not a torus. The description of the straight lines $\{l = 1\}$ for $l \in \mathcal{L}_{G,T,V}$ is equivalent, up to the action of the Weyl group, to the description of all possible straight lines L on the plane $X(T)_{\mathbb{Q}}$ that share the following properties:

- (i) L does not pass through 0;
- (ii) L passes at least through one weight;
- (iii) the end of the perpendicular dropped from 0 onto L is contained in the segment that is the convex hull of the weights lying on L .

If L is such a line, then there are two possibilities: either L is parallel to no root, or it is parallel to a certain root α . In the first case, l is a stratifying element by Corollary C.3.4 to Theorem C.3.2. In the second case, it may happen that $\mathcal{M}_{G[l],T[l],V[l]} \neq \emptyset$. Namely, since $\Delta(V, T)$ is invariant with respect to $W_{G,T}$ and, in particular, with respect to the reflection about a straight line orthogonal to α , it follows from (C.3.7) that this occurs precisely when L contains exactly two different single weights (in Fig. C.7, the weights are depicted by dark, and the roots by light circles).

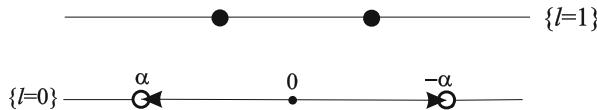


Fig. C.7 The case where $\dim T = 2$ and L is parallel to a root α

In this case, $\mathcal{M}_{G[l],T[l],V[l]}$ consists of a single element l' . Since, obviously, $\mathcal{M}_{G[l][l'],T[l][l'],V[l][l']} = \emptyset$, in this case the tree Γ_l with the appropriate sign allocation has the form shown in Fig. C.8.



Fig. C.8 The tree Γ_l if $\dim T = 2$ and L is parallel to a root

Hence, by Theorem C.3.2, l is not a stratifying element.

C.4.4 Example (dependence on the norm; nullcones with a finite number of orbits)
Let $G = \mathrm{GL}_2$ and $V = F_{1,2} \oplus \wedge^2 F_{1,2}$. There are exactly three nonzero G -orbits in V : $\mathcal{O}_1 := G \cdot x_1$, $\mathcal{O}_2 := G \cdot (x_1 \wedge x_2)$, and $\mathcal{O}_3 := G \cdot (x_1 + x_1 \wedge x_2)$. Let T be the diagonal maximal torus in G and let $\varepsilon_i \in X(T)$ be the weight of the variable x_i . The weights ε_1 and ε_2 form a basis in the lattice $X(T)$ and thereby in $X(T)_{\mathbb{Q}}$. The Weyl group $W_{G,T}$ has order 2 and acts by permutations of ε_1 and ε_2 . The sequence of vectors $x_1, x_2, x_1 \wedge x_2$ is a weight basis in V . Therefore, the system of weights has the form $\Delta(V, T) = \{\varepsilon_1, \varepsilon_2, \varepsilon_1 + \varepsilon_2\}$ and the multiplicity of every weight is 1. The system of roots has the form $\Phi(\mathfrak{g}, T) = \{\varepsilon_1 - \varepsilon_2, \varepsilon_2 - \varepsilon_1\}$. Positive definite $W_{G,T}$ -invariant inner products on $X(T)_{\mathbb{Q}}$ are classified by the pairs of rational numbers $(a, b) \in \mathbb{Q}^2$, satisfying the conditions $a > 0$ and $a^2 > b^2$: to a pair (a, b) is assigned the inner multiplication for which $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ is the Gram matrix of the basis $\varepsilon_1, \varepsilon_2$.

Thus, in this case, the weights and the roots are depicted in Fig. C.9 by dark and light circles, respectively; the left part of the figure illustrates the case when $b > 0$, while the right part, the case when $b \leq 0$:

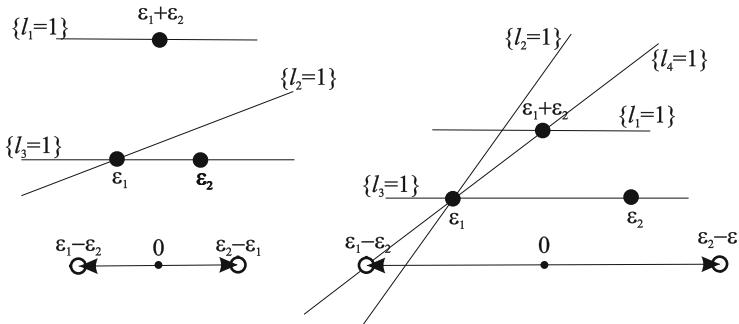


Fig. C.9 Dependence on the norm

Figure C.9 shows that the set $\mathcal{L}_{G,T,V}$ consists of three elements l_1, l_2 , and l_3 for $b > 0$ and of four elements l_1, l_2, l_3 , and l_4 for $b \leq 0$, and that, subjecting these elements, if necessary, to transformations from the Weyl group, one can assume that the straight lines $\{l_i = 1\}$ are such as they are depicted in Fig. C.9. According to Example C.4.2, if $b > 0$, then there are exactly two strata in $\mathcal{N}_{G,V} \setminus \{0\}$, namely, $\mathcal{H}[l_1]$ and $\mathcal{H}[l_2]$; if $b \leq 0$, then there are exactly three such strata, namely, $\mathcal{H}[l_1]$, $\mathcal{H}[l_2]$, and $\mathcal{H}[l_4]$. It is clear that, if $b > 0$, then $\mathcal{H}[l_1] = \mathcal{O}_2$, and $\mathcal{H}[l_2] = \mathcal{O}_1 \cup \mathcal{O}_3$, whereas, if $b \leq 0$, then $\mathcal{H}[l_1] = \mathcal{O}_2$, $\mathcal{H}[l_2] = \mathcal{O}_1$ and $\mathcal{H}[l_4] = \mathcal{O}_3$.

Thus, in the general case, the strata depend on the norm chosen and, if the nullcone contains only a finite number of orbits, then some strata may not be orbits (see [1, Rem. 4.10]).

C.4.5 Example (ternary forms) Let $G = \mathrm{SL}_3$ and $V = F_{d,3}$, $d \geq 1$. Let T be the diagonal maximal torus in G and let $\varepsilon_i \in X(T)$ be the weight of the variable x_i . The

space $X(T)_{\mathbb{Q}}$ is two-dimensional. The weights ε_1 , ε_2 , and ε_3 generate the lattice $X(T)$, and the sum of these weights is equal to 0. The system of roots $\Phi(g, T)$ is the set $\{\varepsilon_i - \varepsilon_j \mid i \neq j\}$. The set $\{\varepsilon_1, \varepsilon_2, \varepsilon_3\}$ is preserved by the Weyl group $W_{G,T}$, and any permutation of the vectors ε_1 , ε_2 , and ε_3 is performed by a certain element from $W_{G,T}$. Therefore, $\|\varepsilon_1\| = \|\varepsilon_2\| = \|\varepsilon_3\|$, and $\angle\{\varepsilon_i, \varepsilon_j\} = 2\pi/3$ for $i \neq j$, which determines $\langle \cdot, \cdot \rangle$ uniquely up to proportionality. If $c_1, c_2, c_3 \in \mathbb{Q}$, then we denote the vector $c_1\varepsilon_1 + c_2\varepsilon_2 + c_3\varepsilon_3 \in X(T)_{\mathbb{Q}}$ by $(c_1c_2c_3)$. Then the system of weights is expressed as $\Delta(V, T) = \{(c_1c_2c_3) \mid c_1 + c_2 + c_3 = d, c_i \in \mathbb{N}\}$. The multiplicity of the weight $(c_1c_2c_3)$ is equal to 1, and the monomial $x_1^{c_1}x_2^{c_2}x_3^{c_3}$ is a basis in $V_{(c_1c_2c_3)}$. Thus the system of weights is given by the set of vertices of regular triangles with the side $\sqrt{3}\|\varepsilon_i\|$ that form a partition of the regular triangle with vertices $(d00)$, $(0d0)$, $(00d)$. In Fig. C.10, the weights are depicted by dark circles and the roots by light circles.

The straight lines $\{l = 1\}$ for $l \in \mathcal{L}_{G,T,V}$ and the stratifying elements in $\mathcal{L}_{G,T,V}$ are described according to Example C.4.2. There is a unique, up to the action of the Weyl group, case when l is not a stratifying element: in this case, the straight line $L_0 := \{l = 1\}$ passes through the weights $(1(d-1)0)$ and $(0(d-1)1)$.

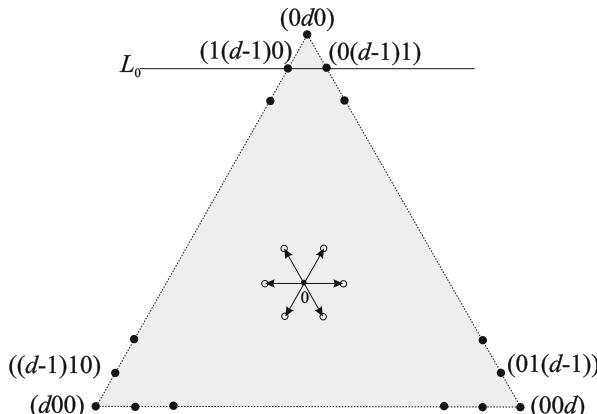


Fig. C.10 The case of ternary forms of degree d

For example, in the case of ternary quartics (i.e., when $d = 4$), one can easily verify that $\mathcal{L}_{G,T,V}$ contains exactly 12 elements l_1, \dots, l_{12} and that, subjecting them, if necessary, to transformations from the Weyl group, one can assume that the straight lines $\{l_i = 1\}$ are such as they are depicted in Fig. C.11 on the next page. Here, only l_2 is not a stratifying element. Thus, in this case there are exactly eleven strata in $\mathcal{N}_{G,V} \setminus \{0\}$, namely, $\mathcal{H}[l_i]$, $i = 1, \dots, 12, i \neq 2$. Formula (C.2.11) gives their dimensions: $\dim \mathcal{H}[l_i] = 3, 8, 11, 7, 9, 5, 9, 10, 10, 7, 8$ for $i = 1, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12$, respectively. Hence, $\dim \mathcal{N}_{G,V} = 11$ and $\mathcal{N}_{G,V}$ has a unique irreducible component of maximal dimension (one can show that $\mathcal{N}_{G,V}$ has another irreducible component of smaller dimension [4]).

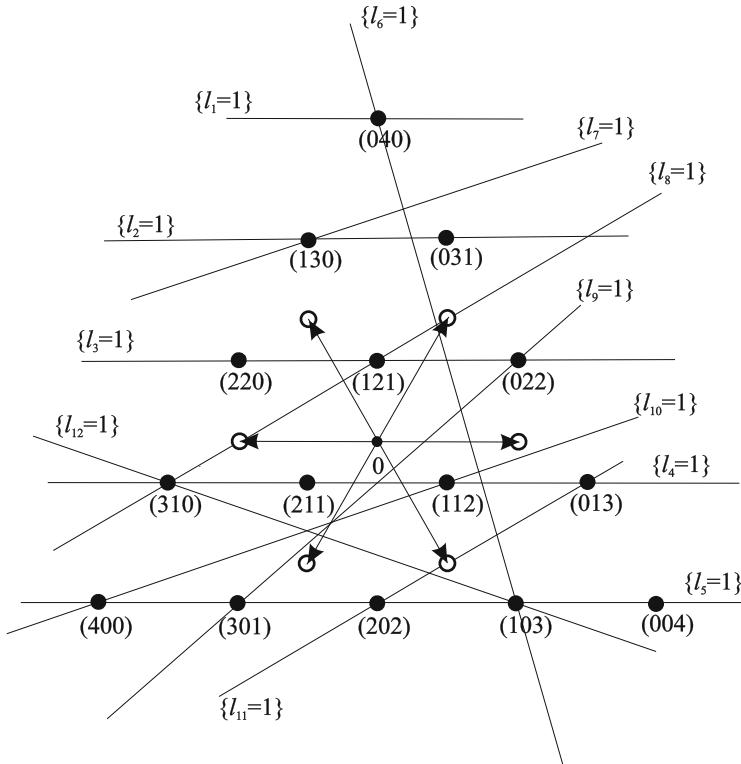


Fig. C.11 The case of ternary quartics

C.4.6 Example (nilpotent elements in reductive Lie algebras) If $V = \mathfrak{g}$, then $\mathcal{N}_{G,V}$ is the variety of nilpotent elements of the Lie algebra \mathfrak{g} . It is well known [7, 10] that, in this case, the strata of the $\mathcal{N}_{G,V} \setminus \{0\}$ are exactly the nonzero G -orbits contained in $\mathcal{N}_{G,V}$, i.e., the conjugacy classes of nonzero nilpotent elements of the Lie algebra \mathfrak{g} . Hence, in this case our algorithm turns into the classification algorithm for the conjugacy classes of nilpotent elements in reductive Lie algebras \mathfrak{g} , which is reduced to only simple geometric-combinatorial operations with the root system $\Phi(\mathfrak{g}, T)$. For the first time, such a classification was obtained in [9] by a different method, which was later improved in [25]. This classification is a particular case of the classification of the orbits of nullforms for the so-called θ -representations (see [3, 8.5], [26], and Sect. C.4.7 below). To obtain the latter classification, Dynkin's method was improved and extended in [16, 17, 27] to the case of θ -representations. A partial computer implementation of this method was obtained in [28].

We will illustrate the solution to this problem by means of our algorithm through the example of the exceptional simple Lie algebra \mathfrak{g} of type G_2 . In this case, the weights are depicted by dark circles in Fig. C.12 on the next page.

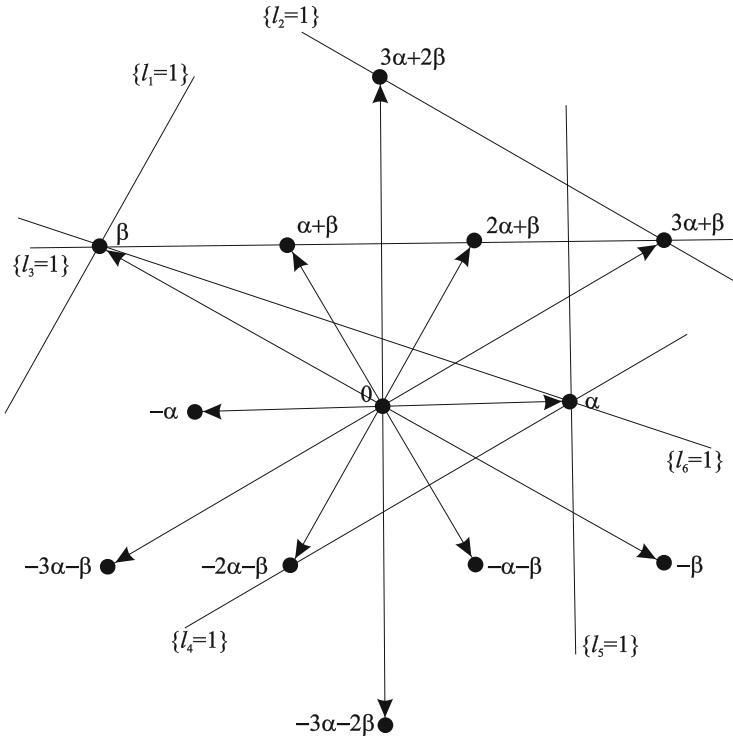


Fig. C.12 The case of the adjoint representation of the exceptional simple Lie algebra of type G_2

Here, the roots are nonzero weights. Using Fig. C.12, one can easily verify that the set $\mathcal{L}_{G,T,V}$ contains exactly six elements l_1, \dots, l_6 and that, subjecting them, if necessary, to transformations from the Weyl group, one can assume that the straight lines $\{l_i = 1\}$ are as is shown in this figure. Of these elements, only l_6 is not orthogonal to any root; for all the other elements l_i , the line $\{l_i = 1\}$ contains exactly two roots precisely for $i = 2$ and 4. Hence, the total number of strata in $\mathcal{N}_{G,V} \setminus \{0\}$ is four (therefore, there are exactly four nonzero conjugacy classes of nonzero nilpotent elements), namely, $\mathcal{H}[l_i]$, where $i = 1, 3, 5$ and 6.

The representatives of these four classes are obtained by means of what has been said in Sect. C.2.11. Namely, it follows from Proposition C.2.6 that, if $x_\gamma \in \mathfrak{g}_\gamma$ is an element of the Chevalley basis of the algebra \mathfrak{g} , then the representatives of the classes $\mathcal{H}[l_1]$, $\mathcal{H}[l_3]$, $\mathcal{H}[l_5]$, and $\mathcal{H}[l_6]$ are x_β , $t_\beta x_\beta + t_{\alpha+\beta} x_{\alpha+\beta} + t_{2\alpha+\beta} x_{2\alpha+\beta} + x_{3\alpha+\beta}$, x_α , and $x_\alpha + t_\beta x_\beta$, respectively, where t_β , $t_{\alpha+\beta}$, $t_{2\alpha+\beta}$ are elements of the field k that are algebraically independent over \mathbb{Q} .

A simple additional argument shows that these representatives can be simplified. Namely, according to (C.2.9) and (C.2.6), if a $G[l_i]$ -orbit of a nonzero vector $v \in V[l_i]$ is closed, then this vector lies in the class $\mathcal{H}[l_i]$. The group $G[l_i]$ is a one-dimensional torus $T[l_i]$ for $i = 6$ and is locally isomorphic to SL_2 for

$i \neq 6$. Therefore, in the first case, the closedness of $G[l_i] \cdot v$ is equivalent to the fact that zero lies in the convex hull of the weights of the $T[l_6]$ -module $V[l_6]$ that take part in the decomposition of v into a sum of weight vectors. This fact and Fig. C.12 imply that $e_\alpha + e_\beta$ is a representative of the class $\mathcal{H}[l_6]$. In the second case, one can use the fact that, if the weights of certain weight vectors possess the following properties:

- (a) all these weights are different;
- (b) zero is an inner point of their convex hull; and
- (c) the difference of any two of these weights is not a root,

then the orbit of the sum of these weight vectors is closed (see [3, Thm. 6.19], [29, Prop. 1.2]). This applies to the case of $i = 3$. Figure C.12 shows that the roots of the group $G[l_3]$ with respect to the torus $T[l_3]$ are $\pm\alpha$, and the weights of $V[l_3]$ are the orthogonal projections of β , $\alpha + \beta$, $2\alpha + \beta$, and $3\alpha + \beta$ onto the straight line $\{l_3 = 0\}$. Hence the $G[l_3]$ -orbit of the vector $e_\beta + e_{3\alpha+\beta}$ is closed. Therefore, $e_\beta + e_{3\alpha+\beta}$ is a representative of the conjugacy class $\mathcal{H}[l_3]$.

C.4.7 In conclusion, consider the G -modules V determined by the θ -representations.

First, recall their definition (see [3, 8.5], [16, 26]). Let m be a positive integer and $\mu_m := \{a \in k \mid a^m = 1\}$. Let H be a semisimple simply connected algebraic group and $\mathfrak{h} := \text{Lie}(H)$. Consider a group homomorphism $\theta: \mu_m \rightarrow \text{Aut } H$ and, for every $i \in \mathbb{Z}/m\mathbb{Z}$, put $\mathfrak{h}_i := \{x \in \mathfrak{h} \mid d_x \theta(t)x = t^i x \text{ for all } t \in \mu_m\}$. Then $\mathfrak{h} = \bigoplus_{i \in \mathbb{Z}/m\mathbb{Z}} \mathfrak{h}_i$ is a $\mathbb{Z}/m\mathbb{Z}$ -grading of the Lie algebra \mathfrak{h} (and every $\mathbb{Z}/m\mathbb{Z}$ -grading of \mathfrak{h} is obtained in this way). In particular, \mathfrak{h}_0 is a subalgebra of \mathfrak{h} and

$$[\mathfrak{h}_0, \mathfrak{h}_1] \subseteq \mathfrak{h}_1. \quad (\text{C.4.1})$$

The algebraic subgroup $H_0 := H^{\theta(\mu_m)}$ is connected and \mathfrak{h}_0 is its Lie algebra. In view of (C.4.1), the adjoint representation of H induces by restriction a linear representation $H_0 \rightarrow \text{GL}(\mathfrak{h}_1)$. It is called a *θ -representation*, and the H_0 -module \mathfrak{h}_1 is called the *H_0 -module determined by this θ -representation*. When $m = 1$, it is the adjoint H -module.

The following proposition shows that, for any G -module determined by a θ -representation, our algorithm turns into a classification algorithm for the orbits of nullforms.

Proposition C.4.1 *If V is determined by a θ -representation, then the strata of $\mathcal{N}_{G,V}$ are G -orbits.*

Proof The existence of a homogeneous version of the Morozov theorem [18, Thm. 1] allows one to apply the arguments similar to those by which this fact was proved in [10, Prop. 1] for the adjoint G -module \mathfrak{g} (in turn, these arguments were inspired by [24, §1, Lem. 1.4]). \square

References

1. W. H. Hesselink, *Desingularizations of varieties of nullforms*, Invent. math. **55** (1979), 141–163.
2. D. Mumford, *Geometric Invariant Theory*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 34, Springer-Verlag, Berlin, 1965.
3. V. L. Popov, E. B. Vinberg, *Invariant Theory*, in: *Algebraic Geometry*, IV, Encyclopaedia of Mathematical Sciences, Vol. 55, Springer-Verlag, Berlin, 1994, pp. 123–284.
4. D. Hilbert, *Über die vollen Invariantensysteme*, Math. Ann. **42** (1893), 313–373.
5. F. A. Bogomolov, *Holomorphic tensors and vector bundles on projective varieties*, Math. USSR, Izv. **13** (1979), 499–555.
6. G. R. Kempf, *Instability in invariant theory*, Ann. of Math. **108** (1978), 299–316.
7. W. H. Hesselink, *Uniform instability in reductive groups*, J. reine angew. Math. **303/304** (1978), 74–96.
8. G. Rousseau, *Immeubles sphériques et théorie des invariants*, C. R. Acad. Sc. Paris **286** (1978), A 247–250.
9. E. B. Dynkin, *Semisimple subalgebras of semisimple Lie algebras*, Amer. Math. Soc. Transl., Ser. 2 **6** (1957), 111–244.
10. P. Slodowy, *Die Theorie der optimalen Einparameteruntergruppen für instabile Vektoren*, in: *Algebraic Transformation Groups and Invariant Theory*, DMV Seminar, Vol. 13, 1989, Birkhäuser Basel, pp. 115–130.
11. V. L. Popov, *The cone of Hilbert nullforms*, Proc. Steklov Inst. Math. **241** (2003), 177–194, arXiv:1009.6107.
12. V. L. Popov, *Representations with a free module of covariants*, Funct. Anal. Appl. **10** (1976), no. 3, 242–244.
13. O. M. Adamovich, *Equidimensional representations of simple algebraic groups*, Amer. Math. Soc. Transl., Ser. 2, Vol. 128, 1986, 25–29.
14. G. W. Schwarz, *Representations of simple Lie groups with a free module of covariants*, Invent. math. **50** (1978), 1–12.
15. P. Littelmann, *Koreguläre und äquidimensionale Darstellungen halbeinfacher Liegruppen*, J. Algebra **123** (1989), no. 1, 193–222.
16. E. B. Vinberg, *On the linear groups associated to periodic automorphisms of semisimple algebraic groups*, Sov. Math., Dokl. **16** (1975), 406–409.
17. E. B. Vinberg, *On the classification of the nilpotent elements of graded Lie algebras*, Sov. Math., Dokl. **16** (1976), 1517–1520.
18. E. B. Vinberg, *Classification of homogeneous nilpotent elements of a semisimple graded Lie algebra*, Sel. Math. Sov. **6** (1987), 15–35.
19. N. A'Campo, V. L. Popov, *The package HNC*, <http://www.geometrie.ch/>.
20. L. Ness, *A stratification of the nullcone via moment map*, Amer. J. Math. **106** (1984), 1281–1329.
21. F. C. Kirwan, *Cohomology of Quotients in Symplectic and Algebraic Geometry*, Math. Notes **31**, Princeton Univ. Press, Princeton, 1984.
22. J. E. Humphreys, *Introduction to Lie Algebras and Representation Theory*, Graduate Texts in Mathematics, Vol. 9, Springer-Verlag, New York, Heidelberg, 1972.
23. V. G. Kac, *On the question of describing the orbit space of linear algebraic groups*, Usp. Mat. Nauk **30** (1975), no. 6(186), 173–174 (Russian). Zbl 0391.20035.
24. V. Kac, *Some remarks on nilpotent orbits*, J. Algebra **64** (1980), 190–213.
25. P. Bala, R. W. Carter, *Classes of unipotent elements in simple algebraic groups, I and II*, Math. Proc. Camb. Phil. Soc. **79** (1976), 401–425 and **80** (1976), 1–18.
26. E. B. Vinberg, *The Weyl group of a graded Lie algebra*, Math. USSR, Izv. **10** (1977), 463–495.
27. V. Gatti, E. Viniberghi, *Spinors of a 13-dimensional space*, Adv. Math. **30** (1978), 137–155.
28. P. Littelmann, *An effective method to classify nilpotent orbits*, in: *Progress in Math.*, Vol. 143, 1996, Birkhäuser Basel, 255–269.
29. J. Dadok, V. Kac, *Polar groups*, J. Algebra **92** (1985), 504–524.

Addendum to Appendix C: The Source Code of HNC

Norbert A'Campo and Vladimir L. Popov

1 Before running hnc.gp you need to have pari-gp [1] and LiE [2] on your system. Download hnc-x.x.z.tar.gz from <http://www.geometrie.ch/>, unpack and go in the directory HNC. Start pari with the command gp. Pari prompt will appear. Check that in your pari session the file .gprc was sourced. Then execute the command
> hnc(GROUP, REPRESENTATION).

Here GROUP is a simply connected semisimple group G given by types of the Dynkin diagrams of its simple factors and REPRESENTATION is a representation of G in V given by the coordinates of the highest weights of its irreducible components in the basis of fundamental weights of G numbered as in [3].

2 *Example* > hnc(A3A2,"X0,0,1,1,0+X1,1,0,0,1") corresponds to the reducible representation of $G = \mathrm{SL}_4 \times \mathrm{SL}_3$ (whose Dynkin diagram has type A_3A_2), which is the direct sum of two irreducible representations: the highest weight of one of them is $\varpi'_3 + \varpi''_1$ and that of the other is $\varpi'_1 + \varpi'_2 + \varpi''_2$. Here $\varpi'_1, \varpi'_2, \varpi'_3$ are the fundamental weights of $G = \mathrm{SL}_4$ and ϖ''_1, ϖ''_2 are that of SL_3 . Using the quotes " " and the X's is necessary.

The output is a list, without repetitions, of all nonzero strata of the nullcone $\mathcal{N}_{G,V}$ and their dimensions. In this list, every stratum $\mathcal{H}[l]$ (see Theorem C.2.1 above) is presented by a row of the form $[d, [a_1, \dots, a_r]]$, where $d = \dim \mathcal{H}[l]$ and a_1, \dots, a_r

N. A' C.: Universität Basel, Mathematisches Institut, Spiegelgasse 1, 4051 Basel, Switzerland.
E-mail address: norbert.acampo@unibas.ch

V. L. P.: Steklov Mathematical Institute, Russian Academy of Sciences, Gubkina 8, Moscow 119991, Russia. National Research University Higher School of Economics, Myasnitskaya 20, Moscow 101000, Russia. E-mail address: popovvl@mi.ras.ru. Supported by the program *Contemporary Problems of Theoretical Mathematics* of the Russian Academy of Sciences, Branch of Mathematics.

are the coordinates of $l/\|l\|^2$ in the basis of simple roots $\alpha_1, \dots, \alpha_r$ numbered as in [3] (in the notation of Sect. C.3.3 above, if $l = l_M$, then $l/\|l\|^2 = \text{perp } M$); every such l lies in the positive Weyl chamber.

3 Example

- (a) Running **HNC** for `> hnc(E6,"X0,1,0,0,0,0")` corresponds to finding all nonzero strata of $\mathcal{N}_{G,V}$ for the adjoint module $V = \text{Lie } G$ of the group G of type E_6 , i.e., for finding all nonzero nilpotent G -orbits in $\text{Lie } G$ (see above Proposition C.4.1). The output of this running is

```
[22, [1, 2, 2, 3, 2, 1]],
[42, [1/2, 1, 1, 3/2, 1, 1/2]],
[32, [1, 1, 3/2, 2, 3/2, 1]],
[40, [2/3, 1, 4/3, 2, 4/3, 2/3]],
[46, [3/5, 4/5, 1, 7/5, 1, 3/5]],
[52, [2/5, 3/5, 7/10, 1, 7/10, 2/5]],
[48, [1/2, 1/2, 3/4, 1, 3/4, 1/2]],
[50, [1/2, 2/3, 1, 4/3, 1, 1/2]],
[60, [3/10, 2/5, 1/2, 7/10, 1/2, 3/10]],
[58, [1/3, 1/2, 2/3, 1, 2/3, 1/3]],
[56, [4/11, 6/11, 8/11, 1, 8/11, 4/11]],
[60, [3/14, 5/14, 3/7, 9/14, 3/7, 3/14]],
[54, [4/9, 5/9, 7/9, 10/9, 7/9, 4/9]],
[66, [2/9, 5/18, 7/18, 5/9, 7/18, 2/9]],
[62, [2/7, 8/21, 11/21, 5/7, 11/21, 2/7]],
[64, [8/35, 2/7, 2/5, 19/35, 2/5, 8/35]],
[64, [7/30, 1/3, 13/30, 3/5, 13/30, 7/30]],
[68, [1/6, 7/30, 3/10, 13/30, 3/10, 1/6]],
[70, [1/7, 4/21, 11/42, 5/14, 11/42, 1/7]],
[72, [4/39, 11/78, 5/26, 7/26, 5/26, 4/39]].
```

Hence there are precisely 20 nonzero nilpotent orbits in $\text{Lie } G$ for the group G of type E_6 , and their dimensions are 22, 32, 40, 42, 46, 48, 50, 52, 54, 56, 58, 60, 60, 62, 64, 64, 66, 68, 70, 72. This agrees with the Dynkin–Kostant classification of such orbits obtained by a different method, see, e.g., [4, p. 129].

- (b) Running **HNC** for `> hnc(D7,"X0,0,0,0,0,0,1")` corresponds to finding all nonzero strata of $\mathcal{N}_{G,V}$ for $G = \text{Spin}_{14}$ and V the half-spin G -module. The latter is determined by a θ -representation, therefore the strata are G -orbits (see above Proposition C.4.1). The output of this running is

$$\begin{aligned} & [22, [1/2, 1, 3/2, 2, 5/2, 5/4, 7/4]], \\ & [35, [1/2, 1, 3/2, 3/2, 3/2, 3/4, 3/4]], \\ & [44, [1/2, 1/2, 1/2, 1/2, 1/2, 1/4, 1/4]], \\ & [43, [1/2, 2/3, 5/6, 1, 7/6, 7/12, 3/4]], \\ & [54, [3/10, 2/5, 1/2, 3/5, 7/10, 9/20, 7/20]], \\ & [50, [1/4, 1/2, 3/4, 1, 1, 1/2, 1/2]], \\ & [59, [1/6, 1/3, 1/2, 1/2, 1/2, 1/4, 1/4]], \\ & [63, [1/14, 1/7, 3/14, 2/7, 5/14, 1/4, 5/28]]. \end{aligned}$$

Therefore, there are precisely eight nonzero G -orbits in $\mathcal{N}_{G,V}$, and their dimensions are 22, 35, 44, 43, 54, 50, 59, 63. This agrees with [5] where the classification of G -orbits in $\mathcal{N}_{G,V}$ is obtained by a different method.

- (c) Let `> hnc(A2,"X4,0")`. This corresponds to the case of Sect. C.4.5 above: $G = \text{SL}_3$ and V is the space of ternary quartics. The output is

$$\begin{aligned} & [7, [2/3, 4/3]], \\ & [8, [2/3, 1/3]], \\ & [5, [5/3, 4/3]], \\ & [3, [8/3, 4/3]], \\ & [10, [8/21, 10/21]], \\ & [9, [20/39, 28/39]], \\ & [11, [1/6, 1/3]], \\ & [9, [1/2, 1/2]], \\ & [10, [5/21, 4/21]], \\ & [8, [2/3, 5/6]], \\ & [7, [1, 1]]. \end{aligned} \tag{C.0.1}$$

Hence there are precisely 11 nonzero strata in $\mathcal{N}_{G,V}$, and their dimensions are 3, 5, 7, 7, 8, 8, 9, 9, 10, 10, 11. This agrees with Sect. C.4.5 above. The rows $[a_1, a_2]$ in (C.0.1) agree with Fig. C.11: for instance, $\frac{1}{6}\alpha_1 + \frac{1}{3}\alpha_2$ and the perpendicular dropped from 0 to the line l_4 lie in the same orbit of the Weyl group.

- (d) The output of running `> hnc(A5,"X0,0,2,0,0")` shows that $\mathcal{N}_{G,V}$ contains precisely 11,548 nonzero strata. In this case, $\dim G = 35$, $\dim V = 175$, $\dim V//G = 140$, and the generic fiber of the natural morphism $\pi: V \rightarrow V//G$ has dimension 35. The output shows that the dimension of $\pi^{-1}(\pi(0)) = \mathcal{N}_{G,V}$ is 100, and the number of irreducible components of $\mathcal{N}_{G,V}$ of maximal dimension is 324. There are infinitely many G -orbits in $\mathcal{N}_{G,V}$.
- (e) In [6] an algorithm is suggested for finding strata of $\mathcal{N}_{G,V}$, where $G = \mathrm{SL}_n$ and V is the space of m -tuples of $n \times n$ -matrices on which G acts by simultaneous conjugation. It is applied in [6] to the cases $n \leq 5$, $m \leq 3$. Using HNC, one obtains the answer for bigger values. For instance, in the case $n = 6$, $m = 2$ (corresponding to `> hnc(A5,"X1,0,0,0,1+X1,0,0,0,1")`), there are precisely 44 nonzero strata and their dimensions are 11, 15, 15, 20, 22, 22, 23, 23, 23, 24, 24, 27, 27, 27, 27, 30, 30, 30, 31, 31, 32, 32, 33, 33, 33, 34, 36, 36, 36, 38, 38, 39, 39, 39, 39, 39, 42, 42, 42, 42, 42, 45. For $n = 5$, $m = 2$, HNC corrects [6]: the dimension of one of the strata should be 17, not 18.
- (f) In [7] the classification of G -orbits in $\mathcal{N}_{G,V}$ for $G = \mathrm{Spin}_{13}$ and the spinor G -module V is obtained (this V is not determined by a theta-representation). According to [7, Table 1], there are precisely 13 nonzero orbits. This case corresponds to `> hnc(B6,"X0,0,0,0,1")` and HNC yields that the number of nonzero strata is 13 as well. Hence in this case the strata are orbits. Herewith HNC corrects [6]: their dimensions are 22, 32, 35, 42, 43, 43, 46, 50, 50, 53, 56, 58, 62, not 22, 31, 35, 37, 43, 43, 48, 50, 51, 53, 56, 58, 62 as stated in [7] (where the calculations are dropped).

Further explanations are contained below in the source code `hnc.gp`.

4 The source code `hnc.gp` of HNC

Here is the Pari-gp code `hnc.gp`.

First, we need global variables:

```

iipm=invariant_inner_product_matrix
cartanm=cartan_matrix
pos_roots=positive_roots
LieRank=dimension of adjoint representation
M=weights

global(pos_roots,twice_rho,MW,m1,
cartanm,iipm,LieRank,list,child_nb,u_nb);
initializes list,child_nb for representation with
multiplicities and weights MW. Output:
[child_nb,mother_nb,new_weights,
mother,child,new_pos_roots]
init_M(M)=
{
list=vector(1); child_nb=1;u_nb=2;
list[child_nb]=
[child_nb, 0, M, [], vector(LieRank), pos_roots];

```

```

write(‘‘data’’, concat([‘‘DimensionRepresentation = ’’,
sum( i=1, matsize(M)[1],M[i,1]), ‘‘; ’']));
}

```

0-SECTION

The function `ist_gleich(u,v)` has Boolean output 0,1;
 1 iff vectors v,w are equal
`ist_gleich(v,w)=`
`{`
`if((v-w)*(v-w)~==0 , 1, 0);`
`}`

The integral vector v of length `k=length(v)` with
`v[k]>v[k-1]>v[k-2]> ...>v[1]>=1` is considered as subset
 with `length(v)` elements of a set
`{1,m}` with `m>=v[length(v)]`.

The function `rankssubset()` computes for a subset
 v its rank with
`1<= rankssubset(v) <= binomial(v[length(v)],length(v)).`
 See: Constructive Combinatorics , by
 Dennis Stanton & Dennis White.

```

rankssubset(v)=
{
1+sum(i=1,length(v),binomial(v[i]-1,1+length(v)-i))
}

```

The function `subset(s,ss)` restores , unranks , from
 size s of the subset {1,s} and from rank ss the subset
 of {1,s}. See: Constructive Combinatorics .

```

subset(s,ss)=
{
local(m,p);
m=ss-1;
vector(s,i,p=s-i;until(binomial(p,s-i+1)>m,p++));
m=m-binomial(p-1,s-i+1);p)
}

```

1-SECTION

In the function `nullproj(N)` N is a matrix with
 rational entries. Its rows are considered as vertices
 of a simplex in the rational span of the roots with its
 invariant inner product `iipm`. The function `nullproj(N)`
 computes the shortest vector in the affine subspace

```

spanned by that simplex.

nullproj(N)=
{
local(s,d,resN,resL,cramer);
s=matsize(N)[1];
cramer=matrix(s,s,i,j,if(i<s,N[j,]*iipm*(N[i,]-N[s,])~,1));
d=matdet(cramer);
resL=vector(s,t,matdet( matrix(s,s,i,j,
           if(j!=t,cramer[i,j], if(i==s,1/d,0)))));
resN=[resL,resL*N]
}

```

The function in_chamber(L,R) has Boolean output
 $0,1$; 1 iff L is member of cone spanned by R

```

in_chamber(L,R)=
{
if(vecmin(R*iipm*L~) < 0, 0, 1)
}
```

The function dim_cond(M,R,L,g) checks a condition:
if $g \geq 2$ it checks that the number of roots r with $(L,r) < 0$
equals the number of weights m counted with
multiplicities and with $(L,m) < (L,L)$. If $g == 1$ it checks
that the number of roots r with $(L,r) < 0$ is less
or equal to the number of weights m counted with
multiplicities and with $(L,m) < (L,L)$. The value of g is
the number of the mother.

```

dim_cond(M,R,L,g)=
{
local(countM,countR);
countR=0; countM=0;
for(i=1,matsize(M)[1],
if(vector(LieRank,j,M[i,j+1]-L[j])*iipm*L~<0,
   countM=countM+M[i,1]);
for(i=1,matsize(R)[1],
if(vector(LieRank,j,R[i,j])*iipm*L~==0,countR++));
if(g>1,if(matsize(R)[1]-countR == countM,1,0),
   if(matsize(R)[1]-countR <= countM,1,0))
}
```

2-SECTION

The function saturlist() computes children of
children ... and stores in the list. The function

non_neg_weight() reduces the list of weights , only non-negative weights can occur as vertices of a simplex with the foot in the Weyl chamber. Moreover we make a list of edges that can belong to simplices with their foot in the Weyl chamber. We store for each weight a the possible weights b such that the number of b exceeds the number of a that $b-a$ is non-negative and non-positive , as done in non_neg_and_non_pos(). all_perp makes the list of foots of simplices that satisfie 4 tests: to be non_zero , to lie in simplex , to lie in Weyl chamber and satisfy according to g=mother_nb the test of dim_cond(). saturL() enhances this list with data according to the child data structure. We do finally the saturation of the list by searching with satur() for children of children

```
saturlist()=
{
non_neg_weights();
all_perp();
saturL();
while(u_nb<=child_nb ,satur(list[u_nb]);u_nb++);
}
```

The function satur(ML) computes the children of ML if we have mother_nb=ML[2]>0. We reproduce new_weights , new_pos_roots in the hyperplane that is perpendicular to the child . Now we search for children that satisfy the 4 tests .

```
satur(ML)=
{
local(ml1,nb_w,nb_r,new_weights,new_pos_roots,dimS,test ,
sub ,item ,sM,v,r,a,candidate ,c,f );
f=0; nb_r=0; r=matsize(ML[6])[1];
v=vector(r); \\compute new_pos_roots
for(i=1,r,
    if(ML[6][i,]*iipm*ML[5]~==0, nb_r++; v[nb_r]=i ); );
    if(nb_r==0, return() ); \\if nb_r==0, do nothing
new_pos_roots=matrix(nb_r,LieRank , i,j , ML[6][v[i],j]);
a=matsize(ML[3])[1];
ml1=matrix(a,LieRank , i,j ,ML[3][i,j+1]);
v=vector(a); nb_w=0; \\compute new_weigths
for(i=1,a,
    if( (ml1[i,]-ML[5])*iipm*ML[5]~==0 ,
        nb_w++;v[nb_w]=i ); );
```

```

new_weights=matrix( nb_w, LieRank+1, i ,j ,
    if (j==1, ML[3][v[i],j] , ML[3][v[i],j]-ML[5][j-1])
        );
dimS=matrank( matrix(nb_w,LieRank,i,j ,
new_weights[i,j+1]) );
for(s=1,dimS ,
for(ss=1,binomial(nb_w,s), \\\ consider (s-1)-simplex sM
    sub=subset(s,ss);
    sM=matrix(s,LieRank,i,j,new_weights[sub[i],j+1]);
if (matrank(sM)==s ,
    candidate=nullproj(sM); \\\ simplex(sM) non degenerate?
if (vecmin(candidate[1])>=0, test=1; \\\ foot in simplex?
if (in_chamber(candidate[2],
    new_pos_roots)==1, \\\ in chamber?
if( f>0, c=f;
    while( c<=child_nb&&test >0,
        if( ist_gleich(list[c][5],
            candidate[2])==1, test=0 );
        c++ );
    );
if( test && dim_cond(new_weights ,new_pos_roots ,
candidate[2],ML[1])==1 ,
    child_nb++;
    if(f==0,f=child_nb); \\\we have a new child
    new_child = [child_nb , ML[1] , new_weights , ML[5] ,
        candidate[2] , new_pos_roots];
    list = concat(list ,[new_child]);
        )))); );\\\4 testing if's, 2 for's .
}

```

The function saturL() enhances the data structures of the children that we have up to this time.

```

saturL()=
{
for( i=1,length(perpLch),
    if( dim_cond(list[1][3],list[1][6] ,
        perpLch[i],1)==1 ,
        child_nb++;
        list=concat( list ,
            [[child_nb ,1 ,list[1][3] ,vector(LieRank) ,
                perpLch[i] ,list[1][6]]]
                    );
        );
    );
}

```

The function non_neg_weights() reduces the number of weights and the number of possible edges of simplices.

```

non_neg_weights()=
{
local(a,v);
\\ we need more global variables:
\\      nb_w
\\      perpLch= list of admissible perpendiculars L
\\      pW
\\      list_edge_cand=
global(nb_w,perpLch,pW,list_edges_cand);
a=matsize(ml)[1]; v=vector(a); nb_w=0;
for( i=1,a,
    if( vecmax(vector(LieRank,j,
        twice_rho[j]*ml[i,j]))>0 ,
        nb_w++;
        v[nb_w]=i );
    );
pW=matrix(nb_w,LieRank,i,j,ml[v[i],j]);
perpLch=vector(0);
list_edges_cand=vector(nb_w);
for( i=1,nb_w, list_edges_cand[i]=Set([]);
for( j=i+1,nb_w,
    if( 1<2, \\ is_non_neg_and_non_pos(pW[i,]-pW[j,]) ,
        list_edges_cand[i]=setunion(list_edges_cand[i],
            Set([j])
        )));
    );
}

```

The function is_non_neg_and_non_pos(v) is used to reduce the number of edges.

```

is_non_neg_and_non_pos(v)=
{
if(vecmin(v) <= 0 && vecmax(v) >= 0, 1, 0)
}
```

The function edges_cand(v) lists given the weight v which weights u can occur in an edge (u,v), i.e., u-v has to be non_neg_and_non_pos.

```

edges_cand(v)=
{
local(res);
```

```

res=list_edges_cand[v[1]];
for(j=2,length(v),
    res=setintersect(res ,list_edges_cand[v[j]])
);
res
}

```

The function stamp(L) helps us to recognize L and to avoid considering L several times.

```

stamp(L)=
{
local(res);
res='''';
for(j=1,length(L), res=if(j<length(L),
    concat([res ,numerator(L[j]), 'a',
    denominator(L[j]), 'b']),
    concat([res ,numerator(L[j]), 'a',
    denominator(L[j])]));
);
res
}

```

The function all_perp() computes the list all children of the first generation with g=mother_nb=1.

```

all_perp ()=
{
local(sM, listperp ,L, signL ,countPerp ,\
z,Z,b,a,C,simplex ,v,d);
listperp=Set ([]);
countPerp=0;
z=vector(nb_w,i ,[[ i ],eval(list_edges_cand[i ])]);
d=sum(i=1,nb_w,length(list_edges_cand[i ]));
for(i=1,nb_w,if( in_chamber(pW[i ,],pos_roots)==1 ,
    countPerp++; print([[ i ],pW[i ,],countPerp ,1]);
    signL=stamp(pW[i ,]);
    listperp=setunion(listperp ,Set([signL]));
    perpLch=concat(perpLch ,[pW[i ,]]));
for( s=2,LieRank ,
    if( s > 2 , Z=C; z=vector(Z,i ,simplex[i ]) ,
        Z=nb_w);
if(s<LieRank , simplex=vector(d));
b=1;C=0;d=0;
while( b<=Z ,

```

```

a=1;v=z[b][2];
while( a<=length(v) ,
cand=concat(z[b][1],[v[a]]);
sM=matrix(s,LieRank,i,j,pW[cand[i],j]);
if( matrank(sM)==s ,
L=nullproj(sM);
signL=stamp(L[2]);
if( s<LieRank , C++;
w=edges_cand(cand);
d=d+length(w);
simplex[C]=[cand, eval(w)];
);
if( vecmin(L[1])>=0 && in_chamber(L[2], pos_roots)==1,
if( setsearch(listperp, signL, 1),
listperp=setunion(listperp, Set([signL]));
countPerp++; print([cand, L[2], countPerp, s]);
perpLch=concat(perpLch, [L[2]]);
));
a++);
b++);
);
}

```

The main function hnc() computes strata given the group g in LiE format, i.e., e.g., A3A2 and the weight vector w = ‘‘X1,0,0,1,0’’ or a formally written ‘‘sum’’ of weight vectors w=‘‘X1,0,1,0,0+X1,0,0,1,0+X1,0,0,0,1’’ in the case of reducible representations.

The quotes ‘‘ ’’ and the X’s are important since we use a shell escape to the LiE script ./PROG/ slie. Some help and examples are given, if one executes

./PROG/ slie without input. See the text of ./PROG/ slie.)

```

hnc(g,w)=
{
local(res);
extern(concat(['./PROG/ slie ',g,' ',w]));
read(''data ''); init_M(MW); res=strata();
\\ uncomment following 2 lines and the
\\ output will appended to ''data<g>x<w>''
\\ and will be formatted.
write(''data '', '''); write(''Number of strata = '',
length(res)/2);

```

```

write(“data”,“”); write(“data”, “[ <Dimension> ,
<Stratum> ]’);
for(i=1,length(res)/2 ,
write(“data”,[res[2*i-1],res[2*i]]));
res
}

dynkin_char(L)=
{
2/(L*iipm*L~)*(L*cantanm);
dc(s)=vector(length(s),i,
if(i%2,dynkin_char(s[i]),s[i]));
}
The function omega2alpha() changes from
omega to alpha base.
omega2alpha(X)=
{
local(Y);
Y=X/cantanm;
matrix( matsize(Y)[1] , matsize(Y)[2]+1 , i , j ,
if(j==matsize(Y)[2]+1,1,Y[i,j]));
}
The function strata() computes admissible
strata from the list
strata()=
{
local(n,t,tB,res0,res1);
saturlist(); t=vector(length(list),i,list[i][2]);
\\ uncomment following 3 lines and the tree t
\\ will formatted and appended to “data<g>”
\\ or data<g>x<w>.
write(“data”,“”);
write(“data”,
“ Tree of candidats for strata given in CAYLEY code :” );
write(“data1”,
vector(length(t),i,if(divrem(i,10)[2]==0,t[i]*BR,t[i])));
);
system(
“sed -f ./PROG/sed_data data1 | cat - >> data;rm data1
”);
n=2; while(n<=length(t)&&t[n]==1,n++);
res0=vector(n-2,i,[list[i+1][5],adm(leaf(t,i+1))]);
res1=[]; for(i=1,n-2,if(res0[i][2]==1,

```

```

res1=concat(res1 ,
[ dimStrata( list[1][3],res0[i][1]), res0[i][1] ))
);

return(res1)
}
adm(t)=
{
local(n);
if(length(t)==0,return(1)); if(length(t)==1,
return(0));
n=1;
while(n<=length(t)&&t[n]==0,
if(adm(leaf(t,n))==1,return(0));n++); return(1);
}
leaf(t,ii)=
{
local(c,s,T,pol,jj);
pol=x-ii;c=0;T=vector(length(t));
s=1; while(s<=length(t),
if(subst(pol,x,t[s])==0, pol=pol*(x-s);c++;
T[c]=[t[s],s]);s++););
vector(c,i,if(t[T[i][1]]==0,0,
for(j=1,i-1,if(T[i][1]==T[j][2],jj=j));jj));
}
The function dimStrata() computes the dimension of
strata.
dimStrata(M,L)=
{
local(ml1,dimO);
dimO=0;
ml1=matrix(matsize(M)[1],length(L),i,j,M[i,j+1]);
for(i=1,matsize(M)[1],
if((ml1[i,]-L)*iipm*L~ >= 0 , dimO=dimO+M[i,1]););
for(i=1,matsize(pos_roots)[1],
if( pos_roots[i,]*iipm*L~ != 0 , dimO++););
dimO
}

```

References

1. The PARI Group, *PARI/GP*, version 2.7.4, Bordeaux, 2015, <http://pari.math.u-bordeaux.fr/>.
2. A Computer Algebra Package for Lie Group Computations, version 2.2.2, Poitiers, <http://wwwmathlabo.univ-poitiers.fr/~maavl/LiE/>.
3. N. Bourbaki, *Groupes et Algèbres de Lie*, Chap. IV, V, VI, Hermann, Paris, 1968.
4. D. H. Collingwood, W. M. McGovern, *Nilpotent Orbits in Semisimple Lie Algebras*, Van Nostrand Reinhold, New York, 1993.
5. V. L. Popov, *Classification of spinors of dimension fourteen*, Trans. Mosc. Math. Soc. **1** (1980), 181–232.
6. L. Le Bruyn, *Nilpotent representations*, J. Algebra **197** (1997), 153–177.
7. V. Gatti, E. Viniberghi, *Spinors of 13-dimensional space*, Adv. in Math. **30** (1978), no. 2, 137–155.

Notation

\hat{A} , 51, 232	(f_1, \dots, f_k) , 1
$\text{ad}(\delta)$, 186	ϕ , 305
$\text{Ad}(\sigma)$, 303	Φ_- , 305
$A(e)$, 19	Φ_+ , 305
α^\vee , 305	$\Phi_\tau(V)$, 84
\mathbb{A}^n , 1	F_R , 259
$\sqrt[p]{A}$, 232	\mathfrak{g} , 184
\mathfrak{b} , 154	\mathbb{G}_a , 36
$\beta(K[V]^G)$, see $\beta(R)$	$\text{Gal}(f)$, 266
$\beta(R)$, 32	\mathfrak{g}_α , 305
$\beta_{\text{sep}}(K[V]^G)$, 139	Γ , 159
\mathfrak{c} , 165	$\gamma(R)$, 216
χ_i , 157	\mathbb{G}_m , 39
χ^V , 202	$G_{p'}$, 84
Δ , 155, 305	G_W , 118
$\bar{\delta}$, 301	G_x , 47
$\Delta(g)$, 34	$\text{hdim}(M)$, 17
$\delta_{\text{gen}}(V)$, 221	$H(K[V]^G, t)$, see $H(V, t)$
Δ^* , 169	$\tilde{H}(K[V], K, t)$, 89
$\delta * \gamma$, 184	$H(R, t)$, see $H(V, t)$
$\delta(V)$, 220	$\text{ht}(I)$, 58
$\text{depth}(I, M)$, 57	$H_T(V, z_1, \dots, z_r, t)$, 202
$\text{depth}(K[V]^G)$, see $\text{depth}(M)$	$H(V, t)$, 18
$\text{depth}(M)$, 58	$I : f$, 11
$\text{depth}(R)$, see $\text{depth}(M)$	$I : f^\infty$, 11
$\det_V^0(1 - t\tau)$, 84	$I(G)$, 156
$\dim(M)$, 58	$I(\Gamma)$, 159
$\dim(R)$, 20	$I : J$, 10
$d\mu$, 198	$I^{[q]}$, 60
ϵ_σ , 184	I^* , 60
$(f_1, \dots, f_k)K[x_1, \dots, x_n]$, 1	i^* , 297
	KG , 72

$K(V)$, 134	$\text{res}(f, a)$, 207
$K[V]$, 32	$\text{Res}(g, h)$, 34
$K[V]_d$, 32	$\mathcal{R}_{G/H}$, 73
$K(V)^G$, 134	ρ , 156
$K[V]_h$, 165	R_+ , 100
$K(X)$, 241	\tilde{R} , 24
$K[X]$, 2	
$K[X]^G$, 32	
$L(A)$, 125	s_α , 305
$\lambda_1, \dots, \lambda_r$, 204	$\sigma \cdot f$, 31
$\text{LC}(f)$, 3	$\sigma_t(V)$, 84
$L(I)$, see $L(S)$	$\text{spol}(f, g)$, 7
$\text{LM}(f)$, 3	$\text{Stab}_G(f)$, 267
$L(S)$, 4	$S(V)$, 119
$\text{LT}(f)$, 3	$\text{Syz}(f_1, \dots, f_k)$, 13
$\text{Mat}_{m,n}(K)$, 156	t , 305
M_{spec} , 126	T_α , 305
m^* , 297	$te_i >_{\mathcal{G}} t'e_j$, 13
$\hat{\mu}$, 169	$T(f)$, 126
$m(V, K)$, 89	$\text{Tr}(A)$, 40
$\text{NF}(f)$, 6	TR_G , 76
\mathcal{N}_V , 55	\mathfrak{u} , 305
$\text{orb}_G(t)$, 126	V_d , 18, 33
π , 45	$V//G$, see $X//G$
$\mathcal{P}^i(f)$, 133	$\mathcal{V}(I)$, see $\mathcal{V}(S)$
$\text{Quot}(R)$, 25	$\mathcal{V}_{\bar{K}}(f_1, \dots, f_n)$, 91
\mathcal{R} , 38	$\mathcal{V}(S)$, 1
R_d , 19	W , 204
$\text{Red}(t)$, 126	$W_C(x, y)$, 281
	$X//G$, 45
	$x_i \gg x_j$, 4

Index

A

- Additive group 36, 44, 254–258, 298
- Affine domain 24
- Affine variety 1
- A_5 -invariants
 - in characteristic 0 103
 - in characteristic 2 89, 90, 96
- Alternating group 67, 266
- Andersen, Kasper 119
- Aronhold xvii
- Artin-Schreier polynomial 274
- Auslander-Buchsbaum formula 113

B

- Baby Noether gap 77
- Bárány 176
- Beta-number 32, 74–83, 106, 129, 139–140, 216–226
 - unchanged under field extension 106
- Bézout's theorem 116
- Bifurcation theory 283
 - equivariant 283
- Binary forms 33–35, 114, 157, 163, 180–182, 191, 197, 201, 206, 209, 223
 - nullcone 55
- Bireflection 99, 142
- Block ordering 4, 8, 252
- Borel subgroup 173, 204, 303
- Bracket invariant 179
- Bracket ring 179
- Brauer character 84, 90
- Braun, Amiram 122

Buchberger's algorithm 7, 13

complexity 7

extended *see* Extended Buchberger algorithm

improvements 7

C

- CAGE 241
- Casimir operator 187
 - for O_n 188
 - for SL_n 187
- Categorical quotient 45, 55, 155, 178, 275, 276
 - geometric properties of 45–48
- Cayley xvii
- Cayley's Ω -process *see* Omega process
- Character 157, 202
- Character theory 85
- Chemistry 285
- Class function 199
- Classical invariant theory xvii, xix
- Clebsch xvii
- Closed orbits 46
- CoCoA 1
- Coding theory 281–283
- Cohen-Macaulay 57–64, 77, 97–101, 106, 111–112, 138, 141, 280
 - counterexample 58
 - counterexample of an invariant ring 98
 - criterion for 111
 - defect 59, 98, 100
 - equivalent properties 58
- Cohomology 99–100, 114, 265–266
 - of A_4 266

- support of 99
- Colon ideal 10–11, 27
- Combinatorics 278–281
- Compact subgroup 38, 198
 - maximal *see* Maximal compact subgroup
- Complete intersection 100, 111, 119, 121, 137, 141, 287
- Computational commutative algebra xix
- Computer algebra systems 1, 71
- Convolution 184, 299
- Coordinate ring 2
- Covariant 86, 98, 167, 172–174
- Cremona xvii
- Cyclic group invariants 79, 98, 113, 130, 280
- D**
- Dade’s algorithm 92
- Database of invariant rings 72
- Dedekind different 121
- Degree
 - of a graded algebra 20, 94, 211
 - of an invariant ring 211
 - of a variety 20, 219
- Degree bound 32, 74–83, 129, 139–140, 216–226
 - Derksen’s *see* Derksen’s degree bound
 - Göbel’s *see* Göbel’s degree bound
 - for modular invariants 78–83, 129, 139–140
 - Noether’s *see* Noether’s degree bound
 - for orbits 219–223
 - Popov’s *see* Popov’s degree bound
 - Richman’s *see* Richman’s degree bound
 - for secondary invariants 66, 129
 - Symonds’ *see* Symonds’ degree bound
 - for tori 224–226
- De Jong’s algorithm 24–28
- Depth 57, 113–114
 - for cyclic groups 113
 - unchanged under integral extensions 113
- Derksen ideal 228, 230, 240–251
- Derksen’s degree bound 217
- Dickson invariants 274
- Differential character 121
- Differential degree 121
- Differential equation 283
- Dimension 2
 - is encoded in Hilbert series 19
 - of an ideal 11
 - of a module 58
- Discriminant 34, 164, 181, 210, 269
- Dixmier map 255
- Dixmier’s conjecture 211
- Dominant weight 173, 306
- Dual code 281
- Dual of $K[G]$ 184–186, 299–303
 - acts on V 301
- Dual representation has different invariants 120
- Dynamical systems 283–285
- E**
- Elementary symmetric polynomials 33, 35, 57, 120, 123, 125, 129, 270, 280
 - polarized 280
- Elimination ideal 8, 26, 228, 275
- Engineering 285
- Equivariant 75, 76, 86, 91, 98, 172, 283
- Extended Buchberger algorithm 8, 14
- Extended Derksen ideal 240–251
- Extended Hilbert series 89, 96
- F**
- Finite generation ideal 259
- First Fundamental Theorem for GL_n 178
- First Fundamental Theorem for SL_n 179
- Fourteenth Hilbert Problem 32
- Free resolution 16–17, 19, 112–113
 - graded *see* Graded free resolution
 - minimal *see* Minimal free resolution
- Fuel tank 285
- Fundamental weights 306
- G**
- Galois theory 112, 266–272
- Generic Hilbert series 88
- Generic polynomial 272–274
- Geometrically reductive 43, 45, 54, 154–156
 - counterexample 44
- Geometrically separating 140
- Geometric quotient 47, 258, 275
- GL_n -invariants 35–36, 178–182
- Global degree bound 81
- G -module 31
- Göbel’s algorithm 125–130
- Göbel’s degree bound 129
- Good quotients 48
- Gordan xvii, 42
- Gorenstein 120–123, 288
- Graded algebra 56, 58, 72, 100, 106, 170
 - standard 266

- Graded free resolution 16, 94, 112, 115
 Graded Gorenstein 121
 Graded lexicographic monomial ordering 3
 Graded monomial ordering 4
 Graded reverse lexicographic monomial ordering 3, 130
 Gram matrix 290
 Graph of the action 141, 246
 Graph theory 276–278
 Grassmann-Plücker relations 179
 G -relative H -invariant 267
 Grevlex-ordering *see* Graded reverse lexicographic monomial ordering
 Grinberg 176
 Gröbner basis 4, 93, 102, 109, 135, 160, 171, 180, 271
 destroys symmetry 275
 existence 4
 over a ring 145
 reduced 6
 of a submodule 13
 truncated 107
 uniqueness 6
 Group ring 72
 Group theoretically reductive *see* Reductive G -variety 31
- H**
- Haar measure 38, 198
 Hartshorne’s connectedness theorem 140, 141
 Head monomial *see* Leading monomial
 Hessian 182
 Highest weight 306
 Highest weight vector 306
 Hilbert *xvii*
 Hilbert ideal 42, 74, 77, 153
 Hilbert-Mumford criterion 55
 Hilbert series *xvii*, 18, 65, 83, 115, 198–215
 computation of 20–22
 for a connected reductive group 204–206
 does not always show degrees of primary invariants 95
 extended 89
 of an invariant ring 66, 94, 101, 115
 for modular invariants 86–89
 of a monomial ideal 21
 multi-graded 280
 of a nonmodular invariant ring *see* Molien’s formula
 for a permutation group 88
 of a polynomial ring 18
 for a torus 202–204
 for a trivial source module 88–89
 Hilbert’s finiteness theorem 41
 converse of 44
 Hilbert’s 14th problem 32
 Hilbert’s nullcone *see* Nullcone
 Hilbert’s syzygy theorem 16, 19
 Hironaka decomposition 66
 Hochster and Eagon
 theorem of 97
 Hochster and Roberts
 converse of theorem of 59
 theorem of 59
 Homogeneous invariants
 computation 182
 Homogeneous system of parameters 19, 54–58, 65, 66, 91, 92, 124, 216, 217
 optimal 93
 Homological dimension 17, 113, 120
 Hughes, Ian 79
 Hypersurface 137, 138, 287
- I**
- Image closure of a morphism 9, 159
 Implementations 71
 Indecomposable projective module 90
 Independent modulo an ideal 12
 Initial ideal *see* Leading ideal
 Initial monomial *see* Leading monomial
 Integral closure *see* Normalization
 Intersection of ideals 10
 INVAR 71
 Invariant 32
 Invariant field 120, 134, 242, 258, 272
 Invariantization 242, 255
 Invariant ring 32
 criterion for generators 134
 finite generation of 32, 36, 42, 44, 72
 localization *see* Localization of the invariant ring
 is normal 50
 polynomiality 115–120, 124, 138
 Invariant theory
 computer algebra packages 71
 Irreducible 2
 Italian problem 245–246
- J**
- Jacobian determinant 117, 122
 Jacobian matrix 135

K

Killing form 186
 King's algorithm 107–109
 k -reflection 100, 142
 Krull dimension 2, 11, 91
 K -weighted graph 276

L

Leading coefficient 3
 Leading ideal 4
 has same dimension 11
 Leading monomial 3
 Leading term 3
 Lexicographic monomial ordering 3, 4, 8,
 124, 130, 160

Lie algebra 184, 299–303
 acts by derivations 303
 for GL_n 185
 for O_n 186
 for SL_n 185

Linear algebraic group 31, 297–299

Linear code 281

Linearly reductive 38–43, 59
 in characteristic 0 43
 equivalent properties 39
 in positive characteristic 44

Localization of the invariant ring 165–169

Locally finite action 299

Locally nilpotent derivation 256

Local slice 255, 260

Luna's slice theorem 166

M

MACAULAY2 1
 MAGMA 1, 71, 88, 94, 103, 105, 109, 114,
 132, 257, 277, 282, 287
 MAPLE 71, 279
 MAS 71
 Material science 285–288
 Maximal compact subgroup 198, 200
 Maximal torus 173, 199, 304
 Membership in an ideal 6
 Minimal basis 273
 Minimal free resolution 16–17, 113
 Minimal set of generators 65, 106
 degrees are unique 106
 Modular case xviii, xx, 72
 Module of covariants 172
 Molien series 85
 Molien's formula 85, 88, 101, 267, 278, 281
 for equivariants 86

evaluation 85
 generalizations 90, 198–202
 for permutation modules 88
 Moment invariants 291–293
 Monomial 2, 13
 regular *see* Regular monomial
 Monomial group 130
 Monomial ordering 3
 Monomial representation 89
 Morphism of affine varieties 2
 Multigraph 277
 Multipartite partitions 279
 Multiplicative group 39, 45, 162, 208, 228,
 240
 Multiplicative invariants 146
 MuPAD 71

N

Nagata's counterexample 36
 Nakayama lemma, graded 100
 Necklace 281
 Newton's formulae 85
 Noether gap 74
 one question still open 77
 Noether Normalization 56, 216
 Noether's degree bound 74–78, 106
 fails in the modular case 79–82
 for separating invariants 139

Noether's problem 272

Nonmodular case 72

Nonreduced algebra 240

Normal form 5, 102, 242
 linearity 6
 not unique 5
 uniqueness 6

Normalization 24, 134

Normalized moments 292

Normal ring 24, 134

Nullcone 50, 55, 154

O

Omega process 193–198
 for SL_2 197
 Orbit space reduction 284
 Orbit variety 275

P

PerMuVAR 71, 277
 p -group 99, 131
 Physics 285
 Poincaré series 18

- Point derivation 300
 Point-wise stabilizer 118, 138, 142
 Polarization 54
 Polarized elementary symmetric polynomials 280
 Popov's degree bound 216
 Positive root 305
 Presentation 10, 109, 135
 Primary decomposition 22
 Primary invariants 56, 83, 91–97
 degrees of 94–97, 132
 geometric criterion 91
 Projective indecomposable character 90
 Projective variety 20
 Pseudo-reflection *see* Reflection
 Purely inseparable closure 51, 232–236
- Q**
- Quasi-affine variety 258
 Quasi-Gorenstein 120
 Queen's University ix
 Quotient ideal 10
- R**
- Radical 304
 Radical computation 22–24
 Radical ideal 2, 22–24
 Radical membership 24, 229
 Rational action 298
 is locally finite 298
 Rational representation 31
 Reduced Gröbner basis 6, 241
 Reductive 37, 43, 303–307
 geometrically *see* Geometrically reductive
 group theoretically *see* Reductive
 linearly *see* Linearly reductive
 typical examples 37
 Reflection 117, 122, *see also* bireflection,
 k -reflection
 Reflection group 115–120, 132, 138,
 140–142, 274, 282
 with nonpolynomial invariants 117,
 119, 133
 Regular action 31, 298
 Regular functions 2
 Regular monomial 181
 Regular sequence 57, 99
 Reinforced composite 285
 Relations between polynomials 9–10, 109,
 134, 284
 Relative invariant *see* Semi-invariant
- Relative Reynolds operator 73, 98
 Representation ring 84, 86
 Residue 207
 Residue Theorem 206–215
 Resolvent 268
 Resolvent form 268
 Resultant 34
 Reynolds operator 38–39, 41, 62, 73, 97,
 102, 183–198
 decomposition for a normal subgroup 184
 for finite groups 38
 for the multiplicative group 39
 relative *see* Relative Reynolds operator
 for semi-simple groups 186–193
 for SL_2 191
 for tori 183
 uniqueness 39
 Richman's degree bound 79–82
 Ring of covariants 173
 Root 204, 305
 positive 305
 simple 305
 Russian Conjecture 227
- S**
- SAGBI basis 125, 130–131, 174
 Saturation ideal 11
 Schreyer's algorithm 16
 Schreyer's monomial ordering 13
 Secondary invariants 56, 83, 100–106
 alternative algorithm 134–136
 modular case 104–106
 nonmodular case 101–103
 number of 111
 Second Fundamental Theorem for GL_n 178
 Second Fundamental Theorem for SL_n 179
 Self-dual code 282
 Semi-algorithm 252
 Semi-invariant 37, 43, 121, 172
 Semi-simple 37, 184, 186–193, 304
 Semi-stable 48
 Separating algebra 48, 139, 292
 Separating invariants 48–54, 139–142,
 228–231, 277, 292
 computation 228–231
 explicit form 139
 Separating subalgebra
 polynomiality 140–142
 Separating subset 48
 geometrically 140
 Separating variety 228
 Shallow 114

- Sigma-series 84
 Simple root 305
SINGULAR 1, 71, 109
 SL_2 -invariants 33–35, 163, 167
 Hilbert series of 200, 206, 209
 SL_3 -invariants 206, 213
 SL_n -invariants 166, 178–182, 222
 Special groups 166
 Special monomial 125, 126
 s-polynomial 7, 13
 Standard graded algebra 266
 Star 289
 Steenrod operations 133
 Straightening 180
 Support of cohomology 99
 Sylvester xvii
 Symbolic method 180
 Symmetric algebra 119
 Symmetric group 33, 103, 119, 123, 158, 277, 280
 action on 2-subsets 277
 vector invariants 280
SYMMETRY 71
 Symonds' degree bound 82–83, 129
 Symplectic group 119
 System of parameters
 homogeneous *see* Homogeneous system of parameters
 Systems of algebraic equations 275–276
 Syzygies 13–17, 109–111
 of a Gröbner basis 14
 Syzygy module 10, 13–17, 144
 computation 13–15
 Syzygy theorem *see* Hilbert's syzygy theorem
- T**
- Tame CAGE 241
 Tamely extended 241
 Tangent space 300
 Term 2
- Term order *see* Monomial ordering
 Theology 42
 T -Hilbert series 202
 Tight closure 60
 Top-reduction 6
 Torus invariants 131, 163, 174–177, 224–226
 Transfer 76
 Trivial source module 77, 88–89
 Truncated Gröbner basis 107
 Tschirnhaus transformation 267
- U**
- Ulam's conjecture 277–278
 Unipotent endomorphism 304
 Unipotent group 304
 Unipotent radical 43, 304
- V**
- Variety
 affine *see* Affine variety
 Vectorial polynomial 272
 Vector invariants 77, 79–82, 99
 Vogel, Denis 114
- W**
- Weight 37, 157, 204
 Weighted degree 3
 Weight enumerator 281
 Weitzenböck Theorem 37
 Weyl group 204, 305
 Weyl's integral formula 205
 Weyl's polarization theorem 54, 74
 Weyl's Theorem 204, 307
- Z**
- Zacharias ring 146, 245
 Zariski topology 2