

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

popovvl@mi.ras.ru

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

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 |