

Encyclopaedia of Mathematical Sciences
Volume 139

Invariant Theory and Algebraic Transformation Groups VIII

Subseries Editors:

Revaz V. Gamkrelidze Vladimir L. Popov

H.E.A. Eddy Campbell • David L. Wehlau

Modular Invariant Theory

 Springer

H.E.A. Eddy Campbell
University of New Brunswick
Sir Howard Douglas Hall
Dept. Mathematics
Bailey Drive 3
Fredericton, New Brunswick
Canada E3B 5A3
heac@unb.ca

David L. Wehlau
Royal Military College of Canada
Dept. Mathematics & Computer Science
Kingston, Ontario
Canada K7K 7B4
wehlau@rmc.ca

Founding editor of the Encyclopaedia of Mathematical Sciences: Revaz V. Gamkrelidze

ISSN 0938-0396

ISBN 978-3-642-17403-2

e-ISBN 978-3-642-17404-9

DOI 10.1007/978-3-642-17404-9

Springer Heidelberg Dordrecht London New York

Mathematics Subject Classification (2010): 13A50

© Springer-Verlag Berlin Heidelberg 2011

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilm or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, 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.

Cover design: deblik

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

For Diane Mary Brennan, Ian Alexander Brennan, Colin Cameron Brennan,
Graham Harold James Brennan and Maggie Orion Cameron.

For Charlene Lynn Janeway and Megan Melinda Jane Wehlau.

Preface

At the time we write this book there are several excellent references available which discuss various aspects of modular invariant theory from various points of view: Benson [6]; Derksen and Kemper [26]; Neusel [85]; Neusel and Smith [86]; and Smith [103]. In this book, we concentrate our attention on the modular invariant theory of finite groups. We have included various techniques for determining the structure of and generators for modular rings of invariants, while attempting to avoid too much overlap with the existing literature. An important goal has been to illustrate many topics with detailed examples. We have contrasted the differences between the modular and non-modular cases, and provided instances of our guiding philosophies and analogies. We have included a quick survey of the elements of algebraic geometry and commutative algebra as they apply to invariant theory. Readers who are familiar with these topics may safely skip this chapter.

We wish to thank our principal collaborators over the years with whom we have had so much pleasure exploring this fascinating subject: Ian Hughes, Gregor Kemper, R. James Shank, John Harris as well as our students and friends, Jianjun Chuai, Greg Smith, Mike Roth, Brandon Fodden, Emilie Dufresne, Asia Matthews and Chester Weatherby. In particular we thank John Harris, R. James Shank, Jianjun Chuai, Mike Roth, Emilie Dufresne, Asia Matthews, Chester Weatherby and Tristram Bogart for reading draft chapters and pointing out errors and suggesting improvements. We also thank Marie-José Bertin for clarifying the history of her own work to us.

Finally, our thanks go to the anonymous referees for many helpful and constructive remarks.

Fredericton, New Brunswick
Kingston, Ontario
August 2010

H. E. A. Eddy Campbell
David L. Wehlau

Contents

1	First Steps	1
1.1	Groups Acting on Vector Spaces and Coordinate Rings	2
1.1.1	V Versus V^*	4
1.2	Constructing Invariants	6
1.3	On Structures and Fundamental Questions	7
1.4	Bounds for Generating Sets	7
1.5	On the Structure of $\mathbb{K}[V]^G$: The Non-modular Case	8
1.6	Structure of $\mathbb{K}[V]^G$: Modular Case	9
1.7	Invariant Fraction Fields	10
1.8	Vector Invariants	11
1.9	Polarization and Restitution	11
1.10	The Role of the Cyclic Group C_p in Characteristic p	16
1.11	C_p Represented on a 2 Dimensional Vector Space in Characteristic p	17
1.12	A Further Example: C_p Represented on $2V_2$ in Characteristic p	20
1.13	The Vector Invariants of V_2	23
2	Elements of Algebraic Geometry and Commutative Algebra	25
2.1	The Zariski Topology	25
2.2	The Topological Space $\text{Spec}(S)$	27
2.3	Noetherian Rings	27
2.4	Localization and Fields of Fractions	29
2.5	Integral Extensions	29
2.6	Homogeneous Systems of Parameters	30
2.7	Regular Sequences	31
2.8	Cohen-Macaulay Rings	32
2.9	The Hilbert Series	34
2.10	Graded Nakayama Lemma	35
2.11	Hilbert Syzygy Theorem	36

3	Applications of Commutative Algebra to Invariant Theory	39
3.1	Homogeneous Systems of Parameters	40
3.2	Symmetric Functions	44
3.3	The Dickson Invariants	45
3.4	Upper Triangular Invariants	46
3.5	Noether's Bound	46
3.6	Representations of Modular Groups and Noether's Bound	48
3.7	Molien's Theorem	50
3.7.1	The Hilbert Series of the Regular Representation of the Klein Group	51
3.7.2	The Hilbert Series of the Regular Representation of C_4	53
3.8	Rings of Invariants of p -Groups Are Unique Factorization Domains	54
3.9	When the Fixed Point Subspace Is Large	55
4	Examples	59
4.1	The Cyclic Group of Order 2, the Regular Representation	61
4.2	A Diagonal Representation of C_2	62
4.3	Fraction Fields of Invariants of p -Groups	62
4.4	The Alternating Group	64
4.5	Invariants of Permutation Groups	65
4.6	Göbel's Theorem	66
4.7	The Ring of Invariants of the Regular Representation of the Klein Group	69
4.8	The Ring of Invariants of the Regular Representation of C_4	72
4.9	A 2 Dimensional Representation of C_3 , $p = 2$	75
4.10	The Three Dimensional Modular Representation of C_p	75
4.10.1	Prior Knowledge of the Hilbert Series	76
4.10.2	Without the Use of the Hilbert Series	78
5	Monomial Orderings and SAGBI Bases	83
5.1	SAGBI Bases	85
5.1.1	Symmetric Polynomials	89
5.2	Finite SAGBI Bases	91
5.3	SAGBI Bases for Permutation Representations	93
6	Block Bases	99
6.1	A Block Basis for the Symmetric Group	101
6.2	Block Bases for p -Groups	103
7	The Cyclic Group C_p	105
7.1	Representations of C_p in Characteristic p	105
7.2	The C_p -Module Structure of $\mathbb{F}[V_n]$	110
7.2.1	Sharps and Flats	110
7.3	The C_p -Module Structure of $\mathbb{F}[V]$	113

7.4	The First Fundamental Theorem for V_2	115
7.4.1	Dyck Paths and Multi-Linear Invariants	117
7.4.2	Proof of Lemma 7.4.3	122
7.5	Integral Invariants	124
7.6	Invariant Fraction Fields and Localized Invariants	130
7.7	Noether Number for C_p	132
7.8	Hilbert Functions	138
8	Polynomial Invariant Rings	141
8.1	Stong's Example	147
8.2	A Counterexample	148
8.3	Irreducible Modular Reflection Groups	149
8.3.1	Reflection Groups	150
8.3.2	Groups Generated by Homologies of Order Greater than 2	151
8.3.3	Groups Generated by Transvections	151
9	The Transfer	153
9.1	The Transfer for Nakajima Groups	164
9.2	Cohen-Macaulay Invariant Rings of p -Groups	170
9.3	Differents in Modular Invariant Theory	173
9.3.1	Construction of the Various Different Ideals	174
10	Invariant Rings via Localization	179
11	Rings of Invariants which are Hypersurfaces	185
12	Separating Invariants	191
12.1	Relation Between $\mathbb{K}[V]^G$ and Separating Subalgebras	195
12.2	Polynomial Separating Algebras and Serre's Theorem	198
12.3	Polarization and Separating Invariants	201
13	Using SAGBI Bases to Compute Rings of Invariants	205
14	Ladders	211
14.1	Group Cohomology	213
14.2	Cohomology and Invariant Theory	214
	References	223
	Index	231

Index of notations

\mathbb{N}	the natural numbers, including 0.
\mathbb{Z}	the integers.
\mathbb{Q}	the rational numbers.
\mathbb{R}	the real numbers.
\mathbb{C}	the complex numbers.
\mathbb{F}	a field of characteristic $p \neq 0$.
\mathbb{F}^\times	$\mathbb{F} \setminus \{0\}$.
\mathbb{F}_p	the prime field of order p .
\mathbb{K}	a field of arbitrary characteristic.
$\overline{\mathbb{K}}$	the algebraic closure of \mathbb{K} .
\otimes	$\otimes_{\mathbb{K}}$ or $\otimes_{\mathbb{F}}$.
V	a vector space over \mathbb{F} or \mathbb{K} , most often of dimension n .
$\mathrm{GL}(V)$	the general linear group of V .
$\mathrm{GL}_n(\mathbb{K})$	the linear automorphisms of \mathbb{K}^n .
$\mathrm{SL}(V)$	the special linear group of V .
$\mathrm{SL}_n(\mathbb{K})$	the linear automorphisms of \mathbb{K}^n of determinant 1.
G	a group, often a subgroup of $\mathrm{GL}(V)$.
σ, τ	group elements.
$\sigma(v), \sigma \cdot v$	2 the image $v \in V$ under the action of σ .
V^G	2 the subspace of V fixed (point-wise) by the action of G .
G_X	2 the stabilizer or isotropy subgroup of $X \subset V$.
G_v	2 the stabilizer or isotropy subgroup of $v \in V$.
V^*	the hom-dual $\mathrm{hom}_{\mathbb{K}}(V, \mathbb{K})$.
x^I	3 the monomial $x_1^{i_1} \cdots x_n^{i_n}$ for $I = (i_1, \dots, i_n)$.
$\mathbb{F}[V]$	3 the coordinate ring of V .
$\mathbb{F}[V]^G$	4 the invariant ring.
$\mathrm{Tr}_G(f)$	6 the trace of $f \in \mathbb{F}[V]$.
$\mathrm{Tr}_H^G(f)$	6 the trace of $f \in \mathbb{F}[V]$ relative to a subgroup $H \subset G$.
$\mathrm{N}(f)^G$	6 the norm of f .
$\mathrm{N}_H^G(f)$	7 the norm of f relative to a subgroup $H \subset G$.
Gf	7 the orbit of f under G , i.e., $Gf := \{\sigma(f) \mid \sigma \in G\}$.
$\beta(G, V)$	8 the Noether degree bound for the invariant ring.
$ G $	the order of G .
V^σ	8 the elements of V fixed by σ .
$\mathbb{K}(V)^G$	10 the field of fractions of $\mathbb{K}[V]^G$.
$\mathrm{Quot}(\mathbb{K}[V]^G)$	10 the field of fractions of $\mathbb{K}[V]^G$.
mV	11 the vector space $V^{\oplus m}$.
$\mathcal{P}\mathrm{ol}$	11 polarization.
\mathcal{R}	11 restitution.
$\mathrm{deg}_y(f)$	18 the degree of f in the variable y .
Δ_σ	22 the twisted derivation $\sigma - 1$.
$\mathcal{V}(T)$	26 the zero-set of the polynomials in T .
$\mathcal{I}(X)$	26 the ideal of the variety or set X .

\sqrt{I}	26	the radical of the ideal I .
$\text{Spec}(S)$	27	the space of all prime ideals of S .
$\text{MaxSpec}(S)$	27	the space of all maximal prime ideals of S .
R		a graded commutative ring with 1.
R_f	29	the localization of R at f .
$\mathcal{H}(R, \lambda)$	34	the Hilbert series of R .
$V//G$	42	the quotient variety.
$(V//G)_{\text{good}}$	56	the “good” locus.
$\text{LM}(f)$	83	the lead monomial of f (with respect to some ordering).
$\text{LT}(f)$	83	the lead term of f .
$\text{LT}(R)$	85	the lead term algebra of R .
$\mathbb{K}[V]_G$	99	the ring of coinvariants.
$G_a(\mathbb{C})$	125	the additive group of \mathbb{C} .
$\text{RL}_n(\mathbb{F})$	150	the subgroup of $\text{GL}_n(\mathbb{F})$ generated by its reflections.
$\text{GU}_n(\mathbb{F})$	150	the unitary group of dimension n over \mathbb{F} .
$\text{RU}_n(\mathbb{F})$	150	the subgroup of $\text{GU}_n(\mathbb{F})$ generated by its reflections.
$\text{GO}_n(\mathbb{F})$	150	the general orthogonal group over \mathbb{F} .
$\text{SO}_n(\mathbb{F})$	150	the special orthogonal group over \mathbb{F} .
$\Omega_n^\pm(\mathbb{F})$	150	the commutator subgroup of $\text{GO}_n(\mathbb{F})$.