THEORY OF ALGEBRAIC INVARIANTS

THEORY OF ALGEBRAIC INVARIANTS

DAVID HILBERT
translated by Reinhard C. Laubenbacher
New Mexico State University
edited by Reinhard C. Laubenbacher and Bernd Sturmfels
with an introduction by Bernd Sturmfels
Cornell University

CAMBRIDGE
UNIVERSITY PRESS

Published by the Press Syndicate of the University of Cambridge
The Pitt Building, Trumpington Street, Cambridge CB2 1RP
40 West 20th Street, New York, NY 10011-4211, USA
10 Stamford Road, Oakleigh, Melbourne 3166, Australia

First published 1993
Reprinted 1994

Printed in the United States of America

Library of Congress cataloguing in publication data

Hilbert, David, 1862–1943.

Theory of algebraic invariants / David Hilbert ; translated by Reinhard C. Laubenbacher ; edited and with an introduction by Bernd Sturmfels.
p. cm.

Includes bibliographical references.

ISBN 0-521-44457-8. – ISBN 0-521-44903-0 (pbk.)

1. Invariants. I. Sturmfels, Bernd. II. Title.
QA201.H716 1993
512′.5–dc20 93-15650
CIP

A catalog record of this book is available from the British Library.

ISBN 0-521-44457-8 hardback
ISBN 0-521-44903-0 paperpack

Contents

Cambridge University Press
978-0-521-44903-8 - Theory of Algebraic Invariants
David Hilbert
Frontmatter
More information

Preface

Around the turn of the century, the University of Göttingen was a Mecca for mathematicians and students from around the world, including the United States. Besides Hilbert, who held Gauss's chair, the other three chairs were held by Klein, Minkowski, and Runge. The visitors took back with them a large number of handwritten lecture notes, some of which eventually found their way into mathematics libraries of several U.S. universities. The present notes of Hilbert's 1897 course on invariant theory comprise 527 handwritten pages, taken by Hilbert's student Sophus Marxsen, who went on to write a dissertation in invariant theory. As part of the estate of John Henry Tanner they were given to the Cornell University Mathematics Library.

The project to translate these notes and make them more widely available was suggested by Keith Dennis. Without his initiative and continuing support this translation would not have been undertaken. Steve Rockey at the Cornell University Mathematics Library was also very helpful. Finally, many thanks are due to the late Eleanor York for her expert typing of the manuscript.

The photograph on the cover of Hilbert in his family surroundings is from the collection of Keith Dennis, who kindly permitted its reproduction. Thanks are also due to Stephen R. Singer for his expert reproduction of the less than perfect original.

Reinhard C. Laubenbacher

Introduction

In the summer semester 1897 David Hilbert gave an introductory course in invariant theory at the University of Göttingen. The present text is an English translation of the handwritten course notes taken by Hilbert's student Sophus Marxsen.

When Hilbert gave this course in 1897, his research in invariant theory had been completed. In particular, Hilbert's famous Finiteness Theorem had been proved and published in two striking papers (Hilbert 1890, 1893).* These papers changed the course of invariant theory dramatically, and they laid the foundation for modern commutative algebra. Thus 1897 was a perfect time for Hilbert to give an introduction to invariant theory, taking into account both the old approach of his predecessors and his new ideas. It is this bridge from nineteenth-century mathematics into twentieth-century mathematics which makes these course notes so special and distinguishes them from other treatments of invariant theory.

Hilbert's course is at a level accessible to graduate students in mathematics. Prerequisites include familiarity with linear algebra and the basics of ring theory and group theory. The text provides a self-contained introduction to classical invariant theory, and it will be of interest to anyone who wishes to study this subject. But we believe that this translation will also be valuable as a historical source for experts in contemporary invariant theory. Mathematicians and computer scientists who are interested in algorithmic aspects of invariant theory can read the present notes in parallel with Sturmfels (1993).

Let us attempt to answer the question, "What is invariant theory?" A nineteenth-century mathematician might have answered, "Invariant theory is *the* bridge between algebra and geometry." This point of view

* For English translations of Hilbert's research papers in invariant theory see M. Ackerman (1978).

found its most explicit expression in Felix Klein's Erlangen Programm (Klein 1872). Today invariant theory is often understood as a common branch of representation theory, algebraic geometry, commutative algebra, and algebraic combinatorics. Each of these four disciplines has roots in nineteenth-century invariant theory. This will become evident from Hilbert's course.

The standard references to today's invariant theory include, among others, Dieudonné and Carell (1971), Springer (1977), and Mumford and Fogarty (1982). In modern terms, the basic problem of invariant theory can be characterized as follows. Let V be a K-vector space on which a group G acts linearly. In the ring of polynomial functions $K[V]$ consider the subring $K[V]^G$ consisting of all polynomial functions on V which are invariant under the action of the group G. The basic problem is to describe the invariant ring $K[V]^G$. In particular, we would like to know whether $K[V]^G$ is finitely generated as a K-algebra and, if so, to give an algorithm for computing generators.

Hilbert essentially proved the following theorem (see Section II.2 of this text): If G is a reductive algebraic group, then $K[V]^G$ is finitely generated as a K-algebra. A minimal set of generators is called a full system of invariants. Recall that a group G is *reductive* if all its linear representations are direct sums of irreducible representations. After Hilbert's complete solution to this outstanding problem of invariant theory, the field was pronounced dead, only to be resurrected thirty years later by the work of Hermann Weyl (1939), in which invariant theory was developed for all classical Lie groups. Weyl developed invariant theory as a special instance of representation theory.

A famous problem, left open by both Hilbert and Weyl, asked whether the Finiteness Theorem continues to hold for every subgroup of the general linear group $GL_m(\mathbf{C})$. It is known as Hilbert's fourteenth problem. In 1959 Nagata answered this question by giving an example of a (nonreductive) group G acting linearly on a vector space V such that $K[V]^G$ is not finitely generated. Popov (1979) extended Nagata's work by proving the following remarkable converse to Hilbert's Finiteness Theorem: For every nonreductive algebraic group G there exists a finitely-generated reduced k-algebra A and a rational action of G on A by k-automorphisms such that A^G is not finitely generated. Another important result in today's invariant theory is the theorem of Hochster and Roberts (1974), which states that the invariant ring $k[V]^G$ is Cohen-Macaulay, provided K has characteristic zero and G is reductive.

Classical invariant theory is concerned with the following special case: the group G is the group $GL_m(\mathbf{C})$ of invertible complex $m \times m$-matrices, acting by linear substitution on a space V of m-ary forms, that is, homogeneous polynomials in m variables. In fact, in Hilbert's course most of the discussion centers around the $m = 2$ case of binary forms. For a complementary point of view on the invariant theory of binary forms we refer to the exposition of Kung and Rota (1984).

We now give a summary of Hilbert's course. In Section I.1 he introduces the space $V = S^n\mathbf{C}^m$ of m-ary n-forms, that is, homogeneous polynomials of degree n in m variables. It is proved that this complex vector space has dimension $\binom{n+m-1}{n}$. The group $GL_m(\mathbf{C})$ acts on $S^n\mathbf{C}^m$ by linear substitutions, which amounts to the nth symmetric power representation. Starting with Section I.2, Hilbert specializes to the case $m = 2$. It is proved that $GL_2(\mathbf{C})$ is generated by diagonal matrices $\begin{pmatrix}\kappa & 0\\ 0 & \lambda\end{pmatrix}$, lower triangular matrices $\begin{pmatrix}1 & 0\\ \mu & 1\end{pmatrix}$, and upper triangular matrices $\begin{pmatrix}1 & \nu\\ 0 & 1\end{pmatrix}$. The concepts of invariants and covariants are introduced in Section I.3.

Let $a_0, a_1, \ldots, a_n$ and x_1, x_2 be coordinates on $S^n\mathbf{C}^2$ and $\mathbf{C}^2$, respectively. A *covariant* is a polynomial $I(a_0, a_1, \ldots, a_n; x_1, x_2)$ which is fixed under the action of any matrix $T \in GL_2(\mathbf{C})$, up to a factor $\det(T)^p$. If I depends only on $a_0, a_1, \ldots, a_n$, then it is called an *invariant*. The number p is called the *weight* of the co- or invariant. It is extremely important to note that here $GL_2(\mathbf{C})$ acts on $\mathbf{C}^2$ by the contragredient (or inverse) representation (cf. Springer 1977, §3.1). Otherwise the whole concept of "covariants" does not make sense. The essence of this point is expressed in Hilbert's statement, "The simplest covariant is the form f itself," at the end of Section I.3.

The action of the group $GL_2(\mathbf{C})$ gives rise to an action of the Lie algebra $sl_2(\mathbf{C})$ on the space $S^n\mathbf{C}^2$ of binary n-forms. The two Lie algebra generators corresponding to the lower- and upper-triangular matrices are denoted $\mathbf{D}$ and $\mathbf{\Delta}$. In Section I.4 it is shown that invariants are annihilated by $\mathbf{D}$ and $\mathbf{\Delta}$. This characterizes invariants among all polynomials in $a_0, a_1, \ldots, a_n$ which are invariant under the action of the diagonal matrices only. A similar criterion is proved for covariants. In Section I.5 we see that in this criterion any one of the two conditions $\mathbf{D}I = 0$ and $\mathbf{\Delta}I = 0$ is implied by the other, and hence can be omitted. In order to show this, Hilbert proves the commutation relation

$$(\mathbf{D\Delta} - \mathbf{\Delta D})\mathcal{A} = (ng - 2p)\mathcal{A}$$

for the action of the Lie algebra generators on the space of polynomials in $a_0, \ldots, a_n$ of degree g and weight p. We refer to Serre (1987, Chapter IV) for an introduction to the representation theory of the Lie algebra $sl_2(\mathbf{C})$.

The action of the Lie algebra generators $\mathbf{D}$ and $\mathbf{\Delta}$ leads in Section I.6 to the "smallest system of conditions for the determination of invariants and covariants." Every covariant can be written as

$$C(a_0, \ldots, a_n; x_1, x_2) \quad = \quad \sum_{i=0}^{m} C_i(a_0, \ldots, a_n)\, x_1^{m-i} x_2^i.$$

The leading coefficient C_0 is called the *source* of the covariant. The main result in Section I.6 is that the following system of differential equations characterizes covariants:

$$\mathbf{D}C_i \quad = \quad i\, C_{i-1} \qquad (i = 1, \ldots, m).$$

These equations imply in particular that each covariant is determined by its source.

Section I.7 is concerned with the Hilbert series of the rings of invariants and covariants. A self-contained introduction is given to the enumerative calculus of Cayley and Sylvester. It is similar to the presentation in Springer (1977). In Section I.8 the concept of *transvections* is introduced. It is proved that each covariant of a binary form f can be expressed as a polynomial in the transvections $f_1, \ldots, f_n$, divided by a suitable power of f itself. Several applications are given, including the determination of the complete system of covariants for the binary quartic. The natural generalization of the concept of invariants and covariants to several base forms is presented in Section I.9. In Section I.10 Hilbert introduces three procedures for generating new covariants from old ones. The first one is the remarkable statement: "Covariants of covariants are again covariants." The other two are the *polarization process* and the *Aronhold process*.

So far invariants and covariants were always represented explicitly as polynomials in $a_0, \ldots, a_n; x_1, x_2$. The last three sections of Part I are concerned with three alternative representations. In Section I.11 we think of (the roots of) a binary form of degree n as an unordered collection of n points on the complex projective line. This allows us to express each covariant as a symmetric function in the coordinates of these n points. The other two representations, in terms of one-sided derivatives (Section I.12) and using the symbolic method (Section I.13), are of historic interest, but they are less important for what follows in Part II of Hilbert's course.

The symmetric function representation of Section I.11 leads to a direct proof of Hilbert's Finiteness Theorem in the case of binary forms. This proof, which is also due to Hilbert, is given in Section II.1. See Sturmfels (1993, Section 3.7) for an alternative presentation of the same proof. The key lemma for this proof is the existence of a finite *Hilbert basis* for a system of linear equations over the natural numbers. Today this lemma is foundational for the theory of integer programming (Schrijver 1977). In Section II.1 of Hilbert's course we can fully appreciate the purpose for which "Hilbert bases" were invented.

The Finiteness Theorem for binary forms is due to Gordan (1868). Gordan's original proof gave an explicit construction of the complete system of invariants based on transvections and the symbolic method, but it is much more complicated than the one given in Section II.1. However, both Gordan's proof and Hilbert's proof in Section II.1 do not generalize to forms in $m \geq 3$ variables. The "generalizable proof" is presented in Section II.2. This is the proof which in 1890 shocked the invariant theory community. It is based on an averaging operator, called *Cayley's* Ω*-process*, and another key lemma, called *Hilbert's Basis Theorem* for polynomial ideals. This proof works in full generality, but it is not constructive.

The remaining sections of the course are based on Hilbert's 1893 paper "On the complete system of invariants." In this paper Hilbert essentially gives an explicit algorithm for computing a full system of invariants. In Section II.3 Hilbert discusses the relation between the ring of invariants and the field of invariant rational functions. He proves that the invariant ring is a unique factorization domain, and that it coincides with the intersection of the invariant field with the polynomial ring $\mathbf{C}[V]$.

The material presented in Section II.4 is fundamental both for Hilbert's algorithm and for geometric invariant theory (Mumford and Forgarty 1982). The vanishing locus of all homogeneous invariants is called the *nullcone*. The forms lying in the nullcone are called *nullforms*. The main theorem in Section II.4 states that, if $I_1, \ldots, I_k$ are any invariants which define the nullcone set-theoretically, then the invariant ring $\mathbf{C}[V]^G$ is integral over $\mathbf{C}[I_1, \ldots, I_k]$. The algorithmic significance of this result is explained in Sturmfels (1993, Section 4.6). The key lemma in the proof of this main theorem is *Hilbert's Nullstellensatz*. It is the very purpose for which the Nullstellensatz was first invented. Several applications of the main theorem to binary forms are given.

In Section II.5 Hilbert gives a more precise combinatorial description of the ternary nullforms. They are precisely those ternary forms f such that after a suitable linear transformation, the Newton polygon of f does not contain the origin. The geometric meaning of a ternary form being a nullform is that the planar curve $\{f = 0\}$ has certain types of singularities, which makes the curve *unstable*. This example is the point of departure in Mumford and Fogarty (1982). In geometric invariant theory the concept of stability (= lying outside the nullcone) is extended to arbitrary projective varieties, and, as the main application, certain moduli spaces are constructed.

Section II.6 deals with *Hilbert's Syzygy Theorem*. In modern language this theorem states that the polynomial ring $\mathbf{C}[x_1, \ldots, x_n]$ has *global dimension* n, that is, every module over the polynomial ring admits a finite free resolution of length at most n. The Syzygy Theorem is applied to prove the fact that the Hilbert series of the invariant ring is a rational function. In commutative algebra this is sometimes called the *Hilbert-Serre Theorem* (cf. Atiyah and Macdonald 1969, Theorem 11.1).

In the last three sections, II.7–9, Hilbert discusses applications of invariant theory to (algebraic) geometry, and he outlines future directions. Some of Hilbert's questions have received an answer during the past century (notably, Nagata's solution to Hilbert's fourteenth problem). Other classical questions are still open, and many new questions arise from the increasing demand for invariant theory as a tool in applied mathematics. These questions guarantee the future of invariant theory as an exciting area of research in mathematics.

References

Ackerman, M. (1978). *Hilbert's Invariant Theory Papers.* Math Sci Press, Brookline, Mass.

Atiyah, M. F., and Macdonald, I. G. (1969). *Introduction to Commutative Algebra.* Addison-Wesley, Reading, Mass.

Dieudonné, J., and Carell, J. B. (1971). *Invariant Theory – Old and New.* Academic Press, New York.

Gordan, P. (1868). Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Funktion mit numerischen Coefficienten einer endlichen Anzahl solcher Formen ist. *J. Reine und Angewandte Mathematik* **69**, 323–54.

Hilbert, D. (1890). Über die Theorie der algebraischen Formen. *Math. Annalen* **36**, 473–531 (also: "Gesammelte Abhandlungen," II, 199–257, Springer, 1970).

Hilbert, D. (1893). Über die vollen Invariantensysteme. *Math. Annalen*

42, 313–70 (also: "Gesammelte Abhandlungen," II, 287–344, Springer, 1970).

Hochster, M., and Roberts, J. (1974). Rings of invariants of reductive groups acting on regular rings are Cohen-Macauley. *Advances in Math.* **13**, 115–75.

Klein, F. (1872). Vergleichende Betrachtungen über neue geometrische Forschungen. Programm zum Eintritt in die philosophische Fakultät und den Senat der Universität zu Erlangen. A Deichert, Erlangen.

Kung, J. P. S., and Rota, G.-C. (1984). The invariant theory of binary forms. *Bulletin Amer. Math. Soc.* **10**, 27–85.

Mumford, D., and Fogarty, F. (1982). *Geometric Invariant Theory* (2nd Edition). Springer, New York.

Nagata, M. (1959). On the 14th problem of Hilbert. *American J. Math.* **81**, 766–72.

Popov, V. L. (1979). Hilbert's theorem on invariants. *Soviet Math. Doklady* **249**, 551–5.

Schrijver, A. (1986). *Theory of Linear and Integer Programming.* Wiley-Interscience, Chichester.

Serre, J.-P. (1987). *Complex semisimple Lie algebras.* Springer, New York.

Springer, T. A. (1977). *Invariant Theory.* Lecture Notes in Mathematics **585**. Springer, Heidelberg.

Sturmfels, B. (1993). *Algorithms in Invariant Theory.* Springer-Verlag, Vienna, to appear.

Weyl, H. (1939). *The Classical Groups – Their Invariants and Representations.* Princeton University Press.

Bernd Sturmfels