INVARIANT THEORY

JOHN FOGARTY

W. A. BENJAMIN, INC.

INVARIANT THEORY

JOHN FOGARTY

University of Pennsylvania

W. A. BENJAMIN, INC.

New York Amsterdam

1969

INVARIANT THEORY

Library of Congress Catalog Card Number 79-81997
Manufactured in the United States of America
12345M32109

The manuscript was put into production on March 1, 1969;
this volume was published on May 1, 1969

W. A. BENJAMIN, INC.
New York, New York 10016

PREFACE

The present notes are devoted to a reasonably exhaustive discussion of the basic qualitative problem of algebraic invariant theory, viz., given a ring R and a group G of automorphisms of R, to describe the ring of G-invariant elements of R. In particular, if R is a finitely generated commutative algebra over the field k and each element of G leaves the elements of k fixed, then is the ring of invariants also a finitely generated algebra over k? This is essentially the famous fourteenth problem of Hilbert. We shall not concern ourselves with the quantitative aspects of the problem, e.g., given generators and relations for R, to obtain the same for the ring of invariants.

Why should one be interested in such a problem, aside from its intrinsic simplicity and natural appeal? One reason is that it is closely related to what might be called the classification problem. This can be stated in very general terms as follows. Given a collection of mathematical objects of a certain type, and a well defined notion of 'equivalence' or 'isomorphism' between these objects, can one find a natural mathematical structure for the set of isomorphism classes of objects of the

given type?

Let us look quickly at one example. By an algebra over the field k we mean a vector space A over k, plus a bilinear mapping $M : A \times A \to A$. Suppose we seek to classify all algebras of dimension d over k, up to isomorphism. Clearly we may fix the underlying vector space A. Then the set of all algebra structures on A is simply the vector space of all k-bilinear maps from $A \times A$ to A. Two such structures M' and M'' are isomorphic if and only if there is a k-linear isomorphism $T : A \to A$ such that $M'(Tx,Ty) = T(M''(x,y))$, for all $x,y \in A$.

If B denotes the space of bilinear maps from $A \times A$ to A and $GL(A)$ the group of k-linear automorphisms of A, then $GL(A)$ acts by linear transformations on B via: $M^T(x,y) = M(Tx,Ty)$, $T \in GL(A)$, $M \in B$. The isomorphism classes of such structures are then in bijective correspondence with the orbits of this action of $GL(A)$ on B. The problem now becomes one of finding a 'reasonable' structure for the set of orbits.

If R is the ring of polynomial functions on B - the symmetric algebra of B^* - then the elements of R invariant under the induced action of $GL(A)$ on R can be regarded as functions on the set of orbits. The problem of invariants and the orbit space problem are thus intimately related.

The first chapter is a utilitarian introduction to affine algebraic geometry over an algebraically closed field. Because we confine ourselves to affine geometry, we must leave aside the relation of invariant theory to projective geometry. In any case, the latter theory deserves a volume to itself.

The second chapter is more detailed, vis-a-vis its subject matter - affine algebraic groups - than the first. We obtain some fairly deep general results on these groups, e.g., we construct the quotient of an affine group by a closed normal subgroup. This quotient turns out to be itself an affine group - a highly non-trivial result requiring invariantive methods for its proof.

In the foregoing chapters our methods are strictly 'global', i.e., we deal with whole 'varieties' at a time. However, 'infinitesimal' methods are often more powerful than global ones, and it is in the third chapter that we introduce them. The idea behind these methods is very simple, and comes down in our case to this. Suppose that the base field is the complex numbers and that a 'continuous' group G operates on a vector space by linear transformations. If a vector $v \in V$ is invariant under this action, then the assertion

$$\frac{\partial}{\partial g}(gv) = 0, \qquad g \in G,$$

is extraordinarily suggestive. The problem is to make it precise. Making use of the algebraic version of derivatives, we show that there is a natural way to attach to each affine group a finite dimensional algebra - called the Lie algebra of the group - which in the arcane language of the nineteenth century is very aptly described as the group of 'infinitesimal transformations' of the given group. Whenever the group acts on a vector space by linear transformations, so does its Lie algebra. Since the Lie algebra is a 'linear' object, whereas the group itself almost always is not, the use of the Lie algebra to analyze the given action eases the task immeasurably. There is, however, one flaw in this seemingly ideal situation. It goes completely awry in positive characteristics. This is perhaps the major reason why invariant theory over modular fields is almost completely uncharted territory.

The fourth chapter digresses to develop the Cartan-Weyl representation theory of Lie algebras in characteristic zero. This is the technical groundwork upon which the invariant theory in characteristic zero is laid. We include a conclusive set of counterexamples to the Cartan-Weyl theory in characteristic p.

In the final chapter, we reap the fruits of our efforts. We give a complete solution of the Hilbert fourteenth problem for semisimple groups

in characteristic zero - due to Weyl - and a complete solution of the orbit space problem for such groups - due to Mumford.

After this, we turn to a more detailed study of the structure of affine groups, enabling us to put our invariantive results in more definitive form. Next we prove some recent results of Nagata and Seshadri on so-called 'semi-reductive' groups - a concept which affords the only general method now available for invariant theory in positive characteristics. We conclude with some results of Weitzenbock and Fischer which, from the viewpoint of the theory as developed today, appear rather isolated, but which may conceal general techniques.

A number of exercises are scattered throughout the text and some supplementary ones are given at the end of the book, but I have made no effort to give full coverage in this respect. Since no familiarity with algebraic geometry is assumed, I have included proofs of all the technical algebraic results needed in the course of the development.

I have, of course, borrowed heavily from many writers in preparing this material. In particular, I have relied upon Serre's "Lie Algebras and Lie Groups" (Benjamin 1965), Nagata's "Lectures on the Fourteenth Problem of Hilbert" (Tata Institute, 1965) and Mumford's "Geometric Invariant Theory" (Springer, 1965)

D. S. Rim has kindly made available to me his unpublished lecture notes on Lie algebras and I am indebted to him for many of the examples that appear here. I should also acknowledge what I have been taught by S.Sternberg, and, above all, by O. Zariski.

The text itself is an elaboration on lecture notes that were prepared for a course in modern invariant theory at the University of Pennsylvania in the spring of 1968. I owe much to the patient criticism of the students who attended those lectures.

JOHN FOGARTY

Philadelphia
February 1969

CONTENTS

CHAPTER V INVARIANTS OF AFFINE GROUPS

CHAPTER I

AFFINE ALGEBRAIC SETS

I-1 ALGEBRAIC SETS IN AFFINE SPACE

We fix, once and for all, an algebraically closed field k, making no assumption about the characteristic of k. Let $\underline{A}^n$ denote the *affine space* $k^n = k \times \cdots \times k$ (n factors). $\underline{A}^n$ is a vector space over k, but for the moment, this fact will play a subordinate role.

If $F = F(X_1,\ldots,X_n)$ is a polynomial in the n variables $X_1,\ldots,X_n$ with coefficients in k, we say that the point $x = (x_1,\ldots,x_n)$ in $\underline{A}^n$ is a *zero of* F if $F(x_1,\ldots,x_n) = 0$. The set of zeroes of F is called the *locus of* F, and is denoted by $\underline{V}(F)$. A subset V of $\underline{A}^n$ is called a *hypersurface* in $\underline{A}^n$ if it is the locus of a non-constant polynomial.

Let $k[\underline{A}^n]$ denote the ring $k[X_1,\ldots,X_n]$ of polynomials in $X_1,\ldots,X_n$ with coefficients in k. If B is a subset of $\underline{A}^n$, the set of $F \in k[\underline{A}^n]$

such that $F(x) = 0$ for all $x \in B$ is an ideal in $k[\underline{A}^n]$ which we denote by $\underline{I}_{\underline{A}^n}(B)$, or simply by $\underline{I}(B)$. Conversely, if I is an ideal in $k[\underline{A}^n]$, the set of $x \in \underline{A}^n$ such that $F(x) = 0$ for all $F \in I$ is called the locus of I in $\underline{A}^n$, and denoted by $\underline{V}_{\underline{A}^n}(I)$, or simply by $\underline{V}(I)$. If S is any subset of $k[\underline{A}^n]$ then the set of all $x \in \underline{A}^n$ such that $F(x) = 0$ for all $F \in S$ is the locus of an ideal in $k[\underline{A}^n]$, viz., the ideal generated by S. In other words, $\bigcap_{F \in S} \underline{V}(F) = \underline{V}(I)$, where I is the ideal generated by S.

EXERCISE. Verify the following assertions. Here, I and J denote ideals in $k[\underline{A}^n]$ and B and C denote subsets of $\underline{A}^n$.

i) $I \subset J$ implies $\underline{V}(J) \subset \underline{V}(I)$.

ii) $B \subset C$ implies $\underline{I}(C) \subset \underline{I}(B)$.

iii) $\underline{I}(B \cup C) = \underline{I}(B) \cap \underline{I}(C)$.

iv) If $I + J = \{F + G : F \in I, G \in J\}$, then $I + J$ is an ideal in $k[\underline{A}^n]$ and $\underline{V}(I + J) = \underline{V}(I) \cap \underline{V}(J)$.

v) If $IJ = \{\sum F_i G_i : F_i \in I, G_i \in J\}$, then IJ is an ideal in $k[\underline{A}^n]$, and $\underline{V}(IJ) = \underline{V}(I \cap J) = \underline{V}(I) \cup \underline{V}(J)$.

vi) $V((0)) = \underline{A}^n$, and $V((1)) = \emptyset$.

Also $\underline{I}(\underline{A}^n) = (0)$, and $\underline{I}(\emptyset) = (1)$.

vii) $\underline{V}(\underline{I}(B)) \supset B$, and $\underline{I}(\underline{V}(I)) \supset I$.

viii) $\underline{I}(\underline{V}(I)) = I$ if and only if $F^n \in I$ implies $F \in I$ for all $n > 0$, and all $F \in k[\underline{A}^n]$.

DEFINITION 1.1. A subset V of $\underline{A}^n$ is called an algebraic set in $\underline{A}^n$ if and only if $V = \underline{V}(I(V))$.

This means that V is an algebraic set in $\underline{A}^n$ if and only if V is the locus of some ideal in $k[\underline{A}^n]$. We note that two ideals in $k[\underline{A}^n]$ may very well have the same locus in $\underline{A}^n$ without being the same. Conversely, if B and C are subsets of $\underline{A}^n$, $\underline{I}(B) = \underline{I}(C)$ does not imply that $B = C$. However if B and C are algebraic sets then this cannot happen, i.e., $\underline{I}(B) = \underline{I}(C)$ implies $B = C$. According to what we have said above, every algebraic set in $\underline{A}^n$ is an intersection of hypersurfaces, viz., if V is an algebraic set, then

$$V = \bigcap_{F \in \underline{I}(V)} \underline{V}(F).$$

We now topologize $\underline{A}^1$ by taking as closed sets the finite sets together with $\underline{A}^1$ and the

empty set. Note that this topology is very coarse, i.e., there are comparatively few closed sets. Now we can regard each $F \in k[\underline{A}^n]$ as a mapping of $\underline{A}^n$ into $\underline{A}^1$. On $\underline{A}^n$, the coarsest topology such that all these mappings are continuous is called the Zariski topology. This means that the Zariski topology is completely determined by the ring $k[\underline{A}^n]$ of k-valued functions on $\underline{A}^n$.

PROPOSITION 1.2. A subset B of $\underline{A}^n$ is closed in the Zariski topology if and only if B is an algebraic set. In fact, the complements of hypersurfaces form a basis for the open sets in the Zariski topology on $\underline{A}^n$.

Proof: Since every proper algebraic set in $\underline{A}^n$ is an intersection of hypersurfaces, and conversely, it suffices to prove the second assertion. However it is clear that $\underline{V}(FG) = \underline{V}(F) \cup \underline{V}(G)$ for all $F, G \in k[\underline{A}^n]$. This means that the hypersurfaces are closed under finite unions. Therefore the weakest topology on $\underline{A}^n$ such that all $F \in k[\underline{A}^n]$ determine continuous mappings is just the one whose closed sets are arbitrary intersections of hypersurfaces.

Henceforth, the terms "closed" and "open"

will refer exclusively to the Zariski topology. If V is a closed subset of $\underline{A}^n$, i.e., an algebraic set in $\underline{A}^n$, then V inherits a topology from $\underline{A}^n$, viz., $Z \subset V$ is closed if and only if there exists a closed subset W of $\underline{A}^n$ such that $Z = V \cap W$. This topology on V will also be called the Zariski topology.

If V is a closed subset of $\underline{A}^n$ let $I = \underline{I}(V)$. Then for any $F, G \in k[\underline{A}^n]$, $F|V = G|V$ if and only $F - G \in I$. Thus $k[\underline{A}^n]/I$ may be regarded as a ring of k-valued function on V. We denote this ring by $k[V]$ and call it the <u>coordinate ring</u> of V.

The following theorem - known as Hilbert's nullstellensatz - is the cornerstone for our entire development. Since the proof which we give uses ideas that are only introduced in chapter V, the reader may omit the proof on a first reading without prejudicing his comprehension of what follows.

THEOREM A. If I is an ideal in $k[\underline{A}^n]$, then $\underline{V}(I) = \emptyset$ if and only if $I = (1)$.

<u>Proof</u>: If $I = (1)$ then $\underline{V}(1) = \emptyset$, as we have already noted. The converse statement is the hard part. We must prove that if I is a proper ideal in $k[\underline{A}^n]$, then there is at least one point $x \in \underline{A}^n$

such that $F(x) = 0$ for all $F \in I$. Clearly, if we can prove this when I is maximal, then we are finished.

Now let I be a maximal ideal in $k[\underline{A}^n] = k[X_1,\ldots,X_n]$. Let x_i denote the residue of X_i modulo I. Now if $F \in I$, then certainly $F(x_1,\ldots,x_n) = 0$. (This is a trivial formality). On the other hand, since I is maximal, the ring $k[\underline{A}^n]/I$ is a field - containing k. If we can show that this field is k itself, then it will follow that the n-tuple $(x_1,\ldots,x_n)$ is a point of $\underline{A}^n$, and we are done! Thus the theorem boils down to the following lemma of Zariski:

LEMMA: If K is a field (not necessarily algebraically closed) and if the ring $K[x_1,\ldots,x_n]$ is a field, then the x_i are algebraic over K.

Proof: We use induction on n. If $n = 1$, then x_1 cannot be transcendental over K since in that case, $K[x_1]$ is isomorphic to the ring of polynomials in one variable, which is certainly not a field.

Now, by assumption, $K[x_1,\ldots,x_n]$ is a field, so that it must contain the fraction field $K(x_1)$ of $K[x_1]$. Therefore it contains the ring $K(x_1)[x_2,\ldots,x_n]$. By induction, we may assume that $x_2,\ldots,x_n$ are algebraic over $K(x_1)$. (Note