Rudiments of Algebraic Geometry

W. E. Jenner

UNIVERSITY TEXTS IN THE MATHEMATICAL SCIENCES

RUDIMENTS OF ALGEBRAIC GEOMETRY

W. E. JENNER
University of North Carolina

NEW YORK • OXFORD UNIVERSITY PRESS • 1963

Library of Congress Catalogue Card Number: 63-7867
Printed in the United States of America

RUDIMENTS OF ALGEBRAIC GEOMETRY

University Texts in the Mathematical Sciences
Advisory Editors, Herbert E. Robbins and Edgar R. Lorch

TITLES PUBLISHED

Derman and Klein	PROBABILITY AND STATISTICAL INFERENCE FOR ENGINEERS
Berberian	INTRODUCTION TO HILBERT SPACE
Rosenblatt	RANDOM PROCESSES
Takacs	INTRODUCTION TO THE THEORY OF QUEUES
Lorch	SPECTRAL THEORY
Jenner	RUDIMENTS OF ALGEBRAIC GEOMETRY

INTRODUCTION

One of the most significant developments in recent mathematics is the resurgence of interest in algebraic geometry, a trend dating more or less from the publication of Weil's *Foundations*. Up to the present time, this revival has manifested itself only at the graduate level and beyond. At the undergraduate level on the other hand, the geometric traditions, if represented at all, usually have been presented in the form of a course in analytic or synthetic projective geometry, culminating in the theory of the conic sections. The transition from this to modern algebraic geometry is beset with imposing obstacles, as most people who have gone through the experience will testify. As matters stand at present, to exaggerate only slightly, students have virtually no geometric experience of much significance between their freshman study of conics and quadrics and some graduate course devoted, more likely than not, to proving the Riemann-Roch Theorem in six easy lessons — using sheaves — and this sometimes without having ever beheld a curve possessed of a singular point. One purpose of this book is to assist graduate students who find themselves in this position and to obviate for them, at least partially, the necessity of struggling with the confusion, obscurity, and downright error which sometimes arise as one extracts the needed information from some of the older literature.

Nevertheless, the book is addressed primarily to undergraduates and is intended to supplement, or to provide an alternative to, more traditional subject matter. In this way it is hoped to suggest some idea of the actual concerns of present-day geometers, and at the same time to make the way easier for those going on to a serious study of algebraic geometry. The prerequisites have been kept to an absolute minimum. I construe these to consist of elementary analytic geometry up through the conics and quadrics, the fundamentals of linear algebra (which may be studied concurrently), and a knowledge of calculus up through partial derivatives. A brief outline of the necessary algebra has been included by way of preamble. It is sufficient to consult this only as the necessity arises; the reader may begin safely with Chapter I.

There is perhaps a legitimate question, particularly among the experts, as to whether it is desirable — or indeed possible — to say anything worthwhile about algebraic geometry at the undergraduate level. My own answer is in the affirmative and this book represents the results of my attempt to deal with the question. In view of the absence of precedents, it is difficult to be convinced that one has chosen the "right" things to talk about. The choices made here are admittedly tentative, and it is hoped that further experimentation by others, more competent than myself, will lead to a more definitive result.

From a technical point of view, the principal aim of the book is to close part of the gap between elementary analytic geometry and abstract algebraic geometry along the lines, for instance, of Lang's recent book [10]. This entails a transition to a new attitude of mind both with regard to subject matter and to method. This transition is exemplified, for instance, in recasting the theory of tangents in algebraic terms. This necessitates reformulation of the required calculus in purely algebraic form, thus extirpating the notion of limit and allowing generalization to arbitrary ground fields. Another theme of constant recurrence is the necessity of working over a sufficiently large field, usually algebraically closed, in order that the geometric results may take on their most felicitous form. It is hoped that in this way some light will be shed on the reasons behind the rather strong initial algebraic assumptions that are usually made in abstract algebraic geometry.

A few words may clarify the point of view taken on certain topics. First of all, points are defined as n-tuples — not even as equivalence classes under certain admissible transformations. This is quite sufficient for the purpose at hand, and bases the theory on a very simple set-theoretical construction rather than on the invention of a new class of things called "points" which are apt to evoke nonsensical metaphysical questions. One consequence of the point of view adopted here is that a transformation always appears as something that moves points around, and not as something that "changes co-ordinates." It is, of course, important to understand the two ways of looking at these things. Usually, however, this is carefully dealt with in courses in linear algebra and it is unnecessary to discuss it here.

Most of what goes on in this book is done over arbitrary fields. This is the only real divergence from current practice in algebraic geometry where it is customary to work over a so-called universal domain. There are several reasons for this decision. In the first place, since generic points are not discussed here, there is no need for transcendentals. So far as algebraic closure is concerned, I have tried to show why it is desirable, and to do this one naturally has to start without it. Actually, a great deal of what is done in this book will work over finite fields, a fact that it seemed worthwhile to point out for the reassurance of young mathematicians who have just heard of Gödel's Theorem and expect the imminent collapse of mathematics! Whatever may be said of such an attitude on their part, it is certainly indicative of a serious concern for our subject and so should be regarded with sympathetic understanding. Certainly no harm is done; they either recover or else go on to become experts in mathematical logic.

The matter of terminology in algebraic geometry is at present in an unsettled state, especially in view of certain recent activities in Paris. Fortunately, however, this difficulty is hardly relevant for a book at this level. The only conventions made here that call for comment are that all fields are assumed to be commutative and that the term "variety" is reserved for algebraic sets that are absolutely irreducible.

I am deeply indebted to several of my friends for their criticisms and helpful advice; in particular to Douglas Derry, William L. Hoyt, Kenneth May, and Maxwell Rosenlicht. The critical comments of A. Seidenberg on an early version of the manuscript were especially helpful to me. I also wish to thank Mrs. Florence Valentine for typing the manuscript. I am especially grateful to Ralph Spielman whose wise counsel and encouragement were instrumental in my decision to write this book.

Chapel Hill, North Carolina W.E.J.
September 1962

RUDIMENTS OF ALGEBRAIC GEOMETRY

CONTENTS

ALGEBRAIC PRELIMINARIES

We collect here some of the basic algebraic facts that we use. These are part of the standard equipment of all mathematicians and so our account is confined to the basic definitions. The account given by Bourbaki [3] of these matters is generally regarded as definitive. Among the best source books in English is Zariski and Samuel [18]. For linear algebra the books of Halmos [6], Hoffman and Kunze [8], and Jaeger [9] can be consulted; the last two give an extensive account of the computational aspects of determinant theory. Basic set-theoretical facts, which we assume known, are given in Halmos [5].

A set S is said to admit a *law of binary composition* if with each ordered pair (x,y) of elements of S is associated an element of S. This element will be denoted here by $x \circ y$ and will be called the "product" or "sum" of x and y (in that order), whichever is the more suggestive in a particular context.

1. A *group* is a set G together with a binary law of composition $(a,b) \longrightarrow a \circ b$ such that

(i) G is closed under $(\circ)$; that is, $a \circ b$ is defined and is an element of G for all $a,\ b \in G$.

(ii) $a \circ (b \circ c) = (a \circ b) \circ c$ for all $a,\ b,\ c \in G$.

(iii) The equations $a \circ x = b$ and $y \circ a = b$ each have solutions for any $a,\ b \in G$.

Remark: For purposes of verification, axiom (iii) is usually replaced by axioms (iii′) and (iii′′) together:

(iii′) There is an element $e \in G$, the *identity element*, such that $a \circ e = a = e \circ a$ for all $a \in G$.

(iii′′) For every $a \in G$ there is an element $a' \in G$, the *inverse* of a, such that $a \circ a' = a' \circ a = e$.

If $a \circ b = b \circ a$, the group G is said to be *abelian* or *commutative*.

2. A *ring* is a set R together with two laws of binary composition, $(a,b) \longrightarrow a + b$ and $(a,b) \longrightarrow a \cdot b$, called addition and multiplication respectively, such that

(i) R is an abelian group under addition.

(ii) R is closed under multiplication.

(iii) $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ for all $a, b, c \in R$.

(iv) $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

If $a \cdot b = b \cdot a$ for all $a, b \in R$, then R is said to be *commutative*.

3. A *field* k is a commutative ring for which the set of elements not equal to 0 (where 0 is the additive identity element) form a group under multiplication. (This is often, if somewhat imprecisely, described by saying that a field behaves like the set of rational (or real) numbers with respect to the basic arithmetic rules of addition, subtraction, multiplication, and division.) A field k is said to be *algebraically closed* if every polynomial equation with coefficients in k has a root in k; for example, the field of complex numbers. If $1 + \cdots + 1$ (n times) $= 0$ in a field k, where 1 is the multiplicative identity element, then the smallest such strictly positive integer n is a prime number called the *characteristic* of k; if there is no such integer n, then k is said to be of *characteristic zero*.

4. In working over arbitrary fields, the notion of *polynomial* must be refined beyond its use in elementary algebra. The trouble is that a polynomial in the elementary sense may be identically zero without its "looking like" the zero polynomial. For instance, in this sense, the polynomial $x^2 - x$ is identically zero in the field F_2 of residue-classes of integers reduced modulo 2 (cf. Chapter I). We avoid this difficulty by regarding "x" only as a symbol: something in its own right beyond the fact that we can substitute things for it. The metaphysical hiatus in this definition can be

avoided as follows: let N be the set of integers greater than or equal to 0. A polynomial in one "variable" over a field k is a mapping $P: N \longrightarrow k$ such that $P(n) = 0$ for all $n \in N$ except a finite number. The idea is that $P(n)$ is the coefficient of what used to be called x. For further details, and the generalization to polynomials in several variables, the reader is referred to Zariski and Samuel [18].

5. Matrices occur in mathematics *almost* always in connection with linear transformations. We define matrices as follows, following Chevalley [4]: let I be the set of integers $1, 2, \cdots, m$ and J the set of integers $1, 2, \cdots, n$. An m by n matrix Φ with coefficients in a ring R is a mapping $\Phi: (i,j) \longrightarrow \alpha_{ij}$ of the cartesian product $I \times J$ into R. We can identify (for notational purposes) the matrix Φ with the array

$$\begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix}.$$

The first subscript i of α_{ij} is called the *row index* and the second subscript j the *column index*. If $\Psi: (i,j) \longrightarrow \beta_{ij}$ is another such matrix, we define their *sum* to be the matrix $\Phi + \Psi: (i,j) \longrightarrow \alpha_{ij} + \beta_{ij}$. The set of m by n matrices with coefficients in R forms an abelian group under addition. If Φ is an l by m matrix and Ψ an m by n matrix, we define their product to be the l by n matrix $\Phi \circ \Psi: (i,j) \longrightarrow \sum_{k=1}^{m} \alpha_{ik}\beta_{kj}$. The product $\Phi \circ \Psi$ is defined if and only if the column index of Φ is equal to the row index of Ψ. The motivation for these definitions lies in the theory of linear transformations. The set $[R]_n$ of n by n matrices with coefficients in a ring R itself forms a ring under the matrix operations.

6. A *vector space* V over a field k is an additive abelian group for which a multiplication of elements of V by ele-

ments of k is defined such that

(i) $\lambda(u + v) = \lambda u + \lambda v$.

(ii) $(\lambda + \mu)v = \lambda v + \mu v$.

(iii) $\lambda u = u\lambda$.

(iv) $1\,u = u$.

Here $u, v \in V$ and $\lambda, \mu \in k$ and 1 is the multiplicative identity element of k. (In some parts of mathematics, axiom (iii) is weakened so that there is a distinction between left and right vector spaces. This generalization will be unnecessary for our purposes.)

A particularly important example is the vector space of n-tuples over a field k. If $(x_1, \cdots, x_n)$ and $(y_1, \cdots, y_n)$ with $x_i, y_i \in k$ are two such n-tuples we define addition component-wise, $(x_1, \cdots, x_n) + (y_1, \cdots, y_n) = (x_1 + y_1, \cdots, x_n + y_n)$, and define $\lambda(x_1, \cdots, x_n) = (x_1, \cdots, x_n)\lambda = (\lambda x_1, \cdots, \lambda x_n)$ for $\lambda \in k$. (For readers of austere tastes, n-tuples over k can be defined as mappings of the set of integers $1, 2, \cdots, n$ into k. An even more austere approach, in terms of the most primitive set-theoretical notions is given in Halmos [5].)

A set of vectors $v_1, \cdots, v_n \in V$ is said to be *linearly dependent* if there is a relation $\lambda_1 v_1 + \cdots + \lambda_n v_n = 0$ with $\lambda_i \in k$ and some $\lambda_i \neq 0$; otherwise it is *linearly independent*. A vector space V is said to be *finite dimensional* if there exist a finite number of vectors $v_1, \cdots, v_n$ such that every $v \in V$ can be expressed in the form $v = \lambda_1 v_1 + \cdots + \lambda_n v_n$ with the $\lambda_i \in k$. If this is so, then the vectors $v_1, \cdots, v_n$ can be chosen to be linearly independent; then the λ_i are unique, and the integer n is unique. This value of n is called the *dimension* of V and $v_1, \cdots, v_n$ constitute a *basis* of V. Any n linearly independent elements of V form a basis.

7. Let V be a vector space of dimension n over k. A *linear transformation* of V is a mapping of V into V, having the properties $\phi(u + v) = \phi(u) + \phi(v)$ and $\phi(\lambda u) = \lambda\phi(u)$ where $u, v \in V$, and $\lambda \in k$. If ψ is another linear transformation of

V we define $\phi + \psi : u \longrightarrow \phi(u) + \psi(u)$ and $\phi \circ \psi : u \longrightarrow \phi(\psi(u))$. The linear transformations of V form a ring. We say ϕ is *invertible* if there is a linear transformation ϕ' such that $\phi \circ \phi' = \phi' \circ \phi$ is the identity mapping on V. The elementary theory of determinants will be assumed known. Determinants are defined directly for linear transformations in Halmos [6]. A linear transformation is invertible if and only if its determinant is non-zero. For an account of the techniques of determinant theory see Jaeger [9].

I

AFFINE SPACES

1. Affine spaces and algebraic sets

Algebraic geometry is concerned with the study of loci of polynomial equations. For the most part, metrical properties of euclidean geometry, distance, and angle, are not considered, and so we work in rather more general kinds of spaces called *affine* and *projective*. These can be defined synthetically along the lines of Euclid's *Elements*, but it is customary nowadays in algebraic geometry to start with purely algebraic definitions.

In this chapter we shall consider affine spaces. Let k be any field. By *affine n-space over k*, denoted $A_n(k)$, is meant the set of n-tuples $(x_1, \cdots, x_n)$ where $x_i \in k$. Such an n-tuple is called a *point*. In case k is the field of real numbers, it is harmless to think of $A_n(k)$ as being euclidean n-space without any mention of distance. In particular, if $n = 2$ or 3 it is possible to draw "pictures" (graphs) in the usual sense. If $f(x_1, \cdots, x_n) = 0$ is a polynomial equation in n variables with coefficients in k, the set of points in $A_n(k)$ satisfying this equation is called an *algebraic hypersurface*. Since we shall consider only loci given by polynomial equations, the adjective "algebraic" will generally be omitted. The intersection of a finite number of hypersurfaces is called an *algebraic set*. (Some writers use the term "algebraic variety"; a convention seems to have developed, however, to reserve this for algebraic sets with certain extra conditions which are too technical for discussion here.) If $n = 2$ or 3, hypersurfaces are called *curves*