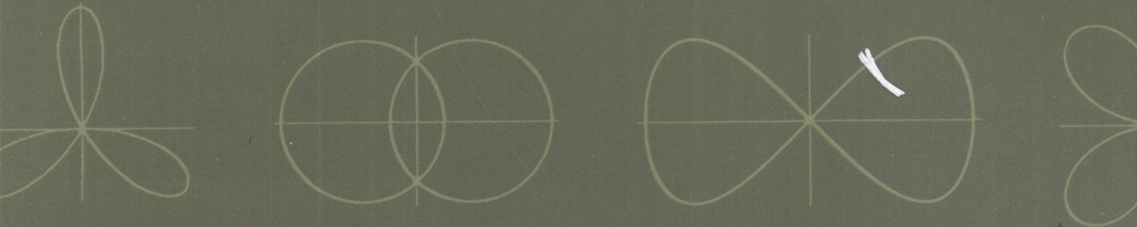
Ernst Kunz

INTRODUCTION TO PLANE ALGEBRAIC CURVES



$a_1, \dots, a_d \in K$). $(X^2+Y^2)^2+3X^2Y-Y^3=0$

Translated by Richard G. Belshoff

Birkhäuser

Ernst Kunz

Introduction to Plane Algebraic Curves

Translated from the original German by Richard G. Belshoff

Birkhäuser
Boston • Basel • Berlin

Ernst Kunz
Universität Regensburg
NWF I – Mathematik
D-93040 Regensburg
Germany

Richard G. Belshoff (Translator)
Southwest Missouri State University
Department of Mathematics
Springfield, MO 65804
U.S.A.

Cover design by Mary Burgess.

Mathematics Subject Classicification (2000): 14-xx, 14Hxx, 14H20, 14H45 (primary);
14-01, 13-02, 13A02, 13A30 (secondary)

Library of Congress Cataloging-in-Publication Data
Kunz, Ernst, 1933-
[Ebene algebraische Kurven. English]
Introduction to plane algebraic curves / Ernst Kunz; translated by Richard G. Belshoff.
p. cm.
Includes bibliographical references and index.
ISBN 0-8176-4381-8 (alk. paper)
1. Curves, Plane. 2. Curves, Algebraic. 3. Singularities (Mathematics) I. Title.

QA567.K8613 2005
516.3'52–dc22 2005048053

ISBN-10 0-8176-4381-8
ISBN-13 978-0-8176-4381-2
eISBN 0-8176-4443-1
Printed on acid-free paper.

Birkhäuser

Based on the original German edition, *Ebene algebraische Kurven*,
Der Regensburg Trichter, 23, Universität Regensburg, ISBN 3-88246-167-5, ©1991 Ernst Kunz

Printed in the United States of America. (SB)

9 8 7 6 5 4 3 2 1 SPIN 11301783

Birkhäuser is a part of *Springer Science+Business Media*

www.birkhauser.com

To the memory of my friend
Hans-Joachim Nastold (1929–2004)
and of our teacher
Friedrich Karl Schmidt (1901–1977)

Preface

This book is a slightly extended elaboration of a course on commutative ring theory and plane algebraic curves that I gave several times at the University of Regensburg to students with a basic knowledge of algebra. I thank Richard Belshoff for translating the German lecture notes into English and for preparing the numerous figures of the present text.

As in my book *Introduction to Commutative Algebra and Algebraic Geometry*, this book follows the philosophy that the best way to introduce commutative algebra is to simultaneously present applications in algebraic geometry. This occurs here on a substantially more elementary level than in my earlier book, for we never leave plane geometry, except in occasional notes without proof, as for instance that the abstract Riemann surface of a plane curve is "actually" a smooth curve in a higher-dimensional space. In contrast to other presentations of curve theory, here the algebraic viewpoint stays strongly in the foreground. This is completely different from, for instance, the book of Brieskorn–Knörrer [BK], where the geometric–topological–analytic aspects are particularly stressed, and where there is more emphasis on the history of the subject. Since these things are explained there in great detail, and with many beautiful pictures, I felt relieved of the obligation to go into the topological and analytical connections. In the lectures I recommended to the students that they read the appropriate sections of Brieskorn–Knörrer [BK]. The book by G. Fischer [F] can also serve this purpose.

We will study algebraic curves over an algebraically closed field K. It is not at all clear a priori, but rather to be regarded as a miracle, that there is a close correspondence between the details of the theory of curves over $\mathbb{C}$ and that of curves over an arbitrary algebraically closed field. The parallel between curves over fields of prime characteristic and over fields of characteristic 0 ends somewhat earlier. In the last few decades algebraic curves of prime characteristic made an entrance into coding theory and cryptography, and thus into applied mathematics.

The following are a few ways in which this course differs from other introductions to the theory of plane algebraic curves known to me: Filtered algebras, the associated graded rings, and Rees rings will be used to a great extent, in order to deduce basic facts about intersection theory of plane curves. There will be modern proofs for many classical theorems on this subject. The techniques which we apply are nowadays also standard tools of computer algebra.

Also, a presentation of algebraic residue theory in the affine plane will be given, and its applications to intersection theory will be considered. Many of the theorems proved here about the intersection of two plane curves carry over with relatively minor changes to the case of the intersection of n hypersurfaces in n-dimensional space, or equivalently, to the solution sets of n algebraic equations in n unknowns.

The treatment of the Riemann–Roch theorem and its applications is based on ideas of proofs given by F.K. Schmidt in 1936. His methods of proof are an especially good fit with the presentation given here, which is formulated in the language of filtrations and associated graded rings.

The book contains an introduction to the algebraic classification of plane curve singularities, a subject on which many publications have appeared in recent years and to which references are given. The lectures had to end at some point, and so resolution of singularities was not treated. For this subject I refer to Brieskorn–Knörrer or Fulton [Fu]. Nevertheless I hope that the reader will also get an idea of the problems and some of the methods of higher-dimensional algebraic geometry.

The present work is organized so that the algebraic facts that are used and that go beyond a standard course in algebra are collected together in Appendices A–L, which account for about one-third of the text and are referred to as needed. A list of keywords in the section "Algebraic Foundations" should make clear what parts of algebra are deemed to be well-known to the reader. We always strive to give complete and detailed proofs based on these foundations

My former students Markus Nübler, Lutz Pinkofsky, Ulrich Probst, Wolfgang Rauscher and Alfons Schamberger have written diploma theses in which they have generalized parts of the book. They have contributed to greater clarity and better readability of the text. To them, and to those who have attended my lectures, I owe thanks for their critical comments. My colleague Rolf Waldi who has used the German lecture notes in his seminars deserves thanks for suggesting several improvements.

Regensburg
December 2004

Ernst Kunz

Conventions and Notation

(a) By a *ring* we shall always mean an associative, commutative ring with identity.

(b) For a ring R, let $\operatorname{Spec} R$ be the set of all prime ideals $\mathfrak{p} \neq R$ of R (the *Spectrum of* R). The set of all maximal (minimal) prime ideals will be denoted by $\operatorname{Max} R$ (respectively $\operatorname{Min} R$).

(c) A ring homomorphism $\rho : R \to S$ shall always map the identity of R to the identity of S. We also say that S/R is an *algebra* over R given by ρ. Every ring is a $\mathbb{Z}$-algebra.

(d) For an algebra S over a field K we denote by $\dim_K S$ the dimension of S as a K-vector space.

(e) For a polynomial f in a polynomial algebra $R[X_1, \dots, X_n]$, we let $\deg f$ stand for the *total degree* of f and $\deg_{X_i} f$ the *degree in* X_i.

(f) If K is a field, $K(X_1, \dots, X_n)$ denotes the *field of rational functions* in the variables $X_1, \dots, X_n$ over K (the quotient field of $K[X_1, \dots, X_n]$).

(g) The minimal elements in the set of all prime ideals containing an ideal I are called the minimal prime divisors of I.

Introduction to Plane Algebraic Curves

Contents

Part I Plane Algebraic Curves

Part II Algebraic Foundations

Part I

Plane Algebraic Curves

1

Affine Algebraic Curves

This section uses only a few concepts and facts from algebra. It assumes a certain familiarity with polynomial rings $K[X_1, \dots, X_n]$ over a field, in particular that $K[X]$ is a principal ideal domain, and that $K[X_1, \dots, X_n]$ is a unique factorization domain in general. Also, ideals and quotient rings will be used. Finally, one must know that an algebraically closed field has infinitely many elements.

We will study algebraic curves over an arbitrary algebraically closed field K. Even if one is only interested in curves over $\mathbb{C}$, the investigation of the $\mathbb{Z}$-rational points of curves by "reduction mod p" leads into the theory of curves over fields with prime characteristic p. Such curves also appear in algebraic coding theory (Pretzel [P], Stichtenoth [St]) and cryptography (Koblitz [K], Washington [W]).

$\mathbb{A}^2(K) := K^2$ denotes the affine plane over K, and $K[X, Y]$ the polynomial algebra in the variables X and Y over K. For $f \in K[X, Y]$, we call

$$\mathcal{V}(f) := \{(x, y) \in \mathbb{A}^2(K) \mid f(x, y) = 0\}$$

the *zero set of f*. We set $D(f) := \mathbb{A}^2(K) \setminus \mathcal{V}(f)$ for the set of points where f does not vanish.

Definition 1.1. A subset $\Gamma \subset \mathbb{A}^2(K)$ is called a (plane) *affine algebraic curve* (for short: curve) if there exists a nonconstant polynomial $f \in K[X, Y]$ such that $\Gamma = \mathcal{V}(f)$. We write $\Gamma : f = 0$ for this curve and call $f = 0$ an *equation for Γ*.

If $K_0 \subset K$ is a subring and $\Gamma = \mathcal{V}(f)$ for a nonconstant polynomial $f \in K_0[X, Y]$, we say that Γ *is defined over* K_0 and call $\Gamma_0 := \Gamma \cap K_0^2$ the set of *K_0-rational points of Γ*.

Examples 1.2.

(a) The zero sets of linear polynomials $aX + bY + c = 0$ with $(a, b) \neq (0, 0)$ are called *lines*. If $K_0 \subset K$ is a subfield and $a, b, c \in K_0$, then the line $g : aX + bY + c = 0$ certainly possesses K_0-rational points. Through two different points of $\mathbb{A}^2(K_0)$ there is exactly one line (defined over K_0).

(b) If $\Gamma_1, \dots, \Gamma_h$ are algebraic curves with equations $f_i = 0$ $(i = 1, \dots, h)$, then $\Gamma := \cup_{i=1}^h \Gamma_i$ is also an algebraic curve. It is given by the equation $\prod_{i=1}^h f_i = 0$. In particular, the union of finitely many lines is an algebraic curve (see Figure 1.1).

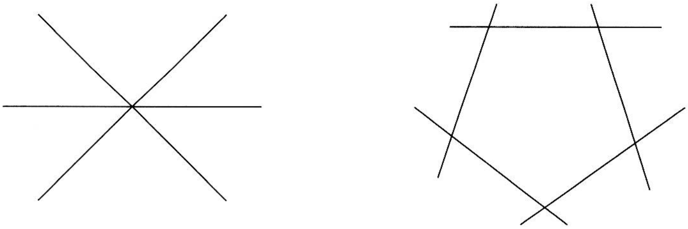


Fig. 1.1. The union of finitely many lines is an algebraic curve.

(c) Let $\varGamma = \mathcal{V}(f)$ with a nonconstant $f \in K[Y]$ (so f does not depend on X). The decomposition of f into linear factors

$$f = c \cdot \prod_{i=1}^{d} (Y - a_i) \qquad (c \in K^* := K \setminus \{0\},\ a_1, \dots, a_d \in K)$$

shows that $\varGamma$ is the union of lines $g_i : Y - a_i = 0$ parallel to the X-axis.

(d) The zero sets of quadric polynomials

$$f = aX^2 + bXY + cY^2 + dX + eY + g \qquad (a, b, \dots g \in K;\ (a, b, c) \neq (0, 0, 0))$$

are called *quadrics.* In case $K = \mathbb{C}$, $K_0 = \mathbb{R}$ we get the *conic sections,* whose $\mathbb{R}$-rational points are shown in Figures 1.2 through 1.5. Defined

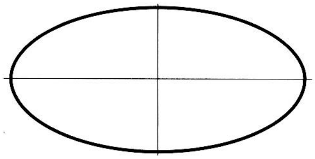


Fig. 1.2. Ellipse: $\frac{X^2}{a^2} + \frac{Y^2}{b^2} = 1$, $(a, b \in \mathbb{R}_+)$

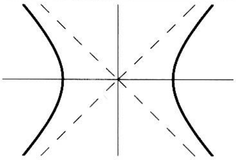


Fig. 1.3. Hyperbola: $\frac{X^2}{a^2} - \frac{Y^2}{b^2} = 1$, $(a, b \in \mathbb{R}_+)$

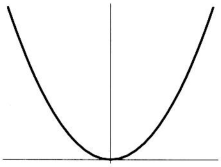


Fig. 1.4. Parabola: $Y = aX^2$, $(a \in \mathbb{R}_+)$

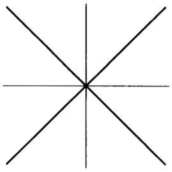


Fig. 1.5. Line pair: $X^2 - Y^2 = 0$

as sections of a cone with a plane, they were thoroughly studied in ancient Greek mathematics. Many centuries later, they became important in Kepler's laws of planetary motion and in Newton's mechanics. Unlike the $\mathbb{R}$-rational points, questions about the $\mathbb{Q}$-rational points of quadrics have, in general, nontrivial answers (cf. Exercises 2–4).

(e) The zero sets of polynomials of degree 3 are called *cubics.* The $\mathbb{R}$-rational points of some prominent cubics are sketched in Figures 1.6 through 1.9. Cubic curves will be discussed in 7.17 and in Chapter 10.

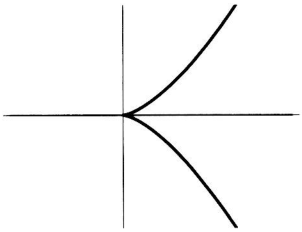


Fig. 1.6. Neil's semicubical parabola: $X^3 - Y^2 = 0$

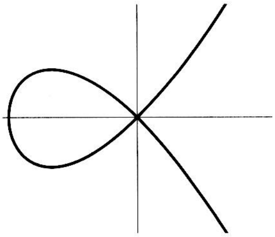


Fig. 1.7. Folium of Descartes: $X^3 + X^2 - Y^2 = 0$

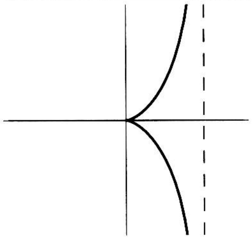


Fig. 1.8. Cissoid of Diocles: $Y^2(1 - X) - X^3 = 0$

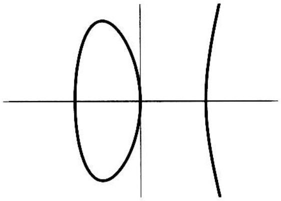


Fig. 1.9. Elliptic curve in Weierstraß normal form ($e_1 < e_2 < e_3$ real): $Y^2 = 4(X - e_1)(X - e_2)(X - e_3)$

(f) Some curves with equations of higher degrees are sketched in Figures 1.10 through 1.15. For the origin of these curves and the others indicated above, one can consult the book by Brieskorn–Knörrer [BK]. See also Xah Lee's "Visual Dictionary of Special Plane Curves" `http://xahlee.org`, and the "Famous Curves Index" at the MacTutor History of Mathematics archive `http://www-history.mcs.st-and.ac.uk/history`.

(g) The *Fermat curve* F_n ($n \geq 3$) is given by the equation $X^n + Y^n = 1$. It is connected with some of the most spectacular successes of curve theory in recent years. *Fermat's last theorem* (1621) asserted that the only $\mathbb{Q}$-rational points on this curve are the obvious ones: $(1, 0)$ and $(0, 1)$ in

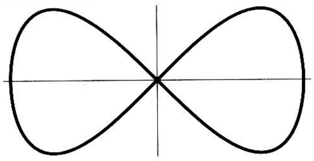


Fig. 1.10. Lemniscate: $X^2(1-X^2)-Y^2=0$

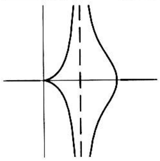


Fig. 1.11. Conchoid of Nichomedes: $(X^2+Y^2)(X-1)^2-X^2=0$

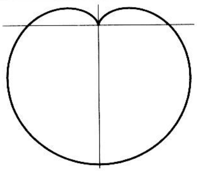


Fig. 1.12. Cardioid: $(X^2+Y^2+4Y)^2-16(X^2+Y^2)=0$

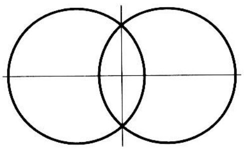


Fig. 1.13. Union of two circles: $(X^2-4)^2+(Y^2-9)^2+2(X^2+4)(Y^2-9)=0$

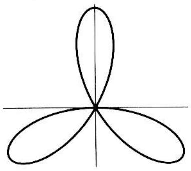


Fig. 1.14. Three-leaf rose: $(X^2+Y^2)^2+3X^2Y-Y^3=0$

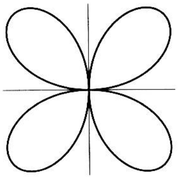


Fig. 1.15. Four-leaf rose: $(X^2+Y^2)^3-4X^2Y^2=0$

case n is odd; and $(\pm 1, 0)$, $(0, \pm 1)$ in case n is even. G. Faltings [Fa] in 1983 showed that there are only finitely many $\mathbb{Q}$-rational points on F_n, a special case of *Mordell's conjecture* proved by him. In 1986 G. Frey observed that Fermat's last theorem should follow from a conjecture about elliptic curves (the *Shimura–Taniyama theorem*), for which Andrew Wiles (see [Wi], [TW]) gave a proof in 1995, hence also proving Fermat's last theorem. These works are far beyond the scope of the present text. The reader interested in the history of the problem and its solution may enjoy Simon Singh's bestselling book *Fermat's last theorem* [Si].

Having seen some of the multifaceted aspects of algebraic curves, we turn now to the general theory of these curves. The examples $X^2 + Y^2 = 0$ and $X^2 + Y^2 + 1 = 0$ show that the set of $\mathbb{R}$-rational points of a curve can be finite, or even empty. For points with coordinates in an algebraically closed field, however, this cannot happen.

Theorem 1.3. *Every algebraic curve $\Gamma \subset \mathbb{A}^2(K)$ consists of infinitely many points, and also $\mathbb{A}^2(K) \setminus \Gamma$ is infinite.*

Proof. Let $\Gamma = \mathcal{V}(f)$ with $f = a_0 + a_1X + \cdots + a_pX^p$, where $a_i \in K[Y]$ $(i = 0, \ldots, p)$ and $a_p \neq 0$. If $p = 0$, we are in the situation of Example 1.2 (c) above, and since an algebraically closed field has infinitely many elements, there is nothing more to be shown. Therefore, let $p > 0$. Since a_p has only finitely many zeros in K, there are infinitely many $y \in K$ with $a_p(y) \neq 0$. Then

$$f(X, y) = a_0(y) + a_1(y)X + \cdots + a_p(y)X^p$$

is a nonconstant polynomial in $K[X]$. If $x \in K$ is a zero of this polynomial, then $(x, y) \in \Gamma$; therefore, Γ contains infinitely many points. If $x \in K$ is not a zero, then $(x, y) \in D(f)$, and therefore there are also infinitely many points in $\mathbb{A}^2(K) \setminus \Gamma$.

An important theme in curve theory is the investigation of the intersection of two algebraic curves. Our first instance of this is furnished by the following theorem. It assumes a familiarity with unique factorization domains.

Theorem 1.4. *Let f and g be nonconstant relatively prime polynomials in $K[X, Y]$. Then*

(a) *$\mathcal{V}(f) \cap \mathcal{V}(g)$ is finite. In other words, the system of equations*

$$f(X, Y) = 0, \quad g(X, Y) = 0$$

has only finitely many solutions in $\mathbb{A}^2(K)$.

(b) *The K-algebra $K[X, Y]/(f, g)$ is finite-dimensional.*

For the proof we will use

Lemma 1.5. *Let R be a UFD with quotient field K. If $f, g \in R[X]$ are relatively prime, then they are also relatively prime in $K[X]$, and there exists an element $d \in R \setminus \{0\}$ such that*

$$d = af + bg$$

for some polynomials $a, b \in R[X]$.

Proof. Suppose that $f = \alpha h$, $g = \beta h$ for polynomials $\alpha, \beta, h \in K[X]$, where h is not a constant polynomial. Since any denominators that appear in h may be brought over to α and β, we may assume that $h \in R[X]$. We then write

$$\alpha = \sum \alpha_i X^i, \quad \beta = \sum \beta_j X^j \qquad (\alpha_i, \beta_j \in K).$$

Let $\delta \in R \setminus \{0\}$ be the least common denominator for the α_i and β_j. Then we have

$$\delta f = \phi h, \qquad \delta g = \psi h$$