Graduate Texts in Mathematics

111

# Elliptic Curves

Springer-Verlag

Dale Husemöller

# Elliptic Curves

With an Appendix by Ruth Lawrence

With 44 Illustrations

Springer-Verlag
New York Berlin Heidelberg
London Paris Tokyo

Dale Husemöller
Department of Mathematics
Haverford College
Haverford, PA 19041
U.S.A.

*Editorial Board*

P. R. Halmos
Department of Mathematics
Santa Clara University
Santa Clara, CA 95053
U.S.A.

F. W. Gehring
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109
U.S.A.

AMS Classifications: 14-01, 14H25, 14K07, 14L15

Library of Congress Cataloging in Publication Data
Husemöller, Dale.
Elliptic curves.
(Graduate texts in mathematics; 111)
Bibliography: p.
Includes index.
1. Curves, Elliptic. 2. Curves, Algebraic. 3. Group schemes (Mathematics)
I. Title. II. Series.
QA567.H897 1986 512'.33 86-11832

© 1987 by Springer-Verlag New York Inc.
All rights reserved. This work may not be translated or copied in whole or in part without written permission of the publisher (Springer-Verlag, 175 Fifth Avenue, New York, New Y 10010, U.S.A.), except for brief excerpts in connection with reviews or scholarly analysis. Us connection with any form of information storage and retrieval, electronic adaptation, compu software, or by similar or dissimilar methodology now known or hereafter developed is forbidc

The use of general descriptive names, trade names, trademarks, etc. in this publication, eve the former are not especially identified, is not to be taken as a sign that such names, as understc by the Trade Marks and Merchandise Marks Act, may accordingly be used freely by anyone

Typeset by Asco Trade Typesetting Ltd., Hong Kong.
Printed and bound by R. R. Donnelley & Sons, Harrisonburg, Virginia.
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-96371-5 Springer-Verlag New York Berlin Heidelberg
ISBN 3-540-96371-5 Springer-Verlag Berlin Heidelberg New York

To
Robert and Roger
with whom I first learned
the meaning of collaboration

# Preface

The book divides naturally into several parts according to the level of the material, the background required of the reader, and the style of presentation with respect to details of proofs. For example, the first part, to Chapter 6, is undergraduate in level, the second part requires a background in Galois theory and the third some complex analysis, while the last parts, from Chapter 12 on, are mostly at graduate level. A general outline of much of the material can be found in Tate's colloquium lectures reproduced as an article in *Inventiones* [1974].

The first part grew out of Tate's 1961 Haverford Philips Lectures as an attempt to write something for publication closely related to the original Tate notes which were more or less taken from the tape recording of the lectures themselves. This includes parts of the Introduction and the first six chapters. The aim of this part is to prove, by elementary methods, the Mordell theorem on the finite generation of the rational points on elliptic curves defined over the rational numbers.

In 1970 Tate returned to Haverford to give again, in revised form, the original lectures of 1961 and to extend the material so that it would be suitable for publication. This led to a broader plan for the book.

The second part, consisting of Chapters 7 and 8, recasts the arguments used in the proof of the Mordell theorem into the context of Galois cohomology and descent theory. The background material in Galois theory that is required is surveyed at the beginning of Chapter 7 for the convenience of the reader.

The third part, consisting of Chapters 9, 10, and 11, is on analytic theory. A background in complex analysis is assumed and in Chapter 10 elementary results on $p$-adic fields, some of which were introduced in Chapter 5, are used in our discussion of Tate's theory of $p$-adic theta functions. This section is based on Tate's 1972 Haverford Philips Lectures.

此为试读,需要完整PDF请访问: www.ertongbook.com

The fourth part, namely Chapters 12, 13, and 14, covers that part of algebraic theory which uses algebraic geometry seriously. This is the theory of endomorphisms and elliptic curves over finite and local fields. While earlier chapters treated an elliptic curve as a curve defined by a cubic equation, here the theory of endomorphisms requires a more subtle approach with varieties and, for some questions of bad reduction, schemes. This part is very carefully covered in the book by Silverman [1985], and thus we frequently do not give detailed arguments. We recommend this book as a reference while reading this part.

The fifth part, consisting of Chapters 15, 16, and 17, surveys recent results in the arithmetic theory of elliptic curves. Here again few proofs are given, but various elementary background results are included for the beginner reader in order to make the main references more accessible. The three chapters include part of Serre's theory of Galois representations including a result of Falting's which played an important role in the proof of the Mordell conjecture, $L$-functions of elliptic curves over a number field, the special case of complex multiplication, modular curves, and finally the Birch and Swinnerton-Dyer conjecture. There is a progress discussion on the Birch and Swinnerton-Dyer conjecture describing the contributions of Coates and Wiles, of Greenberg, and of Gross and Zagier. We also mention the work of Goldfeld which reduced the effective lower bound question of Gauss for the class number of imaginary quadratic fields to a special case of the conjectural framework of Birch and Swinnerton-Dyer contained in the work of Gross and Zagier.

Finally the book concludes with an appendix by Ruth Lawrence. She did all the hundred or so exercises in the book, and from this extensive work the idea of an appendix evolved. It consists of comments on all the exercises including complete solutions for a representative number. Usually there are just answers or hints on how to proceed together with remarks on the level of difficulty. This appendix should be a great help for the reader starting the subject and wishing to do some of the exercises.

# Acknowledgments

Being an amateur in the field of elliptic curves, I would have never completed a project like this without the professional and moral support of a great number of persons and institutions over the long period during which this book was being written.

John Tate's treatment of an advanced subject, the arithmetic of elliptic curves, in an undergraduate context has been an inspiration for me during the last 25 years while at Haverford. The general outline of the project, together with many of the details of the exposition, owe so much to Tate's generous help.

The E.N.S. course by J.-P. Serre of four lectures in June 1970 together with two Haverford lectures on elliptic curves were very important in the early development of the manuscript. I wish to thank him also for many stimulating discussions. Elliptic curves were in the air during the summer seasons at the I.H.E.S. around the early 1970s. I wish to thank P. Deligne, N. Katz, S. Lichtenbaum, and B. Mazur for many helpful conversations during that period. It was the Haverford College Faculty Research Fund that supported many times my stays at the I.H.E.S.

During the year 1974–5, the summer of 1976, the year 1981–2, and the spring of 1986, I was a guest of the Bonn Mathematics Department SFB and later the Max Planck Institute. I wish to thank Professor F. Hirzebruch for making possible time to work in a stimulating atmosphere and for his encouragement in this work. An early version of the first half of the book was the result of a Bonn lecture series on Elliptische Kurven. During these periods, I profited frequently from discussions with G. Harder and A. Ogg.

Conversations with B. Gross were especially important for realizing the final form of the manuscript during the early 1980s. I am very thankful for his encouragement and help. In the spring of 1983 some of the early chapters of

the book were used by K. Rubin in the Princeton Junior Seminar, and I thank him for several useful suggestions. During the same time, J. Coates invited me to an Oberwolfach conference on elliptic curves where the final form of the manuscript evolved.

During the final stages of the manuscript, both R. Greenberg and R. Rosen read through the later chapters, and I am grateful for their comments. I would like to thank P. Landweber for a very careful reading of the manuscript and many useful comments.

Ruth Lawrence read the early chapters along with working the exercises. Her contribution was very great with her appendix on the exercises and suggested improvements in the text. I wish to thank her for this very special addition to the book.

Free time from teaching at Haverford College during the year 1985–6 was made possible by a grant from the Vaughn Foundation. I wish to express my gratitude to Mr. James Vaughn for this support, for this project as well as others, during this difficult last period of the preparation of the manuscript.

# Contents


Introduction to Rational Points on Plane Curves 1
§1. Rational Lines in the Projective Plane 2
§2. Rational Points on Conics 5
§3. Pythagoras, Diophantus, and Fermat 7
§4. Rational Cubics and Mordell's Theorem 10
§5. The Group Law on Cubic Curves and Elliptic Curves 14
§6. Rational Points on Rational Curves. Faltings and the Mordell Conjecture 17
§7. Real and Complex Points on Elliptic Curves 19

CHAPTER 1
Elementary Properties of the Chord-Tangent Group Law on a Cubic Curve 22
§1. Chord-Tangent Computational Methods on a Normal Cubic Curve 22
§2. Illustrations of the Elliptic Curve Group Law 27
§3. The Curves with Equations $y^2 = x^3 + ax$ and $y^2 = x^3 + a$ 33
§4. Multiplication by 2 on an Elliptic Curve 36
§5. Remarks on the Group Law on Singular Cubics 39

CHAPTER 2
Plane Algebraic Curves 43
§1. Projective Spaces 43
§2. Irreducible Plane Algebraic Curves and Hypersurfaces 45
§3. Elements of Intersection Theory for Plane Curves 48
§4. Multiple or Singular Points 50

Appendix to Chapter 2
Factorial Rings and Elimination Theory 55
§1. Divisibility Properties of Factorial Rings 55

§2. Factorial Properties of Polynomial Rings 57
§3. Remarks on Valuations and Algebraic Curves 58
§4. Resultant of Two Polynomials 59

CHAPTER 3
Elliptic Curves and Their Isomorphisms 62
§1. The Group Law on a Nonsingular Cubic 62
§2. Elliptic Curves in Normal Form 64
§3. The Discriminant and the Invariant $j$ 67
§4. Isomorphism Classification in Characteristics $\neq 2, 3$ 70
§5. Isomorphism Classification in Characteristic 3 72
§6. Isomorphism Classification in Characteristic 2 74
§7. Singular Cubic Curves 77

CHAPTER 4
Families of Elliptic Curves and Geometric Properties of Torsion Points 81
§1. The Legendre Family 81
§2. Families of Curves with Points of Order 3: The Hessian Family 84
§3. The Jacobi Family 87
§4. Tate's Normal Form for a Cubic with a Torsion Point 88
§5. An Explicit 2-Isogeny 91
§6. Examples of Noncyclic Subgroups of Torsion Points 96

CHAPTER 5
Reduction mod $p$ and Torsion Points 99
§1. Reduction mod $p$ of Projective Space and Curves 99
§2. Minimal Normal Forms for an Elliptic Curve 102
§3. Good Reduction of Elliptic Curves 105
§4. The Kernel of Reduction mod $p$ and the $p$-Adic Filtration 107
§5. Torsion in Elliptic Curves over $\mathbf{Q}$: Nagell–Lutz Theorem 112
§6. Computability of Torsion Points on Elliptic Curves from Integrality and Divisibility Properties of Coordinates 114
§7. Bad Reduction and Potentially Good Reduction 116
§8. Tate's Theorem on Good Reduction over the Rational Numbers 118

CHAPTER 6
Proof of Mordell's Finite Generation Theorem 120
§1. A Condition for Finite Generation of an Abelian Group 120
§2. Fermat Descent and $x^4 + y^4 = 1$ 122
§3. Finiteness of $(E(\mathbf{Q}):2E(\mathbf{Q}))$ for $E = E[a, b]$ 123
§4. Finiteness of the Index $(E(k):2E(k))$ 124
§5. Quasilinear and Quasiquadratic Maps 127
§6. The General Notion of Height on Projective Space 130
§7. The Canonical Height and Norm on an Elliptic Curve 133
§8. The Canonical Height on Projective Spaces over Global Fields 136

CHAPTER 7
Galois Cohomology and Isomorphism Classification of Elliptic Curves over Arbitrary Fields 138
§1. Galois Theory 138
§2. Group Actions on Sets and Groups 141
§3. Principal Homogeneous $G$-Sets and the First Cohomology Set $H^1(G, A)$ 143
§4. Long Exact Sequence in $G$-Cohomology 146
§5. Some Calculations with Galois Cohomology 147
§6. Galois Cohomology Classification of Curves with Given $j$-Invariant 150

CHAPTER 8
Descent and Galois Cohomology 152
§1. Homogeneous Spaces over Elliptic Curves 152
§2. Primitive Descent Formalism 155
§3. Basic Descent Formalism 158

CHAPTER 9
Elliptic and Hypergeometric Functions 162
§1. Quotients of the Complex Plane by Discrete Subgroups 162
§2. Generalities on Elliptic Functions 164
§3. The Weierstrass $\wp$-Function 166
§4. The Differential Equation for $\wp(z)$ 169
§5. Preliminaries on Hypergeometric Functions 174
§6. Periods Associated with Elliptic Curves; Elliptic Integrals 178

CHAPTER 10
Theta Functions 183
§1. Jacobi $q$-Parametrization: Application to Real Curves 183
§2. Introduction to Theta Functions 187
§3. Embeddings of a Torus by Theta Functions 189
§4. Relation Between Theta Functions and Elliptic Functions 191
§5. The Tate Curve 192
§6. Introduction to Tate's Theory of $p$-Adic Theta Functions 197

CHAPTER 11
Modular Functions 202
§1. Isomorphism and Isogeny Classification of Complex Tori 202
§2. Families of Elliptic Curves with Additional Structures 204
§3. The Modular Curves $X(N)$, $X_1(N)$, and $X_0(N)$ 208
§4. Modular Functions 213
§5. The $L$-Function of a Modular Form 215
§6. Elementary Properties of Euler Products 217
§7. Hecke Operators 220

CHAPTER 12
Endomorphisms of Elliptic Curves 222
§1. Isogenies and Division Points for Complex Tori 223

此为试读,需要完整PDF请访问: www.ertongbook.com

§2. Symplectic Pairings on Lattices and Division Points 224
§3. Isogenies in the General Case 226
§4. Endomorphisms and Complex Multiplication 230
§5. The Tate Module of an Elliptic Curve 234
§6. Endomorphisms and the Tate Module 236
§7. Expansions Near the Origin and the Formal Group 237

CHAPTER 13
Elliptic Curves over Finite Fields 242
§1. The Riemann Hypothesis for Elliptic Curves over a Finite Field 243
§2. Generalities on Zeta Functions of Curves over a Finite Field 245
§3. Definition of Supersingular Elliptic Curves 248
§4. Number of Supersingular Elliptic Curves 252
§5. Points of Order $p$ and Supersingular Curves 253
§6. The Endomorphism Algebra and Supersingular Curves 255
§7. Summary of Criteria for a Curve To Be Supersingular 257
§8. Tate's Description of Homomorphisms 259

CHAPTER 14
Elliptic Curves over Local Fields 262
§1. The Canonical $p$-Adic Filtration on the Points of an Elliptic Curve over a Local Field 262
§2. The Néron Minimal Model 264
§3. Galois Criterion for Good Reduction of Néron–Ogg–Šafarevič 267

CHAPTER 15
Elliptic Curves over Global Fields and $\ell$-Adic Representations 272
§1. Minimal Normal Cubic Forms over a Dedekind Ring 272
§2. Generalities on $\ell$-Adic Representations 274
§3. Galois Representations and the Néron–Ogg–Šafarevič Criterion in the Global Case 277
§4. Ramification Properties of $\ell$-Adic Representations of Number Fields: Čebotarev's Density Theorem 279
§5. Rationality Properties of Frobenius Elements in $\ell$-Adic Representations: Variation of $\ell$ 282
§6. Weight Properties of Frobenius Elements in $\ell$-Adic Representations: Faltings' Finiteness Theorem 284
§7. Tate's Conjecture, Šafarevič's Theorem, and Faltings' Proof 286
§8. Image of $\ell$-Adic Representations of Elliptic Curves: Serre's Open Image Theorem 288

CHAPTER 16
$L$-Function of an Elliptic Curve and Its Analytic Continuation 290
§1. Remarks on Analytic Methods in Arithmetic 290
§2. Zeta Functions of Curves over $\mathbf{Q}$ 291
§3. Hasse–Weil $L$-Function and the Functional Equation 293
§4. Classical Abelian $L$-Functions and Their Functional Equations 296

§5. Grössencharacters and Hecke $L$-Functions 299
§6. Deuring's Theorem on the $L$-Function of an Elliptic Curve with Complex Multiplication 302
§7. Eichler–Shimura Theory 304
§8. The Taniyama–Weil Conjecture 305

CHAPTER 17
Remarks on the Birch and Swinnerton-Dyer Conjecture 306
§1. The Conjecture Relating Rank and Order of Zero 306
§2. Rank Conjecture for Curves with Complex Multiplication I, by Coates and Wiles 308
§3. Rank Conjecture for Curves with Complex Multiplication II, by Greenberg and Rohrlich 308
§4. Rank Conjecture for Modular Curves by Gross and Zagier 309
§5. Goldfeld's Work on the Class Number Problem and Its Relation to the Birch and Swinnerton-Dyer Conjecture 310
§6. The Conjecture of Birch and Swinnerton-Dyer on the Leading Term 311
§7. Heegner Points and the Derivative of the $L$-Function at $s = 1$, after Gross and Zagier 312
§8. Postscript: October 1986 313

APPENDIX
Guide to the Exercises by Ruth Lawrence 315

Bibliography 333

Index 345

# Introduction to Rational Points on Plane Curves

This introduction is designed to bring up some of the main issues of the book in an informal way so that the reader with only a minimal background in mathematics can get an idea of the character and direction of the subject.

An elliptic curve, viewed as a plane curve, is given by a "nonsingular" cubic equation. We wish to point out what is special about the class of elliptic curves among all plane curves from the point of view of arithmetic. In the process the geometry of the curve also enters the picture.

For the first considerations our plane curves are defined by a polynomial equation in two variables $f(x, y) = 0$ with rational coefficients. The main invariant of this $f$ is its degree, a natural number. In terms of plane analytic geometry there is a locus $C_f$ of this equation in the $x$, $y$-plane where the definition is that the point $(x, y)$ is on the locus $C_f$ provided it satisfies the equation $f(x, y) = 0$ as real numbers. To emphasize that the locus consists of points with real coordinates (so is in $\mathbf{R}^2$), we denote this real locus by $C_f(\mathbf{R})$ and consider $C_f(\mathbf{R}) \subset \mathbf{R}^2$.

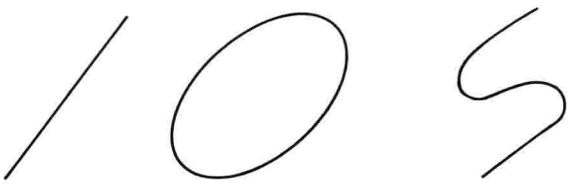
Since some curves $C_f$, like for example $f(x, y) = x^2 + y^2 + 1$, have an empty real locus $C_f(\mathbf{R})$, it is always useful to work also with the complex locus $C_f(\mathbf{C})$ contained in $\mathbf{C}^2$ even though it cannot be completely pictured geometrically.This is especially true for geometric considerations involving the curve.

For arithmetic the locus of special interest is the set $C_f(\mathbf{Q})$ of rational points $(x, y) \in \mathbf{Q}^2$ satisfying $f(x, y) = 0$, that is, points whose coordinates are rational numbers. The fundamental problem is the description of this set $C_f(\mathbf{Q})$. An elementary question is whether or not $C_f(\mathbf{Q})$ is finite or even empty.

The problem is attacked by a combination of geometric and arithmetic arguments using the inclusions $C_f(\mathbf{Q}) \subset C_f(\mathbf{R}) \subset C_f(\mathbf{C})$. A locus $C_f(\mathbf{Q})$ is either compared with another locus $C_g(\mathbf{Q})$, which is better understood, as we illus-

trate for lines where $\deg(f) = 1$ and conics where $\deg(f) = 2$ or by internal operations which is the case for elliptic curves.

In terms of the real locus, curves of degree 1, degree 2, and degree 3 can be pictured respectively as follows.



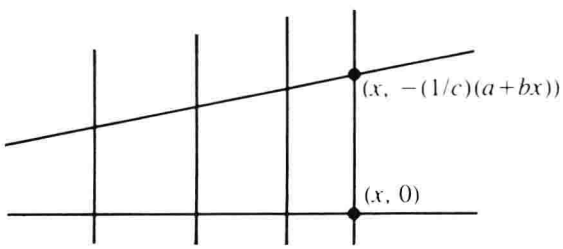
## §1. Rational Lines in the Projective Plane

Plane curves $C_f$ can be defined for any nonconstant complex polynomial $f(x, y) \in \mathbf{C}[x, y]$ by the equation $f(x, y) = 0$. For a nonzero constant $k$ the equations $f(x, y) = 0$ and $kf(x, y) = 0$ have the same solutions and define the same plane curve $C_f = C_{kf}$. When $f$ has complex coefficients, there is only a complex locus defined. If $f$ has real coefficients or if $f$ differs from a real polynomial by a nonzero constant, then there is also a real locus with $C_f(\mathbf{R}) \subset C_f(\mathbf{C})$. Such curves are called real curves.

**(1.1) Definition.** A rational plane curve is one of the form $C_f$ where $f(x, y)$ is a polynomial with rational coefficients.

In the case of a rational plane curve $C_f$ we have rational, real, and complex points $C_f(\mathbf{Q}) \subset C_f(\mathbf{R}) \subset C_f(\mathbf{C})$ or loci.

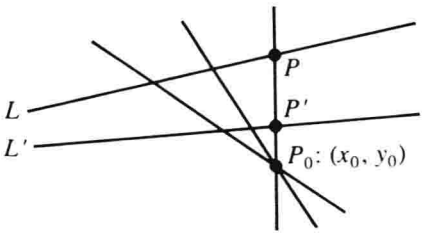
A polynomial of degree 1 has the form $f(x, y) = a + bx + cy$. Assume the coefficients are rational numbers and we begin by describing the set $C_f(\mathbf{Q})$. For $c$ nonzero we can set up a bijective correspondence between rational points on the line $C_f$ and on the $x$-axis using intersections with vertical lines.




The rational point $(x, 0)$ on the $x$-axis corresponds to the rational point $(x, -(1/c)(a + bx))$ on $C_f$. When $b$ is nonzero, the line $C_f(\mathbf{Q})$ can be put in bijective correspondence with the rational points on the $y$-axis using inter-

sections with horizontal lines. Observe that the vertical or horizontal lines relating rational points are themselves rational lines.

Instead of using parallel lines to relate points on two lines $L = C_f$ and $L' = C_{f'}$, we can use a point $P_0 = (x_0, y_0)$ not on either $L$ or $L'$ and relate points using the family of all lines through $P_0$. The pair $P$ on $L$ and $P'$ on $L'$ correspond when $P$, $P'$, and $P_0$ are all on a line.




If $L$ and $L'$ are rational lines, and if $P_0$ is a rational point, then for two corresponding points $P$ on $L$ and $P'$ on $L'$ the point $P$ is rational if and only if $P'$ is rational, and this defines a bijection between $C_f(\mathbf{Q})$ and $C_{f'}(\mathbf{Q})$.

Observe that there are special cases of lines through $P_0$, i.e., those parallel to $L$ or $L'$, which as matters stand do not give a corresponding pair of points between $L$ and $L'$. This is related to the fact that the two types of correspondence with parallel lines and lines through a point are really the same when viewed in terms of the projective plane, for parallel lines intersect at a point on the "line at infinity." The projective plane is the ordinary Cartesian or affine plane together with an additional line called the line at infinity.

**(1.2) Definition.** The projective plane $\mathbf{P}_2$ is the set of all triples $w:x:y$, where $w$, $x$, and $y$ are not all zero and the points $w:x:y = w':x':y'$ provided there is a nonzero constant $k$ with

$$w' = kw, \qquad x' = kx, \qquad y' = ky.$$

As with the affine plane and plane curves we have three basic cases

$$\mathbf{P}_2(\mathbf{Q}) \subset \mathbf{P}_2(\mathbf{R}) \subset \mathbf{P}_2(\mathbf{C})$$

consisting of triples proportional to $w:x:y$, where $x, y, w \in \mathbf{Q}$ for $\mathbf{P}_2(\mathbf{Q})$, where $x, y, z \in \mathbf{R}$ for $\mathbf{P}_2(\mathbf{R})$, and where $x, y, z \in \mathbf{C}$ for $P_2(\mathbf{C})$.

**(1.3) Remarks.** A line $C_F$ in $\mathbf{P}_2$ is the locus of all $w:x:y$ satisfying the equation $F(w, x, y) = aw + bx + cy = 0$. The line at infinity $L_\infty$ is given by the equation $w = 0$. A point in $\mathbf{P}_2 - L_\infty$ has the form $1:x:y$ after multiplying with the factor $w^{-1}$. The point $1:x:y$ in the projective plane corresponds to $(x, y)$ in the usual Cartesian plane. For a line $L$ given by $aw + bx + cy = 0$ and $L'$ given by $a'w + b'x + c'y = 0$ we have $L = L'$ if and only if $a:b:c = a':b':c'$ in the

projective plane. In particular the points $a:b:c$ in the projective plane ca be used to parametrize the lines in the projective plane.

From the theory of elimination of variables in beginning algebra we hav the following geometric assertions of projective geometry whose verificatio is left to the reader.

**(1.4) Assertion.** Two distinct points $P$ and $P'$ in $\mathbf{P}_2(\mathbf{C})$ lie on a unique line in the projective plane, and, further, if $P$ and $P'$ are rational points, then th line $L$ is rational. Two distinct lines $L$ and $L'$ in $\mathbf{P}_2(\mathbf{C})$ intersect at a uniqu point $P$, and, further, if $L$ and $L'$ are rational lines, then the intersection poin $P$ is rational.

The projective line $L$ with equation $L: aw + by + cy = 0$ determines th line $a + bx + cy = 0$ in the Cartesian plane. Two projective lines $L: aw + bx + cy = 0$ and $L': a'w + b'x + c'y = 0$ intersect on the line at infinity $w = 0$ if and only if $b:c = b':c'$, that is, the pairs $(b, c)$ and $(b', c')$ are proportiona The corresponding lines in the $x,y$-plane given by

$$a + bx + cy = 0 \quad \text{and} \quad a' + b'x + c'y = 0$$

have the same slope or are parallel exactly when the projective lines intersec at infinity. Now the reader is invited to reconsider the correspondence betwee rational points on two rational lines $L$ and $L'$ which arises by intersecting $L$ and $L'$ with all rational lines through a fixed point $P_0$ not on either $L$ or $L'$.

To define plane curves in projective space, we use nonzero homogeneou polynomials $F(w, x, y) \in \mathbf{C}[w, x, y]$. Then we have the relation $F(qw, qx, qy) = q^d F(w, x, y)$, where $q \in \mathbf{C}$ and $d$ is the degree of the homogenous polynomia $F(w, x, y)$. The locus $C_F$ is the set of all $w:x:y$ in the projective plane such tha $F(w, x, y) = 0$. Again the complex points of $C_F$ are denoted by $C_F(\mathbf{C}) \subset \mathbf{P}_2(\mathbf{C})$ and, moreover, $C_F(\mathbf{C}) = C_{F'}(\mathbf{C})$ if and only if $F(w, x, y)$ and $F'(w, x, y)$ ar proportional with a nonzero complex number. This assertion is not com pletely evident and is taken up again in Chapter 2.

**(1.5) Definition.** A rational (resp. real) plane curve in $\mathbf{P}_2$ is one of the form $C_F$ where $F(w, x, y)$ has rational (resp. real) coefficients.

As in the $x,y$-plane for a rational plane curve $C_F$, we have rational, real and complex points $C_F(\mathbf{Q}) \subset C_F(\mathbf{R}) \subset C_F(\mathbf{C})$.

**(1.6) Remark.** The above definition of a rational plane curve is an arithmeti notion, and it means the curve is defined over $\mathbf{Q}$. There is a geometric concep of rational curve (genus = 0) which should not be confused with (1.5). Geo metric rationality is defined in terms of the equation of the curve $f(x, y) = 0$ over $k$ and the field of fractions of $k[x, y]/(f)$.

此为试读,需要完整PDF请访问: www.ertongbook.com