Graduate Texts in Mathematics

Joseph H. Silverman

The Arithmetic of Elliptic Curves

2nd Edition

Springer

Graduate Texts in Mathematics 106

For other titles published in this series, go to
http://www.springer.com/series/136

Joseph H. Silverman

The Arithmetic of Elliptic Curves

Second Edition

With 14 Illustrations

Springer

Joseph H. Silverman
Department of Mathematics
Brown University
151 Thayer St.
Providence, RI 02912
USA
jhs@math.brown.edu

ISBN 978-0-387-09493-9 e-ISBN 978-0-387-09494-6
DOI 10.1007/978-0-387-09494-6
Springer Dordrecht Heidelberg London New York

Library of Congress Control Number: 2009926474

Mathematics Subject Classification (2000): 11-01, 11GXX, 14GXX, 11G05

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface to the Second Edition

In the preface to the first edition of this book I remarked on the paucity of introductory texts devoted to the arithmetic of elliptic curves. That unfortunate state of affairs has long since been remedied with the publication of many volumes, among which may be mentioned books by Cassels [43], Cremona [54], Husemöller [118], Knapp [127], McKean et. al [167], Milne [178], and Schmitt et. al [222] that highlight the arithmetic and modular theory, and books by Blake et. al [22], Cohen et. al [51], Hankerson et. al [107], and Washington [304] that concentrate on the use of elliptic curves in cryptography. However, even among this cornucopia of literature, I hope that this updated version of the original text will continue to be useful.

The past two decades have witnessed tremendous progress in the study of elliptic curves. Among the many highlights are the proof by Merel [170] of uniform boundedness for torsion points on elliptic curves over number fields, results of Rubin [215] and Kolyvagin [130] on the finiteness of Shafarevich–Tate groups and on the conjecture of Birch and Swinnerton-Dyer, the work of Wiles [311] on the modularity of elliptic curves, and the proof by Elkies [77] that there exist infinitely many supersingular primes. Although this introductory volume is unable to include proofs of these deep results, it will guide the reader along the beginning of the trail that ultimately leads to these summits.

My primary goals in preparing this second edition, over and above the pedagogical aims of the first edition, are the following:

- Update and expand results and references, especially in Appendix C, which includes a new section on the variation of the trace of Frobenius.
- Add a chapter devoted to algorithmic aspects of elliptic curves, with an emphasis on those features that are used in cryptography.
- Add a section on Szpiro's conjecture and the ABC conjecture.
- Correct, clarify, and simplify the proofs of some results.
- Correct numerous typographical and minor mathematical errors. However, since this volume has been entirely retypeset, I beg the reader's indulgence for any new typos that have been introduced.
- Significantly expand the selection of exercises.

It has been gratifying to see the first edition of this book become a standard text and reference in the subject. In order to maintain backward compatibility of cross-references, I have taken some care to leave the numbering system unchanged. Thus Proposition III.8.1 in the first edition remains Proposition III.8.1 in the second edition, and similarly for Exercise 3.5. New material has been assigned new numbers, and although there are many new exercises, they have been appended to the exercises from the first edition.

Electronic Resources: There are many computer packages that perform computations on elliptic curves. Of particular note are two free packages, Sage [275] and Pari [202], each of which implements an extensive collection of elliptic curve algorithms. For additional links to online elliptic curve resources, and for other material, the reader is invited to visit the *Arithmetic of Elliptic Curves* home page at

`www.math.brown.edu/~jhs/AECHome.html`

No book is ever free from error or incapable of being improved. I would be delighted to receive comments, positive or negative, and corrections from you, the reader. You can send mail to me at

`jhs@math.brown.edu`

Acknowledgments for the Second Edition

Many people have sent me extensive comments and corrections since the appearance of the first edition in 1986. To all of them, including in particular the following, my deepest thanks: Jeffrey Achter, Andrew Bremner, Frank Calegari, Jesse Elliott, Kirsten Eisenträger, Xander Faber, Joe Fendel, W. Fensch, Alexandru Ghitza, Grigor Grigorov, Robert Gross, Harald Helfgott, Franz Lemmermeyer, Dino Lorenzini, Ronald van Luijk, David Masser, Martin Olsson, Chol Park, Bjorn Poonen, Michael Reid, Michael Rosen, Jordan Risov, Robert Sarvis, Ed Schaefer, René Schoof, Nigel Smart, Jeroen Spandaw, Douglas Squirrel, Katherine Stange, Sinan Unver, John Voight, Jianqiang Zhao, Michael Zieve.

Providence, Rhode Island JOSEPH H. SILVERMAN
November, 2008

Preface to the First Edition

The preface to a textbook frequently contains the author's justification for offering the public "another book" on a given subject. For our chosen topic, the arithmetic of elliptic curves, there is little need for such an apologia. Considering the vast amount of research currently being done in this area, the paucity of introductory texts is somewhat surprising. Parts of the theory are contained in various books of Lang, especially [135] and [140], and there are books of Koblitz [129] and Robert [210] (the latter now out of print) that concentrate on the analytic and modular theory. In addition, there are survey articles by Cassels [41], which is really a short book, and Tate [289], which is beautifully written, but includes no proofs. Thus the author hopes that this volume fills a real need, both for the serious student who wishes to learn basic facts about the arithmetic of elliptic curves and for the research mathematician who needs a reference source for those same basic facts.

Our approach is more algebraic than that taken in, say, [135] or [140], where many of the basic theorems are derived using complex analytic methods and the Lefschetz principle. For this reason, we have had to rely somewhat more on techniques from algebraic geometry. However, the geometry of (smooth) curves, which is essentially all that we use, does not require a great deal of machinery. And the small price paid in learning a little bit of algebraic geometry is amply repaid in a unity of exposition that, to the author, seems to be lacking when one makes extensive use of either the Lefschetz principle or lengthy, albeit elementary, calculations with explicit polynomial equations.

This last point is worth amplifying. It has been the author's experience that "elementary" proofs requiring page after page of algebra tend to be quite uninstructive. A student may be able to verify such a proof, line by line, and at the end will agree that the proof is complete. But little true understanding results from such a procedure. In this book, our policy is always to state when a result can be proven by such an elementary calculation, indicate briefly how that calculation might be done, and then to give a more enlightening proof that is based on general principles.

The basic (global) theorems in the arithmetic of elliptic curves are the Mordell–Weil theorem, which is proven in Chapter VIII and analyzed more closely in Chapter X, and Siegel's theorem, which is proven in Chapter IX. The reader desiring to reach these results fairly rapidly might take the following path:

I and II (briefly review), III (§§1–8), IV (§§1–6), V (§1)
VII (§§1–5), VIII (§§1–6), IX (§§1–7), X (§§1–6).

This material also makes a good one-semester course, possibly with some time left at the end for special topics. The present volume is built around the notes for such a course, taught by the author at M.I.T. during the spring term of 1983. Of course, there are many other ways to structure a course. For example, one might include all of chapters V and VI, skipping IX and, if pressed for time, X. Other important topics in the arithmetic of elliptic curves, which do not appear in this volume due to time and space limitations, are briefly discussed in Appendix C.

It is certainly true that some of the deepest results in the subject, such as Mazur's theorem bounding torsion over $\mathbb{Q}$ and Faltings' proof of the isogeny conjecture, require many of the resources of modern "SGA-style" algebraic geometry. On the other hand, one needs no machinery at all to write down the equation of an elliptic curve and to do explicit computations with it; so there are many important theorems whose proof requires nothing more than cleverness and hard work. Whether your inclination leans toward heavy machinery or imaginative calculations, you will find much that remains to be discovered in the arithmetic theory of elliptic curves. Happy Hunting!

Acknowledgements

In writing this book, I have consulted a great many sources. Citations have been included for major theorems, but many results that are now considered "standard" have been presented as such. In any case, I can claim no originality for any of the unlabeled theorems in this book, and I apologize in advance to anyone who may feel slighted. The excellent survey articles of Cassels [41] and Tate [289] served as guidelines for organizing the material. (The reader is especially urged to peruse the latter.) In addition to [41] and [289], other sources that were extensively consulted include [135], [139], [186], [210], and [236].

It would not be possible to catalogue all of the mathematicians from whom I learned this beautiful subject, but to all of them, my deepest thanks. I would especially like to thank John Tate, Barry Mazur, Serge Lang, and the "Elliptic Curves Seminar" group at Harvard (1977–1982), whose help and inspiration set me on the road that led to this book. I would also like to thank David Rohrlich and Bill McCallum for their careful reading of the original draft, Gary Cornell and the editorial staff at Springer-Verlag for encouraging me to undertake this project in the first place, and Ann Clee for her meticulous preparation of the manuscript. Finally, I would like to thank my wife, Susan, for her patience and understanding through the turbulent times during which this book was written, and also Deborah and Daniel, for providing much of the turbulence.

Cambridge, Massachusetts — JOSEPH H. SILVERMAN
September, 1985

Acknowledgments for the Second Printing

I would like to thank the following people, who kindly provided corrections that have been incorporated into this second revised printing: Andrew Baker, Arthur Baragar, Wah Keung Chan, Yen-Mei (Julia) Chen, Bob Colemen, Fred Diamond, David Fried, Dick Gross, Ron Jacobwitz, Kevin Keating, Masato Kuwata, Peter Landweber, H.W.

Lenstra Jr., San Ling, Bill McCallum, David Masser, Hwasin Park, Elisabeth Pyle, Ken Ribet, John Rhodes, David Rohrlich, Mike Rosen, Rene Schoof, Udi de Shalit, Alice Silverberg, Glenn Stevens, John Tate, Edlyn Teske, Jaap Top, Paul van Mulbregt, Larry Washington, Don Zagier.

It has unfortunately not been possible to include in this second printing the many important results proven during the past six years, such as the work of Kolyvagin and Rubin on the Birch and Swinnerton-Dyer conjectures (C.16.5) and the finiteness of the Shafarevich–Tate group (X.4.13), Ribet's proof that the conjecture of Shimuara–Taniyama–Weil (C.16.4) implies Fermat's Last Theorem, and recent work of Mestre on elliptic curves of high rank (C §20). The inclusion of such material (and more) will have to await an eventual second edition, so the reader should be aware that some of our general discussion, especially in Appendix C, is out of date. In spite of this obsolescence, it is our hope that this book will continue to provide a useful introduction to the study of the arithmetic of elliptic curves.

Providence, Rhode Island
August, 1992

JOSEPH H. SILVERMAN

Contents

APPENDIX C

Introduction

The study of Diophantine equations, that is, the solution of polynomial equations in integers or rational numbers, has a history stretching back to ancient Greece and beyond. The term *Diophantine geometry* is of more recent origin and refers to the study of Diophantine equations through a combination of techniques from algebraic number theory and algebraic geometry. On the one hand, the problem of finding integer and rational solutions to polynomial equations calls into play the tools of algebraic number theory that describe the rings and fields wherein those solutions lie. On the other hand, such a system of polynomial equations describes an algebraic variety, which is a geometric object. It is the interplay between these two points of view that is the subject of Diophantine geometry.

The simplest sort of equation is linear:

$$aX + bY = c, \qquad a, b, c \in \mathbb{Z}, \qquad a \text{ or } b \neq 0.$$

Such an equation always has rational solutions. It has integer solutions if and only if the greatest common divisor of a and b divides c, and if this occurs, then we can find all solutions using the Euclidean algorithm.

Next in order of difficulty come quadratic equations:

$$aX^2 + bXY + cY^2 + dX + eY + f = 0, \qquad a, \dots, f \in \mathbb{Z}, \quad a, b \text{ or } c \neq 0.$$

They describe conic sections, and by a suitable change of coordinates *with rational coefficients*, we can transform a given equation into one of the following forms:

$$\begin{aligned} AX^2 + BY^2 &= C && \text{ellipse,} \\ AX^2 - BY^2 &= C && \text{hyperbola,} \\ AX + BY^2 &= 0 && \text{parabola.} \end{aligned}$$

For quadratic equations we have the following powerful theorem that aids in their solution.

Hasse–Minkowski Theorem 0.1. ([232, IV Theorem 8]) *Let $f(X,Y) \in \mathbb{Q}[X,Y]$ be a quadratic polynomial. The equation $f(X,Y) = 0$ has a solution $(x,y) \in \mathbb{Q}^2$ if and only if it has a solution $(x,y) \in \mathbb{R}^2$ and a solution $(x,y) \in \mathbb{Q}_p^2$ for every prime p. (Here $\mathbb{Q}_p$ is the field of p-adic numbers.)*

In other words, a quadratic polynomial has a solution in $\mathbb{Q}$ if and only if it has a solution in every completion of $\mathbb{Q}$. Hensel's lemma says that checking for solutions in $\mathbb{Q}_p$ is more or less the same as checking for solutions in the finite field $\mathbb{Z}/p\mathbb{Z}$, and this is turn is easily accomplished using quadratic reciprocity. We summarize the steps that go into the Diophantine analysis of quadratic equations.

(1) Analyze the equations over finite fields [quadratic reciprocity].
(2) Use this information to study the equations over complete local fields $\mathbb{Q}_p$ [Hensel's lemma]. (We must also analyze them over $\mathbb{R}$.)
(3) Piece together the local information to obtain results for the global field $\mathbb{Q}$ [Hasse principle].

Where does the geometry appear? Linear and quadratic equations in two variables define curves of genus zero. The above discussion says that we have a fairly good understanding of the arithmetic of such curves. The next simplest case, namely the arithmetic properties of curves of genus one (which are given by cubic equations in two variables), is our object of study in this book. The arithmetic of these so-called *elliptic curves* already presents complexities on which much current research is centered. Further, they provide a standard testing ground for conjectures and techniques that can then be fruitfully applied to the study of curves of higher genus and (abelian) varieties of higher dimension.

Briefly, the organization of this book is as follows. After two introductory chapters giving basic material on algebraic geometry, we start by studying the geometry of elliptic curves over algebraically closed fields (Chapter III). We then follow the program outlined above and investigate the properties of elliptic curves over finite fields (Chapter V), local fields (Chapters VI, VII), and global (number) fields (Chapters VIII, IX, X). Our understanding of elliptic curves over finite and local fields will be fairly satisfactory. However, it turns out that the analogue of the Hasse–Minkowski theorem is false for polynomials of degree greater than 2. This means that the transition from local to global is far more tenuous than in the degree 2 case. We study this problem in some detail in Chapter X. Finally, in Chapter XI we investigate computational aspects of the theory of elliptic curves, especially those that have become important in the field of cryptography.

The theory of elliptic curves is rich, varied, and amazingly vast. The original aim of this book was to provide an essentially self-contained introduction to the basic arithmetic properties of elliptic curves. Even such a limited goal proved to be too ambitious. The material described above is approximately half of what the author had hoped to include. The reader will find a brief discussion and list of references for the omitted topics in Appendix C, about half of which are covered in the companion volume [266] to this book.

Our other goal, that of being self-contained, has been more successful. We have, of course, felt free to state results that every reader should know, even when the proofs are far beyond the scope of this book. However, we have endeavored not to use such results for making further deductions. There are three major exceptions to this general policy. First, we do not prove that every elliptic curve over $\mathbb{C}$ is uniformized by elliptic functions (VI.5.1). This result fits most naturally into a discussion of modular functions, which is one of the omitted topics; it is covered [266, I §4] in the companion volume. Second, we do not prove that over a complete local field, the "nonsingular" points sit with finite index inside the set of all points (VII.6.1). This can be proven by quite explicit polynomial computations (cf. [283]), but they are rather lengthy and have not been included for lack of space. (This result is proven in the companion volume [266, IV §§8, 9].) Finally, in the study of integral points on elliptic curves, we make use of Roth's theorem (IX.1.4) without giving a proof. We include a brief discussion of the proof in (IX §8), and the reader who wishes to see the myriad details can proceed to one of the references listed there.

The prerequisites for reading this book are fairly modest. We assume that the reader has had a first course in algebraic number theory, and thus is acquainted with number fields, rings of integers, prime ideals, ramification, absolute values, completions, etc. The contents of any basic text on algebraic number theory, such as [142, Part I] or [25], should more than suffice. Chapter VI, which deals with elliptic curves over $\mathbb{C}$, assumes a familiarity with the basic principles of complex analysis. In Chapter X, we use a little bit of group cohomology, but just H^0 and H^1. The reader will find in Appendix B the cohomological facts needed to read Chapter X. Finally, since our approach is mainly algebraic, there is the question of background material in algebraic geometry. On the one hand, since much of the theory of elliptic curves can be obtained through the use of explicit equations and calculations, we do not want to require that the reader already know a great deal of algebraic geometry. On the other hand, this being a book on number theory and not algebraic geometry, it would not be reasonable to spend half the book developing from first principles the algebro-geometric facts that we will use. As a compromise, the first two chapters give an introduction to the algebraic geometry of varieties and curves, stating all of the facts that we need, giving complete references, and providing enough proofs so that the reader can gain a flavor for some of the basic techniques used in algebraic geometry.

Numerous exercises have been included at the end of each chapter. The reader desiring to gain a real understanding of the subject is urged to attempt as many as possible. Some of these exercises are (special cases of) results that have appeared in the literature. A list of comments and citations for the exercises may be found on page 461. Exercises with a single asterisk are somewhat more difficult, while two asterisks signal an unsolved problem.

References

Bibliographical references are enclosed in square brackets, e.g., [289, Theorem 6]. Cross-references to theorems, propositions, lemmas, etc., are given in full with the chapter roman numeral or appendix letter, e.g., (IV.3.1) and (B.2.1). Reference to an exercise is given by the chapter number followed by the exercise number, e.g., Exercise 3.6.

Standard Notation

Throughout this book, we use the symbols

$$\mathbb{Z},\ \mathbb{Q},\ \mathbb{R},\ \mathbb{C},\ \mathbb{F}_q,\ \text{and } \mathbb{Z}_\ell$$

to denote the integers, rational numbers, real numbers, complex numbers, a field with q elements, and the ℓ-adic integers, respectively. Further, if R is any ring, then R^* denotes the group of invertible elements of R, and if A is an abelian group, then $A[m]$ denotes the subgroup of A consisting of elements of order dividing m. For a more complete list of notation, see page 467.

Chapter I

Algebraic Varieties

In this chapter we describe the basic objects that arise in the study of algebraic geometry. We set the following notation, which will be used throughout this book.

K	a perfect field, i.e., every algebraic extension of K is separable.
$\bar{K}$	a fixed algebraic closure of K.
$G_{\bar{K}/K}$	the Galois group of $\bar{K}/K$.

For this chapter, we also let m and n denote positive integers.

The assumption that K is a perfect field is made solely to simplify our exposition. However, since our eventual goal is to do arithmetic, the field K will eventually be taken to be an algebraic extension of $\mathbb{Q}$, $\mathbb{Q}_p$, or $\mathbb{F}_p$. Thus this restriction on K need not concern us unduly.

For a more extensive exposition of the basic concepts that appear in this chapter, we refer the reader to any introductory book on algebraic geometry, such as [95], [109], [111], or [243].

I.1 Affine Varieties

We begin our study of algebraic geometry with Cartesian (or affine) n-space and its subsets defined by zeros of polynomials.

Definition. *Affine n-space* (*over K*) is the set of n-tuples

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{P = (x_1, \dots, x_n) : x_i \in \bar{K}\}.$$

Similarly, the *set of K-rational points of* $\mathbb{A}^n$ is the set

$$\mathbb{A}^n(K) = \{P = (x_1, \dots, x_n) \in \mathbb{A}^n : x_i \in K\}.$$

J.H. Silverman, *The Arithmetic of Elliptic Curves, Second Edition*, Graduate Texts in Mathematics 106, DOI 10.1007/978-0-387-09494-6_I,

Notice that the Galois group $G_{\bar{K}/K}$ acts on $\mathbb{A}^n$; for $\sigma \in G_{\bar{K}/K}$ and $P \in \mathbb{A}^n$,

$$P^\sigma = (x_1^\sigma, \dots, x_n^\sigma).$$

Then $\mathbb{A}^n(K)$ may be characterized by

$$\mathbb{A}^n(K) = \{P \in \mathbb{A}^n : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

Let $\bar{K}[X] = \bar{K}[X_1, \dots, X_n]$ be a polynomial ring in n variables, and let $I \subset \bar{K}[X]$ be an ideal. To each such I we associate a subset of $\mathbb{A}^n$,

$$V_I = \bigl\{P \in \mathbb{A}^n : f(P) = 0 \text{ for all } f \in I\bigr\}.$$

Definition. An (*affine*) *algebraic set* is any set of the form V_I. If V is an algebraic set, the *ideal of* V is given by

$$I(V) = \bigl\{f \in \bar{K}[X] : f(P) = 0 \text{ for all } P \in V\bigr\}.$$

An algebraic set is *defined over* K if its ideal $I(V)$ can be generated by polynomials in $K[X]$. We denote this by V/K. If V is defined over K, then the *set of K-rational points of* V is the set

$$V(K) = V \cap \mathbb{A}^n(K).$$

Remark 1.1. Note that by the Hilbert basis theorem [8, 7.6], [73, §1.4], all ideals in $\bar{K}[X]$ and $K[X]$ are finitely generated.

Remark 1.2. Let V be an algebraic set, and consider the ideal $I(V/K)$ defined by

$$I(V/K) = \bigl\{f \in K[X] : f(P) = 0 \text{ for all } P \in V\bigr\} = I(V) \cap K[X].$$

Then we see that V is defined over K if and only if

$$I(V) = I(V/K)\bar{K}[X].$$

Now suppose that V is defined over K and let $f_1, \dots, f_m \in K[X]$ be generators for $I(V/K)$. Then $V(K)$ is precisely the set of solutions $(x_1, \dots, x_n)$ to the simultaneous polynomial equations

$$f_1(X) = \cdots = f_m(X) = 0 \quad \text{with } x_1, \dots, x_n \in K.$$

Thus one of the fundamental problems in the subject of *Diophantine geometry*, namely the solution of polynomial equations in rational numbers, may be said to be the problem of describing sets of the form $V(K)$ when K is a number field.

Notice that if $f(X) \in K[X]$ and $P \in \mathbb{A}^n$, then for any $\sigma \in G_{\bar{K}/K}$,

$$f(P^\sigma) = f(P)^\sigma.$$

Hence if V is defined over K, then the action of $G_{\bar{K}/K}$ on $\mathbb{A}^n$ induces an action on V, and clearly

$$V(K) = \{P \in V : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

Example 1.3.1. Let V be the algebraic set in $\mathbb{A}^2$ given by the single equation

$$X^2 - Y^2 = 1.$$

Clearly V is defined over K for any field K. Let us assume that $\mathrm{char}(K) \neq 2$. Then the set $V(K)$ is in one-to-one correspondence with $\mathbb{A}^1(K) \smallsetminus \{0\}$, one possible map being

$$\begin{aligned} \mathbb{A}^1(K) \smallsetminus \{0\} &\longrightarrow V(K), \\ t &\longmapsto \left(\frac{t^2+1}{2t}, \frac{t^2-1}{2t} \right). \end{aligned}$$

Example 1.3.2. The algebraic set

$$V : X^n + Y^n = 1$$

is defined over $\mathbb{Q}$. Fermat's last theorem, proven by Andrew Wiles in 1995 [291, 311], states that for all $n \geq 3$,

$$V(\mathbb{Q}) = \begin{cases} \{(1,0), (0,1)\} & \text{if } n \text{ is odd}, \\ \{(\pm 1, 0), (0, \pm 1)\} & \text{if } n \text{ is even}. \end{cases}$$

Example 1.3.3. The algebraic set

$$V : Y^2 = X^3 + 17$$

has many $\mathbb{Q}$-rational points, for example

$$(-2, 3) \qquad (5234, 378661) \qquad \left(\frac{137}{64}, \frac{2651}{512} \right).$$

In fact, the set $V(\mathbb{Q})$ is infinite. See (I.2.8) and (III.2.4) for further discussion of this example.

Definition. An affine algebraic set V is called an (*affine*) *variety* if $I(V)$ is a prime ideal in $\bar{K}[X]$. Note that if V is defined over K, it is not enough to check that $I(V/K)$ is prime in $K[X]$. For example, consider the ideal $(X_1^2 - 2X_2^2)$ in $\mathbb{Q}[X_1, X_2]$.

Let V/K be a variety, i.e., V is a variety defined over K. Then the *affine coordinate ring of* V/K is defined by

$$K[V] = \frac{K[X]}{I(V/K)}.$$

The ring $K[V]$ is an integral domain. Its quotient field (field of fractions) is denoted by $K(V)$ and is called the *function field of* V/K. Similarly $\bar{K}[V]$ and $\bar{K}(V)$ are defined by replacing K with $\bar{K}$.

Note that since an element $f \in \bar{K}[V]$ is well-defined up to adding a polynomial vanishing on V, it induces a well-defined function $f : V \to \bar{K}$. If $f(X) \in \bar{K}[X]$ is any polynomial, then $G_{\bar{K}/K}$ acts on f by acting on its coefficients. Hence if V is defined over K, so $G_{\bar{K}/K}$ takes $I(V)$ into itself, then we obtain an action of $G_{\bar{K}/K}$ on $\bar{K}[V]$ and $\bar{K}(V)$. One can check (Exercise 1.12) that $K[V]$ and $K(V)$ are, respectively, the subsets of $\bar{K}[V]$ and $\bar{K}(V)$ fixed by $G_{\bar{K}/K}$. We denote the action of $\sigma \in G_{\bar{K}/K}$ on f by $f \mapsto f^\sigma$. Then for all points $P \in V$,

$$\bigl(f(P)\bigr)^\sigma = f^\sigma(P^\sigma).$$

Definition. Let V be a variety. The *dimension of* V, denoted by $\dim(V)$, is the transcendence degree of $\bar{K}(V)$ over $\bar{K}$.

Example 1.4. The dimension of $\mathbb{A}^n$ is n, since $\bar{K}(\mathbb{A}^n) = \bar{K}(X_1, \ldots, X_n)$. Similarly, if $V \subset \mathbb{A}^n$ is given by a single nonconstant polynomial equation

$$f(X_1, \ldots, X_n) = 0,$$

then $\dim(V) = n - 1$. (The converse is also true; see [111, I.1.2].) In particular, the examples described in (I.1.3.1), (I.1.3.2), and (I.1.3.3) all have dimension one.

In studying a geometric object, we are naturally interested in whether it looks reasonably "smooth." The next definition formalizes this notion in terms of the usual Jacobian criterion for the existence of a tangent plane.

Definition. Let V be a variety, $P \in V$, and $f_1, \ldots, f_m \in \bar{K}[X]$ a set of generators for $I(V)$. Then V is *nonsingular* (or *smooth*) *at* P if the $m \times n$ matrix

$$\left(\frac{\partial f_i}{\partial X_j}(P)\right)_{\substack{1 \le i \le m \\ 1 \le j \le n}}$$

has rank $n - \dim(V)$. If V is nonsingular at every point, then we say that V is *nonsingular* (or *smooth*).

Example 1.5. Let V be given by a single nonconstant polynomial equation

$$f(X_1, \ldots, X_n) = 0.$$

Then (I.1.4) tells us that $\dim(V) = n - 1$, so $P \in V$ is a singular point if and only if

$$\frac{\partial f}{\partial X_1}(P) = \cdots = \frac{\partial f}{\partial X_n}(P) = 0.$$

Since P also satisfies $f(P) = 0$, this gives $n + 1$ equations for the n coordinates of any singular point. Thus for a "randomly chosen" polynomial f, one would expect V to be nonsingular. We will not pursue this idea further, but see Exercise 1.1.

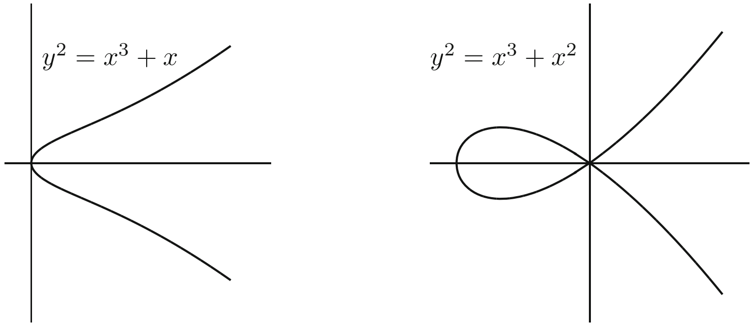

Figure 1.1: A smooth curve and a singular curve.

Example 1.6. Consider the two varieties

$$V_1 : Y^2 = X^3 + X \qquad \text{and} \qquad V_2 : Y^2 = X^3 + X^2.$$

Using (I.1.5), we see that any singular points on V_1 and V_2 satisfy, respectively,

$$V_1^{\text{sing}} : 3X^2 + 1 = 2Y = 0 \qquad \text{and} \qquad V_2^{\text{sing}} : 3X^2 + 2X = 2Y = 0.$$

Thus V_1 is nonsingular, while V_2 has one singular point, namely $(0, 0)$. The graphs of $V_1(\mathbb{R})$ and $V_2(\mathbb{R})$ illustrate the difference; see Figure 1.1.

There is another characterization of smoothness, in terms of the functions on the variety V, that is often quite useful. For each point $P \in V$, we define an ideal M_P of $\bar{K}[V]$ by

$$M_P = \{ f \in \bar{K}[V] : f(P) = 0 \}.$$

Notice that M_P is a maximal ideal, since there is an isomorphism

$$\bar{K}[V]/M_P \longrightarrow \bar{K} \quad \text{given by} \quad f \longmapsto f(P).$$

The quotient M_P/M_P^2 is a finite-dimensional $\bar{K}$-vector space.

Proposition 1.7. *Let V be a variety. A point $P \in V$ is nonsingular if and only if*

$$\dim_{\bar{K}} M_P/M_P^2 = \dim V.$$

PROOF. [111, I.5.1]. (See Exercise 1.3 for a special case.) □

Example 1.8. Consider the point $P = (0, 0)$ on the varieties V_1 and V_2 of (I.1.6). In both cases, M_P is the ideal of $\bar{K}[V]$ generated by X and Y, and M_P^2 is the ideal generated by X^2, XY, and Y^2. For V_1 we have

$$X = Y^2 - X^3 \equiv 0 \pmod{M_P^2},$$

so M_P/M_P^2 is generated by Y alone. On the other hand, for V_2 there is no nontrivial relationship between X and Y modulo M_P^2, so M_P/M_P^2 requires both X and Y as generators. Since each V_i has dimension one, (I.1.7) implies that V_1 is smooth at P and V_2 is not.

Definition. The *local ring of V at P*, denoted by $\bar{K}[V]_P$, is the localization of $\bar{K}[V]$ at M_P. In other words,

$$\bar{K}[V]_P = \{F \in \bar{K}(V) : F = f/g \text{ for some } f, g \in \bar{K}[V] \text{ with } g(P) \neq 0\}.$$

Notice that if $F = f/g \in \bar{K}[V]_P$, then $F(P) = f(P)/g(P)$ is well-defined. The functions in $\bar{K}[V]_P$ are said to be *regular* (or *defined*) at P.

I.2 Projective Varieties

Historically, projective space arose through the process of adding "points at infinity" to affine space. We define projective space to be the collection of lines through the origin in affine space of one dimension higher.

Definition. *Projective n-space* (*over K*), denoted by $\mathbb{P}^n$ or $\mathbb{P}^n(\bar{K})$, is the set of all $(n+1)$-tuples

$$(x_0, \dots, x_n) \in \mathbb{A}^{n+1}$$

such that at least one x_i is nonzero, modulo the equivalence relation

$$(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$$

if there exists a $\lambda \in \bar{K}^*$ such that $x_i = \lambda y_i$ for all i. An equivalence class

$$\{(\lambda x_0, \dots, \lambda x_n) : \lambda \in \bar{K}^*\}$$

is denoted by $[x_0, \dots, x_n]$, and the individual $x_0, \dots, x_n$ are called *homogeneous coordinates* for the corresponding point in $\mathbb{P}^n$. The *set of K-rational points in $\mathbb{P}^n$* is the set

$$\mathbb{P}^n(K) = \{[x_0, \dots, x_n] \in \mathbb{P}^n : \text{all } x_i \in K\}.$$

Remark 2.1. Note that if $P = [x_0, \dots, x_n] \in \mathbb{P}^n(K)$, it does not follow that each $x_i \in K$. However, choosing some i with $x_i \neq 0$, it does follow that $x_j/x_i \in K$ for every j.

Definition. Let $P = [x_0, \dots, x_n] \in \mathbb{P}^n(\bar{K})$. The *minimal field of definition for P* (*over K*) is the field

$$K(P) = K(x_0/x_i, \dots, x_n/x_i) \quad \text{for any } i \text{ with } x_i \neq 0.$$

The Galois group $G_{\bar{K}/K}$ acts on $\mathbb{P}^n$ by acting on homogeneous coordinates,

$$[x_0, \dots, x_n]^\sigma = [x_0^\sigma, \dots, x_n^\sigma].$$

This action is well-defined, independent of choice of homogeneous coordinates, since

$$[\lambda x_0, \dots, \lambda x_n]^\sigma = [\lambda^\sigma x_0^\sigma, \dots, \lambda^\sigma x_n^\sigma] = [x_0^\sigma, \dots, x_n^\sigma].$$

It is not difficult to check that

$$\mathbb{P}^n(K) = \{P \in \mathbb{P}^n : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K}\},$$

and that

$$K(P) = \text{fixed field of } \{\sigma \in G_{\bar{K}/K} : P^\sigma = P\};$$

see Exercise 1.12.

Definition. A polynomial $f \in \bar{K}[X] = \bar{K}[X_0, \dots, X_n]$ is *homogeneous of degree* d if

$$f(\lambda X_0, \dots, \lambda X_n) = \lambda^d f(X_0, \dots, X_n) \quad \text{for all } \lambda \in \bar{K}.$$

An ideal $I \subset \bar{K}[X]$ is *homogeneous* if it is generated by homogeneous polynomials.

Let f be a homogeneous polynomial and let $P \in \mathbb{P}^n$. It makes sense to ask whether $f(P) = 0$, since the answer is independent of the choice of homogeneous coordinates for P. To each homogeneous ideal I we associate a subset of $\mathbb{P}^n$ by the rule

$$V_I = \bigl\{P \in \mathbb{P}^n : f(P) = 0 \text{ for all homogeneous } f \in I\bigr\}.$$

Definition. A (*projective*) *algebraic set* is any set of the form V_I for a homogeneous ideal I. If V is a projective algebraic set, the (*homogeneous*) *ideal of* V, denoted by $I(V)$, is the ideal of $\bar{K}[X]$ generated by

$$\bigl\{f \in \bar{K}[X] : f \text{ is homogeneous and } f(P) = 0 \text{ for all } P \in V\bigr\}.$$

Such a V is *defined over* K, denoted by V/K, if its ideal $I(V)$ can be generated by homogeneous polynomials in $K[X]$. If V is defined over K, then the *set of K-rational points of* V is the set

$$V(K) = V \cap \mathbb{P}^n(K).$$

As usual, $V(K)$ may also be described as

$$V(K) = \{P \in V : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

Example 2.2. A *line* in $\mathbb{P}^2$ is an algebraic set given by a linear equation

$$aX + bY + cZ = 0$$

with $a, b, c \in \bar{K}$ not all zero. If, say, $c \neq 0$, then such a line is defined over any field containing a/c and b/c. More generally, a *hyperplane* in $\mathbb{P}^n$ is given by an equation

$$a_0X_0 + a_1X_1 + \cdots + a_nX_n = 0$$

with $a_i \in \bar{K}$ not all zero.

Example 2.3. Let V be the algebraic set in $\mathbb{P}^2$ given by the single equation

$$X^2 + Y^2 = Z^2.$$

Then for any field K with $\operatorname{char}(K) \neq 2$, the set $V(K)$ is isomorphic to $\mathbb{P}^1(K)$, for example by the map

$$\mathbb{P}^1(K) \longrightarrow V(K), \qquad [s, t] \longmapsto [s^2 - t^2, 2st, s^2 + t^2].$$

(For the precise definition of "isomorphic," see (I.3.5).)

Remark 2.4. A point of $\mathbb{P}^n(\mathbb{Q})$ has the form $[x_0,\ldots,x_n]$ with $x_i \in \mathbb{Q}$. Multiplying by an appropriate $\lambda \in \mathbb{Q}$, we can clear denominators and common factors from the x_i's. In other words, every $P \in \mathbb{P}^n(\mathbb{Q})$ may be written with homogeneous coordinates $[x_0,\ldots,x_n]$ satisfying

$$x_0,\ldots,x_n \in \mathbb{Z} \quad \text{and} \quad \gcd(x_0,\ldots,x_n) = 1.$$

Note that the x_i's are determined by P up to multiplication by -1.

Thus if an ideal of an algebraic set $V/\mathbb{Q}$ is generated by homogeneous polynomials $f_1,\ldots,f_m \in \mathbb{Q}[X]$, then describing $V(\mathbb{Q})$ is equivalent to finding the solutions to the homogeneous equations

$$f_1(X_0,\ldots,X_n) = \cdots = f_m(X_0,\ldots,X_n) = 0$$

in relatively prime integers $x_0,\ldots,x_n$.

Example 2.5. The algebraic set

$$V : X^2 + Y^2 = 3Z^2$$

is defined over $\mathbb{Q}$. However, $V(\mathbb{Q}) = \emptyset$. To see this, suppose that $[x,y,z] \in V(\mathbb{Q})$ with $x,y,z \in \mathbb{Z}$ and $\gcd(x,y,z) = 1$. Then

$$x^2 + y^2 \equiv 0 \pmod 3,$$

so the fact that -1 is not a square modulo 3 implies that

$$x \equiv y \equiv 0 \pmod 3.$$

Hence x^2 and y^2 are divisible by 3^2. It follows from the equation for V that 3 also divides z, which contradicts the assumption that $\gcd(x,y,z) = 1$.

This example illustrates a fundamental tool used in the study of Diophantine equations.

> *In order to show that an algebraic set $V/\mathbb{Q}$ has no $\mathbb{Q}$-rational points, it suffices to show that the corresponding homogeneous polynomial equations have no nonzero solutions modulo p for any one prime p (or even for one prime power p^r).*

A more succinct way to phrase this is to say that if $V(\mathbb{Q})$ is nonempty, then $V(\mathbb{Q}_p)$ is nonempty for every p-adic field $\mathbb{Q}_p$. Similarly, $V(\mathbb{R})$ would also be nonempty. One of the reasons that the study of Diophantine equations is so difficult is that the converse to this statement, which is called the *Hasse principle*, does not hold in general. An example, due to Selmer [225, 227], is the equation

$$V : 3X^3 + 4Y^2 + 5Z^3 = 0.$$

One can check that $V(\mathbb{Q}_p)$ is nonempty for every prime p, yet $V(\mathbb{Q})$ is empty. See, e.g., [41, §4] for a proof. Other examples are given in (X.6.5).

Definition. A projective algebraic set is called a (*projective*) *variety* if its homogeneous ideal $I(V)$ is a prime ideal in $\bar{K}[X]$.

It is clear that $\mathbb{P}^n$ contains many copies of $\mathbb{A}^n$. For example, for each $0 \le i \le n$, there is an inclusion

$$\begin{aligned} \phi_i : \mathbb{A}^n &\longrightarrow \mathbb{P}^n, \\ (y_1, \dots, y_n) &\longmapsto [y_1, y_2, \dots, y_{i-1}, 1, y_i, \dots, y_n]. \end{aligned}$$

We let H_i denote the hyperplane in $\mathbb{P}^n$ given by $X_i = 0$,

$$H_i = \bigl\{P = [x_0, \dots, x_n] \in \mathbb{P}^n : x_i = 0\bigr\},$$

and we let U_i be the complement of H_i,

$$U_i = \bigl\{P = [x_0, \dots, x_n] \in \mathbb{P}^n : x_i \ne 0\bigr\} = \mathbb{P}^n \smallsetminus H_i.$$

There is a natural bijection

$$\begin{aligned} \phi_i^{-1} : U_i &\longrightarrow \mathbb{A}^n, \\ [x_0, \dots, x_n] &\longmapsto \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \dots, \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, \dots, \frac{x_n}{x_i}, \right). \end{aligned}$$

(Note that for any point of $\mathbb{P}^n$ with $x_i \ne 0$, the quantities x_j/x_i are well-defined.) For a fixed i, we will normally identify $\mathbb{A}^n$ with the set U_i in $\mathbb{P}^n$ via the map ϕ_i.

Now let V be a projective algebraic set with homogeneous ideal $I(V) \subset \bar{K}[X]$. Then $V \cap \mathbb{A}^n$, by which we mean $\phi_i^{-1}(V \cap U_i)$ for some fixed i, is an affine algebraic set with ideal $I(V \cap \mathbb{A}^n) \subset \bar{K}[Y]$ given by

$$I(V \cap \mathbb{A}^n) = \bigl\{f(Y_1, \dots, Y_{i-1}, 1, Y_{i+1}, \dots, Y_n) : f(X_0, \dots, X_n) \in I(V)\bigr\}.$$

Notice that the sets $U_0, \dots, U_n$ cover all of $\mathbb{P}^n$, so any projective variety V is covered by subsets $V \cap U_0, \dots, V \cap U_n$, each of which is an affine variety via an appropriate ϕ_i^{-1}. The process of replacing the polynomial $f(X_0, \dots, X_n)$ with the polynomial $f(Y_1, \dots, Y_{i-1}, 1, Y_{i+1}, \dots, Y_n)$ is called *dehomogenization with respect to X_i*.

This process can be reversed. For any $f(Y) \in \bar{K}[Y]$, we define

$$f^*(X_0, \dots, X_n) = X_i^d f\left(\frac{X_0}{X_i}, \frac{X_1}{X_i}, \dots, \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, \dots, \frac{X_n}{X_i}\right),$$

where $d = \deg(f)$ is the smallest integer for which f^* is a polynomial. We say that f^* is the *homogenization of f with respect to X_i*.

Definition. Let $V \subset \mathbb{A}^n$ be an affine algebraic set with ideal $I(V)$, and consider V as a subset of $\mathbb{P}^n$ via

$$V \subset \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n.$$

The *projective closure of V*, denoted by $\bar{V}$, is the projective algebraic set whose homogeneous ideal $I(\bar{V})$ is generated by

$$\bigl\{f^*(X) : f \in I(V)\bigr\}.$$

Proposition 2.6. (a) *Let V be an affine variety. Then $\bar{V}$ is a projective variety, and*

$$V = \bar{V} \cap \mathbb{A}^n.$$

(b) *Let V be a projective variety. Then $V \cap \mathbb{A}^n$ is an affine variety, and either*

$$V \cap \mathbb{A}^n = \emptyset \qquad \textit{or} \qquad V = \overline{V \cap \mathbb{A}^n}.$$

(c) *If an affine (respectively projective) variety V is defined over K, then $\bar{V}$ (respectively $V \cap \mathbb{A}^n$) is also defined over K.*

PROOF. See [111, I.2.3] for (a) and (b). Part (c) is clear from the definitions. □

Remark 2.7. In view of (I.2.6), each affine variety may be identified with a unique projective variety. Notationally, since it is easier to deal with affine coordinates, we will often say "let V be a projective variety" and write down some inhomogeneous equations, with the understanding that V is the projective closure of the indicated affine variety W. The points of $V \smallsetminus W$ are called the *points at infinity* on V.

Example 2.8. Let V be the projective variety given by the equation

$$V : Y^2 = X^3 + 17.$$

This really means that V is the variety in $\mathbb{P}^2$ given by the homogeneous equation

$$\bar{Y}^2\bar{Z} = \bar{X}^3 + 17\bar{Z}^3,$$

the identification being

$$X = \bar{X}/\bar{Z}, \qquad Y = \bar{Y}/\bar{Z}.$$

This variety has one point at infinity, namely $[0, 1, 0]$, obtained by setting $\bar{Z} = 0$. Thus, for example,

$$V(\mathbb{Q}) = \bigl\{(x, y) \in \mathbb{A}^2(\mathbb{Q}) : y^2 = x^3 + 17\bigr\} \cup \bigl\{[0, 1, 0]\bigr\}.$$

In (I.1.3.3) we listed several points in $V(\mathbb{Q})$. The reader may verify (Exercise 1.5) that the line connecting any two points of $V(\mathbb{Q})$ intersects V in a third point of $V(\mathbb{Q})$ (provided that the line is not tangent to V). Using this secant line procedure repeatedly leads to infinitely many points in $V(\mathbb{Q})$, although this is by no means obvious. The variety V is an *elliptic curve*, and as such, it provides the first example of the varieties that will be our principal object of study in this book. See (III.2.4) for further discussion of this example.

Many important properties of a projective variety V may now be defined in terms of the affine subvariety $V \cap \mathbb{A}^n$.

Definition. Let V/K be a projective variety and choose $\mathbb{A}^n \subset \mathbb{P}^n$ such that $V \cap \mathbb{A}^n \neq \emptyset$. The *dimension of* V is the dimension of $V \cap \mathbb{A}^n$.

The *function field of* V, denoted by $K(V)$, is the function field of $V \cap \mathbb{A}^n$, and similarly for $\bar{K}(V)$. We note that for different choices of $\mathbb{A}^n$, the different $K(V)$ are canonically isomorphic, so we may identify them. (See (I.2.9) for another description of $K(V)$.)

Definition. Let V be a projective variety, let $P \in V$, and choose $\mathbb{A}^n \subset \mathbb{P}^n$ with $P \in \mathbb{A}^n$. Then V is *nonsingular* (or *smooth*) *at* P if $V \cap \mathbb{A}^n$ is nonsingular at P. The *local ring of* V *at* P, denoted by $\bar{K}[V]_P$, is the local ring of $V \cap \mathbb{A}^n$ at P. A function $F \in \bar{K}(V)$ is *regular* (or *defined*) at P if it is in $\bar{K}[V]_P$, in which case it makes sense to evaluate F at P.

Remark 2.9. The function field of $\mathbb{P}^n$ may also be described as the subfield of $\bar{K}(X_0, \dots, X_n)$ consisting of rational functions $F(X) = f(X)/g(X)$ for which f and g are *homogeneous* polynomials of the *same* degree. Such an expression gives a well-defined function on $\mathbb{P}^n$ at all point P where $g(P) \neq 0$. Similarly, the function field of a projective variety V is the field of rational functions $F(X) = f(X)/g(X)$ such that:

(i) f and g are homogeneous of the same degree;

(ii) $g \notin I(V)$;

(iii) two functions f_1/g_1 and f_2/g_2 are identified if $f_1 g_2 - f_2 g_1 \in I(V)$.

I.3 Maps Between Varieties

In this section we look at algebraic maps between projective varieties. These are maps that are defined by rational functions.

Definition. Let V_1 and $V_2 \subset \mathbb{P}^n$ be projective varieties. A *rational map from* V_1 *to* V_2 is a map of the form

$$f : V_1 \longrightarrow V_2, \qquad \phi = [f_0, \dots, f_n],$$

where the functions $f_0, \dots, f_n \in \bar{K}(V_1)$ have the property that for every point $P \in V_1$ at which $f_0, \dots, f_n$ are all defined,

$$\phi(P) = \big[f_0(P), \dots, f_n(P)\big] \in V_2.$$

If V_1 and V_2 are defined over K, then $G_{\bar{K}/K}$ acts on ϕ in the obvious way,

$$\phi^\sigma(P) = \big[f_0^\sigma(P), \dots, f_n^\sigma(P)\big].$$

Notice that we have the formula

$$\phi(P)^\sigma = \phi^\sigma(P^\sigma) \qquad \text{for all } \sigma \in G_{\bar{K}/K} \text{ and } P \in V_1.$$

If, in addition, there is some $\lambda \in \bar{K}^*$ such that $\lambda f_0, \dots, \lambda f_n \in K(V_1)$, then ϕ is said to be *defined over* K. Note that $[f_0, \dots, f_n]$ and $[\lambda f_0, \dots, \lambda f_n]$ give the same map on points. As usual, it is true that ϕ is defined over K if and only if $\phi = \phi^\sigma$ for all $\sigma \in G_{\bar{K}/K}$; see Exercise 1.12c.

Remark 3.1. A rational map $\phi : V_1 \to V_2$ is not necessarily a well-defined function at every point of V_1. However, it may be possible to evaluate $\phi(P)$ at points P of V_1 where some f_i is not regular by replacing each f_i by gf_i for an appropriate $g \in \bar{K}(V_1)$.

Definition. A rational map

$$\phi = [f_0, \dots, f_n] : V_1 \longrightarrow V_2$$

is *regular* (or *defined*) *at* $P \in V_1$ if there is a function $g \in \bar{K}(V_1)$ such that

(i) each gf_i is regular at P;

(ii) there is some i for which $(gf_i)(P) \neq 0$.

If such a g exists, then we set

$$\phi(P) = \bigl[(gf_0)(P), \dots, (gf_n)(P)\bigr].$$

N.B. It may be necessary to take different g's for different points. A rational map that is regular at every point is called a *morphism*.

Remark 3.2. Let $V_1 \subset \mathbb{P}^m$ and $V_2 \subset \mathbb{P}^n$ be projective varieties. Recall (I.2.9) that the functions in $\bar{K}(V_1)$ may be described as quotients of homogeneous polynomials in $\bar{K}[X_0, \dots, X_m]$ having the same degree. Thus by multiplying a rational map $\phi = [f_0, \dots, f_n]$ by a homogeneous polynomial that "clears the denominators" of the f_i's, we obtain the following alternative definition:

A *rational map* $\phi : V_1 \to V_2$ is a map of the form

$$\phi = \bigl[\phi_0(X), \dots, \phi_n(X)\bigr],$$

where

(i) the $\phi_i(X) \in \bar{K}[X] = \bar{K}[X_0, \dots, X_n]$ are homogeneous polynomials, not all in $I(V_1)$, having the same degree;

(ii) for very $f \in I(V_2)$,

$$f\bigl(\phi_0(X), \dots, \phi_n(X)\bigr) \in I(V_1).$$

Clearly, $\phi(P)$ is well-defined provided that some $\phi_i(P) \neq 0$. However, even if all $\phi_i(P) = 0$, it may be possible to alter ϕ so as to make sense of $\phi(P)$. We make this precise as follows:

A rational map $\phi = [\phi_0, \dots, \phi_n] : V_1 \to V_2$ as above is *regular* (or *defined*) at $P \in V_1$ if there exist homogeneous polynomials $\psi_0, \dots, \psi_n \in \bar{K}[X]$ such that

(i) $\psi_0, \dots, \psi_n$ have the same degree;

(ii) $\phi_i \psi_j \equiv \phi_j \psi_i \pmod{I(V_1)}$ for all $0 \le i, j \le n$;

(iii) $\psi(P) \neq 0$ for some i.