Graduate Texts in Mathematics

David M. Goldschmidt

# Algebraic Functions and Projective Curves

代数函数和射影曲线

Springer

世界图书出版公司
www.wpcbj.com.cn

David M. Goldschmidt

# Algebraic Functions and Projective Curves

Springer

**图书在版编目（CIP）数据**

代数函数和射影曲线 = Algebraic Functions and Projective Curves：英文/（美）戈德施密特（Goldschmidt，D. M.）著. —北京：世界图书出版公司北京公司，2009. 5

ISBN 978-7-5100-0473-5

Ⅰ. 代… Ⅱ. 戈… Ⅲ. ①代数函数—英文 ②射影几何—英文 Ⅳ. 0174. 53 0185. 1

中国版本图书馆 CIP 数据核字（2009）第 073086 号

| | |
|---|---|
| **书　　名：** | Algebraic Functions and Projective Curves |
| **作　　者：** | David M. Goldschmidt |
| **中 译 名：** | 代数函数和射影曲线 |
| **责任编辑：** | 高蓉　刘慧 |
| **出 版 者：** | 世界图书出版公司北京公司 |
| **印 刷 者：** | 三河国英印务有限公司 |
| **发　　行：** | 世界图书出版公司北京公司（北京朝内大街 137 号　100010） |
| **联系电话：** | 010-64021602，010-64015659 |
| **电子信箱：** | kjb@ wpcbj. com. cn |
| **开　　本：** | 24 开 |
| **印　　张：** | 8. 5 |
| **版　　次：** | 2009 年 06 月 |
| **版权登记：** | 图字：01-2009-1057 |
| **书　　号：** | 978-7-5100-0473-5/O · 688　　**定　　价：** 25. 00 元 |

**世界图书出版公司北京公司已获得 Springer 授权在中国大陆独家重印发行**

*To Cherie, Laura, Katie, and Jessica*

# Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFER. Topological Vector Spaces. 2nd ed.
4 HILTON/STAMMBACH. A Course in Homological Algebra. 2nd ed.
5 MAC LANE. Categories for the Working Mathematician. 2nd ed.
6 HUGHES/PIPER. Projective Planes.
7 J.-P. SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
10 COHEN. A Course in Simple Homotopy Theory.
11 CONWAY. Functions of One Complex Variable I. 2nd ed.
12 BEALS. Advanced Mathematical Analysis.
13 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
14 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
15 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
16 WINTER. The Structure of Fields.
17 ROSENBLATT. Random Processes. 2nd ed.
18 HALMOS. Measure Theory.
19 HALMOS. A Hilbert Space Problem Book. 2nd ed.
20 HUSEMOLLER. Fibre Bundles. 3rd ed.
21 HUMPHREYS. Linear Algebraic Groups.
22 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
23 GREUB. Linear Algebra. 4th ed.
24 HOLMES. Geometric Functional Analysis and Its Applications.
25 HEWITT/STROMBERG. Real and Abstract Analysis.
26 MANES. Algebraic Theories.
27 KELLEY. General Topology.
28 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
29 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
30 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
31 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 ALEXANDER/WERMER. Several Complex Variables and Banach Algebras. 3rd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to $C^*$-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 J.-P. SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. $p$-adic Numbers, $p$-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.
61 WHITEHEAD. Elements of Homotopy Theory.
62 KARGAPOLOV/MERLZJAKOV. Fundamentals of the Theory of Groups.
63 BOLLOBAS. Graph Theory.

*(continued after index)*

# Preface

This book grew out of a set of notes for a series of lectures I orginally gave at the Center for Communications Research and then at Princeton University. The motivation was to try to understand the basic facts about algebraic curves without the modern prerequisite machinery of algebraic geometry. Of course, one might well ask if this is a good thing to do. There is no clear answer to this question. In short, we are trading off easier access to the facts against a loss of generality and an impaired understanding of some fundamental ideas. Whether or not this is a useful tradeoff is something you will have to decide for yourself.

One of my objectives was to make the exposition as self-contained as possible. Given the choice between a reference and a proof, I usually chose the latter. Although I worked out many of these arguments myself, I think I can confidently predict that few, if any, of them are novel. I also made an effort to cover some topics that seem to have been somewhat neglected in the expository literature. Among these are Tate's theory of residues, higher derivatives and Weierstrass points in characteristic $p$, and inseparable residue field extensions. For the treatment of Weierstrass points, as well as a key argument in the proof of the Riemann Hypothesis for finite fields, I followed the fundamental paper by Stöhr–Voloch [19]. In addition to this important source, I often relied on the excellent book by Stichtenoth [17].

It is a pleasure to acknowledge the excellent mathematical environment provided by the Center for Communications Research in which this book was written. In particular, I would like to thank my colleagues Toni Bluher, Brad Brock, Everett Howe, Bruce Jordan, Allan Keeton, David Lieberman, Victor Miller, David Zelinsky, and Mike Zieve for lots of encouragement, many helpful discussions, and many useful pointers to the literature.

# Introduction

## What Is a Projective Curve?

Classically, a projective curve is just the set of all solutions to an irreducible homogeneous polynomial equation $f(X_0,X_1,X_2) = 0$ in three variables over the complex numbers, modulo the equivalence relation given by scalar multiplication. It is very safe to say, however, that this answer is deceptively simple, and in fact lies at the tip of an enormous mathematical iceberg.

The size of the iceberg is due to the fact that the subject lies at the intersection of three major fields of mathematics: algebra, analysis, and geometry. The origins of the theory of curves lie in the nineteenth century work on complex function theory by Riemann, Abel, and Jacobi. Indeed, in some sense the theory of projective curves over the complex numbers is equivalent to the theory of compact Riemann surfaces, and one could learn a fair amount about Riemann surfaces by specializing results in this book, which are by and large valid over an arbitrary ground field $k$, to the case $k = \mathbb{C}$. To do so, however, would be a big mistake for two reasons. First, some of our results, which are obtained with considerable difficulty over a general field, are much more transparent and intuitive in the complex case. Second, the topological structure of complex curves and their beautiful relationship to complex function theory are very important parts of the subject that do not seem to generalize to arbitrary ground fields. The complex case in fact deserves a book all to itself, and indeed there are many such, e.g. [15].

The generalization to arbitrary gound fields is a twentieth century development, pioneered by the German school of Hasse, Schmidt, and Deuring in the 1920s and 1930s. A significant impetus for this work was provided by the development of

algebraic number theory in the early part of the century, for it turns out that there is a very close analogy between algebraic function fields and algebraic number fields.

The results of the German school set the stage for the development of algebraic geometry over arbitrary fields, but were in large part limited to the special case of curves. Even in that case, there were serious difficulties. For example, Hasse was able to prove the Riemann hypothesis only for elliptic curves. The proof for curves of higher genus came from Weil and motivated his breakthrough work on abstract varieties. This in turn led to the "great leap forward" by the French school of Serre, Grothendiek, Deligne, and others to the theory of schemes in the 1950s and 1960s.

The flowering of algebraic geometry in the second half of the century has, to a large extent, subsumed the theory of algebraic curves. This development has been something of a two-edged sword, however. On the one hand, many of the results on curves can be seen as special cases of more general facts about schemes. This provides the usual benefits of a unified and in some cases a simplified treatment, together with some further insight into what is going on. In addition, there are some important facts about curves that, at least with the present state of knowledge, can only be understood with the more powerful tools of algebraic geometry. For example, there are important properties of the Jacobian of a curve that arise from its structure as an algebraic group.

On the other hand, the full-blown treatment requires the student to first master the considerable machinery of sheaves, schemes, and cohomology, with the result that the subject becomes less accessible to the nonspecialist. Indeed, the older algebraic development of Hasse et al. has seen something of a revival in recent years, due in part to the emergence of some applications in other fields of mathematics such as cryptology and coding theory. This approach, which is the one followed in this book, treats the function field of the curve as the basic object of study.

In fact, one can go a long way by restricting attention entirely to the function field (see, e.g., [17]), because the theory of function fields turns out to be equivalent to the theory of nonsingular projective curves. However, this is rather restrictive because many important examples of projective curves have singularities. A feature of this book is that we go beyond the nonsingular case and study projective curves in general, in effect viewing them as images of nonsingular curves.

## What Is an Algebraic Function?

For our purposes, an algebraic function field $K$ is a field that has transcendence degree one over some base field $k$, and is also finitely generated over $k$. Equivalently, $K$ is a finite extension of $k(x)$ for some transcendental element $x \in K$. Examples of such fields abound. They can be constructed via elementary field theory by sim-

ply adjoining to $k(x)$ roots of irreducible polynomials with coefficients in $k(x)$. In addition, however, we will always assume that $k$ is the full field of constants of $K$, that is, that every element of $K$ that is algebraic over $k$ is already in $k$.

When $k$ is algebraically closed, there is another more geometric way to construct such fields, which is more closely related to the subject of this book. Let $\mathbb{P}^2$ be the set of lines through the origin in complex 3-space, and let $V \subseteq \mathbb{P}^2$ be a projective curve as described above. That is, $V$ is the set of zeros of a complex, irreducible, homogenous polynomial $f(X_0,X_1,X_2)$ modulo scalar equivalence. We observe that a quotient of two homogeneous polynomials of the same degree defines a complex-valued function at all points of $\mathbb{P}^2$ where the denominator does not vanish. If the denominator does not vanish identically on $V$, it turns out that restricting this function to $V$ defines a complex-valued function at all but a finite number of points of $V$. The set of all such functions defines a subfield $\mathbb{C}(V)$, which is called the *function field* of $V$.

Of course, there is nothing magical about the complex numbers in this discussion — any algebraically closed field $k$ will do just as well. In fact, every finitely generated extension $K$ of an algebraically closed field $k$ of transcendence degree one arises in this way as the function field of a projective nonsingular curve $V$ defined over $k$ which, with suitable definitions, is unique up to isomorphism. This explains why we call such fields "function fields", at least in the case when $k$ is algebraically closed.

## What Is in This Book?

Here is a brief outline of the book, with only sketchy definitions and of course no proofs.

It turns out that for almost all points $P$ of an algebraic curve $V$, the order of vanishing of a function at $P$ defines a discrete $k$-valuation $v_P$ on the function field $K$ of $V$. The valuation ring $\mathcal{O}_P$ defined by $v_P$ has a unique maximal ideal $I_P$, which, because $v_P$ is discrete, is a principal ideal. A generator for $I_P$ is called a *local parameter* at $P$. It is convenient to identify $I_P$ with $P$. Indeed, for the first three chapters of the book, we forget all about the curve $V$ and its points and focus attention instead on the set $\mathbb{P}_K$ of $k$-valuation ideals of $K$, which we call the set of *prime divisors* of $K$. A basic fact about function fields is that all $k$-valuations are discrete.

A *divisor* on the function field $K$ is an element of the free abelian group $\mathrm{Div}(K)$ generated by the prime divisors. There is a map $\deg : \mathrm{Div}(K) \to \mathbb{Z}$ defined by $\deg(P) = |\mathcal{O}_P/P : k|$ for every prime divisor $P$. For $x \in K$, it is fundamental that the divisor

$$[x] = \sum_P v_P(x)P$$

has degree zero, and of course that the sum is finite. In other words, every function has the same (finite) number of poles and zeros, counting multiplicities. Divisors

of the form $[x]$ for some $x \in K$ are called *principal divisors* and form a subgroup of $\mathrm{Div}(K)$.

A basic problem in the subject is to construct a function with a given set of poles and zeros. Towards this end, we denote by $\leq$ the obvious partial order on $\mathrm{Div}(K)$, and we define for any divisor $D$,

$$L(D) := \{x \in K \mid [x] \geq -D\}.$$

So for example if $S$ is a set of distinct prime divisors and $D$ is its sum, $L(D)$ is the set of all functions whose poles lie in the set $S$ and are simple.

It is elementary that $L(D)$ is a $k$-subspace of dimension at most $\deg(D) + 1$. The fundamental theorem of Riemann asserts the existence of an integer $g_K$ such that for all divisors $D$ of sufficiently large degree, we have

$$(*) \qquad \dim_k(L(D)) = \deg(D) - g_K + 1.$$

The integer $g_K$ is the *genus* of $K$. In the complex case, this number has a topological interpretation as the number of holes in the corresponding Riemann surface. A refinement of Riemann's theorem due to Roch identifies the error term in $(*)$ for divisors of small degree and shows that the formula holds for all divisors of degree at least $2g - 1$.

Our proof of the Riemann–Roch theorem is due to Weil [23], and involves the expansion of a function in a formal Laurent series at each prime divisor. In the complex case, these series have a positive radius of convergence and can be integrated. In the general case, there is no notion of convergence or integration. It is an amazing fact, nevertheless, that a satisfactory theory of differential forms exists in general. Although they are not functions, differential forms have poles and zeros and therefore divisors, which are called *canonical divisors*. Not only that, they have residues that sum to zero, just as in the complex case. Our treatment of the residue theorem follows Tate [20].

There are also higher derivatives, called Hasse derivatives, which present some technical difficulties in positive characteristic due to potential division by zero. This topic seems to have been somewhat neglected in the literature on function fields. Our approach is based on Hensel's lemma. Using the Hasse derivatives, we prove the analogue of Taylor's theorem for formal power series expansion of a function in powers of a local parameter. This material is essential later on when we study Weierstrass points of projective maps.

Thus far, the only assumption required on the ground field $k$ is that it be the full field of constants of $K$. If $k$ is perfect (e.g. of characteristic zero, finite, or algebraically closed), this assumption suffices for the remainder of the book. For imperfect ground fields, however, technical difficulties can arise at this point, and we must strengthen our assumptions to ensure that $k' \otimes_k K$ remains a field for every finite extension $k'/k$. Then the space $\Omega_K$ of differential forms on $K$ has the structure of a (one-dimensional!) $K$-vector space, which means that all canonical divisors are congruent modulo principal divisors, and thus have the same degree (which turns out to be $2g - 2$).

Given a finite, separable extension $K'$ of $K$, there is a natural map

$$K' \otimes_K \Omega_K \to \Omega_{K'},$$

which is actually an isomorphism. This allows us to compare the divisor of a differential form on $K$ with the divisor of its image in $K'$, and leads to the Riemann–Hurwitz formula for the genus:

$$2g_{K'} - 2 = \frac{|K' : K|}{|k' : k|}(2g_K - 2) + \deg \mathscr{D}_{K'/K}.$$

Here, the divisor $\mathscr{D}_{K'/K}$ is the *different*, an important invariant of the extension, and $k'$ is the relative algebraic closure of $k$ in $K'$. The different, a familiar object in algebraic number fields, plays a similar key role in function fields. The formula has many applications, e.g., in the *hyperelliptic* case, where we have $K = k(x)$ and $|K' : K| = 2$.

At this point, further technical difficulties can arise for general ground fields of finite characteristic, and to ensure, for example, that $\mathscr{D}_{K'/K} \geq 0$, we must make the additional technical assumption that all prime divisors are *nonsingular*. Fortunately, it turns out that this condition is always satisfied in some finite (purely inseparable!) scalar extension of $K$.

When $k$ is not algebraically closed, the question of whether $K$ has any prime divisors of degree one (which we call *points*) is interesting. There is a beautiful answer for $k$ finite of order $q$, first proved for genus one by Hasse and in general by Weil. Let $a_K(n)$ denote the number of nonnegative divisors of $K$ of degree $n$, and put

$$Z_K(t) = \sum_{n=1}^{\infty} a_K(n) t^n.$$

Note that $a_K(1)$ is the number of points of $K$. Following Stör–Voloch [19] and Bombieri [2], we prove that

$$Z_K(t) = \frac{1}{(1-t)(1-qt)} \prod_{i=1}^{2g} (1 - \alpha_i t),$$

where $|\alpha_i| = \sqrt{q}$. This leads directly to the so-called "Weil bound" for the number of points of $K$:

$$|a_K(1) - q - 1| \leq 2g\sqrt{q}.$$

Turning our attention now to projective curves, we assume that the ground field $k$ is algebraically closed, and we define a closed subset of projective space to be the set of all zeros of a (finite) set of homogeneous polynomials. A projective variety is an irreducible closed set (i.e., not the union of two proper closed subsets), and a projective curve is a projective variety whose field of rational functions has transcendence degree one.

Given a projective curve $V \subseteq \mathbb{P}^n$, we obtain its function field $K$ by restricting rational functions on $\mathbb{P}^n$ to $V$. To recover $V$ from $K$, let $X_0, \ldots, X_n$ be the coordinates of $\mathbb{P}^n$ with notation chosen so that $X_0$ does not vanish on $V$. Then the rational functions $\phi_i := X_i/X_0$, $(i = 1, \ldots, n)$ are defined on $V$. Given a point $P$ of $K$, we let $e_P = -\min_i\{v_P(\phi_i)\}$ and put

$$\phi(P) := (t^{e_P}\phi_0(P) : t^{e_P}\phi_1(P) : \cdots : t^{e_P}\phi_n(P)) \in \mathbb{P}^n,$$

where $t$ is a local parameter at $P$. It is not hard to see that the image of $\phi$ is $V$. In fact, any finite dimensional $k$-subspace $L \subseteq K$ defines a map $\phi_L$ to projective space in this way whose image is a projective curve.

The map $\phi$ is always surjective. But when is it injective? This question leads us to the notion of singularities. Let $\phi(P) = a \in \mathbb{P}^n$, and let $\mathcal{O}_a$ be the subring of $K$ consisting of all fractions $f/g$ where $f$ and $g$ are homogeneous polynomials of the same degree and $g(a) \neq 0$. We say that $\phi$ is *nonsingular* at $P$ if $\mathcal{O}_a = \mathcal{O}_P$. This is equivalent to the familiar condition that the matrix of partial derivatives of the coordinate functions be of maximal rank.

An everywhere nonsingular projective map is called a *projective embedding*. It turns out that $\phi_{L(D)}$ is an embedding for any divisor $D$ of degree at least $2g + 1$. Another interesting case is the *canonical map* $\phi_{L(D)}$ where $D$ is a canonical divisor. The canonical map is an embedding unless $K$ is hyperelliptic.

The study of singularities is particularly relevant for plane curves. We prove that a nonsingular plane curve of degree $d$ has genus $(d-1)(d-2)/2$, so there are many function fields for which every map to $P^2$ is singular, e.g. any function field of genus 2. In fact, for a plane curve of degree $d$ and genus $g$, we obtain the formula

$$g = \frac{(d-1)(d-2)}{2} - \frac{1}{2}\sum_Q \delta(Q),$$

where for each singularity $Q$, $\delta(Q)$ is a positive integer determined by the local behavior of $V$ at $Q$.

All of the facts discussed above, and many more besides, are proved in this book. We have tried hard to make the treatment as self-contained as possible. To this end, we have also included an appendix on elementary field theory.

Finally, there is a website for the book located at *http://www.functionfields.org*. There you will find the latest errata, a discussion forum, and perhaps answers to some selected exercises.

# Contents

# 1

# Background

This chapter contains some preliminary definitions and results needed in the sequel. Many of these results are quite elementary and well known, but in the self-contained spirit of the book, we have provided proofs rather than references. In this book the word "ring" means "commutative ring with identity," unless otherwise explicitly stated.

## 1.1 Valuations

Let $K$ be a field. We say that an integral domain $\mathcal{O} \subseteq K$ is a *valuation ring* of $K$ if $\mathcal{O} \neq K$ and for every $x \in K$, either $x$ or $x^{-1}$ lies in $\mathcal{O}$. In particular, $K$ is the field of fractions of $\mathcal{O}$. Thus, we call an integral domain $\mathcal{O}$ a valuation ring if it is a valuation ring of its field of fractions.

Given a valuation ring $\mathcal{O}$ of $K$, let $V = K^\times / \mathcal{O}^\times$ where for any ring $R$, $R^\times$ denotes the group of units of $R$. The *valuation* afforded by $\mathcal{O}$ is the natural map $v : K^\times \to V$. Although it seems natural to write $V$ multiplicatively, we will follow convention and write it additively. We call $V$ the group of values of $\mathcal{O}$. By convention, we extend $v$ to all of $K$ by defining $v(0) = \infty$.

For elements $a\mathcal{O}^\times, b\mathcal{O}^\times$ of $V$, define $a\mathcal{O}^\times \leq b\mathcal{O}^\times$ if $a^{-1}b \in \mathcal{O}$, and put $v < \infty$ for all $v \in V$. Then it is easy to check that the relation $\leq$ is well defined, converts $V$ to a totally ordered group, and that

$$v(a+b) \geq \min\{v(a), v(b)\} \tag{1.1.1}$$

for all $a, b \in K^\times$.

Let $P := \{x \in \mathcal{O} \mid v(x) > 0\}$. Then $P$ is the set of nonunits of $\mathcal{O}$. From (1.1.1), it follows that $P$ is an ideal, and hence the unique maximal ideal of $\mathcal{O}$. If $v(a) > v(b)$, then $ab^{-1} \in P$, whence $v(1+ab^{-1}) = 0$ and therefore $v(a+b) = v(b)$. To summarize:

**Lemma 1.1.2.** *If $\mathcal{O}$ is a valuation ring with valuation $v$, then $\mathcal{O}$ has a unique maximal ideal $P = \{x \in \mathcal{O} \mid v(x) > 0\}$ and* (1.1.1) *is an equality unless, perhaps, $v(a) = v(b)$.* □

Given a valuation ring $\mathcal{O}$ of a field $K$, the natural map $K^\times \to K^\times/\mathcal{O}^\times$ defines a valuation. Conversely, given a nontrivial homomorphism $v$ from $K^\times$ into a totally ordered additive group $G$ satisifying $v(a+b) \geq \min\{v(a), v(b)\}$, we put $\mathcal{O}_v := \{x \in K^\times \mid v(x) \geq 0\} \cup \{0\}$. Then it is easy to check that $\mathcal{O}_v$ is a valuation ring of $K$ and that $v$ induces an order-preserving isomorphism from $K^\times/\mathcal{O}^\times$ onto its image. Normally, we will identify these two groups. Note, however, that some care needs to be taken here. If, for example, we replace $v$ by $nv : K^\times \to G$ for any positive integer $n$, we get the same valuation of $K$.

We let $P_v := \{x \in K \mid v(x) > 0\}$ be the maximal ideal of $\mathcal{O}_v$ and $F_v := \mathcal{O}_v/P_v$ be the *residue field* of $v$. If $K$ contains a subfield $k$, we say that $v$ is a $k$-valuation of $K$ if $v(x) = 0$ for all $x \in k^\times$. In this case, $F_v$ is an extension of $k$. Indeed, in the case of interest to us, this extension turns out to be finite. However, there is some subtlety here because the residue fields do not come equipped with any particular fixed embedding into some algebraic closure of $k$, except in the (important) special case $F_v = k$.

Our first main result on valuations is the extension theorem, but first we need a few preliminaries.

**Lemma 1.1.3.** *Let $R$ be a subring of a ring $S$ and let $x \in S$. Then the following conditions are equivalent:*

1. *$x$ satisfies a monic polynomial with coefficients in $R$,*
2. *$R[x]$ is a finitely generated $R$-module,*
3. *$x$ lies in a subring that is a finitely generated $R$-submodule.*

*Proof.* The implications (1) ⇒ (2) ⇒ (3) are clear. To prove (3) ⇒ (1), let $\{x_1, \ldots, x_n\}$ be a set of $R$-module generators for a subring $S_0$ containing $x$, then there are elements $a_{ij} \in R$ such that

$$xx_i = \sum_{j=1}^{n} a_{ij}x_j \quad \text{for } 1 \leq i \leq n.$$

Multiplying the matrix $(\delta_{ij}x - a_{ij})$ by its transposed matrix of cofactors, we obtain

$$f(x)x_j = 0 \quad \text{for all } j,$$

where $f(X)$ is the monic polynomial $\det(\delta_{ij}X - a_{ij})$ and $\delta_{ij}$ is the Kronecker symbol. We conclude that $f(x)S_0 = 0$, and since $1 \in S_0$, that $f(x) = 0$. □

Given rings $R \subseteq S$ and $x \in S$, we say that $x$ is *integral* over $R$ if any of the above conditions is satisfied. We say that $S$ is integral over $R$ if every element of $S$ is integral over $R$. If $R[x]$ and $R[y]$ are finitely generated $R$-modules with generators $\{x_i\}$ and $\{y_j\}$ respectively, it is easy to see that $R[x,y]$ is generated by $\{x_i y_j\}$. Then using (1.1.3) it is straightforward that the sum and product of integral elements is again integral, so the set $\hat{R}$ of all elements of $S$ integral over $R$ is a subring. Furthermore, if $x \in S$ satisfies

$$x^n + \sum_{i=0}^{n-1} a_i x^i = 0$$

with $a_i \in \hat{R}$, then $x$ is integral over $\hat{R}_0 := R[a_0, \ldots, a_{n-1}]$, which is a finitely generated $R$-module by induction on $n$. If $\{b_1, \ldots, b_m\}$ is a set of $R$-module generators for $\hat{R}_0$, then $\{b_i x^j \mid 1 \le i \le m,\ 0 \le j < n\}$ generates $\hat{R}_0[x]$ as an $R$-module, and we have proved

**Corollary 1.1.4.** *The set of all elements of $S$ integral over $R$ forms a subring $\hat{R}$, and any element of $S$ integral over $\hat{R}$ is already in $\hat{R}$.* □

The ring $\hat{R}$ is called the *integral closure* of $R$ in $S$. If $\hat{R} = R$, we say that $R$ is *integrally closed* in $S$. If $S$ is otherwise unspecified, we take it to be the field of fractions of $R$.

Recall that a ring $R$ is called a *local ring* if it has an ideal $M$ such that every element of $R \setminus M$ is a unit. Then $M$ is evidently the unique maximal ideal of $R$, and conversely, a ring with a unique maximal ideal is local. If $R$ is any integral domain with a prime ideal $P$, the *localization* $R_P$ of $R$ at $P$ is the (local) subring of the field of fractions consisting of all $x/y$ with $y \notin P$.

**Lemma 1.1.5 (Nakayama's Lemma).** *Let $R$ be a local ring with maximal ideal $P$ and let $M$ be a nonzero finitely generated $R$-module. Then $PM \subsetneq M$.*

*Proof.* Let $M = Rm_1 + \cdots + Rm_n$, where $n$ is minimal, and put $M_0 := Rm_2 + \cdots + Rm_n$. Then $M_0$ is a proper submodule. If $M = PM$, we can write

$$m_1 = \sum_{i=1}^{n} a_i m_i$$

with $a_i \in P$, but $1 - a_1$ is a unit since $R$ is a local ring, and we obtain the contradiction

$$m_1 = (1 - a_1)^{-1} \sum_{i=2}^{n} a_i m_i \in M_0.$$

□

**Theorem 1.1.6 (Valuation Extension Theorem).** *Let $R$ be a subring of a field $K$ and let $P$ be a nonzero prime ideal of $R$. Then there exists a valuation ring $\mathcal{O}$ of $K$ with maximal ideal $M$ such that $R \subseteq \mathcal{O} \subseteq K$ and $M \cap R = P$.*