VII. Infinite Field Extensions, 403-446

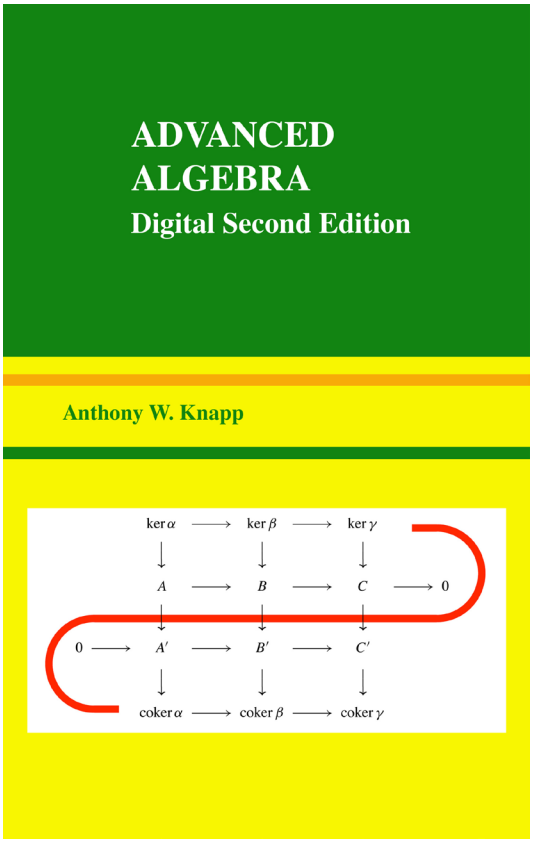
DOI: 10.3792/euclid/9781429799928-7

from

Advanced Algebra
Digital Second Edition

Anthony W. Knapp

Full Book DOI: 10.3792/euclid/9781429799928
ISBN: 978-1-4297-9992-8



Distributed by Project Euclid.
For copyright information, see the following page.

Anthony W. Knapp
81 Upper Sheep Pasture Road
East Setauket, N.Y. 11733–1729, U.S.A.
Email to: aknapp@math.stonybrook.edu
Homepage: www.math.stonybrook.edu/~aknapp

Title: Advanced Algebra
Cover: Content of the Snake Lemma; see page 185.

Mathematics Subject Classification (2010): 11–01, 13–01, 14–01, 16–01, 18G99, 55U99, 11R04, 11S15, 12F99, 14A05, 14H05, 12Y05, 14A10, 14Q99.

First Edition, ISBN-13 978-0-8176-4522-9
©2007 Anthony W. Knapp
Published by Birkhäuser Boston

Digital Second Edition, not to be sold, no ISBN
©2016 Anthony W. Knapp
Published by the Author

All rights reserved. This file is a digital second edition of the above named book. The text, images, and other data contained in this file, which is in portable document format (PDF), are proprietary to the author, and the author retains all rights, including copyright, in them. The use in this file of trade names, trademarks, service marks, and similar items, even if they are not identified as such, is not to be taken as an expression of opinion as to whether or not they are subject to proprietary rights.

All rights to print media for the first edition of this book have been licensed to Birkhäuser Boston, c/o Springer Science+Business Media Inc., 233 Spring Street, New York, NY 10013, USA, and this organization and its successor licensees may have certain rights concerning print media for the digital second edition. The author has retained all rights worldwide concerning digital media for both the first edition and the digital second edition.

The file is made available for limited noncommercial use for purposes of education, scholarship, and research, and for these purposes only, or for fair use as understood in the United States copyright law. Users may freely download this file for their own use and may store it, post it online, and transmit it digitally for purposes of education, scholarship, and research. They may not convert it from PDF to any other format (e.g., EPUB), they may not edit it, and they may not do reverse engineering with it. In transmitting the file to others or posting it online, users must charge no fee, nor may they include the file in any collection of files for which a fee is charged. Any exception to these rules requires written permission from the author.

Except as provided by fair use provisions of the United States copyright law, no extracts or quotations from this file may be used that do not consist of whole pages unless permission has been granted by the author (and by Birkhäuser Boston if appropriate).

The permission granted for use of the whole file and the prohibition against charging fees extend to any partial file that contains only whole pages from this file, except that the copyright notice on this page must be included in any partial file that does not consist exclusively of the front cover page. Such a partial file shall not be included in any derivative work unless permission has been granted by the author (and by Birkhäuser Boston if appropriate).

Inquiries concerning print copies of either edition should be directed to Springer Science+Business Media Inc.

CHAPTER VII

Infinite Field Extensions

Abstract. This chapter provides algebraic background for directly addressing some simple-sounding yet fundamental questions in algebraic geometry. All the questions relate to the set of simultaneous zeros of finitely many polynomials in n variables over a field.

Section 1 concerns existence of zeros. The main theorem is the Nullstellensatz, which in part says that there is always a zero if the finitely many polynomials generate a proper ideal and if the underlying field is algebraically closed.

Section 2 introduces the transcendence degree of a field extension. If L/K is a field extension, a subset of L is algebraically independent over K if no nonzero polynomial in finitely many of the members of the subset vanishes. A transcendence basis is a maximal subset of algebraically independent elements; a transcendence basis exists, and its cardinality is independent of the particular basis in question. This cardinality is the transcendence degree of the extension. Then L is algebraic over the subfield generated by a transcendence basis. Briefly any field extension can be obtained by a purely transcendental extension followed by an algebraic extension. The dimension of the set of common zeros of a prime ideal of polynomials over an algebraically closed field is defined to be the transcendence degree of the field of fractions of the quotient of the polynomial ring by the ideal.

Section 3 elaborates on the notion of separability of field extensions in characteristic p. Every algebraic extension L/K can be obtained by a separable extension followed by an extension that is purely inseparable in the sense that every element x of L has a power x^{p^e} for some integer $e \geq 0$ with x^{p^e} separable over K.

Section 4 introduces the Krull dimension of a commutative ring with identity. This number is one more than the maximum number of ideals occurring in a strictly increasing chain of prime ideals in the ring. For $K[X_1, \ldots, X_n]$ when K is a field, the Krull dimension in n. If P is a prime ideal in $K[X_1, \ldots, X_n]$, then the Krull dimension of the integral domain $R = K[X_1, \ldots, X_n]/P$ matches the transcendence degree over K of the field of fractions of R. Thus Krull dimension extends the notion of dimension that was defined in Section 2.

Section 5 concerns nonsingular and singular points of the set of common zeros of a prime ideal of polynomials in n variables over an algebraically closed field. According to Zariski's Theorem, nonsingularity of a point may be defined in either of two equivalent ways—in terms of the rank of a Jacobian matrix obtained from generators of the ideal, or in terms of the dimension of the quotient of the maximal ideal at the point in question factored by the square of this ideal. The point is nonsingular if the rank of the Jacobian matrix is n minus the dimension of the zero locus, or equivalently if the dimension of the quotient of the maximal ideal by its square equals the dimension of the zero locus. Nonsingular points always exist.

Section 6 extends Galois theory to certain infinite field extensions. In the algebraic case inverse limit topologies are imposed on Galois groups, and the generalization of the Fundamental Theorem of Galois Theory to an arbitrary separable normal extension L/K gives a one-one correspondence between the fields F with $K \subseteq F \subseteq L$ and the closed subgroups of $\mathrm{Gal}(L/K)$.

1. Nullstellensatz

Algebraic geometry studies the geometric properties of sets defined by algebraic equations. In the simplest case some field K is specified, the equations are polynomial equations in several variables with coefficients in K, and one seeks solutions to the system of equations with the variables taking values in K or some larger field.

The nature of the subject is that even fairly simple-sounding geometric questions require algebraic background beyond what is in *Basic Algebra* and the first six chapters of the present book. This chapter addresses the necessary background, largely from the theory of fields, for addressing fundamental questions concerning existence of solutions, the dimension of the space of solutions, singularity of the solution set at a particular point, and effects of changing fields.

The present section supplies background for the question of existence. We have a system of polynomial equations in n variables with coefficients in K, and we are interested in simultaneous solutions in a given extension field L of K. A solution can be regarded as a column vector in L^n. Think of the equations as of the form $F_i(X_1, \dots, X_n) = 0$ with each F_i a polynomial, and then the set of solutions is the locus of common zeros of the F_i's in L^n. The locus of common zeros is unaffected by enlarging the system of equations by allowing all equations of the form $\sum_i G_i F_i = 0$ with each G_i is arbitrary in $K[X_1, \dots, X_n]$; thus we may as well regard the left sides as all members of some ideal I in $K[X_1, \dots, X_n]$. The Hilbert Basis Theorem says that any ideal in $K[X_1, \dots, X_n]$ is finitely generated, and hence studying the common zero locus for an ideal is always the same as studying the common zero locus for a finite set of polynomials.

A proper ideal need not have a nonempty locus of common zeros. For example, if $K = \mathbb{R}$, then the single equation $X^2 + Y^2 + 1 = 0$ has no solutions in $\mathbb{R}^2$. Hilbert's Nullstellensatz[1] is partly the affirmative statement that any proper ideal has a nonzero locus of common zeros under the additional assumption that K is algebraically closed.

Theorem 7.1 (Nullstellensatz). Let K be a field, let $\overline{K}$ be an algebraic closure, and let n be a positive integer. Then every maximal ideal J of $K[X_1, \dots, X_n]$ has the property that $K[X_1, \dots, X_n]/J$ is a finite algebraic extension of K, and in particular the maximal ideals of $\overline{K}[X_1, \dots, X_n]$ are of the form

$$(X_1 - a_1, \dots, X_n - a_n),$$

where $(a_1, \dots, a_n)$ is an arbitrary member of $\overline{K}^n$. Consequently if I is any proper ideal in $K[X_1, \dots, X_n]$, then

(a) the locus of common zeros of I in $\overline{K}^n$ is nonempty,

[1]German for "zero-locus theorem."

(b) any f in $K[X_1, \dots, X_n]$ that vanishes on the locus of common zeros of I in $\overline{K}^n$ has the property that f^k is in I for some integer $k > 0$.

Before coming to the proof, we mention an important corollary.

Corollary 7.2. Let K be a field, let $\overline{K}$ be an algebraic closure, let n be a positive integer, and let I be a *prime* ideal in $K[X_1, \dots, X_n]$. Then I contains every polynomial in $K[X_1, \dots, X_n]$ that vanishes on the locus of common zeros of I in $K[X_1, \dots, X_n]$.

PROOF. If f is a member of $K[X_1, \dots, X_n]$ that vanishes on the locus of common zeros of I, then (b) in the theorem shows that f^k is in I for some k. Since I is prime, one of the factors of $f^k = f \cdots f$ lies in I. □

EXAMPLE FOR COROLLARY. Let $K = L = \mathbb{C}$, and let I be the principal ideal in $\mathbb{C}[X, Y]$ generated by $Y^2 - X(X+1)(X-1)$. Consider $\mathbb{C}[X, Y]$ as isomorphic to $\mathbb{C}[X][Y]$. As a polynomial in Y over $\mathbb{C}[X]$, $p(X, Y) = Y^2 - X(X+1)(X-1)$ is irreducible because $X(X+1)(X-1)$ is not the square of a polynomial in X. Since $\mathbb{C}[X, Y]$ is a unique factorization domain, $p(X, Y)$ is prime. Therefore $I = (p(X, Y))$ is a prime ideal. The corollary says that every polynomial vanishing on the locus of points $(x, y) \in \mathbb{C}^2$ for which $y^2 = x(x+1)(x-1)$ is the product of $Y^2 - X(X+1)(X-1)$ and a polynomial in (X, Y). Consequently the ring of restrictions of polynomials to the locus for which $y^2 = x(x+1)(x-1)$ is isomorphic to $\mathbb{C}[X, Y]/\big(Y^2 - X(X+1)(X-1)\big)$.

Theorem 7.1b has a tidy formulation in terms of the "radical" of an ideal. If R is a commutative ring with identity and I is an ideal in R, then the **radical** of I, denoted by $\sqrt{I}$, is the set of all r in R such that r^k is in I for some $k \geq 1$. It is immediate that the radical of I is an ideal containing I and that $\sqrt{I}$ is proper if I is proper. If I is an ideal in $K[X_1, \dots, X_n]$ and if f is in $\sqrt{I}$, then f^k is in I for some $k > 0$, and hence f vanishes on the locus of common zeros of I. Theorem 7.1b says conversely that any f vanishing on the locus of common zeros of I has f^k in I for some $k > 0$. This means that f is in $\sqrt{I}$. We can therefore rewrite (b) in the theorem as follows:

(b′) the ideal of all f in $K[X_1, \dots, X_n]$ that vanish on the locus of common zeros of I in $\overline{K}^n$ is exactly $\sqrt{I}$.

The proof of Theorem 7.1 will follow comparatively easily from the following two lemmas.

Lemma 7.3. If K is a field and L is an extension field that is generated as a K algebra by n elements $x_1, \dots, x_n$, i.e., if $L = K[x_1, \dots, x_n]$, then every x_j is algebraic over K.

REMARKS. Conversely if $x_1, \ldots, x_n$ are elements of an extension field L that are algebraic over K, then $K(x_1, \ldots, x_n) = K[x_1, \ldots, x_n]$. The reason is that

$$\begin{aligned} K(x_1, \ldots, x_n) &= K(x_1, \ldots, x_{n-1})(x_n) = K(x_1, \ldots, x_{n-1})[x_n] \\ &= K(x_1, \ldots, x_{n-2})(x_{n-1})[x_n] = K(x_1, \ldots, x_{n-2})[x_{n-1}][x_n] \\ &= \cdots = K[x_1] \cdots [x_{n-1}][x_n] = K[x_1, \ldots, x_n]. \end{aligned}$$

PROOF. We proceed by induction on n. For $n = 1$, if $L = K[x_1]$, then we know from the elementary theory of fields that x_1 is algebraic over K.

For the inductive step, suppose that $L = K[x_1, \ldots, x_n]$. Since L is a field, $K(x_1) \subseteq L$, and hence $L = K(x_1)[x_2, \ldots, x_n]$. By the inductive hypothesis applied to L and $K(x_1)$, the elements $x_2, \ldots, x_n$ are algebraic over $K(x_1)$. To complete the proof, it is enough to show that x_1 is algebraic over K.

Fix $j \geq 2$. The element x_j, being algebraic over $K(x_1)$, satisfies a polynomial equation

$$X^m + a_{m-1}X^{m-1} + \cdots + a_0 = 0$$

with $a_{m-1}, \ldots, a_0$ in $K(x_1)$. Clearing fractions, we see that x_j satisfies an equation

$$b_m X^m + b_{m-1}X^{m-1} + \cdots + b_0 = 0$$

with $b_m, \ldots, b_0$ in $K[x_1]$ and $b_m \neq 0$. Multiplying through by b_m^{m-1} shows that x_j satisfies

$$(b_m X)^m + b_{m-1}(b_m X)^{m-1} + \cdots + b_0(b_m)^{m-1} = 0,$$

and we see that $b_m x_j$ is integral over the ring $K[x_1]$. Let us write c_j for the element $b_m \in K[x_1]$ that we have just produced for this j.

In the case of $j = 1$, we can use $m = 1$ and $a_0 = -x_1$ in the above argument, and we are then led to $c_1 = x_1$. If $x_1^{l_1} \cdots x_n^{l_n}$ is any monomial in $K[x_1, \ldots, x_n]$ and if l is defined as $l = \max(l_1, \ldots, l_n)$, then the fact that the integral elements over $K[x_1]$ form a ring implies that $(c_1 \cdots c_n)^l x_1^{l_1} \cdots x_n^{l_n}$ is integral over $K[x_1]$. Hence for any f in $K[x_1, \ldots, x_n]$, $(c_1 \cdots c_n)^l f$ is integral over $K[x_1]$ for a suitable integer $l = l(f)$. Since $K(x_1) \subseteq K[x_1, \ldots, x_n]$, this conclusion applies in particular to any member f of $K(x_1)$.

The ring $K[x_1]$ is a principal ideal domain and is therefore integrally closed in its field of fractions $K(x_1)$. For f in $K(x_1)$, we have seen that $(c_1 \cdots c_n)^l f$ is integral over $K[x_1]$ for some $l = l(f)$. The element $(c_1 \cdots c_n)^l f$ is in $K(x_1)$, and the integral-closure property therefore implies that $(c_1 \cdots c_n)^l f$ is in $K[x_1]$.

Consequently there exists a fixed element h of $K[x_1]$ such that every element f of $K(x_1)$ is of the form g/h^l for some g in $K[x_1]$ and some integer $l \geq 0$. We apply this observation to $f = q(x_1)^{-1}$ for each irreducible polynomial $q(X)$ in $K[X]$, and we obtain $q(x_1)g = h^l$ with g and l depending on $q(X)$. If x_1 is transcendental over K, this equality implies the polynomial identity $q(X)g(X) = h(X)^l$.

Consequently every irreducible polynomial $q(X)$ divides $h(X)$. If K is infinite, this is a contradiction because there are infinitely many distinct polynomials $X-a$ in $K[X]$; if K is finite, this is a contradiction because there exists at least one irreducible polynomial of each degree ≥ 1. We arrive at a contradiction in either case, and therefore x_1 is algebraic over K. This completes the induction and the proof. □

Lemma 7.4. Let K be a field, and let L be an algebraic extension of K. If I is a proper ideal in $K[X_1, \ldots, X_n]$, then $IL[X_1, \ldots, X_n]$ is a proper ideal in $L[X_1, \ldots, X_n]$.

REMARK. As usual, the notation $IL[X_1, \ldots, X_n]$ refers to the set of sums of products of elements of I and elements of $L[X_1, \ldots, X_n]$.

PROOF. First let us identify the integral closure of $K[X_1, \ldots, X_n]$ in the field $L(X_1, \ldots, X_n)$ as $L[X_1, \ldots, X_n]$. The ring $L[X_1, \ldots, X_n]$ is a unique factorization domain, and Proposition 8.41 of *Basic Algebra* shows that it is integrally closed. Consequently the integral closure of $K[X_1, \ldots, X_n]$ in $L(X_1, \ldots, X_n)$ is contained in $L[X_1, \ldots, X_n]$. On the other hand, the integral closure of $K[X_1, \ldots, X_n]$ in $L(X_1, \ldots, X_n)$ contains L because L/K is algebraic, and it contains each X_j. Therefore it contains $L[X_1, \ldots, X_n]$ and must equal $L[X_1, \ldots, X_n]$.

Now we apply Proposition 8.53 of *Basic Algebra* to the ring $K[X_1, \ldots, X_n]$, its field of fractions $K(X_1, \ldots, X_n)$, the extension field $L(X_1, \ldots, X_n)$, and the integral closure $L[X_1, \ldots, X_n]$ of $K[X_1, \ldots, X_n]$ in $L(X_1, \ldots, X_n)$. The proposition says that if P is any maximal ideal of $K[X_1, \ldots, X_n]$, then the ideal $PL[X_1, \ldots, X_n]$ is proper in $L[X_1, \ldots, X_n]$. This result is to be applied to any maximal ideal P of $K[X_1, \ldots, X_n]$ that contains I. □

PROOF OF THEOREM 7.1. Let J be a maximal ideal in $K[X_1, \ldots, X_n]$. Then $L = K[X_1, \ldots, X_n]/J$ is a field. Hence $L = K[x_1, \ldots, x_n]$ is a field if the x_i's are defined by $x_i = X_i + J$. Lemma 7.3 shows that each x_j is algebraic over K, and the first conclusion of the theorem follows.

When this conclusion is applied to $\overline{K}$ instead of K, then the fact that $\overline{K}$ is algebraically closed implies that each x_j lies in the cosets determined by $\overline{K}$, i.e., the cosets of the constant polynomials. Consequently for each j, there is an element a_j in $\overline{K}$ such that $x_j - a_j$ lies in J. Then it follows that $(X_1 - a_1, \ldots, X_n - a_n)$ is contained in J. Since the ideal $(X_1 - a_1, \ldots, X_n - a_n)$ is maximal, $J = (X_1 - a_1, \ldots, X_n - a_n)$. This proves that the maximal ideals are as in the displayed expression in the theorem.

To prove (a), we apply Lemma 7.4 to the ideal I in $K[X_1, \ldots, X_n]$ and to the algebraic extension $\overline{K}$ of K. The lemma produces a proper ideal of $\overline{K}[X_1, \ldots, X_n]$

containing I, and we extend it to a maximal ideal J of $\overline{K}[X_1, \ldots, X_n]$. From the previous paragraph of the proof, J is of the form $J = (X_1 - a_1, \ldots, X_n - a_n)$ for some $(a_1, \ldots, a_n)$ in $\overline{K}^n$. The ideal J is therefore identified as the kernel of the evaluation homomorphism of $\overline{K}[X_1, \ldots, X_n]$ at the point $(a_1, \ldots, a_n)$. Every member of J thus vanishes at $(a_1, \ldots, a_n)$, and the same thing is true of every member of I. This proves (a).

For (b), let I be a proper ideal in $K[X_1, \ldots, X_n]$, and let f be as in (b). Introduce an additional indeterminate Y, and let J be the ideal in $K[X_1, \ldots, X_n, Y]$ generated by I and $fY - 1$. If some point $(x_1, \ldots, x_n, y)$ lies on the locus of common zeros of J in $\overline{K}^{n+1}$, then $(x_1, \ldots, x_n)$ lies on the locus of common zeros of I in $\overline{K}^n$, since $I \subseteq J$; thus $f(x_1, \ldots, x_n) = 0$, since f is assumed to vanish on all common zeros of I in $\overline{K}^n$. Consequently $f(x_1, \ldots, x_n)y - 1 = -1 \neq 0$, and we find that $f(X_1, \ldots, X_n)Y - 1$ does not vanish on the locus of common zeros of J in $\overline{K}^{n+1}$, contradiction. We conclude that no point $(x_1, \ldots, x_n, y)$ lies on the locus of common zeros of J in $\overline{K}^{n+1}$. By (a), we see that

$$J = K[X_1, \ldots, X_n, Y]. \tag{$*$}$$

Let us write X for the expression $X_1, \ldots, X_n$. Then $(*)$ implies that

$$1 = \sum_{i=1}^{r} p_i(X, Y)g_i(X) + q(X, Y)(f(X)Y - 1) \tag{$**$}$$

for some $g_1, \ldots, g_r$ in I and some $p_1, \ldots, p_r$ and q in $K[X, Y]$. Let ψ be the substitution homomorphism of $K[X, Y]$ into $K(X)$ that carries K into itself, X into itself, and Y into $f(X)^{-1}$. Application of ψ to $(**)$ gives

$$1 = \sum_{i=1}^{r} p_i(X, f(X)^{-1})g_i(X), \tag{$\dagger$}$$

since $\psi\big(f(X)Y - 1\big) = 0$. If Y^k is the largest power of Y that appears in any of the polynomials $p_i(X, Y)$, then we can rewrite $(\dagger)$ as

$$f(X)^k = \sum_{i=1}^{r} \big(f(X)^k p_i(X, f(X)^{-1})\big)g_i(X)$$

and exhibit $f(X)^k$ as the sum of products of the members g_i of I by members of $K[X]$. Thus $f(X)^k$ is in I, and (b) is proved. □

2. Transcendence Degree

Let K be a field, and let L be an extension field. The algebraic construction in this section will show that L can be obtained from K in two steps, by a "purely transcendental" extension followed by an algebraic extension. The number of

indeterminates in the first step (or the cardinality if the number is infinite) will be seen to be an invariant of the construction and will be called the "transcendence degree" of L/K.

Before coming to the details, let us mention what transcendence degree will mean geometrically. Suppose that the field K is algebraically closed, suppose that I is a prime ideal in $K[X_1, \ldots, X_n]$, and suppose that V is the locus of common zeros of I. Corollary 7.2 shows that I is the set of all polynomials vanishing on V, and thus the integral domain $K[X_1, \ldots, X_n]/I$ may be regarded as the set of all restrictions to V of polynomials. If L is the field of fractions of $K[X_1, \ldots, X_n]/I$, then the transcendence degree of L/K will be interpreted as the "number of independent variables" or "dimension" of the locus V.

Now we can make the precise definitions. Let K be a field, and let L be an extension field. A finite subset $x_1, \ldots, x_n$ of L is said to be **algebraically independent** over K if the ring homomorphism $K[X_1, \ldots, X_n] \to L$ given by $f \mapsto f(x_1, \ldots, x_n)$ is one-one.[2] Otherwise it is algebraically dependent.

EXAMPLE. Let $K = \mathbb{C}$, and let $p(X, Y) = Y^2 - X(X + 1)(X - 1)$. The principal ideal $I = (p(X, Y))$ was shown to be prime in $\mathbb{C}[X, Y]$ in the example with Corollary 7.2. Therefore $\mathbb{C}[X, Y]/I$ is an integral domain. Let x and y be the cosets $x = X + I$ and $y = Y + I$. If L denotes the field of fractions of $\mathbb{C}[X, Y]/I$, then we may regard x and y as members of L. The subset $\{x, y\}$ of L is algebraically dependent because the polynomial $p(X, Y)$ maps to 0 under the substitution homomorphism of $\mathbb{C}[X, Y]$ into L with $X \mapsto x$ and $Y \mapsto y$.

A subset S of L is called a **transcendence set** over K if each finite subset of S is algebraically independent over K. A maximal transcendence set over K is called a **transcendence basis** of L over K. For each transcendence set S of L over K, we write $K(S)$ for the smallest subfield of L containing K and S. If some transcendence basis S has the property that $K(S) = L$, then L is said to be a **purely transcendental** extension of K; in this case it follows from the definitions that S is a transcendence basis of L over K.

EXAMPLE, CONTINUED. With K and L as in the example above, the sets $S = \{x\}$ and $S = \{y\}$ are transcendence sets over $K = \mathbb{C}$. It is not hard to see that $\{x\}$ is a transcendence basis of L over K. Actually, if z is any member of L that is not in $\mathbb{C}$, then $\{z\}$ is a transcendence set over $\mathbb{C}$. The reason is that $\mathbb{C}$ is algebraically closed; hence either z is transcendental over $\mathbb{C}$ or else z lies in $\mathbb{C}$. Lemma 7.6 below shows that any transcendence set of L over $\mathbb{C}$ can be extended to a transcendence basis, and Theorem 7.9 shows that all transcendence bases of L over $\mathbb{C}$ have the same cardinality. It follows that if z is any member of L that is not in $\mathbb{C}$, then $\{z\}$ is a

[2] By convention the empty set is algebraically independent over K.

transcendence basis of L over $\mathbb{C}$ and that every transcendence basis of L over $\mathbb{C}$ is of this form. The two-element set $\{x, y\}$ cannot be a transcendence set by this reasoning, but we can see this conclusion more directly just by observing that $\{x, y\}$ was shown in the example above to be algebraically dependent.

Shortly we shall establish the existence of transcendence bases in general. If S is a transcendence basis and if K' is defined to be $K(S)$, then we shall show that L is algebraic over K'. The subfield K' of L depends on the choice of S, but there is a uniqueness theorem: the cardinality of a transcendence basis of L/K is independent of the particular transcendence basis.

Lemma 7.5. Let L/K be a field extension, let S be a transcendence set of L over K, let $K(S)$ be the subfield of L generated by K and S, and let x be an element of L not in S. Then $S' = S \cup \{x\}$ is a transcendence set of L over K if and only if x is transcendental over $K(S)$.

PROOF. Suppose that x is transcendental over $K(S)$ and is not in S. Let n distinct elements $x_1, \dots, x_n$ of S' be given. If these are all in S, then $f \mapsto f(x_1, \dots, x_n)$ is one-one because S is a transcendence set. Suppose that one of the n elements is x; say $x_n = x$. If f is in the kernel of the homomorphism $f \mapsto f(x_1, \dots, x_n)$, i.e., if $f(x_1, \dots, x_n) = 0$, then x is a root of the polynomial $g(X) = f(x_1, \dots, x_{n-1}, X)$ in $K(x_1, \dots, x_{n-1})[X]$. Since x is assumed to be transcendental over $K(S)$, the polynomial g must be 0. If we expand the polynomial f in powers of X as

$$f(X_1, \dots, X_{n-1}, X) = c_l(X_1, \dots, X_{n-1})X^l + \cdots + c_0(X_1, \dots, X_{n-1}),$$

the condition that g be 0 says that $c_j(x_1, \dots, x_{n-1}) = 0$ for all j. Since the set $\{x_1, \dots, x_{n-1}\}$ is algebraically independent, we see that $c_j = 0$. Therefore $f = 0$. Hence $\{x_1, \dots, x_n\}$ is algebraically independent, and S' is a transcendence set.

Conversely suppose that S' is a transcendence set of L over K. We are to show that the only polynomial $F(X)$ in $K(S)[X]$ such that $F(x) = 0$ is the 0 polynomial. Since only finitely many coefficients of F are in question, we may view F as in $K(\{x_1, \dots, x_n\})[X]$ for some finite subset $\{x_1, \dots, x_n\}$ of S. Clearing fractions, we can write F as

$$F(X) = d(x_1, \dots, x_n)^{-1}\big(c_l(x_1, \dots, x_n)X^l + \cdots + c_0(x_1, \dots, x_n)\big)$$

for suitable polynomials $d, c_0, \dots, c_l$ in $K[X_1, \dots, X_n]$ with $d(x_1, \dots, x_n) \neq 0$. Define

$$\widetilde{F}(X_1, \dots, X_n, X) = c_l(X_1, \dots, X_n)X^l + \cdots + c_0(X_1, \dots, X_n).$$

The condition $F(x) = 0$ yields $\widetilde{F}(x_1, \dots, x_n, x) = 0$. Since $\{x_1, \dots, x_n, x\}$ is by assumption algebraically independent over K, we see that $\widetilde{F} = 0$. Thus $c_j(X_1, \dots, X_n) = 0$ for all j, and consequently $c_j(x_1, \dots, x_n) = 0$ for all j. Therefore $F = 0$, as required. □

Lemma 7.6. If L/K is a field extension, then

(a) any transcendence set of L over K can be extended to a transcendence basis of L over K,
(b) any subset of L that generates L as a field over K has a subset that is a transcendence basis of L over K.

In particular, there exists a transcendence basis of L over K.

PROOF. For (a), order by inclusion upward the transcendence sets containing the given one. To apply Zorn's Lemma, we need only show that the union of a chain of transcendence sets in L over K is again a transcendence set. Thus let finitely many elements of the union of the sets in the chain be given. Since the sets in the chain are nested, all these elements lie in one member of the chain. Hence they are algebraically independent over K, and it follows from the definition that the union of the sets in the chain is a transcendence set. By Zorn's Lemma there exists a maximal transcendence set, and this is a transcendence basis by definition.

For (b), we argue in the same way as for (a). Let the given generating set be G. Order by inclusion upward the transcendence sets that are subsets of G. The empty set is such a transcendence set. As with (a), the union of a chain of transcendence sets in L over K is again a transcendence set, and the union is contained in G if each individual set is. By Zorn's Lemma there exists a maximal transcendence subset S of G. To complete the proof, it is enough to show that every member of G is algebraic over $K(S)$. Let x be in G. We may assume that x is not in S. By maximality, $S \cup \{x\}$ is not a transcendence set. Then Lemma 7.5 shows that x is algebraic over $K(S)$. Hence S is the required transcendence basis.

For the final conclusion we apply (a) to the empty set, which is a transcendence set of L over K. □

Theorem 7.7. If L/K is a field extension, then there exists an intermediate field K' such that K'/K is purely transcendental and L/K' is algebraic.

PROOF. Lemma 7.6 produces a transcendence basis S for L/K. Define K' to be the intermediate field $K(S)$ generated by K and S. Then K' is purely transcendental over K by definition. If x is a member of L that is not in K', then $S \cup \{x\}$ is not a transcendence set of L over K by maximality of S, and Lemma 7.5 shows that x is algebraic over $K(S) = K'$. Hence L is algebraic over K'. □

As was mentioned earlier in the section, the intermediate field K' with the properties stated in the theorem is not unique. In the example above with $\mathbb{K} = \mathbb{C}$ and with L equal to the field of fractions of $\mathbb{C}[X, Y]/\big(Y^2 - X(X+1)(X-1)\big)$, K' can be any subfield $\mathbb{C}(z)$ with z not in the subfield $\mathbb{C}$. For an even simpler example, let K be arbitrary, and let $L = K(x)$ be any purely transcendental

extension. Use of the transcendence basis $\{x\}$ of L over K leads to $K' = L$ in the proof of Theorem 7.7. But $\{x^2\}$ is another transcendence basis, and for it we have $K' = K(x^2)$. The extension L/K' is algebraic because x is a root of the polynomial $X^2 - x^2$ in $K(x^2)[X]$.

We turn to the matter of showing that any two transcendence bases of L over K have the same cardinality. We shall make use of the following result, which was proved at the end of the appendix of *Basic Algebra*:

> Let S and E be nonempty sets with S infinite, and suppose that to each element s of S is associated a countable subset E_x of E in such a way that $E = \bigcup_{s\in S} E_s$. Then card $E \leq$ card S.

In our application of this result, the sets E_x will all be finite sets.

Lemma 7.8 (Exchange Lemma). Let L/K be a field extension. If E is any subset of L, let $K(E)$ be the subfield of L generated by K and E, and let $\overline{K(E)}$ be the subfield of all elements in L that are algebraic over $K(E)$. If $E \cup \{x\}$ and $E \cup \{y\}$ are finite transcendence sets of L over K and if x lies in $\overline{K(E \cup \{y\})}$ but not $\overline{K(E)}$, then y lies in $\overline{K(E \cup \{x\})}$.

PROOF. The condition that x lie in $\overline{K(E \cup \{y\})}$ implies that there exist a finite subset $\{x_1, \ldots, x_n\}$ of E and a member f of $K(X_1, \ldots, X_n, Y)[Z]$ such that

$$f(x_1, \ldots, x_n, y, Z) \neq 0 \qquad \text{but} \qquad f(x_1, \ldots, x_n, y, x) = 0. \tag{$*$}$$

Clearing fractions, we may assume that f lies in $K[X_1, \ldots, X_n, Y, Z]$. Expand f in powers of Y as

$$f(X_1, \ldots, X_n, Y, Z) = \sum_{j=0}^{l} c_j(X_1, \ldots, X_n, Z)Y^j.$$

Since $f(x_1, \ldots, x_n, y, Z) \neq 0$ by $(*)$, at least one of the coefficients, say c_i, has to satisfy $c_i(x_1, \ldots, x_n, Z) \neq 0$. Lemma 7.5 shows that x is transcendental over $K(E)$, and therefore $c_i(x_1, \ldots, x_n, x) \neq 0$. Consequently $f(x_1, \ldots, x_n, Y, x)$ is nonzero. Since $f(x_1, \ldots, x_n, y, x) = 0$ by $(*)$, y is algebraic over $K(\{x_1, \ldots, x_n, x\})$. Therefore y lies in $\overline{K(E \cup \{x\})}$. □

The statement of Lemma 7.8 defines an operation $E \mapsto \overline{K(E)}$ on subsets of L. Because an algebraic extension of an algebraic extension is algebraic, applying this operation a second time does nothing new: $\overline{K\big(\overline{K(E)}\big)} = \overline{K(E)}$. We shall make use of this fact in the proof of Theorem 7.9 below.

Theorem 7.9. If L/K is a field extension, then any two transcendence bases of L over K have the same cardinality.

REMARKS. The cardinality is called the **transcendence degree** of L/K. For applications to algebraic geometry, the situation of interest is that this cardinality is finite, but we give a complete proof of the theorem anyway.

PROOF. First suppose that L/K has a finite transcendence basis B. Let $|B| = n$. Let B' be another transcendence basis, and let $m = |B \cap B'|$. We prove that $|B'| = |B|$ by induction downward on m. The base case of the induction is that $m = n$. Then $B \subseteq B'$, and we must have $B = B'$ by maximality of B.

For the inductive step, suppose that $m < n$ and that $|B'| = |B|$ whenever $|B \cap B'| \geq m + 1$. We write the elements of B in an order such that $B = \{x_1, \ldots, x_n\}$ and $B \cap B' = \{x_1, \ldots, x_m\}$. Lemma 7.5 shows that x_{m+1} is transcendental over $K(B - \{x_{m+1}\})$. Hence x_{m+1} does not lie in $\overline{K(B - \{x_{m+1}\})}$. A second application of Lemma 7.5 shows that $L = \overline{K(B')}$. The inclusion $B' \subseteq \overline{K(B - \{x_{m+1}\})}$ is impossible because otherwise we would have

$$L = \overline{K(B')} \subseteq \overline{K\big(\overline{K(B - \{x_{m+1}\})}\big)} = \overline{K(B - \{x_{m+1}\})}.$$

Hence there exists an element y of B' that does not lie in $\overline{K(B - \{x_{m+1}\})}$. A third application of Lemma 7.5 shows that $(B - \{x_{m+1}\}) \cup \{y\}$ is a transcendence set for L/K. Since y lies in $L = \overline{K(B)}$, the Exchange Lemma (Lemma 7.8) shows that x_{m+1} lies in $\overline{K\big((B - \{x_{m+1}\}) \cup \{y\}\big)}$. Consequently B is contained in $\overline{K\big((B - \{x_{m+1}\}) \cup \{y\}\big)}$, and $L = \overline{K\big((B - \{x_{m+1}\}) \cup \{y\}\big)}$. A fourth application of Lemma 7.5 shows that the transcendence set $B_1 = (B - \{x_{m+1}\}) \cup \{y\}$ is a transcendence basis. The set B_1 has n elements, and the inclusion $B_1 \cap B' \supseteq \{x_1, \ldots, x_m, y\}$ shows that $|B_1 \cap B'| \geq m + 1$. The inductive hypothesis shows that $|B'| = |B_1|$, and therefore $|B'| = |B|$. This completes the proof under the assumption that L/K has a finite transcendence basis.

We may now suppose that L/K has no finite transcendence basis. Let B be a transcendence basis of L/K; existence is by Lemma 7.6. To each element x of L, we shall associate a canonical finite subset E_x of L.

Since the element x is algebraic over $K(B)$, use of the field polynomial of x over $K(B)$ shows that x is algebraic over $K(E)$ for some finite subset E of B. Let E_0 be such a finite set E with the smallest cardinality; the set E_0 will be the canonical finite subset E_x that we seek. To show that E_0 is canonical, we show that whenever x lies in $\overline{K(E)}$ for some finite subset E of B, then $E_0 \subseteq E$. Arguing by contradiction, suppose that y is a member of E_0 that is not in E, and define $E_1 = E_0 - \{y\}$. By minimality of $|E_0|$, x does not lie in $\overline{K(E_1)}$. However, x does lie in $\overline{K(E_1 \cup \{y\})}$. Application of the Exchange Lemma shows that y lies in $\overline{K(E_1 \cup \{x\})}$. Since

$$\overline{K(E_1 \cup \{x\})} \subseteq \overline{K\big(E_1 \cup \overline{K(E)}\big)} \subseteq \overline{K\big(\overline{K(E_1 \cup E)}\big)} = \overline{K(E_1 \cup E)},$$

y lies in $\overline{K(E_1 \cup E)}$. Since y is in B but is not in $E_1 \cup E$, Lemma 7.5 shows that y is not algebraic over $K(E_1 \cup E)$, and we arrive at a contradiction. This completes the proof that whenever x lies in $\overline{K(E)}$ for some finite subset E of B, then $E_0 \subseteq E$. Hence E_0 is canonical.

For each element x of L, we let E_x be the finite subset of B constructed in the previous paragraph. Then we have a well-defined map of L to the set of all finite subsets of B given by $x \mapsto E_x \subseteq B$. Now let B' be a second transcendence basis of L/K, and restrict the map from L to B'. Taking $S = B'$ and $E = \bigcup_{x \in B'} E_x$ in the indented result quoted just before Lemma 7.8, we find that

$$\operatorname{card}\Big(\bigcup_{x \in B'} E_x\Big) \leq \operatorname{card}(B'). \tag{$*$}$$

On the other hand, any x in B' lies in $\overline{K(E_x)}$ by definition of E_x. Hence $B' \subseteq \overline{K\big(\bigcup_{x \in B'} E_x\big)}$. Applying the operation $\overline{K(\,\cdot\,)}$ to both sides gives

$$L = \overline{K(B')} \subseteq \overline{K\Big(\overline{K\big(\bigcup_{x \in B'} E_x\big)}\Big)} = \overline{K\big(\bigcup_{x \in B'} E_x\big)}.$$

Since $\bigcup_{x \in B'} E_x$ is a subset of B and since a proper subset of B cannot be a transcendence basis of L/K, we conclude that

$$B = \textstyle\bigcup_{x \in B'} E_x.$$

Consequently

$$\operatorname{card} B = \operatorname{card}\big(\textstyle\bigcup_{x \in B'} E_x\big).$$

In combination with $(*)$, this equality implies that $\operatorname{card} B \leq \operatorname{card} B'$. Reversing the roles of B and B' gives $\operatorname{card} B' \leq \operatorname{card} B$. Therefore $\operatorname{card} B = \operatorname{card} B'$ by the Schroeder–Bernstein Theorem.[3] □

3. Separable and Purely Inseparable Extensions

Thus far in this book, we have been interested in the detailed structure of algebraic field extensions only when they are separable. For applications to algebraic geometry, however, algebraic extensions that are not separable arise and even play a special role. Thus it is essential to have some understanding of their nature.

Let us review the material on separability in Section IX.6 of *Basic Algebra*. Let K be a field. An irreducible polynomial in $K[X]$ is defined to be **separable** if it splits into distinct first-degree factors in its splitting field over K. Let L/K be an algebraic extension of fields. An element of L is defined to be **separable** over K if its minimal polynomial over K is separable. Elements of L that fail to be separable over K are called **inseparable** over K. The prototype of an inseparable

[3] A proof of the Schroeder–Bernstein Theorem appears in the appendix of *Basic Algebra*.

element is the element $a^{1/p}$ in the extension $\Bbbk(a^{1/p})$, where $\Bbbk = \mathbb{F}_p(a)$ is a simple transcendental extension of the finite field $\mathbb{F}_p$. Corollary 9.31 of *Basic Algebra* shows that the separable elements of L over K form a subfield, and L/K is defined to be separable if every every member of L is separable over K. As a consequence of Corollary 9.29 of *Basic Algebra*, we know that a separable extension of a separable extension is separable.

One further tool from *Basic Algebra* is needed in order to handle the failure of separability. This is Proposition 9.27, which says that an irreducible polynomial $f(X)$ in $K[X]$ is separable if and only if $f'(X)$ is not the zero polynomial. It is immediate that every irreducible polynomial is separable if K has characteristic 0. Thus we need discuss only characteristic p in the remainder of this section.

The consequence of Proposition 9.27 for characteristic p is that an irreducible polynomial $f(X)$ fails to be separable over K if and only if the only powers of X that appear with nonzero coefficient in $f(X)$ are the powers X^{kp}, i.e., if and only if $f(X) = g(X^p)$ for some g in $K[X]$.

In this case the polynomial $g(X)$ is certainly irreducible in $K[X]$, and we can repeat this process. The polynomial $g(X)$ fails to be separable over $K[X]$ if and only if $g(X) = h(X^p)$ for some h in $K[X]$. Then $f(X) = h(X^{p^2})$. Repeating this process as many times as possible, we see that to each irreducible polynomial $f(X)$ in $K[X]$ correspond a unique nonnegative integer e and a unique *separable* irreducible polynomial $g(X)$ such that $f(X) = g(X^{p^e})$. We call p^e the **degree of inseparability** of $f(X)$ over K. From the definitions an element of an algebraic extension of K is inseparable if and only if the degree of inseparability of its minimal polynomial over K is greater than 1.

If L/K is an algebraic field extension, then an element α of L is said to be **purely inseparable**[4] over K if α^{p^μ} lies in K for some integer $\mu \geq 0$. Let us see in this case that the minimal polynomial of α over K is of the form $X^{p^e} - \alpha^{p^e}$ for some $e \geq 0$.

Proposition 7.10. If K is a field of characteristic p and if α is a member of K such that $\sqrt[p]{\alpha}$ is not in K, then $X^{p^\mu} - \alpha$ is irreducible in $K[X]$ for every $\mu \geq 0$.

PROOF. Let L be a splitting field of $X^{p^\mu} - \alpha$ over K. If β is a root of $X^{p^\mu} - \alpha$, then $\beta^{p^\mu} = \alpha$, and hence $X^{p^\mu} - \alpha = X^{p^\mu} - \beta^{p^\mu} = (X - \beta)^{p^\mu}$.

Let $f(X)$ be a monic irreducible factor of $X^{p^\mu} - \alpha$ in $K[X]$. Let us see that $X^{p^\mu} - \alpha = f(X)^n$ for some n. In fact, if the contrary were true, then there would be a second monic irreducible factor $g(X)$ of $X^{p^\mu} - \alpha$ in $K[X]$ relatively prime to $f(X)$. Then we can write $u(X)f(X) + v(X)g(X) = 1$ for suitable

[4] *Warning:* Not every element of L that is purely inseparable over K is inseparable over K. The elements of K are counterexamples. Corollary 7.12 below shows that the elements of K are the only counterexamples.

polynomials $u(X)$ and $v(X)$ in $K[X]$. As members of $L[X]$, both $f(X)$ and $g(X)$ have to be powers of $X - \beta$ by unique factorization, and thus they both vanish at β. Substitution of β into $uf + vg = 1$ therefore yields a contradiction. Hence $X^{p^\mu} - \alpha = f(X)^n$.

Since $f(X)$ has to be $(X - \beta)^m$ for some m, we obtain $X^{p^\mu} - \alpha = f(X)^n = (X - \beta)^{mn}$. The integers m and n must divide p^μ. Thus $m = p^\nu$, and $f(X) = (X-\beta)^{p^\nu} = X^{p^\nu} - \beta^{p^\nu}$. Since $f(X)$ is assumed to be in $K[X]$, β^{p^ν} lies in K. An inequality $\nu < \mu$ would imply that $\gamma = (\beta^{p^\nu})^{p^{\mu-\nu-1}}$ lies in K; the p^{th} power of γ is α, however, and the hypothesis of the proposition says that such an element γ cannot be in K. We conclude that $\nu = \mu$, and thus $f(X) = X^{p^\mu} - \alpha$. In other words, $X^{p^\mu} - \alpha$ is irreducible in $K[X]$. □

Corollary 7.11. If L/K is an algebraic extension in characteristic p, if α is a purely inseparable element of L over K, and if e is the smallest nonnegative integer such that α^{p^e} lies in K, then the minimal polynomial of α over K is $X^{p^e} - \alpha^{p^e}$.

PROOF. This is immediate from Proposition 7.10. □

Corollary 7.12. If L/K is an algebraic extension in characteristic p and if α is an element of L that is separable and purely inseparable over K, then α lies in K.

PROOF. Since α is purely inseparable over K, Corollary 7.11 says that the minimal polynomial of α over K is $X^{p^e} - \alpha^{p^e}$, where e is the smallest nonnegative integer such that α^{p^e} lies in K. The separability of α says that this polynomial is separable. Unless $p^e = 1$, the polynomial has derivative 0 and thus repeated roots. Therefore $p^e = 1$ and $e = 0$, and we conclude that α lies in K. □

An algebraic field extension L/K in characteristic p is said to be **purely inseparable** if every element of L is purely inseparable over K. Since purely inseparable elements α have minimal polynomials of the form $X^{p^e} - \alpha^{p^e}$, the degree of a purely inseparable extension has to be a power of p.

Theorem 7.13. If L/K is an algebraic field extension in characteristic p and if K_s is the subfield of all elements of L that are separable over K, then L/K_s is a purely inseparable extension.

PROOF. Let α be an element of L, and let $f(X)$ be the minimal polynomial of α over K. Then we can write $f(X) = g(X^{p^e})$, where p^e is the degree of inseparability of f. The polynomial $g(X)$ is irreducible over K, and it is separable. Since α^{p^e} is a root, α^{p^e} is a separable element. Therefore α^{p^e} lies in K_s. By definition of pure inseparability, α is purely inseparable over K_s. Since α is arbitrary in L, L is purely inseparable over K_s. □

Corollary 7.14. Let R be a Dedekind domain, let F be its field of fractions, let K be a finite algebraic extension of F, and let T be the integral closure of R in K. Then T is a Dedekind domain.

REMARKS. This result is quite important. It was used extensively in Chapter VI, as was explained in the remarks with Proposition 6.7, and it plays a foundational role in the theory of algebraic curves as presented in Chapters IX and X. Theorem 8.54 of *Basic Algebra* proved this result under the assumption that K is a finite separable extension of F, and we are now dropping the hypothesis of separability. Since K/F is automatically a separable extension in characteristic 0, we may assume that the characteristic is not 0.

PROOF. Theorem 7.13 shows that K can be obtained in two steps from F, a separable extension followed by a purely inseparable extension. The integral closure of F in the separable extension field is a Dedekind domain D by Theorem 8.54 of *Basic Algebra*, and the integral closure of D in K equals T by the transitivity of integral closure. Consequently it is enough to prove the corollary under the additional hypothesis that K is a purely inseparable extension of F. What needs proof (in view of the statement of Theorem 8.54 of *Basic Algebra*) is that T is Noetherian, i.e., that each ideal of T is finitely generated.

Let p be the characteristic. Since K/F is finite and purely inseparable, there exists some power $q = p^m$ of p such that the field K^q is contained in F; specifically, the integer q is to be large enough for the q^{th} power of each element of a vector-space basis of K over F to lie in F. We begin by proving that

$$T = \{b \in K \mid b^q \in R\}. \tag{$*$}$$

The inclusion $\subseteq$ follows, since $b \in T$ implies that b^q is in $T \cap F = R$. For the inclusion $\supseteq$, let $b \neq 0$ be in K. Corollary 7.11 shows that the minimal polynomial of b over F is $X^{p^e} - b^{p^e}$, where e is the smallest integer ≥ 0 such that b^{p^e} lies in F. Since $K^{p^m} \subseteq F$, $e \leq m$. Thus b is a root of a polynomial $X^{p^m} - a$, where $a = b^{p^m}$ is a member of R. Consequently b is integral over R and must lie in T. This proves $(*)$.

Fix an algebraic closure K_{alg} of K, and let $H = F^{q^{-1}}$ denote the inverse image of F under the q^{th} power isomorphism of K_{alg} onto itself. This is a subfield of K_{alg}, and it contains K because $K^q \subseteq F$. Let $S \subseteq H$ be the ring of all b in H with b^q in R. Since $x \mapsto x^q$ is a field isomorphism of H onto F, $x \mapsto x^q$ is a ring isomorphism of S onto R. Therefore S is a Dedekind domain. It contains T by $(*)$.

Let I be a nonzero ideal in T, and form the ideal $J = SI$ in S generated by I. Since S is Dedekind, J is invertible as a fractional ideal of H relative to S. If J^{-1} denotes the inverse, then J^{-1} is a finitely generated S module in H such that

$J^{-1}J = S$. Thus $S = J^{-1}J = J^{-1}SI = J^{-1}I$. Accordingly, choose finite sets $\{x_i\}$ in J^{-1} and $\{a_i\}$ in I such that $\sum x_i a_i = 1$.

We shall show that $\{a_i\}$ is a set of generators of I as an ideal in T. We apply the q^{th} power mapping to $\sum x_i a_i = 1$, obtaining $\sum x_i^q a_i^q = 1$ with x_i^q in $H^q = F \subseteq K$ and with a_i^q in $S^q = R$. Put $b_i = a_i^{q-1} x_i^q$. Then $\sum x_i^q a_i^q = 1$ implies that $\sum a_i b_i = 1$; here a_i is in I and b_i is in $I^{q-1}K \subseteq K$. If a is in I, then $\sum (b_i a) a_i = a$, and it is enough to show that $b_i a$ is in T for each i, i.e., to show that $b_i I \subseteq T$ for each i.

The q-fold product $(x_i I) \cdots (x_i I)$ is contained in S because $x_i I \subseteq J^{-1}J = S$. Thus $b_i I = x_i^q a_i^{q-1} I \subseteq S$. So $b_i I \subseteq S \cap K$. If s is any element in $S \cap K$, then we know that $r = s^q$ is a member of R because $S^q = R$. Hence s is a root of $X^q - r$ with r in R. That is, s is integral over R. Since s also is in K, s lies in the integral closure of R in K, which is T. Thus $b_i I \subseteq T$, and the proof is complete. □

A field K is **perfect** if either it has characteristic 0 or else it has characteristic p and the field map $x \mapsto x^p$ of K into itself is onto. Examples of perfect fields include all finite fields, all algebraically closed fields, and of course all fields of characteristic 0.

Proposition 7.15. A field K is perfect if and only if every algebraic extension of K is separable.

PROOF. We need to consider only the case that K has characteristic p. Suppose that $x \mapsto x^p$ fails to be onto K. Choose β in K such that $X^p - \beta$ has no root in K. Proposition 7.10 shows that $X^p - \beta$ is irreducible over K. Since this polynomial has derivative 0, it is not separable. Thus $X^p - \beta$ is a polynomial that is irreducible but not separable, and adjunction of a root of $X^p - \beta$ to K produces an extension L of K that is not separable.

Conversely suppose that the field map $x \mapsto x^p$ of K to itself is onto. Then $x \mapsto x^{p^e}$ is onto K for every $e \geq 0$. Let L be an algebraic extension of K, and let K_s be the subfield of elements separable over K. If α is given in L, then Theorem 7.13 shows that there exists a nonnegative integer e such that α^{p^e} is in K_s. Let $g(X)$ be the minimal polynomial of α^{p^e} over K, and write $g(X) = X^m + c_1 X^{m-1} + \cdots + c_m$. Since K is perfect, there exists b_j for each j with $1 \leq j \leq m$ such that $b_j^{p^e} = c_j$. Put $f(X) = X^m + b_1 X^{m-1} + \cdots + b_m$. Then

$$f(\alpha)^{p^e} = (\alpha^{p^e})^m + b_1^{p^e} (\alpha^{p^e})^{m-1} + \cdots + b_m^{p^e} = g(\alpha^{p^e}) = 0,$$

and therefore $f(\alpha) = 0$. Consequently $f(X)$ divides the minimal polynomial of α over K, and the fact that α^{p^e} lies in $K(\alpha)$ implies that

$$[K(\alpha) : K] \leq \deg f(X) = \deg g(X) = [K(\alpha^{p^e}) : K] \leq [K(\alpha) : K].$$

Equality must hold throughout, and therefore $K(\alpha) = K(\alpha^{p^e})$. Since $K(\alpha^{p^e})$ is contained in K_s, α lies in K_s. Therefore every member of L lies in K_s, and L is separable over K. □

A **function field** in r variables over a field K is a field L that is finitely generated over K and has transcendence degree r over K. A transcendence basis $\{x_1, \dots, x_r\}$ of such an extension L/K is called a **separating transcendence basis** of L/K if L is a separable algebraic extension of $K(x_1, \dots, x_r)$. If the function field L in r variables over K has a separating transcendence basis, we say that L is **separably generated** over K.

The two kinds of fields of continual interest in Chapter VI were number fields and function fields in one variable over a base field. In the latter case some results beginning in Section VI.6 assumed in effect that the function field is separably generated over the base field. It was asserted at the beginning of Section VI.9 that function fields in one variable over finite fields are always separably generated; this assertion is a special case of Theorem 7.20 below.

Proposition 4.28 of *Basic Algebra* gave a version of the Factor Theorem valid for all commutative rings with identity. For the present investigation we need a version of the division algorithm that is valid in this wider context.

Lemma 7.16. Let R be a commutative ring with identity, let $f(X)$ and $g(X)$ be members of $R[X]$ of respective degrees m and n, and let a be the leading coefficient of $g(X)$. For the integer $k = \max(m - n + 1, 0)$, there exist $q(X)$ and $r(X)$ in $R[X]$ such that

$$a^k f(X) = g(X)q(X) + r(X) \qquad \text{with } \deg r < n \text{ or } r = 0.$$

PROOF. If $m < n$, then $k = 0$, and the displayed formula holds with $q(X) = 0$ and $r(X) = f(X)$. For $m \geq n - 1$, we proceed by induction on m. The base case of the induction is $m = n - 1$, which we have already handled. For the inductive step, suppose that $m \geq n$. The integer k is $m - n + 1$. If b is the leading coefficient of $f(X)$, then $af(X) - bX^{m-n}g(X)$ is a polynomial that either is 0 or has degree less than m. The inductive hypothesis allows us to write

$$a^{(m-1)-n+1}\big(af(X) - bX^{m-n}g(X)\big) = g(X)q_1(X) + r_1(X)$$

with $\deg r_1 < n$ or $r_1 = 0$. If we set $q(X) = ba^{m-n}X^{m-n} + q_1(X)$ and $r(X) = r_1(X)$, then we obtain $a^k f(X) = g(X)q(X) + r(X)$, and the lemma follows. □

Lemma 7.17. Let L/K be a field extension, let $x_1, \dots, x_n, x_{n+1}$ be elements of L, and suppose that $x_1, \dots, x_n$ are algebraically independent over K but that $x_1, \dots, x_n, x_{n+1}$ are not algebraically independent. Then the ideal I of all polynomials in $K[X_1, \dots, X_{n+1}]$ that vanish at $(x_1, \dots, x_{n+1})$ is principal with a generator that is irreducible in $K[X_1, \dots, X_{n+1}]$ and involves X_{n+1} nontrivially.

PROOF. The algebraic dependence implies that I contains nonzero polynomials. Let $g(X_1, \ldots, X_n, X_{n+1})$ be one whose degree in X_{n+1} is as small as possible, say l. Expand g as

$$g = c_0(X_1, \ldots, X_n)X_{n+1}^l + c_1(X_1, \ldots, X_n)X_{n+1}^{l-1} + \cdots + c_l(X_1, \ldots, X_n).$$

The algebraic independence of $X_1, \ldots, X_n$ implies that at least one of $c_0, \ldots, c_{l-1}$ is nonzero. Since $K[X_1, \ldots, X_n]$ is a unique factorization domain, we can factor out and discard the greatest common divisor of the coefficients $c_0, \ldots, c_l$. Thus we may assume that g is primitive as a polynomial in X_{n+1}. If f is any element in I, then Lemma 7.16 applied to the ring $K[X_1, \ldots, X_n]$ allows us to write $a^k f = gq + r$ with $r = 0$ or $\deg r < k$. Substituting $(x_1, \ldots, x_{n+1})$, we see that r is in I. The minimality of l implies that $r = 0$, and thus $a^k f = gq$. Write $c(h)$ for the greatest common divisor of the coefficients of a polynomial h. Taking the greatest common divisor of the coefficients on each side of $a^k f = gq$ and applying Gauss's Lemma, we obtain $a^k c(f) = c(q)$. Therefore a^k divides q, and we obtain $f = gq_0$ for some q_0. Consequently I is principal. If $g = g_1 g_2$, then the definition of I shows that at least one of g_1 and g_2 is in I, say g_1. The minimality of l implies that the degree of g_1 in X_{n+1} is l. Therefore g_2 is in $K[X_1, \ldots, X_n]$. Since g is primitive, g_2 divides 1. Hence g_2 lies in K. □

Theorem 7.18 (Mac Lane). If L/K is a field extension that is finitely generated and separably generated, then any set of generators contains a subset that is a separating transcendence basis of L/K.

PROOF. Let the characteristic be p. The proof is by induction on the transcendence degree of the extension. For transcendence degree 0, the required set is the empty set, and there is nothing to prove. The main step is transcendence degree 1.

Thus let $L = K(x_1, \ldots, x_n)$, and suppose that $\{z\}$ is a transcendence basis of L over K such that L is separable over $K(z)$. Since z is transcendental, z does not lie in $K(z^p)$. Thus Proposition 7.10 shows that $X^p - z^p$ is irreducible over $K(z^p)$, and z is inseparable over $K(z^p)$. The field L is algebraic over $K(z^p)$, and the subset of separable elements over $K(z^p)$ is a subfield. Since $L = K(x_1, \ldots, x_n)$ and since z is a member of L that is not separable over $K(z^p)$, it follows that some x_i, say x_1, is inseparable over $K(z^p)$. It will be proved that $\{x_1\}$ is a separating transcendence basis of L over K, i.e., that x_1 is transcendental over K and that L is separable algebraic over $K(x_1)$.

We apply Lemma 7.17 with $n = 2$ to the elements z, x_1. The lemma produces an irreducible polynomial $f(Z, X)$ in $K[Z, X]$ such that $f(z, x_1) = 0$. Gauss's Lemma shows that this polynomial remains irreducible when considered in $K(Z)[X]$, and we have a ring isomorphism $K(Z)[X] \cong K(z)[X]$ because z is

transcendental over K. Up to a nonzero factor from $K(z)$, $f(z, X)$ is the minimal polynomial of x_1 over $K(z)$. Since L is separable over $K(z)$, the element x_1 is separable over $K(z)$, and its minimal polynomial over $K(z)$ involves some power of X that is not a power of X^p.

Let us prove that x_1 is transcendental over K. In the contrary case, let $g(X)$ be its minimal polynomial over K. Since g vanishes when $X = x_1$ and $Z = z$, $g(X)$ satisfies an identity $g(X) = q(Z, X)f(Z, X)$ in $K[Z, X]$. It therefore satisfies the same identity in $K(X)[Z]$. Since $g(X)$ is a unit in $K(X)[Z]$, so is $f(Z, X)$. Therefore $f(Z, X)$ is independent of Z. Since $g(X)$ is the minimal polynomial for x_1 over K, $g(X) = cf(Z, X)$ for some c in K. Since $f(Z, X)$ involves a power of X that is not a power of X^p, the same thing is true of $g(X)$, and consequently x_1 is separable over K. Therefore x_1 is separable over the larger field $K(z^p)$, in contradiction to the defining condition on x_1. We conclude that x_1 is transcendental over K.

Since L has transcendence degree 1 over K, it follows that z is algebraic over $K(x_1)$. Let us see that z is separable over $K(x_1)$. In fact, Gauss's Lemma shows that $f(Z, X)$ remains irreducible when considered in $K(X)[Z]$, and we have a ring isomorphism $K(X)[Z] \cong K(x_1)[Z]$ because x_1 is transcendental over K. Therefore $f(Z, x_1)$ is the product of a nonzero member of $K(x_1)$ and the minimal polynomial $m(Z)$ of z over $K(x_1)$. If z were inseparable over $K(x_1)$, then $m(Z)$ would be a polynomial in Z^p, and we would have $f(Z, X) = h(Z^p, X)$ with h in $K[Z, X]$. We know that $f(Z, X)$ involves some power of X that is not a power of X^p, and hence the same thing is true of $h(Z^p, X)$. Since $h(z^p, X)$ is irreducible in $K[X]$, x_1 is separable over $K(z^p)$, in contradiction to the defining property of x_1. Therefore z is separable over $K(x_1)$.

The defining property of z is that all x_j are separable over $K(z)$. Since z is separable over $K(x_1)$, all of $x_2, \ldots, x_n$ are separable over $K(x_1)$. Therefore L is separable over x_1, and $\{x_1\}$ is a separable transcendence basis of L/K. This completes the proof of the theorem for transcendence degree 1.

The inductive step is somewhat a formal consequence of what has just been proved. To see this, suppose that the theorem is known for transcendence degrees 1 and $r - 1$, and let $L = K(x_1, \ldots, x_n)$ have transcendence degree r. The assumption is that L has a transcendence basis $\{z_1, \ldots, z_r\}$ such that L is separable over $K(z_1, \ldots, z_r)$. Put $K_1 = K(z_1)$. Then the set $\{z_2, \ldots, z_r\}$ is a transcendence basis of L over K_1 consisting of $r - 1$ elements, and L is separable over $K_1(z_2, \ldots, z_r) = K(z_1, \ldots, z_r)$ by assumption. By the inductive hypothesis for the case of transcendence degree $r - 1$, some subset of $r - 1$ elements from among $x_1, \ldots, x_n$ forms a separating transcendence basis of L over K_1; let us say that this basis is $\{x_1, \ldots, x_{r-1}\}$. This implies that L is separable over $K_1(x_1, \ldots, x_{r-1}) = K(z_1, x_1, \ldots, x_{r-1})$. In other words, if $K' = K(x_1, \ldots, x_{r-1})$, then $L = K'(x_r, \ldots, x_n)$ is separable over $K'(z_1)$. Since

L/K' has transcendence degree 1, $\{z\}$ is a separating transcendence basis of L/K'. By the inductive hypothesis for transcendence degree 1, some x_j for $r \le j \le n$ forms a separating transcendence basis of L/K'. For this j, $\{x_1, \dots, x_{r-1}, x_j\}$ is then a separating transcendence basis of L/K. □

Lemma 7.19. Suppose that L is a field extension of transcendence degree r over a field K and that L is not separably generated over K. If $x_1, \dots, x_n$ are elements of L such that $L = K(x_1, \dots, x_n)$, then for a suitable relabeling of the x_i's, the subfield $K(x_1, \dots, x_{r+1})$ of L is of transcendence degree r and is not separably generated over K.

PROOF. We fix K and r, and we proceed by induction on n. The base case is that $n = r + 1$, and then there is nothing to prove. For the inductive step, suppose that the lemma has been proved for $n - 1$ when $n > r + 1$. We prove the lemma for n. Since $r < n$, we can renumber the x_i's and assume that $K(x_2, \dots, x_n)$ has transcendence degree r over K. If this field is not separably generated over K, then we are in a situation with $n - 1$ elements. The inductive hypothesis is applicable, and the lemma follows in this case.

Thus suppose that $K(x_2, \dots, x_n)$ is separably generated over K. Theorem 7.18 shows that after a renumbering of the indices, we may assume that $\{x_2, \dots, x_{r+1}\}$ is a separating transcendence basis of $K(x_2, \dots, x_n)$ over K. This implies that $K(x_2, \dots, x_n)$ is a separable extension of $K(x_2, \dots, x_{r+1})$. Since by assumption $L = K(x_1, \dots, x_n)$ is not separably generated over K, $K(x_1, \dots, x_n)$ is not separable over $K(x_2, \dots, x_{r+1})$. A separable extension of a separable extension is separable, and we deduce that $K(x_1, \dots, x_n)$ is not separable over $K(x_2, \dots, x_n)$. Thus x_1 is inseparable over $K(x_2, \dots, x_n)$ and is consequently inseparable over the subfield $K(x_2, \dots, x_{r+1})$. Hence $K(x_1, \dots, x_{r+1})$ is not separably generated over K. □

Theorem 7.20 (F. K. Schmidt). If K is a perfect field, then every finitely generated field extension of K is separably generated over K.

REMARK. In particular, the theorem applies if K is a finite field or is algebraically closed or has characteristic 0.

PROOF. Let K have characteristic p. We induct on the transcendence degree of the field extension of K. The base case of the induction is transcendence degree 0, and then the theorem is handled by Proposition 7.15. For the inductive step, assume that the theorem holds for all finitely generated field extensions of K having transcendence degree $r - 1$ over K. Let $L = K(x_1, \dots, x_n)$ have transcendence degree r over K. Arguing by contradiction, suppose that L is not separably generated over K. Lemma 7.19 shows for a suitable renumbering of the

x_i's that $K' = K(x_1, \ldots, x_{r+1})$ has transcendence degree r and is not separably generated over K.

We divide matters into two cases. First suppose that the transcendence degree of $K'' = K(x_1, \ldots, x_r)$ is $r - 1$. The inductive hypothesis shows that K'' is separably generated over K, and then Theorem 7.18 shows that we may renumber the variables in such a way that $\{x_1, \ldots, x_{r-1}\}$ is a transcendence basis of K'' over K and K'' is separable algebraic over $K(x_1, \ldots, x_{r-1})$. Then $\{x_1, \ldots, x_{r-1}, x_{r+1}\}$ is a transcendence basis of K', and x_r is algebraic over $K(x_1, \ldots, x_{r-1}, x_{r+1})$. Since x_r is separable over $K(x_1, \ldots, x_{r-1})$, it is separable over the larger field $K(x_1, \ldots, x_{r-1}, x_{r+1})$. Therefore K' is separably generated over K, contradiction.

The remaining case is that every subset of r members of $\{x_1, \ldots, x_{r+1}\}$ is a transcendence basis of K' over K. Lemma 7.17 produces an irreducible polynomial f in $K[X_1, \ldots, X_{r+1}]$ such that $f(x_1, \ldots, x_{r+1}) = 0$. Since $\{x_1, \ldots, x_r\}$ is a transcendence basis of K', application of Gauss's Lemma shows that f is irreducible in $K(X_1, \ldots, X_r)[X_{r+1}] \cong K(x_1, \ldots, x_r)[X_{r+1}]$. Hence up to a nonzero factor from K, $f(x_1, \ldots, x_r, X_{r+1})$ is the minimal polynomial of x_{r+1} over $K(x_1, \ldots, x_r)$. The failure of K' to be separably generated over K implies that x_{r+1} is inseparable over $K(x_1, \ldots, x_r)$, and thus the only powers of X_{r+1} that appear in its minimal polynomial over $K(x_1, \ldots, x_r)$ are powers X_{r+1}^{pk}. In other words, f is in $K[X_1, \ldots, X_r, X_{r+1}^p]$. Since we are assuming that any r of the elements $x_1, \ldots, x_{r+1}$ form a transcendence basis of K' over K, there is nothing special about X_{r+1} in this argument. Consequently f is in $K[X_1^p, \ldots, X_r^p, X_{r+1}^p]$. Since K is perfect, any polynomial involving only p^{th} powers of each indeterminate is the p^{th} power of some polynomial. Consequently f is reducible in $K[X_1, \ldots, X_{r+1}]$, in contradiction to the irreducibility guaranteed by Lemma 7.17. All cases thus lead to a contradiction, and the proof is complete. □

4. Krull Dimension

In this section we develop the algebraic background necessary for a discussion of dimension. Suppose that K is an algebraically closed field, suppose that I is a prime ideal in $K[X_1, \ldots, X_n]$, and suppose that $V(I)$ is the locus of common zeros of I. Corollary 7.2 shows that I is the set of all polynomials vanishing on $V(I)$, and thus the integral domain $R = K[X_1, \ldots, X_n]/I$ may be regarded as the set of all restrictions to $V(I)$ of polynomials. If L is the field of fractions of R, then the transcendence degree of L/K is interpreted as the "number of independent variables" on the locus $V(I)$. We define it to be the **dimension** of $V(I)$. The elements $X_j + I$ of R for $1 \leq j \leq n$ generate R as a K algebra, and therefore they generate L over K as a field. We shall make critical use of

the fact implied by Lemma 7.6b that some subset of $\{X_1 + I, \ldots, X_n + I\}$ is a transcendence basis of L. We shall speak of such a subset as a **transcendence basis** of R for economy of words. We denote its cardinality by tr. deg R.

EXAMPLE. We continue with the example from Sections 1–2. Let $K = \mathbb{C}$, let I be the principal ideal $\big(Y^2 - X(X+1)(X-1)\big)$ in $\mathbb{C}[X, Y]$, and let L be the field of fractions of the integral domain $R = \mathbb{C}[X, Y]/I$. Corollary 7.2 shows that the ring R is the ring of restrictions of polynomials to the locus $V(I) = \{(x, y) \in \mathbb{C}^2 \mid y^2 = x(x+1)(x-1)\}$. According to the above definition, the dimension of $V(I)$ is the transcendence degree of L, which we have seen is 1. This is in accord with the intuition that the locus $V(I)$ is a "curve" in the sense of having one independent complex parameter.

The goal of this section is to produce an equivalent definition of dimension that does not depend on the fact that $K[X_1, \ldots, X_n]/I$ is an integral domain. The rephrased definition will extend to any commutative ring with identity and is essential for modern algebraic geometry.

Let R be any commutative ring with identity. The **Krull dimension** of R, denoted by $\dim R$, is the supremum of the indices d of all strictly increasing chains

$$P_0 \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_d$$

of prime ideals in R. We define $\dim R = \infty$ if there is no finite supremum.

EXAMPLES OF KRULL DIMENSION.

(1) R equal to a field. The only prime ideal is 0. Thus the Krull dimension of any field is 0.

(2) $R = \mathbb{Z}$. The prime ideals are of the form $p\mathbb{Z}$ for each prime number p, together with 0. Each nonzero prime ideal is maximal. Consequently there is a strictly increasing chain $0 \subsetneqq p\mathbb{Z}$ of prime ideals for each prime number p, but there are no longer such chains. Thus $\dim \mathbb{Z} = 1$. More generally any principal ideal domain R that is not a field, or even any Dedekind domain R that is not a field, has $\dim R = 1$ because every nonzero prime ideal is maximal.

(3) R commutative Artinian. In Chapter II a ring with identity was defined to be Artinian if its two-sided ideals satisfy the descending chain condition. Problem 8 at the end of that chapter showed that *every* prime ideal in such a ring is maximal. In other words, every commutative Artinian ring has Krull dimension 0.

(4) Polynomial ring $R = K[X_1, \ldots, X_n]$, where K is a field. In geometric terms for the case that K is algebraically closed, the relevant zero locus for this R is K^n, which we certainly want to have dimension equal to n, and the field of fractions of R is $K(X_1, \ldots, X_n)$, which indeed has transcendence degree n. Let

us examine the Krull dimension of R. If $0 \leq k \leq n$ and if we form the ideal $(X_1, \ldots, X_k)$, then the ring isomorphism

$$R \cong K[X_{k+1}, \ldots, X_n][X_1, \ldots, X_k]$$

shows that the quotient $R/(X_1, \ldots, X_k)$ is isomorphic to $K[X_{k+1}, \ldots, X_n]$, which is an integral domain. Therefore $(X_1, \ldots, X_k)$ is prime, and we have a strictly increasing chain

$$0 \subsetneqq (X_1) \subsetneqq \cdots \subsetneqq (X_1, \ldots, X_{n-1}) \subsetneqq (X_1, \ldots, X_n).$$

So $\dim K[X_1, \ldots, X_n] \geq n$. Actually, equality holds, as Theorem 7.22 will show.

Lemma 7.21. Let R be a commutative ring with identity, let $S^{-1}R$ be the localization relative to a multiplicative system S in R, let I be an ideal in R, and let $\overline{S}$ be the image of S in R/I. Then

$$S^{-1}R\big/S^{-1}I \cong \overline{S}^{\,-1}(R/I)$$

via the mapping $s^{-1}r + S^{-1}I \mapsto (s + I)^{-1}(r + I)$.

PROOF. Let $q : R \to R/I$ and $\bar{q} : S^{-1}R \to S^{-1}R/S^{-1}I$ be the quotient homomorphisms, and let $\eta : R \to S^{-1}R$ and $\bar{\eta} : R/I \to \overline{S}^{\,-1}(R/I)$ be the canonical homomorphisms of R and R/I into their localizations. To each of the rings $X_1 = S^{-1}R\big/S^{-1}I$ and $X_2 = \overline{S}^{\,-1}(R/I)$ is associated a canonical map, namely $\eta_1 : R \to X_1$ and $\eta_2 : R \to X_2$ with $\eta_1 = \bar{q}\eta$ and $\eta_2 = \bar{\eta}q$. Let us see that the pairs (X_i, η_i) for $i = 1, 2$ have the following universal mapping property with respect to ring homomorphisms φ of R into a commutative ring T with identity such that $\varphi(1) = 1$, $\varphi(I) = 0$, and $\varphi(S) \subseteq T^\times$: there exists a unique homomorphism $\overline{\varphi}_i : X_i \to T$ such that $\varphi = \overline{\varphi}_i \eta_i$.

For $i = 1$, we first apply the universal mapping property of the localization $S^{-1}R$ to write $\varphi = \varphi_1\eta$ and then apply the universal mapping property of the quotient to write $\varphi = \overline{\varphi}_1\bar{q}\eta$. For $i = 2$, we first apply the universal mapping property of the quotient R/I to write $\varphi = \varphi_2 q$ and then apply the universal mapping property of the localization to write $\varphi = \overline{\varphi}_2\bar{\eta}q$. From these constructions we deduce existence and uniqueness of $\overline{\varphi}_i$ in both cases. The asserted isomorphism then follows from the general fact that objects satisfying a universal mapping property are unique up to isomorphism; tracking down that isomorphism gives the explicit formula in the lemma. □

Theorem 7.22. Let K be a field, let R be an integral domain that is finitely generated as a K algebra, and let L be the field of fractions of R. Then the Krull dimension of R equals the transcendence degree of L over K.

PROOF. If $x_1, \ldots, x_n$ are generators of R as a K algebra, then $R \cong K[X_1, \ldots, X_n]/I$, where I is the ideal of all polynomials in $K[X_1, \ldots, X_n]$ that vanish at $(x_1, \ldots, x_n)$. The ideal I is prime, since R is assumed to be an integral domain. Let r be the transcendence degree of L over K. We know from Lemma 7.6b that some subset of $\{x_1, \ldots, x_n\}$ is a transcendence basis of L over K; therefore $r \leq n$. To prove the theorem, we shall prove that $r \geq \dim R$ and that $r \leq \dim R$.

Suppose that P and Q are prime ideals of R with $P \subseteq Q$. Then the identity map on R descends to a K algebra homomorphism $\varphi : R/P \to R/Q$. If $\alpha_j = x_j + P$ and $\beta_j = x_j + Q$ are the images of x_j under the respective quotient maps $R \to R/P$ and $R \to R/Q$, then $\{\alpha_1, \ldots, \alpha_n\}$ is a set of generators of R/P, $\{\beta_1, \ldots, \beta_n\}$ is a set of generators of R/Q, and $\varphi(\alpha_j) = \beta_j$ for $1 \leq j \leq n$. If $r' = \text{tr. deg } R/Q$, we may assume that $\{\beta_1, \ldots, \beta_{r'}\}$ is a transcendence basis of R/Q. Then $\{\alpha_1, \ldots, \alpha_{r'}\}$ is an algebraically independent subset of R/P over K because if f is a nonzero polynomial in $K[X_1, \ldots, X_{r'}]$ such that $f(\alpha_1, \ldots, \alpha_{r'}) = 0$, then application of φ and use of the fact that φ fixes each coefficient of f yields $f(\beta_1, \ldots, \beta_{r'}) = 0$; the latter equation contradicts the algebraic independence of $\{\beta_1, \ldots, \beta_{r'}\}$. We conclude that

$$P \subseteq Q \qquad \text{implies} \qquad \text{tr. deg}(R/P) \geq \text{tr. deg}(R/Q). \tag{$*$}$$

To prove the inequality $r \geq \dim R$, let a chain of prime ideals

$$0 \subseteq P_0 \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_d$$

of R be given. We are to show that $r \geq d$. Abbreviate $K[X_1, \ldots, X_n]$ as A, so that $R = A/I$. Pull the chain of ideals of R back to a chain of ideals in A as

$$I \subseteq P_0' \subsetneqq P_1' \subsetneqq \cdots \subsetneqq P_d'. \tag{$**$}$$

Inequality $(*)$ shows that

$$\text{tr. deg}(A/P_0') \geq \text{tr. deg}(A/P_1') \geq \cdots \geq \text{tr. deg}(A/P_d'). \tag{$\dagger$}$$

Since taking $P_0' = I$ shows that $\text{tr. deg}(A/I) = \text{tr. deg}(R) = r$, every member of $(\dagger)$ is $\leq r$. It will follow from $(\dagger)$ that $r \geq d$ if we show that each inequality in $(\dagger)$ is strict, i.e., that for prime ideals P and Q in A,

$$P \subsetneqq Q \qquad \text{implies} \qquad \text{tr. deg}(A/P) > \text{tr. deg}(A/Q). \tag{$\dagger\dagger$}$$

Since $\dim R$ is the supremum of the integers d as in (∗∗) and (†), proving (††) will prove that $r \geq \dim R$.

Thus let P and Q be prime ideals in $A = K[X_1, \ldots, X_n]$ with $P \subsetneqq Q$. Put $\alpha_j = X_j + P$ and $\beta_j = X_j + Q$, so that the mappings of A to A/P and A/Q are $f(X_1, \ldots, X_n) \mapsto f(\alpha_1, \ldots, \alpha_n)$ and $f(X_1, \ldots, X_n) \mapsto f(\beta_1, \ldots, \beta_n)$. Then $A/P = K[\alpha_1, \ldots, \alpha_n]$ and $A/Q = K[\beta_1, \ldots, \beta_n]$. As above, if $r' = \text{tr. deg } A/Q$, then we may assume that $\{\beta_1, \ldots, \beta_{r'}\}$ is a transcendence basis of A/Q. Arguing by contradiction, we may assume that $\text{tr. deg } A/P = \text{tr. deg } A/Q$. Then it follows that $\{\alpha_1, \ldots, \alpha_{r'}\}$ is a transcendence basis of A/P. We localize A with respect to the multiplicative system S consisting of the complement of 0 in $K[X_1, \ldots, X_{r'}]$. Then $S^{-1}A = K(X_1, \ldots, X_{r'})[X_{r'+1}, \ldots, X_n]$. To understand $S^{-1}P$, we apply Lemma 7.21 to write

$$S^{-1}A/S^{-1}P \cong \overline{S}^{\,-1}(A/P), \tag{‡}$$

where $\overline{S}$ is the image of S in A/P. The restriction to $K[X_1, \ldots, X_{r'}]$ of the map $A \to A/P$ carries $f(X_1, \ldots, X_{r'})$ to $f(\alpha_1, \ldots, \alpha_{r'})$ and is one-one because $\{\alpha_1, \ldots, \alpha_{r'}\}$ is a transcendence set. Therefore $S \cap P = \varnothing$, and $S \to \overline{S}$ is one-one. Corollary 8.48d of *Basic Algebra* shows from $S \cap P = \varnothing$ that $S^{-1}P$ is a proper ideal of $S^{-1}A$. Since $S \to \overline{S}$ is one-one, let us view $\overline{S}$ as $\overline{S} = \{f(\alpha_1, \ldots, \alpha_{r'}) \mid f \neq 0\}$. Then

$$\overline{S}^{\,-1}(A/P) = K(\alpha_1, \ldots, \alpha_{r'})[\alpha_{r'+1}, \ldots, \alpha_n]. \tag{‡‡}$$

Since $\alpha_{r'+1}, \ldots, \alpha_n$ are algebraic over $K(\alpha_1, \ldots, \alpha_{r'})$ because of the assumption $\text{tr. deg } A/P = \text{tr. deg } A/Q = r'$, the remark with Lemma 7.3 shows that (‡‡) is a field. By (‡), $S^{-1}P$ is a maximal ideal. Arguing similarly with Q, we see that $S \cap Q = \varnothing$ and that $S^{-1}Q$ is a maximal ideal. From $P \subseteq Q$, we have $S^{-1}P \subseteq S^{-1}Q$. Because $S^{-1}P$ and $S^{-1}Q$ are maximal, $S^{-1}P = S^{-1}Q$. Therefore $Q \subseteq S^{-1}P$. Since Q properly contains P, we can choose g in Q that is not in P. This g is an element of $K[X_1, \ldots, X_n]$ such that $g(\alpha_1, \ldots, \alpha_n) \neq 0$ and $g(\beta_1, \ldots, \beta_n) = 0$. From the inclusion $Q \subseteq S^{-1}P$, there exist an f in P and a nonzero s in $K[X_1, \ldots, X_r]$ with $g = s^{-1}f$. Then $f = sg$. Since $f(\alpha_1, \ldots, \alpha_n) = 0$ and $s(\alpha_1, \ldots, \alpha_{r'})g(\alpha_1, \ldots, \alpha_n) \neq 0$, we obtain a contradiction. This contradiction proves (††) and shows that $r \geq \dim R$.

The argument that $r \leq \dim R$ will proceed by induction on r. If $r = 0$, then $R = K[x_1, \ldots, x_n]$ is a field by the remark with Lemma 7.3, and $\dim R = 0$ by Example 1 of Krull dimension. Now suppose inductively that $r > 0$ and that the inequality is known when $\text{tr. deg } R < r$. Put $A = K[X_1, \ldots, X_n]$, and suppose that $R = A/I = K[x_1, \ldots, x_n]$ with x_1 transcendental over K. We localize A with respect to the multiplicative system S consisting of the complement of 0

in $K[X_1]$. Then $S^{-1}A = K(X_1)[X_2, \ldots, X_n]$. To understand $S^{-1}I$, we apply Lemma 7.21 to write

$$S^{-1}A/S^{-1}I \cong \overline{S}^{-1}(A/I),$$

where $\overline{S}$ is the image of S in A/I. Arguing as in the previous paragraph, we see that

$$\overline{S}^{-1}(A/I) \cong K(x_1)[x_2, \ldots, x_n].$$

Combining these two isomorphisms, we see that $S^{-1}A/S^{-1}I$ has transcendence degree $r-1$ over $K(x_1)$. By the inductive hypothesis, $S^{-1}A/S^{-1}I$ has Krull dimension $\geq r-1$. Thus there exists a strictly increasing chain

$$S^{-1}I = Q_0 \subsetneqq Q_1 \subsetneqq \cdots \subsetneqq Q_{r-1}$$

of prime ideals in $S^{-1}A$. If we put $P_i = A \cap Q_i$ for each i, then each P_i is prime in A. From the theory of localization, we know that Q_i is recovered from P_i by $Q_i = S^{-1}P_i$, and thus we have a strictly increasing chain

$$I = P_0 \subsetneqq P_1 \subsetneqq \cdots \subsetneqq P_{r-1} \tag{§}$$

of prime ideals in A. The fact that P_{r-1} is proper implies that $S \cap P_{r-1} = \varnothing$. That is, no nonzero member of $K[X_1]$ lies in P_{r-1}. Consequently the image of X_1 in A/P_{r-1} is transcendental over K. The Nullstellensatz (Theorem 7.1) shows that P_{r-1} is not maximal in A. Hence the chain (§) can be extended by a strict inclusion in a maximal ideal P_r, and $r \leq \dim A/I = \dim R$. This completes the induction and the proof. □

5. Nonsingular and Singular Points

In this section we develop the initial algebraic background necessary for a discussion of nonsingular and singular points. Unlike what happened in previous sections, we shall not try to separate completely the algebra from the geometric setting, because the points to be investigated are the actual points of a zero locus.

The motivation comes from the Implicit Function Theorem in the calculus of several variables. In that setting, suppose that we have l numerical-valued smooth functions $f_1, \ldots, f_l$ of n variables. Let k be an integer with $1 < k < n$, and abbreviate $(x_1, \ldots, x_n)$ as (x, y), where $x = (x_1, \ldots, x_k)$ and $y = (x_{k+1}, \ldots, x_n)$. Suppose that (x_0, y_0) has the property that $f_i(x_0, y_0) = 0$ for $1 \leq i \leq l$. The hope is that there is a smooth vector-valued function $y = g(x)$ defined near $x = x_0$ such that $y_0 = g(x_0)$ and such that $f_i(x, y) = 0$ for $1 \leq i \leq l$ with (x, y) near (x_0, y_0) if and only if $y = g(x)$, i.e., that the locus of common zeros of $f_1, \ldots, f_l$ is locally the graph of a smooth function of k variables. According to the Implicit

Function Theorem, a sufficient condition for this to happen is that $k + l = n$ and that the (square) matrix of the first partial derivatives at (x_0, y_0) of the f_i's for $1 \le i \le l$ with respect to the y_j's for $k + 1 \le j \le n$ be invertible. A little more generally but still with $k + l = n$, the locus of common zeros is locally the graph of a smooth function of l of the variables in terms of the remaining k variables if the matrix of all the first partial derivatives of the f_i's has the maximum possible rank, namely l.

Let us describe the setting for a comparable situation in algebraic geometry. *Throughout this section we assume that K is an algebraically closed field.* Suppose that I is a prime ideal in $K[X_1, \ldots, X_n]$, and let $V(I)$ be the locus of common zeros[5] of I in K^n. The Hilbert Basis Theorem shows that I is finitely generated over K as an ideal, and we let $\{f_1, \ldots, f_l\}$ be a set of generators. Corollary 7.2 shows that I is the set of all polynomials vanishing on $V(I)$, and thus the integral domain $R = K[X_1, \ldots, X_n]/I$ may be regarded as the set of all restrictions to $V(I)$ of polynomials in the following sense: if $x = (x_1, \ldots, x_n)$ is a member of $V(I)$ and $f(X_1, \ldots, X_n)$ is in $K[X_1, \ldots, X_n]$, then every member of the coset $f + I$ has the same value at x, and it is consequently meaningful to write $f(x)$ for f in R.

From Theorem 7.22 the transcendence degree over K of the field of fractions of R equals the Krull dimension of the ring R, and these numbers are what is taken as the dimension of $V(I)$ over K. We write $\dim V(I)$ for this dimension. In this setting, a point x of $V(I)$ is called a **nonsingular point**, or **regular point**, if the matrix $\left[\frac{\partial f_i}{\partial X_j}(x)\right]$ has rank equal to $n - \dim V(I)$. Otherwise x is a **singular point**.

It is important to observe that these definitions do not depend on the choice of the set $\{f_1, \ldots, f_l\}$ of generators of I. In fact, it is enough to show that the row space of the matrix $\left[\frac{\partial f_i}{\partial X_j}(x)\right]$ is exactly the space of all row vectors

$$\left(\frac{\partial f}{\partial X_1}(x) \quad \cdots \quad \frac{\partial f}{\partial X_n}(x) \right) \qquad \text{for } f \in I,$$

since the latter space is manifestly independent of the choice of generators. To see that the displayed space equals the row space of the matrix whose rank appears in the definition of singular point, let $g_1, \ldots, g_n$ be arbitrary polynomials. Then $f = \sum_i g_i f_i$ is the most general member of I. Use of the product rule and the fact that $f_i(x) = 0$ for each i shows that $\frac{\partial f}{\partial X_j}(x) = \sum_i g_i(x) \frac{\partial f_i}{\partial X_j}(x)$. Since the g_i are arbitrary, we can arrange for $(g_1(x), \ldots, g_n(x))$ to be any given member of K^n. Thus the space of all row vectors $\left(\frac{\partial f}{\partial X_1}(x) \quad \cdots \quad \frac{\partial f}{\partial X_n}(x) \right)$ for $f \in I$ is the set of all K linear combinations of row vectors $\left(\frac{\partial f_i}{\partial X_1}(x) \quad \cdots \quad \frac{\partial f_i}{\partial X_n}(x) \right)$ for $1 \le i \le l$, as asserted.

[5] In terminology to be used in later chapters, one says that $V(I)$ is the **affine variety** corresponding to I.

EXAMPLES.

(1) **Irreducible affine curve**[6] in K^2. Suppose that $n = 2$ in the notation above and that I is nonzero and is generated by a single nonconstant polynomial $f(X, Y)$. The condition that I be prime is exactly the condition that $f(X, Y)$ be a prime polynomial. In turn, since $K[X, Y]$ is a unique factorization domain, the condition that $f(X, Y)$ be prime is exactly the condition that $f(X, Y)$ be irreducible. Let us specialize to a case for which the first partial derivatives take an especially simple form: suppose that

$$f(X, Y) = Y^2 - h(X).$$

The only possible factorization is $f(X, Y) = (Y + \sqrt{h(X)}\,)(Y - \sqrt{h(X)}\,)$, and thus $f(X, Y)$ is irreducible in $K[X, Y]$ if $h(X)$ is not the square of a member of $K[X]$. The relevant integral domain is $R = K[X, Y]/(f(X, Y))$, and we let $x = X + (f(X, Y))$ and $y = Y + (f(X, Y))$. Then x is transcendental over K, and the equation $y^2 = h(x)$ shows that y is algebraic over $K(x)$. Hence $\text{tr. deg}\, R = 1$, and the corresponding $V(I)$ has $\dim V(I) = 1$. If (x_0, y_0) is a point of $V(I)$, then the matrix of first partial derivatives is

$$\left(\frac{\partial f}{\partial X} \quad \frac{\partial f}{\partial Y}\right)_{(x_0, y_0)} = \begin{pmatrix} -h'(X) & 2Y \end{pmatrix}_{(x_0, y_0)}.$$

The rank of this matrix is ≤ 1, and nonsingularity of (x_0, y_0) means that the matrix has rank equal to 1. If the characteristic is $\neq 2$, then the condition for a singularity is that $y_0^2 = h(x_0)$, $y_0 = 0$, and $h'(x_0) = 0$ simultaneously. Hence $V(I)$ is everywhere nonsingular[7] if and only if h has no multiple roots in K.

(2) **Irreducible affine hypersurface**[8] in K^n. For general n, again suppose that I is a prime ideal generated by a single nonconstant polynomial $f(X_1, \ldots, X_n)$. The condition on f for I to be prime is that f be irreducible in $K[X_1, \ldots, X_n]$. The relevant ring is $R = K[X_1, \ldots, X_n]/(f(X_1, \ldots, X_n))$, and the image in R of a polynomial $g(X_1, \ldots, X_n)$ is 0 only if g is divisible by f, by Corollary 7.2. The polynomial f is nonconstant in some X_j, say for $j = n$. Then no nonzero polynomial $g(X_1, \ldots, X_{n-1})$ maps to 0 in R. Consequently the elements $x_i = X_i + (f(X_1, \ldots, X_n))$ have the property that $\{x_1, \ldots, x_{n-1}\}$ is a transcendence set in R. The equation $f(x_1, \ldots, x_n) = 0$ shows that x_n is algebraic over $K(X_1, \ldots, X_{n-1})$. Hence the corresponding $V(I)$ has $\dim V(I) = \text{tr. deg}\, R = n - 1$. The nonsingular points of $V(I)$ are the points of $V(I)$ for which some first partial derivative of f is nonzero.

---

[6] Some authors include irreducibility in the definition of "affine curve." This book does not.

[7] If K has characteristic 2 and if x_0 has the property that $h'(x_0) = 0$, then we can choose y_0 with $y_0^2 = h(x_0)$ because K is algebraically closed, and (x_0, y_0) will be a singular point. Hence $V(I)$ is everywhere nonsingular if and only if h has degree exactly 1.

[8] Some authors include irreducibility in the definition of "affine hypersurface." This book does not.

Theorem 7.23 (Zariski's Theorem). With K algebraically closed, let I be a prime ideal in $K[X_1, \ldots, X_n]$, let $R = K[X_1, \ldots, X_n]/I$, and let $V(I)$ be the locus of common zeros of I in K^n. If $x = (x_1, \ldots, x_n)$ is a point of $V(I)$, define $\mathfrak{m}_x$ to be the maximal ideal

$$\mathfrak{m}_x = \{f \in R \mid f(x) = 0\}$$

of R, let R_x be the localization of R with respect to $\mathfrak{m}_x$, and let M_x be the maximal ideal of R_x. Then

$$\dim_K(M_x/M_x^2) = \dim_K(\mathfrak{m}_x/\mathfrak{m}_x^2) \geq \dim V(I),$$

and x is nonsingular if and only if equality holds. The set of nonsingular points of $V(I)$ is nonempty.

REMARKS. We are going to prove for each point x of $V(I)$ that

$$\dim_K(M_x/M_x^2) = \dim_K(\mathfrak{m}_x/\mathfrak{m}_x^2)$$

and that

$$\dim_K(\mathfrak{m}_x/\mathfrak{m}_x^2) + \operatorname{rank}\left[\tfrac{\partial f_i}{\partial X_j}\right] = n,$$

where $\{f_i\}$ is a finite set of generators of I. Since by definition x is nonsingular if and only if $\operatorname{rank}\left[\tfrac{\partial f_i}{\partial X_j}\right] = n - \dim V(I)$, it will follow that x is a nonsingular point if and only if $\dim_K(\mathfrak{m}_x/\mathfrak{m}_x^2) = \dim V(I)$. Only for the special case that $V(I)$ is an irreducible affine hypersurface do we prove that the inequality $\dim_K(\mathfrak{m}_x/\mathfrak{m}_x^2) \geq \dim V(I)$ always holds for all x and that equality always holds for some x. The general case will ultimately be reduced to the special case; we return to this matter in Chapter X. The partial proof that we give in the present section will be preceded by an example.

EXAMPLE 1, CONTINUED. Suppose that an affine variety V in K^2 is obtained from the irreducible polynomial $f(X, Y) = Y^2 - h(X)$. Let us assume that K has characteristic $\neq 2$ and that $(0, 0)$ lies in V. The latter condition means that $h(0) = 0$. Let $x = X + (f(X, Y))$ and $y = Y + (f(X, Y))$. Since $y^2 = h(x)$, any polynomial in (x, y) can be rewritten in such a way that the only powers of y that occur are 0 and 1. Thus $R = \{p(x) + yq(x) \mid p \in K[x], q \in K[x]\}$, and

$$\mathfrak{m}_{(0,0)} = \big\{xp(x) + yq(x) \mid p \in K[x],\ q \in K[x]\big\}.$$

The ideal $\mathfrak{m}_{(0,0)}^2$ consists of all sums of products of two elements of this kind. From two polynomials $xp(x)$, we can get any polynomial $x^2a(x)$; from $xp(x)$

and $yq(x)$, we can get any $xyb(x)$; and from two polynomials $yq(x)$, we can get any $y^2c(x) = h(x)c(x)$. Thus

$$\mathfrak{m}_{(0,0)}^2 = \{x^2a(x) + h(x)c(x) + yxb(x)\}.$$

What happens depends on the first-degree term in $h(x)$. Examining the possibilities, we see that

$$\mathfrak{m}_{(0,0)}^2 = \begin{cases} \{xa(x) + yxb(x)\} & \text{if } h'(0) \neq 0, \\ \{x^2a(x) + yxb(x)\} & \text{if } h'(0) = 0. \end{cases}$$

Hence

$$\mathfrak{m}_{(0,0)}/\mathfrak{m}_{(0,0)}^2 \cong \begin{cases} Ky & \text{if } h'(0) \neq 0, \\ Kx + KY & \text{if } h'(0) = 0. \end{cases}$$

In other words, $\dim_K \mathfrak{m}_{(0,0)}/\mathfrak{m}_{(0,0)}^2$ equals 1 if $(0, 0)$ is nonsingular and equals 2 if $(0, 0)$ is singular. Since $\dim V(I) = 1$, this result is consistent with the statement of Theorem 7.23.

PARTIAL PROOF OF THEOREM 7.23. As mentioned in the remarks, one thing that we are going to prove for each point x of $V(I)$ is that

$$\dim_K(\mathfrak{m}_x/\mathfrak{m}_x^2) + \operatorname{rank}\left[\tfrac{\partial f_i}{\partial X_j}\right] = n, \tag{$*$}$$

where $\{f_1, \ldots, f_l\}$ is a finite set of generators of I.

Let I_x be the pullback to $K[X_1, \ldots, X_n]$ of the ideal $\mathfrak{m}_x$, i.e., let

$$I_x = \{f \mid f + I \in \mathfrak{m}_x\} = \{f \in K[X_1, \ldots, X_n] \mid f(x_1, \ldots, x_n) = 0\}.$$

The K linear mapping $f \mapsto f + I$ carries I_x onto $\mathfrak{m}_x$; composing with the quotient mapping $\mathfrak{m}_x \to \mathfrak{m}_x/\mathfrak{m}_x^2$ gives a K linear mapping φ of I_x onto $\mathfrak{m}_x/\mathfrak{m}_x^2$. If f maps under φ to the 0 coset, then $f + I = \sum_j (g_j + I)(h_j + I)$ for suitable polynomials g_j and h_j with $g_j + I$ and $h_j + I$ in $\mathfrak{m}_x$. Then $f - \sum_j g_j h_j$ lies in I, and f is exhibited as a member of $I_x^2 + I$. Conversely φ does carry I_x^2 and I to the 0 coset. Thus the kernel of φ is exactly $I_x^2 + I$, and φ descends to a K linear isomorphism $I_x/(I_x^2 + I) \cong \mathfrak{m}_x/\mathfrak{m}_x^2$. Therefore

$$\dim_K\left(I_x/(I_x^2 + I)\right) \cong \dim_K(\mathfrak{m}_x/\mathfrak{m}_x^2). \tag{$**$}$$

We define a K linear map θ of $K[X_1, \ldots, X_n]$ to the space $M_{1n}(K)$ of all n-dimensional row vectors over K by

$$\theta(f) = \left(\tfrac{\partial f}{\partial X_1}(x) \quad \cdots \quad \tfrac{\partial f}{\partial X_n}(x)\right).$$

The product rule for differentiation shows that $\theta(I_x^2) = 0$. The ideal I_x, considered as a K vector space, is spanned by I_x^2 and the various polynomials $X_j - x_j$. Since $\theta(X_j - x_j)$ is the j^{th} standard basis vector of $M_{1n}(K)$, the vectors $\theta(X_j - x_j)$ form a basis of $M_{1n}(K)$. Therefore θ descends to a K linear isomorphism $\bar{\theta} : I_x/I_x^2 \to M_{1n}(K)$.

We observed just before Examples 1 and 2 that the vector space of all row vectors $\theta(f)$ for $f \in I$ equals the row space for the matrix $\left[\frac{\partial f_i}{\partial X_j}\right]$. Hence

$$\dim_K \theta(I) = \operatorname{rank}\left[\tfrac{\partial f_i}{\partial X_j}\right].$$

Since $\theta(I) = \bar{\theta}\big((I + I_x^2)/I_x^2\big)$ and since $\bar{\theta}$ is one-one, this equality shows that

$$\dim_K \big((I + I_x^2)/I_x^2\big) = \operatorname{rank}\left[\tfrac{\partial f_i}{\partial X_j}\right]. \tag{$\dagger$}$$

Adding $(**)$ and $(\dagger)$ gives

$$\dim_K (I_x/I_x^2) = \dim_K (\mathfrak{m}_x/\mathfrak{m}_x^2) + \operatorname{rank}\left[\tfrac{\partial f_i}{\partial X_j}\right].$$

Since, as we have seen, I_x/I_x^2 is isomorphic to $M_{1n}(K)$ via $\bar{\theta}$, the left side is n, and $(*)$ is proved.

The second thing that we are going to prove now is that

$$\dim_K (\mathfrak{m}_x/\mathfrak{m}_x^2) = \dim_K (M_x/M_x^2). \tag{$\dagger\dagger$}$$

If L is the field of fractions of the integral domain R, then the localization R_x is the subring of L of all quotients g/h with g and h in R and $h(x) \neq 0$. The inclusion $\mathfrak{m}_x \subseteq M_x$ induces a K linear ring homomorphism $\varphi : \mathfrak{m}_x/\mathfrak{m}_x^2 \to M_x/M_x^2$, and $(\dagger\dagger)$ will follow if φ is shown to be one-one onto.

If g/h is given in M_x with $g \in \mathfrak{m}_x$ and with $h \in R$ having $h(x) \neq 0$, then the decomposition

$$h(x)^{-1}g = \tfrac{g}{h} + \left(\tfrac{g}{h}\right)\left(\tfrac{h(x)^{-1}h - 1}{1}\right)$$

exhibits $h(x)^{-1}g$ in $\mathfrak{m}_x$ as mapping to $g/h + M_x^2$. Therefore φ is onto.

If g in $\mathfrak{m}_x$ maps to $\sum_i \left(\frac{g_i}{h_i}\right)\left(\frac{g_i'}{h_i'}\right)$ in M_x^2, then we can clear fractions and write $hg = \sum_i g_i g_i' h_i''$ for an element h of R with $h(x) \neq 0$. Here $\sum_i g_i g_i' h_i''$ is in $\mathfrak{m}_x^2$. The set of elements f in R such that fg is in $\mathfrak{m}_x^2$ is an ideal in R that contains $\mathfrak{m}_x$ and that contains h. Since h is not in $\mathfrak{m}_x$ and since $\mathfrak{m}_x$ is maximal, this ideal in R contains $f = 1$, and it follows that g is in $\mathfrak{m}_x^2$. Consequently φ is an isomorphism, and $(\dagger\dagger)$ is proved. □

PROOF OF REMAINDER OF THEOREM 7.23 FOR IRREDUCIBLE AFFINE HYPERSURFACES. Let I be the principal ideal $(f(X_1, \dots, X_n))$, where f is irreducible. We saw in Example 2 above that $\dim V(I) = n - 1$. The matrix that appears in $(*)$ has only one row, corresponding to f, and hence it has rank 1 or rank 0. Substituting this fact into $(*)$, we see that $\dim_K(\mathfrak{m}_x/\mathfrak{m}_x^2) \geq n - 1 = \dim V(I)$.

Arguing by contradiction, suppose that strict inequality holds for every x in $V(I)$. Then $\frac{\partial f}{\partial X_j}(x) = 0$ for all $x \in V(I)$ and for all j. By Corollary 7.2, each $\frac{\partial f}{\partial X_j}$ is the product of f and a polynomial. Since the degree of $\frac{\partial f}{\partial X_j}$ in X_j is less than the degree of f in X_j, it follows that $\frac{\partial f}{\partial X_j} = 0$ for all j. In characteristic 0, this condition forces f to be constant and contradicts the assumption that f is an irreducible polynomial (and in particular the assumption that f is not a unit). In characteristic p, this condition forces each power of each X_j that occurs in f to be a multiple of p. That is, it says that $f(X_1, \dots, X_n) = g(X_1^p, \dots, X_n^p)$. Let $\mathrm{Fr} : K \to K$ be the field map given by $a \mapsto a^p$. This is onto K, since K is algebraically closed. Hence there exists a polynomial $h(X_1, \dots, X_n)$ such that $h^{\mathrm{Fr}} = g$. Then $f(X_1, \dots, X_n) = g(X_1^p, \dots, X_n^p) = \big(h(X_1, \dots, X_n)\big)^p$ exhibits f as reducible, contradiction. Hence strict inequality cannot hold for all $x \in V(I)$, and some point of $V(I)$ is nonsingular. □

6. Infinite Galois Groups

In this section, K denotes a field, and K_{alg} denotes a fixed algebraic closure of K. We define K_{sep} to be the subfield of all elements of K_{alg} that are separable over K. The field K_{sep} is called a **separable algebraic closure** of K. Theorem 7.13 shows that K_{alg} is a purely inseparable extension of K_{sep}. If F_1 and F_2 are any fields with $F_1 \subseteq F_2$, then the group of all field automorphisms of F_2 fixing F_1 is denoted by $\mathrm{Gal}(F_2/F_1)$ and is called the **Galois group** of F_2 over F_1.

The purpose of this section is to extend the theory of Galois groups to handle infinite extensions. Such an extended theory has at least two important applications in the current context. A first application is to developments in algebraic number theory beyond what appears in Chapters V and VI. For example one way of viewing traditional class field theory for a number field F is that one forms $\mathrm{Gal}(F_{\mathrm{alg}}/F)$, defines the maximal abelian extension F_{ab} of F to be the fixed field of the closure of the commutator subgroup of $\mathrm{Gal}(F_{\mathrm{alg}}/F)$, and asks for a description of F_{ab} in terms of F. A second application is to the study of varieties over fields that are not algebraically closed. If a field K is given and a prime ideal I in $K_{\mathrm{alg}}[X_1, \dots, X_n]$ is specified by giving a finite set of generators, we can ask whether the same ideal can be defined via generators that lie in K. The given generators have coefficients in K_{alg}, and it is usually not obvious whether they

can be adjusted to have coefficients in K. However, if Galois theory is available, then the question becomes whether the operation of each element of the Galois group $\mathrm{Gal}(K_{\mathrm{alg}}/K)$ carries each generator into a member of the ideal,[9] and this question is decidable by methods to be discussed in Chapter VIII. More generally algebraic geometry from before 1960 frequently worked with a field K and an algebraically closed field L that is larger than K_{alg}, for example with $K = \mathbb{Q}$ and $L = \mathbb{C}$. Under the assumption that K is perfect and L is algebraically closed, Theorem 7.34 below shows that $\mathrm{Gal}(L/K)$ fixes only the elements of K, and thus Galois theory can still be used to decide in this situation whether a prime ideal in $L[X_1, \dots, X_n]$ is generated by members of $K[X_1, \dots, X_n]$.

The definition of "normal field extension" in *Basic Algebra* was limited to finite algebraic extensions, and the extensions were often assumed to be separable. We now drop both the finiteness assumption and the separability assumption: A field L with $K \subseteq L \subseteq K_{\mathrm{alg}}$ is said to be a **normal extension** of K if there exists some nonempty family $\{f_i\}_{i\in S}$ of nonconstant polynomials in $K[X]$ such that L is generated by K and all the roots in K_{alg} of all the polynomials f_i. More specifically all the polynomials f_i split in K_{alg}, say as $f_i(X) = c_i \prod_{j=1}^{d(i)} (X - \alpha_{ij})$, and L is to be the subfield of K_{alg} generated by K and all the roots α_{ij}.

Proposition 7.24. The following conditions on a field L with $K \subseteq L \subseteq K_{\mathrm{alg}}$ are equivalent:

(a) L is a normal extension of K,
(b) $\mathrm{Gal}(K_{\mathrm{alg}}/K)$ carries L to itself,
(c) any K isomorphism of L into K_{alg} carries L to itself,
(d) any polynomial f in $K[X]$ that is irreducible over K and has one root in L necessarily splits in L.

PROOF. If (a) holds, let L be generated by K and elements α_{ij} as in the paragraph before the proposition. If φ is in $\mathrm{Gal}(K_{\mathrm{alg}}/K)$, then $\varphi(\alpha_{ij})$ is a root of $f_i^{\varphi} = f_i$ because f_i has coefficients in K. Hence α_{ij} equals some $\alpha_{ij'}$. Thus φ permutes the generators of L over K, and $\varphi(L) = L$. Therefore (b) holds.

If (b) holds, then any K field map of L into K_{alg} extends to a K automorphism of K_{alg}, by Theorem 9.23 of *Basic Algebra*. By (b), the extended mapping carries L into itself. Thus (c) holds.

If (c) holds, let f in $K[X]$ be irreducible over K, and suppose that x_0 is a root of f in L. Let x_1 be another root of f in K_{alg}. By the uniqueness of simple extensions, we know that there exists a K isomorphism $\varphi_0 : K(x_0) \to K(x_1) \subseteq K_{\mathrm{alg}}$, and we can regard φ_0 as a K field map of $K(x_0)$ into K_{alg}. The map φ_0 extends to a K field automorphism of K_{alg}, and we restrict the extension

[9] This condition is always necessary. For it to be sufficient, one has to show that the only members of K_{alg} fixed by all elements of $\mathrm{Gal}(K_{\mathrm{alg}}/K)$ are the members of K.

to a map $\varphi : L \to K_{\text{alg}}$. By (c), $\varphi(L) \subseteq L$. Since $K(x_0) \subseteq L$, we obtain $K(x_1) = \varphi(K(x_0)) \subseteq \varphi(L) \subseteq L$. Thus x_1 is in L, and (d) holds.

If (d) holds, then for each element x_i of L, let f_i be the minimal polynomial of x_i over K. Certainly the field L is generated by K and the elements x_i. By (d), each f_i splits in L. Therefore L is generated over K by all the roots of the polynomials f_i and is normal. Thus (a) holds. □

Proposition 7.25. Every member of $\text{Gal}(K_{\text{alg}}/K)$ carries K_{sep} into itself, any two members of $\text{Gal}(K_{\text{alg}}/K)$ that agree on K_{sep} are equal on K_{alg}, and any field map of K_{sep} into K_{alg} extends to an automorphism of K_{alg}. Consequently the operation of restriction from K_{alg} to K_{sep} defines an isomorphism

$$\text{Gal}(K_{\text{alg}}/K) \cong \text{Gal}(K_{\text{sep}}/K).$$

PROOF. The first statement has three conclusions to it. For the first conclusion, if φ is in $\text{Gal}(K_{\text{alg}}/K)$ and if x_0 is in K_{sep}, let f be the minimal polynomial of x_0 over K. By separability, f is a separable polynomial over K. Since φ fixes f, φ carries x_0 to some root x_1 of f, and hence f is the minimal polynomial of x_1 over K. Since f is a separable polynomial over K, x_1 is separable over K and lies in K_{sep}.

For the second conclusion, let φ be a member of $\text{Gal}(K_{\text{alg}}/K)$ that is 1 on K_{sep}. If x is in K_{alg}, then the pure inseparability of $K_{\text{alg}}/K_{\text{sep}}$ implies that $x^{p^e} = a$ for some $a \in K_{\text{sep}}$ and some integer $e \geq 0$. The element x has $(X - x)^{p^e} = X^{p^e} - x^{p^e} = X^{p^e} - a$ and hence is the unique root of $X^{p^e} - a$. Since $\varphi(x)$ has to be a root of this polynomial, $\varphi(x) = x$.

The third conclusion is a special case of the extendability to all of K_{alg} of any field mapping of a subfield of K_{alg} into K_{alg}.

The displayed isomorphism follows: the first conclusion shows that restriction carries $\text{Gal}(K_{\text{alg}}/K)$ into $\text{Gal}(K_{\text{sep}}/K)$, the second conclusion shows that restriction is one-one, and the third conclusion shows that restriction is onto. □

Corollary 7.26. Let L be a field with $K \subseteq L \subseteq K_{\text{sep}}$, form $\text{Gal}(L/K)$, and let $L^{\text{Gal}(L/K)}$ be the fixed field

$$L^{\text{Gal}(L/K)} = \{x \in L \mid \gamma x = x \text{ for all } x \in \text{Gal}(L/K)\}.$$

Then L is normal over K if and only if $L^{\text{Gal}(L/K)} = K$.

PROOF. Let L be normal over K, let x be in $L^{\text{Gal}(L/K)}$, and let f be the minimal polynomial of x over K. Since L is normal, f splits in L. Since $L \subseteq K_{\text{sep}}$, the roots of f in L all have multiplicity one. Arguing by contradiction, suppose that x is not in K. Then $\deg f > 1$, and f has another root x_1 besides x.

Hence we can find a K isomorphism $\varphi : K(x) \to K(x_1)$ with $\varphi(x) = x_1$. The mapping φ extends to a field automorphism of K_{alg}, and Proposition 7.24 shows that $\varphi(L) = L$, since L is normal. Thus φ defines by restriction a member of $\text{Gal}(L/K)$. Since $\varphi(x) = x_1$, we have a contradiction to the assumption that x is in $L^{\text{Gal}(L/K)} = K$.

Conversely let $L^{\text{Gal}(L/K)} = K$. Let x be in L, and let f be its minimal polynomial over K. Let $x_1 = x$ and $x_2, \dots, x_r$ be the distinct images of x in L under members of $\text{Gal}(L/K)$. These are all roots of f, and the roots of f have multiplicity 1 because x lies in K_{sep}. Each member of $\text{Gal}(L/K)$ permutes $x_1, \dots, x_r$ and hence acts via a permutation in the symmetric group $\mathfrak{S}_r$. Put $g(X) = \prod_{i=1}^{r} (X - x_i)$. Expanding g gives

$$g(X) = X^r - \Big(\sum_i x_i\Big)X^{r-1} + \Big(\sum_{i<j} x_i x_j\Big)X^{r-2} - \cdots \pm \Big(\prod_i x_i\Big).$$

Each permutation of $\{x_1, \dots, x_r\}$ fixes the coefficients of $g(X)$, which are members of L, and hence the coefficients are in $L^{\text{Gal}(L/K)} = K$. Therefore $g(X)$ is in $K[X]$. Since $g(x) = 0$, $f(X)$ divides $g(X)$. Over L, $g(X)$ splits. By unique factorization in $L[X]$, $f(X)$ must split, too. By Proposition 7.24, L is normal over K. □

To obtain a version of the Fundamental Theorem of Galois Theory in the present context, it is necessary to introduce a topology on each Galois group. An example will illustrate.

EXAMPLE. Let K be the finite field $\mathbb{F}_q$, where $q = p^r$ for a prime p. If L_n is a finite extension of K of degree n, then Proposition 9.40 of *Basic Algebra* shows that $\text{Gal}(L_n/K)$ is cyclic of order n, a generator being the **Frobenius element** Fr_q defined by $\text{Fr}_q(x) = x^q$. The thing about the Frobenius element is that it really makes sense on all L_n's simultaneously. We know (from Proposition 7.15 for example) that every algebraic extension of K is separable, and hence $K_{\text{sep}} = K_{\text{alg}}$. Here we can view K_{sep} as an aligned union of the fields L_n for $n \geq 1$, and Fr_q really makes sense as a member of $\text{Gal}(K_{\text{sep}}/K)$ under the same definition: $\text{Fr}_q(x) = x^q$. On each L_n, some nonzero power of Fr_q is the identity, but this is no longer true on the infinite field K_{sep}. Thus the mapping $1 \mapsto \text{Fr}_q$ extends to a one-one homomorphism of $\mathbb{Z}$ into $\text{Gal}(K_{\text{sep}}/K)$. However, it is not onto. Any element γ of $\text{Gal}(K_{\text{sep}}/K)$ has the property that for each n, there is a unique integer k_n with $0 \leq k_n < n$ such that $\gamma\big|_{L_n} = \text{Fr}_q^{k_n}$, and the sequence $\{k_n\}$ determines γ; nevertheless Problem 3 at the end of the chapter shows that the sequence need not ultimately be constant, and therefore γ need not be in the image of $\mathbb{Z}$. The Galois group $\text{Gal}(K_{\text{sep}}/K)$ is instead a certain topological completion of $\mathbb{Z}$ that is usually denoted by $\widehat{\mathbb{Z}}$. Taking the topology into account

will be essential to extending the Fundamental Theorem of Galois Theory, since $\mathbb{Z}$ and $\widehat{\mathbb{Z}}$ are distinct subgroups of $\mathrm{Gal}(K_{\mathrm{sep}}/K)$ that have the same fixed field, namely K itself.

If L is a normal extension of K with $L \subseteq K_{\mathrm{sep}}$, we shall introduce a topology on $\mathrm{Gal}(L/K)$ to make "close" mean "equal on a large finite-dimensional subspace." With this intuition as a guide, we could define a basic neighborhood of an element γ_0 of $\mathrm{Gal}(L/K)$ by taking finitely many elements $\alpha_1, \dots, \alpha_n$ in K and forming

$$\{\gamma \in \mathrm{Gal}(L/K) \mid \gamma\alpha_i = \gamma_0\alpha_i \text{ for } 1 \le i \le n\}.$$

It is more useful, however, to define the topology in another way, and then it will turn out that we indeed would have obtained a neighborhood basis by the above definition. In any event, the topology turns out to be compact Hausdorff and to make $\mathrm{Gal}(L/K)$ into a topological group.

The method we use will be to define the topology as an "inverse limit." Inverse limit is a general notion in category theory defined by a universal mapping property. As usual it consists of an object and a morphism; it need not exist in a general category, but when it does exist, it is unique up to canonical isomorphism. For the category of interest, the objects are the compact (Hausdorff) topological groups, and the morphisms are continuous group homomorphisms. If we wanted to emphasize the category-theory aspects of the construction, we would also need products of this category with itself, but we shall not belabor this point.

Let I be a **directed set**, i.e., a nonempty partially ordered set under an ordering $\le$ such that for any a and b in I, there is an element c in I with $a \le c$ and $b \le c$. We allow ourselves to write $b \ge a$ in place of $a \le b$ whenever convenient. Two examples of directed sets of particular interest both have $I = \{1, 2, 3, \dots\}$; in one case the ordering is given by $a \le b$ if a divides b, and in the other case the ordering is given by the usual notion of inequality.

An **inverse system** $(I, \{G_i\}, \{f_{ij}\})$ in the category of compact topological groups consists of a directed set I, a system of compact topological groups G_i, one for each $i \in I$, and a system of continuous homomorphisms $f_{ij} : G_j \to G_i$, defined whenever i and j are in I with $i \le j$, such that

- $f_{ii} = 1$ for all $i \in I$,
- $f_{ij} \circ f_{jk} = f_{ik}$ whenever $i \le j \le k$.

EXAMPLES.

(1) Let $I = \{1, 2, 3, \dots\}$ with $a \le b$ meaning that a divides b. Let G_a be the cyclic group $\mathbb{Z}/a\mathbb{Z}$ of order a. Define $f_{ab} : G_b \to G_a$ to be the homomorphism such that $f_{ab}(1 + b\mathbb{Z}) = 1 + a\mathbb{Z}$.

(2) Let $I = \{1, 2, 3, \dots\}$ with the usual ordering. Fix a prime number p, and define G_a to be the cyclic group $\mathbb{Z}/p^a\mathbb{Z}$ of order p^a. Define $f_{ab} : G_b \to G_a$ to be the homomorphism such that $f_{ab}(1 + p^b\mathbb{Z}) = 1 + p^a\mathbb{Z}$.

An **inverse limit** $(G, \{f_i\}_{i\in I})$ of the inverse system $(I, \{G_i\}, \{f_{ij}\})$, often written $G = \varprojlim G_i$ and sometimes also called the **projective limit**, consists of a compact topological group G and continuous homomorphisms $f_i : G \to G_i$ such that

(i) $f_{ij} \circ f_j = f_i$ whenever $i \le j$,

(ii) whenever $(G', \{f_i'\}_{i\in I})$ is a pair consisting of a compact topological group G' and continuous homomorphisms $f_i' : G' \to G_i$ such that $i \le j$ implies $f_{ij} \circ f_j' = f_i'$, then there exists a unique continuous homomorphism $F : G' \to G$ such that $f_i \circ F = f_i'$ for all i.

In the two examples the inverse limit group in the first case is $\widehat{Z}$; in the second case the inverse limit is isomorphic to the additive group $\mathbb{Z}_p$ of p-adic integers. In the first case we omit a description of the homomorphisms $f_a : \widehat{\mathbb{Z}} \to \mathbb{Z}/a\mathbb{Z}$. In the second case the homomorphisms f_a are easy to describe: $f_a : \mathbb{Z}_p \to \mathbb{Z}/p^a\mathbb{Z}$ is given by the composition of the quotient homomorphism $\mathbb{Z}_p \to \mathbb{Z}_p/p^a\mathbb{Z}_p$ and the isomorphism $\mathbb{Z}_p/p^a\mathbb{Z}_p \to \mathbb{Z}/p^a\mathbb{Z}$ asserted by Theorem 6.26e.

Proposition 7.27. In the category of compact topological groups, an inverse system $(I, \{G_i\}, \{f_{ij}\})$ has at least one inverse limit, namely $(G, \{f_i\}_{i\in I})$ with

$$G = \Big\{(g_i)_{i\in I} \in \prod_{i\in I} G_i \;\Big|\; f_{ij}(g_j) = g_i \text{ whenever } i \le j\Big\},$$

$$f_i = \text{restriction to } G \text{ of the } i^{\text{th}} \text{ projection } \prod_j G_j \to G_i.$$

REMARKS. It is to be understood from the statement that G gets the relative topology from $\prod_{i\in I} G_i$. We refer to this $(G, \{f_i\}_{i\in I})$ as the **standard inverse limit** of $(I, \{G_i\}, \{f_{ij}\})$.

PROOF. If $(g_i)_{i\in I}$ and $(g_i')_{i\in I}$ are in G, then the fact that each f_{ij} is a homomorphism implies that $f_{ij}(g_j g_j') = g_i g_i'$ and that $f_{ij}(g_j^{-1}) = g_i^{-1}$. Therefore $(g_i g_i')_{i\in I}$ and $(g_i^{-1})_{i\in I}$ are in G, and G is a group. The subset of $G_i \times G_j$ with $f_{ij}(x_j) = x_i$ is topologically closed, and it follows that G is the intersection of closed sets and hence is closed. Since $\prod_{j\in I} G_j$ is compact Hausdorff, G is compact Hausdorff. The continuity of the multiplication and inversion is a consequence of those properties for $\prod_{j\in I} G_j$. The i^{th} projection of $\prod_{j\in I} G_j$ onto G_i is a continuous homomorphism, and hence so is the restriction of this projection to G.

Condition (i) in the definition of inverse limit is immediate, and we have to prove (ii). Let $(G', \{f_i'\}_{i\in I})$ be given with each $f_i' : G' \to G_i$ having the property that $i \le j$ implies $f_{ij} \circ f_j' = f_i'$. For each g' in G', the I-tuple $(f_i'(g'))_{i\in I}$ is a member of $\prod_i G_i$, and the map $g' \mapsto (f_i'(g'))_{i\in I}$ is continuous into the product topology because each entry is continuous. If $i \le j$, then

the tuple $(f_i'(g'))_{i\in I}$ has the property that $f_{ij}(f_j'(g')) = f_i'(g')$ because of the given compatibility condition for the f_i''s. Therefore the map F given by $g' \mapsto (f_i'(g'))_{i\in I}$ has its image in the subset G of $\prod_i G_i$, and it is evidently a continuous group homomorphism. The map F proves the existence assertion in (ii) because $f_i \circ F(g') = f_i\big((f_j'(g'))_{j\in I}\big) = f_i'(g')$.

For uniqueness, suppose that $H : G' \to G$ is a continuous homomorphism such that $f_i \circ H = f_i'$ for all i. For each $g' \in G'$, we have $f_i(H(g')) = f_i'(g')$. Thus $H(g')$ is the member $(g_i)_{i\in I}$ of $\prod_{i\in I} G_i$ for which $g_i = f_i'(g')$ for all i. Hence H is uniquely determined. □

Proposition 7.28. In the category of compact topological groups, any two inverse limits for an inverse system $(I, \{G_i\}, \{f_{ij}\})$ are canonically isomorphic.

PROOF. This is a special case of the uniqueness in category theory of objects having a specific universal mapping property, as established in *Basic Algebra*. □

It is important in applications that the inverse limit of an inverse system of compact groups depend only on what happens far out in the directed set. We have not yet used that the indexing set is a directed set, rather than merely a partially ordered set, and we shall use this property now.

Corollary 7.29. Let I be a directed set, let j_0 be in I, and let I' be the set of members of I that are $\geq j_0$. If $(I, \{G_i\}, \{f_{ij}\})$ is an inverse system of compact groups, then the two inverse systems $(I, \{G_i\}, \{f_{ij}\})$ and $(I', \{G_i\}, \{f_{ij}\})$ have canonically isomorphic inverse limits, the isomorphism of the standard inverse limit $G \subseteq \prod_{i\in I} G_i$ onto the standard inverse limit $G' \subseteq \prod_{i\geq j_0} G_i$ being given by projection to the coordinates $\geq j_0$.

PROOF. Let $P : G \to G'$ be the projection, and let $f_i' : G' \to G_i$ for $i \geq j_0$ be the associated maps. Certainly $f_i' \circ P = f_i$ for $i \geq j_0$. We shall extend the definition of f_i' to apply to all $i \in I$. If $i \in I$ is given, we use the fact that I is directed to choose i' with $i' \geq i$ and $i' \geq j_0$. Define $f_i' = f_{ii'} \circ f_{i'}'$. Let us see that f_i' is well defined. Let i'' have $i'' \geq i$ and $i'' \geq j_0$. Choose i''' with $i''' \geq i'$ and $i''' \geq i''$. The computation

$$f_{ii'''} \circ f_{i'''}' = f_{ii'} \circ f_{i'i'''} \circ f_{i'''}' = f_{ii'} \circ f_{i'}'$$

shows that i' and i''' yield the same definition of f_i', and a similar argument shows that i'' and i''' yield the same definition. Therefore i' and i'' yield the same definition. Thus f_i' is now defined for all i in I.

We shall show that $(G', \{f_i'\}_{i\in I})$ is an inverse limit of $(I, \{G_i\}, \{f_{ij}\})$, and then the corollary follows from Proposition 7.28. Property (i) of inverse limits is built into the definition of the homomorphisms f_i'. For property (ii) of G', suppose that

$(\widetilde{G}, \{\widetilde{f_i}\}_{i\in I})$ is a pair consisting of a compact topological group $\widetilde{G}$ and continuous homomorphisms $\widetilde{f_i} : \widetilde{G} \to G_i$ such that $i \le j$ implies $f_{ij} \circ \widetilde{f_j} = \widetilde{f_i}$. By (ii) for existence with G, find a continuous homomorphism $F : \widetilde{G} \to G$ with $f_i \circ F = \widetilde{f_i}$ for all i. Substituting from $f_i' \circ P = f_i$, we obtain $f_i' \circ (P \circ F) = \widetilde{f_i}$, and this says that $P \circ F : \widetilde{G} \to G'$ is the map we seek for the existence in (ii) for G'. For uniqueness in (ii), suppose that $F' : \widetilde{G} \to G'$ satisfies $f_i' \circ F' = \widetilde{f_i}$ for all i. Then $f_i' \circ F' = f_i' \circ (P \circ F)$ for $i \ge j_0$. By (ii) for uniqueness with G', $F' = P \circ F$. This says that the map from $\widetilde{G}$ to G' in (ii) is unique. □

Let us now apply these considerations to topologize Galois groups of infinite separable normal algebraic extensions. The topologized Galois group will be the inverse limit of finite Galois groups, each with the discrete topology.[10]

We return to our field K, its algebraic closure K_{alg}, and its separable algebraic closure K_{sep} within K_{alg}. Let L be a field with $K \subseteq L \subseteq K_{\text{sep}}$, and assume that L/K is a normal extension, not necessarily finite. We shall topologize $\text{Gal}(L/K)$. Let x be any element of L, and let F be the finite extension $F = K(x)$ of K. If f is the minimal polynomial of x over K, then f has a root in L and must split in L because L/K is normal. Let $x_1, \dots, x_n$ be the roots of f, with $x_1 = x$. Then $E = K(x_1, \dots, x_n)$ is a finite normal extension of K with $K \subseteq F \subseteq E \subseteq L$. Since x is arbitrary in L, L is the union of all the finite normal extensions of K lying within L.

For each pair (E, E') of normal extensions of K with $K \subseteq E \subseteq E' \subseteq L$, Proposition 7.24 gives us restriction homomorphisms $\varphi_{EE'} : \text{Gal}(E'/K) \to \text{Gal}(E/K)$. We write φ_E for the special case that $E' = L$, so that $\varphi_{EL} = \varphi_E$. If $K \subseteq E \subseteq E' \subseteq E'' \subseteq L$, then $\varphi_{EE'} \circ \varphi_{E'E''} = \varphi_{EE''}$, and consequently the system

$$\left(\left\{ \begin{matrix} E \text{ finite normal} \\ \text{extension of } K \\ \text{in } L \end{matrix} \right\}, \{\text{Gal}(E/K)\}, \{\varphi_{EE'}\} \right)$$

is an inverse system of (discrete finite) topological groups. Meanwhile, we can form the group $\text{Gal}(L/K)$ and the system $\{\varphi_E\}$ of homomorphisms with $\varphi_E = \varphi_{EL}$.

Proposition 7.30. With the above notation, the group $\text{Gal}(L/K)$ may be identified with the underlying abstract group of the inverse limit $\varprojlim_{L \leftarrow E} \text{Gal}(E/K)$, taken over finite normal extensions E/K with $E \subseteq L$, in such a way that the homomorphisms φ_E become the homomorphisms of the inverse limit.

[10]The inverse limit of a finite group is called a **profinite group**. Profinite groups have special properties by comparison with general compact groups, but it will not be necessary for us to undertake a study of them.

PROOF. Let $G = \varprojlim_{L \leftarrow E} \mathrm{Gal}(E/K)$, put $G_E = \mathrm{Gal}(E/K)$, and regard G as the standard inverse limit given as in Proposition 7.27:

$$G = \big\{(\gamma_E)_E \in \textstyle\prod_E G_E \;\big|\; \varphi_{EE'}(\gamma_{E'}) = \gamma_E \text{ whenever } E \subseteq E'\big\}.$$

For each E, we have a homomorphism $\varphi_E : \mathrm{Gal}(L/K) \to G_E$, and the product of the values of these defines a homomorphism $\Phi : \mathrm{Gal}(L/K) \to \prod_E G_E$. The relations $\varphi_{EE'} \circ \varphi_{E'E''} = \varphi_{EE''}$ show that the image of Φ is contained in the subgroup G of $\prod_E G_E$. We shall show that $\Phi : \mathrm{Gal}(L/K) \to G$ is one-one onto.

Let us see that Φ is one-one. If $\gamma \neq 1$ is in $\mathrm{Gal}(L/K)$, then there exists $x \in K$ with $\gamma(x) \neq x$. Let E be a finite normal extension of K within L containing x. Then $\gamma\big|_E \neq 1$, and thus $\varphi_E(\gamma) \neq 1$. Hence $\Phi(\gamma) \neq 1$, and Φ is one-one.

Let us see that Φ is onto G. Let $(\gamma_E)_E \in G$ be given. For x in L, choose a finite normal E with $x \in E$ and $E \subseteq L$, and define $\gamma(x) = \gamma_E(x)$. The relations among the $\varphi_{EE'}$ show that this definition of $\gamma(x)$ is independent of the choice of E, and γ is therefore a field map of L into itself. Certainly γ fixes K, and we can construct an inverse to γ from the mappings γ_E^{-1}. Thus γ is in $\mathrm{Gal}(L/K)$. Application of Φ gives $\Phi(\gamma) = (\varphi_E(\gamma))_E = (\gamma_E)_E$, and Φ is onto. □

Using Proposition 7.30, we transfer the topology from $\varprojlim_{L \leftarrow E} \mathrm{Gal}(E/K)$ to $\mathrm{Gal}(L/K)$, and we can now regard $\mathrm{Gal}(L/K)$ as a compact topological group. For any finite normal extension F of K with $F \subseteq L$, consider the group $\mathrm{Gal}(L/F)$. The inverse-limit topology identifies $\mathrm{Gal}(L/K)$ with a subgroup of $\prod_{E \supseteq K} \mathrm{Gal}(E/K)$, the product being taken over all finite normal extensions E of K contained in L, and Corollary 7.29 allows us to identify $\mathrm{Gal}(L/K)$ with a subgroup of

$$\prod_{E \supseteq F} \mathrm{Gal}(E/K),$$

the product being taken over all finite normal extensions E of F contained in L. Under this identification $\mathrm{Gal}(L/F)$ is identified with the subgroup of elements γ of the image of $\mathrm{Gal}(L/K)$ for which $\varphi_F(\gamma) = 1$. Since φ_F is continuous, this is a closed set. In turn, this set equals the image of $\mathrm{Gal}(L/F)$ in the subset

$$\prod_{E \supseteq F} \mathrm{Gal}(E/F).$$

The latter gives the standard inverse limit topology on $\mathrm{Gal}(L/F)$. Except for some details, the conclusion is as follows.

Corollary 7.31. With the notation of Proposition 7.30, give $\mathrm{Gal}(L/K)$ the inverse-limit topology. If F is a finite normal extension of K contained in L, then $\mathrm{Gal}(L/F)$ is a closed subgroup of $\mathrm{Gal}(L/K)$, and the relative topology on $\mathrm{Gal}(L/F)$ coincides with the inverse-limit topology of $\mathrm{Gal}(L/F)$. The subgroup $\mathrm{Gal}(L/F)$ of $\mathrm{Gal}(L/K)$ is a normal subgroup of finite index in $\mathrm{Gal}(L/K)$. Being a closed subgroup of finite index, it is an open subgroup.

PROOF. We still need to prove that $\mathrm{Gal}(L/F)$ has finite index in $\mathrm{Gal}(L/K)$. Proposition 7.24 shows that the restriction to F of any member of $\mathrm{Gal}(L/K)$ is an automorphism of F. Since F is a finite extension of K, there are only finitely many possibilities for this automorphism. If two elements γ and γ' of $\mathrm{Gal}(L/K)$ restrict to the same automorphism of F, then $\gamma^{-1}\gamma'$ is a member of $\mathrm{Gal}(L/K)$ fixing F, i.e., a member of $\mathrm{Gal}(L/F)$. Thus γ' lies in the coset $\gamma\,\mathrm{Gal}(L/F)$, and we conclude that there are only finitely many cosets. Since every member of $\mathrm{Gal}(L/K)$ restricts on F to an automorphism of F, the subgroup of members of $\mathrm{Gal}(L/K)$ restricting to the identity on F is a normal subgroup. Thus $\mathrm{Gal}(L/F)$ is normal in $\mathrm{Gal}(L/K)$. □

Corollary 7.32. With the notation of Proposition 7.30, $\mathrm{Gal}(L/K)$ has a system of open normal subgroups with intersection $\{1\}$. Hence the same thing is true of any closed subgroup of T of $\mathrm{Gal}(L/K)$. Moreover, if U is any open neighborhood of 1 in T, then some open normal subgroup lies in U; consequently the open normal subgroups of T form a neighborhood base about the identity.

PROOF. The open normal subgroups in the first conclusion are the subgroups $\mathrm{Gal}(L/F)$ as in Corollary 7.31. Since every member of L lies in some finite normal extension of K within L, a member of $\mathrm{Gal}(L/K)$ cannot lie in every $\mathrm{Gal}(L/F)$ unless it is the identity on L.

Let U be an open neighborhood of 1 in the closed subgroup T of $\mathrm{Gal}(L/K)$. The set-theoretic complement U^c of U in T is a compact set, and the complements of the open normal subgroups of T are open sets whose union covers U^c, by the result of the previous paragraph. By compactness finitely many complements of open normal subgroups of T together cover U^c. The intersection of these open normal subgroups is then an open normal subgroup contained in U. □

Theorem 7.33 (Fundamental Theorem of Galois Theory). Let K be a field, and let K_{alg} be an algebraic closure, so that $K \subseteq K_{\mathrm{sep}} \subseteq K_{\mathrm{alg}}$. Let L be a normal extension of K lying in K_{sep}. Let $\mathcal{S}$ be the set of all closed subgroups of $\mathrm{Gal}(L/K)$, and let $\mathcal{F}$ be the set of all intermediate fields between K and L. Then $F \mapsto \mathrm{Gal}(L/F)$ is a one-one mapping of $\mathcal{F}$ onto $\mathcal{S}$ with inverse $S \mapsto L^S$, L^S being the fixed field within L of the group S.

PROOF. First we show that $\mathrm{Gal}(L/F)$ is closed; Corollary 7.31 shows this only when F is a *normal* extension of K. Let $\{F_\alpha\}$ be the set of all finite extensions

of K contained in F. Then $F = \bigcup_\alpha F_\alpha$, and thus $\mathrm{Gal}(L/F) = \bigcap_\alpha \mathrm{Gal}(L/F_\alpha)$. Each F_α is contained in a finite normal extension E_α of K lying in L, and hence $\mathrm{Gal}(L/F_\alpha) \supseteq \mathrm{Gal}(L/E_\alpha)$. Corollary 7.31 shows that $\mathrm{Gal}(L/E_\alpha)$ is an open subgroup of $\mathrm{Gal}(L/K)$, and hence the larger subgroup $\mathrm{Gal}(L/F_\alpha)$ is open (as a union of cosets, each of which is open). Open subgroups are closed. Thus $\mathrm{Gal}(L/F_\alpha)$ is closed, and so is $\mathrm{Gal}(L/F) = \bigcap_\alpha \mathrm{Gal}(L/F_\alpha)$.

Next if F is in $\mathcal{F}$, then the inclusion $L \supseteq F$ and the fact that L is normal over K together imply that L is normal over F. By Corollary 7.26, $F = L^{\mathrm{Gal}(L/F)}$. Hence $F \mapsto \mathrm{Gal}(L/F)$ is one-one, and $S \mapsto L^S$ is a left inverse of it.

Finally we show that $S \mapsto L^S$ is a right inverse by showing that $\mathrm{Gal}(L/L^S) = S$ for any closed subgroup S of $\mathrm{Gal}(L/K)$. Define $T = \mathrm{Gal}(L/L^S)$. Certainly $S \subseteq T$. The previous step shows that $F = L^{\mathrm{Gal}(L/F)}$ for all $F \in \mathcal{F}$. Taking $F = L^S$ gives $L^S = L^{\mathrm{Gal}(L/L^S)} = L^T$. Let V be an arbitrary open normal subgroup of T, and put $E = L^V$. The members of T/V give well-defined automorphisms of E, and

$$E^{T/V} = (L^V)^{T/V} = L^T = L^S = (L^V)^{SV/V} = E^{SV/V}. \tag{$*$}$$

The group T/V is a finite group of automorphisms of E fixing K, and Corollary 9.37 of *Basic Algebra*, when applied to the group T/V and the separable extension $E/E^{T/V}$, shows that $T/V = \mathrm{Gal}(E/E^{T/V})$. Similarly it shows that $SV/V = \mathrm{Gal}(E/E^{SV/V})$. By $(*)$, $T/V = SV/V$, i.e., $T = SV$. Corollary 7.32 shows that the open normal subgroups of T form a neighborhood base about the identity of T. From the equality $T = SV$ for arbitrary V, let us see that

$$S \text{ is dense in } T. \tag{$**$}$$

Arguing by contradiction, let g be in T but not in the closure of S. Find V small enough so that $gV^{-1} \cap S = \varnothing$. From $T = SV$, we can write $g = sv$ with $s \in S$ and $v \in V$. Then $svV^{-1} \cap S = \varnothing$, and hence $vV^{-1} \cap S = \varnothing$. This last equality is a contradiction, since the identity lies in vV^{-1}, and $(**)$ is proved. Since S is closed, it follows from $(**)$ that $S = T$. But $T = \mathrm{Gal}(L/L^S)$ by definition. Therefore $\mathrm{Gal}(L/L^S) = S$, and the proof of the theorem is complete. □

Theorem 7.34. Let K be a perfect field, and L be an algebraically closed field containing K. Then the only members of L fixed by every element of $\mathrm{Gal}(L/K)$ are the members of K.

PROOF. Proposition 7.15 shows that $K_{\mathrm{sep}} = K_{\mathrm{alg}}$, and Corollary 7.26 implies that the only members of K_{alg} fixed by $\mathrm{Gal}(K_{\mathrm{alg}}/K)$ are the members of K. Thus we are done unless L contains elements not in K_{alg}.

Let x and y be any two members of L not in K_{alg}, and let ψ be in $\mathrm{Gal}(K_{\mathrm{alg}}/K)$. The singleton sets $\{x\}$ and $\{y\}$ are transcendence sets over K_{alg}, and Lemma 7.6

shows that they can be extended to transcendence bases of L over K_{alg}. Call these transcendence bases E and F, respectively. Theorem 7.9 shows that E and F have the same cardinality. Therefore there exists a one-one function φ of E onto F such that $\varphi(x) = y$. This function φ extends uniquely to a field map Φ of $K_{\text{alg}}(E)$ onto $K_{\text{alg}}(F)$ that restricts to ψ on K_{alg}. Theorem 7.7 shows that L is an algebraic extension of $K_{\text{alg}}(E)$ and of $K_{\text{alg}}(F)$; hence L is an algebraic closure of $K_{\text{alg}}(E)$ and of $K_{\text{alg}}(F)$. The composition of Φ followed by inclusion is a field map of $K_{\text{alg}}(E)$ into L, and Theorem 9.23 of *Basic Algebra* shows that it can be extended to a field map $\widetilde{\Phi}$ of L into L. Since $\widetilde{\Phi}(L)$ is an algebraic closure of $K_{\text{alg}}(F)$, $\widetilde{\Phi}(L) = L$. Thus there exists a member $\widetilde{\Phi}$ of $\text{Gal}(L/K_{\text{alg}})$ with $\widetilde{\Phi}(x) = y$ such that $\widetilde{\Phi}\big|_{K_{\text{alg}}} = \psi$.

Taking ψ to be the identity shows that no element of L transcendental over K is fixed by $\text{Gal}(L/K)$. If an element z of K_{alg} is given that is not in K, then the first paragraph of the proof produces a member ψ of $\text{Gal}(K_{\text{alg}}/K)$ that moves z. Applying the result of the second paragraph to this ψ with x arbitrary and with $y = x$ shows that ψ extends to a member of $\text{Gal}(L/K)$ that moves z. □

7. Problems

1. Let L/K be a field extension in characteristic p. Prove that the set of elements of L that are purely inseparable over K is a subfield of L.
2. In characteristic p, let $K(\alpha)$ be an algebraic extension of a field K, and form the inclusions $K \subseteq K(\alpha^{p^e}) \subseteq K(\alpha)$, where α^{p^e} is the smallest power of α that is separable over K. Prove that the subfield of separable elements in the extension $K(\alpha)/K$ consists exactly of $K(\alpha^{p^e})$, i.e., that no separable elements of $K(\alpha)$ over K lie outside $K(\alpha^{p^e})$.
3. Partially order the positive integers by saying that $a \le b$ if a divides b. Let $(\widehat{\mathbb{Z}}, \{f_a\}_{a\ge 1})$ be the inverse limit of the cyclic groups $\mathbb{Z}/a\mathbb{Z}$, with the homomorphism f_{ab} from $\mathbb{Z}/b\mathbb{Z}$ to $\mathbb{Z}/a\mathbb{Z}$ being given by $f_{ab}(1 + b\mathbb{Z}) = 1 + a\mathbb{Z}$ when a divides b. Each member c of $\mathbb{Z}$ defines a member z_c of $\widehat{\mathbb{Z}}$ such that $f_a(z_c) = c + a\mathbb{Z}$ for all a. Exhibit some other explicit member of $\widehat{\mathbb{Z}}$.
4. Prove that the only members of $\mathbb{C}$ fixed by all members of $\text{Gal}(\mathbb{C}/\mathbb{Q})$ are the members of $\mathbb{Q}$. What members of $\mathbb{R}$ are fixed by $\text{Gal}(\mathbb{R}/\mathbb{Q})$?
5. By making use of the field $K = \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}, \sqrt{7}, \dots)$, show that there exist subgroups of $\text{Gal}(\mathbb{Q}_{\text{alg}}/\mathbb{Q})$ of index 2 that are not open.

Problems 6–14 concern primary ideals and make use of the notion of the radical $\sqrt{I}$ of an ideal I as defined in Section 1. Throughout, R will denote a commutative ring with identity. A proper ideal I of R is **primary** if whenever a and b are in R, ab is

in I, and a is not in I, then b^m is in I for some integer $m > 0$. It is immediate that every prime ideal is primary.

6. Prove that an ideal I of R is primary if and only if every zero divisor in R/I is nilpotent (in the sense that some power of it is 0), if and only if 0 is primary in R/I.

7. (a) Prove that if I is a primary ideal, then $\sqrt{I}$ is a prime ideal. (Educational note: In this case the prime ideal $\sqrt{I}$ is called the **associated prime ideal** to I.)
   (b) Prove that if I is any ideal and if $I \subseteq J$ for a prime ideal J, then $\sqrt{I} \subseteq J$.

8. (a) Show that the primary ideals in $\mathbb{Z}$ are 0 and (p^n) for p prime and $n > 0$.
   (b) Let $R = \mathbb{C}[x, y]$ and $I = (x, y^2)$. Use Problem 6 to show that I is primary. Show that $P = \sqrt{I}$ is given by $P = (x, y)$. Deduce that $P^2 \subsetneqq I \subsetneqq P$ and that a primary ideal is not necessarily a power of a prime ideal.
   (c) Let K be a field, let $R = K[X, Y, Z]/(XY - Z^2)$, and let x, y, z be the images of X, Y, Z in R. Show that $P = (x, z)$ is prime by showing that R/P is an integral domain. Show that P^2 is not primary by starting from the fact that $xy = z^2$ lies in P^2.

9. Prove that if I is an ideal such that $\sqrt{I}$ is maximal, then I is primary. Deduce that the powers of a maximal ideal are primary.

10. An ideal is **reducible** if it is the finite intersection of ideals strictly containing it; otherwise it is **irreducible**.
    (a) Show that every prime ideal is irreducible.
    (b) Let $R = \mathbb{C}[x, y]$, and let I be the maximal ideal (x, y). Show that I^2 is primary and that the equality $I^2 = (Rx + I^2) \cap (Ry + I^2)$ exhibits I^2 as reducible.

11. Prove that if R is Noetherian, then every ideal is a finite intersection of proper irreducible ideals. (The ideal R is understood to be an empty intersection.)

12. Suppose that R is Noetherian and that Q is a proper irreducible ideal in R. Prove that 0 is primary in R/Q, and deduce that Q is primary in R.

13. Prove that if $Q_1, \ldots, Q_n$ are primary ideals in R that all have $\sqrt{Q_i} = P$, then $Q = \bigcap_{i=1}^n Q_i$ is primary with $\sqrt{Q} = P$.

14. **(Lasker–Noether Decomposition Theorem)** The expression $I = \bigcap_{i=1}^n Q_i$ of an ideal I as an intersection of primary ideals Q_i is said to be **irredundant** if
    (i) no Q_i contains the intersection of the other ones, and
    (ii) the Q_i have distinct associated prime ideals.

    Prove that if R is Noetherian, then every ideal is the irredundant intersection of finitely many primary ideals.