

Advanced Algebra

Final Version, September, 2007
For Publication by Birkhäuser Boston
Along with a Companion Volume *Basic Algebra*
In the Series

Cornerstones

Selected Pages from Chapter VII: pp. 403–408

Anthony W. Knapp

Copyright © 2007 by Anthony W. Knapp
All Rights Reserved

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 $K[X_1, \dots, X_n]$ when K is a field, the Krull dimension is n . If P is a prime ideal in $K[X_1, \dots, X_n]$, then the Krull dimension of the integral domain $R = K[X_1, \dots, X_n]/P$ 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 $\text{Gal}(L/K)$.

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 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 Nullstellensatz¹ 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 \bar{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 $\bar{K}[X_1, \dots, X_n]$ are of the form

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

where (a_1, \dots, a_n) is an arbitrary member of \bar{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 \bar{K}^n is nonempty,

¹German 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 . \square

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 $\mathbb{C}[X, Y]/(Y^2 - X(X + 1)(X - 1))$.

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

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

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 $L = K[x_1, \dots, x_n]$. Since L is a field, $K(x_1) \subseteq L$, and hence $L = K(x_1)[x_2, \dots, x_n]$. By the inductive hypothesis applied to L and $K(x_1)$, the elements x_2, \dots, 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}, \dots, 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, \dots, 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 $b_m x_j \in K[x_1]$ 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 $K[x_1, \dots, x_n]$ and if l is defined as $l = \max(l_1, \dots, l_n)$, 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 $K[x_1, \dots, x_n]$, $(c_1 \cdots c_n)^l f$ is integral over $K[x_1]$ for a suitable integer $l = l(f)$. Since $K(x_1) \subseteq K[x_1, \dots, x_n]$, 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. \square

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

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

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

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

PROOF OF THEOREM 7.1. Let J be a maximal ideal in $K[X_1, \dots, X_n]$. Then $L = K[X_1, \dots, X_n]/J$ is a field. Hence $L = K[x_1, \dots, x_n]$ 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 $(X_1 - a_1, \dots, X_n - a_n)$ is contained in J . Since the ideal $(X_1 - a_1, \dots, X_n - a_n)$ is maximal, $J = (X_1 - a_1, \dots, X_n - a_n)$. 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 $K[X_1, \dots, X_n]$ and to the algebraic extension \overline{K} of K . The lemma produces a proper ideal of $\overline{K}[X_1, \dots, X_n]$

containing I , and we extend it to a maximal ideal J of $\overline{K}[X_1, \dots, X_n]$. From the previous paragraph of the proof, J is of the form $J = (X_1 - a_1, \dots, X_n - a_n)$ for some (a_1, \dots, a_n) in \overline{K}^n . The ideal J is therefore identified as the kernel of the evaluation homomorphism of $\overline{K}[X_1, \dots, X_n]$ at the point (a_1, \dots, a_n) . Every member of J thus vanishes at (a_1, \dots, 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 $K[X_1, \dots, X_n]$, and let f be as in (b). Introduce an additional indeterminate Y , and let J be the ideal in $K[X_1, \dots, X_n, Y]$ generated by I and $fY - 1$. If some point (x_1, \dots, x_n, y) lies on the locus of common zeros of J in \overline{K}^{n+1} , then (x_1, \dots, x_n) lies on the locus of common zeros of I in \overline{K}^n , since $I \subseteq J$; thus $f(x_1, \dots, x_n) = 0$, since f is assumed to vanish on all common zeros of I in \overline{K}^n . Consequently $f(x_1, \dots, x_n)y - 1 = -1 \neq 0$, and we find that $f(X_1, \dots, X_n)Y - 1$ does not vanish on the locus of common zeros of J in \overline{K}^{n+1} , contradiction. We conclude that no point (x_1, \dots, x_n, y) lies on the locus of common zeros of J in \overline{K}^{n+1} . By (a), we see that

$$J = K[X_1, \dots, X_n, Y]. \quad (*)$$

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

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

for some g_1, \dots, g_r in I and some p_1, \dots, 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

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

since $\psi(f(X)Y - 1) = 0$. 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

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

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. \square

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