A Brief Introduction to Algebraic Geometry

- Preliminary Version # 4 - Parts I, II & III -

R.C. Churchill

September, 2007

Prepared for the

Kolchin Seminar on Differential Algebra

Department of Mathematics
Graduate Center, CUNY
August and September, 2007

Algebraic geometry is fairly easy to describe from the classical viewpoint: it is the study of algebraic sets (defined in §2) and regular mappings (also defined in §2) between such sets. Unfortunately, many contemporary treatments can be so abstract (prime spectra of rings, structure sheaves, schemes, étale cohomology, etc.) that one can quickly lose sight of (and interest in) the forest while becoming mired in the technical quicksand surrounding the trees. It is hoped that these lectures will assist students in untangling the morass. However, one is never going to learn a thriving mathematical discipline simply by reading a few pages.

A bit of category theory is used, but hardly anything beyond the definition of “category” and “functor.” Once one becomes comfortable with that language it is relatively easy to understand, by analogy with already familiar mathematical topics, what algebraic geometry is all about, and what questions one should ask.

A cautionary note: One can do classical algebraic geometry locally (on the “affine” level, i.e., within vector spaces), or projectively (i.e., within projective spaces). In these notes we only work locally, whereas many of the most elegant results in the subject are at the projective level.
Contents

Part I - Basics

§1. Motivation: Fermat’s Last Theorem as a Geometry Problem
§2. Classical Affine Algebraic Geometry
§3. The Ring-Theoretic Approach
§4. The Topological Approach
§5. The Contemporary Combined Approach
§6. A Generalization of Affine Algebraic Sets

Part II - Topological Considerations

§7. Zariski Closures
   The Case of Affine Algebraic Sets
   The Case of the Prime Spectrum of a Ring
§8. Irreducible Spaces
§9. Noetherian Spaces
§10. An Algebraic Interlude - Maximal Ideals
§11. Closed Points
§12. An Application of the Prime Spectrum - The Infinitude of Primes
§13. Specializations and Generic Points
§14. The Compactness of Spec(\(R\))

Part III - Algebraic Considerations

§15. The Weak Nullstellensatz
§16. The Nullstellensatz
§17. Applications to the Mapping \(\varphi : \mathcal{V} \to \text{Spec}(K_K[\mathcal{V}])\)

Notes and Comments
References
Part I - Basics

In Part I we describe the subject matter of Algebraic Geometry, introduce the basic ring-theoretic and topological methods of the discipline, and then indicate how and why these two methods were combined midway through the past century.

1. Motivation: Fermat’s Last Theorem as a Geometry Problem

Fermat’s Last Theorem, which dates from the 1630s, is:

The equation $x^n + y^n = z^n$ has no solution in non-zero integers for any integer $n \geq 3$.

In other words, there are no integers $a, b, c$ satisfying both $a^n + b^n = c^n$ and $abc \neq 0$ when the exponent $n$ is an integer greater than 2. Despite the name the problem was treated historically as a conjecture rather than as a theorem: Fermat never communicated a proof, and for 360 years no one else was able to produce a proof except in special cases, e.g., Fermat did successfully handle the case $n = 4$, and Lagrange completed a proof formulated by Euler for $n = 3$. The general result was finally established in 1995 by Andrew Wiles, of Princeton University, with help from his former student Richard Taylor ([W, W-T]). We are not going to pursue Wiles’ solution: our only interest in the theorem is to illustrate how algebraic sets arise in mathematical pursuits. It seems a reasonable candidate for this purpose since practically anyone with a mathematical inclination has given the theorem some thought.

It has been long known that it suffices to prove Fermat’s Last Theorem when $n \geq 3$ is a prime number. To see this suppose $n \geq 3$ and that $a, b, c$ are non-zero integers satisfying $a^n + b^n = c^n$. First consider the case when $n$ is multiple of 4, say $n = 4\ell$ for some integer $\ell$. Under this assumption we see from from

$$(c^\ell)^4 = c^{4\ell} = c^n = a^n + b^n = (a^\ell)^4 + (b^\ell)^4$$

that $a^\ell, b^\ell, c^\ell$ would be a solution of $x^4 + y^4 = z^4$ in non-zero integers, and this contradicts Fermat’s result for $n = 4$.

\footnote{Success was first reported in 1993; full details were first published in 1995.}
Conversely, suppose the Fermat curve contains a rational point (non-zero integer solutions for any integer arguments of this and the previous paragraph show that if one can show that the ideas in greater generality to avoid later digressions.

There are various ways to reformulate Fermat’s theorem geometrically. We develop the number-theoretic connection with the Fermat surface is as follows. If the Fermat surface contains the non-trivial integer point \((a, b, c)\), the curve contains the “rational point” \((\frac{a}{c}, \frac{b}{c})\) in \(\mathbb{Q}^2\) with \(\frac{a}{c} \neq 0 \neq \frac{b}{c}\). Indeed, \(a^p + b^p = c^p\) and \(abc \neq 0\) certainly imply \((\frac{a}{c})^p + (\frac{b}{c})^p = 1\). Conversely, suppose the Fermat curve contains a rational point \((\frac{a}{c}, \frac{b}{d})\) in \(\mathbb{Q}^2\) with \(\frac{a}{c} \neq 0 \neq \frac{b}{d}\), where w.l.o.g. the integer pairs \(a, c\) and \(b, d\) are relatively prime. Then \(a^p \cdot b^p + b^p \cdot c^p = c^p \cdot d^p\), hence \(c^p(d^p - b^p) = a^p \cdot d^p\), and from the unique factorization of

\[ (c^n)^p = c^{mp} = c^n = a^n + b^n = (a^m)^p + (b^m)^p \]

we then conclude that \(a^n, b^n, c^m\) is a solution of \(x^p + y^p = z^p\) in non-zero integers. If one can show that \(x^p + y^p = z^p\) has no such solutions for any prime \(p \geq 3\), the arguments of this and the previous paragraph show that \(x^n + y^n = z^n\) can have no non-zero integer solutions for any integer \(n \geq 3\).

The definition varies from author to author, e.g., in [Lang, Chapter II, §1, p. 36] the field \(\mathbb{Q}\) is replaced by \(\mathbb{C}\), and in [Hart, Chapter IV, §6, Example 4.6.2, p. 320] one finds a slightly different definition. When one becomes familiar with algebraic geometry the distinctions are easily explained, and for that reason are generally ignored (if noticed at all).
integers into primes we conclude that $c|d$ (i.e., that $c$ divides $d$). A similar argument shows that $d|c$, hence $d = \pm c$, and it follows that $(a, \pm b, c) \in \mathbb{Z}^3 \setminus \{(0, 0, 0)\}$ provides a counterexample to Fermat’s Last Theorem. The theorem is therefore equivalent to the non-existence of rational points with all non-zero coordinates on the Fermat curves corresponding to primes $p \geq 3$.

The “all non-zero coordinates” restriction ending the last paragraph is a nagging qualification which is easily eliminated by pushing the relevant portion of the Fermat curve into one higher dimension. Specifically, consider the subset $\mathcal{V} \subset \mathbb{Q}^3$ consisting of points $(x, y, z)$ satisfying the two conditions

\begin{equation}
(1.1) \quad x^p + y^p = 1 \quad \text{and} \quad xyz = 1.
\end{equation}

Then a point $(r, s, t) \in \mathbb{Q}^3$ is in $\mathcal{V}$ if and only if $(r, s)$ is a point of the Fermat curve with non-zero coordinates and $t = (rs)^{-1}$. Algebraic geometers would again refer to $\mathcal{V}$ as a “curve,” since it can be viewed as the intersection of two surfaces in $\mathbb{Q}^3$, but it is not a “plane curve” since it is not within the $xy$-plane. We will call it the non-planar Fermat curve.\footnote{The terminology is not standard, but proves convenient.} When $(r, s, t) \in \mathcal{V}$ and $(r, s, t) \in \mathbb{Q}^3$ one refers to this triple as a rational point of $\mathcal{V}$. Fermat’s Last Theorem is now seen to be equivalent to: the non-planar Fermat curve corresponding to any prime $p \geq 3$ has no rational points.

The eventual resolution of Fermat’s Last Theorem was actually based on curves, but not the Fermat curves associated with the various primes $p$. To indicate the idea that eventually succeeded assume Fermat was wrong, i.e., that for some prime $p \geq 5$ there are non-zero integers $a, b, c$ such that $a^p + b^p = c^p$, and in conjunction with this triple $(a, b, c)$ introduce the Frey curve, i.e., the set of solutions in $\mathbb{C}^2$ of the equation

\begin{equation}
(1.2) \quad y^2 = x(x - a^p)(x + b^p).
\end{equation}

This curve is elliptic, i.e., topologically a torus,\footnote{Technically, only after projectivizing; we are merely attempting to convey the flavor of the argument.}, and quite a bit is known about such entities. But the Frey curve did not conform to the usual expectations for an elliptic curve, and mathematicians quickly became suspicious. In 1990 K. Ribet proved the
curve would be counterexample to the “Tanayama conjecture” if it truly existed [Ribet], and Wiles then established enough of that conjecture to prove Fermat’s Last Theorem\textsuperscript{7} from Ribet’s result.

\textsuperscript{7}For an elementary introduction to the Tanayama conjecture, as well as a clear explanation of the implications for Fermat’s Last Theorem, see [Maz]. Notice that the article appeared before Wiles’ proof was announced.
2. Classical Affine Algebraic Geometry

Throughout the notes rings are assumed commutative with unities unless specifically stated to the contrary, and ring homomorphisms are assumed to carry unities to unities.

The hypersurfaces and curves discussed in the previous section are examples of affine algebraic sets. To give the precise definition suppose \( B \supset A \) is an extension of rings, \( n \in \mathbb{Z}_+ \), and \( \mathcal{P} = \{ p_\alpha \}_{\alpha \in \Omega} \subset A[x] = A[x_1, x_2, \ldots, x_n] \) is a collection of polynomials. Then the collection \( \mathcal{V} = \mathcal{V}(\mathcal{P}) \subset B^n \) of points \( (b_1, \ldots, b_n) \in B^n \) satisfying \( p_\alpha(b_1, \ldots, b_n) = 0 \) for all \( \alpha \), i.e., the collection of solutions of the system of equations

\[
(2.1) \quad p_\alpha(x_1, \ldots, x_n) = 0, \quad \alpha \in \Omega,
\]

is the classical \((A, B)\)-affine algebraic set determined by \( \mathcal{P} \), the \((A, B)\)-affine algebraic set in the classical sense determined by \( \mathcal{P} \), or simply the zero set of \( \mathcal{P} \) (in \( B^n \)). The non-planar Fermat curve corresponding to a fixed prime \( p \) suggests an example: take \( A = \mathbb{Z} \), \( B = \mathbb{Q} \), \( n = 3 \), and let \( \mathcal{P} \) be the collection \( \{ x_1^p + x_2^p - 1, x_1x_2x_3 - 1 \} \). The plane Fermat and Frey curves provide examples in which the corresponding collections \( \mathcal{P} \) are singletons, i.e., \( \mathcal{P} = \{ x_1^p + x_2^p - 1 \} \) (with \((A, B) = (\mathbb{Z}, \mathbb{Q})\)) and \( \mathcal{P} = \{ x_2 - x_1(x_1 - a^p)(x_1 + b^p) \} \) (with \((A, B) = (\mathbb{Z}, \mathbb{C})\)) respectively. For an example with a bit more geometric flavor take \( A = B = \mathbb{R} \), \( n = 3 \) and let \( \mathcal{P} \) denote the two-element set \( \{ x_1^2 + x_2^2 - 1, x_1^2 + x_2^2 + x_3^2 - 2 \} \). The collection of points in \( \mathbb{R}^3 \) satisfying \( x_1^2 + x_2^2 - 1 = 0 \) is a cylinder, and the collection satisfying \( x_1^2 + x_2^2 + x_3^2 - 2 = 0 \) is a sphere. The classical \((\mathbb{Z}, \mathbb{R})\)-affine algebraic set corresponding to the two polynomials is the intersection of these two figures: it consists of two circles, one above and one below the \( x_1x_2 \)-plane. The given cylinder and sphere provide further examples of classical \((\mathbb{Z}, \mathbb{R})\)-affine algebraic sets.

It is important to realize, assuming the notation of the previous paragraph, that each space \( B^n \) is a classical \((A, B)\)-affine algebraic set: take \( \mathcal{P} = \{0\} \).

When \( A \) is not the trivial ring the empty set, regarded as a subset of \( B^n \), is also a classical \((A, B)\)-affine algebraic set: take \( \mathcal{P} = A[x] \) and note that (2.1) has no solutions when \( p_\alpha \) is a non-zero constant polynomial.

To better understand the role of the extension \( A \subset B \) take \( A = \mathbb{Z} \), \( n = 1 \) and \( \mathcal{P} := \{x^2 - 2\} \subset A[x] \). When \( B = \mathbb{Z} \) or \( \mathbb{Q} \) we have \( \mathcal{V}(\mathcal{P}) = \emptyset \), since the

\[\text{We have added the qualification “classical” for reference purposes. It is not standard terminology. The “(A,B)” prefix is adapted from [Mac, p. 4]; it is somewhat awkward, and as a result not common, but can be quite helpful when first learning the subject.}\]
polynomial $x^2 - 2$ as no rational roots. However, when $B = \mathbb{R}$ or $\mathbb{C}$ we have $\mathcal{V}(\mathcal{P}) = \{ \pm \sqrt{2} \} \subset B^n = B$.

A singleton set $\{ c \} = \{ (b_1, b_2, \ldots, b_n) \} \subset B^n$ need not be classically $(A, B)$-affine algebraic. To see a specific example take $A = \mathbb{Z}$, $B = \mathbb{R}$ and $n = 1$. Then any polynomial $p \in \mathbb{Z}[x]$ which vanishes at $\sqrt{2}$ must also vanish at $\sqrt{2}$, and we conclude that any zero set of a subset $\mathcal{P} \subset \mathbb{Z}[x]$ containing $\sqrt{2}$ must also contain $-\sqrt{2}$. In particular, the singleton set $\{ \sqrt{2} \} \subset \mathbb{R} = \mathbb{R}^1$ is not a classical $(\mathbb{Z}, \mathbb{R})$-affine algebraic set. This singleton set is, however, a classical $(\mathbb{R}, \mathbb{R})$-affine algebraic set: it is the zero set of the polynomial $x - \sqrt{2} \in \mathbb{R}[x]$.

When a classical $(A, B)$-affine algebraic set $\mathcal{V} \subset B^n$ is defined as in the paragraph surrounding (2.1) one refers to $B^n$ as the ambient space of $\mathcal{V}$, and when specific reference to this space proves helpful the notations $\mathcal{V}$ and $\mathcal{V}(\mathcal{P})$ are replaced by $\mathcal{V}_{B^n}$ and $\mathcal{V}_{B^n}(\mathcal{P})$ respectively.

In practice affine algebraic sets are generally indicated with less formality than employed thus far. For example, the Fermat curve in $\mathbb{Q}^2$ corresponding to a prime number $p \geq 3$ might be described as “the curve (in $\mathbb{Q}^2$) defined by the polynomial $x_1^p + x_2^p = 1$,” or simply as “the curve $x_1^p + x_2^p = 1$;” the two circle example in $\mathbb{R}^3$ given towards the end of the paragraph containing (2.1) might be described as “the intersection of the cylinder $x_1^2 + x_2^2 = 1$ with the sphere $x_1^2 + x_2^2 + x_3^2 = 2$.”

When $A = B$ a classical $(A, B)$-affine algebraic set is called a classical $B$-affine algebraic set, or simply a classical affine algebraic set when this ring is clear from context.

When $B$ is a field, the inclusion $A \subset B$ is proper, and $\mathcal{V} \subset B^n$ is a classical $(A, B)$-affine algebraic set, the elements of $\mathcal{V}\!\setminus\!A^n$ are called $B$-rational points of $\mathcal{V}$, or simply rational points when $B$ is understood. We have already encountered the concept: the “rational points” discussed in connection with the Fermat curves are simply the $\mathbb{Q}$-rational points on these curves ($A = \mathbb{Z}$, $B = \mathbb{Q}$).

In the study of affine algebraic geometry one must distinguish between polynomials and the “polynomial functions” they define. For our purposes a polynomial in the “variables” $x_1, \ldots, x_n$ having coefficients in the ring $A$ simply means an element of the particular extension ring $A[x_1, \ldots, x_n]$ of $A$; there is no requirement that such an entity be regarded as a function. But of course any such element $p$ defines a function $p(x) : B^n \to B$ in the usual way: the value $p(b)$ of $p(x)$ at a point $b = (b_1, \ldots, b_n)$ is obtained by substituting $b_j$ for $x_j$ in $p$, $j = 1, \ldots, n$. In particular, the precise

---

9 Argue as follows. Assuming $p \in \mathbb{Z}[x]$ vanishes at $\sqrt{2}$ use the Euclidean algorithm to write $p$ as $p = q \cdot (x^2 - 2) + r$, with $q, r \in \mathbb{Z}[x]$ and $r$ of the form $ax + b$. Then $0 = p(\sqrt{2}) = a\sqrt{2} + b$ and $a, b \in \mathbb{Z}$ force $a = b = 0$ (because $\sqrt{2} \notin \mathbb{Q}$), hence $p(-\sqrt{2}) = q \cdot ((-\sqrt{2})^2 - 2) = 0$. 

8
meaning of a point \( c = (b_1, \ldots, b_n) \in B^n \) being a solution of the system of polynomial equations (2.1) is that each of the associated polynomial functions \( p_\alpha(x) \) maps \( c \) to \( 0 \in B \).

We distinguish between the polynomial \( p \in A[x] \) and the function \( p(x) : B^n \to B \) for two reasons.

- Distinct \( p \) can define the same function \( p(x) : B^n \to B \). To see an example take \( A = B = \mathbb{Z}/2\mathbb{Z} \), \( n = 1 \), \( p = x^2 + x \in \mathbb{Z}[x] \) and \( q = 0 \in (\mathbb{Z}/2\mathbb{Z})[x] \). Then \( p \neq q \), but \( p(x) = q(x) \) does hold; each is the zero function \([b] \in \mathbb{Z}/2\mathbb{Z} \mapsto [0] \in B \).

- A polynomial can define many functions, e.g., \( x^2 \in \mathbb{Z}[x] \) defines the function \( n \in \mathbb{Z} \mapsto n^2 \in \mathbb{Z} \), the function \( q \in \mathbb{Q} \mapsto q^2 \in \mathbb{Q} \), and the function \( M \mapsto M^2 \) in the \( \mathbb{Z} \)-algebra of \( k \times k \) matrices with entries in \( \mathbb{Z} \) for any integer \( k \geq 1 \).

In practice the polynomial/polynomial function distinction discussed in the previous two paragraphs is often blurred. Indeed, strict adherence to precision can result in lengthy explanations of basically trivial matters\(^{10}\). For such reasons we will write an element \( p \in A[x_1, \ldots, x_n] \) as \( p(x) \) when this proves convenient.

Suppose \( V \subset B^n \) and \( W \subset B^m \) are classical \((A, B)\)-affine algebraic sets. A mapping \( g : V \to W \) is a classical \((A, B)\)-morphism, or a classical \((A, B)\)-regular function, if it is the restriction to \( V \) of a polynomial mapping \( h : B^n \to B^m \), i.e., a mapping \( h = (h_1(x), \ldots, h_m(x)) \) with with polynomial component functions \( h_j(x) = h_j(x_1, \ldots, x_n) \) arising from elements \( h_j \in A[x] \) for \( j = 1, \ldots, m \). When \( A = B \) an \((A, B)\)-morphism is called a classical \( B \)-morphism or a classical \( B \)-regular function, or simply a morphism or regular function when \( B = A \) is clear from context.

**Examples 2.2 :**

(a) Choose a prime \( p \geq 3 \) and let \( V \subset \mathbb{Q}^3 \) and \( W \subset \mathbb{Q}^2 \) denote the associated non-plane and plane Fermat curves respectively. Then the projection

\[
\begin{align*}
y_1 &= x_1, \\
y_2 &= x_2,
\end{align*}
\]

restricts to a \((\mathbb{Z}, \mathbb{Q})\)-morphism from \( V \) into \( W \), i.e., the mapping \( (x_1, x_2, x_3) \in V \mapsto (x_1, x_2) \in W \) is a \((\mathbb{Z}, \mathbb{Q})\)-morphism. It is not an isomorphism since the image does not contain the points \((1, 0)\) and \((0, 1)\) of \( W \).

\(^{10}\)For example, it is far easier to say “replace \( p(x) \) by \( p(x+1) \)” than to describe the result in a manner which avoids any reference to the symbol \( x \).
Proof: 

by replacing where

Proposition 2.3: Suppose \( f: \mathbb{B}^n \to \mathbb{B}^m \) is a polynomial mapping and \( Q \subset A[y_1, y_2, \ldots, y_m] \). Define \( f^*(Q) \subset A[x_1, x_2, \ldots, x_n] \) by 

\[
    f^*(Q) := \{ q \circ f : q \in Q \},
\]

where \( q \circ f \in A[x_1, x_2, \ldots, x_n] \) denotes the polynomial obtained from \( q(y_1, y_2, \ldots, y_m) \) by replacing \( y_j \) with \( f_j(x_1, x_2, \ldots, x_n), \quad j = 1, 2, \ldots, m \). Then

\[
    f^{-1}(\mathbb{V}_m(Q)) = \mathbb{V}_n(f^*(Q)).
\]

Proof: For any point \( c = (b_1, b_2, \ldots, b_n) \in \mathbb{B}^n \) we have

\[
    c \in f^{-1}(\mathbb{V}_m(Q)) \iff f(c) \in \mathbb{V}_m(Q) \notag
\]

\[
    \iff q(f(c)) = 0 \text{ for all } q \in Q \notag
\]

\[
    \iff (q \circ f)(c) = 0 \text{ for all } q \in Q \notag
\]

\[
    \iff (q \circ f)(c) = 0 \text{ for all } q \circ f \in f^*(Q) \notag
\]

\[
    \iff c \in \mathbb{V}_n(f^*(Q)).
\]

q.e.d.

(b) Let \( V \subset \mathbb{R}^2 \) denote the hyperbola defined by the polynomial \( x_1^2 - x_2^2 = 1 \) and let \( W \subset \mathbb{R}^3 \) denote the intersection of the hyperbolic paraboloid defined by \( x_1^2 - x_2^2 = x_3 \) and the plane \( x_3 = 1 \). Then the polynomial mapping \( h: (x_1, x_2) \in \mathbb{R}^2 \mapsto (x_1, x_2, 1) \in \mathbb{R}^3 \) restricts to a morphism \( g := h|_V: V \to W \). In fact this is an isomorphism: the inverse is the restriction to \( W \) of the polynomial mapping \( (x_1, x_2, x_3) \in \mathbb{R}^3 \mapsto (x_1, x_2) \in \mathbb{R}^2 \).

(c) We have seen that \( \mathbb{R} = \mathbb{R}^1 \) is an affine algebraic set (within \( \mathbb{R} \)). Let \( W \subset \mathbb{R}^2 \) be defined by the polynomial \( x_1^2 - x_2^2 \), i.e., the union of lines \( x_1 = x_2 \) and \( x_1 = -x_2 \). Then the mappings \( x \in \mathbb{R} \mapsto (x, x) \in W \) and \( x \in \mathbb{R} \mapsto (x, -x) \in W \) are morphisms.

(d) Let \( V \subset \mathbb{R}^3 \) denote the unit sphere, i.e., the classical affine algebraic set defined by the polynomial \( x_1^2 + x_2^2 + x_3^2 = 1 \), and let \( W \subset \mathbb{R}^2 \) denote the unit circle, i.e., the classical affine algebraic set defined by \( x_1^2 + x_2^2 = 1 \). Then the restriction of the polynomial mapping \( (x_1, x_2, x_3) \in \mathbb{R}^3 \mapsto (x_1, x_2) \in \mathbb{R}^2 \) to \( V \) is not a morphism from \( V \) to \( W \) since the latter is a proper subset of the image of \( V \).

One of the major reasons for involving only polynomial mappings in the definition of a morphism is that preimages of affine algebraic sets under such functions again have that structure. Here is the precise result.

\textbf{Proposition 2.3 :} Suppose \( f: \mathbb{B}_m \to \mathbb{B}^m \) is a polynomial mapping and \( Q \subset A[y_1, y_2, \ldots, y_m] \). Define \( f^*(Q) \subset A[x_1, x_2, \ldots, x_n] \) by 

\[
    f^*(Q) := \{ q \circ f : q \in Q \},
\]

where \( q \circ f \in A[x_1, x_2, \ldots, x_n] \) denotes the polynomial obtained from \( q(y_1, y_2, \ldots, y_m) \) by replacing \( y_j \) with \( f_j(x_1, x_2, \ldots, x_n), \quad j = 1, 2, \ldots, m \). Then

\[
    f^{-1}(\mathbb{V}_m(Q)) = \mathbb{V}_n(f^*(Q)).
\]

Proof: For any point \( c = (b_1, b_2, \ldots, b_n) \in \mathbb{B}_m \) we have

\[
    c \in f^{-1}(\mathbb{V}_m(Q)) \iff f(c) \in \mathbb{V}_m(Q) \iff q(f(c)) = 0 \text{ for all } q \in Q \iff (q \circ f)(c) = 0 \text{ for all } q \in Q \iff c \in \mathbb{V}_n(f^*(Q)).
\]

q.e.d.
Classical affine algebraic geometry is now easily described (assuming a fixed ring extension $B \supset A$): it is the study of the category having classical $(A, B)$-affine algebraic sets as objects and classical $(A, B)$-morphisms as morphisms. The goal, as in other familiar categories (e.g., the category of topological spaces and continuous functions or the category of groups and group homomorphisms), is to classify the objects up to isomorphism\textsuperscript{11}. Attaining that goal is presently unrealistic, and as a result one must often (but not always) settle for finding invariants\textsuperscript{12} (e.g., dimension, cohomology, ...) which enable one to distinguish isomorphism classes. The construction of these invariants, more often than not, is most easily achieved with functors.

\textsuperscript{11}In other words, to create a list $\{O_\alpha\}_{\alpha \in \Omega}$ of objects of the category which satisfies the following two conditions: (i) any object of the category is isomorphic to an object on the list; and (ii) no two objects on the list are isomorphic.

\textsuperscript{12}One familiar context in which the goal is achieved is elementary linear algebra. Specifically, fix a field $K$ and consider the category having finite-dimensional vector spaces over $K$ as objects and $K$-linear mappings between such spaces as morphisms. In this instance the classification assumes the following form. \textbf{Theorem:} A finite-dimensional vector space $V$ over $K$ is isomorphic to $K^n$ if and only if $V$ has dimension $n$. In other words: Any finite dimensional vector space over $K$ is isomorphic to one of the spaces on the list $\{K^n\}_{n \geq 0}$, and no two distinct spaces on this list are isomorphic. From the categorical viewpoint it is quite remarkable that the invariant $n$ is all one needs. Among the categories of wide mathematical interest, this is by far the easiest to handle. This is one of many reasons why a solid background in elementary linear algebra is crucial for understanding contemporary higher mathematics.
3. The Ring-Theoretic Approach

In this section $B \supset A$ is an extension of rings, $n$ is a positive integer, and $A[x] := A[x_1, x_2, \ldots, x_n]$. To ease terminology and notation the “classical,” “$(A, B)$,” and “affine” prefixes will henceforth be omitted when there is little risk of confusion, e.g., “algebraic set” will mean “classical $(A, B)$-affine algebraic set.”

Readers are reminded that all rings are assumed commutative with unities unless specifically stated to the contrary, and that all ring homomorphisms are assumed to preserve unities.

Let $V \subset B^n$ be an algebraic set and let

\begin{equation}
(3.1) \quad i(V) := \{ p \in A[x] : p(b_1, b_2, \ldots, b_n) = 0 \text{ for all } (b_1, b_2, \ldots, b_n) \in V \}.
\end{equation}

This is an ideal of $A[x]$, as is easily verified; it is the defining $(A, B)$-ideal of $V$, or simply the defining ideal of $V$ when $A$ and $B$ are understood. The factor ring $A_B[V] := A[x]/i(V)$ is the $(A, B)$-coordinate ring of $V$, or simply the coordinate ring of $V$, and is generally identified with the collection of regular functions\(^{16}\) from $V$ into $B$. Indeed, for any $p \in A[x]$ the restriction $p(x)|_V$ is such a function, and the functions corresponding to polynomials $p, q \in A[x]$ have the same restriction if and only if the difference $p(x) - q(x)$ vanishes on $V$, i.e., if and only if $p - q \in i(V)$.

Despite the function-theoretic interpretation of the coordinate ring, several of our examples will have a number-theoretic flavor. We do this to stress the sweeping viewpoint that the contemporary approach to algebraic geometry achieves.

**Examples 3.2**: In Examples (a)-(c) we take $A = \mathbb{Z}$ and let $B$ be initially unspecified. In (a) and (b) we take\(^{17}\) $\mathcal{P} = \{x^2 - 2\} \subset A[x]$ (one variable).

(a) When $B = \mathbb{Q}$ we have $V = V(\mathcal{P}) = \emptyset$ (because $x^2 - 2$ has no roots in $\mathbb{Q}$). The condition $b \in V \Rightarrow p(b) = 0$ is vacuously satisfied for all $p \in A[x]$, and $i(V) = A[x]$ follows. The coordinate ring $A_B[V]$ is the trivial (i.e., one element) ring.

---

\(^{13}\)I.e., for the remainder of the notes; not simply within this section.

\(^{14}\)The definitions in this section are patterned after those in [Mac, Introduction, pp. 3-5], but there $A$ and $B$ are assumed fields.

\(^{15}\)The notation $A_B[V]$ is not standard. The standard notation, when $A = B$, is $B[V]$, and when that is used $B$ is usually assumed a field.

\(^{16}\)I.e., $(A, B)$-regular functions.

\(^{17}\)That is, $\mathcal{P}$ is the singleton set $\{x^2 - 2\}$.
(b) When \( B = \mathbb{R} \) we have \( \mathcal{V} = \{-\sqrt{2}, \sqrt{2}\} \), in which case we claim that \( \mathfrak{i}(\mathcal{V}) = (x^2 - 2) \) (i.e., the principal ideal \((x^2 - 2)\mathbb{Z}[x]\)). To see this first note that \( x^2 - 2 \in \mathfrak{i}(\mathcal{V}) \); then use the Euclidean algorithm\(^{18}\) to prove that any polynomial \( p \) vanishing at both points must be a multiple of \( x^2 - 2 \). The coordinate ring is therefore \( \mathbb{Z}[x]/(x^2 - 2) \), which is immediately identified with the subring \( \{ a + b\sqrt{2} : a, b, \in \mathbb{Z}\} \) of \( \mathbb{R} \).

(c) Replace \( \mathcal{P} = \{ x^2 - 2 \} \) and \( B = \mathbb{R} \) in (b) with \( \mathcal{P} = \{ x^2 + 1 \} \) and \( B = \mathbb{C} \). Then \( \mathcal{V} = \{-i, i\} \), \( \mathfrak{i}(\mathcal{V}) = (x^2 + 1) \subset \mathbb{Z}[x] \), and the coordinate ring can be identified with the ring \( \{ a + ib : a, b \in \mathbb{Z}\} \) of Gaussian integers. This ring is useful for producing infinitely many non-zero integer solutions of the Pythagorean equation \( x^2 + y^2 = z^2 \). (For a curious variation of this application, involving the quotient field \( \mathbb{Q}(i) \) of the ring of Gaussian integers, see see [El].)

(d) When \( p \geq 3 \) is prime number the \( p^{th}\)-cyclotomic polynomial \( \Phi_p(x) \in \mathbb{Z}[x] \) is defined by

\[
\Phi_p(x) := x^{p-1} + x^{p-2} + \cdots + x + 1.
\]

It is well-known\(^{19}\) that this polynomial is irreducible over \( \mathbb{Z}[x] \). From the factorization

\[
x^p - 1 = (x - 1)\Phi_p(x)
\]

one sees that the roots of \( \Phi_p(x) \) are the \( p-1 \) distinct \( p^{th}\)-roots \( \mathcal{V} := \{e^{j2\pi i/p}\}_{j=1}^{p-1} \) of unity (i.e., of 1). In particular, \( \mathcal{V} = \mathcal{V}(\{\Phi_p(x)\}) \subset \mathbb{C}^1 = \mathbb{C} \) is a classical \((\mathbb{Z}, \mathbb{C})\)-affine algebraic set\(^{20}\). We follow custom and write \( \mathcal{V} \) as \( \{\zeta^j\}_{j=1}^{p-1} \), where \( \zeta := e^{2\pi i/p} \).

Choose any polynomial \( q \in \mathbb{Z}[x] \) and (once again use the Euclidean algorithm to) write \( q = s \cdot \Phi_p(x) + r \), where \( \deg(r) < p - 1 = \deg(\Phi_p(x)) \) if \( r \neq 0 \). If \( q \) vanishes on \( \mathcal{V} \) then \( r \) must also vanish on \( \mathcal{V} \) (because this is the case for \( \Phi_p(x) \)), and if \( r \neq 0 \) this is impossible since \( r \) can have at most \( p - 2 \) roots.

We conclude that \( q \) is divisible by \( \Phi_p(x) \), hence that \( \mathfrak{i}(\mathcal{V}) = (\Phi_p(x)) \subset \mathbb{Z}[x] \).

\(^{18}\)As in Footnote 9.

\(^{19}\)This is generally established as a first or second application of the Eisenstein irreducibility criterion, as in [L, Chapter IV, §3, p. 184].

\(^{20}\)The “cyclotomic” terminology arises from the observation that \( \mathcal{V} \cup \{1\} \) is a cyclic group (under complex multiplication). Geometrically this group is the set of vertices of a regular \( p \)-gon inscribed in the unit circle, positioned so as to have one vertex at 1.
Since $\Phi_p(x)$ is irreducible it follows that the coordinate ring $\mathbb{Z}_C[V] = \mathbb{Z}[x]/i(V)$ can be identified with the subring

\begin{equation}
\{ a_0 + a_1 \zeta + \cdots + a_{p-2} \zeta^{p-2} : a_0, a_1, \ldots, a_{p-2} \in \mathbb{Z} \}
\end{equation}

of $\mathbb{C}$.

In algebraic number theory this is the ring of $p$-\textit{cyclotomic integers}. E.E. Kummer investigated these rings in the mid-nineteenth century in connection with Fermat’s Last Theorem, and was able to prove many new cases of that result based on his investigations\textsuperscript{21}.

(c) Suppose $B = A$, $n \geq 1$, and $c = (b_1, b_2, \ldots, b_n)$ is a point of $B^n$. Then the singleton set $\{c\}$ is the zero set of the collection $\{x_j - b_j\}_{j=1}^n$, and is therefore algebraic. We claim that

\[ i(\{c\}) = (x_1 - b_1, x_2 - b_2, \ldots, x_n - b_n), \]

where the right-hand-side denotes the ideal of $A[x] = A[x_1, x_2, \ldots, x_n]$ “generated” by the collection $\{x_j - b_j\}_{j=1}^n$, i.e.\textsuperscript{22} the ideal consisting of all sums $\sum_{j=1}^n q_j(x_1, x_2, \ldots, x_n)(x_j - b_j)$ with $q_j \in A[x]$. To see this first note that each of the polynomials $x_j - b_j \in B[x] = A[x]$ vanishes on $c$, and therefore belongs to $i(\{c\})$. If $p \in i(\{c\})$ is arbitrary write each occurrence of $x_n$ in $p$ in the form $(x_n - b_n) + b_n$, expand associated powers $x_n^m = ((x_n - b_n) + b_n)^m$ using the binomial theorem, and then collect coefficients so as to express $p$ as a polynomial in $x_n - b_n$ with coefficients in $A[x_1, x_2, \ldots, x_{n-1}]$, say

\[
p = q_0(x_1, x_2, \ldots, x_{n-1}) + \sum_{j=1}^\ell q_j(x_1, x_2, \ldots, x_{n-1})(x_n - b_n)^j
\]

\[
= q_0(x_1, x_2, \ldots, x_{n-1}) + \left( \sum_{j=1}^\ell q_j(x_1, x_2, \ldots, x_{n-1})(x_n - b_n)^{j-1} \right) \cdot (x_n - b_n)
\]

\[
= q_0(x_1, x_2, \ldots, x_{n-1}) + q(x_1, x_2, \ldots, x_n) \cdot (x_n - b_n).
\]

Since $p$ and $x_n - b_n$ vanish at $c$, the polynomial $q_0$ must vanish at the point $(b_1, b_2, \ldots, b_{n-1}) \in B^{n-1}$. If $n = 1$ this forces $q_0$ to be the zero polynomial, and we conclude that $p$ is a multiple of $x_1 - b_1 = x - b_1$ as claimed. If $n \geq 2$ and the result holds for $n - 1$ then $q_0$ must be in the ideal generated by $x_1 - b_1, x_2 - b_2, \ldots, x_{n-1} - b_{n-1}$, and from $p = q_0 + q \cdot (x_n - b_n)$ we then see that $p \in (x_1 - b_1, x_2 - b_2, \ldots, x_n - b_n)$.

\textsuperscript{21}For a quick and entertaining sketch of Kummer’s work see, e.g., [Ribet, Chapter 5, §1, pp. 223-7].
\textsuperscript{22}The concept of generating sets of ideals is defined formally in the first bulleted item following implication (4.1). However, the description given here should suffice for present purposes.
(f) By taking $V = B^n$ in (3.1) we see that

(i) $i(B^n) := \{ p \in A[x] : p(x) : B^n \to B \text{ is the zero function} \}$.

Suppose $B$ is a field. Since a polynomial with coefficients in a field has at most finitely many roots, $i(B^n) = \{0\}$ when $B$ is infinite, in which case

$$A_B[B^n] = A[x]/\{0\} \simeq A[x].$$

The following observation is immediate from the definition of the canonical mapping of a factor space, but useful to record for later reference.

**Proposition 3.3 :** Suppose $W \subset B^n$ is an algebraic set and $f : A[x] \to A_B[W]$ is the canonical homomorphism. Then

$$i(W) = \ker(f).$$

When $B$ is an integral domain the defining ideals of algebraic sets have a rather special structure, and that structure is worth introducing in a more general setting. For this purpose let $R$ be a ring and let $i \subset R$ be an ideal. The *radical* of $i$, denoted $\sqrt{i}$, is the collection of all elements $r \in R$ such that $r^m \in i$ for some positive integer $m$ (generally depending on $r$). One checks easily that $\sqrt{i}$ is an ideal containing $i$; one calls $i$ a radical ideal when $\sqrt{i} = i$.

Our first example of a radical ideal is given as a proposition for later reference. For the statement recall that an ideal $p$ of a ring $R$ is prime if $p \neq R$ and $R/p$ is an integral domain. An equivalent definition, which is the one used in the proof of Proposition 3.4, is: if $r, s \in R$ and $rs \in p$ then $r \in p$ or $s \in p$ (or both).

---

23 Read the symbol “$\simeq$” as “(which) is (being) identified with.”

24 In the older literature radical ideals were also called perfect ideals, e.g., see [Kol, Chapter 0, §5, p. 7], and that terminology is still used by some authors. Unfortunately, “perfect ideal” now has another meaning, e.g., see [Eis, Chapter 19, §5, Exercise 19.9, p. 489].

25 For completeness we recall the proof of this equivalence. Let $p \subset R$ be an ideal and for each $r \in R$ let $[r] \in R/p$ denote the coset $r + p$ of $r$. Then for any $r, s \in R$ we have

(i) $[r][s] = [rs] = [0] \iff rs \in p$.

If $rs \in p$ and $R/p$ is an integral domain the left hand equality in (i) forces $[r] = [0]$ or $[s] = [0]$, hence $r \in p$ or $s \in p$. Conversely, if $rs \in p$ implies $r \in p$ or $s \in p$ then (i) implies $[r] = [0]$ or $[s] = [0]$, and $R/p$ is therefore an integral domain.
Proposition 3.4 : Any prime ideal is radical.

Proof : Suppose \( p \) is a prime ideal of a ring \( R \) and \( r \in R \) satisfies \( r^m \in p \) for some positive integer \( m \). We need to prove that \( r \in p \), which we note is obvious if \( m = 1 \). Proceeding by induction, suppose \( m > 1 \) and write \( r^m = r r^{m-1} \). Since \( p \) is prime this forces either \( r \in R \), as desired, or \( r^{m-1} \in R \), whence \( r \in R \) by induction. q.e.d.

To see further examples of radicals of ideals and radical ideals let \( R = \mathbb{Z} \), and for any \( k \in \mathbb{Z} \) let \( (k) \) denote the principal ideal \( k \mathbb{Z} \subset \mathbb{Z} \) generated by \( k \) (i.e., \( (k) := k \mathbb{Z} \)). Readers are assumed familiar with origin of the terminology “prime ideal”: a non-zero ideal \( (k) \subset \mathbb{Z} \) is prime if and only if \( |k| \) is a prime number. Fix a positive integer \( n \) and let \( n = \prod_{j=1}^{k} p_{j}^{n_{j}} \) be the unique factorization of \( n \) into non-zero positive integer powers of distinct primes. Then \( \sqrt[\text{prime}]{n} = (\prod_{j=1}^{k} p_{j}) \), and \( (n) \) is radical if and only if all \( n_{j} = 1 \). Specific examples: \( \sqrt[\text{prime}]{250} = (10) \) (because the prime factorization of 250 is \( 2 \cdot 125 = 2^1 \cdot 5^3 \) and \( 2 \cdot 5 = 10 \)); the ideal \( (30) \) is radical (because \( 30 = 2 \cdot 3 \cdot 5 \)).

Proposition 3.5 : The radical of any ideal of a ring \( R \) is a radical ideal, i.e., for all ideals \( i \subset R \) one has \( \sqrt{\sqrt{i}} = \sqrt{i} \).

Proof : The inclusion \( \sqrt{i} \subset \sqrt{\sqrt{i}} \) is immediate from the definition of the radical. To prove the opposite inclusion choose any \( q \in \sqrt{\sqrt{i}} \). Then \( q^n \in \sqrt{i} \) for some integer \( n \geq 1 \), hence \( q^{n+m} = (q^n)^m \in i \) for some integer \( m \geq 1 \), and \( q \in \sqrt{i} \) follows. q.e.d.

Again let \( R \) be a ring. An element \( r \in R \) is nilpotent if there is a positive integer \( m \) such that \( r^m = 0 \), e.g., the coset \( [2] \in \mathbb{Z}/8\mathbb{Z} \) is nilpotent. Equivalently, \( r \in R \) is nilpotent if and only if \( r \in \sqrt{(0)} \).

A reduced ring is a ring with no nilpotents other than 0 (which is always nilpotent). Any integral domain is a reduced ring, but the converse is false, e.g., \( \mathbb{Z}/6\mathbb{Z} \) is reduced, but is not an integral domain. Of course any field is a reduced ring. As is evident from the previous paragraph, an example of a ring which is not reduced is provided by \( \mathbb{Z}/8\mathbb{Z} \).
Proposition 3.6: Let $R$ be a ring and let $i \subset R$ be a radical ideal. Then $R/i$ is reduced.

Proof: Suppose $r \in R$ and (the coset) $[r] \in R/i$ satisfies $[r]^m = [0]$ for some positive integer $m$. This gives $r^m \in i$, hence $r \in i$ (because $i$ is assumed radical), and $[r] = [0]$ follows. \hfill q.e.d.

Reduced rings enter algebraic geometry though the follow result.

Proposition 3.7: When $B$ is reduced the defining ideal of any algebraic set is a radical ideal and the associated coordinate ring is reduced.

Proof: Assume, in the notation of (3.1), that $q \in A[x]$ is contained in $\sqrt{i(V)}$. Then for some positive integer $m$ we have $q^m \in i(V)$, hence $0 = q^m(c) = (q(c))^m$ for all $c = (b_1, b_2, \ldots, b_n) \in V$. Since $B$ is assumed reduced we must have $q(c) = 0$ for all such $c$, and $q \in i(V)$ follows. This proves that $i(V)$ is radical; the final assertion is then immediate from Proposition 3.6. \hfill q.e.d.

Assume the notation of the paragraph surrounding (3.1), suppose $W \subset B^m$ is a second algebraic set, and suppose that $g : V \to W$ is a regular function, i.e., the restriction to $V$ of a polynomial function $h = (h_1, h_2, \ldots, h_m) : B^n \to B^m$ with component polynomials $h_j \in A[x]$, $j = 1, 2, \ldots, m$. Then a ring homomorphism $h^* : A[y] := A[y_1, y_2, \ldots, y_m] \to A[x] = A[x_1, x_2, \ldots, x_n]$ is defined by

$$(3.8) \quad h^* : q \in A[y] \mapsto q \circ h \in A[x].$$

If $q \in i(W)$ and $x \in V$ then $(q \circ h)(x) = q(h(x)) = 0$ (because $h(x) = g(x) \in W$), and we then see from (3.8) that $h^* q \in i(V)$. In this way we see that $g$ induces a ring homomorphism $h^* : A_B[W] := A[y]/i(W) \to A_B[V] := A[x]/i(V)$ between the associated coordinate rings. Specifically,

$$(3.9) \quad h^*(q) := [q \circ h], \quad q \in A[y],$$

wherein the left and middle square brackets denote equivalence classes (w.r.t. the equivalence relation “have the same restriction to $V$”).

Suppose $g : V \to W$ in the previous paragraph is also the restriction to $V$ of a second polynomial function $f = (f_1, f_2, \ldots, f_m) : B^n \to B^m$. Then for any $x \in V$ we have

$$(q \circ h)(x) = q(h(x)) = q(g(x)) = q(f(x)) = (q \circ f)(x),$$

hence $[q \circ h] = [q \circ f]$, and it follows that definition (3.9) depends only on the equivalence class of $h$. For this reason one writes $h^* : A_B[W] \to A_B[V]$ as $g^* : A_B(W) \to A_B(V)$. 

17
Theorem 3.10: The assignments

\[ V \mapsto A_B[V] \]

and

\[ g : V \rightarrow W \mapsto g^* : A_B[W] \rightarrow A_B[V] \]

defined above constitute a contravariant functor \( \alpha \) from the category of classical \((A,B)\)-affine algebraic sets and classical \((A,B)\)-regular functions to the category of reduced rings and homomorphisms thereof.

Proof: Verification of the properties required of a functor is routine. \( \text{q.e.d.} \)

One could say that the adjective “algebraic” entered “algebraic geometry” because the functor just introduced played such a dominant role in the study of classical affine algebraic sets\(^{26}\). More recently the study of such sets was simplified by the introduction of two additional functors, and these are the focus of the next two sections.

\[ \text{\textsuperscript{26}The “functor” terminology is far more recent than the use of algebraic techniques. It offers a most welcome helping hand for understanding a massive quantity of ideas.} \]
4. The Topological Approach

Again $B \supset A$ is an extension of rings, $n$ is a positive integer, and $A[x] := A[x_1, x_2, \ldots, x_n]$.

We will use the algebraic subsets of $B^n$ to construct a topology on this space, and then endow any algebraic subset with the induced topology. The construction requires a few preliminaries.

First observe that when $\mathcal{P}$ and $\mathcal{Q}$ are subsets of $A[x]$ one has the implication

\[(4.1) \quad \mathcal{P} \subset \mathcal{Q} \Rightarrow \mathcal{V}(\mathcal{Q}) \subset \mathcal{V}(\mathcal{P}).\]

Indeed, for any $c = (b_1, b_2, \ldots, b_n) \in B^n$ one has

\[c \in \mathcal{V}(\mathcal{Q}) \iff p(c) = 0 \text{ for all } p \in \mathcal{Q} \]
\[\Rightarrow p(c) = 0 \text{ for all } p \in \mathcal{P} \]
\[\Rightarrow c \in \mathcal{V}(\mathcal{P}),\]

and (4.1) follows.

Now let $R$ be a (commutative) ring (with unity $1 = 1_R$).

- The intersection of any family of ideals of $R$ is again an ideal, as is easily checked. When $S$ is any subset of $R$ the intersection $(S) \subset R$ of all those ideals containing $S$ is therefore an ideal, known as the ideal generated by $S$: it consists of all finite sums $\sum_j r_j s_j$ with $(r_j, s_j) \in R \times S$. (Indeed, this collection is an ideal which is obviously contained within any ideal containing $S$, and must therefore coincide with the intersection of all such ideals.) When $S$ is finite, say $S = \{s_1, s_2, \ldots, s_n\}$, one writes $(s_1, s_2, \ldots, s_n)$ in place of $(\{s_1, s_2, \ldots, s_n\})$. When $S$ is a singleton $\{s\}$ the notations $(s)$ and $sR$ are used interchangeably. We have already encountered this concept, as well as a special case of the notation $(s_1, s_2, \ldots, s_n)$, in Example 3.2(e). Here are some further examples assuming $R = \mathbb{Z}$: $(2, 3) = \mathbb{Z}$; $(2) = 2\mathbb{Z}$ (wherein $2\mathbb{Z}$ denotes all integer multiples of 2); $(-6, 36) = (6) = 6\mathbb{Z}$.

- The sum $\sum_{\alpha} i_\alpha$ of a family $\{i_\alpha\}$ of ideals of $R$ is defined as the collection of all finite sums $\sum_j r_j i_{\alpha_j}$ with $(r_j, i_{\alpha_j}) \in R \times i_{\alpha_j}$. Note that $\sum_{\alpha} i_\alpha$ is again an ideal. Indeed, in the notation of the previous item one has

\[(4.2) \quad \sum_{\alpha} i_\alpha = (\cup_{\alpha} i_\alpha).\]

Examples when $R = \mathbb{Z}$: $(2) + (4) = (2)$; $(2) + (3) = \mathbb{Z}$. 19
As we now show, the collection \( P \) of polynomials defining an algebraic set \( V(P) \) can always be assumed an ideal, and when \( B \) is reduced that ideal can be assumed radical.

**Proposition 4.3 :** For any subset \( P \subset A[x] \) one has

(i) \( V(P) = V((P)) \),

and when \( B \) is reduced one also has

(ii) \( V(P) = V((P)) = V(\sqrt{(P)}) \).

The practical consequence is: when studying algebraic sets within \( B^n \) nothing is lost by only considering those of the form \( V(i) \), where \( i \subset A[x] \) is an ideal. However, when using this approach one must be careful to distinguish the given ideal \( i \) from the defining ideal \( i(V(i)) \) of \( V(i) \). One always has

\[
(4.4) \quad i \subset i(V(i)),
\]

as is easily checked, but the inclusion can be proper. For example, the zero set in \( \mathbb{Q} \) of the (non-radical) ideal \((x^2) \subset \mathbb{Z}[x] \) is the singleton \( \{0\} \), i.e., \( V((x^2)) = \{0\} \), but the defining ideal of this classical \((\mathbb{Z}, \mathbb{Q})\)-affine algebraic set is \((x)\) (which we note is the radical \( \sqrt{(x^2)} \) of \((x^2))\).

**Proof of Proposition 4.3 :** For any point \( c = (b_1, b_2, \ldots, b_n) \in B^n \) one has

\[
c \in V(P) \iff p(c) = 0 \quad \text{for all} \quad p \in P
\]
\[
\iff \sum_j r_j p_j(c) = 0 \quad \text{for all finite sums}
\]
\[
\sum_j r_j p_j \quad \text{with} \quad (r_j, p_j) \in B \times P
\]
\[
\iff c \in V((P)).
\]

Equality (i) follows.

Only the second equality in (ii) requires proof. (The first repeats (i).) From \( (P) \subset \sqrt{(P)} \) and (4.1) we see that \( V(\sqrt{(P)}) \subset V((P)) \) (which we note does not require the added hypothesis on \( B \)), and we are thereby reduced to establishing

(iii) \( V((P)) \subset V(\sqrt{(P)}) \).
To this end choose \( c = (b_1, b_2, \ldots, b_n) \in B^n \), \( q \in \sqrt{\mathcal{P}} \), and \( m \geq 1 \) such that \( q^m \in \mathcal{P} \). Then

\[
\begin{align*}
  c \in \mathcal{V}(\mathcal{P}) & \Rightarrow q^m(c) = 0 \\
  & \Leftrightarrow (q(c))^m = 0 \\
  & \Leftrightarrow q(c) = 0 \quad \text{(because } B \text{ is reduced)},
\end{align*}
\]

which by the arbitrariness of \( q \in \sqrt{\mathcal{P}} \) gives \( c \in \mathcal{V}(\sqrt{\mathcal{P}}) \). This establishes (iii) and completes the argument. \( \text{q.e.d.} \)

**Theorem 4.5 :** Let \( i, j \) and \( i_\alpha \), where \( \alpha \) varies through some index set, be ideals of \( A[x] \). Then:

(a) \( \mathcal{V}(A[x]) = \emptyset \) and \( \mathcal{V}((0)) = B^n \);

(b) \( \cap \alpha \mathcal{V}(i_\alpha) = \mathcal{V}(\sum \alpha i_\alpha) = \mathcal{V}((\cup \alpha i_\alpha)) \); and

(c) \( \mathcal{V}(i) \cup \mathcal{V}(j) \subset \mathcal{V}(i \cap j) \), and when \( B \) is an integral domain one has

\[ \mathcal{V}(i) \cup \mathcal{V}(j) = \mathcal{V}(i \cap j). \]

**Proof :**

(a) These observations were already noted at the beginning of §2 (see the two paragraphs following that surrounding (2.1)).

(b) For \( c = (b_1, b_2, \ldots, b_n) \in B^n \) we have

\[
\begin{align*}
  c \in \cap \alpha \mathcal{V}(i_\alpha) & \Leftrightarrow c \in \mathcal{V}(i_\alpha) \quad \text{for all } \alpha \\
  & \Leftrightarrow p(c) = 0 \quad \text{for all } \alpha \text{ and all } p \in i_\alpha \\
  & \Leftrightarrow (\sum p_j)(c) = 0 \quad \text{for all finite sums} \\
  & \quad \text{of elements } p_j \in \bigcup \alpha i_\alpha \\
  & \Leftrightarrow c \in \mathcal{V}(\sum \alpha i_\alpha).
\end{align*}
\]

For the second equality use (4.2).

(c) From \( i \cap j \subset i \) and (4.1) we have \( \mathcal{V}(i) \subset \mathcal{V}(i \cap j) \). The same reasoning gives \( \mathcal{V}(j) \subset \mathcal{V}(i \cap j) \), and \( \mathcal{V}(i) \cup \mathcal{V}(j) \subset \mathcal{V}(i \cap j) \) follows.

Now assume \( B \) is an integral domain and the asserted equality fails. Then there is an element \( c \in \mathcal{V}(i \cap j) \setminus (\mathcal{V}(i) \cup \mathcal{V}(j)) \). From \( c \notin \mathcal{V}(i) \) there must be an element \( p \in i \) such that \( p(c) \neq 0 \), and, similarly, there must be an element \( q \in j \) such that...
From \( p \in \mathfrak{i} \cap \mathfrak{j} \), \( c \in \mathcal{V}(\mathfrak{i} \cap \mathfrak{j}) \) and the integral domain hypothesis we then reach the contradiction

\[ 0 = pq(c) := p(c)q(c) \neq 0. \]

\textbf{Corollary 4.6 :} When \( B \) is an integral domain the complements of the algebraic subsets of \( B^n \) form a topology on this vector space. Moreover, the mapping \( \mathfrak{i} \subset A[x] \mapsto \mathcal{V}(\mathfrak{i}) \subset B^n \) is an inclusion reversing surjection from the collection of radical ideals of \( A[x] \) to the closed subsets of \( B^n \).

In particular, under the stated hypotheses on \( B \) and \( A[x] \) the closed subsets of \( B^n \) are parameterized by the radical ideals of \( A[x] \), although not necessarily in a one-to-one fashion.

\textbf{Proof :} Since integral domains are reduced rings, the final assertion is immediate from Proposition 4.3.

Unfortunately, the mapping \( \mathfrak{i} \mapsto \mathcal{V}(\mathfrak{i}) \) of Corollary 4.6 is generally not a bijection. To see a specific example take \( A = B = \mathbb{R} \) and \( n = 1 \). It is not difficult to verify that the distinct principal ideals \((x^2 + 1)\) and \((x^2 + 2)\) are prime\(^{27}\), hence radical, and the mapping assigns both to \( \mathcal{V} = \emptyset \subset \mathbb{R} = \mathbb{R}^1 \). To ensure bijectivity one needs an additional hypothesis.

\textbf{Proposition 4.7 :} Suppose \( B \) is an integral domain and the following “Nullstellensatz property” holds: for any ideal \( \mathfrak{i} \subset A[x] \) and any \( p \in A[x] \) the condition \( p(x) = 0 \) for all \( x \in \mathcal{V}(\mathfrak{i}) \) implies \( p \in \sqrt{\mathfrak{i}} \). Then:

(a) the mapping \( \mathfrak{i} \mapsto \mathcal{V}(\mathfrak{i}) \) from radical ideals of \( A[x] \) to classical \((A, B)\)-affine algebraic subsets of \( \mathbb{B}^n \) is an inclusion reversing bijection;

(b) \( \mathcal{V}(\mathfrak{i}) \neq \emptyset \) for all proper ideals \( \mathfrak{i} \subset A[x] \).

\(^{27}\)If the product of polynomials \( p_1, p_2 \in \mathbb{R}[x] \) is in \((x^2 + 1)\) then \( p_1p_2 = q \cdot (x^2 + 1) \) for some \( q \in \mathbb{R}[x] \). From this identity one sees that w.l.o.g. that \( p_1 \) must vanish on \( i := \sqrt{-1} \), and one can then mimic the argument of Footnote 9 to see that \( p_1 \) must be divisible by \( x^2 + 1 \), hence must be in \((x^2 + 1)\). With a completely analogous argument one can show that that \((x^2 + 2) \subset \mathbb{R}[x] \) is also prime.

Alternatively, and assuming familiarity with the result, one could simply invoke the theorem that when \( K \) is a field and \( x \) is a single indeterminate over \( K \) any principal ideal in \( K[x] \) generated by an irreducible polynomial must be prime.
The Nullstellensatz terminology\textsuperscript{28} is used because the property is closely related to Hilbert’s Nullstellensatz, as we will see in Corollary 16.3.

**Proof:** By (4.1) and (ii) of Proposition 4.3 the mapping of (a) is an inclusion reversing surjection, and as a result it suffices to establish the proposition with “bijection” replaced by “injection.”

(a) : Suppose, to the contrary, that there are distinct radical ideals $i, j \subset A[x]$ such that

(i) \hspace{1cm} \mathcal{V}(i) = \mathcal{V}(j).

Then w.l.o.g. there is a ring element

(ii) \hspace{1cm} p \in j \setminus i,

and for $x \in \mathcal{V}(i)$ we see from (i) that $p(x) = 0$. The Nullstellensatz property then forces $p \in \sqrt{i} = i$, contradicting (ii).

(b) : By Proposition 4.3 we can assume $i$ is radical, and in that case the result is immediate from (a) and Theorem 4.5(a).

\textbf{q.e.d.}

The topology on $B^n$ defined in Corollary 4.6 is the $(A, B)$-Zariski topology, or the $A$-topology\textsuperscript{29} and when this topology is assumed $B^n$ is written as $\mathbb{B}^n$. The induced topology\textsuperscript{30} on any affine algebraic subset of $\mathbb{B}^n$, also called the $(A, B)$-Zariski topology, is henceforth assumed unless specifically stated to the contrary. When more than one space is involved (as in the next proposition) ambient spaces are indicated by subscripts, e.g., $\mathcal{V}_{\mathbb{B}^m}$ would mean that $\mathcal{V}_{\mathbb{B}^m}$ is an algebraic subset of $\mathbb{B}^m$.

By a Zariski closed set one means a closed set in the $(A, B)$-Zariski topology; by the Zariski closure of a set $C$ one means the closure\textsuperscript{31} $\text{cl}(C)$ in the $(A, B)$-Zariski topology; by Zariski dense one means dense in the $(A, B)$-Zariski topology,

\textsuperscript{28}Which is not standard.

\textsuperscript{29}The definitions of the two topologies in this paragraph are adapted from [Mac, Introduction, p. 6], although in that reference $A$ and $B$ are assumed fields with $B$ algebraically closed (this final assumption is imposed in [Mac] in the sentence connecting pages 2 and page 3). The definition of the $(A, B)$-Zariski topology on an affine algebraic subset of $\mathbb{B}^n$ given here is not the one found there, but is shown to be equivalent in (our) Proposition 4.11. Our definition is more in the spirit of [Hart, Chapter I, §1, p. 3], but there $A = B$ and $B$ a field are assumed.

\textsuperscript{30}Also called the relative or subspace topology. When $X$ is a topological space and $S \subset X$ the open sets of the induced topology are, by definition, the intersections with $S$ of the open sets of $X$.

\textsuperscript{31}When $X$ is a topological space and $S$ is a subset we denote the closure of $S$ by $\text{cl}(S)$. The notation $\overline{S}$ is more common.
etc. To remind readers of the underlying integral domain extension $B \supset A$ we may on occasion refer to an $(A, B)$-Zariski closed set, or to a set being $(A, B)$-Zariski dense, etc. On the other hand, when the extension $B \supset A$ is clear from context the prefix $(A, B)$ will be dropped, and since this is the only topology we will consider on algebraic sets the name Zariski will often be dropped.

**Proposition 4.8**: Suppose $B$ is an integral domain and $n$ and $m$ are positive integers. Then any polynomial mapping $f : \mathbb{B}^n \to \mathbb{B}^m$ is continuous.

**Proof**: Immediate from Proposition 2.3. q.e.d.

**Corollary 4.9**: When $B$ is an integral domain any morphism $g : \mathcal{V} \to \mathcal{W}$ between algebraic sets is continuous.

**Proof**: By definition such a $g$ must be the restriction to $\mathcal{V}$ of a polynomial mapping $f : \mathbb{B}^n \to \mathbb{B}^m$ between the ambient spaces of $\mathcal{V}$ and $\mathcal{W}$ respectively. If $C \subset \mathcal{W}$ is a closed subset then (by the definition of the induced topology) $C = \mathcal{W} \cap C$ for some algebraic subset $C \subset B^m$. We can therefore write

$$g^{-1}(C) = f^{-1}(\mathcal{W} \cap C) = f^{-1}(\mathcal{W}) \cap f^{-1}(C) = \mathcal{V} \cap f^{-1}(C),$$

which by Proposition 4.8 (and one more appeal to the definition of the induced topology) is a closed subset of $\mathcal{V}$. q.e.d.

**Theorem 4.10**: When $B$ is an integral domain, endowing the algebraic subsets of the various $\mathbb{B}^n$ with the Zariski topology constitutes a covariant functor $\beta$ from the category of all such sets and regular functions to the category of topological spaces and continuous mappings.

**Proof**: Verification of the properties required of a functor is routine. q.e.d.

In later sections we will use this functor to derive information about algebraic sets.

It is worth pointing out that when $B$ is an integral domain and $\mathcal{V} \subset \mathbb{B}^n$ is an algebraic set the Zariski topology on $\mathcal{V}$ can be defined in terms of the vanishing of regular functions on $\mathcal{V}$. This is immediately evident from the following result.

**Proposition 4.11**: Suppose $B$ is an integral domain, $n \geq 1$ is an integer, and $\mathcal{V} \subset \mathbb{B}^n$ is an algebraic set. Then a subset $C \subset \mathcal{V}$ is closed (in the induced Zariski topology) if and only if there is a collection of regular functions $\{r_\alpha : \mathcal{V} \to \mathbb{B}\}$ such that

$$C = \{ c \in \mathcal{V} : r_\alpha(c) = 0 \text{ for all } \alpha \}.$$
**Proof:** From the definition of the induced topology we know that $C$ is closed if and only if there is an algebraic set $\mathcal{W} \subset \mathbb{B}^n$ such that

$$C = \mathcal{V} \cap \mathcal{W}.$$ 

Moreover, since $\mathcal{W}$ is algebraic we have $\mathcal{W} = \mathcal{V}(\{p_\alpha\})$ for some collection $\{p_\alpha\} \subset A[x] = A[x_1, x_2, \ldots, x_n]$. For each $\alpha$ define $r_\alpha := p_\alpha(x)|_\mathcal{V}$, and define $D := \{ c \in \mathcal{V} : r_\alpha(c) = 0 \text{ for all } \alpha \}$. The for any $c \in \mathbb{B}^n$ we have

$$c \in C \iff c \in \mathcal{V} \cap \mathcal{V}(\{p_\alpha\})$$

$$\iff c \in \mathcal{V} \text{ and } c \in \mathcal{V}(\{p_\alpha\})$$

$$\iff c \in \mathcal{V} \text{ and } p_\alpha(c) = 0 \text{ for all } \alpha$$

$$\iff c \in \mathcal{V} \text{ and } r_\alpha(c) = 0 \text{ for all } \alpha$$

$$\iff c \in D.$$ 

This gives $C = D$, and the proof is complete. 

* q.e.d. 

25
5. The Contemporary Combined Approach

In this section \( R \) denotes a ring and \( B \supset A \) is an extension of integral domains\(^{32}\). Keep in mind that “ring” always means “commutative ring with unity.”

Our work thus far can be summarized as the construction of two functors represented by the arrows in the following diagram of categories:

\[
\begin{array}{ccc}
\text{Classical } (A, B)-\text{affine algebraic sets} & \xrightarrow{\alpha} & \text{Reduced Rings} \\
\downarrow & \alpha & \downarrow \\
\text{Topological Spaces} & \beta & \text{Topological Spaces}
\end{array}
\]

Diagram 5.1

Viewed from this perspective it seems natural to ask if the picture can be completed to a triangular diagram by means of a horizontal arrow (in either direction) along the bottom. The answer is “yes,” although the custom is to go quite a bit further: one constructs a functor \( \gamma \) from the category of (commutative) rings (with unities) to the category of topological spaces which allows one to embed the picture above within a second commutative diagram

\[
\begin{array}{ccc}
\text{Classical } (A, B)-\text{affine algebraic sets} & \xrightarrow{\alpha} & \text{Reduced Rings} \\
\downarrow & \alpha & \downarrow \\
\text{Rings} & \xrightarrow{\iota} & \text{Topological Spaces}
\end{array}
\]

Diagram 5.2

In this augmented diagram the functor \( \iota \) is simply the inclusion of the indicated categories; our task is to define \( \gamma \) and \( \delta \), and this will take a bit of work.

Before we begin it is certainly fair to ask if there is any advantage to this larger framework. Absolutely: it formulates classical affine algebraic geometry within a context which makes transparent the connections with many other areas of mathematics, particularly algebraic number theory (which is one of the reasons we began with Fermat’s Last Theorem, and included examples of coordinate rings having number-theoretic connections\(^{33}\)).

\(^{32}\)Without the integral domain restriction there would be no \((A, B)\)-Zariski topology on classical \((A, B)\)-affine algebraic sets.

\(^{33}\)Recall Examples 3.2(c) and (d).
Our first task is the construction of the functor $\gamma$ appearing at the bottom of Diagram 5.2, and for this purpose the remainder of that diagram can be ignored. We begin by associating a set, and then a topological space, with the ring $R$.

The set we associate with $R$ is the collection of all prime ideals of this ring; this is the (prime) spectrum of $R$ and is denoted $\text{Spec}(R)$ (read “speck are”). Recall that prime ideals are (by definition) proper ideals, hence $R \notin \text{Spec}(R)$.

Examples 5.1 :

(a) The trivial ring $0$ has no prime ideals, hence $\text{Spec}(0) = \emptyset$.

(b) When $R$ is an integral domain the zero ideal $(0)$ is prime, hence $\text{Spec}(R) \neq \emptyset$.

(c) With the exception of the zero ideal the prime ideals of the ring $\mathbb{Z}$ of integers have the form $(p)$, where $p$ runs through the collection of prime numbers. One can therefore think of $\text{Spec}(\mathbb{Z})$ as the collection of prime numbers together with $0$.

(d) $\text{Spec}(R)$ is a one-point space if $R$ is a field; this is immediate from (b) and the fact that there are no other ideals. The converse, however, is false: $\text{Spec}(\mathbb{Z}_4)$ consists of the single prime ideal $\{[0], [2]\}$ (the ideal $([0])$ is not prime), but $\mathbb{Z}_4$ is not a field.

To endow $\text{Spec}(R)$ with a topology we first associate to each element $r \in R$ the subset $D(r) \subset \text{Spec}(R)$ defined by

\[
D(r) := \{ p \in \text{Spec}(R) : r \notin p \}.
\]

One then has

\[
(a) \quad D(0) = \emptyset;
(b) \quad D(1) = D(-1) = \text{Spec}(R); \quad \text{and}
(c) \quad D(rs) = D(r) \cap D(s),
\]

where in (c) the elements $r, s \in R$ are arbitrary. Indeed, (a) and (b) are immediate from the definition, and since any ideal $p \in \text{Spec}(R)$ is (by definition) prime we have

\[
p \in D(rs) \iff rs \notin p \iff r \notin p \text{ and } s \notin p \iff p \in D(r) \text{ and } p \in D(s) \iff p \in D(r) \cap D(s),
\]
thereby giving (c).

It is immediate from (5.3) that the collection \( \{ D(r) \}_{r \in R} \) is a basis for a topology on \( \text{Spec}(R) \). This is the Zariski topology, and \( \text{Spec}(R) \) is assumed endowed with this topology unless specifically stated to the contrary.

Of course the name “Zariski topology” was also used for the topology introduced in §4, and that topology is defined on a different space. This abuse of terminology is standard, and, since the meaning is usually clear from context, seldom causes problems.

Since our goal is to construct a functor from the category of rings to the category of topological spaces, our next task should be to construct a continuous mapping between such spaces from a given ring homomorphism. A ring-theoretic preliminary is required. When \( f : R \to S \) is a ring homomorphism and \( i \subset S \) is an ideal the preimage \( f^{-1}(i) \subset R \) is called the pull-back\(^{34}\) of \( i \) (by \( f \)).

**Proposition 5.4 :** Assume the notation of the previous paragraph. Then:

(a) the pull-back \( f^{-1}(i) \) is an ideal of \( R \);

(b) this pull-back is prime when \( i \) is prime;

(c) when \( f \) is surjective the image of any ideal \( j \subset R \) is an ideal of \( S \) and the correspondence \( j \mapsto f(j) \) is an order preserving bijection between the ideals of \( R \) containing \( \ker(f) \) and the ideals of \( S \); and

(d) when \( f \) is surjective the association \( p \subset S \mapsto f^{-1}(p) \subset R \) is an order preserving bijection between prime ideals of \( S \) and prime ideals of \( R \) containing \( \ker(f) \).

It is not true that \( f(i) \subset S \) is an ideal whenever \( j \subset R \) is an ideal, e.g., when \( f : \mathbb{Z} \to \mathbb{R} \) is inclusion the image of any non-zero ideal \( (n) \subset \mathbb{Z} \) is not an ideal. In particular, assertion (c) fails when the surjectivity hypothesis is dropped.

**Proof :**

(a) When \( r \in R \) and \( v, w \in f^{-1}(i) \) we see from \( f(v + w) = f(v) + f(w) \in i \) and \( f(rv) = f(r)f(v) \in i \) that \( v + w, rv \in f^{-1}(i) \).

(b) Suppose \( r, v \in R \) and \( rv \in f^{-1}(i) \). Then from \( f(r)f(v) = f(rv) \in i \) we see that \( f(r) \in i \) or \( f(v) \in i \), hence \( r \in f^{-1}(i) \) or \( v \in f^{-1}(i) \).

\(^{34}\)Some texts, e.g., [A-M], refer to \( f^{-1}(i) \) as the contraction of \( i \) in \( R \). I use “pull-back” because that term is used with analogous constructions in differential geometry.
(c) Suppose \( j \subseteq R \) is an ideal, \( r, v \in j \), and \( s \in S \), say \( s = f(w) \). Then from \( f(r + v) = f(r) + f(v) \), \( sf(r) = f(w)f(r) = f(wr) \) and \( wr \in j \) we see that \( f(j) \subseteq S \) is an ideal.

Order preservation is clear; to complete the proof of (c) it remains to show that any ideal \( j \subseteq R \) containing \( \ker(f) \) satisfies \( j = f^{-1}(f(j)) \). Since the inclusion \( j \subseteq f^{-1}(f(j)) \) is automatic this can fail only if there is an element \( r \in f^{-1}(f(j)) \setminus j \). If so then \( f(r) \in f(j) \), hence \( f(r) = f(v) \) for some \( v \in j \). It follows that \( r - v \in \ker(f) \subseteq j \), whence \( r \in j \), and we have a contradiction.

(d) It suffices, by (b) and (c), to prove that \( f(p) \subseteq S \) is prime whenever \( p \subseteq R \) is a prime ideal containing \( \ker(f) \). To this end suppose \( s, t \in S \) satisfy \( st \in f(p) \), and invoke the surjectivity hypothesis to choose \( r, v \in R \) such that \( f(r) = s \), \( f(v) = t \). Then from \( st \in f(p) \) and (c) we have \( rv \in p \), whence \( r \in p \) or \( s \in p \) (or both), and \( s = f(r) \in f(p) \) or \( t = f(v) \in f(p) \) follows.

q.e.d.

It is immediate from Proposition 5.4(b) that any ring homomorphism \( f : R \to S \) induces a mapping\(^{35}\) \( f^* : \text{Spec}(S) \to \text{Spec}(R) \), i.e.,

\[
(5.5) \quad f^* : p \in \text{Spec}(S) \mapsto f^{-1}(p) \in \text{Spec}(R).
\]

**Proposition 5.6** : When \( f : R \to S \) is a ring homomorphism the following assertions hold.

(a) For any \( r \in R \) one has

(i) \( (f^*)^{-1}(D(r)) = D(f(r)) \).

(b) When \( \text{Spec}(R) \) and \( \text{Spec}(S) \) are endowed with the Zariski topologies the mapping \( f^* : \text{Spec}(S) \to \text{Spec}(R) \) is continuous.

In (i) the sets \( D(r) \) and \( D(f(r)) \) are collections of prime ideals within \( R \) and \( S \) respectively. Notation such as \( D_R(r) \) and \( D_S(f(a)) \) would be helpful for keeping the distinction in mind, but is not customary.

\(^{35}\)The notation \( f^* \) (read \( f \) “upper star”) is from [A-M, Exercise 21, p. 13], and is consistent with notation used for analogous induced mappings in differential geometry. Another common notation for \( f^* \) is \( \dagger f \) (read “\( f \) adjoint”, “\( f \)’” or “the adjoint of \( f \)”).
Proof:

(a) For any $q \in \text{Spec}(S)$, i.e., for any prime ideal $q \subset S$, one has

\[ q \in (f^*)^{-1}(D(r)) \iff f^*(q) \in D(r) \]
\[ \iff f^{-1}(q) \in D(r) \]
\[ \iff r \notin f^{-1}(q) \]
\[ \iff f(r) \notin q \]
\[ \iff q \in D(f(r)), \]

and (i) follows.

(b) Since $\{D(r)\}_{r \in R}$ is a basis for the Zariski topology on any ring $R$, this is immediate from (a).

q.e.d.

Corollary 5.7: Any surjective ring homomorphism $f : R \rightarrow S$ induces a continuous injection $f^* : \text{Spec}(S) \rightarrow \text{Spec}(R)$ having as range those prime ideals containing $\ker(f)$. Indeed, the mapping $f^*$ is an embedding, i.e., a homeomorphism onto this range (when this range is given the induced topology).

Proof: The initial assertion is immediate from Proposition 5.6 and Proposition 5.4(d). To verify the final assertion we need the following observation: for any $p \in \text{Spec}(R)$ not containing $\ker(f)$ and any $r \in R$ one has

(i) \[ f(r) \in f(p) \iff r \in p. \]

Indeed, $f(r) \in f(p)$ holds if and only if $r \in f^{-1}(f(p))$, and $f^{-1}(f(p)) = p$ by Proposition 5.4(d).

We claim that for any $r \in R$ we have

(ii) \[ f^*(D(f(r))) = D(r). \]

To verify this simply note that for any $p \in \text{Spec}(R)$ not containing $\ker(f)$ we have

\[ p \in f^*(D(f(r))) \iff p \in f^{-1}(D(f(r))) \]
\[ \iff f(p) \in D(f(r)) \]
\[ \iff f(r) \notin f(p) \]
\[ \iff r \notin p \quad (\text{by (i)}) \]
\[ \iff p \in D(r). \]

The continuity of $(f^*)^{-1}$ is immediate from (ii).

q.e.d.
Theorem 5.8: Assigning $\text{Spec}(R)$ to each (commutative) ring $R$ (with unity) and $f^*: \text{Spec}(S) \to \text{Spec}(R)$ to each ring homomorphism $f: R \to S$ constitutes a contravariant functor $\gamma$ from the category of rings and ring homomorphisms to the category of topological spaces and continuous functions.

Proof: Verification of the properties required of a functor is again routine. q.e.d.

We now have two covariant functors from the category of classical $(A,B)$-affine algebraic sets and $(A,B)$-morphisms to the category of topological spaces and continuous functions: the composition of the functors $\alpha$, $\iota$ and $\gamma$ of Theorem 3.10, Diagram 5.2 and Theorem 5.8, and the functor $\beta$ of Theorem 4.10 and Diagram 5.1. The functor $\delta$ of Diagram 5.2 is now defined by composition in the obvious way. We begin by forgetting topological structure so as to construct the inverse of the functor $\beta$, i.e., we assign to any classical $(A,B)$-affine algebraic set with the $(A,B)$-Zariski topology the underlying classical $(A,B)$-affine algebraic set, and we assign to any continuous mapping between such topological spaces (within the range of $\beta$) to the classical $(A,B)$-morphism which induced that continuous function. (As set functions the continuous function and morphism are identical, and the assignment is therefore unambiguous, i.e., it involves no choices). We then define $\delta := \gamma \circ \iota \circ \alpha \circ \beta^{-1}$ and, by construction, obtain the desired commutativity of Diagram 5.2.

At the object level the functor $\delta$ assigns, to each classical $(A,B)$-affine algebraic set $V \subseteq B^n$ with the $(A,B)$-Zariski topology, the topological space $\text{Spec}(A_B[V])$. Although it is not relevant at the categorical level, this suggests that it might be possible to define a function from $V$ into $\text{Spec}(A_B[V])$. This is our next goal. A few preliminaries are necessary.

For any point $c = (b_1, b_2, \ldots, b_n) \in B^n$ the collection

$$i(\{c\}) := \{ p \in A[x] : p(c) = 0 \}$$

is easily seen to be an ideal of $A[x] = A[x_1, x_2, \ldots, x_n]$. It is the defining $(A,B)$-ideal\textsuperscript{37} of $c$.

\textsuperscript{36}The functor $\delta$ simply assigns $V$ to $\text{Spec}(A_B[V])$; it does not assign points of $V$ to points of $\text{Spec}(A_B[V])$.

\textsuperscript{37}Since a singleton subset $\{c\} \subseteq B^n$ need not be algebraic, this definition cannot be regarded as a special case of (3.1).
Examples 5.10: Suppose $\mathbb{Z} \subset A \subset B = \mathbb{R}$ and $x$ is a single indeterminate over $B$. Let $c := \sqrt{2} \in \mathbb{R}$.

(a) When $A = \mathbb{Z}$ we have \(^{38} i(\{c\}) = (x^2 - 2) \subset \mathbb{Z}[x].

(b) When $A = B = \mathbb{R}$ we have $i(\{c\}) = (x - \sqrt{2}) \subset \mathbb{R}[x].$

Proposition 5.11: When $B$ has infinitely many elements and $n$ is a positive integer the following assertions hold.

(a) The defining $(A, B)$-ideal $i(\{c\}) \subset A[x]$ of any point $c = (b_1, b_2, \ldots, b_n) \in \mathbb{B}^n$ is prime.

(b) Suppose $\mathcal{V} \subset \mathbb{B}^n$ is an algebraic set, $f : A[x] \to A_B[\mathcal{V}]$ is the canonical homomorphism onto the coordinate ring of $\mathcal{V}$, and $c \in \mathcal{V}$. Then $\ker(f) \subset i(\{c\}).$

(c) When $\mathcal{V} \subset \mathbb{B}^n$, $c \in \mathcal{V}$ and $f : A[x] \to A_B[\mathcal{V}]$ are as in (b) the image $f(i(\{c\})) \subset A_B[\mathcal{V}]$ is a prime ideal.

Recall that $B$ is assumed an integral domain throughout the section.

Proof:

(a) Suppose $p, q \in A[x]$ and $p, q \in i := i(\{c\})$. Then $0 = (pq)(c) = p(c)q(c)$, and since $B$ is an integral domain this forces either $p(c) = 0$ or $q(c) = 0$, i.e., $p \in i$ or $q \in i$ (or both). This proves the result so long as the ideal $i$ is proper, and that is guaranteed by the cardinality hypothesis on $B$.

(b) For $p \in A[x]$ we have $p \in \ker(f)$ if and only if $p(b_1, b_2, \ldots, b_n) = 0$ for all $(b_1, b_2, \ldots, b_n) \in \mathcal{V}$. Since $c$ is assumed in $\mathcal{V}$, $p(c) = 0$ follows, hence $p \in i(\{c\})$.

(c) Use (a), (b), and Proposition 5.4(d).

q.e.d.

Assume the hypotheses of Proposition 5.11, let $\mathcal{V} \in \mathbb{B}^n$ be a classical $(A, B)$-affine algebraic set endowed with the $(A, B)$-Zariski topology, and let $f : A[x] \to A_B[\mathcal{V}]$ be the canonical (surjective) homomorphism. Then a mapping $\varphi_\mathcal{V} : \mathcal{V} \to \text{Spec}(A_B[\mathcal{V}])$ is defined by

$$
(5.12) \quad \varphi_\mathcal{V} : c \in \mathcal{V} \mapsto f(i(\{c\})) \in \text{Spec}(A_B[\mathcal{V}]).
$$

\(^{38}\text{Argue as in Footnote 9. (The notations } (x^2 - 2) \text{ and } (x - \sqrt{2}) \text{ indicate principal ideals of the indicated rings.)} \)
It can be useful to imagine $\varphi_V(V) \subset \Spec(A_B[V])$ as the “image” of $V$ under the functor $\delta$. Indeed, with an eye on Diagram 5.2 recall that $\beta^{-1}$ is forgetful; it simply strips the topology from $V$ and therefore carries $c \in V$ to $c \in V$. One then imagines $\alpha$ and $\iota \circ \alpha$ as carrying $c$ to the prime ideal $f(i(\{c\})) \subset A_B[V]$, and of $\gamma$ as converting this prime ideal to the point $\varphi_V(c)$ of $\Spec(A_B[V])$.

**Proposition 5.13:** Let $\varphi_V : V \to \Spec(A_B[V])$ be defined as in (5.12). Then:

(a) for any $p \in A[x]$ one has

\[
\varphi_V^{-1}(D(f(p))) = V \setminus V(f(p));
\]

and

(b) $\varphi_V$ is continuous.

**Proof:** In the proof we denote cosets in $A_B[V]$ with brackets $[\;]$. In particular, we write (i) as

\[
\varphi_V^{-1}(D([p])) = V \setminus V(\{p\}).
\]

(a) Choose any $c \in \mathcal{W}$ and observe that

\[
f(p) \in f(i(\{c\})) \iff p \in i(\{c\}).
\]

Indeed, the forward implication is immediate from Proposition 5.4(d), and the reverse is obvious. It follows that

\[
c \in \varphi_V^{-1}(D([p])) \iff \varphi_V(c) \in D([p])
\]

\[
\iff f(i(\{c\})) \in D([p])
\]

\[
\iff [p] \notin f(i(\{c\}))
\]

\[
\iff f(p) \notin f(i(\{c\}))
\]

\[
\iff p \notin i(\{c\}) \quad (\text{by (ii)})
\]

\[
\iff p(c) \neq 0
\]

\[
\iff c \in V \setminus V(\{p\}),
\]

---

39So long as one does not take the discussion in this paragraph too seriously: under closer scrutiny many of the statements are easily seen to be unsupportable.

40When $A$ and $B$ are subsets of a set $C$ we denote the *difference* $\{ c \in A : c \notin B \}$ of $A$ and $B$ by $A \setminus B$. (It is not assumed that $B \subset A$.)
and \((i')\) is thereby established.

(b) The collection \(\{D([q])\}_{q \in A_B[V]}\) is a basis for the Zariski topology on \(\text{Spec}(A_B[V])\), and and \(V(\{p\})\) is closed in \(\mathbb{B}^n\). The result is therefore immediate from (a).

\[\text{q.e.d.}\]

This idea of “pushing” an algebraic set \(V\) into \(\text{Spec}(A_B[V])\) (as in (5.12)) has proven so successful that many contemporary algebraic geometry texts, after paying the obligatory lip service to the origins of the subject, immediately launch into the study of prime spectra of rings and the associated sheaves and schemes (whatever these may be). When these objects are well-understood one can recapture the classical settings up to isomorphism, and one can therefore argue that nothing has been lost. Admittedly, tremendous generality has been gained, but these modern treatments often sacrifice geometric intuition, at least at the outset, when this is not really necessary\textsuperscript{41}.

We will have more to say about the mapping (5.12) after introducing a few new ideas and refining several of those developed thus far.

\textsuperscript{41}It has not escaped this author’s thinking that one could criticize the presentation in these notes on precisely the same grounds. The problem is: a considerable amount of material must be presented before one can achieve any real benefits, and there is always the possibility that dwelling too long on background material will kill all interest on the part of readers, even those who arrived on the scene with good intentions.
6. A Generalization of Affine Algebraic Sets

We need a few basic ideas from category theory.

Let $\mathcal{C}$ and $\mathcal{D}$ be arbitrary categories, and let $\mathcal{S}$ be the category of sets and set mappings.

(a) A functor $T : \mathcal{C} \to \mathcal{D}$ is \textit{faithful} if for any two objects $C_1, C_2$ of $\mathcal{C}$ and any two morphisms $C_1 \xrightarrow{f_1} C_2, C_1 \xrightarrow{f_2} C_2$ one has $f_1 = f_2$ if $Tf_1 = Tf_2$. Examples: the forgetful functor on the category of groups and group homomorphisms and the forgetful functor on the category of topological spaces and continuous mappings. (The definition is from [M, Chapter I, §3, p. 14].)

(b) The category $\mathcal{C}$ is \textit{concrete} if there is a faithful functor $T : \mathcal{C} \to \mathcal{S}$, and when this is the case and $C$ is an object of $\mathcal{C}$ one refers to $TC$ as the \textit{underlying set (of $C$)}. Faithfulness allows one to view each morphism in $\mathcal{C}$ as a set mapping between the underlying sets. Examples: The category of topological spaces and continuous mappings is concrete. Indeed, when one defines a topological space as a pair $(X, \tau)$, with $\tau$ the topology (i.e., the collection of subsets forming the topology), the underlying set is $X$. Similarly, the category of groups and group homomorphisms is a concrete category. (The definition is from [M, Chapter I, §7, p. 26]. For a somewhat less formal definition see [H, Chapter I, §7, Definition 7.6, p. 55].)

(c) Let $\mathcal{C}$ be a concrete category, let $X$ be a set, let $C$ be an object of $\mathcal{C}$, and let $\iota : X \to C$ be a set mapping. The object $C$ is \textit{free on $X$} if for any object $B$ of $\mathcal{C}$ and any set mapping $f : X \to B$ there is a unique morphism $f_C : C \to B$ which makes the diagram

\[
\begin{array}{ccc}
C & \xrightarrow{f_C} & B \\
\iota \uparrow & & \nearrow f \\
X & & \\
\end{array}
\]

of set mappings commute. Example: When $A$ is a ring the polynomial algebra $A[x] = A[x_1, x_2, \ldots, x_n]$ is free on the set $X := \{x_1, x_2, \ldots, x_n\}$ of (algebraically independent) indeterminates. (The definition is from [H, Chapter I, §7, Definition 7.7, p. 55].)
Let \( C \) be a concrete category and let \( C \) be an object of \( C \) which is free on a non-empty finite set \( X = \{x_1, x_2, \ldots, x_n\} \). Fix an object \( D \) of \( C \) and consider:

- the set \( \text{mor}(C, D) \) of morphisms from \( C \) to \( D \);
- the set \( \mathcal{F}(X, D) \) of functions from \( X \) to \( D \); and
- the set \( D^n := D \times D \times \cdots \times D \) of \( n \)-tuples of elements of \( D \), wherein \( D \) and the Cartesian product are considered as sets.

From the definition of “free” the first two sets are in bijective correspondence. Specifically, a bijection \( \alpha : \text{mor}(C, D) \rightarrow \mathcal{F}(X, D) \) is given by the restriction mapping

\[
\alpha : f \in \text{mor}(C, D) \mapsto f|X \in \mathcal{F}(X, D).
\]

The second and third sets are also in bijective correspondence: in this case a bijection \( \beta : \mathcal{F}(X, D) \rightarrow D^n \) is given by

\[
\beta : g \in \mathcal{F}(X, D) \mapsto (g(x_1), g(x_2), \ldots, g(x_n)) \in D^n.
\]

Using these bijections one can define, for each element \( c \in C \), a function \( \varphi_c : D^n \rightarrow D \), i.e.,

\[
\varphi_c : (d_1, d_2, \ldots, d_n) \in D^n \mapsto ((\alpha^{-1} \circ \beta^{-1})(d_1, d_2, \ldots, d_n))(c) = ((\beta \circ \alpha)^{-1})(d_1, d_2, \ldots, d_n))(c).
\]

Now fix an element \( d_0 \in D \) and let \( \mathcal{P} \) be any collection of elements of \( C \). We define the abstract\(^{42} \) affine algebraic set \( \mathcal{V}(\mathcal{P}) \subset D^n \) (corresponding to \( \mathcal{P} \)) to be \( \cap_{c \in \mathcal{P}} \varphi_c^{-1}(\{d_0\}) \), i.e.,

\[
\mathcal{V}(\mathcal{P}) := \{ (d_1, d_2, \ldots, d_n) \in D^n : \varphi_c(d_1, d_2, \ldots, d_n) = d_0 \ \text{for all} \ c \in \mathcal{P} \}.
\]

The idea is hopefully clear: the distinguished element \( d_0 \) plays the role of \( 0 \) in classical affine algebraic geometry.

**Examples 6.5 :**

(a) Let \( B \supset A \) be an extension of integral domains and let \( C \) be the category of \( A \)-algebras, which we note is concrete. Choose algebraically independent elements \( x_1, x_2, \ldots, x_n \) over \( B \), wherein \( n \geq 1 \), and take \( C := B[x] := B[x_1, x_2, \ldots, x_n] \), \( D := B \), and \( d_0 := 0 \). Then \( C \) is free on \( \{x_1, x_2, \ldots, x_n\} \) and

\(^{42}\)The terminology proves to be convenient, but is not standard.
all conditions in the discussion above are satisfied. For \((d_1, d_2, \ldots, d_n) \in D^n\) the morphism \((\beta \circ \alpha)^{-1} \in \text{mor}(C, D)\) is simply evaluation at \((d_1, d_2, \ldots, d_n)\) and \(\mathcal{V}(\mathcal{P})\), for any collection \(\mathcal{P} \subset A[x] := A[x_1, x_2, \ldots, x_n]\), is the classical \((A, B)\)-algebraic set defined by \(\mathcal{P}\).

(b) In the subject of differential algebraic geometry one mimics the situation in (a) by replacing \(B[x]\) with \(B\{x\} = B\{x_1, x_2, \ldots, x_n\}\), wherein \(B \supset A\) is a differential ring extension and the \(x_j\) are “differential indeterminates,” this last condition having the implication that \(B[x]\) is free on the set \(\{x_1, x_2, \ldots, x_n\}\). In this context sets of the form \(\mathcal{V}(\mathcal{P}) \subset B^n\) are called differential algebraic sets, and one can construct analogues of the functors we have developed for the classical \((A, B)\)-affine algebraic sets. Defining ideals become defining differential ideals, and \(\text{Spec}(R)\) is replaced by \(\text{DifSpec}(R)\) (read “diff speck are”).

(c) There are even more abstract variations on the notion of an algebraic set, e.g., see [B-M-R], where one works in a category of groups and defining ideals are replaced by defining normal subgroups.
Part II - Topological Considerations

In Part II we concentrate on the topological aspects of affine algebraic geometry. So far as seems reasonable we keep the treatment fairly general, although not in §7. The main result of Part II is Theorem 9.15, which shows that when \( B \) is an integral domain, any classical \((A, B)\)-affine algebraic set decomposes into a finite number of “irreducible components.” This is somewhat analogous to factoring an integer into a finite product of primes.

When \( X \) is a non-empty set the complement \( X \setminus Y \) in \( X \) of a subset \( Y \subset X \) is denoted \( Y^c \).

7. Zariski Closures

The Case of Classical Affine Algebraic Sets

In this subsection \( B \supset A \) is an extension of rings, \( n \) is a positive integer, and \( A[x] = A[x_1, x_2, \ldots, x_n] \) is the usual polynomial algebra in \( n \)-variables.

The \((A, B)\)-Zariski topology on \( B^n \) was defined in terms of the association between ideals \( \mathfrak{i} \subset A[x] \) and their corresponding zero sets \( \mathcal{V}(\mathfrak{i}) \subset B^n \) (under the assumption that \( B \) is an integral domain). We can get a deeper understanding of the closed sets in this topology by generalizing definition (3.1) beyond classical \((A, B)\)-affine algebraic sets. Specifically, given any subset \( C \subset B^n \) we generalize (3.1) and (5.9) simultaneously by setting

\[
\mathfrak{i}(C) := \{ p \in A[x] : p(c) = 0 \text{ for all } c = (c_1, c_2, \ldots, c_n) \in C \}.
\]

This is easily seen to be an ideal; it is the defining \((A, B)\)-ideal of \( C \), or simply the defining ideal of \( C \) when the extension \( B \supset A \) is understood. We have already seen examples, i.e., immediately following (2.1) and in Examples 5.10.

Proposition 7.1 : When \( B \) is reduced the defining ideal of any subset of \( B^n \) is radical.

The proof is essentially the same as that of Proposition 3.7.

Proof : If \( p \in A[x] \) satisfies \( p^m \in \mathfrak{i}(C) \) for some integer \( m \geq 1 \) then \( 0 = p^m(c) = (r(c))^m \) for all \( c \in C \). By hypothesis this gives \( p(c) = 0 \) for all such \( c \), hence \( p \in \mathfrak{i}(C) \). q.e.d.
In analogy with (4.1) note that for any subsets $C, D \subseteq B^n$ one has

\[(7.2) \quad C \subseteq D \implies i(D) \subseteq i(C).\]

Indeed, for $p \in A[x]$ we have $p \in i(D)$ if and only if $p(d) = 0$ for all $d \in D$. The inclusion $C \subseteq D$ then guarantees that $p(c) = 0$ for all $c \in C$, hence $p \in i(C)$.

**Proposition 7.3**: Suppose $C \subseteq B^n$ and $i \subseteq A[x]$ is an ideal. Then the following assertions hold.

(a) $i(B^n) = \{ p \in A[x] : p(x) \text{ is the zero function} \}$ and $i(\emptyset) = A[x]$.

(b) $i \subseteq i(V(i))$.

(c) $C \subseteq V(i)$.

(d) $C \subseteq V(i) \implies i \subseteq i(C)$.

(e) $C \subseteq V(i) \implies V(i)$.

Assertion (b) was already noted in (4.4), where it was pointed out that the inclusion can be proper. The inclusion in (c) can also be proper. For example, take $A = \mathbb{Z}$, $B = \mathbb{C}$, $n = 1$ and $C = \{i\} \subseteq B = B^1$. Then $i(C) = (x^2 + 1)$ and $\{-i, i\} = V(i(C)) \neq C$.

Useful pictures to keep in mind for (b) and (c) are:

<table>
<thead>
<tr>
<th>ideals</th>
<th>subsets</th>
<th>ideals</th>
<th>subsets</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i$</td>
<td></td>
<td>$V(i)$</td>
<td></td>
</tr>
<tr>
<td>$i \leftarrow V(i)$</td>
<td>$\downarrow$</td>
<td>$j \rightarrow V(i)$</td>
<td>$\nearrow$</td>
</tr>
<tr>
<td>inc $\downarrow$</td>
<td>$C \rightarrow i(C)$</td>
<td>$\uparrow$ inc</td>
<td>$D \rightarrow i(D)$</td>
</tr>
<tr>
<td>$i(V(i))$</td>
<td></td>
<td>$i(C)$</td>
<td></td>
</tr>
<tr>
<td>(b)</td>
<td></td>
<td>(c)</td>
<td></td>
</tr>
</tbody>
</table>

39
Proof:
(a) This initial assertion is immediate from the definition of $i(B^n)$. The second equality holds since anything implied by a false premise must be true: $x \in \emptyset \Rightarrow p(x) = 0$ must hold for all polynomials $p \in A[x]$.

(b) As noted above, this result was already given in (4.4).

(c) $p \in i(C)$ and $c \in C$ imply $p(c) = 0$, hence $c \in V(i(C))$.

(d) If $p \in i$ and $c \in C$ then $C \subset V(i) \Rightarrow p(c) = 0 \Rightarrow p \in i(C)$.

(e) By (d) and (4.1).

Recall that when $X$ is a topological space we denote the closure of any subset $S \subset X$ by $\text{cl}(S)$.

Corollary 7.4: Suppose $B$ is an integral domain and $C, D \subset B^n$. Assume the $(A, B)$-Zariski topology on $B^n$. Then:

(a) $\text{cl}(C) = V(i(C))$;

(b) $C$ is Zariski closed if and only if $C = V(i(C))$; and

(c) when $C$ and $D$ are (Zariski) closed one has $C = D$ if and only if $i(C) = i(D)$.

The assertion of (a), in simple English, is this: a point $c \in B^n$ is in the closure of $C$ if and only if every polynomial which vanishes on $C$ also vanishes on $c$. To see a specific example assume the notation of Examples 5.10; in particular, let $C = \{ \pm \sqrt{2} \}$. Then for $A = \mathbb{Z}$ and $B = \mathbb{R}$ we have $\text{cl}(C) = \{ \pm \sqrt{2} \} = V((x^2 - 2))$, i.e., $c = \pm \sqrt{2}$ (are the two possibilities for $c$), whereas for $A = B = \mathbb{R}$ we have $\text{cl}(C) = \{ \sqrt{2} \} = V((x - \sqrt{2}))$, i.e., $c = \sqrt{2}$ (is the only possibility for $c$).

Proof:
(a) Any closed set containing $C$ has the form $V(i)$ for some ideal $i \subset A[x]$, and by Proposition 7.3(c) this is the case for $V(i(C))$. The result is then immediate from Proposition 7.3(c).

(b) By (a).

(c) The forward implication does not require proof, and when $i(C) = i(D)$ we see from (b) that $C = V(i(C)) = V(i(D)) = D$.

q.e.d.
Corollary 7.5 : Suppose $B$ is an integral domain, $A = B$, and $n \geq 1$ is an integer. Then for any point $c = (b_1, b_2, \ldots, b_n) \in \mathbb{B}^n$ one has

(i) $\mathcal{V}(i(\{c\})) = \{c\},$

and any singleton subset of $\mathbb{B}^n$ is therefore $(B, B)$-Zariski closed. Moreover,

(ii) $i(\{c\}) \neq B[x].$

**Proof :** From Example 3.2(e) we have $i(\{c\}) = (x_1 - b_1, x_2 - b_2, \ldots, x_n - b_n),$ and $c \in \mathcal{V}(i(\{c\}))$ follows easily. If $e = (d_1, d_2, \ldots, d_n) \in \mathcal{V}(i(\{c\}))$ then each of the polynomials $x_j - b_j \in A[x] = B[x],$ must vanish on $e,$ hence $b_j = d_j$ for all $j,$ $e = c$ follows, and (i) is thereby established.

As for (ii): if $i(\{c\}) = B[x]$ then (i) and Theorem 4.5(a) would yield the contradiction $\{c\} = \mathcal{V}(i(\{c\})) = \mathcal{V}(B[x]) = \emptyset.$ \hfill q.e.d.

Corollary 7.6 : Suppose $B$ is an integral domain, $\mathcal{W} \subset \mathbb{B}^n$ is an algebraic set, and $f : A[x] \rightarrow AB[\mathcal{W}]$ is the canonical epimorphism. Then

$$\mathcal{W} = \mathcal{V}(\ker(f)).$$

**Proof :** For any $c = (b_1, b_2, \ldots, b_n) \in B^n$ we have

$$c \in \mathcal{V}(\ker(f)) \iff p(c) = 0 \text{ for all } p \in \ker(f) \iff p(c) = 0 \text{ for all } p \in A[x] \text{ such that } p(x)|_{\mathcal{W}} \equiv 0 \iff c \in \mathcal{W},$$

the last equivalence by Corollary 7.4(a) and the fact that algebraic sets are (by definition) closed. \hfill q.e.d.

Thus far we have concentrated on the $(A, B)$-Zariski topology on $B^n.$ We now turn our attention to the (induced) $(A, B)$-Zariski topology on algebraic subsets thereof.

Corollary 7.7 : Suppose $B$ is an integral domain and $\mathcal{W} \subset \mathbb{B}^n$ is an algebraic set. Then for any subset $C \subset \mathcal{W}$ the following assertions hold:

(a) the closure of $C$ in the $(A, B)$-Zariski topology on $\mathcal{W}$ is $\mathcal{V}(i(C)),$ i.e., it coincides with the closure of $C$ in the $(A, B)$-Zariski topology on $B^n$;
(b) the following statements are equivalent:

(i) \( C \) is closed in the induced \((A, B)\)-Zariski topology on \( \mathcal{W} \);
(ii) \( C \) is closed in the \((A, B)\)-Zariski topology on \( B^n \); and
(iii) \( C = \mathcal{V}(i(C)) \);

and

(c) when \( C \) and \( D \subset \mathcal{W} \) are \((A, B)\)-Zariski closed (in the induced \((A, B)\)-Zariski topology) one has \( C = D \) if and only if \( i(C) = i(D) \) (both ideals being ideals of \( A[x] \)).

In the following proof sets relating to the induced \((A, B)\)-Zariski topology are indicated with the subscript \( \mathcal{W} \); unscripted topological symbols refer to the \((A, B)\)-Zariski topology on \( B^n \). To ease notation we drop the prefix \((A, B)\) throughout the argument.
Proof:

(a) Let \( \{X_\alpha\}_\alpha \) denote the family of closed sets (of the induced topology) which contain \( C \). Then for each index \( \alpha \) there is a Zariski closed set \( Y_\alpha \) (in the topology on \( \mathbb{B}^n \)) such that \( X_\alpha := Y_\alpha \cap \mathcal{W} \). By definition we have \( \text{cl}_\mathcal{W}(C) = \cap_\alpha X_\alpha \), hence

\[
\text{cl}_\mathcal{W}(C) = \cap_\alpha X_\alpha \\
= \cap_\alpha (Y_\alpha \cap \mathcal{W}) \\
= (\cap_\alpha (Y_\alpha)) \cap \mathcal{W} \\
= \cap_\alpha Y_\alpha,
\]

the last equality since \( \mathcal{W} \) is among the collection \( \{Y_\alpha\}_\alpha \). We claim that \( \cap_\alpha Y_\alpha = \text{cl}(C) \). Indeed, since \( \text{cl}(C) \subset \cap_\alpha Y_\alpha \) obviously holds, there would otherwise be a Zariski closed set \( K \) (in the topology on \( \mathbb{B}^n \)) containing \( C \) such that \( (\cap_\alpha Y_\alpha) \cap K \) is a proper subset of \( \cap_\alpha Y_\alpha \). This, however, would imply that the closed set \( (\cap_\alpha Y_\alpha) \cap (K \cap \mathcal{W}) \) is a proper subset of \( \cap_\alpha Y_\alpha \), thereby contradicting \( \text{cl}_\mathcal{W}(C) = \cap_\alpha Y_\alpha \). We conclude that \( \text{cl}_\mathcal{W}(C) = \text{cl}(C) \), and (a) is then immediate from Corollary 7.4(a).

(b) By (a).

(c) Use Corollary 7.4(c).

q.e.d.

The Case of the Prime Spectrum of a Ring

In this subsection \( R \) denotes a ring and \( \text{Spec}(R) \) is the prime spectrum of \( R \).

A deeper study of the Zariski closed sets of \( \text{Spec}(R) \) requires algebraic preliminaries.

A subset \( S \subset R \) is multiplicative if it is closed under multiplication and contains 1. Examples: \( S = R \setminus \{0\} \) when \( R \) is an integral domain; \( S = R \setminus \mathfrak{p} \) when \( \mathfrak{p} \subset R \) is any prime ideal; the set \( \{1, r, r^2, r^3, \ldots \} \) for any \( r \in R \).

**Proposition 7.8 (Krull\textsuperscript{43})**: Suppose \( S \subset R \) is a non-empty multiplicative subset and \( \mathfrak{i} \subset R \) is an ideal disjoint from \( S \). Then the collection of ideals of \( R \) which contain \( \mathfrak{i} \) and are disjoint from \( S \) admits a maximal element, and any such maximal element must be prime.

\[\text{43} \text{The attribution to Krull is from [Ku, Chapter 1, §4, p. 23].}\]
“Maximal” means: maximal w.r.t. the inclusion relation, i.e., there is no ideal disjoint from \( S \) which contains the asserted prime ideal as a proper subset.

To illustrate the result let \( R = \mathbb{Z}[x] \) (one variable), let \( S = 2\mathbb{Z} \subset \mathbb{Z} \subset R \) and let \( i = (x^2) \). Then \( p := (x) \) is a prime ideal which contains \( i \), is disjoint from \( S \), and is maximal w.r.t. these two properties.

**Proof:** The collection \( Y \) of all ideals of \( R \) containing \( i \) having empty intersection with \( S \) contains \( i \), hence is non-empty, and is inductively ordered by inclusion; Zorn’s Lemma therefore guarantees a maximal element.

To prove any such maximal element \( p \) is prime suppose, to the contrary, that there are elements \( a, b \in R \setminus p \) satisfying \( ab \in p \). From the maximality of \( p \) the ideal generated by \( p \) and \( a \) must contain an element \( s_a \in S \), say \( s_a = ma + xp \) with \( m, x \in R \) and \( p \in p \). Repeating the argument with \( a \) replaced by \( b \) we conclude that there is an element \( s_b \in S \) of the form \( nb + yq \) with \( n, y \in R \) and \( q \in p \). Multiplication then gives \( s_a s_b = mnab + r \), with the left-hand side in \( S \) (by the multiplicative assumption) and the right-hand side in \( p \) (because \( ab \in p \) and \( r := mayq + nbxp + xpyq \in p \)). Since \( 0 \notin S \) this contradicts \( p \cap S = \emptyset \), and we conclude that at least one of \( a \) and \( b \) must be contained in \( p \). \( \text{q.e.d.} \)

**Corollary 7.9:** When \( S \subset R \) is a multiplicative set not containing 0 the collection of ideals of \( R \) disjoint from \( S \) contains a maximal element, and any such maximal element must be prime.

**Proof:** Take \( i = (0) \) in Proposition 7.8. \( \text{q.e.d.} \)

**Corollary 7.10:** Suppose \( i \subset R \) is an ideal and \( r \in R \) is an element satisfying \( r^n \notin i \) for all integers \( n \geq 1 \). Then there is a prime ideal \( p \) containing \( i \) such that \( r^n \notin p \) for all integers \( n \geq 1 \).

**Proof:** Take \( S = \{1, r, r^2, r^3, \ldots \} \) in Proposition 7.8. \( \text{q.e.d.} \)

We also need some additional results on radical ideals.

**Proposition 7.11:**

(a) The collection of radical ideals of \( R \) is closed under arbitrary intersection.

Moreover, for any ideal \( i \subset R \) the following assertions hold.

(b) \( \sqrt{\sqrt{i}} = \sqrt{i} \), i.e., the radical of any ideal is a radical ideal.
(c) For any prime ideal \( p \subset R \) one has

\[ i \subset p \iff \sqrt{i} \subset p. \]

(d) The radical \( \sqrt{i} \) of \( i \) is the intersection of all prime ideals containing \( i \).

(e) An ideal of \( R \) is radical if and only if it is the intersection of all the prime ideals which contain it.

**Proof:**

(a) Suppose \( \{i_\alpha\} \) is a collection of radical ideals of \( R \), \( i := \cap_\alpha i_\alpha \), and \( r \in R \) satisfies \( r^n \in i \) for some integer \( n \geq 1 \). Then \( r^n \in i_\alpha \) for each \( \alpha \), hence \( r \in i_\alpha \), and \( r \in i \) follows.

(b) This is a restatement of Proposition 3.5. (The result is repeated above for ease of reference.)

(c) \[ \Rightarrow i \subset p \Rightarrow \sqrt{i} \subset \sqrt{p}, \text{ and } \sqrt{p} = p \text{ since prime ideals are radical (Proposition 3.4)}. \]

\[ \Leftarrow \] Immediate from \( i \subset \sqrt{i} \).

(d) Let \( \mathcal{I} \) denote the intersection of all those prime ideals of \( R \) containing \( i \).

The inclusion \( \sqrt{i} \subset \mathcal{I} \) is immediate from (c).

To prove the reverse inclusion note that for any \( r \in R \setminus \sqrt{i} \) one has \( r^n \not\in i \) for all integers \( n \geq 1 \), and so by Corollary 7.10 there is a prime ideal \( p \) containing \( i \) but not containing \( r \). This gives \( r \not\in \mathcal{I} \), whence \( \mathcal{I} \subset \sqrt{i} \), and the proof of (d) is complete.

(e) Let \( \mathcal{I} \) be as in the proof of (d).

\( \Rightarrow \) : When an ideal \( i \subset R \) is radical we have \( i = \sqrt{i} \), whence \( i = \mathcal{I} \) by (d).

\( \Leftarrow \) : We have already noted that prime ideals are radical, and by (a) the same must be true of \( \mathcal{I} \).

**q.e.d.**

This ends the algebraic preliminaries; we can turn to a study of the Zariski topology on \( \text{Spec}(R) \).

For any subset \( S \subset R \) define

\[ V(S) := \{ p : S \subset p \} \subset \text{Spec}(R), \]

(7.12)
and when \( S = \{ s \} \) is a singleton write \( V(s) \) for \( V(\{ s \}) \). Since prime ideals of \( R \) must be proper, it is immediate from this definition that

\[
\text{(7.13)} \quad V(R) = \emptyset.
\]

In terms of this notation we can reformulate Corollary 5.7 as follows.

**Proposition 7.14:** Any surjective ring homomorphism \( f : R \to S \) induces a homeomorphism \( f^* : \text{Spec}(S) \to V(\ker(f)) \) onto the subset \( V(\ker(f)) \subset \text{Spec}(R) \).

The basic properties of the sets \( V(S) \) are (by no accident) reminiscent of those described in Proposition 4.3 and Theorem 4.5 for algebraic sets.

**Proposition 7.15:**

(a) \( V(r) = \text{Spec}(R) \setminus D(r) \) for any \( r \in R \). In particular, each \( V(r) \) is closed.

(b) For any subset \( S \subset R \) one has

\[
V(S) = \cap_{s \in S} V(s).
\]

In particular, each \( V(S) \) is closed.

(c) For subsets \( S, T \subset R \) one has

\[
S \subset T \implies V(T) \subset V(S).
\]

(d) For any collection \( \{ S_\alpha \} \) of subsets of \( R \) one has

\[
V(\bigcup_\alpha S_\alpha) = \bigcap_\alpha V(S_\alpha).
\]

(e) For any ideals \( i, j \subset R \) one has

\[
V(i \cap j) = V(ij) = V(i) \cup V(j).
\]

(f) For any subset \( S \subset R \) one has

\[
V(S) = V((S)),
\]

where \( (S) \subset R \) denotes the ideal generated by \( S \).
Proof:

(a) Obvious from the definitions.
(b) For $p \in \text{Spec}(R)$ we have

$$p \in V(S) \iff S \subset p$$

$$\iff s \in p \text{ for all } s \in S$$

$$\iff p \in V(s) \text{ for all } s \in S$$

$$\iff p \in \cap_{s \in S} V(s).$$

(c) Immediate from (7.12).
(d) For any $p \in \text{Spec}(R)$ we have

$$p \in V(\cup_{\alpha} S_{\alpha}) \iff \cup_{\alpha} S_{\alpha} \subset p$$

$$\iff S_{\alpha} \subset p \text{ for all } \alpha$$

$$\iff p \in V(S_{\alpha}) \text{ for all } \alpha$$

$$\iff p \in \cap_{\alpha} V(S_{\alpha}).$$

(e) First note that

(i) $ij \subset i \cap j$.

We claim that for any $p \in \text{Spec}(R)$ we have

(ii) $ij \subset p \iff i \cap j \subset p,$

and to establish this we will first show that

(iii) $ij \subset p \iff i \subset p \text{ or } j \subset p$

(which is what one might expect of a prime ideal). Indeed, if $i \not\subset p$ there must be an element $a \in i \setminus p$, and it then follows from $ij \subset p$ that $ab \in p$ for all $b \in j$. Since $p$ is prime and $a \not\in p$ this in turn forces $b \in p$, and $j \subset p$ follows. This gives the forward implication in (iii), and the reverse implication is obvious from (i).

The forward implication in (ii) is immediate from the corresponding implication in (iii), and the reverse implication is evident from (i).

For any $p \in \text{Spec}(R)$ we conclude from (ii) that

$$p \in V(i \cap j) \iff i \cap j \subset p$$

$$\iff ij \subset p$$

$$\iff p \in V(ij),$$

47
and the first equality $V(i \cap j) = V(ij)$ of assertion (e) follows.

The second equality is obtained by a second appeal to (iii): for $p \in \text{Spec}(R)$ we have

$$p \subset V(ij) \iff ij \subset p \iff i \subset p \text{ or } j \subset p \iff p \in V(i) \text{ or } p \in V(j) \iff p \in V(i) \cup V(j).$$

(f) For any $p \in \text{Spec}(R)$ we have

$$p \in V(S) \iff S \subset p \iff (S) \subset p \iff p \in V((S)).$$

q.e.d.

**Corollary 7.16 :** For any subset $V \subset \text{Spec}(R)$ the following statements are equivalent:

(a) $V$ is closed;
(b) $V = \cap_{s \in S} V(s)$ for some subset $S \subset R$;
(c) $V = V(S)$ for some subset $S \subset R$;
(d) $V = V(i)$ for some ideal $i \subset R$; and
(e) $V = V(r)$ for a unique radical ideal $r \subset R$.

Moreover, for any ideal $i \subset R$ one has

(i) $V(i) = V(\sqrt{i})$.

**Proof :**

(a) $\Rightarrow$ (b) : By assumption $\text{Spec}(R) \setminus V$ is open, hence has the form $\cup_{s \in S} D(s)$ for some subset $S \subset R$. De Morgan and Proposition 7.15(b) then give

$$V = \cap_{s \in S} V(s),$$

and (b) follows.

(b) $\Rightarrow$ (c) : By Proposition 7.15(b).

(c) $\Rightarrow$ (d) : By Proposition 7.15(f).
(d) \implies (e) and (i): For any prime ideal $p \subseteq R$ one has

$$p \in V(i) \iff i \subseteq p \iff \sqrt{i} \subseteq p \quad \text{(because } \sqrt{p} = p) \iff p \in V(\sqrt{i}).$$

This proves (i), and since $r := \sqrt{i}$ is radical (by Proposition 7.11(a)) it also establishes the existence assertion of (e).

The uniqueness assertion is a consequence of Proposition 7.11(d). Indeed, when $r \subseteq R$ and $s \subseteq R$ are radical ideals satisfying $V(r) = V(s)$ that result gives

$$r = \cap_{p \in V(r)} p = \cap_{p \in V(s)} p = s.$$

The converse implication $r = s \implies V(r) = V(s)$ does not require proof.

(e) \implies (a): Proposition 7.15(b).

\textbf{q.e.d.}

\textbf{Corollary 7.17 :} The mapping $r \in R \to V(r) \subseteq \text{Spec}(R)$ between radical ideals of $R$ and closed subsets of $\text{Spec}(R)$ is an inclusion reversing bijection. In particular, for any radical ideal $r \subseteq R$ one has

(a) $V(r) = \emptyset \iff r = R$ and

(b) $V(r) = \text{Spec}(R) \iff r = \sqrt{(0)},$

and when $R$ is an integral domain one has

(c) $V(r) = \text{Spec}(R) \iff r = (0).$

Less formally: the radical ideals parameterize the closed subsets of $\text{Spec}(R)$ (recall Corollary 4.6).

The result shows that, even though defined only in terms of prime ideals, $\text{Spec}(R)$ with the Zariski topology contains information about ideals of $R$ which may not be prime.

\textbf{Proof :} Use Corollary 7.16 and Proposition 7.15(c). \textbf{q.e.d.}
Corollary 7.18: For a proper ideal $i \subset R$ the following statements are equivalent:
(a) $V(i) = \text{Spec}(R)$; and
(b) $i \subset \sqrt{(0)}$.

Proof: From (i) of Corollary 7.16 we have $V(i) = V(\sqrt{i})$, and by Corollary 7.17 the radical ideals of $R$ parameterize the closed subsets of $\text{Spec}(R)$ in a bijective manner. Since $i \subset \sqrt{i}$, the result now follows from Corollary 7.17(b). q.e.d.

We can, at last, describe closures of subsets of $\text{Spec}(R)$.

Proposition 7.19: For any subset $Y \subset \text{Spec}(R)$ the following statements hold.
(a) For any ideal $i \subset R$ one has
\[ Y \subset V(i) \iff i \subset \bigcap_{p \in Y} p. \]
(b) Let $\mathcal{I}_Y$ denote the collection of ideals $i$ satisfying $i \subset \bigcap_{p \in Y} p$. Then the closure $\text{cl}(Y)$ of $Y$ (in $\text{Spec}(R)$) is given by
\[ \text{cl}(Y) = V(\bigcup_{i \in \mathcal{I}_Y} i) = V(\sum_{i \in \mathcal{I}_Y} i). \]
Moreover, for any prime ideal $q \subset R$ one has
(i) $\text{cl}\{q\} = V(q)$.

Proof:
(a) We have
\[ Y \subset V(i) \iff p \in V(i) \text{ for all } p \in Y \]
\[ \iff i \subset p \text{ for all } p \in Y \]
\[ \iff i \subset \bigcap_{p \in Y} p. \]

(b) By Corollary 7.16(d) any closed set of $\text{Spec}(R)$ has the form $V(i)$ for some ideal $i \subset R$, and so from (a) and Proposition 7.15(d) we have
\[ \text{cl}(Y) = \cap_{i \in \mathcal{I}_Y} V(i) = V(\cup_{i \in \mathcal{I}_Y} i). \]
But one sees easily that the ideal generated by $\cup_{i \in \mathcal{I}_Y} i$ is precisely $\sum_{i \in \mathcal{I}_Y} i$, and the result follows.

To establish (i) note that when $Y = \{q\}$ is a singleton we have $\cap_{p \in Y} p = \{q\}$, hence $\mathcal{I}_{\{q\}} = \{ i : i \subset q \}$, and therefore $\sum_{i \in \mathcal{I}_{\{q\}}} i = q$. Equality (i) is now immediate from (b).

q.e.d.
With Proposition 7.15(a) as motivation we define an open set $D(i)$, for any ideal $i \subset R$, by

$$D(i) := \text{Spec}(R) \setminus V(i).$$

Note from Corollary 7.17(a) that

$$D(R) = \text{Spec}(R).$$

Also note that

$$D(i) = \bigcup_{r \in i} D(r).$$

Indeed, from De Morgan and Proposition 7.15(b) we have

$$D(i) = \text{Spec}(R) \setminus V(i)$$
$$= \text{Spec}(R) \setminus \bigcap_{r \in i} V(r)$$
$$= \bigcup_{r \in i} \text{Spec}(R) \setminus V(r)$$
$$= \bigcup_{r \in i} D(r).$$
8. Irreducible Spaces

A non-empty topological space is irreducible if it is not the union of two proper closed subsets. Any one-point space has this property, or consider any infinite set \( X \) in which the open sets are \( \emptyset, X, \) and complements of finite subsets of \( X \). For an example of a space which is reducible, i.e., not irreducible, consider the real numbers with the usual topology.

**Proposition 8.1 :** For any non-empty topological space \( X \) the following assertions are equivalent:

(a) \( X \) is irreducible;

(b) at least one member of any finite closed cover of \( X \) must coincide with \( X \);

(c) the intersection of any finite collection of non-empty open subsets of \( X \) is non-empty;

(d) any non-empty open set is dense in \( X \); and

(e) every open subset of \( X \) is connected.

**Proof :**

(a) \( \Rightarrow \) (b) : Let \( \{C_j\}_{j=1}^n \) be a closed cover of \( X \). When \( n = 1 \) the result is obvious and when \( n = 2 \) the assertion is a rephrasing of the definition of irreducible. When \( n > 2 \) and \( C_n \not= X \) we see from (a) the closed set \( \bigcup_{j=1}^{n-1} C_j \) must coincide with \( X \). Then collection \( \{C_j\}_{j=1}^{n-1} \) is therefore a closed cover and induction applies.

(b) \( \Rightarrow \) (c) : Let \( \{U_j\}_{j=1}^n \) be a collection of non-empty open subsets and for \( j = 1, \ldots, n \) set \( C_j := U_j^c \). If \( \cap_j U_j = \emptyset \) then (by de Morgan) \( \cup_j C_j = X \) and by (b) we then have \( C_j = X \) for at least one \( j \). But this implies \( U_j = \emptyset \), contrary to the stated hypothesis.

(c) \( \Rightarrow \) (d) : If some non-empty open set \( U \) is not dense then \( \{U, \text{cl}(U)^c\} \) constitutes a finite collection of open subsets having empty intersection, thereby contradicting (c).

(d) \( \Rightarrow \) (e) : If some non-empty open set \( U \) is not connected then \( U = V \cup W \) where \( V \) and \( W \) are disjoint non-empty open subsets of \( U \). It follows that \( V \) and \( W \) non-empty non-dense open subsets of \( X \), thereby contradicting (d).

(e) \( \Rightarrow \) (a) : If (a) fails we can write \( X = C \cup D \) with \( C \) and \( D \) proper non-empty closed subsets of \( X \). The non-empty open sets \( U := C^c \) and \( V = D^c \) then satisfy \( U \cap V = \emptyset \), and \( U \cup V \) is therefore a non-connected open subset of \( X \). Contradiction.

q.e.d.
Corollary 8.2: A Hausdorff space $X$ is irreducible if and only if $X$ is a one-point space, i.e., if and only if $X$, when considered only as a set, is a singleton.

Proof: The forward implication is immediate from Proposition 8.1(c); the reverse is obvious. \textbf{q.e.d.}

Corollary 8.3: Any irreducible space is connected.

The converse is false, e.g., we have already noted that the set of real numbers $\mathbb{R}$ with the usual topology is reducible.

Proof: Apply Proposition 8.1(e) to the open set $X$. \textbf{q.e.d.}

Proposition 8.4: Suppose $X$ is a topological space and $Y \subset X$ is a non-empty subspace. Assume the relative topologies on both $Y$ and $\text{cl}(Y)$. Then $Y$ is irreducible if and only if $\text{cl}(Y)$ is irreducible.

Proof: \begin{align*}
\Rightarrow & \text{ When } \{C_j\}_{j=1}^n \text{ is a closed cover of } \text{cl}(Y) \text{ the collection } \{C_j \cap Y\}_{j=1}^n \text{ is such a cover for } Y, \text{ and from (b) of Proposition 8.1 we conclude that } C_i \cap Y = Y \text{ for at least one index } i. \text{ Because } C_i \text{ is also closed in } X \text{ we have } \text{cl}(Y) \subset C_i \subset \bigcup_j \text{cl}(C_j) = \text{cl}(Y), \text{ hence } C_i = \text{cl}(Y), \text{ and a second appeal to Proposition 8.1(b) establishes the irreducibility of } \text{cl}(Y). \\
\Leftarrow & \text{ When } \{C_j\}_{j=1}^n \text{ is a closed cover of } Y \text{ we must have } C_j = Y \cap D_j \text{ for some closed } D_j \subset X. \text{ For } j = 1, \ldots, n \text{ set } E_j := \text{cl}(Y) \cap D_j \subset \text{cl}(Y) \text{ and note that } C_j = Y \cap D_j = (Y \cap \text{cl}(Y)) \cap D_j = Y \cap E_j. \text{ Since each } E_j \text{ is closed the same is true of } \bigcup_j E_j, \text{ and we conclude from } Y = \bigcup_j C_j \subset \bigcup_j E_j \text{ and } E_j \subset \text{cl}(Y) \text{ that } \{E_j\}_{j=1}^n \text{ is a closed cover of } \text{cl}(Y). \text{ From (a) and Proposition 8.1(b) we therefore have } E_i = \text{cl}(Y) \text{ for at least one index } i, \text{ whence } C_i = Y \cap E_i = Y \cap \text{cl}(Y) = Y. \text{ A final appeal to Proposition 8.1(b) completes the proof.} \textbf{q.e.d.}
\end{align*}

Corollary 8.5: The closure $\text{cl}(\{x\})$ of any point $x \in X$ is irreducible.

When the $(A, B)$-Zariski topology is assumed on a classical affine algebraic set the closure of a point is (sometimes) called the \textit{locus} of that point. The result could therefore be stated: \textit{the locus of any point is irreducible.}

For the Zariski topology associated with Example 5.10(a) we have $\text{cl}(\{\sqrt{2}\}) = \{\pm \sqrt{2}\}$, whereas for that associated with Example 5.10(b) we have $\text{cl}(\{\sqrt{2}\}) =$
In particular, when the Zariski topology of Example 5.10(a) is assumed the two-point set \( \{-\sqrt{2}, \sqrt{2}\} \) is irreducible, and therefore connected (by Corollary 8.3).

**Proof:** Apply Proposition 8.4 to the irreducible space \( Y = \{x\} \). \( \text{q.e.d.} \)

We now investigate irreducibility in connection with the Zariski topology, first considering that topology on an algebraic set.

**Theorem 8.6:** Let \( B \supset A \) be an extension of integral domains, let \( n \geq 1 \) be an integer, and endow \( B^n \) with the \((A,B)\)-Zariski topology. Assume \( V \subset B^n \) is \((A,B)\)-Zariski closed. Then \( V \) is irreducible if and only if the defining ideal \( i(V) \subset A[x] \) is prime.

With this result one begins to truly appreciate the interplay between geometry (here wearing topological garb) and algebra: one can define “irreducible” from either standpoint with no gain or loss of information. Indeed, prior to the introduction of the Zariski topology this algebraic characterization was used as the definition of an irreducible algebraic set.

**Proof:**

\( \Rightarrow \): Suppose \( p,q \in A[x] = A[x_1,x_2,\ldots,x_n] \) and \( pq \in i(V) \). Then for any \( x \in V \) we have \( pq(x) = p(x)q(x) = 0 \). Since \( B \) is an integral domain this forces \( p(x) = 0 \) or \( q(x) = 0 \), hence \( V \subset V((p)) \cup V((q)) \), and as a result we can write \( V = (V \cap V((p))) \cup (V \cap V((q))) \). From the irreducibility assumption we may assume w.l.o.g. that \( V = V \cap V((p)) \subset V((p)) \). We then have \( p(x) = 0 \) for all \( x \in V \), hence \( p \in i(V) \).

\( \Leftarrow \): Suppose \( i(V) \) is prime and that \( V = V_1 \cup V_2 \), where each \( V_j \subset V \) is closed and the inclusions \( V_j \subset V \) are proper. Then by (c) of Corollary 7.4 and (7.2) there is an element \( p_j \in i(V_j) \) with \( p_j \notin i(V) \) for \( j = 1,2 \). But \( p_1p_2 \in i \), and this contradicts the assumption that \( i(V) \) is prime.

**q.e.d.**

**Corollary 8.7:** Let \( W \subset B^n \) be an algebraic set and let \( f : A[x] \to A_B[W] \) be the canonical epimorphism. Then the mapping \( C \subset W \mapsto f(i(C)) \in \text{Spec}(A_B[W]) \) is an injection of the closed irreducible subsets of \( W \) (w.r.t. the induced Zariski topology) into \( \text{Spec}(A_B[W]) \).
The result indicates what sort of information about $\mathcal{W}$ is packaged within $\text{Spec}(A_B[\mathcal{W}])$. Since $\mathcal{W} = \mathbb{B}^n$ is a special case, it suggests what information about $\mathbb{B}^n$ is stored in $\text{Spec}(A_B[\mathbb{B}^n])$.

As we will see in Part III, one obtains a much cleaner result when $B$ is an algebraically closed field.

**Proof:** Let $C \subset \mathcal{W}$ be both closed and irreducible in the induced topology. By Corollary 7.7(b) the subset $C$ must be closed in the Zariski topology on $B^n$. We claim that $C$ must also be irreducible in that topology. Otherwise $C = D \cup E$, where $D$ and $E$ are proper subsets of $C$ which are Zariski closed in $\mathbb{B}^n$. However, from $C \subset \mathcal{W}$ we would also have $D, E \subset \mathcal{W}$, and by a second appeal to Corollary 7.7(b) we would conclude that $C$ was reducible.

By Theorem 8.6 the ideal $i(C) \subset A[x]$ must be prime. It then follows from Corollary 7.4(c) that the mapping $C \mapsto i(C)$ is an injection of the irreducible closed subsets $C \subset \mathcal{W}$ into the prime ideals of $A[x]$. From Proposition 3.3, $C \subset \mathcal{W}$ and (7.2) we have $\text{ker}(f) = i(\mathcal{W}) \subset i(C)$, and the image of the mapping is therefore contained in $V(\text{ker}(f))$. The result is now immediate from Proposition 5.4(d). $\text{q.e.d.}$.

Our next task is to investigate irreducibility in connection with the Zariski topology on the prime spectrum of a ring. For this we need a simple ideal-theoretic preliminary.

Let $R$ be a ring (commutative with unity as usual) and let $i, j \subset R$ be ideals. Define their product $ij$ to be the collection of all finite sums $\sum k i_k j_k$ with $i_j \in i$ and $j_i \in j$. One verifies easily that $ij$ is an ideal.

**Proposition 8.8:** When $R$ be a ring and $p \subset R$ is a proper ideal the following statements are equivalent:

(a) the ideal $p$ is prime;

(b) for any $r, s \in R$ the condition $rs \in p$ implies $r \in p$ or $s \in p$ (or both); and

(c) for any ideals $i, j \subset R$ the condition $ij \subset p$ implies $i \subset p$ or $j \subset p$.

The equivalence of (a) and (b) has already been noted and established (see the paragraph immediately preceding Proposition 3.4). It has been included here to highlight the analogy between (b) and (c). Indeed, for particularly nice rings ("Dedekind domains," of which PIDs are fundamental examples) that analogy allows one to replace unique factorization of ring elements into primes by unique factorization of ideals into prime ideals; a reformulation of factorization which resulted in significant
progress on Fermat’s Last Theorem.

**Proof :** In view of the preceding remarks it suffices to prove (b) ⇔ (c).

(b) ⇒ (c) : Otherwise there are elements \( r \in i \setminus p \) and \( s \in j \setminus p \). Since \( rs \in ij \subset p \) we have \( rs \in p \), hence \( r \in p \) or \( s \in p \) (or both), and we have a contradiction.

(c) ⇒ (b) : Suppose \( r, s \in R \) and \( rs \in p \). Then for \( i := (r) := rR \) and \( j := (s) \) we have \( ij \subset p \), hence \( r \in i \subset p \) or \( s \in j \subset p \).

q.e.d.

**Theorem 8.9 :** Suppose \( R \) is an integral domain and \( C \subset \text{Spec}(R) \) is closed, say \( C = V(\mathfrak{r}) \), where \( \mathfrak{r} \subset R \) is the uniquely associated radical ideal. Then \( C \) is irreducible if and only if \( \mathfrak{r} \) is prime.

By the “uniquely associated radical ideal” we mean the unique radical ideal provided by Corollary 7.17.

When taken together with Theorem 8.6, the result suggests a connection between the Zariski topology on classical affine algebraic sets and the Zariski topology on the prime spectrum of a ring.

**Proof :**

⇒ : Suppose \( i, j \subset R \) are ideals such that \( ij \subset \mathfrak{r} \) and \( D := V(i), E := V(j) \). Then from Corollary 7.17 and Proposition 7.15(e) we have \( C = V(\mathfrak{r}) \subset V(ij) = V(i) \cup V(j) = D \cup E \). Because \( C \) is assumed irreducible this forces either \( V(\mathfrak{r}) \subset V(i) = V(\sqrt{i}) \) or \( V(\mathfrak{r}) \subset V(j) \). In the first case \( i \subset \sqrt{i} \subset \mathfrak{r} \); in the second \( j \subset \mathfrak{r} \). From Proposition 8.8(c) we conclude that the ideal \( \mathfrak{r} \) is prime.

⇐ : Suppose \( C = D \cup E \), where \( D, E \subset \text{Spec}(R) \) are closed. By Corollary 7.17 that there are unique radical ideals \( i, j \) such that \( D = V(i) \) and \( E = V(j) \), and from Proposition 7.15 we have

(i) \[ C = D \cup E \iff V(\mathfrak{r}) = V(i) \cup V(j) = V(i \cap j). \]

By Proposition 7.11(a) the ideal \( i \cap j \) is radical, and from a second appeal to Corollary 7.17 we conclude from (i) that

(ii) \[ C = D \cup E \iff \mathfrak{r} = i \cap j. \]

One sees easily that \( ij \subset i \cap j \), hence \( ij \subset \mathfrak{r} \) by (ii). By Proposition 8.8(c) this forces \( i \subset \mathfrak{r} \) or \( j \subset \mathfrak{r} \), hence \( C = V(\mathfrak{r}) \subset V(i) = D \) or \( C \subset E \). The closed set \( C \) is therefore irreducible.

q.e.d.
9. Noetherian Spaces

Again $R$ denotes a ring.

Several algebraic preliminaries are required. An $R$-module $M$ is Noetherian if every $R$-submodule (including $M$) is finitely generated\textsuperscript{44}. When this is the case and $M$ is also an $R$-algebra we speak of a Noetherian $R$-algebra, and when $M = R$ of a Noetherian ring. Since the $R$-submodules of $R$ coincide with the ideals, $R$ is Noetherian if and only if every ideal is finitely generated.

Examples 9.1:

(a) Every finite-dimensional vector space over a field $K$ is a Noetherian $K$-module (because every subspace of a finite-dimensional vector space is finite-dimensional).

(b) Every PID is a Noetherian ring (because each ideal is generated by a single element).

(c) $\mathbb{Z}$ is a Noetherian ring (by (b)).

(d) Every field is a Noetherian ring (because every field is a PID).

(e) For any field $K$ the polynomial ring $K[x_1, x_2, \ldots]$ in infinitely many indeterminates is not Noetherian (because the ideal $(x_1, x_2, \ldots)$ is not finitely generated).

(f) A subring of a Noetherian ring need not be Noetherian. For example, the ring $K[x_1, x_2, \ldots]$ of Example (e) is an integral domain, and the quotient field $K(x_1, x_2, \ldots)$, which we regard as an extension of $K[x_1, x_2, \ldots]$, is therefore Noetherian. But we have seen in Example (e) that $K[x_1, x_2, \ldots]$ is not Noetherian.

Alternate characterizations of Noetherian modules and rings will simplify the presentation of more substantial examples. Some elementary set theory proves useful in this regard\textsuperscript{45}.

When $X$ is a non-empty set with a partial order relation $\leq$ a sequence $\{x_j\}_{j_0 \leq j \in \mathbb{Z}}$ is ascending (resp. descending) if $x_{j_0} \leq x_{j_0+1} \leq \cdots$ (resp. $x_{j_0} \leq x_{j_0+1} \leq x_{j_0+2} \leq \cdots$).

\textsuperscript{44}That is, generated by a finite subset. In other words, there must be a finite set $S = \{s_1, s_2, \ldots, s_n\} \subset M$ such that every element $m \in M$ can be written (not necessarily uniquely) in the form $m = \sum_{j=1}^{n} r_j s_j$ with $r_j \in R$ and $s_j \in S$.

\textsuperscript{45}In our set-theoretic formulation of the Noetherian conditions we follow [A-M, Chapter 6].
and such a sequence stabilizes if there is an integer \( r \geq 1 \) such that \( X_{r+j} = X_r \) for all \( j \geq 0 \); when the integer \( r \) in this last equality is minimal we say that the sequence stabilizes at \( r \). An element \( x_\beta \) within a subset \( \{x_\alpha\} \subset X \) is maximal (resp. minimal) if \( x_\alpha \preceq x_\beta \) (resp. \( x_\beta \preceq x_\alpha \)) for all \( \alpha \). To see examples let \( X \) be a collection of subsets of some given set, e.g., ideals within a ring, and let the partial order relation be inclusion: a sequence \( \{X_j\}_{j \geq j_0} \in \mathbb{Z} \) of subsets is then ascending if \( X_{j_0} \subset X_{j_0+1} \subset \cdots \), descending if \( X_{j_0} \supset X_{j_0+1} \supset \cdots \), and an element \( X_\beta \) within a collection \( \{X_\alpha\} \), is maximal (resp. minimal) if and only if \( X_\alpha \subset X_\beta \) (resp. \( X_\alpha \supset X_\beta \)) for all \( \alpha \).

**Proposition 9.2 :** When \( X \) is a non-empty set with a partial order relation the following statements are equivalent:

1. every ascending sequence of elements stabilizes; and
2. every non-empty subset has a maximal element.

The result also holds (and will be used) when ascending is replaced by descending in (a) and maximal by minimal in (b). The proof in that case is a simple modification of what follows.

**Proof :** Denote the partial order relation by \( \preceq \).

(a) \( \Rightarrow \) (b) : Given a non-empty subset \( Y \) choose \( y_1 \in Y \) and, inductively, \( y_{n+1} \in Y \) satisfying \( y_n \preceq y_{n+1} \) if \( y_n \) is not maximal. If \( Y \) has no maximal element this construction produces an ascending sequence which does not stabilize, contrary to (a). The process therefore terminates after finitely many steps, and the final \( y_r \) must be a maximal element of \( Y \).

(b) \( \Rightarrow \) (a) : When \( \{x_j\} \subset X \) is an ascending sequence and \( x_m \in \{x_j\} \) is a maximal element we have \( x_j = x_m \) for all \( j \geq m \).

q.e.d.

**Corollary 9.3 :** For any \( R \)-module \( M \) the following statements are equivalent.

1. \( M \) is Noetherian;
2. every ascending sequence \( M_0 \subset M_1 \subset M_2 \subset \cdots \) of \( R \)-submodules of \( M \) stabilizes; and
3. every collection \( \{M_\alpha\} \) of \( R \)-submodules of \( M \) has a maximal element.

The equivalence of (a) and (b) is often stated: an \( R \)-module \( M \) is Noetherian if and only if it satisfies the ascending chain condition (ACC) on submodules.
Proof:

(a) $\Rightarrow$ (b): $\cup M_j$ is a subspace, hence finitely generated, say by \{${m_1, \ldots, m_n}$\} $\subset M$. For $r \geq 0$ sufficiently large we have $m_j \in M_r$ for $j = 1, \ldots, n$, whence $M_{r+j} = M_r$ for all $j \geq 0$.

(b) $\Leftrightarrow$ (c): By Proposition 9.2.

(b) $\Rightarrow$ (a): If a subspace $N \subset M$ is not finitely generated we can choose elements $m_0, m_1, \ldots \in N$ such that the subspace $M_j$ generated by \{${m_0, \ldots, m_j}$\} is proper in $M_{j+1}$, and the ascending sequence $M_0 \subset M_1 \subset M_2 \subset \cdots$ would therefore not stabilize.

q.e.d.

Corollary 9.4: The following assertions concerning the ring $R$ are equivalent:

(a) $R$ is Noetherian;
(b) every ascending sequence of ideals in $R$ stabilizes; and
(c) every collection of ideals of $R$ contains a maximal element.

The equivalence of (a) and (b) is often stated: a ring is Noetherian if and only if it satisfies the ascending chain condition (ACC) on ideals.

Corollary 9.4 suggests an alternate proof of the assertion of Example 9.1(e): the ascending sequence $(x_1) \subset (x_1, x_2) \subset \cdots$ does not stabilize.

Corollary 9.5: Suppose $R$ is a Noetherian ring and $f: R \to S$ is a ring epimorphism. Then $S$ is also Noetherian.

Proof: When $j_0 \subset j_1 \subset \cdots$ is an ascending chain of ideals in $S$ we see from Proposition 5.4(c) that the inverse images $f^{-1}(j_0) \subset f^{-1}(j_1) \subset f^{-1}(j_2) \subset \cdots$ form an ascending chain of ideals in $R$ which by hypothesis must stabilize at some integer $r \geq 0$. From $j_i = f(f^{-1}(j_i))$ we conclude that given sequence in $S$ also stabilizes at the index $r$.

q.e.d.

The fundamental result on Noetherian rings is the following.
Theorem 9.6 (The Hilbert Basis Theorem) : When $R$ is a Noetherian ring the polynomial algebra $R[x]$ is also Noetherian.

Proof : Let $i \subset R[x]$ be an ideal and for $n = 0, 1, \ldots$ let $a_n \subset R$ be the ideal consisting of 0 and the leading coefficients of polynomials in $i$ of degree $n$. (The “leading coefficient” of $p(x) = \sum_{j=0}^{k} a_j x^j$, where $a_k \neq 0$, is $a_k$; the leading coefficient of the 0 polynomial is 0.) Note that $a_0 \subset a_1 \subset a_2 \subset \cdots$, and as a consequence for some $r \geq 0$ we have $a_{r+j} = a_r$ for all $j \geq 0$. For $i = 0, 1, \ldots, r$ let $\{a_{ij}\}_{j=1}^{m_i}$ generate $a_i$, and let $p_{ij}(x) \in i$ be a polynomial of degree $i$ with leading coefficient $\alpha_{ij}$. It suffices to prove that $i \subset i'$, where $i'$ is the ideal generated by the finite collection $\{p_{ij}(x)\}$.

Any $a \in a_0$ is of the form $a = \sum_{j=1}^{m_0} a_j \alpha_{0j} = \sum_{j} a_j p_{0j}(x)$, and therefore belongs to $i'$. Inductively, assume any polynomial in $i$ of degree at most $n - 1 \geq 0$ belongs to $i'$ and let $p(x) \in i$ have degree $n$, say $p(x) = ax^n + \hat{p}(x)$, where $a \neq 0$ and $\hat{p}(x)$ has degree at most $n - 1$. Then $a = \sum_{j=1}^{m_n} b_j \alpha_{nj}$, and for $q(x) := \sum_{j=1}^{m_n} b_j p_{nj}(x)$ and $\tilde{p}(x) := p(x) - q(x)$ we then have $p(x) = \tilde{p}(x) + q(x)$, where $\tilde{p}(x) \in i$ has degree at most $n - 1$ and $q(x) \in i'$. By induction $\tilde{p} \in i'$, hence $p(x) \in i'$, and the proof is complete.

Corollary 9.7 : When $R$ is a Noetherian ring the polynomial algebra $R[x_1, \ldots, x_n]$ is also Noetherian.

In particular, each polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ is a Noetherian ring. We now understand the general structure of the ideals of such rings.

Proof : Use the identification $R[x_1, \ldots, x_n] \simeq (R[x_1, \ldots, x_{n-1}])[x_n]$ and induction on $n$.

q.e.d.

Corollary 9.8 : Suppose $B \supset A$ is an extension of rings, $A$ is Noetherian, and $n \geq 1$ is an integer. Then any classical $(A, B)$-affine algebraic subset of $B^n$ is the zero set of a finite collection of polynomials with coefficients in $A$.

This is one of the fundamental results of classical affine algebraic geometry.

Proof : For any subset $S \subset A[x_1, \ldots, x_n]$ we have $\mathcal{V}(S) = \mathcal{V}((S))$, and the ideal $(S)$ is finitely generated.

q.e.d.

Corollary 9.9 : Suppose $R$ is Noetherian and $S \supset R$ is a ring extension which is finitely generated as an $R$-algebra. Then $S$ is also Noetherian.
This result also goes by the name “Hilbert Basis Theorem”.

**Proof**: By hypothesis there is a finite set $x_1, \ldots, x_n$ of indeterminates, algebraically independent over $R$, and a ring epimorphism $f : R[x_1, \ldots, x_n] \to S$. From Corollary 9.7 we know that $R[x_1, \ldots, x_n]$ is Noetherian, and the result is then immediate from Corollary 9.5. \[\text{q.e.d.}\]

This ends the algebraic preliminaries.

A topological space $X$ is *Noetherian* if every descending sequence of closed sets stabilizes. The defining condition is also stated: $X$ satisfies the descending chain condition (DCC) on closed sets. An equivalent definition is obviously: $X$ satisfies the ascending chain condition (ACC) on open sets, i.e., every ascending sequence of open sets stabilizes. To see a simple example let $X$ be an infinite set with open sets $X$, $\emptyset$, and complements of finite subsets. As a non-example consider the closed unit interval $[0,1] \subset \mathbb{R}$ with the usual topology: the descending sequence of closed sets $[0,1/n]$ does not stabilize.

One of the fundamental examples of a Noetherian space arises in classical algebraic geometry, and as an indication of its importance is presented in the form of a theorem.

**Theorem 9.10**: Suppose $A$ is a Noetherian integral domain, $B \supset A$ is an extension of integral domains, and $n \geq 1$ is an integer. Then $B^n$ is a Noetherian space.

Recall that $B^n$ is the notation used to indicate $B^n$ when this set is assumed endowed with the $(A, B)$-Zariski topology\(^46\). The integral domain assumption on $B$ is needed to guarantee the existence of this topology.

**Proof**: By (7.2) a decreasing sequence of (not necessarily closed) subsets $X_j \subset X$ corresponds to an increasing sequence of ideals $i(X_j) \subset R$. By Corollary 9.7 the ring $R$ is Noetherian, the latter sequence therefore stabilizes, and from Corollary 7.4(c) we conclude that the same must hold for the sequence $\{X_j\}$ when these sets are closed. \[\text{q.e.d.}\]

\(^{46}\)See the first paragraph following the proof of Corollary 4.6.
Proposition 9.11: For any topological space $X$ the following statements are equivalent:

(a) $X$ is Noetherian;

(b) any non empty collection of closed subsets of $X$ contains a minimal element;

(c) every subspace of $X$ is Noetherian in the relative topology.

Proof:

(a) $\Leftrightarrow$ (b): Immediate from the comments following the statement of Proposition 9.2.

(b) $\Rightarrow$ (c): Suppose $Y \subseteq X$ and $\{C_\alpha\}$ is a collection of relatively closed subsets of $Y$. By (b) the collection $\{\text{cl}(C_\alpha)\}$ of closed subsets of $X$ has a minimal element $\text{cl}(C_\beta)$, and for any $C_\gamma \in \{C_\alpha\}$ we then have

$$C_\gamma \subseteq C_\beta \Rightarrow \text{cl}(C_\gamma) \subseteq \text{cl}(C_\beta)$$

$$\Rightarrow \text{cl}(C_\gamma) = \text{cl}(C_\beta)$$

$$\Rightarrow C_\gamma = \text{cl}(C_\gamma) \cap Y = \text{cl}(C_\beta) \cap Y = C_\beta,$$

and $C_\beta$ is therefore minimal for $\{C_\alpha\}$. Applying the already-established implication (b) $\Rightarrow$ (a) to $Y$ then gives (c).

(c) $\Rightarrow$ (a): Obvious.

q.e.d.

The following result explains why Noetherian spaces are of interest in affine algebraic geometry.

Corollary 9.12: When $B \supset A$ is an extension of integral domains and the $(A, B)$-Zariski topology is assumed classical affine $(A, B)$-algebraic sets are Noetherian spaces.

Proof: By Proposition 9.10.

q.e.d.

We next relate the Noetherian property to irreducibility.
Theorem 9.13: When $X$ is a Noetherian topological space there is a unique finite collection $\{X_j\}_{j=1}^m$ of closed subspaces of $X$ with the following three properties:

(a) $X = X_1 \cup \cdots \cup X_m$;
(b) each $X_j$ is irreducible (in the relative topology); and
(c) $X_i$ is not a subset of $X_j$ for all $1 \leq i \neq j \leq m$.

The $X_j$ are called the irreducible components of $X$, and the expression in (a) is the irreducible decomposition of $X$. It is important to note, as will be illustrated in Example 9.16(b), that the $X_j$ need not be disjoint.

The result reduces the study of Noetherian spaces to that of irreducible Noetherian spaces.

Proof: Let $\{X_\alpha\}$ denote the collection of all closed subsets of $X$ which are not finite unions of irreducible closed subsets. If there is no decomposition as in (a) and (b) this collection contains $X$, hence is non empty, and by Proposition 9.11(b) contains a minimal element $X_\mu$.

From the defining property of the collection this element must be reducible, say $X_\mu = A \cup B$, where $A, B \subseteq X_\mu$ are proper and closed, and by the minimality property each of $A$ and $B$ can be expressed as a finite union of closed irreducible subsets. But $X_\mu$ can then be so expressed, which is a contradiction. Decompositions as in (a) and (b) therefore exist, and we assume $\{X_j\}_{j=1}^m$ is such a collection. Note that by discarding any redundant $X_j$ we may assume the condition in (c).

Suppose $\{Y_i\}_{i=1}^t$ is another such decomposition. Then for each $1 \leq j \leq n$ we have $X_j = \bigcup_i (Y_i \cap X_j)$, and by irreducibility we conclude that $X_j = Y_i \cap X_j$ for some $i$, i.e., that $X_j \subseteq Y_i$. Reversing the roles of $X_j$ and $Y_i$ in this argument results an analogous opposite inclusion, whereupon $m = t$ and $X_j = Y_i$ follows immediately from the assumption in (c).

Corollary 9.14: Suppose $X = X_1 \cup \cdots \cup X_n$ is the irreducible decomposition of a Noetherian space $X$ and $\tilde{X} \subset X$ is irreducible. Then $\tilde{X} \subset X_j$ for some $j$.

Proof: By Proposition 8.4 we may assume $\tilde{X}$ is closed. If the assertion is false the decomposition $X = X_1 \cup \cdots \cup X_n \cup \tilde{X}$ would then satisfy the conditions of Theorem 9.13, contradicting uniqueness.

It is now a relatively simple matter to understand the the topological structure of any classical affine algebraic set.
Theorem 9.15: Suppose $A$ is a Noetherian integral domain, $B \supset A$ is an extension of integral domains, and $n \geq 1$ is an integer. Then to each classical $(A, B)$-affine algebraic subset $V \subset \mathbb{B}^n$ there corresponds a unique finite collection $\{V_j\}_{j=1}^n$ of irreducible classical $(A, B)$-affine algebraic subsets with the following three properties:

(a) $V = V_1 \cup \cdots \cup V_m$;

(b) each of the defining ideals $i(V_j) \subset A[x] = A[x_1, x_2, \ldots, x_n]$ is prime; and

(c) $V_i$ is not a subset of $V_j$ for all $1 \leq i \neq j \leq m$.

Irreducible affine algebraic sets are called affine algebraic varieties\textsuperscript{47}; the study of classical affine algebraic sets is thereby reduced to the study of such sets having this particular form. The collection $\{V_j\}_{j=1}^m$ is the irreducible decomposition of $V$.

Proof: Immediate from Corollary 9.12 and Theorem 8.6. q.e.d.

Examples 9.16:

(a) When $X$ is an irreducible Noetherian space we have $n = 1$ and $X = X_1$ in the statement of Theorem 9.13.

(b) In Corollary 9.15 take $A = B = \mathbb{R}$, $n = 2$, and let $V := V(\{x_1^2 - x_2^2\}) \subset X = \mathbb{R}^2$. Then $V$ is closed, and the irreducible components are two the lines defined by the equations $x_2 = x_1$ and $x_2 = -x_1$ respectively. In particular, irreducible components need not be disjoint.

(c) Suppose $X$ is a finite Noetherian space, say $X = \{x_1, \ldots, x_n\}$, and each point is closed. Then $X = \{x_1\} \cup \cdots \cup \{x_n\}$ is the irreducible decomposition of $X$.

\textsuperscript{47}The definition varies from author to author. In particular, what we have called an affine algebraic set might be referred to as an affine algebraic variety, and when that convention is used what we call an affine algebraic variety would be referred to as an irreducible algebraic variety.
10. An Algebraic Interlude - Maximal Ideals

Throughout the section $R$ is a ring.

A proper ideal $m \subset R$ is (a) maximal (ideal) if $R/m$ is a field. Example: for any prime $p \in \mathbb{Z}$ the factor ring $\mathbb{Z}_p = \mathbb{Z}/(p)$ is a field, and the ideal $(p) \subset \mathbb{Z}$ is therefore maximal.

**Proposition 10.1 :**

(a) Any maximal ideal is a prime ideal.

(b) Any maximal ideal is a radical ideal.

**Proof :**

(a) All fields are integral domains.

(b) All prime ideals are radical ideals.

q.e.d.

The “maximal” designation arises from the following characterization.

**Proposition 10.2 :** For any proper ideal $i \subset R$ the following assertions are equivalent:

(a) $i$ is maximal;

(b) for any ideal $j$ satisfying $i \subset j$ one has either $j = i$ or $j = R$.

Assertion (b) is a common definition of a maximal ideal.

**Proof :**

(a) $\Rightarrow$ (b) : Suppose the inclusion $i \subset j$ is proper and $r \in j \setminus i$. Since $R/i$ is a field the element $[r] \in R/i$ is invertible, and we can therefore find an element $[s]$ in this factor ring such that $[r][s] = [1]$, i.e., an element $s \in R$ such that $1 - rs =: t \in i \subset j$. But $r \in j \Rightarrow rs \in j$, hence $rs + t = 1 \in j$, and $j = R$ follows.

(b) $\Rightarrow$ (a) : Choose any non-zero element $[r] \in R/i$ and let $j \subset R$ be the ideal generated by $i$ and $r$. Since $r \notin i$ the inclusion $i \subset j$ is proper, hence $j = R$, and we conclude that there must be elements $t \in i$ and $s \in R$ such that $t + sr = 1$. This gives $[r][s] = [1]$ in $R/i$, proving that $[r]$ is invertible.

q.e.d.
Corollary 10.3 : Every proper ideal of $R$ is contained in a maximal ideal.

Proof : Choose $S = \{1\}$ in Theorem 7.8 to produce a prime ideal $p \subseteq R$ which contains the given ideal and is maximal among all such ideals. Since any proper ideal containing $p$ will also have these two properties we see from Proposition 10.2 that $p$ must be a maximal ideal.

q.e.d.

Corollary 10.4 : Every proper ideal of $R$ is contained in a prime ideal.

Proof : Maximal ideals are prime (Proposition 10.1(a)).

q.e.d.

Corollary 10.5 : Every proper ideal of $R$ is contained in a radical ideal.

Proof : Maximal ideals are radical (Proposition 10.1(b)).

q.e.d.

Corollary 10.6 : For any non-zero element $r \in R$ the following assertions are equivalent:

(a) $r$ is a unit;
(b) $D(r) = \text{Spec}(R)$; and
(c) $V(r) = \emptyset$.

The equivalence of (a) and (b) may also be stated: $r$ is a unit if and only if $r$ is not contained in any prime ideal of $R$.

Proof :

(a) $\Rightarrow$ (b) : If $r$ is a unit the ideal $(r) \subseteq R$ generated by $r$ must coincide with $R$. If $i$ is any ideal containing $r$ then we also have $(r) \subseteq i$, hence $i = R$. Since prime ideals must be proper, $r \notin p$ for and prime ideal $p$, and (b) follows.

(b) $\Leftrightarrow$ (c) : By Proposition 7.15(a).

(c) $\Rightarrow$ (a) : If $V(r) = \emptyset$ there is no prime ideal containing $r$, hence no prime ideal containing the ideal $(r)$. It is then immediate from Corollary 10.4 that $(r) = R$, hence that $rs = 1$ for some $s \in R$, hence that $r$ is a unit.

q.e.d.

Corollary 10.7 : Suppose $R$ is non-trivial and $i \subseteq R$ is an ideal. Then in $\text{Spec}(R)$ one has $V(i) = \emptyset$ if and only if $i = R$.  

66
Proof:
⇒: When $i \neq R$ there is a prime ideal $p$ containing $i$, hence $p \in V(i)$.
⇐: Recall (7.13).

q.e.d.

Proposition 10.8: Suppose $f : R \to S$ is a surjective ring homomorphism and $p \subseteq R$ is a prime ideal not containing $\ker(f)$. Then $p$ is maximal if and only if $f(p) \subseteq S$ is maximal.

Proof: Immediate from Propositions 5.4(d) and 10.2(b).

q.e.d.

Let $\text{maxSpec}(R)$ denote the collection of maximal ideals of $R$. Since every maximal ideal is prime (Proposition 10.1(a)) we have $\text{maxSpec}(R) \subseteq \text{Spec}(R)$. The induced topology on $\text{maxSpec}(R)$, which we always assume, is again called the Zariski topology.

Proposition 10.9: The following assertions are equivalent:

(a) $\text{maxSpec}(R)$ is dense in $\text{Spec}(R)$; and

(b) For each non-zero element $r \in R$ there is a maximal ideal $m \subseteq R$ not containing $r$.

Proof: Recall from (5.3a) that $D(0) = \emptyset$. It therefore suffices to prove that (b) is equivalent to $D(r) \cap \text{maxSpec}(R) \neq \emptyset$ for all $0 \neq r \in R$. But this is immediate from the definitions: we have

$D(r) \cap \text{maxSpec}(R) \neq \emptyset$ $\iff$ there is a maximal ideal $m \subseteq D(r)$
$\iff$ there is a maximal ideal $m \subseteq R$ such that $r \notin m$.

q.e.d.
11. Closed Points

A point \( x \) of a topological space \( X \) is (a) **closed (point)** if \( \text{cl}(\{x\}) = \{x\} \), i.e., if the singleton subset \( \{x\} \subset X \) is closed. Example: when the usual topology is assumed all points of \( \mathbb{R} \) are closed.

When \( B \subset A \) is an extension of rings and \( B \) is an integral domain we see from Corollary 7.4 (or Corollary 7.7) that a point \( c \in \mathbb{B}^n \) is closed if and only if

\[
(11.1) \quad \{c\} = \mathcal{V}(i(\{c\})).
\]

**Proposition 11.2**: Suppose, in the notation of the previous paragraph, that \( A = B \). Then all points of \( \mathbb{B}^n \) are closed points.

The result fails if \( A \neq B \), as can be seen from the example involving \( A = \mathbb{Z}, B = \mathbb{R} \) and \( C = \sqrt{2} \) immediately following the statement of Corollary 7.4.

**Proof**: This is simply a restatement of Proposition 7.5. \( \text{q.e.d.} \)

When the Zariski topology on a classical \((A, B)\)-affine algebraic set \( \mathcal{V} \subset \mathbb{B}^n \) is under consideration we see from Corollary 7.7 that a point \( v \in \mathcal{V} \) is closed in the (induced) Zariski topology on \( \mathcal{V} \) if and only if \( v \) is closed in the Zariski topology on \( B^n \).

**Proposition 11.3**: Suppose \( B \supset A \) is an extension of integral domains, \( n \geq 1 \) is an integer, and \( \mathcal{W} \subset \mathbb{B}^n \) is a classical \((A, B)\)-affine algebraic set. Then a point \( w \in \mathcal{W} \) is closed (in the induced \((A, B)\)-Zariski topology) if and only if for each ideal \( j \subset A[x] \) containing \( i(\{w\}) \subset A[x] \) one has either \( \mathcal{V}(j) = \emptyset \) or \( \mathcal{V}(j) = \{w\} \).

Note that the given necessary and sufficient conditions do not involve \( \mathcal{W} \). This is explained by Corollary 7.7: closures of subsets of \( \mathcal{W} \) in the induced topology are the same as Zariski closures in \( \mathbb{B}^n \).

**Proof**:

\( \Rightarrow \) Suppose \( w \in \mathcal{W} \) is a closed point and \( j \) is an ideal containing \( i(\{w\}) \). Then from (4.1) and (11.1) we see that \( \mathcal{V}(j) \subset \mathcal{V}(i(\{w\})) = \{w\} \), and the result immediately follows.

\( \Leftarrow \) By choosing \( j = i(\{w\}) \) we see that \( \mathcal{V}(i(\{w\})) = \emptyset \) or \( \mathcal{V}(i(\{w\})) = \{w\} \), and the first alternative is impossible since \( w \in \mathcal{V}(i(\{w\})) \). Now make a second appeal to (11.1).

\( \text{q.e.d.} \)

68
Corollary 11.4: Suppose $B$ has infinitely many elements and the surjective mapping $i \mapsto \mathcal{V}(i)$ of Corollary 4.6, from the radical ideals of $A[x]$ to the classical $(A, B)$-affine algebraic subsets of $\mathbb{B}^n$, is bijective. Then the following assertions hold for any classical $(A, B)$-affine algebraic set $W \subset \mathbb{B}^n$.

(a) A point $w \in W$ is $(A, B)$-Zariski closed (in both the $(A, B)$-Zariski topology on $\mathbb{B}^n$ and the induced $(A, B)$-Zariski topology on $W$) if and only if the defining ideal $i\{w\} \subset A[x]$ of $\{w\}$ is maximal.

(b) Any maximal ideal $m \subset A[x]$ satisfying $\mathcal{V}(m) \subset W$ is the defining ideal of some point of $W$.

(c) The mapping $w \in W \mapsto i\{w\} \subset A[x]$ is a bijection between $W$ and the maximal ideals $m \subset A[x]$ satisfying $\mathcal{V}(m) \subset W$.

Less formally: under the stated hypotheses one can think of points as maximal ideals and vice versa.

The choice $W = \mathbb{B}^n$ is a very important special case of the proposition.

Proof:

(a) 
\[ \Rightarrow \] Otherwise we can invoke Corollary 10.3 to choose a maximal ideal $j$ properly containing $i\{w\}$, which by Proposition 10.1(b) must be radical. In view of the bijectivity hypothesis we see from Theorem 4.5(a) that $\mathcal{V}(j) \neq \emptyset$, and we therefore have $\mathcal{V}(j) = \{w\} = \mathcal{V}(i\{w\})$ by Proposition 11.3. Since $i\{w\}$ is also radical (by Proposition 5.11 [which requires that $B$ be infinite] and Proposition 3.4), a second appeal to the bijectivity hypothesis then gives $j = i\{w\}$, and we have a contradiction.

\[ \Leftarrow \] If $i\{w\}$ is maximal then the only ideal which properly contains this ideal is $A[x]$, and $\mathcal{V}(A[x]) = \emptyset$ by Theorem 4.5(a). The necessary and sufficient conditions of Proposition 11.3 are therefore met, and $w$ is therefore closed.

(b) First note from the bijectivity assumption that $\mathcal{V}(m) \neq \emptyset$, and $\mathcal{V}(m)$ therefore contains at least one point $c$. From $\mathcal{V}(m) \subset W$ we see that $c \in W$.

From $\{c\} \subset \mathcal{V}(m)$, (7.2) and Proposition 7.3(b) we have $i\{c\} \supset i(\mathcal{V}(m)) \supset m$, and since $m$ is maximal this forces either $i\{c\} = A[x]$ or the desired conclusion $i\{c\} = m$. The first alternative is easily dismissed: non-zero constant functions cannot vanish at the point $c$.

---

48This is the sort of result one comes to expect. After all, our subject is called “algebraic geometry.”
(c) Use (a), (b) and the hypothesized bijectivity of $i \to \mathcal{V}(i)$. \hfill q.e.d.

The closed points of the prime spectrum $\text{Spec}(R)$ of any ring $R$ have a characterization analogous to that given in Corollary 11.4(a), and the annoying qualifications (e.g., that regarding bijectivity and the requirement that $B$ be an integral domain) are absent.

**Proposition 11.5 :** For any prime ideal $p \subset R$ the following statements are equivalent:

(a) the point $p \in \text{Spec}(R)$ is closed;
(b) $\mathcal{V}(p) = \{p\}$; and
(c) $p$ is a maximal ideal.

Recall that $\text{Spec}(R)$ is assumed endowed with the Zariski topology.

**Proof :**

(a) $\iff$ (b): From (i) of Proposition 7.19 and (7.12) we have

(i) \[ \overline{\{p\}} = \mathcal{V}(p) = \{q \in \text{Spec}(R) : p \subset q\}, \]

and as a result we see that

(ii) \[ p \text{ is closed} \iff \mathcal{V}(p) = \{p\} = \{q \in \text{Spec}(R) : p \subset q\}. \]

(a) $\Rightarrow$ (c): If $p$ is closed but not maximal there is an ideal $j$ satisfying $p \subset j \subset R$ with both inclusions proper, and by Corollary 10.3 we may assume $j$ is maximal. But $j$ is then a prime ideal distinct from $p$ contained in $\mathcal{V}(p)$, and this contradicts the final equality in (ii).

(c) $\Rightarrow$ (a): When $p$ is maximal there can be no prime ideal $q$ properly containing $p$ (in fact there can be no proper ideal containing $p$ as a proper subset), and from (i) we conclude that $\overline{\{p\}} = \{p\}$. \hfill q.e.d.
12. An Application of the Prime Spectrum - The Infinitude of Primes

This section represents what I hope will be an amusing diversion for the reader: we will use the Zariski topology on Spec(\mathbb{Z}) to prove Euclid’s Theorem that the set of prime numbers is infinite.

To keep the diversion brief we will use a few standard ring-theoretic results which have not been rigorously established. Proofs can be found in [H, Chapter III, §3, pp. 135-40], or else are trivial consequences of material therein. Let \( A \) be any PID.

I. The maximal and non-zero prime ideals of \( A \) coincide.

II. An element \( a \in A \) is prime if and only if the ideal \( (p) \subset A \) is non-zero and prime. (See, e.g., [H, Chapter III, §3, Theorem 3.4(a), p. 136].)

III. Primes \( p, q \in A \) are associates if there is a unit \( u \in A \) such that \( p = uq \) or, equivalently, if \( (p) = (q) \). This is an equivalence relation: a set of representatives of the resulting equivalence classes (i.e., one element from each class) is a set of representatives of the primes. Example: The collection \( \{2, 3, 5, 7, 11, 13, \ldots \} \) is a set of representatives of the primes of \( \mathbb{Z} \); it excludes the negatives of these primes, which by definition are also primes.

IV. Units are not divisible by primes.

V. Any Euclidean domain is a PID, and therefore a UFD.

**Theorem 12.1**: Suppose a commutative ring \( A \) with unity satisfies the following conditions:

(a) \( A \) is a PID;

(b) \( A \) is infinite; and

(c) for any non-zero non-unit \( a \in A \) there is a unit \( u \in A \) such that \( a + u \) is also a non-zero non-unit.

Then Spec(\( A \)) is infinite, and there must be infinitely many primes in \( A \).

---

49 We say “amusing diversion” because there are certainly easier ways to prove the results achieved.

50 In particular, see Theorem 3.4, p. 136, of that reference.

51 I.e., any principal ideal domain.

52 An element \( p \in A \) is prime if for any \( a, b \in A \) the condition \( p|ab \) implies \( p|a \) or \( p|b \). Here \( p|a \) means “\( p \) divides \( a \),” i.e., \( a = pc \) for some \( c \in A \).

53 Unique factorization domain, or what is now sometimes called a factorial ring, e.g., as in [L, Chapter II, §5, p. 111].
The proof was inspired by H. Fürstenberg’s topological proof of Euclid’s Theorem [Fur]. His argument, however, made use of a different topology: one based on arithmetic progressions rather than prime ideals.

**Proof**: For any set of representatives \( P \subset A \) of the primes we see from (II) that the assignment \( p \in P \mapsto (p) \in \text{Spec}(A) \setminus \{(0)\} \) is a bijection. In particular, \( \text{Spec}(A) \) is infinite if and only if this is the case for \( P \), and it therefore suffices to prove that \( \text{Spec}(A) \) is infinite. We argue by contradiction.

By (I) and Proposition 11.5 all \( p \in \text{Spec}(A) \) except the zero ideal \((0)\) are closed (points). If \( \text{Spec}(A) \) is finite then \( \text{Spec}(A) \setminus \{(0)\} \) must be closed, and \((0) \in \text{Spec}(A)\) is therefore open. Since \( \{D(a)\}_{a \in A} \) is a basis for the topology there must be an element \( a \in A \) such that \((0) \in D(a)\) and \( p \notin D(a) \) for all non-zero prime ideals \( p \). Writing \( p \) as \((p)\), with \( p \in P \), we see from Proposition 7.15(a) that

\[
\begin{align*}
  p \notin D(a) \iff p \in V(a) \\
  \iff a \in p \\
  \iff a \in (p) \\
  \iff p | a.
\end{align*}
\]

In other words, \( p \notin D(a) \) for all non-zero prime ideals \( p \) if and only if all primes divide \( a \). Note from \((0) \in D(a)\) and \((a) \) of (5.3) that \( a \neq 0 \). Since units are not divisible by primes we see that \( a \) is not a unit.

Let \( u \in A \) be as in (c) and consider the element \( b := a + u \in A \). Since \( b \) is a non-zero non-unit it must, by unique factorization, be divisible by some prime \( p \). Since \( p | a \) this would imply \( p | u \), and this contradicts (IV). \( \text{q.e.d.} \)

**Corollary 12.2 :**

(a) (Euclid) The ring \( \mathbb{Z} \) has infinitely many primes.

(b) The ring of Gaussian integers has infinitely many primes.

(c) The ring of 3-cyclotomic integers has infinitely many primes.

**Proof**: That \( \mathbb{Z} \) is a PID is assumed familiar to readers. For a proof that the other two rings have the same property see, e.g., [N-Z-M, Chapter 9, §8. (the proof of)

\[54\] Which this author has not seen elsewhere, but which is probably well-known to number theorists and has probably been rediscovered many times over the years.
Theorem 9.27, pp. 431-2]. Since these rings are obviously infinite, it only remains to verify condition (c) of Theorem 12.1. To that end first note that the group of units of $\mathbb{Z}$ is $\{1, -1\}$. What we will use without proof is that the group of units of the Gaussian integers is $\{1, -1, i, -i\}$, and that of the 3-cyclotomic integers is $\{1, -1, \zeta, -\zeta, \zeta^2, -\zeta^2\}$, where $\zeta := e^{2\pi i/3} \in \mathbb{C}$.

To verify condition (c) of Theorem 12.1 for the rings listed in (a)-(c) of the current result make the following choice for the unit $u$ in the corresponding case.

(a) Take $u = 1$ if $a > 0$; $u = -1$ if $a < 0$.
(b) Here we have $a = n + im$. Take $u = 1$ if $n \geq 0; u = -1$ otherwise.
(c) In this case $a = n + \zeta m$. Take $u = 1$ if $n \geq 0; u = -1$ otherwise.

q.e.d.

---

\[\text{For proofs see, e.g., [N-Z-M, Chapter 9, §6, Theorem 9.22, p. 428].}\]
13. Specializations and Generic Points

Throughout the section $X$ is a non-empty topological space.

Let $c$ be a point of $X$ and let $C$ be a closed subset of $X$.

- $\text{cl}(\{c\})$ is the locus\(^{56}\) of $c$;
- any point of $\text{cl}(\{c\})$ is a specialization of $c$;
- $c$ is a generic point of $C$ if $\text{cl}(\{c\}) = C$ (in which case $c \in C$ must hold).

In particular, $c$ is a generic point of its locus.

When we deal with $(A, B)$-Zariski topologies and confusion might otherwise result we refer to $(A, B)$-loci, $(A, B)$-specializations, and $(A, B)$-generic points.

Examples 13.1 : In (a)-(c) we assume the $(A, B)$-Zariski topology on $B^1 = B$, with $(A, B) \subset (\mathbb{R}, \mathbb{R})$ as indicated.

(a) When $(A, B) = (\mathbb{Z}, \mathbb{R})$ we have\(^{57}\) $\text{cl}(\{\sqrt{2}\}) = \{-\sqrt{2}, \sqrt{2}\}$. The $(\mathbb{Z}, \mathbb{R})$-locus of $\sqrt{2}$ is therefore $\{-\sqrt{2}, \sqrt{2}\}$, $-\sqrt{2}$ is a $(\mathbb{Z}, \mathbb{Q})$-specialization of $\sqrt{2}$, and $\sqrt{2}$ is a $(\mathbb{Z}, \mathbb{R})$-generic point of $\{-\sqrt{2}, \sqrt{2}\}$.

(b) When $(A, B) = (\mathbb{Z}, \mathbb{R})$ we have\(^{58}\) $\text{cl}(\{\pi\}) = \mathbb{R}$ (and one can replace $\pi$ in this argument with any real number transcendental over $\mathbb{Q}$). The locus of $\pi$ is therefore $\mathbb{R}$, any real number is a specialization of $\pi$, and $\pi$ is a generic point of $\mathbb{R}$.

(c) When $(A, B) = (\mathbb{R}, \mathbb{R})$ we see from Proposition 11.2 that all points of $\mathbb{R}$ are closed. In particular, the loci of any point is that point alone, the only specialization of a point is that point alone, and no closed set other than a singleton has a generic point. (When this last condition is met the custom is to say that “there are no generic points” [“within the closed sets”], whereas the actual meaning is that no closed set with at least two distinct points admits a generic point.)

---

\(^{56}\)We have seen this definition before: immediately following the statement of Corollary 8.5. It is repeated here for ease of reference.

\(^{57}\)Argue as in Footnote 9.

\(^{58}\)Since $\pi$ is transcendental over $\mathbb{Q}$ there is no polynomial $p \in \mathbb{Z}[x]$ such that $p(\pi) = 0$. The condition that every polynomial in $\mathbb{Z}[x]$ that vanishes on $\pi$ also vanishes on $\mathbb{R}$ is therefore vacuously satisfied, and $\text{cl}(\{\pi\}) = \mathbb{R}$ follows.
(d) Suppose $R$ is a ring in which $\{0\}$ is a prime ideal. Then in \text{Spec}(R)$ with the Zariski topology: the locus of $\{0\}$ is \text{Spec}(R)$; every prime ideal is a specialization of $\{0\}$; and $\{0\}$ is the unique generic point of \text{Spec}(R)$.

(e) Suppose $(A, B) = (\mathbb{Z}, \mathbb{R})$ and $t \in R$ is such that $\sin t$ is transcendental over $\mathbb{Q}$. We claim that $(\cos t, \sin t) \in \mathbb{R}^2$ is a generic point of the circle $x^2 + y^2 = 1$ (i.e., of the algebraic subset of $\mathbb{R}^2$ corresponding to the singleton $\{x^2_1 + x^2_2 - 1\} \subset \mathbb{Z}[x]$). It follows immediately from this claim that when $\sin t$ has this property all points of the circle are specializations of $(\cos t, \sin t)$.

To prove the claim first make the identification $\mathbb{Z}[x, y] = R[x]$, where $R$ is the polynomial ring $\mathbb{Z}[y]$. Now choose any $p \in \mathbb{Z}[x]$ and use the Euclidean algorithm to write

\begin{equation}
 p(x, y) = q(x, y)(x^2 + y^2 - 1) + r(y)x + s(y),
\end{equation}

where $q(x, y) \in R[x]$ and $r(y), s(y) \in R$. If $p$ vanishes on $(\cos t, \sin t)$ then from (i) we have $r(\sin t) \cos t + s(\sin t) = 0 \Rightarrow s(\sin t) = -\cos t \cdot r(\sin t) \Rightarrow s^2(\sin t) = \cos^2 t \cdot r^2(\sin t) \Rightarrow s^2(\sin t) - (1 - \sin^2 t)r^2(\sin t) = 0$. If $r(y)$ and/or $s(y)$ is not the zero polynomial this last equality exhibits a non-zero polynomial in $\mathbb{Z}[x]$ satisfied by $\sin t$, contradicting the transcendency of $\sin t$. Thus $r[y] = s[y] = 0$, and we conclude that $p(x, y)$ is divisible by $x^2 + y^2 - 1$ when $p$ vanishes on $(\cos t, \sin t)$. But $p$ then vanishes on all points of the circle, and our claim is thereby established.

It is worth noting that not all points of the circle are generic points. For a specific example consider the point $(\sqrt{2}, \sqrt{2})$, which is obviously a zero of the polynomial $t = x - y \in \mathbb{Z}[x, y]$. If $u \in \mathbb{Z}[x, y]$ also vanishes on this point then as in (i) we can write

\begin{equation}
 u(x, y) = v(x, y)(x - y) + w(y),
\end{equation}

where $w(y) \in R := \mathbb{Z}[x]$. Then $0 = u(\sqrt{2}, \sqrt{2}) = v(\sqrt{2}, \sqrt{2}) \cdot 0 + w(\sqrt{2})$, hence $w(\sqrt{2}) = 0$. But this implies $w(-\sqrt{2}) = 0$, and we conclude that $\text{cl}(\{\sqrt{2}, -\sqrt{2}\})$ is the two-point set $\{\pm(\sqrt{2}, \sqrt{2})\}$ (which is far from being the entire circle).

\textsuperscript{59}Since $\mathbb{Z}[x]$ is a UFD one can factor $w(x)$ as a product $\Pi_{j=1}^n p_j(x)$, where each $p_j(x)$ is irreducible. Since the irreducibles of $\mathbb{Z}[x]$ are either linear or quadratic, and since $\sqrt{2}$ is not the root of a linear polynomial in $\mathbb{Z}[x]$, it follows from the quadratic formula that $-\sqrt{2}$ must also be a root of $w$. 

75
Proposition 13.2:
(a) The locus of any point \( c \in X \) is an irreducible closed subset of \( X \).
(b) If a closed set \( C \) admits a generic point then \( C \) must be irreducible.

Proof:
(a) This is a restatement of Corollary 8.5.
(b) By (a).

q.e.d.

In the following result we employ the notation surrounding (5.12).

Proposition 13.3: Suppose \( B \supset A \) is an extension of integral domains, \( n \geq 1 \) is an integer, and \( V \subset \mathbb{B}^n \) is a classical \((A,B)\)-affine algebraic set. Then the following assertions hold.

(a) A necessary condition for a prime ideal \( p \in \text{Spec}(A_B[V]) \) to be in the range of the mapping \( \varphi_V : V \to \text{Spec}(A_B[V]) \) of (5.12) is that the irreducible algebraic set \( V(f^{-1}(p)) \) admit a generic point.

(b) The condition of (a) is both necessary and sufficient when the mapping \( i \mapsto V(i) \) of Corollary 4.6, between the radical ideals of \( A[x] \) and the \((A,B)\)-Zariski closed subsets of \( \mathbb{B}^n \), is a bijection.

The hypothesis of (b) has been encountered before: recall Proposition 4.7(a).

Proof:
(a) If \( p \in \text{Spec}(A_B[V]) \) is in the range of \( \varphi_V \) we must have \( p = f(i(\{c\})) \) for some point \( c \in V \). However,
\[
p = f(i(\{c\})) \iff f^{-1}(p) = i(\{c\})
\]
\[
\implies V(f^{-1}(p)) = V(i(\{c\})) = \text{cl}(\{c\}),
\]
the last equality by Corollary 7.4(a), and the result follows.

(b) In view of (a), all we need prove is sufficiency.

It \( C \subset V \) is a closed subset there is, by hypothesis, a unique radical ideal \( q \subset A[x] \) such that \( C = V(q) \). By Proposition 5.4(d) we can write \( q = f^{-1}(p) \) for a unique prime ideal \( p \subset A_B[V] \). If \( C \) admits a generic point \( c \) then \( C = \text{cl}(\{c\}) = V(i(\{c\})) \) (by Corollary 7.7(a)). Since \( i(\{c\}) \) is radical\(^{60}\) the hypotheses force \( q = i(\{c\}) \), hence \( p = \varphi_V(C) = f(i(\{c\})) = \varphi_V(c) \).

q.e.d.

\(^{60}\)By Proposition 7.1.
14. The Compactness of Spec($R$)

Once again $R$ denotes a ring.

A topological space is \textit{quasi-compact} if every open cover has a finite subcover. For a topologist this is the definition of “compact”; algebraic geometers add “quasi” as a reminder that such spaces need not be Hausdorff.

**Theorem 14.1** : Spec($R$) is quasi-compact.

**Proof** : Since the collection $\{D(r)\}_{r \in R}$ is a basis for the Zariski topology it suffices to prove that any open cover of Spec($R$) of the form $\{D(r)\}_{r \in S \subseteq R}$ admits a finite-subcover.

So assume such a cover and let $i \subseteq R$ be the ideal generated by $S$. Then Spec($R$) = $\bigcup_{r \in S} D(r)$ and $S \subseteq i$ give Spec($R$) = $\bigcup_{r \in i} D(r) = D(i)$, whence $V(i) = \emptyset$, whereupon from (i) of Corollary 7.16, Proposition 7.11 and Corollary 7.17 we see that $\sqrt{i} = R$. But this means $1 \in \sqrt{i}$, and since $1 = 1^n$ for any integer $n \geq 1$ it follows that $1 \in i$, i.e., that there a finite collection $\{s_j\}_{j \in J} \subseteq S$ and a corresponding collection $\{r_j\}_{j \in J} \subseteq R$ such that

(i) \hspace{1cm} $1 = \sum_{j \in J} r_j s_j$.

Let $j \subseteq R$ denote the ideal generated by $\{s_j\}_{j \in J}$. Then from (i) we have $j = R$, hence $\sqrt{j} = j = R$, and from Corollary 7.17(a) and Proposition 7.12(b) we conclude that $\emptyset = V(j) = \cap_{j \in J} V(s_j)$. Taking complements then gives Spec($R$) = $\bigcup_{j \in J} D(s_j)$, and the proof is complete. \hfill \textbf{q.e.d.}
Part III - Algebraic Considerations

The two fundamental results underlying all of contemporary algebraic geometry are due to David Hilbert: the Basis Theorem and the Nullstellensatz (“theorem of zeros”). The first we have already encountered (Theorem 9.6); the second will be established, along with several important consequences, in this final part of the notes. We will see why algebraic geometers prefer to work over algebraically closed fields: under this assumption the mapping \( i \mapsto \mathcal{V}(i) \) of Corollary 4.6, from radical ideals of \( A[x] \) to classical \((B,B)\)-affine algebraic subsets of \( B^n \), is then a bijection (see Corollary 16.3).

15. The Weak Nullstellensatz

In this section we are interested in the following question: given a positive integer \( n \) and an ideal \( i \subset A[x] = A[x_1, \ldots, x_n] \), does there exist at least one point \( a = (a_1, a_2, \ldots, a_n) \in \mathbb{A}^n \) such that \( p(a) = 0 \) for all \( p \in i \)?

If \( i = A[x] \) the answer is no: in this case \( i \) contains the polynomial 1, which has no zeros.

If the inclusion \( i \subset K[x] \) is assumed proper the answer can still be no, even in the case \( n = 1 \): take \( A = \mathbb{Z} \) and let \( i = (x^2 + 1) \). On the other hand, when \( n = 1 \) and \( A = K \) is an algebraically closed field the answer is yes. Indeed, the polynomial ring \( K[x] \) is a PID, and \( i \) therefore has the form \( (q) = qK[x] \) for some polynomial \( q \in K[x] \). Since \( K \) is algebraically closed \( q \) admits a root \( a \in K \), and since every element \( p \in i \) is a multiple of \( q \) it follows that \( p(a) = 0 \) for every \( p \in i \). The Weak Nullstellensatz (“Zeros Theorem”) generalizes this last result to proper ideals of \( K[x_1, x_2, \ldots, x_n] \).

We need a preliminary result: a counterpoint to the fundamental theorem of algebra.

**Proposition 15.1:** Suppose \( K \) is an infinite field and \( 0 \neq p \in K[x] \). Then there is a point \( b = (b_1, \ldots, b_n) \in K^n \) such that \( p(b) \neq 0 \).

The hypothesis on \( K \) applies when the field is algebraically closed\(^{61}\).

**Proof:** For \( n = 1 \) this is immediate from the assumption that \( K \) is infinite and the fact that non-zero polynomials in \( K[x] \) have only finitely many roots.

\(^{61}\)This follows, e.g., from [H, Chapter V, §5, Corollary 5.9, p. 281] or [L, Chapter V, §5, Theorem 5.5, p. 247].
Assume the result for \( n \geq 1 \), suppose \( p \in K[x_1, \ldots, x_{n+1}] \), and write \( p = \sum_{j=0}^{d} p_j(x_1, \ldots, x_n)x_{n+1}^j \). Since \( p \neq 0 \) this must also be the case for at least one \( p_j \), and by the induction hypothesis we can choose \( k_1, k_2, \ldots, k_n \in K \) such that \( p_j(k_1, k_2, \ldots, k_n) \neq 0 \). The polynomial \( p(k_1, k_2, \ldots, k_n, x_{n+1}) \in K[x_{n+1}] \) is therefore non-zero, and for the reasons given in the previous paragraph we can choose \( k_{n+1} \in K \) such that \( p(k_1, k_2, \ldots, k_{n+1}) \neq 0 \).

**Theorem 15.2 (The Weak Nullstellensatz):** Suppose \( K \) is an algebraically closed field and \( i \subset K[x] = K[x_1, \ldots, x_n] \) is a proper ideal. Then \( \mathcal{V}(i) \neq \emptyset \), i.e., there must be a point \( a = (a_1, a_2, \ldots, a_n) \in K^n \) such that \( p(a) = 0 \) for all \( p \in i \).

**Proof**\(^{62} \): The proof is by induction on \( n \), and the argument for \( n = 1 \) has already been given\(^{63} \). We may therefore assume \( n \geq 1 \), and that the theorem holds for proper ideals of \( K[x_1, x_2, \ldots, x_n] \). Let \( i \) be a proper ideal of \( K[x_1, x_2, \ldots, x_{n+1}] \).

For any \( n \)-tuple \( k = (k_1, \ldots, k_n) \in K^n \) the assignment
\[
x_j \mapsto \begin{cases} x_j + k_jx_{n+1} & \text{if } 1 \leq j \leq n \\ x_{n+1} & \text{if } j = n + 1 \end{cases}
\]
determines a unique \( K \)-algebra automorphism \( \sigma_k : K[x] \rightarrow K[x] \), and the image \( \sigma_k(i) \subset K[x] \) is again a proper ideal. If for \( p \in K[x] \) we let \( q := \sigma_k(p) = p(x_1 + k_1x_{n+1}, x_2 + k_2x_{n+1}, \ldots, x_n + k_nx_{n+1}, x_{n+1}) \), then for any \( a = (a_1, a_2, \ldots, a_{n+1}) \in K^{n+1} \) and \( b := (a_1 + k_1a_{n+1}, a_2 + k_2a_{n+1}, \ldots, a_n + k_na_{n+1}, a_{n+1}) \in K^{n+1} \) we have \( q(a) = 0 \iff p(b) = 0 \). Since \( a \) can be recovered from \( b \) via \( a = (b_1 - k_1b_{n+1}, b_2 - k_2b_{n+1}, \ldots, b_n - k_nb_{n+1}, b_{n+1}) \), we conclude that it suffices to prove the theorem with \( i \) replaced by \( \sigma_k(i) \). The trick is to pick the \( n \)-tuple \( k \) in a judicious way.

Select any non-constant polynomial \( p \in i \subset K[x_1, x_2, \ldots, x_{n+1}] \) and let \( d \geq 1 \) denote the total degree\(^{64} \) of \( p \). We claim we can choose \( k = (k_1, k_2, \ldots, k_n) \in K^n \) such that \( \sigma_k(p) \) can be expressed in the form
\[
(cx_{n+1}^d + \sum_{j=0}^{d-1} q_j(x_1, x_2, \ldots, x_n)x_{n+1}^j, 0 \neq c \in K).
\]

\(^{62}\)From [Arrondo].

\(^{63}\)Two paragraphs before the statement of Proposition 15.1.

\(^{64}\)The **total degree** of a non-zero monomial \( kx_1^{d_1}x_2^{d_2}\cdots x_{n+1}^{d_{n+1}} \in K[x] = K[x_1, x_2, \ldots, x_{n+1}] \) is \( \sum d_i \); the **total degree** of a non-zero polynomial in \( K[x] \) is the maximum of the total degrees of the associated monomials.
Indeed, for any monomial \( s_m = s_m(x_1, x_2, \ldots, x_{n+1}) = t \prod_{j=1}^{n+1} x_j^{m_j} \in K[x_1, \ldots, x_{n+1}] \) \((t \in K)\) of total degree \( m \) we see that

\[
\sigma_k(s_m) = t \left( \prod_{j=1}^{n} (x_j + k_j x_{n+1})^{m_j} \right) x_{n+1}^{m_{n+1}}
\]

\[
= t \left( \prod_{j=1}^{n} (k_j x_{n+1} + x_j)^{m_j} \right) x_{n+1}^{m_{n+1}}
\]

\[
= t \left( \prod_{j=1}^{n} \left( k_j^{m_j} x_{n+1}^{m_j} + \text{monomials of total degree less than } \sum_{j=1}^{n} m_j \right) \right) x_{n+1}^{m_{n+1}}
\]

\[
= t \left( \prod_{j=1}^{n} k_j^{m_j} x_{n+1}^{m_j} \right) x_{n+1}^{m_{n+1}} + \text{monomials of total degree less than } m = \sum_{j=1}^{n+1} m_j
\]

\[
= s_m(k_1, \ldots, k_n, x_{n+1}) + \text{monomials of total degree less than } m
\]

It follows immediately that the homogeneous terms of \( \sigma_k(p) \) of total degree \( d \) are given by the polynomial \( p_d(k_1, \ldots, k_n, x_{n+1}) \in K[x_{n+1}] \). By Proposition 15.1 we can choose \((k_1, k_2, \ldots, k_{n+1}) \in K^{n+1}\) such that \( p_d(k_1, k_2, \ldots, k_n, k_{n+1}) \neq 0 \), and our claim is then established by taking \( k := (k_1, k_2, \ldots, k_n) \in K^n \).

For this particular choice for \( k \in K^n \) it follows from (i) that the ideal \( \sigma_k(i) \) contains a non-zero polynomial \( g(x) \) which is “monic in \( x_{n+1} \),” i.e., of the form

\[
\text{(ii)} \quad g(x) = x_{n+1}^d + \sum_{j=0}^{d-1} q_j x_{n+1}^j = x_{n+1}^d + \sum_{j=0}^{d-1} q_j (x_1, x_2, \ldots, x_n) x_{n+1}^j.
\]

Let \( i' \subset K[x_1, x_2, \ldots, x_n] \) denote the collection of polynomials \( p \in \sigma_k(i) \) which do not involve the indeterminate \( x_{n+1} \). This collection is easily seen to be an ideal of \( K[x_1, x_2, \ldots, x_n] \), and since \( 1 \notin \sigma_k(i) \) it must be proper. By the induction hypothesis there is a point \( \tilde{a} = (a_1, a_2, \ldots, a_n) \in K^n \), which we fix for the remainder of the proof, such that

\[
\text{(iii)} \quad p(\tilde{a}) = p(a_1, a_2, \ldots, a_n) = 0 \quad \text{for all } p \in i'.
\]

Now introduce

\[
\text{(iv)} \quad j := \{ p(a_1, a_2, \ldots, a_n, x_{n+1}) : p \in \sigma_k(i) \} \subset K[x_{n+1}],
\]

which is easily seen to be an ideal of \( K[x_{n+1}] \). We claim \( j \) is proper. If not there is a polynomial \( p \in \sigma_k(i) \) such that

\[
\text{(v)} \quad p(a_1, a_2, \ldots, a_n, x_{n+1}) = 1.
\]

Express \( p \) in the form

\[
\text{(vi)} \quad p = \sum_{j=0}^{e} p_j x_{n+1}^j = \sum_{j=0}^{e} p_j (x_1, x_2, \ldots, x_n) x_{n+1}^j,
\]

80
and note from (v) that

(vii) \[ p_0(a_1, a_2, \ldots, a_n) = 1, \quad p_j(a_1, a_2, \ldots, a_n) = 0, \quad j = 1, \ldots, e. \]

Consider the polynomial \( r \in K[x_1, x_2, \ldots, x_n] \) defined by\(^65\)

\[
(r) \quad r := \det \begin{pmatrix}
p_0 & p_1 & \cdots & p_e & 0 & 0 & \cdots & 0 \\
p_0 & 0 & \cdots & p_{e-1} & p_e & 0 & \cdots & 0 \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
g_0 & g_1 & \cdots & g_{d-1} & 1 & 0 & \cdots & 0 \\
g_0 & 0 & \cdots & g_{d-2} & g_{d-1} & 1 & 0 & \cdots \\
\vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots \\
0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{d-1} & 1 \\
\end{pmatrix}
\]

We compute the determinant by means of elementary column operations while viewing \( r \) as a polynomial in \( K[x_1, x_2, \ldots, x_{n+1}] \): first multiply column two by \( x_{n+1} \) and add the result to column one; then multiply column three by \( x_{n+1}^2 \) and add the result to (the modified) column one, etc. From (vi) and (ii) the first column is ultimately converted to

\[
\begin{pmatrix}
p \\
x_{n+1}p \\
\vdots \\
x_{n+1}^{d+e-1}p \\
g \\
x_{n+1}g \\
\vdots \\
x_{n+1}^{d+e-1}g \\
\end{pmatrix}
\]

whereupon expanding the determinant of the full matrix down this column leads to the conclusion that \( r \) must be a linear combination of \( p \) and \( g \). Since \( p, g \in \sigma_{k}(i) \) it follows that the same holds for \( r \), i.e., that

(ix) \[ r \in i'. \]

\(^{65}\)This polynomial is commonly called the “resultant” of \( p \) and \( g \).
However, one sees from (vii) that when the polynomials appearing in (viii) are evaluated at $a = (a_1, a_2, \ldots, a_n)$ the matrix reduces to a lower triangular matrix with entry 1 in each diagonal position. This gives $r(a) = r(a_1, a_2, \ldots, a_n) = 1$, which by virtue of (ix) is a contradiction to (iii). The claim, i.e., that the ideal $j \subset K[x_{n+1}]$ is proper, is thereby established.

Since $K[x_{n+1}]$ is a PID we can write $j = (s)$ for some $s \in K[x_{n+1}]$. If $s \neq 0$ pick a zero $a_{n+1} \in K$ of $s$, and we then have $p(a_1, a_2, \ldots, a_n, a_{n+1}) = 0$ for all $p \in \sigma_k(i)$. If $s = 0$ we see from (iv) that for any choice of $a_{n+1} \in K$ we have $p(a_1, a_2, \ldots, a_n, a_{n+1}) = 0$ for all $p \in \sigma_k(i)$, and the proof is complete. \textbf{q.e.d.}

\textbf{Corollary 15.3 :} Suppose the field $K$ is algebraically closed, $m \geq 1$, and polynomials $p_1, \ldots, p_m \in K[x] = [x_1, \ldots, x_n]$ have no common zero. Then there are elements $q_1, \ldots, q_m \in K[x]$ such that $\sum_{j=1}^m q_j p_j = 1$, i.e., the ideal $(p_1, \ldots, p_m) \subset K[x]$ generated by $p_1, \ldots, p_m$ is the algebra $K[x]$.

\textbf{Proof :} By the Weak Nullstellensatz (Theorem 15.2) the ideal $(p_1, \ldots, p_m) \subset K[x]$ cannot be proper. \textbf{q.e.d.}

The Weak Nullstellensatz has some additional consequences which are not so immediately evident.

\textbf{Corollary 15.4 :} Suppose $A$ is a subdomain of $K$ and $B \supset A$ is a finitely generated $A$-algebra. Then there is an $A$-algebra homomorphism $r : B \to K$.

If $B \subset K$ we could take $r$ to be inclusion. The interesting case occurs when $B \subsetneq K$.

\textbf{Proof :} By assumption there is an $A$-algebra epimorphism $f : A[x] = A[x_1, \ldots, x_n] \to B$ for some positive integer $n$. Set $i := \ker f$ and let $j$ be the ideal of $K[x]$ generated by $i$. By Theorem 15.2 we can choose an element $a = (a_1, \ldots, a_n) \in K^n$ such that

\begin{enumerate}
  \item [(i)] $p(a) = 0$ for all $p \in j$.
\end{enumerate}

Let $q : A[x] \to K$ be the ring homomorphism characterized by $x_j \mapsto a_\ell$, $\ell = 1, \ldots, n$. By (i) we have $i \subset \ker q$, and since $B \simeq K[x]/i$ the existence of $r$ is now a consequence of the First Isomorphism Theorem of commutative ring theory.\textsuperscript{66} \textbf{q.e.d.}

\textsuperscript{66}More precisely, of the straightforward analogue of that theorem for algebras. See, e.g., [H, Chapter III, §2, Corollaries 2.10 and 2.11, p. 126].
Corollary 15.5: Suppose \( L \) is a field and \( M \supset L \) is an extension of fields with the added property that \( M \) is finitely generated as an \( L \)-algebra\(^{67}\). Then the extension \( M \supset L \) is finite algebraic.

This result also goes by the name “Hilbert’s Nullstellensatz.”

Proof: Letting \( K \) be an algebraic closure of \( L \) we see from Corollary 15.4 that there is an \( L \)-algebra homomorphism \( r : M \rightarrow K \), and since \( M \) is a field this must be an embedding.

q.e.d.

Corollary 15.6: Suppose \( B \subset A \) is an extension of integral domains with \( B \) a finitely generated \( A \)-algebra. Then any embedding \( f : A \rightarrow K \) of \( A \) into an algebraically closed field extends to an \( A \)-algebra homomorphism \( g : B \rightarrow K \).

We derive this as a consequence of the weak Nullstellensatz, but it is in fact equivalent\(^{68}\).

Proof: Choose a set \( S \) disjoint from \( B \cup K \) having the same cardinality as \( B \setminus A \). By definition there must be a bijection \( \alpha : B \setminus A \rightarrow S \), and we can extend this to a bijection \( \beta : B \rightarrow \hat{B} := S \cup f(A) \) by

\[
\beta : b \mapsto \begin{cases} 
  f(b) & \text{if } b \in A, \\
  \alpha(b) & \text{if } b \in B \setminus A.
\end{cases}
\]

Using \( \beta \) we can transfer the ring extension structure \( B \supset A \) to \( \hat{B} \supset f(A) \), and \( \beta \) then becomes a \( A \)-algebra isomorphism\(^{69}\). By Corollary 15.4 there is an \( A \)-algebra homomorphism \( r : \hat{B} \rightarrow K \), and the composition \( r \circ \beta : B \rightarrow K \) is then an \( A \)-algebra homomorphism extending \( f \).

q.e.d.

\(^{67}\)In other words, there is a finite subset \( S \subset M \) such that every element of \( M \) can be written as a polynomial in the elements of \( S \) with coefficients in \( K \).

\(^{68}\)For a proof of the weak Nullstellensatz assuming Corollary 15.6 see, e.g., [L, Chapter IX, §1, pp. 379-80].

\(^{69}\)Such set-theoretic constructions of extensions are common in field theory, e.g., see the proof of [L, Proposition 2.3, Chapter V, §2, p. 231].
16. The Nullstellensatz

Theorem 16.1 (Hilbert’s Nullstellensatz) : Suppose $K$ is an algebraically closed field, $i \subset K[x] = K[x_1, \ldots, x_n]$ is an ideal, and $p \in K[x]$ vanishes at all zeros of $i$. Then $p \in \sqrt{i}$.

The conclusion can also be stated: $p \in \mathcal{V}(i) \Rightarrow p \in \sqrt{i}$, where $\mathcal{V} \subset K^n$.

Proof: If $p = 0$ there is nothing to prove, so assume otherwise. By the Hilbert Basis Theorem (Theorem 9.6) the ideal $i$ is finitely generated, say by $p_1, \ldots, p_m \in K[x]$.

The trick\(^70\) is to add an additional indeterminate $y$ to the collection $\{x_1, \ldots, x_n\}$ and consider the ideal of $K[x, y] = K[x_1, \ldots, x_n, y]$ generated by $\{p_1, \ldots, p_m, 1 - yp\}$. By assumption $p_1, \ldots, p_m$ and $1 - yp$ have no common zero, and from Corollary 15.3 we conclude that there are elements $q_1, \ldots, q_{m+1} \in K[x, y]$ such that

$$q_1p_1 + \cdots + q_mp_m + q_{m+1}(1 - yp) = 1.$$  

Substituting $1/p$ for $y$ and multiplying by a sufficiently high power of $p$ to clear the resulting denominators we can convert the resulting equality to the form

$$h_1p_1 + \cdots + h_mp_m = p^r,$$

and $p \in \sqrt{i}$ is thereby established. \(\text{q.e.d.}\)

Corollary 16.2 : For any ideal $i \subset K[x]$ one has $\sqrt{i} = \mathcal{V}(i)$.

Proof: We have $\mathcal{V}(i) \subset \sqrt{i}$ by Theorem 16.1. For the reverse inclusion first recall from Proposition 7.3(b) that $i \subset \mathcal{V}(i)$. By Proposition 7.1 the last ideal is radical, and $\sqrt{i} \subset \sqrt{i(\mathcal{V}(i))} = \mathcal{V}(i)$ follows. \(\text{q.e.d.}\)

Corollary 16.3 : When $K$ is an algebraically closed field the mapping $i \mapsto \mathcal{V}(i)$ from radical ideals of $K[x] = K[x_1, \ldots, x_n]$ to classical affine algebraic subsets of $K^n$ is an inclusion reversing bijection.

Proof: By Proposition 4.7. \(\text{q.e.d.}\)

\(^70\)Called the “Rabinowitsch trick.”

84
17. Applications to the Mapping  
\( \varphi_\mathcal{V} : \mathcal{V} \to \text{Spec}(K_K[\mathcal{V}]) \)

In this section \( K \) is an algebraically closed field, \( n \geq 1 \) is an integer, and \( \mathcal{V} \subset \mathcal{B}^n \) is a classical \((K,K)\)-affine set.

The mapping \( \varphi_\mathcal{V} : \mathcal{V} \to \text{Spec}(K_K[\mathcal{V}]) \) was introduced (in greater generality) in (5.12). For ease of reference we recall the definition:

\[
(17.1) \quad \varphi_\mathcal{V} : c \in \mathcal{V} \mapsto f(i\{c\}) \in \text{Spec}(K_K[\mathcal{V}]),
\]

where \( f : K[x] \to K_K[\mathcal{V}] \) is the canonical homomorphism. We have seen (in Proposition 5.13(b)) that \( \varphi_\mathcal{V} \) is continuous. As we will see, with the algebraically closed assumption on \( K \) we can say far more. We need the following consequence of the Weak Nullstellensatz.

**Proposition 17.2**: When the field \( K \) is algebraically closed all maximal ideals of \( K[x] \) have the form \((x - b_1, x - b_2, \ldots, x - b_n)\), where \( b_j \in K \) for \( j = 1, 2, \ldots, n \). By means of this association the maximal ideals of \( A[x] \) are in one-to-one correspondence with the points \((b_1, b_2, \ldots, b_n) \in K^n\), and all such points are closed.

**Proof**: First recall from Example 3.2(e) that the defining ideal \( i\{c\} \) of a point \( c = (b_1, b_2, \ldots, b_n) \in K^n \) must have the form \((x - b_1, x - b_2, \ldots, x - b_n)\); then recall from Proposition 7.5 that

\[
(i) \quad \mathcal{V}(i\{c\}) = \{c\}
\]

and that the defining ideal of any point of \( K^n \) is proper.

We claim that any maximal ideal \( m \subset K[x] \) has the form \( i\{e\} \) for some point \( e \in K^n \). Indeed, by Theorem 15.2 there is a zero \( e = (d_1, d_2, \ldots, d_n) \in K^n \) of \( m \), and since any polynomial in \( m \) vanishes on \( e \) it follows that \( m \subset i\{e\} \). Since \( m \) is maximal and \( i\{e\} \) is proper this forces \( m = i\{e\} = (x_1 - d_1, x_2 - d_2, \ldots, x_n - d_n) \).

We claim that any ideal of the form \( i\{c\} = (x_1 - b_1, x_2 - b_2, \ldots, x_n - b_n) \) is maximal. Otherwise we see from the proper inclusion \( i\{c\} \subset K[x] \) and Corollary 10.3 that there must be a maximal ideal \( m \) containing \( i\{c\} \), whence from the previous paragraph that \( m = i\{d\} \) for some point \( d \in K^n \). However, from \( i\{c\} \subset m \) and \( (i) \) we have \( \{d\} = \mathcal{V}(m) \subset \mathcal{V}\{c\} = \{c\} \), hence \( c = d \), and \( i\{c\} = i\{d\} = m \) is therefore maximal.

This proves all but the final assertion, and that is a special case of Proposition 11.2.

q.e.d.

85
Theorem 17.3: The mapping $\varphi_V : V \to \text{Spec}(K_K[V])$ is injective with image $\text{maxSpec}(K_K[V])$, and this image is dense in $\text{Spec}(K_K[V])$.

Proof: For the injectivity and initial image assertions use (17.1) and Proposition 10.8 in combination with Proposition 17.2. To establish the final assertion it suffices, by Proposition 10.9, to prove that for any non-zero $[p] \in K_K[V]$ there is a maximal ideal of $K_K[V]$ not containing $[p]$. Taking $b$ as in Proposition 15.1 we have $p \notin i(\{b\})$, and the desired result follows easily. (If $i(\{b\}) \in \ker(f)$ for all such $b$, where $f$ is as in (17.1), then $[p] = [0]$, contrary to assumption.) q.e.d.
Notes and Comments

References [Ku] and [Mac] were very influential in the organization of the material herein. In particular, Proposition 13.3 is adapted from [Ku, Chapter 1, §4, p. 25]. References [Ful], [Iit], [Ueno-1] and [Ueno-2] were consulted with such frequency that it is difficult to attribute proper credit.

References


R.C. Churchill
Department of Mathematics
Hunter College (CUNY),
the Graduate Center, CUNY, and
the University of Calgary
e-mail rchurchi@hunter.cuny.edu