A Brief Introduction to Algebraic Geometry

- Corrected, Revised, and Extended as of 25 November 2007 -

R.C. Churchill

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 between such sets. (Regular mappings are also defined in §2.) 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 bogging down in the technical quicksand surrounding the trees. It is hoped that these notes will assist students in untangling the morass: they approach the subject from what could cynically be described as a rather narrow perspective, but they contain far more than the usual amount of detail and they include simple examples illustrating how algebraic geometers would work within this limited context. Their perusal should allow readers to get at least one foot in the door. Wishing for anything more would be unrealistic: one is never going to achieve a deep understanding of 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 regarding our narrow perspective: 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 (e.g., Bezout's Theorem[1] on the intersection of projective varieties).

[1]See, e.g., [Mum, Chapter 5, §5.B, pp. 80-85].

Contents

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 for arbitrary $n \geq 3$, 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[2] 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 ℓ. 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^ℓ, b^ℓ, c^ℓ would be a solution of $x^4 + y^4 = z^4$ in non-zero integers, and this contradicts Fermat's result for $n = 4$.

[2]Success was first reported in 1993; full details were first published in 1995.

If n is not a multiple of 4 then from $n \geq 3$ we see from the Fundamental Theorem of Arithmetic that n must have an odd prime factor p, and we can therefore write $n = mp$ for some positive integer m. From

$$(c^m)^p = c^{mp} = c^n = a^n + b^n = (a^m)^p + (b^m)^p$$

we then conclude that a^m, b^m, 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 $n \geq 3$.

There are various ways to reformulate Fermat's theorem geometrically. We develop the ideas in greater generality to avoid later digressions.

Let K be a field and let $2 \leq n \in \mathbb{Z}$. A subset $S \subset K^n$ is a *hypersurface* if there is a polynomial $q \in K[x_1, x_2, \ldots, x_n]$ such that $S := \{\, (r_1, r_2, \ldots, r_n) \in K^n \,:\, q(r_1, r_2, \ldots, r_n) = 0 \,\}$. Any such q is a *defining polynomial* of S. Example: the *unit* $(n-1)$*-sphere* $S^{n-1} := \{\, v \in \mathbb{R}^n \,:\, |v|^2 = 1 \,\} \subset \mathbb{R}^n$ is a hypersurface with defining polynomial $q = (\sum_{j=1}^n x_j^2) - 1$. When $n = 3$ hypersurfaces are called *surfaces*; when $n = 2$ they are called (*planar* or *plane*) *curves*.

Consider the case $K = \mathbb{Q}$ and $n = 3$ of the previous paragraph, write (x_1, x_2, x_3) as (x, y, z), let $p \geq 3$ be a prime, and let $q = x^p + y^p - z^p$. Then q is the defining polynomial of a surface $S_p \subset \mathbb{Q}^3$ called the[3] *Fermat surface* (*corresponding to* p). The reason for the name should be evident: Fermat's Last Theorem is equivalent to the assertion that this surface contains no "non-trivial integer points", i.e., points $(a, b, c) \in \mathbb{Z}^3 \subset \mathbb{Q}^3$ satisfying $abc \neq 0$.

The *Fermat curve*[4] associated with a prime $p \geq 3$ is the curve in $\mathbb{Q}^2$ with defining polynomial $x^p + y^p - 1$, i.e., $\{(x, y) \in \mathbb{Q}^2 \,:\, x^p + y^p = 1\}$. 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 $a^p d^p + b^p c^p = c^p d^p$, hence $c^p(d^p - b^p) = a^p d^p$, and from the unique factorization of

[3]This terminology is not standard. However, the "Fermat curve" terminology about to be introduced is standard, although for technical reasons one often regards that curve as a subset of $\mathbb{C}^2$.

[4]The definition varies from author to author, e.g., in [Lang_{aaf}, 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 $(a, \pm b, c) \in \mathbb{Z}^3 \backslash \{(0,0,0)\}$ 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

$$x^p + y^p = 1 \qquad \text{and} \qquad xyz = 1. \tag{1.1}$$

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*[5]. 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[6]

$$y^2 = x(x - a^p)(x + b^p). \tag{1.2}$$

This curve is *elliptic*, i.e., topologically a torus[7], and quite a bit is known about such entities. But the Frey curve did not conform to the usual expectations for an elliptic

[5]The terminology is not standard, but proves convenient.

[6]The equation appears to ignore the integer c, but it is hidden within. Specifically, define the *discriminant* of a monic cubic polynomial $x^3 + Bx^2 + Cx + D$ to be the square of the product of the differences of the roots, i.e., $-4C^2 - 27D^2 - 4B^3D + B^2C^2 + 18BCD$, and check that the discriminant of $x(x - a^p)(x + b^p)$ is given by $(abc)^{2p}$.

[7]Technically, only after projectivizing; we are merely attempting to convey the flavor of the argument. A heuristic justification of our geometric description of the curve will be given in Example 2.2(c).

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[8] from Ribet's result.

[8]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 α, i.e., the collection of solutions of the system of equations

$$p_\alpha(x_1, \ldots, x_n) = 0, \qquad \alpha \in \Omega, \tag{2.1}$$

is the *classical* (A, B)*-affine algebraic set* determined by[9] $\mathcal{P}$, 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). When $n = 2$ a classical (A, B)-affine algebraic set is called a (A, B)*-planar curve*. 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 B is clear from context.

Examples 2.2 :

(a) Take $A = \mathbb{Z}$, $B = \mathbb{R}$, $n = 3$, and let $\mathcal{P}$ denote the two-element subset $\{\, x_1^2 + x_2^2 - 1,\, x_1^2 + x_2^2 + x_3^2 - 2 \,\} \subset \mathbb{Z}[x] = \mathbb{Z}[x_1, x_2, x_3]$. 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 with radius exceeding that of the cylinder. The classical $(\mathbb{Z}, \mathbb{R})$-affine algebraic set determined by $\mathcal{P}$ 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.

(b) The non-planar Fermat curve corresponding to a fixed prime $p \geq 3$ is a classical $(\mathbb{Z}, \mathbb{Q})$-affine algebraic subset of $\mathbb{Q}^3$: take $\mathcal{P}$ to be the two-element collection $\{\, x_1^p + x_2^p - 1,\, x_1x_2x_3 - 1 \,\} \subset \mathbb{Z}[x_1, x_2]$.

[9] 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.

(c) The plane Fermat and Frey curves provide examples of classical (A, B)-algebraic sets 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 $\mathcal{P} = \{\, x_2^2 - x_1(x_1 - a^p)(x_1 + b^p) \,\}$ (with $(A, B) = (\mathbb{Z}, \mathbb{C})$ respectively.

To satisfy the curious we briefly (and non-rigorously) indicate how the Frey curve can be viewed as an elliptic curve[10] (i.e., as a torus). This is also done to convince readers that the geometric aspects of algebraic sets need not be lost when one moves to the complex domain.

Write the defining polynomial as

(i) $$y^2 = x(x - a^p)(x + b^p),$$

and begin with the observation that $(x, y) = (0, 0)$, $(a^p, 0)$ and $(-b^p, 0)$ are three distinct[11] points on curve, i.e., they provide three solutions of (i). We can visualize the remaining solutions by first imagining three copies of the complex plane $\mathbb{C}$ stacked one above the other, with the middle plane regarded as the "actual" $\mathbb{C}$. Label the planes above and below $\mathbb{C}$ as $\mathbb{C}_A$ and $\mathbb{C}_B$. For each choice of $x \in \mathbb{C} \setminus \{0, a^p, -b^p\}$ there are evidently two distinct choices for y such that (x, y) satisfies (i), with one choice being the negative of the other. Imagine these two choices as being represented by the points of $\mathbb{C}_A$ and $\mathbb{C}_B$ directly above and below x respectively (ignoring the fact that these two points, when regarded as complex numbers, would generally not correspond to the complex numbers y of the two solution pairs $(x, \pm y)$). The totality of solutions is then seen to be represented by the union of $\mathbb{C}_A \setminus \{0, a^p, -b^p\} \subset \mathbb{C}_A$, $\mathbb{C}_B \setminus \{0, a^p, -b^p\} \subset \mathbb{C}_B$, and the three-point subset $\{0, a^p, -b^p\} \subset \mathbb{C}$. Put another way: the totality of solutions can be regarded as $\mathbb{C}_A \cup \mathbb{C}_B$ with the understanding that the three particular solutions $(0, 0)$, $(a^p, 0)$ and $(-b^p, 0)$ (and no others) have been represented twice.

To achieve a more aesthetically pleasing description let $S^2 \subset \mathbb{R}^3$ denote the unit sphere centered at the origin, i.e., $\{\, x = (x_1, x_2, x_3) \in \mathbb{R}^3 \,:\, x_1^2 + x_2^2 + x_3^2 = 1 \,\}$, designate $(0, 0, 1) =: np \in S^2$ as the "north pole" of this sphere, and identify each of $\mathbb{C}_A$ and $\mathbb{C}_B$ with disjoint copies of $S^2 \setminus \{np\}$ by means of stereographic

[10] For a rigorous and far more general treatment of this situation see, e.g., [Gunn, §10(b), pp. 229-240]. For a brief discussion restricted to the Riemann surface perspective see, e.g., [Fors, Chapter 1, §8, Example 8.10, pp. 55-6].

[11] $a^p \neq 0 \neq b^p$ since a, b and c are assumed non-zero integers, and $a^p \neq -b^p$ for the same reason: otherwise $a^p + b^p = c^p$ implies $c = 0$.

projection from np. The totality of solutions of (i) is then represented by two copies of $S^2 \setminus \{np\}$, again with the understanding the the three specific solutions mentioned above have duplicate representations.

We can do slightly better by first agreeing that the pair (∞, ∞) also provides a solution[12] to (i). By associating this pair with $np \in S^2$ the totality of solutions can then be viewed as the disjoint union $S^2_A \cup S^2_B$ of two 2-spheres, although now four solutions have duplicate representations, i.e., $(0,0)$, $(a^p, 0)$, $(-b^p, 0)$ and (∞, ∞).

Now slit each of S^2_A and S^2_B between[13] 0 and a^p and between $-b^p$ and np, force each of the slits open[14], and reshape each into a circle[15] with 0 and a^p diametrically opposite on one circle and $-b^p$ and np diametrically opposite on the other. Now pucker small neighborhoods of each of these circles slightly outward. The result will be two spheres with two volcanic peaks on each, with the peaks labeled by the base pairs $(0, a^p)$ and $(-b^p, np)$ respectively. Glue corresponding crater rims together, i.e., glue S^2_A to S^2_B along the craters corresponding to $(0, a^p)$, and then along the craters corresponding to $(-b^p, np)$. Notice that duplications have now been eliminated[16]. The totality of solutions of (i), with (∞, ∞) tossed in for good measure, is thereby given the appearance of two spheres connected by two tubes. Anyone with a bit of topological training will immediately recognize this as a torus[17].

(d) Each space B^n is a classical (A, B)-affine algebraic set, no matter what the

[12]For those seeking a rigorous treatment: this is where projective space enters the picture.

[13]That is, think of each sphere as the skin of a hollow orange, and use a sharp knife to cut one slice in each from 0 to a^p, and another, again in each, from $-b^p$ to np.

[14]In terms of the hollow orange skin analogy, pull each of the four slits open with two fingers or both thumbs.

[15]That is, reshape the forced-opened slits so that each of the two spheres now appears with two circular holes in the surface.

[16]Provided one is sufficiently careful when slitting, reshaping, and gluing. Specifically, when making the prescribed slits in S^2_A and S^2_B and re-forming these slits into circles an edge will appear on half of each circle, e.g., running clockwise from 0 to a^p, but not on the other half. A simple analogy would be: if you are sufficiently careful when slitting the plane along the x-axis, and if you then pull the two resulting half-planes apart, one of the half-planes will have an edge (i.e., it will be closed when regarded as a subset of the plane) and the other will not (i.e., it will be open when so regarded). When the craters are glued together one must glue the closed edge on one crater to the open edge on the other. Moreover, one must glue 0 to 0, a^p to a^p, $-b^p$ to $-b^p$, and ∞ to ∞. Otherwise duplication will not be eliminated.

[17]Others might think of it this way: if you blow enough air into the figure it will eventually begin to look like an inner tube.

extension $B \supset A$: take $\mathcal{P} = \{0\}$. When viewed in this manner B^n is called *A-affine n-space* and is written as[18] $\mathbb{A}^n_A(B)$. When this notation is employed a classical (A, B)-affine algebraic set within $\mathbb{A}^n_A(B)$ is sometimes called[19] an *A-algebraic set* in[20] $\mathbb{A}^n_B(B)$.

When the manner of regarding B^n is not of consequence we ease notation by writing B^n in place of $\mathbb{A}^n_A(B)$. For example, when dealing with functions between such spaces we generally write $f : B^n \to B^m$ rather than $f : \mathbb{A}^n_A(B) \to \mathbb{A}^m_A(B)$.

(e) 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_α is a non-zero constant polynomial.

(f) To better understand the role of the extension $B \supset A$ 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 polynomial $x^2 - 2$ as no rational roots. However, when $B = \mathbb{R}$ or $\mathbb{C}$ we have $\mathcal{V}(\mathcal{P}) = \{\pm\sqrt{2}\} \subset B^1 = B$.

(g) 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[21] $-\sqrt{2}$, 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 $x - \sqrt{2} \in \mathbb{R}[x]$.

The reader needs to be aware of certain terminology associated with a classical (A, B)-affine algebraic set $\mathcal{V} \subset B^n$.

- B^n is the *ambient space* of $\mathcal{V}$. When specific reference to this space proves useful the notations $\mathcal{V}$ and $\mathcal{V}(\mathcal{P})$ are replaced by $\mathcal{V}_{\mathbb{A}^n_A(B)}$ and $\mathcal{V}_{\mathbb{A}^m_A(B)}(\mathcal{P})$ respectively.

[18] The symbol $\mathbb{A}$ within the notation $\mathbb{A}^n_A(B)$ is an abbreviation for the term "affine." In particular, it has no connection with the subscript A.

[19] Particularly when A and B are fields.

[20] Many authors assume from the outset that B is a field, that $A = B$, and that B is algebraically closed. Put another way, they impose hypotheses which exclude many important examples from number theory.

[21] 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 $p(-\sqrt{2}) = q \cdot \big((-\sqrt{2})^2 - 2\big) = 0$.

- When C is a ring intermediate to A and B the points of $\mathcal{V} \cap C^n$ are called[22] *C-rational points* of $\mathcal{V}$. This generalizes the definition of "rational point" given in the paragraph surrounding (1.1). The definition given there corresponds to the case $A = \mathbb{Z}$ and $C = B = \mathbb{Q}$, whereas we can now speak, for example, of $\mathbb{Q}$-rational points of the classical $(\mathbb{Z}, \mathbb{C})$-affine algebraic curve $x^p + y^p = 1$ within $\mathbb{C}^2$.

- When B is an algebraically closed field the points of a classical B-affine algebraic set $\mathcal{V} \subset B^n$ are called *geometric points*[23] of $\mathcal{V}$.

- Suppose $B \supset A$ is a ring extension. An element $b \in B$ is *integral*[24] over A if b is a zero of a monic polynomial $p \in A[x]$. (Example: Take $B \supset A$ to be $\mathbb{R} \supset \mathbb{Z}$, $b = \sqrt{2}$, and $p = x^2 - 2$.) Now suppose $A = \mathbb{Z}$, that B is an integral domain, that $n \geq 1$ is an integer, and that $\mathcal{V} \subset B^n$ is a classical $(\mathbb{Z}, B)$-affine algebraic set. A point $c = (b_1, b_2, \ldots, b_n) \in \mathcal{V}$ is an *arithmetic point*[25] of $\mathcal{V}$ if each coordinate b_j of c is integral over $\mathbb{Z}$. Note this will be the case if and only if there is a finite algebraic extension field $C \supset \mathbb{Q}$ contained in the quotient field of B such that $b_j \in C$ for $j = 1, 2, \ldots, n$. In algebraic number theory a finite extension field of $\mathbb{Q}$ is called an *algebraic number field*, and a great deal of the work in that subject is done within such fields.

- Suppose that B is an algebraically closed field, $A = B$, $C \subset B$ is a subfield, and $\mathcal{V}$ is the zero set of a collection of polynomials in $C[x_1, x_2, \ldots, x_n]$. Then one says that $\mathcal{V}$ is *defined over* C and that C is a *field of definition*[26] for $\mathcal{V}$. This definition is rather subtle. It appears that one could simply assume $A = C$, and this is indeed the case regarding our work up to this point. However, the

[22]The terminology is generally restricted to the case when A, B and C are fields, e.g., see [EDM, §16.A, p. 68].

[23]The definition is adapted from [Mac, Chapter 6, p. 49].

[24]The "integral" terminology is used because when $B = \mathbb{Q}$ and $A = \mathbb{Z}$ the defining condition characterizes those rational numbers which are integers, i.e., a rational number $r \in \mathbb{Q}$ is integral over $\mathbb{Z}$ if and only if $r \in \mathbb{Z}$. See, e.g., [Sw-D, Chapter I, §1, Theorem 1, pp. 1-2].

Of course when $B \supset A$ is a field extension the definition of b being integral over A is equivalent to that of b being algebraic over A. Readers are assumed familiar with the latter concept.

[25]This definition is, admittedly, a guess on the part of this author. I have heard the terminology used quite frequently, but none of the many references I have consulted (including [EDM]) offers a definition of an arithmetic point. Arithmetic schemes, however, are another matter: see, e.g., [E-H, Chapter II, §4, pp. 81-89]. The definition I offer was motivated by this particular reference, but does not appear there explicitly.

[26]These definitions are taken from [EDM, §16.A, p. 68].

choice $A = C$ would change the morphisms we will be associating with $\mathcal{V}$ (see Example 2.5).

In practice affine algebraic sets are generally indicated with less formality than employed thus far. For example, the two-circle classical affine algebraic subset of $\mathbb{R}^3$ introduced in Example 2.2(a) might be described as "the intersection of the cylinder $x_1^2 + x_2^2 = 1$ with the sphere $x_1^2 + x_2^2 + x_3^2 = 2$." Similarly, 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 $x_1^p + x_2^p = 1$."

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 does define 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 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 $0 \in B$.

One distinguishes 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[27]. For such reasons we will write an element $p \in A[x_1, \ldots, x_n]$ as $p(x)$ when this proves convenient.

Suppose $\mathcal{V} \subset B^n$ and $\mathcal{W} \subset B^m$ are classical (A, B)-affine algebraic sets. A mapping $g : \mathcal{V} \to \mathcal{W}$ is a *classical* (A, B)*-morphism*, or a *classical* (A, B)*-regular function*, if it is the restriction to $\mathcal{V}$ of a *polynomial mapping* $h : B^n \to B^m$,

[27]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.

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 $j = 1, \ldots, m$. An (A, B)-morphism $g : \mathcal{V} \to \mathcal{W}$ is an (A, B)-*isomorphism*, or simply an *isomorphism* when A and B are understood, if there is an (A, B)-morphism $r : \mathcal{W} \to \mathcal{V}$ such that[28] $r \circ g = \mathrm{id}_{\mathcal{V}}$ and $g \circ r = \mathrm{id}_{\mathcal{W}}$. 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 2.3 :

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

$$\begin{aligned} y_1 &= x_1, \\ y_2 &= x_2, \end{aligned}$$

restricts to a $(\mathbb{Z}, \mathbb{Q})$-morphism from $\mathcal{V}$ into $\mathcal{W}$, i.e., the mapping $(x_1, x_2, x_3) \in \mathcal{V} \mapsto (x_1, x_2) \in \mathcal{W}$ 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 $\mathcal{W}$.

(b) Let $\mathcal{V} \subset \mathbb{R}^2$ denote the hyperbola defined by the polynomial $x_1^2 - x_2^2 = 1$ and let $\mathcal{W} \subset \mathbb{R}^3$ 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 $g := h|_{\mathcal{V}} : \mathcal{V} \to \mathcal{W}$. In fact this is an isomorphism: the inverse is the restriction to $\mathcal{W}$ 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 $\mathcal{W} \subset \mathbb{R}^2$ 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 $x \in \mathbb{R} \mapsto (x, x) \in \mathcal{W}$ and $x \in \mathbb{R} \mapsto (x, -x) \in \mathcal{W}$ are morphisms.

(d) Let $\mathcal{V} \subset \mathbb{R}^3$ 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 $\mathcal{W} \subset \mathbb{R}^2$ denote the unit circle, i.e., the classical affine algebraic set define 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 $\mathcal{V}$ is not a morphism from $\mathcal{V}$ to $\mathcal{W}$ since the latter is a proper subset of the image of $\mathcal{V}$.

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.

[28] Here and throughout the notes id_X denotes the identity mapping $x \in X \mapsto x \in X$ of a set X.

Proposition 2.4 : *Suppose* $f : B^n \to B^m$ *is a polynomial mapping and* $\mathcal{Q} \subset A[y_1, y_2, \ldots, y_m]$. *Define* $f^*(\mathcal{Q}) \subset A[x_1, x_2, \ldots, x_n]$ *by*

$$f^*(\mathcal{Q}) := \{\, q \circ f : q \in \mathcal{Q} \,\},$$

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* $f_j(x_1, x_2, \ldots, x_n),\ j = 1, 2, \ldots, m$. *Then*

$$f^{-1}(\mathcal{V}_{\mathbb{A}^m(B)}(\mathcal{Q})) = \mathcal{V}_{\mathbb{A}^n_A(B)}(f^*(\mathcal{Q})).$$

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

$$\begin{aligned} c \in f^{-1}(\mathcal{V}_{\mathbb{A}^m(B)}(\mathcal{Q})) &\Leftrightarrow f(c) \in \mathcal{V}_{\mathbb{A}^m(B)}(\mathcal{Q}) \\ &\Leftrightarrow q(f(c)) = 0 \ \text{ for all } \ q \in \mathcal{Q} \\ &\Leftrightarrow (q \circ f)(c) = 0 \ \text{ for all } \ q \in \mathcal{Q} \\ &\Leftrightarrow (q \circ f)(c) = 0 \ \text{ for all } \ q \circ f \in f^*(\mathcal{Q}) \\ &\Leftrightarrow c \in \mathcal{V}_{\mathbb{A}^n_A(B)}(f^*(\mathcal{Q})). \end{aligned}$$

q.e.d.

Example 2.5 : The singleton set $\{2\} \subset \mathbb{R}$ is a classical (A, B)-affine algebraic subset of $\mathbb{R} = \mathbb{R}^1$, both for $(A, B) = (\mathbb{Z}, \mathbb{R})$ and $(A, B) = (\mathbb{R}, \mathbb{R})$, whereas $\{\sqrt{2}\} \subset \mathbb{R}$ is only classically $(\mathbb{R}, \mathbb{R})$-affine algebraic. If $\{2\}$ and $\{\sqrt{2}\}$ were $(\mathbb{Z}, \mathbb{R})$-isomorphic then $\{\sqrt{2}\}$ would be a classical $(\mathbb{Z}, \mathbb{R})$-affine algebraic subset of $\mathbb{R}$ by Proposition 2.4, which we have just seen is not the case. On the other hand, these two singleton sets are $(\mathbb{R}, \mathbb{R})$-isomorphic: such an isomorphism is given by the restriction to $\{\sqrt{2}\,\}$ of the mapping defined by the polynomial $\sqrt{2}\,x \in \mathbb{R}[x]$. The moral is: *the choice of* A *makes a difference regarding which functions are morphisms.*

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[29]. Unfortunately, that goal has yet to achieved. Moreover, attaining that goal within the near future seems totally unrealistic; the correct

[29] 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.

mathematical tools for the job seem lacking[30]. As a result one is often (but not always) forced to settle for less, e.g., one seeks invariants (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.

We close the section by introducing some terminology which the reader might encounter when consulting other references, but which might well be formulated in those references with slightly different notation. Let $B \supset A$ be an extension of fields, let $n \geq 1$ be an integer, and let $\mathcal{V} \subset B^n$ be a classical B-affine algebraic set. Suppose there is a classical A-affine algebraic set $\mathcal{W} \subset A^m$ such that $\mathcal{W}$, when considered as a subset of B^m, is both classically (A, B)-affine algebraic and (A, B)-isomorphic to $\mathcal{V}$. Then one says that $\mathcal{W}$ can be (or "is") obtained from $\mathcal{V}$ by[31] *descending the base field of* $\mathcal{V}$ *from* B *to* A. Example: $\{2\} \subset \mathbb{R}$ is defined as a classical $(\mathbb{R}, \mathbb{R})$-affine algebraic set by the polynomial $x - 2 \in \mathbb{R}[x]$, and $\{3\} \subset \mathbb{Q}$ is defined as a classical $(\mathbb{Q}, \mathbb{Q})$-affine algebraic set by the polynomial $x - 3 \in \mathbb{Q}[x]$. However, since $\mathbb{R} \supset \mathbb{Q}$, and since the defining polynomials are both in $\mathbb{Q}[x]$, each of these sets can be considered as classical $(\mathbb{Q}, \mathbb{R})$-affine algebraic sets, and as such they are $(\mathbb{Q}, \mathbb{R})$-isomorphic by means of the mapping of $\{3\} \to \{2\}$ associated with the polynomial $p = (2/3)x \in \mathbb{Q}[x]$. In other words, $\{3\}$ can be obtained from $\{2\}$ by descending the base field from $\mathbb{R}$ to $\mathbb{Q}$.

[30]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. **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.

[31]The definition is adapted from [S, Chapter V, §4.20, p. 102].

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*[32] *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 $\mathcal{V} \subset B^n$ be an algebraic set and let[33]

$$\mathfrak{i}(\mathcal{V}) := \{\, p \in A[x] \,:\, p(b_1, b_2, \ldots, b_n) = 0 \text{ for all } (b_1, b_2, \ldots, b_n) \in \mathcal{V} \,\}. \tag{3.1}$$

This is an ideal of $A[x]$, as is easily verified; it is the *defining* (A, B)*-ideal* of $\mathcal{V}$, or simply the *defining ideal* of $\mathcal{V}$ when A and B are understood. The factor ring[34]

$$A_B[\mathcal{V}] := A[x]/\mathfrak{i}(\mathcal{V}) \tag{3.2}$$

is the (A, B)*-coordinate ring* of $\mathcal{V}$, or simply the *coordinate ring* of $\mathcal{V}$, and is generally identified with the collection of regular functions[35] from $\mathcal{V}$ into B. Indeed, for any $p \in A[x]$ the restriction $p(x)|_{\mathcal{V}}$ 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 $p(x) - g(x)$ vanishes on $\mathcal{V}$, i.e., if and only if $p - q \in \mathfrak{i}(\mathcal{V})$.

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

Examples 3.3 :

(a) Take $(A, B) = (\mathbb{Z}, \mathbb{Q})$, $n = 1$, and $\mathcal{P} = \{\, x^2 - 2 \,\}$. Then $\mathcal{V} = \mathcal{V}(\mathcal{P}) = \emptyset$ (because $x^2 - 2$ has no roots in $\mathbb{Q}$). The condition $b \in \mathcal{V} \Rightarrow p(b) = 0$ is

[32] I.e., for the remainder of the notes; not simply within this section.

[33] The definitions in this section are patterned after those in [Mac, Introduction, pp. 3-5], but there A and B are assumed fields.

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

[35] I.e., (A, B)-regular functions.

vacuously satisfied for all $p \in A[x]$, and $\mathfrak{i}(\mathcal{V}) = A[x]$ follows. The coordinate ring $A_B[\mathcal{V}]$ is the trivial (i.e., one element) ring[36].

(b) Take $(A, B) = (\mathbb{Z}, \mathbb{R})$, $n = 1$, and $\mathcal{P} = \{\, x^2 - 2 \,\}$. (Except for B, these are the same choices made in (a).) Then we obviously have $\mathcal{V} = \{-\sqrt{2}, \sqrt{2}\,\}$; what might not be quite so obvious is 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[37] 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 $\mathbb{Z}[\sqrt{2}\,] := \{\, a + b\sqrt{2} \,:\, a, b, \in \mathbb{Z}\,\}$ 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 $\mathbb{Z}[\sqrt{-1}\,] := \{\, a + ib \,:\, a, b \in \mathbb{Z}\,\}$ 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 [El].)

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

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

It is well-known[38] 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 $\mathcal{V} := \{e^{j \cdot 2\pi i/p}\}_{j=1}^{p-1}$ 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[39]. We follow custom and write $\mathcal{V}$ as $\{\zeta^j\}_{j=1}^{p-1}$, where $\zeta := e^{2\pi i/p}$.

---

[36]Note that this is consistent with the set-theoretical result that for any non-empty set Y there is precisely one function from $\emptyset$ into Y. Indeed, in set theory one defines a function from a set X to a set Y to be a subset of $X \times Y$ having certain properties. If $X = \emptyset$ then $X \times Y = \emptyset$, and $\emptyset \subset X \times Y$ vacuously satisfies the properties required of a function, and even those of a regular function. Since $\emptyset$ is the only subset of $\emptyset \times Y$ it is the unique function mapping $\emptyset$ into Y.

[37]As in Footnote 21.

[38]This is generally established as a first or second application of the Eisenstein irreducibility criterion, as in [L, Chapter IV, §3, p. 184].

[39]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.

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 $\mathfrak{i}(\mathcal{V}) = (\Phi_p(x)) \subset \mathbb{Z}[x]$. Since $\Phi_p(x)$ is irreducible it follows that the coordinate ring $\mathbb{Z}_{\mathbb{C}}[\mathcal{V}] = \mathbb{Z}[x]/\mathfrak{i}(\mathcal{V})$ can be identified with the subring

$$\text{(ii)} \qquad \mathbb{Z}[\zeta] := \{\, a_0 + a_1\zeta + \cdots + a_{p-2}\zeta^{p-2} \,:\, a_0, a_1, \ldots, a_{p-2} \in \mathbb{Z} \,\}$$

of $\mathbb{C}$.

In algebraic number theory this is the ring of *p-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[40].

(e) 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

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

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.[41] 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 $\mathfrak{i}(\{c\})$. If $p \in \mathfrak{i}(\{c\})$ 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

$$\begin{aligned} p &= q_0(x_1, x_2, \ldots, x_{n-1}) + \textstyle\sum_{j=1}^{\ell} q_j(x_1, x_2, \ldots, x_{n-1})(x_n - b_n)^j \\ &= {}_0(x_1, x_2, \ldots, x_{n-1}) + \left(\textstyle\sum_{j=1}^{\ell} q_j(x_1, x_2, \ldots, x_{n-1})(x_n - b_n)^{j-1} \right) \cdot (x_n - b_n) \\ &= q_0(x_1, x_2, \ldots, x_{n-1}) + q(x_1, x_2, \ldots, x_n) \cdot (x_n - b_n). \end{aligned}$$

[40] For a quick and entertaining sketch of Kummer's work see, e.g., [Riben, Chapter 5, §1, pp. 223-7].

[41] The concept of generating sets of ideals is defined formally in the paragraph following the proof of Proposition 3.8. However, the description given here should suffice for present purposes.

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 $p \in (x_1 - b_1, x_2 - b_2, \ldots, x_n - b_n)$.

As for the coordinate ring, note from from the definition of the defining ideal that

$$\text{(i)} \qquad \mathfrak{i}(\{c\}) = \ker(f_c), \qquad \text{where} \qquad f_c : p \in B[x] \mapsto p(c) \in B.$$

Since f_c is a surjection we see from the First Isomorphism Theorem of Ring Theory[42] that

$$\text{(ii)} \qquad B[\{c\}] = B_B[\{c\}] := B[x]/\mathfrak{i}(\{c\}) \simeq B.$$

With the benefit of hindsight we can see that this identification should have been expected: since $\{c\}$ consists of a single point, the collection of functions $r : \{c\} \to B$ is in one-one correspondence with the collection of values $r(c) \in B$; since any $b \in B$ is such a value (because $A = B$), the collection is in one-one correspondence with B.

---

[42] The First Isomorphism Theorem is a consequence of a more general result which we will also find useful. (As usual, "ring" means "commutative ring with unity," and homomorphisms are assumed to carry unities to unities.)

Theorem : Let $f : R \to S$ be a ring homomorphism and let $\mathfrak{i} \subset R$ be an ideal contained in $\ker(f)$. Then f factors uniquely through the canonical homomorphism $g : R \to R/\mathfrak{i}$, i.e., there is a unique ring homomorphism $h : R/\mathfrak{i} \to S$ which makes the diagram

$$\begin{array}{ccc} R & \xrightarrow{f} & S \\ {\scriptstyle g}\downarrow & \overset{h}{\nearrow} & \\ R/\mathfrak{i} & & \end{array}$$

commute. Moreover, h is an isomorphism if and only if f is an epimorphism and $\mathfrak{i} = \ker(f)$.

Corollary (The First Isomorphism Theorem of Ring Theory) : Any homomorphism $f : R \to S$ of rings induces an isomorphism between $R/\ker(f)$ and the image of f in S.

For proofs of both result see, e.g., [H, Chapter III, §2, Theorem 2.9 and Corollary 2.10, pp. 125-66].

(f) By taking $\mathcal{V} = B^n$ in (3.1) we see that

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

Suppose B is a field. Since a polynomial with coefficients in a field has at most finitely many roots, $\mathfrak{i}(B^n) = \{0\}$ when B is infinite, in which case[43] $A_B[B^n] = A[x]/\{0\} \simeq A[x]$.

(g) The usual unit circle S^1 of the Euclidean plane, i.e., the planar curve $x^2+y^2 = 1$, is obviously a $(\mathbb{Z}, \mathbb{R})$-algebraic subset of $\mathbb{R}^2$. To determine the defining ideal and coordinate ring make the identification $\mathbb{Z}[x, y] = R[x]$, where R is the polynomial ring $\mathbb{Z}[y]$. Now choose any $p \in R[x]$ and use the Euclidean algorithm to write

(i) $$p(x, y) = q(x, y) \cdot (x^2 + y^2 - 1) + r(y)x + s(y),$$

where $q(x, y) \in R[x]$ and $r(y), s(y) \in R$. Finally, choose any $t \in \mathbb{R}$ such that $\sin t$ is transcendental[44] over $\mathbb{Q}$. If p vanishes on the circle then in particular p vanishes on $(\cos t, \sin t)$, whereupon from (i) we see that $r(\sin t)\cos t + s(\sin t) = 0 \Rightarrow s(\sin t) = -\cos t \cdot r(\sin t) \Rightarrow s^2(\sin t) = \cos^2 t \cdot r^2(\sin t) \Rightarrow s^2(\sin t) - (1 - \sin^2 t)r^2(\sin t) = 0$. 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 the unit circle. The defining ideal $\mathfrak{i}(S^1)$ of S^1 is therefore the principal ideal $(x^2+y^2-1) \subset \mathbb{Z}[x, y]$, and the coordinate ring must then be

(ii) $$\mathbb{Z}_{\mathbb{R}}[S^1] = \mathbb{Z}[x, y]/(x^2 + y^2 - 1).$$

One should think of this coordinate ring as the polynomial ring $\mathbb{Z}[x, y]$ subject to the relation

(iii) $$y^2 = 1 - x^2.$$

For example, the product $(1+x^2y)(y+x^2y^3)$ in the ring would then be computed

[43] Read the symbol "$\simeq$" as "(which) is (being) identified with."

[44] Since the elements of $\mathbb{R}$ which are algebraic over $\mathbb{Q}$ form a countable set, "most" $t \in \mathbb{R}$ will have the required property.

as

$$\begin{aligned}(1+x^2y)(y+x^2y^3) &= y+x^2y^2+x^2y^3+x^4y^4\\ &= y+x^2y^2+x^2y^2y+x^4(y^2)^2\\ &= y+x^2(1-x^2)+x^2(1-x^2)y+x^4(1-x^2)^2\\ &= x^2-2x^6+x^8+(1+x^2-x^4)y.\end{aligned}$$

The argument concluding with (ii) actually establishes more than the structure of the defining ideal and coordinate ring of the unit circle, and for later use[45] we record the additional result: *if* $t \in \mathbb{R}$ *is such that* $\sin t$ *is transcendental over* $\mathbb{Q}$*, and if* $p \in \mathbb{Z}[x,y]$ *vanishes on the point* $(\cos t, \sin t) \in S^1$*, then* p *vanishes on* S^1*.*

(h) The parabola $P \subset \mathbb{R}^2$ given by the graph of $y = x^2$ is a $(\mathbb{Z},\mathbb{R})$-algebraic set, and we can determine the coordinate ring with a minor variation of the argument used in the previous example. Specifically, in this case we define $R := \mathbb{Z}[x]$ (rather than $R := \mathbb{Z}[y]$), make the identification $\mathbb{Z}[x,y] \simeq R[y]$, and use the Euclidean algorithm to to write any polynomial $p \in R[y]$ as

$$p(x,y) = q(x,y)\cdot(y-x^2) + r(x),$$

where $q(x,y) \in R[y]$ and $r(x) \in R$.

Assuming p vanishes on P choose any real number t transcendental over $\mathbb{Q}$. Then p vanishes on the point (t,t^2), hence $r(t) = 0$, and this contradicts transcendency unless $r(x) = 0$. We conclude that

(i) $$\mathbb{Z}_{\mathbb{R}}[P] = \mathbb{Z}[x,y]/(y-x^2) \simeq \mathbb{Z}[x,x^2] \simeq \mathbb{Z}[x].$$

Just as in the previous example, we have established more than the structure on the defining ideal and coordinate ring: we have shown that *if* $t \in \mathbb{R}$ *is transcendental over* $\mathbb{Q}$*, and if* $p \in \mathbb{Z}[x,y]$ *vanishes on the point* $(t,t^2) \in P$*, then* p *vanishes on* P*.*

(i) The usual "y-axis" of the Euclidean plane is a classical $(\mathbb{R},\mathbb{R})$-affine algebraic set: it is the zero set of the singleton $\mathcal{P} = \{x\}$. By using the Euclidean algorithm in a manner similar to that seen in several previous examples it is a simple matter to show that defining ideal is the principal ideal (x), and the coordinate ring is therefore $\mathbb{R}[x]/(x) \simeq \mathbb{R}$.

[45] See Example 14.3(e).

(j) Thus far the examples of defining ideals and coordinate rings have involved only the empty set, finite sets of points, and curves. To construct "higher dimensional" examples choose any integer $n \geq 2$ and note that the n-sphere $S^n := \{ x = (x_1, x_2, \ldots, x_{n+1}) \in \mathbb{R}^{n+1} : \sum_{j=1}^{n+1} x_j^2 = 1 \}$ is a classical $(\mathbb{Z}, \mathbb{R})$-affine algebraic subset of $\mathbb{R}^{n+1}$. Following the idea seen in Examples (g) and (h) define $R := \mathbb{Z}[x_1, x_2, \ldots, x_n]$, make the identification $\mathbb{Z}[x] := \mathbb{Z}[x_1, x_2, \ldots, x_{n+1}] \simeq R[x_{n+1}]$, choose any $p \in \mathbb{Z}[x]$ and write

$$p(x) = q(x) \cdot \left(\sum_{j=1}^{n+1} x_j^2 - 1 \right) + r(x_1, x_2, \ldots, x_n) x_{n+1} + s(x_1, x_2, \ldots, x_n).$$

(Note that $r, s \in R$.) Choose any $t \in (0, 1)$ which is transcendental over $\mathbb{Q}$ and consider the point $c := (t, t, \ldots, t, \sqrt{1 - nt^2}) \in S^n$. If p vanishes on S^n then in particular p vanishes on c, hence $r(t, t, \ldots, t) \cdot \sqrt{1 - nt^2} + s(t, t, \ldots, t) = 0$, and therefore

$$r^2(t, t, \ldots, t) \cdot (1 - nt^2) - s^2(t, t, \ldots, t) = 0.$$

As before, the transcendency of t over $\mathbb{Q}$ then forces $r[x_1, x_2, \ldots, x_n] = s[x_1, x_2, \ldots, x_n] = 0$. It follows that

(i) $$\mathfrak{i}(S^n) = (\textstyle\sum_{j=1}^{n+1} x_j^2 - 1)$$

and that

(ii) $$\mathbb{Z}_{\mathbb{R}}[S^n] = \mathbb{Z}[x_1, x_2, \ldots, x_{n+1}]/(\textstyle\sum_{j=1}^{n+1} x_j^2 - 1).$$

Note that in Example 3.3(b) the element $\sqrt{2}$ is integral[46] over $\mathbb{Z}$ (because $\sqrt{2}$ is a zero of the monic polynomial $t^2 - 2 \in \mathbb{Z}[t]$); in Example (c) the element i is integral over $\mathbb{Z}$ (because $i := \sqrt{-1}$ is a zero of the monic polynomial $t^2 + 1 \in \mathbb{Z}[t]$); in Example (d) the element ζ is integral over $\mathbb{Z}$ (because it is a zero of the (monic) third cyclotomic polynomial); in Example (g) the element y is integral over $R[x]$ (because y is a zero of the monic polynomial $t^2 + (x^2 - 1) \in (R[x])[t]$).

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

Proposition 3.4 : *Suppose $\mathcal{W} \subset B^n$ is an algebraic set and $f : A[x] \to A_B[\mathcal{W}]$ is the canonical homomorphism. Then*

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

[46]The concept was defined in the fourth bulleted item following Examples 2.2.

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 $\mathfrak{i} \subset R$ be an ideal. The *radical* of $\mathfrak{i}$, denoted $\sqrt{\mathfrak{i}}$, is the collection of all elements $r \in R$ such that $r^m \in \mathfrak{i}$ for some positive integer m (generally depending on r). One checks easily that $\sqrt{\mathfrak{i}}$ is an ideal containing $\mathfrak{i}$; one calls $\mathfrak{i}$ a[47] *radical ideal* when $\sqrt{\mathfrak{i}} = \mathfrak{i}$.

Our first example of a radical ideal is given as a proposition for later reference. For the statement recall that an ideal $\mathfrak{p}$ of a ring R is *prime* if $\mathfrak{p} \neq R$ and $R/\mathfrak{p}$ is an integral domain. An equivalent definition[48], which is the one used in the proof of Proposition 3.5, is: if $r, s \in R$ and $rs \in \mathfrak{p}$ then $r \in \mathfrak{p}$ or $s \in \mathfrak{p}$ (or both). Example: When A is an integral domain and x is a single indeterminate the principal ideal $(x) \in A[x]$ is prime (because $A[x]/(x) \simeq A$ is an integral domain).

Proposition 3.5 : *Any prime ideal is radical.*

Proof : Suppose $\mathfrak{p}$ is a prime ideal of a ring R and $r \in R$ satisfies $r^m \in \mathfrak{p}$ for some positive integer m. We need to prove that $r \in \mathfrak{p}$, which we note is obvious if $m = 1$. Proceeding by induction, suppose $m > 1$ and write $r^m = rr^{m-1}$. Since $\mathfrak{p}$ 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 $(k) \in \mathbb{Z}$ 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 $\sqrt{(n)} = (\prod_{j=1}^{k} p_j)$, and (n) is radical if and only if all $n_j = 1$. Specific examples: $\sqrt{(250)} = (10)$ (because

[47] 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].

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

$$\text{(i)} \qquad [r][s] = [rs] = [0] \qquad \Leftrightarrow \qquad rs \in \mathfrak{p}.$$

If $rs \in \mathfrak{p}$ and $R/\mathfrak{p}$ is an integral domain the left hand equality in (i) forces $[r] = [0]$ or $[s] = [0]$, hence $r \in \mathfrak{p}$ or $s \in \mathfrak{p}$. Conversely, if $rs \in \mathfrak{p}$ implies $r \in \mathfrak{p}$ or $s \in \mathfrak{p}$ then (i) implies $[r] = [0]$ or $[s] = [0]$, and $R/\mathfrak{p}$ is therefore an integral domain.

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 3.6 : *The radical of any ideal of a ring R is a radical ideal, i.e., for all ideals $\mathfrak{i} \subset R$ one has $\sqrt{\sqrt{\mathfrak{i}}} = \sqrt{\mathfrak{i}}$.*

Proof : The inclusion $\sqrt{\mathfrak{i}} \subset \sqrt{\sqrt{\mathfrak{i}}}$ is immediate from the definition of the radical. To prove the opposite inclusion choose any $q \in \sqrt{\sqrt{\mathfrak{i}}}$. Then $q^n \in \sqrt{\mathfrak{i}}$ for some integer $n \geq 1$, hence $q^{n+m} = (q^n)^m \in \mathfrak{i}$ for some integer $m \geq 1$, and $q \in \sqrt{\mathfrak{i}}$ 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[49]. 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 3.7 : *Let R be a ring and let $\mathfrak{i} \subset R$ be an ideal. Then $R/\mathfrak{i}$ is reduced if and only if $\mathfrak{i}$ is radical.*

Proof : For any $r \in R$ the coset $[r] \in R/\mathfrak{i}$ satisfies $[r]^m = [0]$ for some positive integer m if and only $r^m \in \mathfrak{i}$. It follows that $R/\mathfrak{i}$ has no non-zero nilpotent elements if and only if for all $r \in R$ the condition $r^m \in \mathfrak{i}$ for some positive integer m implies $r \in \mathfrak{i}$, i.e., if and only if $\mathfrak{i}$ is radical. **q.e.d.**

Radical ideals and reduced rings enter algebraic geometry though the follow result.

Proposition 3.8 : *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 $\sqrt{\mathfrak{i}(\mathcal{V})}$. Then for some positive integer m we have $q^m \in \mathfrak{i}(\mathcal{V})$, hence $0 = q^m(c) = (q(c))^n$ for all $c = (b_1, b_2, \ldots, b_n) \in \mathcal{V}$. Since B is assumed reduced we must have $q(c) = 0$ for all such c, and $q \in \mathfrak{i}(\mathcal{V})$ follows. This proves that $\mathfrak{i}(\mathcal{V})$ is radical; the final assertion is then immediate from Proposition 3.7. **q.e.d.**

[49] As is the coset $[2] \in \mathbb{Z}/4\mathbb{Z}$. The simultaneous conditions $[2]^3 = [0]$ and $[2]^2 \neq [0]$ are somehow more interesting to this author than the single condition $[2]^2 = [0]$.

Coordinate rings have an additional structure which will play a crucial role later in the notes. To give details we need a few preliminaries, and to avoid later digressions with analogous constructions these are presented in greater generality than our current needs require.

Let R be a (commutative) ring (with unity) and let S be either:

(a) a ring containing R as a subring;

(b) a (left) R-module; or

(c) an R-algebra.

Note that (a) may be regarded as a special case of (c); nevertheless, it proves useful to list them separately. Also note that (b) includes the case when $S \subset R$ is an ideal and, by taking $R = \mathbb{Z}$, the case when S is an abelian group (written additively). To treat the three possibilities simultaneously we introduce provisional terminology, valid only in this paragraph: we refer structures assumed in each of the three cases as "algebraic structures" of types (a)-(c) respectively. Let (d) denote any one of (a), (b) and (c) and let $E \subset S$ be any non-empty subset. Then the intersection $E_R \subset S$ of all the algebraic structures of type (d) containing E is again such a structure, with $E_R = S$ a distinct possibility. E_R is said to be *generated* by E, the collection E is a *generating set* of E_R, and the elements of E are said to be *generators* of E_R. (Generators need not be unique, as one learns from the study of bases in elementary linear algebra.) When E is finite one says that E_R is *finitely generated* (*over* R). In particular, one says that S is *finitely generated* (*over* R) when $S = E_R$ for some finite set E. In case (a) the algebraic structure E_R consists of all finite sums $\sum_j r_j e_j$ with $r_j \in R$ and $e_j \in E \subset S$. This is immediately evident from two observations: this collection is a subring of R containing E; this collection must be contained in any subring containing E. In case (b) the algebraic structure E_R has the same description (for virtually the same reasons). In case (c) E_R consists of polynomials in the elements of E with coefficients in R (again for virtually the same reasons). In cases (a) and (c) one writes E_R as $R[E]$, or simply as $R[e_1, e_2, \ldots, e_n]$ when $E = \{e_1, e_2, \ldots, e_n\}$ is finite. In particular, one writes E_R as $R[e]$ when $E = \{e\}$ is a singleton[50]. Note that in (c) the R-algebra $R[E]$ can also be considered as an R-module (by ignoring multiplication amongst the elements of E). In these circumstances it is quite possible that $R[E]$ is finitely generated as an R-algebra while not being finitely generated as an R-module. For example, the usual polynomial ring $\mathbb{R}[x]$ in one indeterminate is finitely generated as an $\mathbb{R}$-algebra (it is generated by the singleton $\{x\}$), but is not finitely generated as an $\mathbb{R}$-module

[50]This notation has already been employed in Examples 3.3(b)-(d).

(because $\{1, x, x^2, x^3, \dots\}$ is a basis). When an R-algebra is finitely generated as an R-module one says that the R-algebra is a[51] *finite R-algebra*, or, when R is understood, that it is *finite*.

Proposition 3.9 : *Let R be a ring and let S be an R-algebra. Then S is finitely generated as an R-algebra, by a generating set consisting of n elements, if and only if there is a surjective R-algebra homomorphism $f : R[x_1, x_2, \dots, x_n] \to S$ from the usual polynomial ring $R[x_1, x_2, \dots, x_n]$ onto S. Moreover, when this is the case there is a ring isomorphism*

$$\text{(i)} \qquad S \simeq R[x_1, x_2, \dots, x_n]/\ker(f).$$

To indicate that the stated conditions hold one often writes S as $R[a_1, a_2, \dots, a_n]$, where $a_j := f(x_j)$ for $j = 1, 2, \dots, n$, although any particular a_j would generally not appear if that element could be expressed as an R-coefficient polynomial in the a_i with[52] $1 \leq i < j$. In particular, the integer n is not unique. We have already encountered this notational convention in Examples 3.3, e.g., in denoting the ring of 3-cyclotomic integer by $\mathbb{Z}[\zeta]$ (see Example 3.3(d)).

Proof :

$\Rightarrow$ By assumption we have $S = E_R$ for some finite set $E = \{e_1, e_2, \dots, e_n\}$. Consider the polynomial algebra $R[x_1, x_2, \dots, x_n]$ and recall, from standard properties of such algebras, that the assignment $x_j \mapsto e_j$ for $j = 1, 2, \dots, n$ lifts to an R-algebra homomorphism $f : R[x_x, x_2, \dots, x_n] \to S$. To see that f is surjective recall from the paragraph preceding the proposition that any $s \in S$ can be written as a polynomial $p(e_1, e_2, \dots, e_n)$ with coefficients in R, hence $s = f(p)$.

$\Leftarrow$ By assumption any $s \in S$ can be written $s = f(p)$ for some polynomial $p \in R[x_1, x_2, \dots, x_n]$. Since $f(r \prod_j x_j^{n_j}) = r \prod_j (f(x_j))^{n_j}$ it follows that any element of S can be written as a polynomial in the elements $f(x_j) \in S$, hence that S is generated by this finite collection.

The identification (i) is a consequence of the First Isomorphism Theorem of Ring Theory[53]. **q.e.d.**

Corollary 3.10 : *The coordinate ring of any classical (A, B)-affine algebraic set is finitely generated as an A-algebra.*

[51] Our definition is taken from [A-M, Chapter 2, p. 30].

[52] For example, one would most likely write $\mathbb{Z}[\sqrt{2}, -\sqrt{2}]$ as $\mathbb{Z}[\sqrt{2}]$.

[53] See Footnotefirstiso.

Proof : Immediate from (3.2). **q.e.d.**

Any finitely generated A-algebra is called an *affine A-algebra*. (One is tempted to say "affine (A, B)-algebra," but the definition has nothing to do with B.)

Corollary 3.11 : *When B is reduced the coordinate ring of any classical (A, B)-affine algebraic set is a reduced affine A-algebra.*

Proof : Recall Proposition 3.8. **q.e.d.**

One easily checks that the collection of all affine A-algebras, together with all A-algebra homomorphisms between such rings, forms a category, and that the collection of reduced affine A-algebras[54] and homomorphisms between such rings is a subcategory thereof.

Assume the notation of the paragraph surrounding (3.1), suppose $\mathcal{W} \subset B^m$ is a second algebraic set, and suppose that $g : \mathcal{V} \to \mathcal{W}$ is a regular function, i.e., the restriction to $\mathcal{V}$ 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 $\tilde{h}^* : A[y] := A[y_1, y_2, \ldots, y_m] \to A[x] = A[x_1, x_2, \ldots, x_n]$ is defined by

$$\tilde{h}^* : q \in A[y] \mapsto q \circ h \in A[x]. \tag{3.12}$$

If $q \in \mathfrak{i}(\mathcal{W})$ and $x \in \mathcal{V}$ it is then evident that $(q \circ h)(x) = q(h(x)) = 0$ (because $h(x) = g(x) \in \mathcal{W}$), whence from (3.12) that $\tilde{h}^* q \in \mathfrak{i}(\mathcal{V})$. In this way we see that g induces a ring homomorphism $h^* : A_B[\mathcal{W}] := A[y]/\mathfrak{i}(W) \to A_B[\mathcal{V}] := A[x]/\mathfrak{i}(\mathcal{V})$ between the associated coordinate rings. Specifically,

$$h^*([q]) := [q \circ h], \qquad q \in A[y], \tag{3.13}$$

wherein the left and middle square brackets denote equivalence classes (w.r.t. the equivalence relation "have the same restriction to $\mathcal{V}$").

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

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

[54] Affine A-algebras are not automatically reduced, e.g., the non-reduced ring $\mathbb{Z}/4\mathbb{Z}$ is an affine $\mathbb{Z}$-algebra. Nor is the reverse inclusion true: the polynomial ring $\mathbb{Z}[x_1, x_2, x_3, \ldots]$ in infinitely many variables is reduced, but is not finitely generated.

hence $[q\circ h] = [q\circ f]$, and it follows that definition (3.13) depends only on the equivalence class of h. For this reason one writes $h^* : A_B[\mathcal{W}] \to A_B[\mathcal{V}]$ as $g^* : A_B(\mathcal{W}) \to A_B[\mathcal{V}]$.

To summarize: when $g : \mathcal{V} \subset B^n \to \mathcal{W} \subset B^m$ is a morphism of classical (A, B)-affine algebraic sets an A-algebra homomorphism $g^* : A_B[\mathcal{W}] \to A_B[\mathcal{V}]$ is well-defined by the rule

$$g^* : [q] \in A_B[\mathcal{W}] \mapsto [q \circ h] \in A_B[\mathcal{V}], \tag{3.14}$$

where $h : B^n \to B^m$ is any polynomial function satisfying $g = h|_{\mathcal{V}}$.

Theorem 3.15 : *When B is reduced the assignments*

$$\mathcal{V} \mapsto A_B[\mathcal{V}]$$

and

$$g : \mathcal{V} \to \mathcal{W} \qquad \mapsto \qquad g^* : A_B[\mathcal{W}] \to A_B[\mathcal{V}]$$

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

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

To conclude the section we offer an elementary example of how the functor of Theorem 3.15 can be used in connection with the classification problem discussed at the end of the previous section.

Example 3.16 : *The unit circle $x^2 + y^2 = 1$ and the parabola $y = x^2$, considered as classical $(\mathbb{Z}, \mathbb{R})$-affine algebraic subsets of $\mathbb{R}^2$, are not isomorphic* (within the category of classical $(\mathbb{Z}, \mathbb{R})$-affine algebraic sets[55]). Indeed, if they were isomorphic it would follow from Theorem 3.15 that their coordinate rings would be isomorphic as $\mathbb{Z}$-algebras. In Examples 3.3(g) and (h) we found these coordinate rings to be $\mathbb{Z}[x, y]$, subject to the relation

$$y^2 = 1 - x^2,$$

and $\mathbb{Z}[x]$ respectively. The second is a UFD[56], but one sees from the two factorizations $x^2 = x \cdot x = (1 - y)(1 + y)$ that this is not the case for the first. The rings are therefore not isomorphic.

[55]The result may seem obvious, but perhaps less so when one realizes that at the projective level [which involves a different category] these two curves are isomorphic.

[56]I.e., a unique factorization domain. See, e.g., [H, Chapter III, §6, Theorem 6.14, p. 164].

One could say that the adjective "algebraic" entered "algebraic geometry" because the functor introduced in Theorem 3.15 played such a dominant role in the study of classical affine algebraic sets[57]. More recently the study of such sets was transformed by the introduction of two additional functors, and these are the focus of the next two sections.

[57]The "functor" terminology is far more recent than the use of algebraic techniques. That terminology 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* $A[x] := A[x_1, x_2, \ldots, x_n]$.

In this section we abandon the ring-theoretic approach to the study of affine algebraic sets and move in a completely different direction. Specifically, we use the algebraic subsets of B^n to construct a topology on this space, then endow any algebraic subset with the induced topology, and examine the consequences by means of a functor into the category of topological spaces and continuous mappings. The construction requires a few preliminaries.

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

$$\mathcal{P} \subset \mathcal{Q} \qquad \Rightarrow \qquad \mathcal{V}(\mathcal{Q}) \subset \mathcal{V}(\mathcal{P}). \tag{4.1}$$

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

$$\begin{aligned} c \in \mathcal{V}(\mathcal{Q}) &\Leftrightarrow p(c) = 0 \text{ for all } p \in \mathcal{Q} \\ &\Rightarrow p(c) = 0 \text{ for all } p \in \mathcal{P} \\ &\Leftrightarrow c \in \mathcal{V}(\mathcal{P}), \end{aligned}$$

and (4.1) follows.

As we now show, the collection $\mathcal{P}$ of polynomials defining an algebraic set $\mathcal{V}(\mathcal{P})$ can always be assumed an ideal, and when B is reduced that ideal can be assumed radical.

Proposition 4.2 : *For any subset* $\mathcal{P} \subset A[x]$ *one has*

$$\text{(i)} \qquad \mathcal{V}(\mathcal{P}) = \mathcal{V}((\mathcal{P})),$$

and when B *is reduced one also has*

$$\text{(ii)} \qquad \mathcal{V}(\mathcal{P}) = \mathcal{V}((\mathcal{P})) = \mathcal{V}(\sqrt{(\mathcal{P})}\,).$$

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

$$\mathfrak{i} \subset \mathfrak{i}(\mathcal{V}(\mathfrak{i})), \tag{4.3}$$

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., $\mathcal{V}((x^2)) = \{0\}$, 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 4.2 : For any point $c = (b_1, b_2, \ldots, b_n) \in B^n$ one has

$$\begin{aligned} c \in \mathcal{V}(\mathcal{P}) &\Leftrightarrow p(c) = 0 \text{ for all } p \in \mathcal{P} \\ &\Leftrightarrow \textstyle\sum_j r_j p_j(c) = 0 \text{ for all finite sums} \\ &\qquad \textstyle\sum_j r_j p_j \text{ with } (r_j, p_j) \in B \times \mathcal{P} \\ &\Leftrightarrow c \in \mathcal{V}((\mathcal{P})). \end{aligned}$$

Equality (i) follows.

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

$$\text{(iii)} \qquad \mathcal{V}((\mathcal{P})) \subset \mathcal{V}(\sqrt{(\mathcal{P})}\,).$$

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

$$\begin{aligned} c \in \mathcal{V}((\mathcal{P})) &\Rightarrow q^m(c) = 0 \\ &\Leftrightarrow (q(c))^m = 0 \\ &\Leftrightarrow q(c) = 0 \text{ (because } B \text{ is reduced)}, \end{aligned}$$

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. **q.e.d.**

When R is a (commutative) ring (with unity $1 = 1_R$). the *sum* $\Sigma_\alpha \mathfrak{i}_\alpha$ of a family $\{\mathfrak{i}_\alpha\}$ of ideals of R is defined as the collection of all finite sums $\sum_j r_j i_{\alpha_j}$ with $(r_j, i_{\alpha_j}) \in R \times \mathfrak{i}_{\alpha_j}$. Note that $\Sigma_\alpha \mathfrak{i}_\alpha$ is again an ideal. Indeed, one has

$$(4.4) \qquad \textstyle\sum_\alpha \mathfrak{i}_\alpha = (\cup_\alpha \mathfrak{i}_\alpha),$$

where the right-hand side denotes the ideal within R generated by the set $\cup_\alpha \mathfrak{i}_\alpha$. Examples when $R = \mathbb{Z}$: $(2) + (4) = (2)$; $(2) + (3) = \mathbb{Z}$.

Theorem 4.5 : *Let* $\mathfrak{i}, \mathfrak{j}$ *and* $\mathfrak{i}_\alpha$*, where* α *varies through some index set, be ideals of* $A[x]$*. Then:*

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

(b) $\cap_\alpha \mathcal{V}(\mathfrak{i}_\alpha) = \mathcal{V}(\sum_\alpha \mathfrak{i}_\alpha) = \mathcal{V}((\cup_\alpha \mathfrak{i}_\alpha))$*; and*

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

$$\mathcal{V}(\mathfrak{i}) \cup \mathcal{V}(\mathfrak{j}) = \mathcal{V}(\mathfrak{i} \cap \mathfrak{j}).$$

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

$$\begin{aligned} c \in \cap_\alpha \mathcal{V}(\mathfrak{i}_\alpha) &\Leftrightarrow c \in \mathcal{V}(\mathfrak{i}_\alpha) \text{ for all } \alpha \\ &\Leftrightarrow p(c) = 0 \text{ for all } \alpha \text{ and all } p \in \mathfrak{i}_\alpha \\ &\Leftrightarrow (\textstyle\sum p_j)(c) = 0 \text{ for all finite sums} \\ &\qquad \text{of elements } p_j \in \cup_\alpha \mathfrak{i}_\alpha \\ &\Leftrightarrow c \in \mathcal{V}(\textstyle\sum_\alpha \mathfrak{i}_\alpha). \end{aligned}$$

For the second equality use (4.4).

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

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

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

q.e.d.

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* $\mathfrak{r} \subset A[x] \mapsto \mathcal{V}(\mathfrak{r}) \subset B^n$ *is an inclusion reversing surjection from the collection of radical ideals of* $A[x]$ *to the closed subsets of* B^n*.*

Proof : Since integral domains are reduced rings, the final assertion is immediate from Proposition 4.2. **q.e.d**.

Unfortunately, the mapping $\mathfrak{r} \mapsto \mathcal{V}(\mathfrak{r})$ 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[58], 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.

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 $\mathfrak{r} \mapsto \mathcal{V}(\mathfrak{r})$ from radical ideals of $A[x]$ to classical (A, B)-affine algebraic subsets of $\mathbb{A}^n_A(B)$ is an inclusion reversing bijection;*

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

The Nullstellensatz terminology[59] is used because the property is closely related to Hilbert's Nullstellensatz, as we will see in Corollary 19.3.

Proof : By (4.1) and (ii) of Proposition 4.2 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 $\mathfrak{i}, \mathfrak{j} \subset A[x]$ such that

$$\mathcal{V}(\mathfrak{i}) = \mathcal{V}(\mathfrak{j}). \tag{i}$$

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

$$p \in \mathfrak{j} \backslash \mathfrak{i}, \tag{ii}$$

[58] If the product of polynomials $p_1, p_2 \in \mathbb{R}[x]$ is in $(x^2 + 1)$ then $p_1 p_2 = q \cdot (x^2 + 1)$ 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 21 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.

[59] Which is not standard.

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

(b) : By Proposition 4.2 we can assume $\mathfrak{i}$ is radical, and in that case the result is immediate from (a) and Theorem 4.5(a).

q.e.d.

The topology on B^n defined in Corollary 4.6 is the (A, B)-*Zariski topology*, or the A-*topology*[60] and when this topology is assumed B^n is written as[61] $\mathbb{A}^n_A(B)$. The induced topology[62] on any affine algebraic subset of $\mathbb{A}^n_A(B)$ 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., $\mathcal{V}_{\mathbb{A}^m(B)}$ would mean that $\mathcal{V}_{\mathbb{A}^m(B)}$ is an algebraic subset of $\mathbb{A}^m(B)$.

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[63] $\mathrm{cl}(C)$ in the (A, B)-Zariski topology; by *Zariski dense* one means dense in the (A, B)-Zariski topology, 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 $f : \mathbb{A}^n_A(B) \to \mathbb{A}^m_A(B)$ is continuous.*

Proof : Immediate from Proposition 2.4. **q.e.d.**

[60]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 $\mathbb{A}^n_A(B)$ given here is not the one found there, but is shown to be equivalent in (our) Proposition 4.12. Our definition is more in the spirit of [Hart, Chapter I, §1, p. 3], but there $A = B$ and B a field are assumed.

[61]This notation has been seen before: it was introduced in Example 2.2(d) to indicate when the A-module B^n was being regarded as a classical (A, B)-affine algebraic set. Since we will always assume classical affine algebraic set is endowed with the Zariski topology, the ambiguity should not cause problems.

[62]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.

[63]When X is a topological space and S is a subset we denote the closure of S by $\mathrm{cl}(S)$. The notation $\overline{S}$ is more common.

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 $f : \mathbb{A}^n_A(B) \to \mathbb{A}^m_A(B)$ between the ambient spaces of $\mathcal{V}$ and $\mathcal{Y}$ respectively. If $C \subset \mathcal{W}$ is a closed subset then (by the definition of the induced topology) $C = \mathcal{W} \cap \mathcal{C}$ for some algebraic subset $\mathcal{C} \subset B^m$. We can therefore write

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

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 $\mathbb{A}^n_A(B)$ with the Zariski topology constitutes a covariant functor β 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 analogy with Example 3.16, we illustrate the use of this functor in connection with the classification problem introduced at the very end of §2.

Example 4.11 : *The two-point classical $(\mathbb{Z}, \mathbb{R})$-affine algebraic subsets $\mathcal{V}_1 := \{\pm\sqrt{2}\} \subset \mathbb{R}$ and $\mathcal{V}_2 := \{\pm 2\} \subset \mathbb{R}$ of are not isomorphic* (within the category of classical $(\mathbb{Z}, \mathbb{R})$-affine algebraic sets). For if the algebraic sets were isomorphic Theorem 4.10 would imply that the two sets would be homeomorphic when endowed with the $(\mathbb{Z}, \mathbb{R})$-Zariski topologies. We claim this is not the case. Indeed, we have seen[64] that any polynomial $p \in \mathbb{Z}[x]$ which vanishes on $\sqrt{2}$ must also vanish on $-\sqrt{2}$, and it follows from the definition of the Zariski topology that the closure of the singleton $\{\sqrt{2}\}$ is $\mathcal{V}_1$. In particular, this algebraic set is connected. In contrast, $\mathcal{V}_2$ is not connected: the two points ± 2 are the zero sets of the polynomials $x \mp 2 \in \mathbb{Z}[x]$, and the singleton sets $\{\pm 2\}$ are therefore closed.

It is worth pointing out that when B is an integral domain and $\mathcal{V} \subset \mathbb{A}^n_A(B)$ 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.

[64] In Footnote 21.

Proposition 4.12 : *Suppose* B *is an integral domain,* $n \geq 1$ *is an integer, and* $\mathcal{V} \subset \mathbb{A}^n_A(B)$ *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*

$$C = \{\, c \in \mathcal{V} \,:\, r_\alpha(c) = 0 \ \ \textit{for all} \ \ \alpha \,\}.$$

Proof : From the definition of the induced topology we know that C is closed if and only if there is an algebraic set $\mathcal{W} \subset \mathbb{A}^n_A(B)$ 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 α 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 $c \in \mathbb{A}^n_A(B)$ we have

$$\begin{aligned}
c \in C \ &\Leftrightarrow \ c \in \mathcal{V} \cap \mathcal{V}(\{p_\alpha\}) \\
&\Leftrightarrow \ c \in \mathcal{V} \ \text{ and } \ c \in \mathcal{V}(\{p_\alpha\}) \\
&\Leftrightarrow \ c \in \mathcal{V} \ \text{ and } \ p_\alpha(c) = 0 \ \text{ for all } \ \alpha \\
&\Leftrightarrow \ c \in \mathcal{V} \ \text{ and } \ r_\alpha(c) = 0 \ \text{ for all } \ \alpha \\
&\Leftrightarrow \ c \in D.
\end{aligned}$$

This gives $C = D$, and the proof is complete. **q.e.d.**

5. The Contemporary Combined Approach

In this section R denotes a ring and $B \supset A$ is an extension of integral domains[65]*. 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:

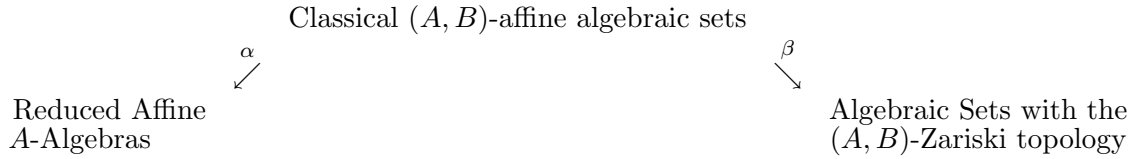


Diagram 5.1

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 easily seen to be "yes:" one can construct a functor β^{-1} inverse to β simply by "forgetting" the topology[66], and by then defining $\rho := \alpha \circ \beta^{-1}$ one completes Diagram 5.1 to the commutative triangle seen in Diagram 5.2.

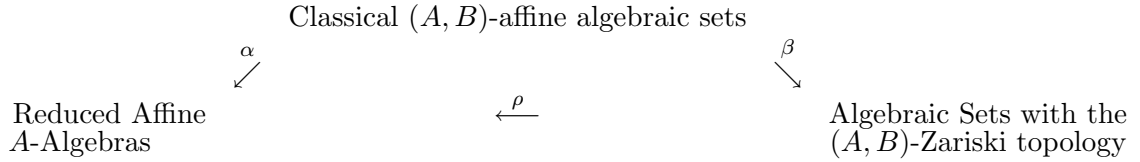


Diagram 5.2

However, the current trend in algebraic geometry is somewhat different, and far more ambitious: one constructs a functor γ from the category of (commutative) rings (with unities) to the category of topological spaces which allows one to embed Diagram 5.1 into a commutative diagram

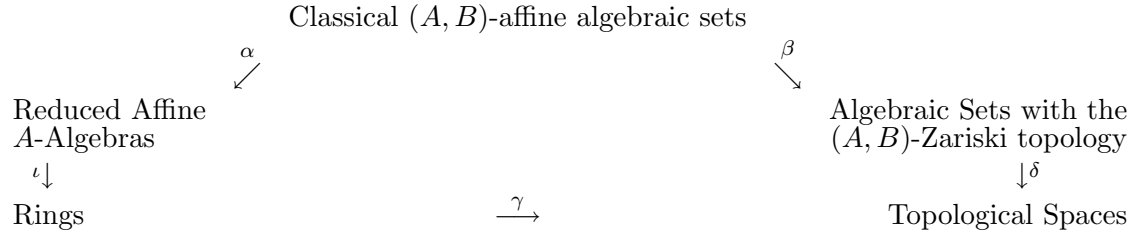


Diagram 5.3

[65] Without the integral domain restriction there would be no (A, B)-Zariski topology on classical (A, B)-affine algebraic sets.

[66] In the spirit of forgetful functors.

wherein ι is the inclusion of the indicated categories and $\delta := \gamma \circ \iota \circ \rho$.

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[67]).

Our task in this section is to define the functor γ of Diagram 5.3, 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 $\mathrm{Spec}(R)$ (read "speck are"). Recall that prime ideals are (by definition) proper ideals, hence $R \notin \mathrm{Spec}(R)$.

Examples 5.1 :

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

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

(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 $\mathrm{Spec}(\mathbb{Z})$ as the collection of prime numbers together with 0.

(d) $\mathrm{Spec}(R)$ 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: $\mathrm{Spec}(\mathbb{Z}/4\mathbb{Z})$ consists of the single prime ideal $\{[0],[2]\}$ (the ideal $([0])$ is not prime), but $\mathbb{Z}/4\mathbb{Z}$ is not a field.

(e) Suppose R is an integral domain and x is an indeterminate over R. Then the principal ideal $(x) \subset A[x]$ is prime, as was noted immediately before the statement of Proposition 3.5. The zero ideal (0) is also prime, and $\mathrm{Spec}(R[x])$ therefore contains at least two elements.

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

$$D(r) := \{\, \mathfrak{p} \in \mathrm{Spec}(R) \,:\, r \notin \mathfrak{p} \,\}. \tag{5.2}$$

[67] Recall Examples 3.3(c) and (d).

One then has

$$\text{(5.3)} \qquad \begin{cases} \text{(a)} & D(0) = \emptyset; \\ \text{(b)} & D(1) = D(-1) = \mathrm{Spec}(R); \quad \text{and} \\ \text{(c)} & D(rs) = D(r) \cap D(s), \end{cases}$$

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

$$\begin{aligned} \mathfrak{p} \in D(rs) &\Leftrightarrow rs \notin \mathfrak{p} \\ &\Leftrightarrow r \notin \mathfrak{p} \text{ and } s \notin \mathfrak{p} \\ &\Leftrightarrow \mathfrak{p} \in D(r) \text{ and } \mathfrak{p} \in D(s) \\ &\Leftrightarrow \mathfrak{p} \in D(r) \cap D(s), \end{aligned}$$

thereby giving (c). For later use note from the choice $s = r$ in (5.3c) that $D(r^2) = D(r)$, whence by induction that

$$\text{(5.4)} \qquad D(r^n) = D(r), \qquad n = 1, 2, 3, \ldots .$$

It is immediate from (5.3) that the collection $\{D(r)\}_{r \in R}$ is a basis for a topology on $\mathrm{Spec}(R)$. This is the *Zariski topology*, and $\mathrm{Spec}(R)$ 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 $\mathfrak{i} \subset S$ is an ideal the preimage $f^{-1}(\mathfrak{i}) \subset R$ is called the *pull-back*[68] of $\mathfrak{i}$ (*by* f).

[68]Some texts, e.g., [A-M], refer to $f^{-1}(\mathfrak{i})$ as the *contraction* of $\mathfrak{i}$ in R. I use "pull-back" because that term is used with analogous constructions in differential geometry.

Proposition 5.5 : *Assume the notation of the previous paragraph. Then:*

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

(b) *this pull-back is prime when* $\mathfrak{i}$ *is prime;*

(c) *when* f *is surjective the image of any ideal* $\mathfrak{j} \subset R$ *is an ideal of* S *and the correspondence* $\mathfrak{j} \mapsto f(\mathfrak{j})$ *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* $\mathfrak{p} \subset S \mapsto f^{-1}(\mathfrak{p}) \subset R$ *is an order preserving bijection between prime ideals of* S *and prime ideals of* R *containing* $\ker(f)$*.*

It is not true that $f(\mathfrak{j}) \subset S$ is an ideal whenever $\mathfrak{j} \subset R$ 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 $v, w \in f^{-1}(\mathfrak{i})$ we see from $f(v+w) = f(v) + f(w) \in \mathfrak{i}$ and $f(rv) = f(r)f(v) \in \mathfrak{i}$ that $v + w,\ rv \in f^{-1}(\mathfrak{i})$.

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

(c) Suppose $\mathfrak{j} \subset R$ is an ideal, $r, v \in \mathfrak{j}$, 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 $wr \in \mathfrak{j}$ we see that $f(\mathfrak{j}) \subset S$ is an ideal.

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

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

q.e.d.

It is immediate from Proposition 5.5(b) that any ring homomorphism $f : R \to S$ induces a mapping[69] $f^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$, i.e.,

$$f^* : \mathfrak{p} \in \mathrm{Spec}(S) \mapsto f^{-1}(\mathfrak{p}) \in \mathrm{Spec}(R). \tag{5.6}$$

Proposition 5.7 : *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 $\mathrm{Spec}(R)$ and $\mathrm{Spec}(S)$ are endowed with the Zariski topologies the mapping $f^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ 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.

Proof :

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

$$\begin{aligned} \mathfrak{q} \in (f^*)^{-1}(D(r)) &\Leftrightarrow f^*(\mathfrak{q}) \in D(r) \\ &\Leftrightarrow f^{-1}(\mathfrak{q}) \in D(r) \\ &\Leftrightarrow r \notin f^{-1}(\mathfrak{q}) \\ &\Leftrightarrow f(r) \notin \mathfrak{q} \\ &\Leftrightarrow \mathfrak{q} \in D(f(r)), \end{aligned}$$

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 5.8 : *Any surjective ring homomorphism $f : R \to S$ induces a continuous injection $f^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ 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).

[69] 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 ${}^a f$ (read "f adjoint", "adjoint f" or "the adjoint of f").

Proof : The initial assertion is immediate from Proposition 5.7 and Proposition 5.5(d). To verify the final assertion we need the following observation: for any $\mathfrak{p} \in \mathrm{Spec}(R)$ not containing $\ker(f)$ and any $r \in R$ one has

$$\text{(i)} \qquad f(r) \in f(\mathfrak{p}) \qquad \Leftrightarrow \qquad r \in \mathfrak{p}.$$

Indeed, $f(r) \in f(\mathfrak{p})$ holds if and only if $r \in f^{-1}(f(\mathfrak{p}))$, and $f^{-1}(f(\mathfrak{p})) = \mathfrak{p}$ by Proposition 5.5(d).

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

$$\text{(ii)} \qquad f^*(D(f(r))) = D(r).$$

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

$$\begin{aligned} \mathfrak{p} \in f^*(D(f(r))) &\Leftrightarrow \mathfrak{p} \in f^{-1}(D(f(r))) \\ &\Leftrightarrow f(\mathfrak{p}) \in D(f(r)) \\ &\Leftrightarrow f(r) \notin f(\mathfrak{p}) \\ &\Leftrightarrow r \notin \mathfrak{p} \quad \text{(by (i))} \\ &\Leftrightarrow \mathfrak{p} \in D(r). \end{aligned}$$

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

Theorem 5.9 : *Assigning* $\mathrm{Spec}(R)$ *to each* (commutative) *ring* R (with unity) *and* $f^* : \mathrm{Spec}(S) \to \mathrm{Spec}(R)$ *to each ring homomorphism* $f : R \to S$ *constitutes a contravariant functor* γ *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.**

As a consequence of Theorem 5.9 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 α, ι and γ of Theorem 3.15, Diagram 5.3 and Theorem 5.9, and the functor β of Theorem 4.10 and Diagram 5.1. The finishing touch on that diagram is achieved by defining $\delta := \gamma \circ \iota \circ \alpha \circ \beta^{-1}$.

Example 5.10 : *The parabola* $y = x^2$ *and* y*-axis are not isomorphic as classical* $(\mathbb{R}, \mathbb{R})$*-affine algebraic subsets of* $\mathbb{R}^2$*.* To verify this first note that an isomorphism (in the category of classical $(\mathbb{R}, \mathbb{R})$-affine algebraic sets and regular mappings) between

the usual x-axis and the given parabola is defined by the polynomial mapping $t \in \mathbb{R} \mapsto (t, t^2) \in \mathbb{R}^2$, with the inverse being the restriction of the projection $(x_1, x_2) \mapsto t = x_1$. The coordinate rings of these two algebraic sets are therefore isomorphic, and from Example 3.3(f) we see that this coordinate ring must be (ring isomorphic to) $\mathbb{R}[x]$. On the other hand, from Example 3.3(i) we see that the coordinate ring of the y-axis is $\mathbb{R}$. If the parabola and y-axis were isomorphic it would follow from Theorem 5.9 that $\mathrm{Spec}(\mathbb{R})$ and $\mathrm{Spec}(\mathbb{R}[x])$ would be homeomorphic, whereas from Examples 5.1(d) and (e) we see that this cannot be the case[70].

[70] As the reader has undoubtedly noticed, one can give a simple straightforward proof of the italicized statement beginning this example without mentioning prime spectra at all. But to have done so would have defeated the purpose of illustrating Theorem 5.9. One needs to develop additional machinery before serious examples of that result can be presented.

6. Viewing an Algebraic Set $\mathcal{V}$ within $\mathrm{Spec}(A_B[\mathcal{V}])$

We continue with the notation of the previous section. In particular, $B \supset A$ is an extension of integral domains unless specifically stated otherwise.

For ease of reference we reproduce Diagram 5.3, which we henceforth reference as Diagram 5.4.

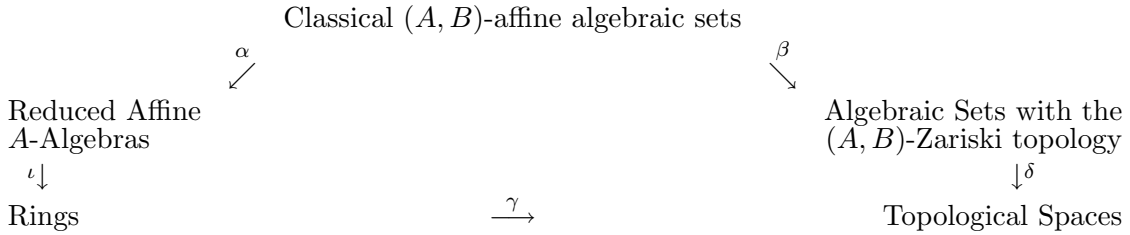


Diagram 5.4

At the object level the functor δ assigns, to each classical (A, B)-affine algebraic set $\mathcal{V} \subset \mathbb{A}^n_A(B)$ with the (A, B)-Zariski topology, the topological space $\mathrm{Spec}(A_B[\mathcal{V}])$. Although it is not relevant at the categorical level[71], this suggests that it might be possible to define, for each classical (A, B)-affine algebraic set $\mathcal{V}$, a function from $\mathcal{V}$ into $\mathrm{Spec}(A_B[\mathcal{V}])$. 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

$$\mathfrak{i}(\{c\}) := \{\, p \in A[x] \,:\, p(c) = 0 \,\} \tag{6.1}$$

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*[72] *of* c. Equivalently,

$$\mathfrak{i}(\{c\}) := \ker(f_c), \qquad \text{where} \qquad f_c : p \in A[x] \mapsto p(c) \in B, \tag{6.2}$$

i.e., $f_c : A[x] \to B$ is evaluation at c. (The definition and equivalence assertion in this paragraph do not require the integral domain assumption on the extension $B \supset A$.)

[71] The functor δ simply assigns $\mathcal{V}$ to $\mathrm{Spec}(A_B[\mathcal{V}])$; it does not assign points of $\mathcal{V}$ to points of $\mathrm{Spec}(A_B[\mathcal{V}])$.

[72] Since a singleton subset $\{c\} \subset B^n$ need not be algebraic, this definition cannot be regarded as a special case of (3.1).

Examples 6.3 : 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[73] $\mathfrak{i}(\{c\}) = (x^2 - 2) \subset \mathbb{Z}[x]$.

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

Proposition 6.4 : *For any positive integer n the following assertions hold.*

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

(b) *Suppose $\mathcal{V} \subset \mathbb{A}^n_A(B)$ 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 $\ker(f) \subset \mathfrak{i}(\{c\})$.*

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

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

Proof :

(a) From (6.2) and the First Isomorphism Theorem of ring theory[74] we see that $A[x]/\mathfrak{i}$ is isomorphic to a subring of an integral domain, and is therefore an integral domain.

(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 $p \in \mathfrak{i}(\{(c)\})$.

(c) Use (a), (b), and Proposition 5.5(d).

q.e.d.

Assume the hypotheses of Proposition 6.4, let $\mathcal{V} \in \mathbb{A}^n_A(B)$ 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 $\varphi_{\mathcal{V}} : \mathcal{V} \to \mathrm{Spec}(A_B[\mathcal{V}])$ is defined by

$$\varphi_{\mathcal{V}} : c \in \mathcal{V} \mapsto f(\mathfrak{i}(\{c\})) \in \mathrm{Spec}(A_B[\mathcal{V}]). \tag{6.5}$$

[73] Argue as in Footnote 21. (The notations $(x^2 - 2)$ and $(x - \sqrt{2}\,)$ used in these two examples indicate principal ideals of the indicated rings.)

[74] See Footnote 42.

It can be useful to imagine[75] $\varphi_{\mathcal{V}}(\mathcal{V}) \subset \mathrm{Spec}(A_B[\mathcal{V}])$ as the "image" of $\mathcal{V}$ under the functor δ. Indeed, with an eye on Diagram 5.4 recall that β^{-1} is forgetful; it simply strips the topology from $\mathcal{V}$ and therefore carries $c \in \mathcal{V}$ to $c \in \mathcal{V}$. One then imagines α and $\iota \circ \alpha$ as carrying c to the prime ideal $f(\mathfrak{i}(\{c\})) \subset A_B[\mathcal{V}]$, and of γ as converting this prime ideal to the point $\varphi_{\mathcal{V}}(c)$ of $\mathrm{Spec}(A_B[\mathcal{V}])$.

Proposition 6.6 : *Let* $\varphi_{\mathcal{V}} : \mathcal{V} \to \mathrm{Spec}(A_B[\mathcal{V}])$ *be defined as in* (6.5). *Then:*

(a) *for any* $p \in A[x]$ *one has*[76]

(i) $$\varphi_{\mathcal{V}}^{-1}(D(f(p))) = \mathcal{V} \setminus \mathcal{V}(\{p\});$$

and

(b) $\varphi_{\mathcal{V}}$ *is continuous.*

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

(i′) $$\varphi_{\mathcal{V}}^{-1}(D([p])) = \mathcal{V} \setminus \mathcal{V}(\{p\}).$$

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

(ii) $$f(p) \in f(\mathfrak{i}(\{c\})) \;\Leftrightarrow\; p \in \mathfrak{i}(\{c\}).$$

Indeed, the forward implication is is immediate from Proposition 5.5(d), and the reverse is obvious. It follows that

$$\begin{aligned} c \in \varphi_{\mathcal{V}}^{-1}(D([p])) &\Leftrightarrow \varphi_{\mathcal{V}}(c) \in D([p]) \\ &\Leftrightarrow f(\mathfrak{i}(\{c\})) \in D([p]) \\ &\Leftrightarrow [p] \notin f(\mathfrak{i}(\{c\})) \\ &\Leftrightarrow f(p) \notin f(\mathfrak{i}(\{c\})) \\ &\Leftrightarrow p \notin \mathfrak{i}(\{c\}) \;\text{ (by (ii))} \\ &\Leftrightarrow p(c) \neq 0 \\ &\Leftrightarrow c \in \mathcal{V} \setminus \mathcal{V}(\{p\}), \end{aligned}$$

[75] So 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.

[76] When A and B are subsets of a set C we denote the *difference* $\{\, c \in A : c \notin B\}$ of A and B by $A \backslash B$. (It is not assumed that $B \subset A$.)

and (i′) is thereby established.

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

q.e.d.

This idea of "pushing" an algebraic set $\mathcal{V}$ into $\mathrm{Spec}(A_B[\mathcal{V}])$ (as in (6.5)) 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[77].

We will have much more to say about the mapping (6.5). Indeed, it could well be regarded as the central focus of these notes[78]. However, understanding the role of this mapping in contemporary formulations algebraic geometry will require the introduction of several new ideas, as well as refinements of several of those already introduced.

[77]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.

[78]Our main references were [Mac, Chapter 3, pp. 23-4] and [Ku, Chapter 1, §4, pp. 24-5]. For the full story see [Hart, Chapter 2, §2, pp. 77-8, particularly Proposition 2.6].

7. Maximal Ideals

Throughout the section R is a ring.

A proper ideal $\mathfrak{m} \subset R$ is (a) *maximal* (*ideal*) if $R/\mathfrak{m}$ 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. In algebraic geometry the most important example is that given in assertion (c) of the next result.

Theorem 7.1 : *Suppose $B \supset A$ is an extension of rings, $n \geq 1$ is an integer, and $c = (b_1, b_2, \ldots, b_n)$ is any point of $\mathbb{A}^n_A(B)$. Then:*

(a) *the defining ideal $\mathfrak{i}(\{c\})$ of c* (i.e., of the singleton set $\{c\}$) *is the kernel of the A-algebra homomorphism $f_c : p \in A[x] := A[x_1, x_2, \ldots, x_n] \mapsto p(c) \in B$;*

(b) *$\mathfrak{i}(\{c\})$ is prime if $A = B$ and B is an integral domain; and*

(c) *$\mathfrak{i}(\{c\})$ is maximal if $A = B$ and B is a field.*

Moreover, when $A = B$ one has

(i) $$\mathfrak{i}(\{c\}) = (x_1 - b_1, x_2 - b_2, \ldots, x_n - b_n) \subset B[x] = B[x_1, x_2, \ldots, x_n]$$

(regardless of any field or integral domain assumption on B).

Proof : Assertion (a) we noted in (6.2), and the final assertion was established in Example 3.3(e). (They are restated here simply for ease of reference.) Only (b) and (c) require proof.

The hypothesis $A = B$ ensures that the ring homomorphism $f : B[x] \to B$ is surjective, since an arbitrary point $b \in B$ is then the image of c under the mapping associated with the constant polynomial b. The First Isomorphism Theorem of ring theory[79] then guarantees that $B \simeq B[x]/\ker(f)$. If B is an integral domain it follows (from the definition of a prime ideal) that $\ker(f)$ must be prime; if B is a field it must be maximal. **q.e.d.**

Proposition 7.2 :

(a) *Any maximal ideal is a prime ideal.*

(b) *Any maximal ideal is a radical ideal.*

[79] See Footnote 42.

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 7.3 : *For any proper ideal* $\mathfrak{i} \subset R$ *the following assertions are equivalent :*

(a) $\mathfrak{i}$ *is maximal ;*

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

Assertion (b) is a common definition of a maximal ideal. Indeed, in many of our proofs it will be used in place of the definition we have given.

Proof :

(a) $\Rightarrow$ (b) : Suppose the inclusion $\mathfrak{i} \subset \mathfrak{j}$ is proper and $r \in \mathfrak{j} \backslash \mathfrak{i}$. Since $R/\mathfrak{i}$ is a field the element $[r] \in R/\mathfrak{i}$ 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 $1 - rs =: t \in \mathfrak{i} \subset \mathfrak{j}$. But $r \in \mathfrak{j} \Rightarrow rs \in \mathfrak{j}$, hence $rs + t = 1 \in \mathfrak{j}$, and $\mathfrak{j} = R$ follows.

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

q.e.d.

Corollary 7.4 : *When* $f : R \to S$ *is a surjective ring homomorphism the correspondence* $\mathfrak{m} \subset R \mapsto f(\mathfrak{m}) \subset S$ *is a bijection between the maximal ideals of* R *containing* $\ker(f)$ *and the maximal ideals of* S.

Proof : Immediate from Propositions 7.2(a) and 5.5(d). **q.e.d.**

Let $\mathrm{maxSpec}(R)$ denote the collection of maximal ideals of R. Since every maximal ideal is prime (Proposition 7.2(a)) we have $\mathrm{maxSpec}(R) \subset \mathrm{Spec}(R)$. The induced topology on $\mathrm{maxSpec}(R)$, which we always assume, is again called the *Zariski topology.*

The next result offers a hint as to why maximal ideals might be of interest to algebraic geometers.

Proposition 7.5 : *Suppose* B *is a field,* $A = B$, $n \geq 1$, *and* $\mathcal{V} \subset \mathbb{A}^n_A(B)$ *is a classical* B*-affine algebraic set. Then*

$$\varphi_{\mathcal{V}}(\mathcal{V}) \subset \text{maxSpec}(B_B[\mathcal{V}]).$$

Proof : This is immediate from Theorem 7.1(c) (and definition (6.5)). **q.e.d.**

Proposition 7.5, in turn, should suggest why we might be interested in the following result.

Proposition 7.6 : *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* $\mathfrak{m} \subset R$ *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

$$\begin{aligned} D(r) \cap \text{maxSpec}(R) \neq \emptyset \quad &\Leftrightarrow \quad \text{there is a maximal ideal } \mathfrak{m} \subset D(r) \\ &\Leftrightarrow \quad \text{there is a maximal ideal } \mathfrak{m} \subset R \text{ such that } r \notin \mathfrak{m}. \end{aligned}$$

q.e.d.

8. 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 *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 *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 *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, τ), with τ 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 *free on* X if for any object B of $\mathcal{C}$ and any set mapping $f : X \to B$ there is a unique morphism $f_{\mathcal{C}} : C \to B$ which makes the diagram

$$\begin{array}{ccc} C & \xrightarrow{f_{\mathcal{C}}} & B \\ & \overset{f}{\nearrow} & \\ \iota \uparrow & & \\ X & & \end{array}$$

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 $\mathcal{C}$ be a concrete category and let C be an object of $\mathcal{C}$ which is free on a non-empty finite set $X = \{x_1, x_2, \ldots, x_n\}$. Fix an object D of $\mathcal{C}$ and consider:

- the set $\mathrm{mor}(C, D)$ 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 $\alpha : \mathrm{mor}(C, D) \to \mathcal{F}(X, D)$ is given by the restriction mapping

$$\alpha : f \in \mathrm{mor}(C, D) \mapsto f|_X \in \mathcal{F}(X, D). \tag{8.1}$$

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

$$\beta : g \in \mathcal{F}(X, D) \mapsto (g(x_1), g(x_2), \ldots, g(x_n)) \in D^n. \tag{8.2}$$

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

$$\begin{array}{rcl} \varphi_c : (d_1, d_2, \ldots, d_n) \in D^n & \mapsto & ((\alpha^{-1} \circ \beta^{-1})(d_1, d_2, \ldots, d_n))\,(c) \\ & = & ((\beta \circ \alpha)^{-1})(d_1, d_2, \ldots, d_n))\,(c). \end{array} \tag{8.3}$$

Now fix an element $d_0 \in D$ and let $\mathcal{P}$ be any collection of elements of C. We define the *abstract*[80] *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.,

$$\mathcal{V}(\mathcal{P}) := \{\, (d_1, d_2, \ldots, d_n) \in D^n \,:\, \varphi_c(d_1, d_2, \ldots, d_n) = d_0 \ \text{ for all } \ c \in \mathcal{P} \,\}. \tag{8.4}$$

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

Examples 8.5 :

(a) Let $B \supset A$ be an extension of integral domains and let $\mathcal{C}$ 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

[80] 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 $(\beta \circ \alpha)^{-1} \in \mathrm{mor}(C, D)$ 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 $\mathrm{Spec}(R)$ is replaced by $\mathrm{Diffspec}(R)$ (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, i.e., we formulate definitions and propositions in arbitrary topological spaces, although not in §9. The main result of Part II is Theorem 11.15, 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 the Fundamental Theorem of Arithmetic: any integer factors 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.

9. 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 extending definition (3.1) beyond classical (A, B)-affine algebraic sets. Specifically, given any subset $C \subset B^n$ we generalize (3.1) and (6.1) simultaneously by setting

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

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 will be content with the examples we have seen in Examples 3.3 and 6.3.

Proposition 9.1 : *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 3.8.

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 $C, D \subset B^n$ one has

$$C \subset D \quad \Rightarrow \quad \mathfrak{i}(D) \subset \mathfrak{i}(C). \tag{9.2}$$

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

Proposition 9.3 : *Suppose $C \subset B^n$ and $\mathfrak{i} \subset A[x]$ is an ideal. Then the following assertions hold.*

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

(b) $\mathfrak{i} \subset \mathfrak{i}(\mathcal{V}(\mathfrak{i}))$.

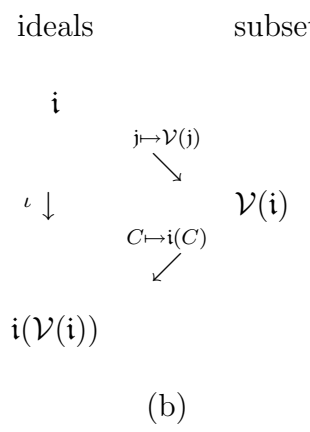
(c) $C \subset \mathcal{V}(\mathfrak{i}(C))$.

(d) $C \subset \mathcal{V}(\mathfrak{i}) \Rightarrow \mathfrak{i} \subset \mathfrak{i}(C)$.

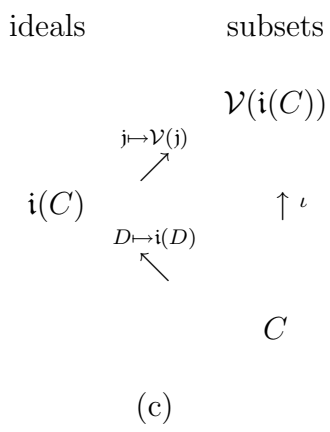
(e) $C \subset \mathcal{V}(\mathfrak{i}) \Rightarrow \mathcal{V}(\mathfrak{i}(C)) \subset \mathcal{V}(\mathfrak{i})$.

Assertion (b) was already noted in (4.3), 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 $C = \{i\} \subset B = B^1$. Then $\mathfrak{i}(C) = (x^2 + 1)$ and $\{-i, i\} = \mathcal{V}(\mathfrak{i}(C)) \neq C$.

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



(b)



(c)

Proof :

(a) This initial assertion is immediate from the definition of $\mathfrak{i}(B^n)$. 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 (4.3).

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

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

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

q.e.d.

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

Corollary 9.4 : *Suppose B is an integral domain and $C, D \subset B^n$. Assume the (A, B)-Zariski topology on B^n. Then:*

(a) $\mathrm{cl}(C) = \mathcal{V}(\mathfrak{i}(C))$*;*

(b) *C is Zariski closed if and only if $C = \mathcal{V}(\mathfrak{i}(C))$; and*

(c) *when C and D are* (Zariski) *closed one has $C = D$ if and only if $\mathfrak{i}(C) = \mathfrak{i}(D)$.*

The assertion of (a), in simple English, is this: a point $c \in \mathbb{A}^n_A(B)$ 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 6.3; in particular, let $C = \{\sqrt{2}\}$. Then for $A = \mathbb{Z}$ and $B = \mathbb{R}$ we have $\mathrm{cl}(C) = \{\pm\sqrt{2}\} = \mathcal{V}((x^2 - 2))$, i.e, $c = \pm\sqrt{2}$ (are the two possibilities for c), whereas for $A = B = \mathbb{R}$ we have $\mathrm{cl}(C) = \{\sqrt{2}\} = \mathcal{V}((x - \sqrt{2}))$, i.e., $c = \sqrt{2}$ (is the only possibility for c).

Proof :

(a) Any closed set containing C has the form $\mathcal{V}(\mathfrak{i})$ for some ideal $\mathfrak{i} \subset A[x]$, and by Proposition 9.3(c) this is the case for $\mathcal{V}(\mathfrak{i}(C))$. The result is then immediate from Proposition 9.3(e).

(b) By (a).

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

q.e.d.

Corollary 9.5 : *Suppose* B *is an integral domain,* $A = B$*, and* $n \geq 1$ *is an integer. Then for any point* $c = (b_1, b_2, \ldots, b_n) \in \mathbb{A}_A^n(B)$ *one has*

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

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

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

Proof : From Example 3.3(e) we have $\mathfrak{i}(\{c\}) = (x_1 - b_1, x_2 - b_2, \ldots, x_n - b_n)$, and $c \in \mathcal{V}(\mathfrak{i}(\{c\})$ follows easily. If $e = (d_1, d_2, \ldots, d_n) \in \mathcal{V}(\mathfrak{i}(\{c\})$ 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 $\mathfrak{i}(\{c\}) = B[x]$ then (i) and Theorem 4.5(a) would yield the contradiction $\{c\} = \mathcal{V}(\mathfrak{i}(\{c\}) = \mathcal{V}(B[x]) = \emptyset$. **q.e.d.**

Corollary 9.6 : *Suppose* B *is an integral domain,* $\mathcal{W} \subset \mathbb{A}_A^n(B)$ *is an algebraic set, and* $f : A[x] \to A_B[\mathcal{W}]$ *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

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

the last equivalence by Corollary 9.4(a) and the fact that algebraic sets are (by definition) closed. **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 9.7 : *Suppose* B *is an integral domain and* $\mathcal{W} \subset \mathbb{A}_A^n(B)$ *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* $\mathcal{V}(\mathfrak{i}(C))$*, 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) $C = \mathcal{V}(\mathfrak{i}(C))$*;*

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* $\mathfrak{i}(C) = \mathfrak{i}(D)$ (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 α there is a Zariski closed set Y_α (in the topology on $\mathbb{A}^n_A(B)$) such that $X_\alpha := Y_\alpha \cap \mathcal{W}$. By definition we have $\mathrm{cl}_\mathcal{W}(C) = \cap_\alpha X_\alpha$, hence

$$\begin{aligned} \mathrm{cl}_\mathcal{W}(C) &= \cap_\alpha X_\alpha \\ &= \cap_\alpha (Y_\alpha \cap \mathcal{W}) \\ &= (\cap_\alpha (Y_\alpha)) \cap \mathcal{W} \\ &= \cap_\alpha Y_\alpha, \end{aligned}$$

the last equality since $\mathcal{W}$ is among the collection $\{Y_\alpha\}_\alpha$. We claim that $\cap_\alpha Y_\alpha = \mathrm{cl}(C)$. Indeed, since $\mathrm{cl}(C) \subset \cap_\alpha Y_\alpha$ obviously holds, there would otherwise be a Zariski closed set K (in the topology on $\mathbb{A}^n_A(B)$) 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 $\mathrm{cl}_\mathcal{W}(C) = \cap_\alpha Y_\alpha$. We conclude that $\mathrm{cl}_\mathcal{W}(C) = \mathrm{cl}(C)$, and (a) is then immediate from Corollary 9.4(a).

(b) By (a).

(c) Use Corollary 9.4(c).

q.e.d.

The Case of the Prime Spectrum of a Ring

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

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

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

Proposition 9.8 (Krull[81]) : *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.*

"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. It does not mean that the ideal is a maximal ideal.

To illustrate the result let $R = \mathbb{Z}[x]$ (one variable), let $S = 2\mathbb{Z} \subset \mathbb{Z} \subset R$ and let $\mathfrak{i} = (x^2)$. Then $\mathfrak{p} := (x)$ is a prime ideal which contains $\mathfrak{i}$, is disjoint from S, and is maximal w.r.t. these two properties. It is not, however, a maximal ideal: for any prime $p \in \mathbb{Z}^+$ it is properly contained in the maximal ideal[82] $\mathfrak{m} \subset \mathbb{Z}[x]$ generated by the set $\{p, x\}$.

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

To prove any such maximal element $\mathfrak{p}$ is prime suppose, to the contrary, that there are elements $a, b \in R\backslash\mathfrak{p}$ satisfying $ab \in \mathfrak{p}$. From the maximality of $\mathfrak{p}$ the ideal generated by $\mathfrak{p}$ and a must contain an element $s_a \in S$, say $s_a = ma + xp$ with $m, x \in R$ and $p \in \mathfrak{p}$. 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 $q \in \mathfrak{p}$. 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 $\mathfrak{p}$ (because $ab \in \mathfrak{p}$ and $r := mayq + nbxp + xpyq \in \mathfrak{p}$). Since $0 \notin S$ this contradicts $\mathfrak{p} \cap S = \emptyset$, and we conclude that at least one of a and b must be contained in $\mathfrak{p}$. **q.e.d.**

The proposition has some very important consequences.

[81] The attribution to Krull is from [Ku, Chapter 1, §4, p. 23].

[82] One sees that $\mathfrak{m}$ is maximal from the isomorphism $\mathbb{Z}[x]/\mathfrak{m} \simeq \mathbb{Z}/p\mathbb{Z}$.

Corollary 9.9 : *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 $\mathfrak{i} = (0)$ in Proposition 9.8. **q.e.d.**

Corollary 9.10 : *Suppose $\mathfrak{i} \subset R$ is an ideal and $r \in R$ is an element satisfying $r^n \notin \mathfrak{i}$ for all integers $n \geq 1$. Then there is a prime ideal $\mathfrak{p}$ containing $\mathfrak{i}$ such that $r^n \notin \mathfrak{p}$ for all integers $n \geq 1$.*

Proof : Take $S = \{1, r, r^2, r^3, \dots\}$ in Proposition 9.8. **q.e.d.**

Corollary 9.11 : *Every proper ideal of R is contained in a maximal ideal.*

Proof : Choose $S = \{1\}$ in Theorem 9.8 to produce a prime ideal $\mathfrak{p} \subset R$ which contains the given ideal and is maximal among all such ideals. Since any proper ideal containing $\mathfrak{p}$ will also have these two properties we see from Proposition 7.3 that $\mathfrak{p}$ must be a maximal ideal. **q.e.d.**

Corollary 9.12 : *Every proper ideal of R is contained in a prime ideal.*

Proof : Maximal ideals are prime (Proposition 7.2(a)). **q.e.d.**

Corollary 9.13 : *Every proper ideal of R is contained in a radical ideal.*

Proof : Maximal ideals are radical (Proposition 7.2(b)). **q.e.d.**

Corollary 9.14 : *Suppose R is non-trivial and $\mathfrak{i} \subset R$ is an ideal. Then in* $\mathrm{Spec}(R)$ *one has $V(\mathfrak{i}) = \emptyset$ if and only if $\mathfrak{i} = R$.*

Proof :

$\Rightarrow$: When $\mathfrak{i} \neq R$ there is a prime ideal $\mathfrak{p}$ containing $\mathfrak{i}$, hence $\mathfrak{p} \in V(\mathfrak{i})$.

$\Leftarrow$: Recall (9.17).

q.e.d.

We also need some additional results on radical ideals.

Proposition 9.15 :

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

Moreover, for any ideal $\mathfrak{i} \subset R$ *the following assertions hold.*

(b) $\sqrt{\sqrt{\mathfrak{i}}} = \sqrt{\mathfrak{i}}$, *i.e., the radical of any ideal is a radical ideal.*

(c) *For any prime ideal* $\mathfrak{p} \subset R$ *one has*

$$\mathfrak{i} \subset \mathfrak{p} \quad \Leftrightarrow \quad \sqrt{\mathfrak{i}} \subset \mathfrak{p}.$$

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

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

(b) This is a restatement of Proposition 3.6. (The result is repeated above for ease of reference.)

(c)

$\Rightarrow \mathfrak{i} \subset \mathfrak{p} \Rightarrow \sqrt{\mathfrak{i}} \subset \sqrt{\mathfrak{p}}$, and $\sqrt{\mathfrak{p}} = \mathfrak{p}$ since prime ideals are radical (Proposition 3.5).

$\Leftarrow$ Immediate from $\mathfrak{i} \subset \sqrt{\mathfrak{i}}$.

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

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

To prove the reverse inclusion note that for any $r \in R \backslash \sqrt{\mathfrak{i}}$ one has $r^n \notin \mathfrak{i}$ for all integers $n \geq 1$, and so by Corollary 9.10 there is a prime ideal $\mathfrak{p}$ containing $\mathfrak{i}$ but not containing r. This gives $r \notin \mathcal{I}$, whence $\mathcal{I} \subset \sqrt{\mathfrak{i}}$, and the proof of (d) is complete.

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

$\Rightarrow$: When an ideal $\mathfrak{r} \subset R$ is radical we have $\mathfrak{r} = \sqrt{\mathfrak{r}}$, whence $\mathfrak{r} = \mathcal{I}$ 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 $\mathrm{Spec}(R)$.

For any subset $S \subset R$ define

$$V(S) := \{\, \mathfrak{p} \,:\, S \subset \mathfrak{p} \,\} \subset \mathrm{Spec}(R), \tag{9.16}$$

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

$$V(R) = \emptyset. \tag{9.17}$$

In terms of this notation we can reformulate Corollary 5.8 as follows.

Proposition 9.18 : *Any surjective ring homomorphism $f : R \to S$ induces a homeomorphism $f^* : \mathrm{Spec}(S) \to V(\ker(f))$ onto the subset $V(\ker(f)) \subset \mathrm{Spec}(R)$.*

The basic properties of the sets $V(S)$ are (by no accident) reminiscent of those described in Proposition 4.2 and Theorem 4.5 for algebraic sets.

Proposition 9.19 :

(a) *$V(r) = \mathrm{Spec}(R) \backslash D(r)$ 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*

$$S \subset T \quad \Rightarrow \quad V(T) \subset V(S).$$

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

$$V(\cup_\alpha S_\alpha) = \cap_\alpha V(S_\alpha).$$

(e) *For any ideals $\mathfrak{i}, \mathfrak{j} \subset R$ one has*

$$V(\mathfrak{i} \cap \mathfrak{j}) = V(\mathfrak{ij}) = V(\mathfrak{i}) \cup V(\mathfrak{j}).$$

(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 $\mathfrak{p} \in \mathrm{Spec}(R)$ we have

$$\begin{aligned} \mathfrak{p} \in V(S) &\Leftrightarrow S \subset \mathfrak{p} \\ &\Leftrightarrow s \in \mathfrak{p} \text{ for all } s \in S \\ &\Leftrightarrow \mathfrak{p} \in V(s) \text{ for all } s \in S \\ &\Leftrightarrow \mathfrak{p} \in \cap_{s \in S} V(s). \end{aligned}$$

(c) Immediate from (9.16).

(d) For any $\mathfrak{p} \in \mathrm{Spec}(R)$ we have

$$\begin{aligned} \mathfrak{p} \in V(\cup_\alpha S_\alpha) &\Leftrightarrow \cup_\alpha S_\alpha \subset \mathfrak{p} \\ &\Leftrightarrow S_\alpha \subset \mathfrak{p} \text{ for all } \alpha \\ &\Leftrightarrow \mathfrak{p} \in V(S_\alpha) \text{ for all } \alpha \\ &\Leftrightarrow \mathfrak{p} \in \cap_\alpha V(S_\alpha)\,. \end{aligned}$$

(e) First note that

(i) $$\mathfrak{ij} \subset \mathfrak{i} \cap \mathfrak{j}.$$

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

(ii) $$\mathfrak{ij} \subset \mathfrak{p} \quad \Leftrightarrow \quad \mathfrak{i} \cap \mathfrak{j} \subset \mathfrak{p},$$

and to establish this we will first show that

(iii) $$\mathfrak{ij} \subset \mathfrak{p} \quad \Leftrightarrow \quad \mathfrak{i} \subset \mathfrak{p} \text{ or } \mathfrak{j} \subset \mathfrak{p}$$

(which is what one might expect of a prime ideal). Indeed, if $\mathfrak{i} \not\subset \mathfrak{p}$ there must be an element $a \in \mathfrak{i} \setminus \mathfrak{p}$, and it then follows from $\mathfrak{ij} \subset \mathfrak{p}$ that $ab \in \mathfrak{p}$ for all $b \in \mathfrak{j}$. Since $\mathfrak{p}$ is prime and $a \notin \mathfrak{p}$ this in turn forces $b \in \mathfrak{p}$, and $\mathfrak{j} \subset \mathfrak{p}$ 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 $\mathfrak{p} \in \mathrm{Spec}(R)$ we conclude from (ii) that

$$\begin{aligned} \mathfrak{p} \in V(\mathfrak{i} \cap \mathfrak{j}) &\Leftrightarrow \mathfrak{i} \cap \mathfrak{j} \subset \mathfrak{p} \\ &\Leftrightarrow \mathfrak{ij} \subset \mathfrak{p} \\ &\Leftrightarrow \mathfrak{p} \in V(\mathfrak{ij}), \end{aligned}$$

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

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

$$\begin{aligned} \mathfrak{p} \subset V(\mathfrak{ij}) &\Leftrightarrow \mathfrak{ij} \subset \mathfrak{p} \\ &\Leftrightarrow \mathfrak{i} \subset \mathfrak{p} \text{ or } \mathfrak{j} \subset \mathfrak{p} \\ &\Leftrightarrow \mathfrak{p} \in V(\mathfrak{i}) \text{ or } \mathfrak{p} \in V(\mathfrak{j}) \\ &\Leftrightarrow \mathfrak{p} \in V(\mathfrak{i}) \cup V(\mathfrak{j}). \end{aligned}$$

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

$$\begin{aligned} \mathfrak{p} \in V(S) &\Leftrightarrow S \subset \mathfrak{p} \\ &\Leftrightarrow (S) \subset \mathfrak{p} \\ &\Leftrightarrow \mathfrak{p} \in V((S)). \end{aligned}$$

q.e.d.

Corollary 9.20 : *For any ideal $\mathfrak{i} \subset R$ and any positive integer n one has $V(\mathfrak{i}^n) = V(\mathfrak{i})$.*

Proof : Use Proposition 9.19(e) and induction. **q.e.d.**

Corollary 9.21 : *For any non-zero element $r \in R$ the following assertions are equivalent:*

(a) *r is a unit;*

(b) *$D(r) = \mathrm{Spec}(R)$; 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 $(r) \subset R$ generated by r must coincide with R. If $\mathfrak{i}$ is any ideal containing r then we also have $(r) \subset \mathfrak{i}$, hence $\mathfrak{i} = R$. Since prime ideals must be proper, $r \notin \mathfrak{p}$ for and prime ideal $\mathfrak{p}$, and (b) follows.

(b) $\Leftrightarrow$ (c) : By Proposition 9.19(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 9.12 that $(r) = R$, hence that $rs = 1$ for some $s \in R$, hence that r is a unit.

q.e.d.

Corollary 9.22 : *For any subset $V \subset \mathrm{Spec}(R)$ 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) *$V = V(\mathfrak{i})$ for some ideal $\mathfrak{i} \subset R$; and*

(e) *$V = V(\mathfrak{r})$ for a unique radical ideal $\mathfrak{r} \subset R$.*

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

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

Proof :

(a) $\Rightarrow$ (b) : By assumption $\mathrm{Spec}(R) \backslash V$ is open, hence has the form $\cup_{s \in S} D(s)$ for some subset $S \subset R$. De Morgan and Proposition 9.19(b) then give

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

and (b) follows.

(b) $\Rightarrow$ (c) : By Proposition 9.19(b).

(c) $\Rightarrow$ (d) : By Proposition 9.19(f).

(d) $\Rightarrow$ (e) and (i): For any prime ideal $\mathfrak{p} \subset R$ one has

$$\begin{aligned} \mathfrak{p} \in V(\mathfrak{i}) &\Leftrightarrow \mathfrak{i} \subset \mathfrak{p} \\ &\Leftrightarrow \sqrt{\mathfrak{i}} \subset \mathfrak{p} \qquad (\text{because } \sqrt{\mathfrak{p}} = \mathfrak{p}) \\ &\Leftrightarrow \mathfrak{p} \in V(\sqrt{\mathfrak{i}}). \end{aligned}$$

This proves (i), and since $\mathfrak{r} := \sqrt{\mathfrak{i}}$ is radical (by Proposition 9.15(a)) it also establishes the existence assertion of (e).

The uniqueness assertion is a consequence of Proposition 9.15(d). Indeed, when $\mathfrak{r} \subset R$ and $\mathfrak{s} \subset R$ are radical ideals satisfying $V(\mathfrak{r}) = V(\mathfrak{s})$ that result gives

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

The converse implication $\mathfrak{r} = \mathfrak{s} \Rightarrow V(\mathfrak{r}) = V(\mathfrak{s})$ does not require proof.

(e) $\Rightarrow$ (a) : Proposition 9.19(b).

q.e.d.

Corollary 9.23 : *The mapping $\mathfrak{r} \subset R \to V(\mathfrak{r}) \subset \mathrm{Spec}(R)$ between radical ideals of R and closed subsets of $\mathrm{Spec}(R)$ is an inclusion reversing bijection. In particular, for any radical ideal $\mathfrak{r} \subset R$ one has*

(a) $V(\mathfrak{r}) = \emptyset \;\Leftrightarrow\; \mathfrak{r} = R$ *and*

(b) $V(\mathfrak{r}) = \mathrm{Spec}(R) \;\Leftrightarrow\; \mathfrak{r} = \sqrt{(0)}$,

and when R is an integral domain one has

(c) $V(\mathfrak{r}) = \mathrm{Spec}(R) \;\Leftrightarrow\; \mathfrak{r} = (0)$.

Less formally: the radical ideals parameterize the closed subsets of $\mathrm{Spec}(R)$. The analogous result for affine algebraic sets with the Zariski topology, i.e., Corollary 4.6, is less satisfactory: the correspondence in that case is surjective, but we need to assume the Nullstellensatz property to ensure bijectivity (Proposition 4.7).

Corollary 9.23 shows that, even though defined only in terms of prime ideals, $\mathrm{Spec}(R)$ with the Zariski topology contains information about ideals of R which may not be prime.

Proof : Use Corollary 9.22 and Proposition 9.19(c). **q.e.d.**

Corollary 9.24 : *For a proper ideal* $\mathfrak{i} \subset R$ *the following statements are equivalent:*

(a) $V(\mathfrak{i}) = \mathrm{Spec}(R)$*; and*

(b) $\mathfrak{i} \subset \sqrt{(0)}$.

Proof : From (i) of Corollary 9.22 we have $V(\mathfrak{i}) = V(\sqrt{\mathfrak{i}})$, and by Corollary 9.23 the radical ideals of R parameterize the closed subsets of $\mathrm{Spec}(R)$ in a bijective manner. Since $\mathfrak{i} \subset \sqrt{\mathfrak{i}}$, the result now follows from Corollary 9.23(b). **q.e.d**.

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

Proposition 9.25 : *For any subset* $Y \subset \mathrm{Spec}(R)$ *the following statements hold.*

(a) *For any ideal* $\mathfrak{i} \subset R$ *one has*

$$Y \subset V(\mathfrak{i}) \;\Leftrightarrow\; \mathfrak{i} \subset \cap_{\mathfrak{p} \in Y} \mathfrak{p}\,.$$

(b) *Let* $\mathcal{I}_Y$ *denote the collection of ideals* $\mathfrak{i}$ *satisfying* $\mathfrak{i} \subset \cap_{\mathfrak{p} \in Y} \mathfrak{p}$. *Then the closure* $\mathrm{cl}(Y)$ *of* Y (in $\mathrm{Spec}(R)$) *is given by*

$$\mathrm{cl}(Y) = V(\cup_{\mathfrak{i} \in \mathcal{I}_Y} \mathfrak{i}) = V(\textstyle\sum_{\mathfrak{i} \in \mathcal{I}_Y} \mathfrak{i}).$$

Moreover, for any prime ideal $\mathfrak{q} \subset R$ *one has*

(i) $$\mathrm{cl}(\{\mathfrak{q}\}) = V(\mathfrak{q}).$$

Proof :

(a) We have

$$\begin{aligned} Y \subset V(\mathfrak{i}) &\Leftrightarrow \mathfrak{p} \in V(\mathfrak{i}) \text{ for all } \mathfrak{p} \in Y \\ &\Leftrightarrow \mathfrak{i} \subset \mathfrak{p} \text{ for all } \mathfrak{p} \in Y \\ &\Leftrightarrow \mathfrak{i} \subset \cap_{\mathfrak{p} \in Y} \mathfrak{p}\,. \end{aligned}$$

(b) By Corollary 9.22(d) any closed set of $\mathrm{Spec}(R)$ has the form $V(\mathfrak{i})$ for some ideal $\mathfrak{i} \subset R$, and so from (a) and Proposition 9.19(d) we have

$$\mathrm{cl}(Y) = \cap_{\mathfrak{i} \in \mathcal{I}_Y} V(\mathfrak{i}) = V(\cup_{\mathfrak{i} \in \mathcal{I}_Y} \mathfrak{i}).$$

But one sees easily that the ideal generated by $\cup_{\mathfrak{i} \in \mathcal{I}_Y} \mathfrak{i}$ is precisely $\sum_{\mathfrak{i} \in \mathcal{I}_Y} \mathfrak{i}$, and the result follows.

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

q.e.d.

With Proposition 9.19(a) as motivation we define an open set $D(\mathfrak{i})$, for any ideal $\mathfrak{i} \subset R$, by

$$D(\mathfrak{i}) := \mathrm{Spec}(R)\backslash V(\mathfrak{i}). \tag{9.26}$$

Note from Corollary 9.23(a) that

$$D(R) = \mathrm{Spec}(R). \tag{9.27}$$

Also note that

$$D(\mathfrak{i}) = \cup_{r\in\mathfrak{i}} D(r)\,. \tag{9.28}$$

Indeed, from De Morgan and Proposition 9.19(b) we have

$$\begin{aligned} D(\mathfrak{i}) &= \mathrm{Spec}(R)\backslash V(\mathfrak{i}) \\ &= \mathrm{Spec}(R)\backslash \cap_{r\in\mathfrak{i}} V(r) \\ &= \cup_{r\in\mathfrak{i}}\mathrm{Spec}(R)\backslash V(r) \\ &= \cup_{r\in\mathfrak{i}} D(r). \end{aligned}$$

10. 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 10.1 : *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 $C_n \neq X$ we see from (a) the closed set $\cup_{j=1}^{n-1} C_j$ 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 $\{ U, \mathrm{cl}(U)^c \}$ 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 10.2 : *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 10.1(c); the reverse is obvious. **q.e.d.**

Corollary 10.3 : *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 10.1(e) to the open set X. **q.e.d.**

Proposition 10.4 : *Suppose X is a topological space and $Y \subset X$ is a non-empty subspace. Assume the relative topologies on both Y and $\mathrm{cl}(Y)$. Then Y is irreducible if and only if $\mathrm{cl}(Y)$ is irreducible.*

Proof :

$\Rightarrow$ When $\{C_j\}_{j=1}^n$ is a closed cover of $\mathrm{cl}(Y)$ the collection $\{C_j \cap Y\}_{j=1}^n$ is such a cover for Y, and from (b) of Proposition 10.1 we conclude that $C_i \cap Y = Y$ for at least one index i. Because C_i is also closed in X we have $\mathrm{cl}(Y) \subset C_i \subset \cup_j \mathrm{cl}(C_j) = \mathrm{cl}(Y)$, hence $C_i = \mathrm{cl}(Y)$, and a second appeal to Proposition 10.1(b) establishes the irreducibility of $\mathrm{cl}(Y)$.

$\Leftarrow$ When $\{C_j\}_{j=1}^n$ is a closed cover of Y we must have $C_j = Y \cap D_j$ for some closed $D_j \subset X$. For $j = 1, \ldots, n$ set $E_j := \mathrm{cl}(Y) \cap D_j \subset \mathrm{cl}(Y)$ and note that $C_j = Y \cap D_j = (Y \cap \mathrm{cl}(Y)) \cap D_j = Y \cap E_j$. Since each E_j is closed the same is true of $\cup_j E_j$, and we conclude from $Y = \cup_j C_j \subset \cup_j E_j$ and $E_j \subset \mathrm{cl}(Y)$ that $\{E_j\}_{j=1}^n$ is a closed cover of $\mathrm{cl}(Y)$. From (a) and Proposition 10.1(b) we therefore have $E_i = \mathrm{cl}(Y)$ for at least one index i, whence $C_i = Y \cap E_i = Y \cap \mathrm{cl}(Y) = Y$. A final appeal to Proposition 10.1(b) completes the proof.

q.e.d.

Corollary 10.5 : *The closure $\mathrm{cl}(\{x\})$ 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 *locus* of that point. The result could therefore be stated: *the locus of any point is irreducible.*

For the Zariski topology associated with Example 6.3(a) we have $\mathrm{cl}(\{\sqrt{2}\}) = \{\pm\sqrt{2}\}$, whereas for that associated with Example 6.3(b) we have $\mathrm{cl}(\{\sqrt{2}\}) =$

$\{\sqrt{2}\}$. In particular, when the Zariski topology of Example 6.3(a) is assumed the two-point set $\{-\sqrt{2},\ \sqrt{2}\}$ is irreducible, and therefore connected (by Corollary 10.3).

Proof : Apply Proposition 10.4 to the irreducible space $Y = \{x\}$. **q.e.d.**

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

Theorem 10.6 : *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 $\mathcal{V} \subset B^n$ is (A, B)-Zariski closed. Then the following three statements are equivalent:*

(a) *$\mathcal{V}$ is irreducible;*

(b) *the defining ideal $\mathfrak{i}(\mathcal{V})$ is prime; and*

(c) *the coordinate ring $A_B[\mathcal{V}]$ is an integral domain.*

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 the algebraic characterization given in (b) was used as the definition of an irreducible algebraic set.

Proof :

(a) $\Rightarrow$ (b) : Suppose $p, q \in A[x] = A[x_1, x_2, \ldots, x_n]$ and $pq \in \mathfrak{i}(\mathcal{V})$. Then for any $x \in \mathcal{V}$ 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 $\mathcal{V} \subset \mathcal{V}((p)) \cup \mathcal{V}((q))$, and as a result we can write $\mathcal{V} = (\mathcal{V} \cap \mathcal{V}((p))) \cup (\mathcal{V} \cap \mathcal{V}((q)))$. From the irreducibility assumption we may assume w.l.o.g. that $\mathcal{V} = \mathcal{V} \cap \mathcal{V}((p)) \subset \mathcal{V}((p))$. We then have $p(x) = 0$ for all $x \in \mathcal{V}$, hence $p \in \mathfrak{i}(\mathcal{V})$.

(b) $\Rightarrow$ (a) : Suppose $\mathfrak{i}(\mathcal{V})$ is prime and that $\mathcal{V} = \mathcal{V}_1 \cup \mathcal{V}_2$, where each $\mathcal{V}_j \subset \mathcal{V}$ is closed and the inclusions $\mathcal{V}_j \subset \mathcal{V}$ are proper. Then by (c) of Corollary 9.4 and (9.2) there is an element $p_j \in \mathfrak{i}(\mathcal{V}_j)$ with $p_j \notin \mathfrak{i}(\mathcal{V})$ for $j = 1, 2$. But $p_1 p_2 \in \mathfrak{i}$, and this contradicts the assumption that $\mathfrak{i}(\mathcal{V})$ is prime.

(b) $\Leftrightarrow$ (c) : Immediate from the definitions of a coordinate ring and a prime ideal.

q.e.d.

In the following result the mapping $\varphi_{\mathcal{V}} : \mathcal{V} \to \mathrm{Spec}(A_B[\mathcal{V}])$ is that defined in (6.5).

Corollary 10.7 : *For any classical (A, B)-affine algebraic set $\mathcal{V} \subset \mathbb{A}^n_A(B)$ mapping $C \subset \mathcal{V} \mapsto \varphi_{\mathcal{V}}(C)$ is an injection of the closed irreducible subsets of $\mathcal{V}$* (w.r.t. the induced Zariski topology) *into* $\mathrm{Spec}(A_B[\mathcal{V}])$.

The result indicates what sort of information about $\mathcal{V}$ is packaged within $\mathrm{Spec}(A_B[\mathcal{V}])$. Since $\mathcal{V} = \mathbb{A}^n_A(B)$ is a special case, it suggests what information about $\mathbb{A}^n_A(B)$ is stored in $\mathrm{Spec}(A_B[\mathbb{A}^n_A(B)])$.

Proof : Let $C \subset \mathcal{V}$ be both closed and irreducible in the induced topology. By Corollary 9.7(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 $\mathbb{A}^n_A(B)$. However, from $C \subset \mathcal{V}$ we would also have $D, E \subset \mathcal{V}$, and by a second appeal to Corollary 9.7(b) we would conclude that C was reducible.

By Theorem 10.6 the ideal $\mathfrak{i}(C) \subset A[x]$ must be prime. It then follows from Corollary 9.4(c) that the mapping $C \mapsto \mathfrak{i}(C)$ is an injection of the irreducible closed subsets $C \subset \mathcal{V}$ into the prime ideals of $A[x]$. From Proposition 3.4, $C \subset \mathcal{V}$ and (9.2) we have $\ker(f) = \mathfrak{i}(\mathcal{V}) \subset \mathfrak{i}(C)$, and the image of the mapping is therefore contained in $V(\ker(f))$. The result is now immediate from Proposition 5.5(d). **q.e.d**.

Examples 10.8 :

(a) *The circle $x^2 + y^2 = 1$, when considered as a classical $(\mathbb{Z}, \mathbb{R})$-affine algebraic subset of $\mathbb{R}^2$, is both irreducible and connected. Moreover, the principal ideal $(x^2 + y^2 - 1) \subset \mathbb{Z}[x, y]$ is prime.* In Example 3.3(g) we found that the circle S^1 with the $(\mathbb{Z}, \mathbb{R})$-Zariski topology was the closure of many points therein, and is therefore irreducible by Corollary 10.5. It then follows from Theorem 10.6 that the ideal $(x^2 + y^2 - 1) \subset \mathbb{Z}[x, y]$ is prime (or, equivalently, that the $(\mathbb{Z}, \mathbb{R})$-coordinate ring $\mathbb{Z}[x, y]/(x^2 + y^2 - 1)$ is an integral domain), and from Corollary 10.3 that S^1 is connected.

(b) *The parabola $y = x^2$, when considered as a classical $(\mathbb{Z}, \mathbb{R})$-affine algebraic subset of $\mathbb{R}^2$, is both irreducible and connected. Moreover, the principal ideal $(y - x^2) \subset \mathbb{Z}[x, y]$ is prime.* We could again argue as in Example (a), but for variety we take a slightly different route. In Example 3.3(h) we found that the coordinate ring $\mathbb{Z}[x, y]/(y - x^2)$ is isomorphic to $\mathbb{Z}[x]$, and, since the polynomial

ring $\mathbb{Z}[x]$ is an integral domain, it follows (from the definition of a prime ideal) that $(y - x^2)$ is prime. Irreducibility is then immediate from Theorem 10.6, whereupon connectivity becomes a consequence of Corollary 10.3.

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 $\mathfrak{i}, \mathfrak{j} \subset R$ be ideals. Define their *product* $\mathfrak{ij}$ to be the collection of all finite sums $\sum_k i_k j_k$ with $i_j \in \mathfrak{i}$ and $\mathfrak{j}_i \in \mathfrak{j}$. One verifies easily that $\mathfrak{ij}$ is an ideal.

Proposition 10.9 : *When R be a ring and $\mathfrak{p} \subset R$ is a proper ideal the following statements are equivalent:*

(a) *the ideal $\mathfrak{p}$ is prime;*

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

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

The equivalence of (a) and (b) has already been noted and established (see the paragraph immediately preceding Proposition 3.5). It has been included here to highlight the analogy between (b) and (c). Indeed, for particularly nice rings ("Dedekind domains," of which[83] 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) $\Leftrightarrow$ (c).

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

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

q.e.d.

Theorem 10.10 : *Suppose R is an integral domain and $C \subset \mathrm{Spec}(R)$ 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.*

[83] PID is the standard abbreviation for Principal Ideal Domain. We assume familiarity with such entities.

By the "uniquely associated radical ideal" we mean the unique radical ideal provided by Corollary 9.23.

When taken together with Theorem 10.6, 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 :

$\Rightarrow$: Suppose $\mathfrak{i}, \mathfrak{j} \subset R$ are ideals such that $\mathfrak{ij} \subset \mathfrak{r}$ and $D := V(\mathfrak{i})$, $E := V(\mathfrak{j})$. Then from Corollary 9.23 and Proposition 9.19(e) we have $C = V(\mathfrak{r}) \subset V(\mathfrak{ij}) = V(\mathfrak{i}) \cup V(\mathfrak{j}) = D \cup E$. Because C is assumed irreducible this forces either $V(\mathfrak{r}) \subset V(\mathfrak{i}) = V(\sqrt{\mathfrak{i}}\,)$ or $V(\mathfrak{r}) \subset V(\mathfrak{j})$. In the first case $\mathfrak{i} \subset \sqrt{\mathfrak{i}} \subset \mathfrak{r}$; in the second $\mathfrak{j} \subset \mathfrak{r}$. From Proposition 10.9(c) we conclude that the ideal $\mathfrak{r}$ is prime.

$\Leftarrow$: Suppose $C = D \cup E$, where $D, E \subset \mathrm{Spec}(R)$ are closed. By Corollary 9.23 that there are unique radical ideals $\mathfrak{i}, \mathfrak{j}$ such that $D = V(\mathfrak{i})$ and $E = V(\mathfrak{j})$, and from Proposition 9.19 we have

$$\text{(i)} \qquad C = D \cup E \quad \Leftrightarrow \quad V(\mathfrak{r}) = V(\mathfrak{i}) \cup V(\mathfrak{j}) = V(\mathfrak{i} \cap \mathfrak{j}).$$

By Proposition 9.15(a) the ideal $\mathfrak{i} \cap \mathfrak{j}$ is radical, and from a second appeal to Corollary 9.23 we conclude from (i) that

$$\text{(ii)} \qquad C = D \cup E \quad \Leftrightarrow \quad \mathfrak{r} = \mathfrak{i} \cap \mathfrak{j}\,.$$

One sees easily that $\mathfrak{ij} \subset \mathfrak{i} \cap \mathfrak{j}$, hence $\mathfrak{ij} \subset \mathfrak{r}$ by (ii). By Proposition 10.9(c) this forces $\mathfrak{i} \subset \mathfrak{r}$ or $\mathfrak{j} \subset \mathfrak{r}$, hence $C = V(\mathfrak{r}) \subset V(\mathfrak{i}) = D$ or $C \subset E$. The closed set C is therefore irreducible.

q.e.d.

11. 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[84]. 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 11.1 :

(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 $K[x_1, x_2, \dots]$ in infinitely many indeterminates is not Noetherian (because the ideal $(x_1, x_2, \dots)$ is not finitely generated).

(f) A subring of a Noetherian ring need not be Noetherian. For example, the ring $K[x_1, x_2, \dots]$ of Example (e) is an integral domain, and the quotient field $K(x_1, x_2, \dots)$, which we regard as an extension of $K[x_1, x_2, \dots]$, is therefore Noetherian. But we have seen in Example (e) that $K[x_1, x_2, \dots]$ 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[85].

[84] That is, generated by a finite subset. In other words, there must be a finite set $S = \{s_1, s_2, \dots, s_n\} \subset M$ 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 $s_j \in S$. (See the discussion of generators immediately before the statement of Proposition 3.9.)

[85] In our set-theoretic formulation of the Noetherian conditions we follow [A-M, Chapter 6].

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

Proposition 11.2 : *When X is a non-empty set with a partial order relation the following statements are equivalent:*

(a) *every ascending sequence of elements stabilizes; and*

(b) *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 11.3 : *For any R-module M the following statements are equivalent.*

(a) *M is Noetherian;*

(b) *every ascending sequence $M_0 \subset M_1 \subset M_2 \subset \cdots$ of R-submodules of M stabilizes; and*

(c) *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 11.2.

(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 11.4 : *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 11.4 suggests an alternate proof of the assertion of Example 11.1(e): the ascending sequence $(x_1) \subset (x_1, x_2) \subset \cdots$ does not stabilize.

Corollary 11.5 : *Suppose R is a Noetherian ring and $f : R \to S$ is a ring epimorphism. Then S is also Noetherian.*

Proof : When $\mathfrak{j}_0 \subset \mathfrak{j}_1 \subset \cdots$ is an ascending chain of ideals in S we see from Proposition 5.5(c) that the inverse images $f^{-1}(\mathfrak{j}_0) \subset f^{-1}(\mathfrak{j}_1) \subset f^{-1}(\mathfrak{j}_2) \subset \cdots$ form an ascending chain of ideals in R which by hypothesis must stabilize at some integer $r \geq 0$. From $\mathfrak{j}_i = f(f^{-1}(\mathfrak{j}_i))$ 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 11.6 (The Hilbert Basis Theorem) : *When R is a Noetherian ring the polynomial algebra $R[x]$ is also Noetherian.*

Proof : Let $\mathfrak{i} \subset R[x]$ be an ideal and for $n = 0, 1, \ldots$ let $\mathfrak{a}_n \subset R$ be the ideal consisting of 0 and the leading coefficients of polynomials in $\mathfrak{i}$ 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 $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$, and as a consequence for some $r \geq 0$ we have $\mathfrak{a}_{r+j} = \mathfrak{a}_r$ for all $j \geq 0$. For $i = 0, \ldots, r$ let $\{\alpha_{ij}\}_{j=1}^{m_i}$ generate $\mathfrak{a}_i$, and let $p_{ij}(x) \in \mathfrak{i}$ be a polynomial of degree i with leading coefficient α_{ij}. It suffices to prove that $\mathfrak{i} \subset \mathfrak{i}'$, where $\mathfrak{i}'$ is the ideal generated by the finite collection $\{p_{ij}(x)\}$.

Any $a \in \mathfrak{a}_0$ 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 $\mathfrak{i}'$. Inductively, assume any polynomial in $\mathfrak{i}$ of degree at most $n-1 \geq 0$ belongs to $\mathfrak{i}'$ and let $p(x) \in \mathfrak{i}$ 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 $\tilde{p}(x) \in \mathfrak{i}$ has degree at most $n-1$ and $q(x) \in \mathfrak{i}'$. By induction $\tilde{p} \in \mathfrak{i}'$, hence $p(x) \in \mathfrak{i}'$, and the proof is complete. **q.e.d.**

Corollary 11.7 : *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 11.8 : *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 11.9 : *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 11.7 we know that $R[x_1, \ldots, x_n]$ is Noetherian, and the result is then immediate from Corollary 11.5. **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 11.10 : *Suppose A is a Noetherian integral domain, $B \supset A$ is an extension of integral domains, and $n \geq 1$ is an integer. Then $\mathbb{A}^n_A(B)$ is a Noetherian space.*

Recall that $\mathbb{A}^n_A(B)$ is the notation used to indicate B^n when this set is assumed endowed with the (A, B)-Zariski topology[86]. The integral domain assumption on B is needed to guarantee the existence of this topology.

Proof : By (9.2) a decreasing sequence of (not necessarily closed) subsets $X_j \subset X$ corresponds to an increasing sequence of ideals $\mathfrak{i}(X_j) \subset R$. By Corollary 11.7 the ring R is Noetherian, the latter sequence therefore stabilizes, and from Corollary 9.4(c) we conclude that the same must hold for the sequence $\{X_j\}$ when these sets are closed. **q.e.d.**

[86] See the first paragraph following the proof of Corollary 4.6.

Proposition 11.11 : *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; and*

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

Proof :

(a) $\Leftrightarrow$ (b) : Immediate from the comments following the statement of Proposition 11.2.

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

$$\begin{aligned} C_\gamma \subset C_\beta &\Rightarrow \mathrm{cl}(C_\gamma) \subset \mathrm{cl}(C_\beta) \\ &\Rightarrow \mathrm{cl}(C_\gamma) = \mathrm{cl}(C_\beta) \\ &\Rightarrow C_\gamma = \mathrm{cl}(C_\gamma) \cap Y = \mathrm{cl}(C_\beta) \cap Y = C_\beta, \end{aligned}$$

and C_β 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 11.12 : *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 11.10. **q.e.d.**

We next relate the Noetherian property to irreducibility.

Theorem 11.13 : *When X is a Noetherian topological space there is a unique finite collection $\{X_j\}_{j=1}^m$ of closed subspaces of X satisfying 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 11.16(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 11.11(b) contains a minimal element X_μ.

From the defining property of the collection this element must be reducible, say $X_\mu = A \cup B$, where $A, B \subset X_\mu$ 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_μ 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 $X_j = \cup_i (Y_i \cap X_j)$, and by irreducibility we conclude that $X_j = Y_i \cap X_j$ for some i, i.e., that $X_j \subset Y_i$. 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). **q.e.d.**

Corollary 11.14 : *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 10.4 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 11.13, contradicting uniqueness. **q.e.d.**

It is now a relatively simple matter to understand the the topological structure of any classical affine algebraic set.

Theorem 11.15 : *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 $\mathcal{V} \subset \mathbb{A}^n_A(B)$ there corresponds a unique finite collection $\{\mathcal{V}_j\}_{j=1}^n$ of irreducible classical (A, B)-affine algebraic subsets with the following three properties:*

(a) $\mathcal{V} = \mathcal{V}_1 \cup \cdots \cup \mathcal{V}_m$;

(b) *each of the defining ideals $\mathfrak{i}(\mathcal{V}_j) \subset A[x] = A[x_1, x_2, \ldots, x_n]$ is prime; and*

(c) $\mathcal{V}_i$ *is not a subset of* $\mathcal{V}_j$ *for all* $1 \leq i \neq j \leq m$.

Irreducible affine algebraic sets are called *affine algebraic varieties*[87]; the study of classical affine algebraic sets is thereby reduced to the study of such sets having this particular form. The collection $\{\mathcal{V}_j\}_{j=1}^m$ is the *irreducible decomposition* of $\mathcal{V}$.

Proof : Immediate from Corollary 11.12 and Theorem 10.6. **q.e.d.**

Examples 11.16 :

(a) When X is an irreducible Noetherian space we have $n = 1$ and $X = X_1$ in the statement of Theorem 11.13.

(b) In Corollary 11.15 take $A = B = \mathbb{R}$, $n = 2$, and let $\mathcal{V} := \mathcal{V}(\{x_1^2 - x_2^2\}) \subset X = \mathbb{R}^2$. 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.

[87] 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.

12. Closed Points

In this section $B \supset A$ *is an extension of integral domains, and* $n \geq 1$ *is an integer.* $\mathbb{A}^n_A(B)$ *and algebraic subsets thereof are always assumed endowed with the* (A, B)*-Zariski topologies.*

A point x of a topological space X is (a) *closed* (*point*) if $\mathrm{cl}(\{x\}) = \{x\}$, 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 $X = \mathbb{A}^n_A(B)$ we see from Corollary 9.4 (or Corollary 9.7) that a point $c \in \mathbb{A}^n_A(B)$ is closed if and only if

$$\{c\} = \mathcal{V}(\mathfrak{i}(\{c\})). \tag{12.1}$$

When $\mathcal{V} \subset \mathbb{A}^n_A(B)$ is a classical (A, B)-affine algebraic set it follows from Corollary 9.7 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 12.2 : *When* $A = B$ *all points of* $\mathbb{A}^n_A(B)$ *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 9.4.

Proof : This is simply a restatement of Corollary 9.5. **q.e.d.**

Proposition 12.3 : *Suppose* $\mathcal{W} \subset \mathbb{A}^n_A(B)$ *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* $\mathfrak{j} \subset A[x]$ *containing* $\mathfrak{i}(\{w\}) \subset A[x]$ *one has either* $\mathcal{V}(\mathfrak{j}) = \emptyset$ *or* $\mathcal{V}(\mathfrak{j}) = \{w\}$.

Note that the given necessary and sufficient conditions do not involve $\mathcal{W}$. This is explained by Corollary 9.7: closures of subsets of $\mathcal{W}$ in the induced topology are the same as Zariski closures in $\mathbb{A}^n_A(B)$.

Proof :

$\Rightarrow$ Suppose $w \in \mathcal{W}$ is a closed point and $\mathfrak{j}$ is an ideal containing $\mathfrak{i}(\{w\})$. Then from (4.1) and (12.1) we see that $\mathcal{V}(\mathfrak{j}) \subset \mathcal{V}(\mathfrak{i}(\{w\})) = \{w\}$, and the result immediately follows.

$\Leftarrow$ By choosing $\mathfrak{j} = \mathfrak{i}(\{w\})$ we see that $\mathcal{V}(\mathfrak{i}(\{w\})) = \emptyset$ or $\mathcal{V}(\mathfrak{i}(\{w\})) = \{w\}$, and the first alternative is impossible since $w \in \mathcal{V}(\mathfrak{i}(\{w\}))$. Now make a second appeal to (12.1).

q.e.d.

Corollary 12.4 : *Suppose that the surjective mapping* $\mathfrak{i} \mapsto \mathcal{V}(\mathfrak{i})$ *of* Corollary 4.6, *from the radical ideals of* $A[x]$ *to the classical* (A, B)*-affine algebraic subsets of* $\mathbb{A}^n_A(B)$, *is bijective. Then the following assertions hold for any classical* (A, B)*-affine algebraic set* $\mathcal{W} \subset \mathbb{A}^n_A(B)$.

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

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

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

Less formally: under the stated hypotheses one can think of points as maximal ideals and vice versa[88].

The choice $\mathcal{W} = \mathbb{A}^n_A(B)$ is a very important special case of the proposition.

Sufficient conditions for the bijectivity hypothesis were given in Proposition 4.7.

Proof :

(a)

$\Rightarrow$ Otherwise we can invoke Corollary 9.11 to choose a maximal ideal $\mathfrak{j}$ properly containing $\mathfrak{i}(\{w\})$, which by Proposition 7.2(b) must be radical. In view of the bijectivity hypothesis we see from Theorem 4.5(a) that $\mathcal{V}(\mathfrak{j}) \neq \emptyset$, and we therefore have $\mathcal{V}(\mathfrak{j}) = \{w\} = \mathcal{V}(\mathfrak{i}(\{w\}))$ by Proposition 12.3. Since $\mathfrak{i}(\{w\})$ is also radical (by Proposition 6.4 and Proposition 3.5), a second appeal to the bijectivity hypothesis then gives $\mathfrak{j} = \mathfrak{i}(\{w\})$, and we have a contradiction.

$\Leftarrow$ If $\mathfrak{i}(\{w\})$ 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 12.3 are therefore met, and w is therefore closed.

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

From $\{c\} \subset \mathcal{V}(\mathfrak{m})$, (9.2) and Proposition 9.3(b) we have $\mathfrak{i}(\{c\}) \supset \mathfrak{i}(\mathcal{V}(\mathfrak{m})) \supset \mathfrak{m}$, and since $\mathfrak{m}$ is maximal this forces either $\mathfrak{i}(\{c\}) = A[x]$ or the desired conclusion $\mathfrak{i}(\{c\}) = \mathfrak{m}$. The first alternative is easily dismissed: non-zero constant functions cannot vanish at the point c.

[88] This 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 $\mathfrak{i} \to \mathcal{V}(\mathfrak{i})$.

q.e.d.

The closed points of the prime spectrum $\mathrm{Spec}(R)$ of any ring R have a characterization analogous to that given in Corollary 12.4(a), and the annoying qualifications (e.g., that regarding bijectivity and the requirement that B be an integral domain) are absent.

Proposition 12.5 : *For any prime ideal $\mathfrak{p} \subset R$ the following statements are equivalent:*

(a) *the point $\mathfrak{p} \in \mathrm{Spec}(R)$ is closed;*

(b) $V(\mathfrak{p}) = \{\mathfrak{p}\}$*; and*

(c) $\mathfrak{p}$ *is a maximal ideal.*

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

Proof :

(a) $\Leftrightarrow$ (b) : From (i) of Proposition 9.25 and (9.16) we have

$$\text{(i)} \qquad \mathrm{cl}(\{\mathfrak{p}\}) = V(\mathfrak{p}) = \{\, \mathfrak{q} \in \mathrm{Spec}(R) \,:\, \mathfrak{p} \subset \mathfrak{q} \,\},$$

and as a result we see that

$$\text{(ii)} \qquad \mathfrak{p} \text{ is closed} \quad \Leftrightarrow \quad V(\mathfrak{p}) = \{\mathfrak{p}\} = \{\, \mathfrak{q} \in \mathrm{Spec}(R) \,:\, \mathfrak{p} \subset \mathfrak{q} \,\}.$$

(a) $\Rightarrow$ (c) : If $\mathfrak{p}$ is closed but not maximal there is an ideal $\mathfrak{j}$ satisfying $\mathfrak{p} \subset \mathfrak{j} \subset R$ with both inclusions proper, and by Corollary 9.11 we may assume $\mathfrak{j}$ is maximal. But $\mathfrak{j}$ is then a prime ideal distinct from $\mathfrak{p}$ contained in $V(\mathfrak{p})$, and this contradicts the final equality in (ii).

(c) $\Rightarrow$ (a) : When $\mathfrak{p}$ is maximal there can be no prime ideal $\mathfrak{q}$ properly containing $\mathfrak{p}$ (in fact there can be no proper ideal containing $\mathfrak{p}$ as a proper subset), and from (i) we conclude that $\mathrm{cl}(\{\mathfrak{p}\}) = \{\mathfrak{p}\}$. **q.e.d.**

13. An Application of the Prime Spectrum - The Infinitude of Primes

This section represents what I hope will be an amusing diversion[89] for the reader: we will use the Zariski topology on $\mathrm{Spec}(\mathbb{Z})$ 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][90], 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 $p \in A$ is prime[91] 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 $\{2, 3, 5, 7, 11, 13, \dots\}$ 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[92].

Theorem 13.1 : *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 $\mathrm{Spec}(A)$ *is infinite, and there must be infinitely many primes in A.*

---

[89] I say "amusing diversion" because there are certainly easier ways to prove the results achieved.

[90] In particular, see Theorem 3.4, p. 136, of that reference.

[91] 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 $c \in A$.

[92] Unique factorization domain, or what is now sometimes called a *factorial ring*, e.g., as in [L, Chapter II, §5, p. 111].

The proof[93] was inspired by H. Fürstenberg's topological proof of Euclid's Theorem [Für]. 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 $p \in P \mapsto (p) \in \mathrm{Spec}(A) \setminus \{(0)\}$ is a bijection. In particular, $\mathrm{Spec}(A)$ is infinite if and only if this is the case for P, and it therefore suffices to prove that $\mathrm{Spec}(A)$ is infinite. We argue by contradiction.

By (I) and Proposition 12.5 all $\mathfrak{p} \in \mathrm{Spec}(A)$ except the zero ideal (0) are closed (points). If $\mathrm{Spec}(A)$ is finite then $\mathrm{Spec}(A) \setminus \{(0)\}$ must be closed, and $(0) \in \mathrm{Spec}(A)$ 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 $\mathfrak{p} \notin D(a)$ for all non-zero prime ideals $\mathfrak{p}$. Writing $\mathfrak{p}$ as (p), with $p \in P$, we see from Proposition 9.19(a) that

$$\begin{aligned} \mathfrak{p} \notin D(a) &\Leftrightarrow \mathfrak{p} \in V(a) \\ &\Leftrightarrow a \in \mathfrak{p} \\ &\Leftrightarrow a \in (p) \\ &\Leftrightarrow p|a. \end{aligned}$$

In other words, $\mathfrak{p} \notin D(a)$ for all non-zero prime ideals $\mathfrak{p}$ 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). **q.e.d.**

Corollary 13.2 :

(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) Theorem 9.27, pp. 431-2]. Since these rings are obviously infinite, it only remains

[93] 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.

to verify condition (c) of Theorem 13.1. 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[94] $\{1, -1, \zeta, -\zeta, \zeta^2, -\zeta^2\}$, where $\zeta := e^{2\pi i/3} \in \mathbb{C}$.

To verify condition (c) of Theorem 13.1 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.

[94]For proofs see, e.g., [N-Z-M, Chapter 9, §6, Theorem 9.22, p. 428].

14. 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.

- $\mathrm{cl}(\{c\})$ is the *locus*[95] of c;
- any point of $\mathrm{cl}\{c\})$ is a *specialization* of c;
- c is a *generic point* of C if $\mathrm{cl}(\{c\}) = C$ (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.

Proposition 14.1 :

(a) *The locus of any point* $c \in X$ *is an irreducible closed subset of* X.

(b) *If a closed set* $C \subset X$ *admits a generic point then* C *must be irreducible.*

(c) *If a closed set* $C \subset X$ *admits a generic point then* C *must be connected.*

Proof :

(a) This is a restatement of Corollary 10.5.

(b) By (a).

(c) By (b) and Corollary 10.3.

q.e.d.

Corollary 14.2 : *Suppose* $B \supset A$ *is an extension of integral domains,* $n \geq 1$ *is an integer, and* $\mathcal{V} \subset \mathbb{A}^n_A(B)$ *is a classical* (A, B)*-affine algebraic set which admits a generic point. Then* $\mathcal{V}$ *is irreducible and connected, and the defining ideal* $\mathfrak{i}(\mathcal{V}) \subset A[x]$ *is prime.*

Proof : Use Proposition 14.1 and Theorem 10.6. **q.e.d.**

[95] We have seen this definition before: immediately following the statement of Corollary 10.5. It is repeated here for ease of reference.

Examples 14.3 : 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[96] $\mathrm{cl}(\{\sqrt{2}\}) = \{\sqrt{2},-\sqrt{2}\}$. 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 $\{\sqrt{2},-\sqrt{2}\}$. By Corollary 14.2 this two-point set is both irreducible and connected, and the defining ideal $(x^2-2) \subset \mathbb{Z}[x]$ (derived in Example 3.3(b)) is prime.

(b) When $(A,B) = (\mathbb{Z},\mathbb{R})$ we have[97] $\mathrm{cl}(\{\pi\}) = \mathbb{R}$ (and one can replace π in this argument with any real number transcendental over $\mathbb{Q}$). The locus of π is therefore $\mathbb{R}$, any real number is a specialization of π, and π is a generic point of $\mathbb{R}$. In particular, $\mathbb{R}$ with the $(\mathbb{Z},\mathbb{R})$-Zariski topology is both irreducible and connected. (We have noted that $\mathbb{R}$ with the usual topology is reducible.)

(c) When $(A,B) = (\mathbb{R},\mathbb{R})$ we see from Proposition 12.2 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.)

(d) Suppose R is a ring in which $\{0\}$ is a prime ideal. Then in $\mathrm{Spec}(R)$ with the Zariski topology: the locus of $\{0\}$ is $\mathrm{Spec}(R)$; every prime ideal is a specialization of $\{0\}$; and $\{0\}$ is the unique generic point of $\mathrm{Spec}(R)$. In particular, under the stated hypothesis $\mathrm{Spec}(R)$ is both irreducible and connected.

(e) Suppose $(A,B) = (\mathbb{Z},\mathbb{R})$ and $t \in R$ is such that $\sin t$ is transcendental over $\mathbb{Q}$. Then $(\cos t, \sin t) \in \mathbb{R}^2$ 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 $\{x_1^2+x_2^2-1\} \subset \mathbb{Z}[x]$). This was already noted in Examples 3.3(g) and 10.8(a), although without the "generic point" terminology.

It might be worth noting that not all points of the circle are generic points. For a specific example consider the point $(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})$, which is obviously a zero of the

[96] Argue as in Footnote 21.

[97] Since π 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 π also vanishes on $\mathbb{R}$ is therefore vacuously satisfied, and $\mathrm{cl}(\{\pi\}) = \mathbb{R}$ follows.

polynomial $t = x - y \in \mathbb{Z}[x,y]$. If $u \in \mathbb{Z}[x,y]$ also vanishes on this point one can use the Euclidean algorithm to write

$$u(x,y) = v(x,y)(x-y) + w(y),$$

where $w(y) \in R := \mathbb{Z}[x]$. Then $0 = u(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}) = v(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}) \cdot 0 + w(\frac{\sqrt{2}}{2})$, hence $w(\frac{\sqrt{2}}{2}) = 0$. But this implies[98] $w(-\frac{\sqrt{2}}{2}) = 0$, and we conclude that $\mathrm{cl}(\{\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\})$ is the two-point set $\{\pm(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})\}$ (which is far from being the entire circle).

(f) Suppose $(A,B) = (\mathbb{Z}, \mathbb{R})$ and $t \in \mathbb{R}$ is transcendental over $\mathbb{Q}$. Then the point (t, t^2) is a generic point of the parabola $y = x^2$, i.e., of the classical $(\mathbb{Z}, \mathbb{R})$-affine algebraic subset of $\mathbb{R}^2$ defined by $y = x^2$. This was also previously noted, again without the "generic point" terminology: recall Example 3.3(h).

In the following result we employ the notation surrounding (6.5).

Proposition 14.4 : *Suppose $B \supset A$ is an extension of integral domains, $n \geq 1$ is an integer, and $\mathcal{V} \subset \mathbb{A}^n_A(B)$ is a classical (A,B)-affine algebraic set. Then the following assertions hold.*

(a) *A necessary condition for a prime ideal $\mathfrak{p} \in \mathrm{Spec}(A_B\mathcal{V}])$ to be in the range of the mapping $\varphi_{\mathcal{V}} : \mathcal{V} \to \mathrm{Spec}(A_B[\mathcal{V}])$ of* (6.5) *is that the irreducible algebraic set $\mathcal{V}(f^{-1}(\mathfrak{p}))$ admit a generic point.*

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

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

Proof :

(a) If $\mathfrak{p} \in \mathrm{Spec}(A_B[\mathcal{V}])$ is in the range of $\varphi_{\mathcal{V}}$ we must have $\mathfrak{p} = f(\mathfrak{i}(\{c\}))$ for some point $c \in \mathcal{V}$. However,

$$\begin{aligned} \mathfrak{p} = f(\mathfrak{i}(\{c\})) &\Leftrightarrow f^{-1}(\mathfrak{p}) = \mathfrak{i}(\{c\}) \\ &\Rightarrow \mathcal{V}(f^{-1}(\mathfrak{p})) = \mathcal{V}(\mathfrak{i}(\{c\})) = \mathrm{cl}(\{c\}), \end{aligned}$$

[98] 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 $\frac{\sqrt{2}}{2}$ is not the root of a linear polynomial in $\mathbb{Z}[x]$, it follows from the quadratic formula that $-\frac{\sqrt{2}}{2}$ must also be a root of w.

the last equality by Corollary 9.4(a), and the result follows.

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

It $C \subset \mathcal{V}$ is a closed subset there is, by hypothesis, a unique radical ideal $\mathfrak{q} \subset A[x]$ such that $C = \mathcal{V}(\mathfrak{q})$. By Proposition 5.5(d) we can write $\mathfrak{q} = f^{-1}(\mathfrak{p})$ for a unique prime ideal $\mathfrak{p} \subset A_B[\mathcal{V}]$. If C admits a generic point c then $C = \mathrm{cl}(\{c\}) = \mathcal{V}(\mathfrak{i}(\{c\}))$ (by Corollary 9.7(a)). Since $\mathfrak{i}(\{c\})$ is radical[99] the hypotheses force $\mathfrak{q} = \mathfrak{i}(\{c\})$, hence $\mathfrak{p} = \varphi_{\mathcal{V}}(C) = f(\mathfrak{i}(\{c\})) = \varphi_{\mathcal{V}}(c)$.

q.e.d.

In the older literature specializations and generic points were defined in terms of ring homomorphisms. Specifically, a specialization of a point $c \in \mathbb{A}^n_A(B)$ referred to any point $d \in \mathbb{A}^n_A(B)$ satisfying condition (f) of the following result[100].

Proposition 14.5 : *Suppose $B \supset A$ is an extension of integral domains, $n \geq 1$ is an integer, and $c = (c_1, c_2, \ldots, c_n)$, $d = (d_1, d_2, \ldots, c_n) \in \mathbb{A}^n_A(B)$. Then the following assertions are equivalent.*

(a) *d is a specialization of c;*

(b) *d is in the locus of c;*

(c) *every polynomial in $A[x] = A[x_1, x_2, \ldots, x_n]$ which vanishes on c must also vanish on d;*

(d) $\mathfrak{i}(\{c\}) \subset \mathfrak{i}(\{d\})$*;*

(e) *the canonical homomorphism $g : A[x] \to A[x]/\mathfrak{i}(\{d\})$ factors through the canonical homomorphism $f : A[x] \to A[x]/\mathfrak{i}(\{c\})$, i.e., there is an an A-algebra homomorphism $h : A[x]/\mathfrak{i}(\{c\}) \to A[x]/\mathfrak{i}(\{d\})$ which makes the diagram*

$$\begin{array}{ccc} A[x] & & \\ {\scriptstyle f}\downarrow & \overset{g}{\searrow} & \\ A[x]/\mathfrak{i}(\{c\}) & \xrightarrow{h} & A[x]/\mathfrak{i}(\{d\}) \end{array}$$

commute; and

[99] By Proposition 9.1.

[100] In fact this definition is still found in contemporary algebra texts, e.g., see [L, Chapter IX, §2, p. 383].

(f) *there is an* A*-algebra homomorphism*[101] $h : A[c_1, c_2, \ldots, c_n] \to A[d_1, d_2, \ldots, d_n]$ *satisfying* $h : c_j \mapsto d_j$ *for* $j = 1, 2, \ldots, n$.

Moreover, precisely the same conditions are equivalent if c *and* d *are assumed points on a classical* (A, B)*-affine algebraic set* $\mathcal{V} \subset \mathbb{A}^n_A(B)$ *and the topology is assumed to be the* (A, B)*-Zariski topology on* $\mathcal{V}$.

Proof :

(a) $\Leftrightarrow$ (b) : Immediate from the definitions.

(a) $\Leftrightarrow$ (c) : This is a special case of the remark immediately following the statement of Corollary 9.4.

(c) $\Leftrightarrow$ (d) : Immediate from the definitions.

(d) $\Rightarrow$ (e) : Obvious.

(e) $\Rightarrow$ (d) : From (6.2) we have $\mathfrak{i}(\{c\}) = \ker(f)$ and $\mathfrak{i}(\{d\}) = \ker(d)$, and commutativity obviously gives $\ker(f) \subset \ker(g)$.

(e) $\Leftrightarrow$ (f) : From (6.2) we have identifications $A[x]/\mathfrak{i}(\{c\}) \simeq A[c_1, c_2, \ldots, c_n]$ and $A[x]/\mathfrak{i}(\{d\}) \simeq A[d_1, d_2, \ldots, d_n]$, and from this point the equivalence is evident.

For the final assertion recall Corollary 9.7. **q.e.d.**

[101] The ring $A[c_1, c_2, \ldots, c_n]$ is obtained by replacing x_j with $c_j \in B$, for $j = 1, 2, \ldots, n$, in each polynomial of $A[x]$, i.e., $A[c_1, c_2, \ldots, c_n]$ consists of "polynomials in $c_1, c_2, \ldots, c_n$ with coefficients in A." We note that $c_i = c_j$ for $i \neq j$ is allowed. Such notation is discussed in greater detail in the paragraph immediately before the statement of Proposition 3.9.

15. Compactness

Once again R denotes a ring.

A topological space is *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 15.1 : $\mathrm{Spec}(R)$ *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 $\mathrm{Spec}(R)$ of the form $\{D(r)\}_{r\in S\subset R}$ admits a finite-subcover.

So assume such a cover and let $\mathfrak{i} \subset R$ be the ideal generated by S. Then $\mathrm{Spec}(R) = \cup_{r\in S} D(r)$ and $S \subset \mathfrak{i}$ give $\mathrm{Spec}(R) = \cup_{r\in\mathfrak{i}} D(r) = D(\mathfrak{i})$, whence $V(\mathfrak{i}) = \emptyset$, whereupon from (i) of Corollary 9.22, Proposition 9.15 and Corollary 9.23 we see that $\sqrt{\mathfrak{i}} = R$. But this means $1 \in \sqrt{\mathfrak{i}}$, and since $1 = 1^n$ for any integer $n \geq 1$ it follows that $1 \in \mathfrak{i}$, i.e., that there a finite collection $\{s_j\}_{j\in J} \subset S$ and a corresponding collection $\{r_j\}_{j\in J} \subset R$ such that

$$\text{(i)} \qquad 1 = \textstyle\sum_{j\in J} r_j s_j.$$

Let $\mathfrak{j} \subset R$ denote the ideal generated by $\{s_j\}_{j\in J}$. Then from (i) we have $\mathfrak{j} = R$, hence $\sqrt{\mathfrak{j}} = \mathfrak{j} = R$, and from Corollary 9.23(a) and Proposition 9.16(b) we conclude that $\emptyset = V(\mathfrak{j}) = \cap_{j\in J} V(s_j)$. Taking complements then gives $\mathrm{Spec}(R) = \cup_{j\in J} D(s_j)$, and the proof is complete. **q.e.d.**

16. Connectedness

R denotes a ring with $0 \neq 1$.

An element $r \in R$ is (an) *idempotent* if $r^2 = r$, e.g., 0 and 1.

Proposition 16.1 : *The following assertions are equivalent.*

(a) *There are non-trivial subrings $R_1, R_2 \subset R$ such that the mapping $(r_1, r_2) \in R_1 \times R_2 \mapsto r_1 + r_2 \in R$ is a ring isomorphism.*

(b) *R is* (isomorphic to) *the direct sum of two non-trivial rings.*

(c) *There is an idempotent $e \in R \backslash \{0, 1\}$.*

(d) *There are idempotents $e_1, e_2 \in R \backslash \{0, 1\}$ such that $e_1 e_2 = 0$ and $e_1 + e_2 = 1$.*

Proof :

(a) $\Leftrightarrow$ (b) : Obvious.

(a) $\Rightarrow$ (c) : W.l.o.g. we may assume $R = R_1 \times R_2$; $e := (1, 0)$ then satisfies the required condition.

(c) $\Rightarrow$ (d) : Take $e_1 := e$ and $e_2 := 1 - e$.

(d) $\Rightarrow$ (a) : Set $R_j := Re_j$, $j = 1, 2$ and check, using the properties of e_1, e_2, that both are subrings of R, and that the mapping $f : (r_1, r_2) \in R_1 \times R_2 \mapsto r_1 + r_2 \in R$ is a ring homomorphism.

Write $r_j = \hat{r}_j e_j$, $j = 1, 2$, and suppose $f((r_1, r_2)) = \hat{r}_1 e_1 + \hat{r}_2 e_2 = 0$. Multiplying this last equality by e_j then gives $\hat{r}_j = 0$, and injectivity follows.

To verify surjectivity simply note from $1 = e_1 + e_2$ that for any $r \in R$ we have $r = re_1 + re_2 = f((r_1 e_1, r_2 e_2))$.

q.e.d.

The following result is useful for establishing the existence of non-zero idempotents.

Proposition 16.2 : *Suppose $\mathfrak{i}_1$ and $\mathfrak{i}_2$ are non-zero ideals of R such that*

(i) $$\mathfrak{i}_1 + \mathfrak{i}_2 = R$$

and

(ii) $$\mathfrak{i}_1 \cap \mathfrak{i}_2 = (0).$$

Then $\mathfrak{i}_1$ *and* $\mathfrak{i}_2$ *are principal ideals generated by non-zero idempotents* $e_1, e_2 \in R$ *such that*

(iii) $$e_1 e_2 = 0.$$

In particular, R *contains an idempotent distinct from* 0 *and* 1.

The result generalizes to any finite collection of ideals, but that level of generality will not be needed[102].

Proof : By (i) there are elements $e_j \in \mathfrak{i}_j$ such that

(iv) $$e_1 + e_2 = 1,$$

and since $e_1 e_2 \in \mathfrak{i}_1 \cap \mathfrak{i}_2$ we see from (ii) that (iii) must hold. Moreover, from (iv) we then have

$$e_j^2 = e_j(e_1 + e_2) = e_j \cdot 1 = e_j, \qquad j = 1, 2,$$

proving that the e_j are idempotent. To complete the proof note from $e_j \in \mathfrak{j}$ that $(e_j) \subset \mathfrak{i}_j$, and from (iv) and (ii) that $(e_1) + (e_2) = R$ as well as $(e_1) \cap (e_j) = \{0\}$; the equalities $\mathfrak{i}_j = (e_j)$ for $j = 1, 2$ follow. **q.e.d.**

Theorem 16.3 : *The following assertions are equivalent:*

(a) $\mathrm{Spec}(R)$ *is connected;*

(b) *the only idempotents of* R *are* 0 *and* 1*; and*

(c) *there are no non-trivial subrings* $R_1, R_2 \subset R$ *such that the mapping* $f : (r_1, r_2) \in R_1 \times R_2 \mapsto r_1 + r_2 \in R$ *is a ring isomorphism.*

(d) R *is not* (isomorphic to) *the direct sum of two non-trivial rings.*

Proof :

(a) $\Rightarrow$ (b) : Suppose $e \in R \backslash \{0, 1\}$ is such that $e^2 = e$. Then $0 = e^2 - e = e(e-1)$, and from (5.3) we conclude that $\emptyset = D(e) \cap D(e-1)$, whence that

(i) $$\mathrm{Spec}(R) = V(e) \cup V(e-1).$$

[102] Our principal source for this result is the proof of Proposition 15 in [Bour, Chapter II, §4.3, p. 103], which covers the more general case.

We claim that

(ii) $$V(e) \cap V(e-1) = \emptyset.$$

Otherwise there is a $\mathfrak{p} \in \mathrm{Spec}(R)$ such that $e \in \mathfrak{p}$ and $e-1 \in \mathfrak{p}$, whence $e-(e-1) = 1 \in \mathfrak{p}$, contradicting that $\mathfrak{p}$ is a prime (and therefore proper) ideal of R. Since $V(e)$ and $V(1-e)$ are closed (Proposition 9.19(a)) it follows from (i) and (ii) that $V(e) = \mathrm{Spec}(R) \backslash V(1-e)$ is both open and closed, and from (i) that the inclusion $V(e) \subset \mathrm{Spec}(R)$ is proper. This contradicts (a).

(b) $\Rightarrow$ (a) : If (a) fails we can realize $\mathrm{Spec}(R)$ as the union of non-empty disjoint closed sets, and by Corollary 9.22(d) these closed sets must be of the form $V(\mathfrak{i}_j)$, $j = 1, 2$, where $\mathfrak{i}_1, \mathfrak{i}_2 \subset R$ are ideals.

From Proposition 9.19(e) we have

(iii) $$\mathrm{Spec}(R) = V(\mathfrak{i}_1) \cup V(\mathfrak{i}_2) = V(\mathfrak{i}_1 \mathfrak{i}_2),$$

and we conclude from Corollary 9.24 that

(iv) $$\mathfrak{i}_1 \mathfrak{i}_2 \subset \sqrt{(0)}.$$

On the other hand, from Proposition 9.19(d) we have

$$\emptyset = V(\mathfrak{i}_1) \cap V(\mathfrak{i}_2) = V(\mathfrak{i}_1 + \mathfrak{i}_2),$$

and we conclude from Corollary 9.14 that

(v) $$\mathfrak{i}_1 + \mathfrak{i}_2 = R.$$

By (v) we can choose elements $e_1 \in \mathfrak{i}_1$ and $e_2 \in \mathfrak{i}_2$ such that

(vi) $$e_1 + e_2 = 1,$$

and by (iv) we can choose a positive integer n such that

(vii) $$e_1^n e_2^n = 0.$$

From Corollary 9.20 and the observation $(e_j)^n = (e_j^n)$ we have

$$V((e_j)) = V((e_j)^n) = V((e_j^n)), \qquad j = 1, 2,$$

it follows from (iii), (vi) and (9.17) that

$$V((e_1^n) + (e_2^n)) = V((e_1^n)) \cap V((e_2^n)) = V((e_1)) \cap V((e_2)) = V((e_1) + (e_2)) = V(R) = \emptyset,$$

and from Corollary 9.14 we conclude that

(viii) $$(e_1^n) + (e_2^n) = R.$$

We claim that

(ix) $$(e_1^n) \cap (e_2^n) = (0).$$

To verify this first use (viii) to choose elements $g, h \in R$ such that

(x) $$1 = ge_1^n + he_1^n.$$

If $r \in (e_1^n) \cap (e_2^n)$ there are elements $s, t \in R$ such that $se_1^n = r = te_2^n$, and from (x) we then have

$$r = gre_1^n + hre_2^n = gse_1^n e_2^n + hte_1^n e_2^n = 0.$$

Equality (ix) is thereby established.

From (viii), (ix) and Proposition 16.2 (applied to the ideals (e_1^n) and (e_2^n)) we see that R admits an idempotent distinct from 0 and 1, and we have achieved a contradiction to (b).

(b) $\Leftrightarrow$ (c) $\Leftrightarrow$ (d) : By Proposition 16.1.

q.e.d.

17. Trés Dense Subspaces

Throughout this section $X = (X, \tau)$ *denotes a non-empty topological space.*

Let $Y \subset X$ be a subset and let τ_Y be the induced topology on Y. By the definition of τ_Y there is a surjective mapping

$$U \subset \tau \mapsto \hat{U} := U \cap Y \in \tau_Y. \tag{17.1}$$

One says that Y is[103] *trés dense* in X if this mapping is a bijection. Equivalently:

$$U, W \in \tau \qquad \Rightarrow \qquad \hat{U} = \hat{W} \ \Leftrightarrow \ U = W. \tag{17.2}$$

Since $U = W \Rightarrow \hat{U} = \hat{W}$ always holds, to establish trés density all one needs to prove is that

$$U, W \in \tau \qquad \Rightarrow \qquad \hat{U} = \hat{W} \ \Rightarrow \ U = W. \tag{17.3}$$

Before offering specific examples it is useful to give the the following result.

Proposition 17.4 : *Suppose* X *admits a family* $\{x_\alpha\}$ *of generic points. Then* $Y := X \setminus \{x_\alpha\}$*, with the induced topology, is trés dense in* X*.*

Proof : We claim that any $x \in \{x_\alpha\}$ is contained in every non-empty open subset $U \subset X$: otherwise U^c, for at least one $U \in \tau$, would be a proper closed subset of X containing x, thereby contradicting the definition $\mathrm{cl}\{x\}) = X$ of a generic point. For any $U, W \in \tau$ we conclude that

$$\begin{aligned}
\hat{U} = \hat{W} \ &\Leftrightarrow \ U \cap Y = W \cap Y \\
&\Leftrightarrow \ (U \cap Y) \cup \{x_\alpha\} = (W \cap Y) \cup \{x_\alpha\} \\
&\Leftrightarrow \ (U \cap Y) \cup (U \cap \{x_\alpha\}) = \cup (W \cap Y) \cup (W \cap \{x_\alpha\}) \\
&\Leftrightarrow \ (U \cap (Y \cup \{x_\alpha\})) = (W \cap (Y \cup \{x_\alpha\})) \\
&\Leftrightarrow \ U \cap X = W \cap X \\
&\Leftrightarrow \ U = W.
\end{aligned}$$

q.e.d.

[103] The English translation of trés dense is "very dense," as in "This author of these notes is very dense." Somehow I find the French name a bit more elegant.

For additional characterizations of trés dense subsets see [A-M, Chapter 5, Exercise 26, pp. 71-2].

Examples 17.5 :

(a) *When* R *is a* PID *the subspace* $\mathrm{maxSpec}(R)$ *is trés dense in* $\mathrm{Spec}(R)$. In a PID the maximal ideals are the same as the non-zero prime ideals[104], and the two sets therefore differ only by the single point $(0) \in \mathrm{Spec}(R) \setminus \mathrm{maxSpec}(R)$. Since (0) is a generic point of $\mathrm{Spec}(R)$ (see Example 14.3(d)), the result is then immediate from Proposition 17.4. (Alternatively, use Proposition 17.6(c).)

(b) *When the usual topology is assumed* $\mathbb{Q}$ *is not trés dense in* $\mathbb{R}$. For example, the open sets $U_{\sqrt{2}} := \mathbb{R} \setminus \{\sqrt{2}\}$ and $U_\pi := \mathbb{R} \setminus \{\pi\}$ have the same intersection (namely $\mathbb{Q}$) with $\mathbb{Q}$.

(c) *Let* X *be a two-point space* $\{a, b\}$ *with the indiscrete topology*[105] *and let* $Y := \{a\}$. *Then* Y *is trés dense in* X.

(d) *Let* $X := \{\, r \in \mathbb{R} \,:\, 0 \le r \le 1 \,\}$ *with the "ray topology," i.e., only sets of the form* $(r, \infty) \cap X$, *with* $r \in \mathbb{R}$ *arbitrary, are open. Let* $Y := X \setminus \{\frac{1}{2}\}$. *Then* Y *is trés dense in* X.

Proposition 17.6 : *For any ring* R *the following conditions are equivalent.*

(a) $\mathrm{maxSpec}(R)$ *is trés dense in* $\mathrm{Spec}(R)$*;*

(b) *for any* $r, s \in R$ *the condition* $D(r) \cap \mathrm{maxSpec}(R) = D(s) \cap \mathrm{maxSpec}(R)$ *implies* $D(r) = D(s)$*;*

(c) *any prime ideal* $\mathfrak{p} \subset R$ *is the intersection of all the maximal ideals containing* $\mathfrak{p}$*; and*

(d) *for any prime ideal* $\mathfrak{p} \subset R$ *and any ring element* $r \notin \mathfrak{p}$ *there is a maximal ideal containing* $\mathfrak{p}$ *which does not contain* r.

Any ring satisfying any of these equivalent conditions is called a *Jacobson ring*, with (c) being the standard definition.

Proof :

(a) $\Leftrightarrow$ (b) : Since the collection $\{D(r)\}_{r \in R}$ forms a basis for the Zariski topology, this equivalence is immediate from the definition of a trés dense subset.

[104] We encountered this fact in I. of §13, where a reference is given.

[105] I.e., the only open sets are X and $\emptyset$.

For the remainder of the proof the symbols $\mathfrak{p}$ and $\mathfrak{m}$ will be used to denote prime and maximal ideals of R respectively, and $\mathrm{maxSpec}(R)$ will be written as $\mathcal{M}$. The assertion of (c) will be expressed in the abbreviated form

(i) $$\mathfrak{p} = \cap_{\mathfrak{p}\subset\mathfrak{m}}\mathfrak{m}.$$

(a) $\Rightarrow$ (c) : If (c) fails there must be a prime ideal $\mathfrak{p} \subset R$ which is properly contained in the ideal $\mathfrak{q} := \cap_{\mathfrak{p}\subset\mathfrak{m}}\mathfrak{m}$. One checks easily that the collection of prime ideals within a ring is closed under arbitrary intersections, and $\mathfrak{q}$ is therefore prime. Now observe from $\mathfrak{p} \subset \mathfrak{q}$ and Proposition 9.19(b) and (c) that $V(\mathfrak{q}) \subset V(\mathfrak{p})$ is an inclusion of closed sets, and, since $\mathfrak{p} \in V(\mathfrak{p}) \setminus V(\mathfrak{q})$, this inclusion must proper. However, from the definition of $\mathfrak{q}$ we see that every maximal ideal containing $\mathfrak{p}$ also contains $\mathfrak{q}$, whence

$$V(\mathfrak{p}) \cap \mathcal{M} = V(\mathfrak{q}) \cap \mathcal{M}.$$

It follows that the distinct open sets $V(\mathfrak{p})^c$ and $V(\mathfrak{q})^c$ have the same intersection with $\mathcal{M}$, and this contradicts (a).

(c) $\Rightarrow$ (b) : First note that

(ii) $$\mathfrak{p} = \cap_{\mathfrak{p}\subset\mathfrak{m}}\mathfrak{m} \;\Leftrightarrow\; \forall r \in R,\;\; \mathfrak{p} \in D(r) \;\Rightarrow\; \exists \mathfrak{m} \supset \mathfrak{p} \;\text{ s.t. }\; \mathfrak{m} \in D(r) \cap \mathcal{M}.$$

Indeed, we have

$$\begin{aligned}
\mathfrak{p} = \cap_{\mathfrak{p}\subset\mathfrak{m}}\mathfrak{m} &\;\Leftrightarrow\; \mathfrak{p}^c = \cup_{\mathfrak{p}\subset\mathfrak{m}}\mathfrak{m}^c \\
&\;\Leftrightarrow\; \forall r \in \mathfrak{p}^c \;\; \exists \mathfrak{m} \supset \mathfrak{p} \;\text{ s.t. }\; r \in \mathfrak{m}^c \\
&\;\Leftrightarrow\; \forall r \notin \mathfrak{p} \;\; \exists \mathfrak{m} \supset \mathfrak{p} \;\text{ s.t. }\; r \notin \mathfrak{m} \\
&\;\Leftrightarrow\; \forall r \in R,\;\; \mathfrak{p} \in D(r) \;\Rightarrow\; \exists \mathfrak{m} \supset \mathfrak{p} \;\text{ s.t. }\; \mathfrak{m} \in D(r) \cap \mathcal{M}.
\end{aligned}$$

Now suppose that $r, s \in R$ satisfy $D(r) \cap \mathcal{M} = D(s) \cap \mathcal{M}$ and $D(r) \neq D(s)$. Then w.l.o.g. there is a prime ideal

(iii) $$\mathfrak{p} \in D(r) \setminus D(s),$$

and from $\mathfrak{p} \in D(r)$ and (ii) we see that there must be a maximal ideal $\mathfrak{m} \in D(r) \cap \mathcal{M} = D(s) \cap \mathcal{M}$ containing $\mathfrak{p}$. However, this last equality gives $\mathfrak{m} \in D(s)$, hence $s \notin \mathfrak{m}$, whereupon the exclusion in (iii) then results in the contradiction $s \in \mathfrak{p} \subset \mathfrak{m}$.

(c) $\Leftrightarrow$ (d) : By de Morgan's Law equality (i) holds if and only if

$$\mathfrak{p}^c = \cup_{\mathfrak{p}\subset\mathfrak{m}}\mathfrak{m}^c,$$

and

$$\begin{aligned}\mathfrak{p}^c = \cup_{\mathfrak{p}\subset\mathfrak{m}}\mathfrak{m}^c \;\; &\Leftrightarrow \;\; \forall r \in R, \;\; r \notin \mathfrak{p} \Leftrightarrow r \in \mathfrak{m}^c \;\; \text{for some} \;\; \mathfrak{m} \supset \mathfrak{p} \\ &\Leftrightarrow \;\; \forall r \in R, \;\; r \notin \mathfrak{p} \Leftrightarrow r \notin \mathfrak{m} \;\; \text{for some} \;\; \mathfrak{m} \supset \mathfrak{p}.\end{aligned}$$

q.e.d.

Proposition 17.7 : *A subspace $Y \subset X$ is trés dense if and only if the mapping $C \mapsto C \cap Y$ between closed sets of X and closed sets of Y in the induced topology is a bijection.*

Proof : For any closed set $C \subset X$ one has

$$Y = (C \cap Y) \cup (C^c \cap Y).$$

If $\hat{C} \subset X$ is also closed it follows from the trés dense hypothesis that

$$\begin{aligned}C \cap Y = \hat{C} \cap Y \;\; &\Leftrightarrow \;\; C^c \cap Y = \hat{C}^c \cap Y \\ &\Leftrightarrow \;\; C^c = \hat{C}^c \\ &\Leftrightarrow \;\; C = \hat{C}.\end{aligned}$$

q.e.d.

When Y is trés dense in X many topological properties possessed by either of τ and τ_Y is also possessed by the other. Specifically, we have the following result.

Theorem 17.8 : *When Y is trés dense in X the following assertions hold.*

(a) *Y is dense in X.*

(b) *An open set $U \subset X$ is a proper subset of X if and only if $\hat{U}$ is a proper subset of Y.*

(c) *A closed subset $C \subset X$ is a proper subset of X if and only if $C \cap Y$ is a proper subset of Y.*

(d) *Y is irreducible if and only if X is irreducible.*

(e) *Y is connected if and only if X is connected.*

(f) *A subset $Z \subset Y$ is compact w.r.t. τ if and only if Z is compact w.r.t. τ_Y.*

Proof :

(a) Since the mapping of (17.1) is a bijection we have $\hat{U} = \emptyset$ if and only if $U = \emptyset$. It follows that every non-empty element of τ has non-empty intersection with Y, hence that every point of X is a limit point of Y.

(b) $\hat{U} \subset Y$ is a proper inclusion if and only if $\hat{U} \neq Y = \hat{X}$ if and only if $U \neq X$ if and only if $U \subset X$ is a proper inclusion.

(c) Immediate from (b).

(d) In view of (c) the space X is the union of two proper closed sets C and D if and only if Y is the union of the two proper relatively closed sets $C \cap Y$ and $D \cap Y$.

(e) One can take the definition of "connected" to be: there is no proper open and closed subset[106]. The result is then immediate from (b) and (c).

(f) From the hypothesis $Z \subset Y$ one sees that a family $\{U_\alpha\} \subset \tau$ is an open cover of Z if and only if $\{\hat{U}_\alpha\} \subset \tau_Y$ is an open cover of Z in the relative topology.

q.e.d.

There are, however, topological properties not shared by a space and a trés dense subspace. Recall that a topological space is a T_1-*space* if all points are closed points. In particular, any Hausdorff space is T_1.

Proposition 17.9 : *When $Y \subset X$ is trés dense no point of $X \setminus Y$ is closed. In particular, when the inclusion $Y \subset X$ is proper and Y is a T_1 or Hausdorff space X cannot have the same property.*

Proof : If $x \in X$ were a closed point the open set $X \setminus \{x\}$ would have the same intersection with Y as does X, and the bijectivity assumption on the mapping $U \in \tau \mapsto U \cap Y \in \tau_Y$ would be contradicted. **q.e.d.**

It is reasonable to ask if trés density behaves well w.r.t. mappings. Specifically, suppose Z is a topological space, $Y \subset X$ and $W \subset Z$ are trés dense subspaces, and $g : Y \to W$ is a continuous function. Does g determine a unique continuous function $f : X \to Z$ such that the diagram

$$\begin{array}{ccc} X & \xrightarrow{f} & Z \\ {\scriptstyle \text{inc}}\uparrow & & \uparrow{\scriptstyle \text{inc}} \\ Y & \xrightarrow{g} & W \end{array} \tag{17.10}$$

[106] See, e.g., [Mun, Chapter 3, §3.1, p. 147].

commutes? The answer is no. For example, let $X = \{a, b\}$ and $Y = \{a\}$ be as in Example 17.5(c), set $Z := X$ and $W := Y$, and let $g : Y \to W$ be the identity mapping. Then the diagram commutes if we take f to be the (continuous) identity mapping, and it also commutes if we take f to be the (continuous) constant mapping $f : x \mapsto a$. The example also shows that when g is injective and/or surjective a lifting f (as in (17.10)) need not share that property.

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 11.6); 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. Specifically, we will see that if $B \supset A$ is an extension of fields, with B algebraically closed, the mapping $\mathfrak{i} \mapsto \mathcal{V}(\mathfrak{i})$ of Corollary 4.6, from radical ideals of $A[x]$ to classical (A, B)-affine algebraic subsets of B^n, is a bijection (see Corollary 19.3).

18. The Weak Nullstellensatz

In this section we are interested in the following question: given a ring extension $B \supset A$, with A non-trivial, a positive integer n, and an ideal $\mathfrak{i}$ within the polynomial algebra $A[x] = A[x_1, \ldots, x_n]$, does there exist at least one point $c = (c_1, c_2, \ldots, c_n) \in B^n$ such that $p(c) = 0$ for all $p \in \mathfrak{i}$?

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

If the inclusion $\mathfrak{i} \subset A[x]$ is assumed proper the answer can still be no, even in the case $n = 1$: take $A = B = \mathbb{Z}$ and let $\mathfrak{i} = (x^2 + 1)$. On the other hand, when $n = 1$ and $A =: K$ and $B =: L$ are fields, with L algebraically closed, the answer is yes. Indeed, the polynomial ring $K[x]$ is then a PID[107], and $\mathfrak{i}$ therefore has the form $(q) = qK[x]$ for some polynomial $q \in K[x] \subset L[x]$. Since L is algebraically closed q admits a root $c \in L$, and since every element $p \in \mathfrak{i}$ is a multiple of q it follows that $p(c) = 0$ for every $p \in \mathfrak{i}$. 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 18.1 : *Suppose L is an infinite field and $0 \neq p \in L[x]$. Then there is a point $b = (b_1, \ldots, b_n) \in L^n$ such that $p(b) \neq 0$.*

The hypothesis on L applies when the field is algebraically closed[108].

[107] See, e.g., [L, Chapter IV, §1, Theorem 1.2, p. 174].

[108] This follows, e.g., from [H, Chapter V, §5, Corollary 5.9, p. 281] or [L, Chapter V, §5, Theorem 5.5, p. 247].

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

Assume the result for $n \geq 1$, suppose $p \in L[x_1, \ldots, x_{n+1}]$, 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 $b_1, b_2, \ldots, b_n \in L$ such that $p_j(b_1, b_2, \ldots, b_n) \neq 0$. The polynomial $p(b_1, b_2, \ldots, b_n, x_{n+1}) \in L[x_{n+1}]$ is therefore non-zero, and for the reasons given in the previous paragraph we can choose $b_{n+1} \in L$ such that $p(b_1, b_2, \ldots, b_{n+1}) \neq 0$. **q.e.d.**

We also need a preliminary lemma.

Lemma 18.2 : *Suppose $L \supset K$ is an extension of fields and $\{x_1, x_2, \ldots, x_n\}$ is a collection of elements algebraically independent over L. Suppose $\mathfrak{i}$ is a proper ideal of the polynomial algebra $K[x] := K[x_1, x_2, \ldots, x_n]$. Then the ideal $\mathfrak{i}_L \subset L[x] = L[x_1, x_2, \ldots, x_n]$ generated by $\mathfrak{i}$ is also proper.*

One says that the ideal $\mathfrak{i}_L$ *lies over* $\mathfrak{i}$.

Proof : Extend the singleton set $\{1\} \subset K \subset L$ to a basis $\{1\} \cup \{\ell_\alpha\} \subset L$ of the K-vector space L. Next, write the basis $\{ x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n} : i_j \in \{0, 1, 2, \ldots\} \}$ of the K-vector space $K[x]$ as $\{x^I\}$. Then $\{x^I\} \cup \{\ell_\alpha x^I\}$ is a basis of the K-vector space $L[x]$, by means of which any $q \in L[x]$ can be expressed in the form $q = q^{(K)} + q^{(R)}$, where $q^{(K)}$ is in the span of $\{x^I\}$, i.e., $q^{(K)} \in K[x]$, and $q^{(R)}$ is in the span of $\{\ell_\alpha x^I\}$.

If $\mathfrak{i}_L = L[x]$ we can write $1 = \sum_j q_j p_j$ where $q_j \in L[x]$, $p_j \in \mathfrak{i} \subset K[x]$, and the sum is finite. By comparing coefficients relative to the basis $\{x^I\} \cup \{\ell_\alpha x^I\}$ we then see that

$$1 = 1^{(K)} = \textstyle\sum_j q_j^{(K)} p_j + \sum_j q_j^{(R)} p_j = \sum_j q_j^{(K)} p_j + 0 = \sum_j q_j^{(K)} p_j \in \mathfrak{i},$$

hence $\mathfrak{i} = K[x]$, and we have thereby achieved a contradiction. **q.e.d.**

Theorem 18.3 (The Weak Nullstellensatz) : *Suppose $L \supset K$ is an extension of fields, L is algebraically closed, $\{x_1, x_2, \ldots, x_n\}$ is any collection of indeterminates*[109] *over L, and $\mathfrak{i}$ is a proper ideal of the polynomial algebra $K[x_1, \ldots, x_n]$. Then the classical (K, L)-affine algebraic set $\mathcal{V}(\mathfrak{i})$ is not empty, i.e., there must be a point $b = (b_1, b_2, \ldots, b_n) \in L^n$ such that $p(b) = 0$ for all $p \in \mathfrak{i}$.*

[109] I.e., algebraically independent elements over L.

Proof : The proof is divided into two parts: the first[110] deals with the case $K = L$; the second deals with the general case. Interestingly enough, most of the work is involved in the first part.

Part I ($K = L$): Assuming this more restrictive hypothesis we argue by induction on n, first noting that the case $n = 1$ was already established[111]. We therefore assume $n \geq 1$, and that the theorem holds for proper ideals of $L[x_1, x_2, \ldots, x_n]$. Let $\mathfrak{i}$ be a proper ideal of $L[x_1, x_2, \ldots, x_{n+1}]$.

For any n-tuple $\ell = (\ell_1, \ldots, \ell_n) \in L^n$ the assignment

$$x_j \mapsto \begin{cases} x_j + \ell_j x_{n+1} & \text{if } 1 \leq j \leq n \\ x_{n+1} & \text{if } j = n+1 \end{cases}$$

determines a unique L-algebra automorphism $\sigma_\ell : L[x] \to L[x]$, and the image $\sigma_\ell(\mathfrak{i}) \subset L[x]$ is again a proper ideal. If for $p \in L[x]$ we let $q := \sigma_\ell(p) = p(x_1 + \ell_1 x_{n+1}, x_2 + \ell_2 x_{n+1}, \ldots, x_n + \ell_n x_{n+1}, x_{n+1})$, then for any $b = (b_1, b_2, \ldots, b_{n+1}) \in L^{n+1}$ and $c := (b_1 + \ell_1 b_{n+1}, b_2 + \ell_2 b_{n+1}, \ldots, b_n + \ell_n b_{n+1}, b_{n+1}) \in L^{n+1}$ we have $q(b) = 0 \Leftrightarrow p(c) = 0$. Since b can be recovered from c via $b = (c_1 - \ell_1 c_{n+1}, c_2 - \ell_2 c_{n+1}, \ldots, c_n - \ell_n c_{n+1}, c_{n+1})$, we conclude that it suffices to prove the theorem with $\mathfrak{i}$ replaced by $\sigma_\ell(\mathfrak{i})$. The trick is to pick the n-tuple ℓ in a judicious way.

Select any non-constant polynomial $p \in \mathfrak{i} \subset L[x_1, x_2, \ldots, x_{n+1}]$ and let $d \geq 1$ denote the total degree[112] of p. We claim we can choose $\ell = (\ell_1, \ell_2, \ldots, \ell_n) \in L^n$ such that $\sigma_\ell(p)$ can be expressed in the form

$$\text{(i)} \qquad c x_{n+1}^d + \textstyle\sum_{j=0}^{d-1} q_j(x_1, x_2, \ldots, x_n) x_{n+1}^j, \qquad 0 \neq e \in L.$$

Indeed, for any monomial $s_m = s_m(x_1, x_2, \ldots, x_{n+1}) = t \prod_{j=1}^{n+1} x_j^{m_j} \in L[x_1, \ldots, x_{n+1}]$ ($t \in L$) of total degree m we see that

$$\begin{aligned} \sigma_\ell(s_m) &= t \left(\textstyle\prod_{j=1}^n (x_j + \ell_j x_{n+1})^{m_j} \right) x_{n+1}^{m_{n+1}} \\ &= t \left(\textstyle\prod_{j=1}^n (\ell_j x_{n+1} + x_j)^{m_j} \right) x_{n+1}^{m_{n+1}} \\ &= t \left(\textstyle\prod_{j=1}^n \left(\ell_j^{m_j} x_{n+1}^{m_j} + \text{monomials of total degree less than } \sum_{j=1}^n m_j \right) \right) x_{n+1}^{m_{n+1}} \\ &= t \left(\textstyle\prod_{j=1}^n \ell_j^{m_j} x_{n+1}^{m_j} \right) x_{n+1}^{m_{n+1}} + \text{monomials of total degree less than } m = \sum_{j=1}^{n+1} m_j \\ &= s_m(\ell_1, \ldots, \ell_n, x_{n+1}) + \text{monomials of total degree less than } m \end{aligned}$$

[110] The proof of the first part is from [Arrondo].

[111] Two paragraphs before the statement of Proposition 18.1.

[112] The *total degree* of a non-zero monomial $\ell x_1^{d_1} x_2^{d_2} \cdots x_{n+1}^{d_{n+1}} \in L[x] = L[x_1, x_2, \ldots, x_{n+1}]$ is $\sum_i d_i$; the *total degree* of a non-zero polynomial in $L[x]$ is the maximum of the total degrees of the associated monomials.

It follows immediately that the homogeneous terms of $\sigma_\ell(p)$ of total degree d are given by the polynomial $p_d(\ell_1, \ldots, \ell_n, x_{n+1}) \in L[x_{n+1}]$. By Proposition 18.1 we can choose $(\ell_1, \ell_2, \ldots, \ell_{n+1}) \in L^{n+1}$ such that $p_d(\ell_1, \ell_2, \ldots, \ell_n, \ell_{n+1}) \neq 0$, and our claim is then established by taking $\ell := (\ell_1, \ell_2, \ldots, \ell_n) \in L^n$.

For this particular choice for $\ell \in L^n$ it follows from (i) that the ideal $\sigma_\ell(\mathfrak{i})$ contains a non-zero polynomial $g(x)$ which is "monic in x_{n+1}," i.e., of the form

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

Let $\mathfrak{i}' \subset L[x_1, x_2, \ldots, x_n]$ denote the collection of polynomials $p \in \sigma_\ell(\mathfrak{i})$ which do not involve the indeterminate x_{n+1}. This collection is easily seen to be an ideal of $L[x_1, x_2, \ldots, x_n]$, and since $1 \notin \sigma_\ell(\mathfrak{i})$ it must be proper. By the induction hypothesis there is a point $\hat{b} = (b_1, b_2, \ldots, b_n) \in L^n$, which we fix for the remainder of the proof, such that

(iii) $$p(\hat{b}) = p(b_1, b_1, \ldots, b_n) = 0 \qquad \text{for all } p \in \mathfrak{i}'.$$

Now introduce

(iv) $$\mathfrak{j} := \{\, p(b_1, b_2, \ldots, b_n, x_{n+1}) \,:\, p \in \sigma_\ell(\mathfrak{i}) \,\} \subset L[x_{n+1}|,$$

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

(v) $$p(b_1, b_2, \ldots, b_n, x_{n+1}) = 1.$$

Express p in the form

(vi) $$p = \textstyle\sum_{j=0}^{e} p_j x_{n+1}^j = \sum_{j=0}^{e} p_j(x_1, x_2, \ldots, x_n) x_{n+1}^j,$$

and note from (v) that

(vii) $$p_0(b_1, b_2, \ldots, b_n) = 1, \qquad p_j(b_1, b_2, \ldots, b_n) = 0, \qquad j = 1, \ldots, e.$$

Consider the polynomial $r \in L[x_1, x_2, \ldots, x_n]$ defined by[113]

$$\text{(viii)} \qquad r := \det \left(\begin{array}{cccccccc} p_0 & p_1 & \cdots & p_e & 0 & 0 & \cdots & 0 \\ 0 & p_0 & \cdots & p_{e-1} & p_e & 0 & \cdots & 0 \\ & & \ddots & & & & & \\ 0 & \cdots & 0 & p_0 & p_1 & \cdots & p_{e-1} & p_e \\ g_0 & g_1 & \cdots & g_{d-1} & 1 & 0 & \cdots & 0 \\ 0 & g_0 & \cdots & g_{d-2} & g_{d-1} & 1 & 0 & \vdots \\ & & \ddots & & & & \ddots & 0 \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{d-1} & 1 \end{array} \right) \begin{array}{l} \left. \begin{array}{l} \\ \\ \\ \\ \end{array} \right\} \text{d rows} \\ \left. \begin{array}{l} \\ \\ \\ \\ \end{array} \right\} \text{e rows} \end{array}$$

We compute the determinant by means of elementary column operations while viewing r as a polynomial in $L[x_1, x_2, \ldots, x_{n+1}]$: 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

$$\left(\begin{array}{c} p \\ x_{n+1}p \\ \vdots \\ x_{n+1}^{d+e-1}p \\ g \\ x_{n+1}g \\ \vdots \\ x_{n+1}^{d+e-1}g \end{array} \right),$$

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 $p, g \in \sigma_\ell(\mathfrak{i})$ it follows that the same holds for r, i.e., that

$$\text{(ix)} \qquad r \in \mathfrak{i}'.$$

However, one sees from (vii) that when the polynomials appearing in (viii) are evaluated at $\hat{b} = (b_1, b_2, \ldots, b_n)$ the matrix reduces to a lower triangular matrix with entry 1 in each diagonal position. This gives $r(\hat{b}) = r(b_1, b_2, \ldots, b_n) = 1$, which by

[113] This polynomial is commonly called the "resultant" of p and g.

virtue of (ix) is a contradiction to (iii). The claim, i.e., that the ideal $\mathfrak{j} \subset L[x_{n+1}]$ is proper, is thereby established.

Since $L[x_{n+1}]$ is a PID we can write $\mathfrak{j} = (s)$ for some $s \in L[x_{n+1}]$. If $s \neq 0$ pick a zero $b_{n+1} \in L$ of s, and we then have $p(b_1, b_2, \ldots, b_n, b_{n+1}) = 0$ for all $p \in \sigma_\ell(\mathfrak{i})$. If $s = 0$ we see from (iv) that for any choice of $b_{n+1} \in L$ we have $p(b_1, b_2, \ldots, b_n, b_{n+1}) = 0$ for all $p \in \sigma_\ell(\mathfrak{i})$, and the proof of part one is complete.

Part II ($K \subset L$) : For the general case let $\mathfrak{i}_L$ be the ideal of $L[x]$ generated by $\mathfrak{i}$ and recall from Lemma 18.2 that the inclusion $\mathfrak{i}_L \subset L[x]$ is proper. The work of Part I therefore applies, and we conclude that corresponding classical (L, L)-affine algebraic set $\mathcal{V}_L(\mathfrak{i}_L) \subset L^n$ is non-empty, hence contains a point b such that $p(b) = 0$ for all $p \in \mathfrak{i}_L$. Since $\mathfrak{i} \subset \mathfrak{i}_L$ it follows that $p(b) = 0$ for all $p \in \mathfrak{i}$, hence b is contained in the classical (K, L)-affine algebraic set $\mathcal{V}(\mathfrak{i})$, and $\mathcal{V}(\mathfrak{i})$ is therefore non-empty.

q.e.d.

In the following corollaries $L \supset K$ is an extension of fields with L algebraically closed.

Corollary 18.4 : *Suppose $\{p_1, p_2, \ldots, p_m\} \subset K[x]$ is a non-empty collection of polynomials having no common zero in L^n. 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 $K[x]$.*

Proof : By the Weak Nullstellensatz (Theorem 18.3) the ideal $(p_1, \ldots, p_m) \subset K[x]$ cannot be proper. **q.e.d.**

Corollary 18.5 : *All maximal ideals of $L[x]$ have the form $(x - b_1, x - b_2, \ldots, x - b_n)$, where $b_j \in L$ for $j = 1, 2, \ldots, n$. By means of this association the maximal ideals of $L[x]$ are in one-to-one correspondence with the points $(b_1, b_2, \ldots, b_n) \in L^n$, and all these points are closed in the (L, L)-Zariski topology.*

Proof : First recall from Example 3.3(e) that the defining ideal $\mathfrak{i}(\{c\})$ of a point $c = (b_1, b_2, \ldots, b_n) \in L^n$ must have the form $(x_1 - b_1, x_2 - b_2, \ldots, x_n - b_n)$; then recall from Proposition 9.5 that

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

and that the defining ideal of any point of L^n is proper.

We claim that any maximal ideal $\mathfrak{m} \subset L[x]$ has the form $\mathfrak{i}(\{e\})$ for some point $e \in L^n$. Indeed, by Theorem 18.3 there is a zero $e = (d_1, d_2, \ldots, d_n) \in L^n$ of $\mathfrak{m}$,

and since any polynomial in $\mathfrak{m}$ vanishes on e it follows that $\mathfrak{m} \subset \mathfrak{i}(\{e\})$. Since $\mathfrak{m}$ is maximal and $\mathfrak{i}(\{e\})$ is proper this forces $\mathfrak{m} = \mathfrak{i}(\{e\}) = (x_1 - d_1, x_2 - d_2, \ldots, x_n - d_n)$.

We claim that any ideal of the form $\mathfrak{i}(\{c\}) = (x_1 - b_1, x_2 - b_2, \ldots, x_n - b_n)$ is maximal. Otherwise we see from the proper inclusion $\mathfrak{i}(\{c\}) \subset L[x]$ and Corollary 9.11 that there must be a maximal ideal $\mathfrak{m}$ containing $\mathfrak{i}(\{c\})$, whence from the previous paragraph that $\mathfrak{m} = \mathfrak{i}(\{d\})$ for some point $d \in L^n$. However, from $\mathfrak{i}(\{c\}) \subset \mathfrak{m}$ and (i) we have $\{d\} = \mathcal{V}(\mathfrak{m}) \subset \mathcal{V}(\{c\}) = \{c\}$, hence $c = d$, and $\mathfrak{i}(\{c\}) = \mathfrak{i}(\{d\}) = \mathfrak{m}$ is therefore maximal.

This proves all but the final assertion, and that is a special case of Proposition 12.2. **q.e.d.**

The Weak Nullstellensatz has some further important consequences which at first glance appear to be of a purely algebraic nature.

Corollary 18.6 : *Suppose A is a subdomain of L and $B \supset A$ is a finitely generated A-algebra. Then there is an A-algebra homomorphism $r : B \to L$.*

If $B \subset L$ we could take r to be inclusion. The interesting case occurs when $B \not\subset L$.

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 $\mathfrak{i} := \ker f$ and let $\mathfrak{j}$ be the ideal of $L[x]$ generated by $\mathfrak{i}$. By Lemma 18.2 the ideal $\mathfrak{j} \subset L[x]$ is proper, and by Theorem 18.3 we can therefore choose an element $b = (b_1, b_2, \ldots, b_n) \in L^n$ such that

$$\text{(i)} \qquad p(b) = 0 \qquad \text{for all} \qquad p \in \mathfrak{j}.$$

Let $q : A[x] \to L$ be the ring homomorphism characterized by $x_\ell \mapsto b_\ell$, $\ell = 1, \ldots, n$. By (i) we have $\mathfrak{i} \subset \ker q$, and since $B \simeq L[x]/\mathfrak{i}$ the existence of r is now a consequence of the First Isomorphism Theorem of commutative ring theory[114]. **q.e.d.**

Corollary 18.7 : *Suppose $M \supset K$ is a field extension such that M is finitely generated as a K-algebra*[115]*. Then the extension $M \supset K$ is finite algebraic.*

This result also goes by the name "Hilbert's Nullstellensatz."

Proof : By Corollary 18.6 there is a K-algebra homomorphism $r : M \to L$, and since M is a field this must be an embedding. **q.e.d.**

[114] More precisely, of the straightforward analogue of that theorem for algebras. See Footnote 42.

[115] 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.

Corollary 18.8 : *Suppose* $B \supset A$ *is an extension of integral domains with* B *a finitely generated* A*-algebra. Then any embedding* $f : A \to L$ *of* A *into the algebraically closed field* L *extends to an* A*-algebra homomorphism* $g : B \to L$.

We derive this as a consequence of the weak Nullstellensatz, but it is in fact equivalent[116].

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

$$\beta : b \mapsto \begin{cases} f(b) & \text{if} \quad b \in A, \\ \alpha(b) & \text{if} \quad b \in B \backslash A. \end{cases}$$

Using β we can transfer the ring extension structure $B \supset A$ to $\hat{B} \supset f(A)$, and β then becomes a A-algebra isomorphism[117]. By Corollary 18.6 there is an A-algebra homomorphism $r : \hat{B} \to L$, and the composition $r \circ \beta : B \to L$ is then an A-algebra homomorphism extending f. **q.e.d**.

[116]For a proof of the weak Nullstellensatz assuming Corollary 18.8 see, e.g., [L, Chapter IX, §1, pp. 379-80].

[117]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].

19. The Nullstellensatz

Theorem 19.1 (Hilbert's Nullstellensatz) : *Suppose* $L \supset K$ *is an extension of fields, with* L *algebraically closed,* $\mathfrak{i} \subset K[x] = K[x_1, \ldots, x_n]$ *is an ideal, and* $p \in K[x]$ *vanishes at all zeros of* $\mathfrak{i}$ *in* L^n*. Then* $p \in \sqrt{\mathfrak{i}}$*.*

The conclusion can also be stated: $p \in \mathfrak{i}(\mathcal{V}(\mathfrak{i})) \Rightarrow p \in \sqrt{\mathfrak{i}}$, where $\mathcal{V} \subset L^n$.

Proof : If $p = 0$ there is nothing to prove, so assume otherwise. By the Hilbert Basis Theorem (Theorem 11.6) the ideal $\mathfrak{i}$ is finitely generated, say by $p_1, \ldots, p_m \in K[x]$.

The trick[118] 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 18.4 we conclude that there are elements $q_1, \ldots, q_{m+1} \in K[x, y]$ such that

$$q_1 p_1 + \cdots + q_m p_m + q_{m+1}(1 - yp) = 1.$$

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

$$h_1 p_1 + \cdots + h_m p_m = p^r,$$

and $p \in \sqrt{\mathfrak{i}}$ is thereby established. **q.e.d.**

In the following corollaries $L \supset K$ is an extension of fields with L algebraically closed, and the sets $\mathcal{V}(\mathfrak{j})$, where $\mathfrak{j} \subset K[x]$ is an ideal, are classical (K, L)-affine algebraic subsets of L^n.

Corollary 19.2 : *For any ideal* $\mathfrak{i} \subset K[x]$ *one has*

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

In particular, for any radical ideal $\mathfrak{r} \subset K[x]$ *one has*

(ii) $$\mathfrak{r} = \mathfrak{i}(\mathcal{V}(\mathfrak{r})).$$

Proof : We have $\mathfrak{i}(\mathcal{V}(\mathfrak{i})) \subset \sqrt{\mathfrak{i}}$ by Theorem 19.1. For the reverse inclusion first recall from Proposition 9.3(b) that $\mathfrak{i} \subset \mathfrak{i}(\mathcal{V}(\mathfrak{i}))$. By Proposition 9.1 the last ideal is radical, and $\sqrt{\mathfrak{i}} \subset \sqrt{\mathfrak{i}(\mathcal{V}(\mathfrak{i}))} = \mathfrak{i}(\mathcal{V}(\mathfrak{i}))$ follows. **q.e.d.**

[118] Called the "Rabinowitsch trick."

Corollary 19.3 : *The mapping* $\mathfrak{r} \mapsto \mathcal{V}(\mathfrak{r})$ *from radical ideals of* $K[x] = K[x_1, \ldots, x_n]$ *to classical* (K, L)*-affine algebraic subsets of* L^n *is an inclusion reversing bijection with inverse* $\mathcal{V} \mapsto \mathfrak{i}(\mathcal{V})$.

Proof : By Proposition 4.7, Proposition 3.8, and (ii) of Corollary 19.2. **q.e.d.**

The remaining consequences of Theorem 19.1 are concerned with how much information is lost when the functor α of Theorem 3.15 is applied. As we will see, the answer, up to isomorphism, is: none.

Corollary 19.4 : *Any reduced affine* K*-algebra is* (up to isomorphism) *the coordinate ring of some classical* (K, L)*-affine algebraic set.*

Proof : By Proposition 3.9 a reduced affine K-algebra S must be isomorphic to a factor ring of the form $K[x_1, x_2, \ldots, x_n]/\mathfrak{r}$, and by Proposition 3.7 the ideal $\mathfrak{r}$ must be radical. From (ii) of Corollary 19.2 we then see that the coordinate ring $K_L[\mathcal{V}]$ of $\mathcal{V} := \mathcal{V}(\mathfrak{r}) \subset L^n$ satisfies

$$K_L[\mathcal{V}] := K[x_1, x_2, \ldots, x_n]/\mathfrak{i}(\mathcal{V}(\mathfrak{r})) = K[x_1, x_2, \ldots, x_n]/\mathfrak{r} \simeq S.$$

q.e.d.

Corollary 19.5 : *Suppose* $f : T \to S$ *is a morphism of reduced affine* K*-algebras. Then there are classical* (K, L)*-affine algebraic sets* $\mathcal{V}$ *and* $\mathcal{W}$ *with coordinate rings isomorphic to* S *and* T *respectively, and for any such choice of* $\mathcal{V}$ *and* $\mathcal{W}$ *there is a unique morphism* $g : \mathcal{V} \to \mathcal{W}$ *giving rise to a commutative diagram*

$$\text{(i)} \qquad \begin{array}{ccc} K_L[\mathcal{W}] & \xrightarrow{g^*} & K_L[\mathcal{V}] \\ \approx\uparrow & & \uparrow\approx \\ T & \xrightarrow{f} & S \end{array}$$

of reduced affine K*-algebra homomorphisms in which the vertical mappings are isomorphisms.*

The K-algebra homomorphism g^* in (i) is that defined from the morphism $g : \mathcal{V} \to \mathcal{W}$ as in (3.14).

Proof[119] **:** As in the proof of Corollary 19.4 write $S \simeq K[x_1, x_2, \ldots, x_n]/\mathfrak{r}$ and, analogously, write $T = K[y_1, y_2, \ldots, y_m]/\mathfrak{t}$, where $\mathfrak{r} \in K[x] := K[x_1, x_2, \ldots, x_n]$ and

[119] The proof is adapted from that of [C-L-OS$_2$, Chapter 5, §4, Proposition 8, pp. 243-4].

$\mathfrak{t} \in K[y] := K[y_1, y_2, \ldots, y_m]$ are radical ideals. As in that proof define $\mathcal{V} := \mathcal{V}(\mathfrak{r}) \subset L^n$ and, again analogously, define $\mathcal{W} := \mathcal{V}(\mathfrak{t}) \subset L^m$. The resulting identifications

$$K_L[\mathcal{V}] \simeq S \qquad \text{and} \qquad K_L[\mathcal{W}] \simeq T$$

(given by Corollary 19.4) correspond to the vertical mappings in (i). We use these identifications for the remainder of the proof so as to regard f as a homomorphism of $K_L[\mathcal{W}]$ into $K_L[\mathcal{V}]$. What we must prove is that f is induced by a polynomial mapping, i.e., we must produce a polynomial mapping $h = (h_1, h_2, \ldots, h_m) : L^n \to L^m$, with $h_j \in K[x]$ for $j = 1, 2, \ldots, m$, such that:

I. the restriction $g := h|_{\mathcal{V}}$ maps $\mathcal{V}$ into $\mathcal{W}$; and

II. $f = g^* : K_L[\mathcal{W}] \to K_L[\mathcal{V}]$ (as defined in (3.14)).

To this end denote cosets by brackets and write

$$f([y_j]) = [h_j(x_1, x_2, \ldots, x_n)], \qquad j = 1, 2, \ldots, m, \tag{ii}$$

where the h_j are polynomials[120] in $K[x]$. Define a polynomial mapping $h : L^n \to L^m$ by

$$h = (h_1(x), h_2(x), \ldots, h_m(x)), \qquad x = (x_1, x_2, \ldots, x_n).$$

Suppose $q \in K[y]$, say

$$q = \textstyle\sum_{(j_1, j_2, \ldots, j_m)} k_{(j_1, j_2, \ldots, j_m)} y_1^{j_1} y_2^{j_2} \cdots y_m^{j_m} =: \sum_J k_J y_1^{j_1} y_2^{j_2} \cdots y_m^{j_m},$$

wherein the sum is finite and all indices are non-negative. Then

$$\begin{aligned}
[q \circ h] &= [q(h_1, h_2, \ldots, h_m)] \\
&= q([h_1], [h_2], \ldots, [h_m]) \\
&= q(f([y_1]), f([y_2]), \ldots, f([y_m])) \\
&= \textstyle\sum_J k_J f([y_1]^{j_1}) f([y_2]^{j_2}) \cdots f([y_m]^{j_m}) \\
&= f\left(\textstyle\sum_J k_J [y_1]^{j_1} [y_2]^{j_2} \cdots [y_m]^{j_m}\right),
\end{aligned}$$

from which we see that

$$[q \circ h] = f([q]). \tag{iii}$$

[120] As can be seen from the discussion of Case (c) in the paragraph preceding Proposition 3.9.

I. Suppose $\ell \in \mathfrak{i}(\mathcal{W})$. Then $[\ell] = [0] \in K_L[\mathcal{W}]$, and since f is an algebra homomorphism it follows that $f([\ell]) = [0] \in K_L[\mathcal{V}]$. For any $c = (b_1, b_2, \ldots, b_n) \in \mathcal{V}$ we then have $[0] = f([\ell])(c) = [\ell \circ h](c) = \ell(h(c))$, hence $h(c) \in \mathcal{W}$, and I. follows.

II. The desired equality $f = g^*$ is immediate from (iii) and (3.14). Indeed, by means of (3.14) equality (iii) can be written $g^*([q]) = f([q])$ for all $q \in K[y]$.

To prove uniqueness suppose $\hat{g} : \mathcal{V} \to \mathcal{W}$ is a morphism such that diagram (i) commutes when g^* is replaced by $\hat{g}^*$. Further, suppose $p = (p_1, p_2, \ldots, p_m) : L^n \to L^m$ is a polynomial function with $p_j \in K[x]$ for $j = 1, 2, \ldots, m$ such that $p|_{\mathcal{V}} = \hat{g}$. Then from $\hat{g}^* = f$ we have the analogue

$$\text{(iv)} \qquad f([y_j]) = [p_j(x_1, x_2, \ldots, x_n)], \qquad j = 1, 2, \ldots, m,$$

of (ii) for p. However, it then follows from (iv) and (ii) that each of p_j and h_j have the same restriction to $\mathcal{V}$, and the same therefore holds for the restrictions $p|_{\mathcal{V}} = \hat{g}$ and $h|_{\mathcal{V}} = g$. This gives $\hat{g} = g$, and the proof is complete. **q.e.d.**

Theorem 19.6 : *Suppose $L \subset K$ is an extension of fields with L algebraically closed. Then two classical (K, L)-affine algebraic sets are isomorphic if and only if their coordinate rings are isomorphic as K-algebras.*

Less formally: knowing the coordinate ring is equivalent to knowing the algebraic set.

Proof : The forward implication is immediate from Theorem 3.15.

To establish the reverse implication suppose $\mathcal{V} \subset L^n$ and $\mathcal{W} \subset L^m$ have isomorphic (K, L)-coordinate rings. Specifically, suppose $f : K_L[\mathcal{W}] \to K_L[\mathcal{V}]$ is an isomorphism. Then by Corollary 19.5 there are unique morphisms $g : \mathcal{V} \to \mathcal{W}$ and $\hat{g} : \mathcal{W} \to \mathcal{V}$ which make the diagram

$$\begin{array}{ccccc} K_L[\mathcal{W}] & \xrightarrow{g^*} & K_L[\mathcal{V}] & \xrightarrow{\hat{g}^*} & K_L[\mathcal{W}] \\ =\uparrow & & =\uparrow & & \uparrow= \\ K_L[\mathcal{W}] & \xrightarrow{f} & K_L[\mathcal{V}] & \xrightarrow{f^{-1}} & K_L[\mathcal{W}] \end{array}$$

commute. Since the outer rectangle also commutes when[121] $\hat{g}^* \circ g^* = (g \circ \hat{g})^* : K_L[\mathcal{W}] \to K_L[\mathcal{W}]$ is replaced by $\mathrm{id}_{K_L[\mathcal{W}]}$ we conclude from the uniqueness assertion of Corollary 19.5 that $g \circ \hat{g} = \mathrm{id}_{\mathcal{W}}$ and, similarly, that $\hat{g} \circ g = \mathrm{id}_{\mathcal{V}}$. **q.e.d.**

[121] The equality $\hat{g}^* \circ g^* = (g \circ \hat{g})^*$ is a straightforward consequence of definition (3.14).

20. Localization

In this section R *is a (commutative) ring (with unity).*

Recall that a subset $S \subset R$ is[122] *multiplicative* if S is closed under multiplication and contains 1. An important example to keep in mind for this section is $S := R \setminus \mathfrak{p}$, where $\mathfrak{p} \in \mathrm{Spec}(R)$.

Any multiplicative subset $S \subset R$ defines a relation $\sim$ on $R \times S$ by $(r_1, s_1) \sim (r_2, s_2)$ if and only if there is an element $s \in S$ such that $sr_1s_2 = sr_2s_1$. This is an equivalence relation; the verification is straightforward. Write the equivalence class of an element $(r, s) \in R \times S$ as a/s and denote the set of equivalence classes by $S^{-1}R$. Addition and multiplication are well-defined on $S^{-1}R$ by

$$r_1/s_1 + r_2/s_2 := (r_1s_2 + r_2s_1)/s_1s_2$$

and

$$(r_1/s_1) \cdot (r_2/s_2) := r_1r_2/s_1s_2$$

respectively, and the collection is thereby given the structure of a (commutative) ring with unity $1/1$; this is the *ring of fractions of* R *by* S. The mapping $f : r \in R \mapsto r/1 \in S^{-1}R$ is easily seen to be a ring homomorphism, called the *canonical homomorphism*. Note that for any $s \in S$ the element $f(s) = s/1 \in S^{-1}R$ is invertible (with inverse $1/s$).

When R *is an integral domain and* $S \subset R\setminus\{0\}$ *one has* $(r_1, s_1) \sim (r_2, s_2)$ *if and only if* $r_1s_2 = r_2s_1$. Argue as follows: by definition one has $(r_1, s_1) \sim (r_2, s_2)$ if and only if there is an element $s \in S$ such that $sr_1s_2 = sr_2s_1$, which in turn holds if and only if $s(r_1s_2 - r_2s_1) = 0$. However, since R is an integral domain and $s \neq 0$ this is equivalent to $r_1s_2 = r_2s_1$.

When R *is an integral domain and* $S \subset R\setminus\{0\}$ *the canonical homomorphism* $f : R \to S^{-1}R$ *is an embedding.* Indeed, from the previous paragraph one has $f(r_1) = f(r_2) \Leftrightarrow r_1/1 = r_2/1 \Leftrightarrow r_1 \cdot 1 = r_2 \cdot 1 \Leftrightarrow r_1 = r_2$. In this context f is used to identify R with the subdomain $f(R) \subset S^{-1}R$. For example, one might replace the notation $f : R \to S^{-1}R$ with $R \subset S^{-1}R$ and refer to the ring $S^{-1}R$ as an extension of R. Moreover, when $r \in R$ is identified with $f(r) := r/1 \in S^{-1}R$ one would more likely write $r \in S^{-1}R$ than $r/1 \in S^{-1}R$.

In general one thinks of $f : R \to S^{-1}R$ as "pushing" R into a ring stocked with inverses for the elements of S, i.e., in which the elements of S become units. Of

[122]The definition first appears immediately before the statement of Proposition 9.8.

course when f fails to be an embedding one cannot take this intuitive viewpoint very seriously. In practice one tends to identify an element $s \in S$ with the element $f(s) = s/1 \in S^{-1}R$, even going so far as to write $s/1$ as s, and one often does this regardless of the injective nature of f. The reader is hereby on notice that we will follow this practice.

Examples:

(a) When $R = \mathbb{Z}$ and $S = \mathbb{Z}\backslash\{0\}$ the ring $S^{-1}\mathbb{Z}$ is the usual field $\mathbb{Q}$ of rational numbers and the canonical homomorphism is the standard embedding $n \in \mathbb{Z} \mapsto n/1 \in \mathbb{Q}$ used to regard $\mathbb{Z}$ as a subdomain of $\mathbb{Q}$.

(b) More generally, when R is an integral domain and $S := R\backslash\{0\}$ the ring $S^{-1}R$ is nothing but the quotient field of R, and the canonical homomorphism is again a ring embedding. For example, when R is the polynomial ring $\mathbb{Z}[x_1, \ldots, x_n]$ in n indeterminates the quotient field is $\mathbb{Q}(x_1, \ldots, x_n)$, i.e., it consists of all quotients of polynomials in $\mathbb{Q}[x_1, \ldots, x_n]$. The canonical homomorphism carries a polynomial $p \in \mathbb{Z}[x_1, \ldots, x_n]$ to the element $p/1 \in \mathbb{Q}(x_1, \ldots, x_n)$.

(c) When $\mathfrak{p} \subset R$ is a prime ideal and $S := R \setminus \mathfrak{p}$ the ring of fractions $S^{-1}R$ is written $R_{\mathfrak{p}}$ and is called the *localization* of R at $\mathfrak{p}$. When R is a PID such an ideal $\mathfrak{p}$ will have the form $(p) = pR$, where $p \in R$ is prime, and one then refers to $R_{(p)} = R_{\mathfrak{p}}$ as the *localization* of R *at the prime* p. This particular construction is very important in algebraic number theory: the canonical embedding $f : R \to R_{(p)}$ pushes R into a ring which emphasizes factorization by p. Indeed, within $R_{\mathfrak{p}}$ the element $p/1$ is, up to multiplication by units, the only prime.

(d) Fix any non-zero element $s \in R$ and let $S := \{s^n\}_{n=0}^{\infty}$. Then $S^{-1}R$, which is generally written as R_s or $R[s^{-1}]$, consists of all quotients r/s^n with $r \in R$ and $0 \leq n \in \mathbb{Z}$ arbitrary. Alternatively, $R[s^{-1}]$ can be viewed as the collection of "polynomials $r_0 + r_1 s^{-1} + \cdots + r_n s^{-n}$ in s^{-1} with coefficients in R;" any such expression is easily reduced to the quotient form r/s^n. One refers to the ring R_s as R *localized at* s. Within this ring the element $s \simeq s/1$, and all powers thereof, become units.

(e) When $S \subset R$ is multiplicative and contains 0 all pairs within $R \times S$ are equivalent and $S^{-1}R$ is the trivial ring 0 (i.e., the ring with only one element). In particular, in this context identities such as $0/1 = 1/0$ make sense.

By taking R to be a non-trivial ring we see that the canonical homomorphism $f : R \to S^{-1}R$ need not be an embedding. In particular, our intuitive description of f "pushing" R into another ring is a bit misleading, since we now see that collapsing can occur.

(f) In Example (c) take $R = \mathbb{Z}/6\mathbb{Z}$ and $s = [2]$, in which case $S = \{[1], [2], [4]\}$. The ring of fractions $S^{-1}R = (\mathbb{Z}/6\mathbb{Z})_{[2]}$ consists of the three elements[123] $[1]/[1]$, $[2]/[1]$ and $[3]/[1]$; it is a field isomorphic to $\mathbb{Z}/3\mathbb{Z}$. This provides a second example in which $f : R \to S^{-1}R$ is not an embedding.

Recall that a ring is *Jacobson* if every prime ideal is the intersection of all the maximal ideals containing it[124].

Theorem 20.1 : *Suppose L is an algebraically closed field, $n \geq 1$ is an integer, and $x_1, x_2, \ldots, x_n$ are indeterminates. Then the polynomial ring $L[x] := L[x_1, x_2, \ldots, x_n]$ is a Jacobson ring.*

Proof : Write $L[x]$ as R. To establish the theorem it suffices, by Proposition 17.6(d), to prove that if $\mathfrak{p} \subset R$ is a prime ideal, and if $r \in R \setminus \mathfrak{p}$, then there is a maximal ideal $\mathfrak{m}$ containing $\mathfrak{p}$ which does not contain r. To this end choose any prime ideal $\mathfrak{p} \subset R$ and any $r \in R \setminus \mathfrak{p}$.

By Theorem 9.8 we can choose a prime ideal[125] $\mathfrak{m} \subset R$ which is (not necessarily a maximal ideal but is) maximal w.r.t. those ideals containing $\mathfrak{p}$ but not containing r.

Let R_r be the localization of R at r and regard R as a subring of the ring R_r by means of the canonical embedding $R \to R_r$. Since $K \subset R$ this justifies the picture

(i) $$K \subset R \subset R_r.$$

Now check that the collection $\mathfrak{m}R_r$ of all finite sums $\sum_j q_j r_j$ with $q_j \in \mathfrak{m}$ and $r_j \in R_r$ is an ideal which (obviously) contains $\mathfrak{m}$, and therefore contains $\mathfrak{p}$. We claim that

(ii) $$r \notin \mathfrak{m}R_r.$$

[123] For example, one sees from $[2]([5][1] - [2][1]) = [0]$ that $[5]/[2] = [1]/[1]$. More generally, one checks easily that $[1]/[1]$, $[2]/[1]$ and $[3]/[1]$ are distinct, and that $[1]/[1] = [4]/[1] = [2]/[2] = [5]/[2] = [1]/[4] = [4]/[4]$, $[2]/[1] = [5][/[1] = [1]/[2] = [4]/[2] = [2]/[4] = [5]/[4]$, and $[3]/[1] = [0]/[1] = [0]/[2] = [0]/[4] = [3]/[2] = [3]/[4]$.

[124] The definition appears immediately after the statement of Theorem 17.6.

[125] We use the notation $\mathfrak{m}$ because we will eventually prove this is a maximal ideal as desired.

Otherwise r can be written as a finite sum $r = \sum_j q_j r_j$ with $q_j \in \mathfrak{m}$ and each r_j of the form t_j/s^{n_j} with $t_j \in R$ and $1 \leq n_j \in \mathbb{Z}$. Multiplying by a sufficiently high power of s then results in an equality of the form $s^m r = \sum_j q_j v_j$ with all terms in R and the right-hand-side in $\mathfrak{m}$. Since $\mathfrak{m} \subset R$ is prime this forces at least one of $s \in \mathfrak{m}$ and $r \in \mathfrak{m}$, and either possibility results in a contradiction.

From (ii) we have $\mathfrak{m}R_r \neq R_r$, and we can then conclude (from Corollary 9.11) that there is a maximal ideal $\mathfrak{M} \subset R_r$ containing $\mathfrak{m}R_r$. Since $r \simeq r/1 \in R_r$ is a unit[126] we have

$$r \simeq r/1 \notin \mathfrak{M}.$$

Because L embeds into $R_q/\mathfrak{M}$ we see from (i) and $\mathfrak{m} \subset \mathfrak{M}$ that (up to identifications) we have the following chain of inclusions:

(iii) $$L \subset R/\mathfrak{m} \subset M := R_a/\mathfrak{M}.$$

Since the ideal $\mathfrak{M} \subset R_r$ is maximal the factor ring M appearing in (iii) is actually a field[127]. Since $R = L[x_1, x_2, \ldots, x_n]$ is finitely generated as a K-algebra it is clear that from the quotient representations r/s^m that R_a is also finitely generated as such (in fact by $x_1, x_2, \ldots, x_n$ and $1/s$), whereupon from Proposition 3.9 we conclude that M is finitely generated as an L-algebra. Since M can be regarded as an extension of L it then follows from Corollary 18.7 that this extension is algebraic, hence from the algebraically closed assumption on L that $R_a/\mathfrak{M} = M$. The inclusions (iii) then force $R/\mathfrak{m} = L$, and we conclude that $\mathfrak{m} \subset R$ is a maximal ideal. **q.e.d.**

Corollary 20.2 : *Every finitely generated L-algebra is a Jacobson ring.*

Proof : Use Propositions 3.9 and 5.5 together with Corollary 7.4. **q.e.d.**

Corollary 20.3 : *The coordinate ring of any classical (L, L)-affine algebraic set is a Jacobson ring.*

Proof : Recall Corollary 3.10. **q.e.d.**

Keep in mind that L is assumed algebraically closed in these last two corollaries.

[126] This is the key to the proof: push R into a ring in which r is a unit and <u>then</u> pick a maximal ideal containing $\mathfrak{p}$. This will keep the ideal "away from" r. Then push this ideal back down to the original ring to obtain the desired maximal ideal. (Unfortunately, the argument is not quite so straightforward.)

[127] Up to this point of the proof no use has been made of the polynomial structure of R, i.e., everything stated thus far is valid in any (commutative) K-algebra R (with unity). But from this point on this is no longer the case.

21. Finishing Touches

In this section L is an algebraically closed field, $n \geq 1$ is an integer, and $\mathcal{V} \subset \mathbb{A}^n_L[L]$ is a classical[128] *L-affine algebraic set.*

The mapping $\varphi_{\mathcal{V}} : \mathcal{V} \to \mathrm{Spec}(L_L[\mathcal{V}])$ was introduced (in greater generality) in (6.5). For ease of reference we recall the definition:

$$\varphi_{\mathcal{V}} : c \in \mathcal{V} \mapsto f(\mathfrak{i}(\{c\})) \in \mathrm{Spec}(L_L[\mathcal{V}]), \tag{21.1}$$

where $f : K[x] \to L_L[\mathcal{V}]$ is the canonical homomorphism. We have seen (in Proposition 6.6(b)) that $\varphi_{\mathcal{V}}$ is continuous. As we now show, with the algebraically closed assumption on L we can say much more.

Theorem 21.2 : *Under the algebraically closed assumption on L the mapping $\varphi_{\mathcal{V}} : \mathcal{V} \to \mathrm{Spec}(L_L[\mathcal{V}])$ satisfies the following properties.*

(a) *It is an embedding with range* $\mathrm{maxSpec}(L_L[\mathcal{V}])$*, i.e., it is a homeomorphism onto this range.*

(b) *The range* $\mathrm{maxSpec}(L_L[\mathcal{V}])$ *is trés dense in* $\mathrm{Spec}(L_L[\mathcal{V}])$.

Particular consequences are:

(c) $\mathrm{maxSpec}(L_L[\mathcal{V}])$ *is dense in* $\mathrm{Spec}(L_L[\mathcal{V}])$*;*

(d) $\mathcal{V}$ *is irreducible if and only if* $\mathrm{Spec}(L_L[\mathcal{V}])$ *is irreducible; and*

(e) $\mathcal{V}$ *is connected if and only if* $\mathrm{Spec}(L_L[\mathcal{V}])$ *is connected.*

Assertion (a) shows how $\mathcal{V}$ can be recovered from $\mathrm{Spec}(L_L[\mathcal{V}])$. In particular, replacing $\mathcal{V}$ with $\mathrm{Spec}(L_L[\mathcal{V}])$ involves no loss of information.

Proof :

(a) For the injectivity and range assertions use (21.1) and Proposition 7.4 in combination with Corollary 18.5.

To establish the embedding assertion first recall that the continuity of $\varphi_{\mathcal{V}}$ has already been established (in Proposition 6.6(b)). To prove that the inverse mapping $\varphi_{\mathcal{V}}^{-1}|_{\mathrm{maxSpec}(L_L[\mathcal{V}])} : \mathrm{maxSpec}(L_L[\mathcal{V}]) \to \mathcal{V}$ is continuous begin by factoring $\varphi_{\mathcal{V}}$ as $f_* \circ g|_{\mathcal{V}}$, where $f_* : \mathfrak{i}(\{c\}) \in \mathrm{maxSpec}(K[x]) \mapsto f(\mathfrak{i}(\{c\}) \in L_L[\mathcal{V}]$ and $g : c \in$

[128] Recall that "classical L-affine algebraic set" means "classical (L, L)-affine algebraic set."

$\mathbb{A}^n[K] \mapsto \mathfrak{i}(\{c\}) \in \mathrm{maxSpec}(K[x])$. We have seen in Corollary 5.8 that f_* is a homeomorphism, and it therefore suffices to prove that

$$h := g^{-1} : \mathfrak{i}(\{c\}) \mapsto c \in \mathcal{V}$$

is continuous. To ease notation write $\mathrm{maxSpec}(K[x])$ as $\mathcal{M}$. Then for any ideal $\mathfrak{i} \subset K[x]$ and any $c \in \mathbb{A}^n[K]$ we have

$$\begin{aligned}
\mathfrak{i}(\{c\}) \in h^{-1}(\mathcal{V}(\mathfrak{i}))^c &\Leftrightarrow h(\mathfrak{i}(\{c\})) \in \mathcal{V}(\mathfrak{i}) \\
&\Leftrightarrow c \notin \mathcal{V}(\mathfrak{i}) \\
&\Leftrightarrow p(c) \neq 0 \ \text{ for some } \ p \in \mathfrak{i} \\
&\Leftrightarrow p \notin \mathfrak{i}(\{c\}) \ \text{ for some } \ p \in \mathfrak{i} \\
&\Leftrightarrow \mathfrak{i}(\{c\}) \in D(p) \ \text{ for some } \ p \in \mathfrak{i} \\
&\Leftrightarrow \mathfrak{i}(\{c\}) \in \cup_{p\in\mathfrak{i}} D(p).
\end{aligned}$$

This gives

$$h^{-1}((\mathcal{V}(\mathfrak{i}))^c) = \cup_{p\in\mathfrak{i}} D(p),$$

and continuity is thereby established[129].

(b) Immediate from Corollary 20.3 and Proposition 17.6.

For (c), (d) and (e) recall (a), (d) and (e) of Theorem 17.8.

q.e.d.

[129] In view of (9.28) the calculation also establishes the identity

$$h^{-1}(\mathcal{V}(\mathfrak{i})^c) = D(\mathfrak{i}).$$

Appendix: Schemes

An *étale space* over a topological space X is a local homeomorphism $\pi : E \to X$ from a topological space E onto X. The pre-images $\pi^{-1}(\{x\})$ of the points of X are the *fibers* of the étale space. When $U \subset X$ is open a mapping $s : U \to E$ such that $\pi \circ s = \mathrm{id}_U$ is a *local section* of π; a (*global*) *section* when $U = X$. When the fibers have algebraic structure (e.g., binary operations on each) this structure can often be transferred to the local sections, and a sheaf on X (whatever that means) can then result. There are (cohomology) groups associated with any (reasonable) sheaf, and these groups reflect the geometry of X, e.g., they can detect twisting within X as well as cavities and connecting tunnels of varying dimension.

An affine scheme can be regarded[130] as an étale space $\pi_R : E_R \to \mathrm{Spec}(R)$ associated in a particular way with some (commutative) ring R (with unity). The fibers of the space are the localizations $R_{\mathfrak{p}}$ of R at the prime ideals $\mathfrak{p} \in \mathrm{Spec}(R)$, and the global sections form a ring isomorphic to R. Most of the grunt work in developing the theory of such objects is in defining the topology on E_R so as to render certain local sections continuous. One has a functor from the category of rings into a category of such entities, and since the original ring can be recovered (up to isomorphism) from the global section one sees that applying the functor involves no loss of information. A *scheme* is an étale space which results from patching together affine schemes.

Algebraic geometers now study affine (and projective) algebraic sets by means of schemes, i.e., by means of étale spaces over concatenated prime spectra of various coordinate rings. One can sense from Theorem 21.2 why such an approach might prove useful, and the results have more than justified this optimism.

Notes and Comments

References [Ku] and [Mac] were very influential in the organization of the material herein. In particular, Proposition 14.4 is adapted from [Ku, Chapter 1, §4, p. 25]. References [C-L-OS$_2$], [Ful], [Iit], [Ueno-1] and [Ueno-2] were consulted with such frequency that it is difficult to attribute proper credit.

It should not surprise readers that Theorem 21.2 can be formulated in terms of a functor: see, e.g., [Hart, Chapter II, §2, Proposition 2.6, p. 78]. I simply felt that a less abstract version might be better for an initial exposure.

Heartfelt thanks my colleagues in the Kolchin Seminar on Differential Algebra for allowing me to speak on topics which many understood far better than I, and for

[130] However, this is not the standard definition.

graciously answering literally hundreds of questions from me on this material. Of course any mistakes which remain are my responsibly alone; I am confident there are many, and I would be happy to have them pointed out.

References

[Arrondo] E. Arrondo, Another Elementary Proof of the Nullstellensatz, *Am. Math. Monthly*, **113**, 2006, 169-171.

[A-M] M. Atiyah and I.G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, Reading, MA, 1969.

[B-M-R] G. Baumslag, A. Miasnikov and V. Remeslennikov, Algebraic geometry over groups. I. Algebraic sets and ideal theory, *J. Algebra* **219** (1999), no. 1, 16-79.

[Bour] N. Bourbaki, *Elements of Mathematics, Commutative Algebra, Chapters 1-7*, Springer-Verlag, Berlin, 1989.

[C-L-OS$_1$] D. Cox, J. Little and D O'Shea, *Using Algebraic Geometry*, GTM 185, Springer-Verlag, New York, 1998.

[C-L-OS$_2$] D. Cox, J. Little and D O'Shea, *Ideals, Varieties, and Algorithms*, Third Edition, Springer, New York, 2007.

[Eis] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, GTM 150, Springer, New York, 1995.

[E-H] D. Eisenbud and J. Harris, *The Geometry of Schemes*, GTM 197, Springer, New York, 2000.

[El] N.D. Elkies, Pythagorean Triples and Hilbert's Theorem 90, *Amer. Math. Monthly*, **110**, (2003), 678.

[Fors] O. Forster, *Lectures on Riemann Surfaces*, GTM 81, Springer-Verlag, New York, 1981.

[Ful] W. Fulton, *Algebraic Curves*, W.A. Benjamin, New York, 1969.

[Für] H. Fürstenberg, *On the infinitude of primes*, Amer. Math. Monthly **62** (1955), 353.

[Gunn] R.C. Gunning, *Lectures on Riemann Surfaces*, Princeton Mathematical Notes **2**, Princeton University Press, Princeton, 1966.

[Hart] R. Hartshorne, *Algebraic Geometry*, GTM 52, Springer, New York, 1977.

[H] T.W. Hungerford, *Algebra*, GTM 73, Springer-Verlag, New York, 1974.

[Iit] S. Iitaka, *Algebraic Geometry, An Introduction to Birational Geometry of Algebraic Varieties*, GTM 76, Springer-Verlag, New York, 1982.

[EDM] *Encyclopedic Dictionary of Mathematics*, Second Edition, Volume I, K. Itô, ed., MIT Press, Cambridge, MA, 1993.

[Kol] E.R. Kolchin, *Differential Algebra and Algebraic Groups*, Academic Press, New York, 1973.

[Ku] E. Kunz, *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhäuser, Boston, 1985.

[Lang_{aaf}] S. Lang, *Introduction to Algebraic and Abelian Functions*, Second Edition, GTM 89, Springer-Verlag, New York, 1982.

[L] S. Lang, *Algebra*, Revised Third Edition, GTM 211, Springer-Verlag, New York, 2002.

[M] S. Mac Lane, *Categories for the Working Mathematician*, GTM 5, Springer-Verlag, New York, 1971.

[Mac] I.G. Macdonald, *Algebraic Geometry - Introduction to Schemes*, W.A. Benjamin, New York, 1968.

[Maz] B. Mazur, Number Theory as Gadfly, *Am. Math. Monthly*, **98**, (1991), 593-610.

[Mat] H. Matsumura, *Commutative Ring Theory* (with corrections), Cambridge Studies in Advanced Mathematics 8, Cambridge University Press, Cambridge, 1989.

[Mum] D. Mumford, *Algebraic Geometry I, Complex Projective Varieties*, (Corrected Second Printing), Grund. der math. Wissen. 221, Springer-Verlag, Berlin, 1970.

[Mun] J.R. Munkres, *Topology, A First Course*, Prentice-Hall, Englewood Cliffs, NJ, 1975.

[N-Z-M] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An Introduction to the Theory of Numbers*, Fifth Edition, John Wiley & Sons, New York, 1991.

[Riben] P. Ribenboim, *The Little Book of Bigger Primes*, Second Edition, Springer-Verlag, New York, 2004.

[Ribet] K. Ribet, On modular representations of $\mathrm{Gal}(\bar{(}Q)/Q)$ arising from modular forms, *Invent. Math.*, **100**, (1990), 431-476.

[S] J.-P. Serre, *Algebraic Groups and Class Fields*, GTM 117, Springer-Verlag, New York, 1988.

[Sw-D] H.P.F. Swinnerton-Dyer, *A Brief Guide to Algebraic Number Theory*, London Math. S

[Ueno-1] K. Ueno, *Algebraic Geometry 1, From Algebraic Varieties to Schemes*, Translations of Mathematical Monographs, Volume 185, American Mathematical Society, Providence, 1999.

[Ueno-2] K. Ueno, *Algebraic Geometry 2, Sheaves and Cohomology*, Translations of Mathematical Monographs, Volume 197, American Mathematical Society, Providence, 2001.

[W] A. Wiles, Modular Elliptic Curves and Fermat's Last Theorem, *Annals of Mathematics* **141**, (1995), 443-551.

[W-T] A. Wiles and R. Taylor, Ring-Theoretic Properties of Certain Hecke Algebras, *Annals of Mathematics* **141**, (1995), 553-572.

R.C. Churchill
Department of Mathematics
Hunter College (CUNY),
the Graduate Center, CUNY, and
the University of Calgary
e-mail rchurchi@hunter.cuny.edu