IV.G. Affine varieties

In this final section, we make explicit the correspondence between algebraic spaces and rings (of functions on them). Fix a field k, an algebraically closed field $K \supset k$, and a positive integer n.

IV.G.1. DEFINITION. Let $\mathcal{S} \subset k[x_1, \ldots, x_n]$ be a subset. The **(affine) *k*-variety** defined by $\mathcal{S}$ is

$$V(\mathcal{S}) := \{\underline{a} \in K^n \mid f(\underline{a}) = 0 \ (\forall f \in \mathcal{S})\},$$

the common zero-locus of the polynomials in $\mathcal{S}$.

Algebraic geometry has its origins in the study of such solution sets of polynomial equations. Here "affine" refers to the affine n-space K^n (or "$\mathbb{A}^n_K$") in which our varieties lie, as opposed (for example) to projective n-space $\mathbb{P}^n_K$. I should mention that, when algebraic geometers talk about a variety W, they really mean an object called a *scheme* that has more structure; the K-points would then be written $W(K)$. For us there is no difference — it makes no sense to get that sophisticated in a brief treatment — but this does force us to work with points over an algebraically closed field.

IV.G.2. PROPOSITION. *Any variety is defined by a finite set of equations.*

PROOF. Writing $(\mathcal{S})$ for the ideal generated by $\mathcal{S}$ in $k[x_1, \ldots, x_n]$, we have $V(\mathcal{S}) = V((\mathcal{S}))$. By the Hilbert basis theorem, $(\mathcal{S})$ is finitely generated, say by $f_1, \ldots, f_m$; and then $V(\mathcal{S}) = V(\{f_1, \ldots, f_m\})$. $\square$

We can also turn things around:

IV.G.3. DEFINITION. The **vanishing ideal** associated to a subset $\mathrm{X} \subset K^n$ is

$$J(\mathrm{X}) := \{f \in k[x_1, \ldots, x_n] \mid f(\underline{a}) = 0 \ (\forall \underline{a} \in \mathrm{X})\}.$$

IV.G.4. PROPOSITION. *For any* X, $J(\mathrm{X})$ *is a radical ideal.*

PROOF. First, the vanishing ideal is in fact an ideal: if $f_i(\underline{a}) = 0$ $(\forall a \in \mathrm{X})$, and $g_i \in k[x_1, \ldots, x_n]$, then $(\sum_i g_i f_i)(\underline{a}) = 0$ $(\forall \underline{a} \in \mathrm{X})$. To see that it is its own radical: if $(f^n)(\underline{a}) = 0$ ($\forall \underline{a} \in \mathrm{X}$), then $f(\underline{a}) = 0$ ($\forall \underline{a} \in \mathrm{X}$). $\square$

We have inclusions of sets

$$\begin{array}{ll}
\mathscr{S} := \text{set of subsets of } k[x_1, \ldots, x_n] & \\
\cup & \\
\mathscr{I} := \text{set of ideals in } k[x_1, \ldots, x_n] & \\
\cup & \\
\mathscr{R} := \text{set of radical ideals} & \mathscr{X} := \text{set of subsets of } K^n \\
\cup & \cup \\
\mathscr{P} := \text{set of prime ideals} & \mathscr{V} := \text{set of } K\text{-varieties}
\end{array}$$

Here $\mathscr{P}$ is often called the **spectrum** of $k[x_1, \ldots, x_n]$, and written $\mathrm{Spec}(k[x_1, \ldots, x_n])$. Definitions IV.G.1 and IV.G.3 produce maps

$$\begin{array}{ccc}
V \colon \mathscr{S} \to \mathscr{V} & \text{and} & J \colon \mathscr{X} \to \mathscr{R} \\
I \mapsto V(I) & & \mathrm{X} \mapsto J(\mathrm{X}).
\end{array}$$

This is of course far from a bijection at this level: certainly, $J \circ V$ can't send a non-radical ideal to itself; and for the other composition $V \circ J$, the situation is even worse.

IV.G.5. EXAMPLE. In $\mathbb{C}^2$, if we take X to be $\{\underline{a} \in \mathbb{C}^2 \mid |a_1|^2 + |a_2|^2 \leq 1\}$ or $\{\underline{a} \in \mathbb{C}^2 \mid a_1 = e^{a_2}\}$ or $\mathbb{Q} \times \mathbb{Q}$, we end up (regardless of k) with $J(\mathrm{X}) = \{0\}$ hence $V(J(\mathrm{X})) = \mathbb{C}^2$. This can also depend on the choice of k: for instance, if $k = \mathbb{Q}$ and $n = 1$, and $\mathrm{X} = \{\pi\}$ [resp. $\{\sqrt{5}\}$], then we get $V(J(\mathrm{X})) = \mathbb{C}$ [resp. $\{\sqrt{5}, -\sqrt{5}\}$].[9]

IV.G.6. DEFINITION. (a) Given a subset $\mathrm{X} \subset K^n$, the variety $\overline{\mathrm{X}} := V(J(\mathrm{X})) \subset K^n$ is called the ***k*-Zariski closure** of X. It is the intersection of all k-varieties (equiv., the smallest k-variety) containing X.

(b) Similarly, we can define the *closure* of a set $\mathcal{S} \in \mathscr{S}$ by $\overline{\mathcal{S}} := J(V(\mathcal{S}))$. Clearly, the ideal generated by $\mathcal{S}$ is contained in $\overline{\mathcal{S}}$.

[9]You should be able to supply proofs of these statements, using the fact that a polynomial in one variable has finitely many roots, together with Lindemann-Weierstrass etc.

As to what one *can* say right off the bat about V and J, here is what follows (mostly) tautologically from the definitions. Note in particular the inclusion-reversing property (iii-iv):

IV.G.7. PROPOSITION. *Let* $\mathcal{S}, \mathcal{T} \in \mathscr{S}$, *and* $\mathrm{X}, \mathrm{Y} \in \mathscr{X}$.
(i) $V(k[x_1, \ldots, x_n]) = \emptyset$ *and* $V((0)) = K^n$.
(ii) $J(\emptyset) = k[x_1, \ldots, x_n]$ *and* $J(K^n) = (0)$.
(iii) $\mathcal{S} \subset \mathcal{T} \implies V(\mathcal{T}) \subset V(\mathcal{S})$.
(iv) $\mathrm{X} \subset \mathrm{Y} \implies J(\mathrm{Y}) \subset J(\mathrm{X})$.
(v) $\mathcal{S} \subset J(V(\mathcal{S})) = \overline{\mathcal{S}}$ *and* $\mathrm{X} \subset V(J(\mathrm{X})) = \overline{\mathrm{X}}$.
(vi) $V(\mathcal{S}) = V(J(V(\mathcal{S})))$ *and* $J(\mathrm{X}) = J(V(J(\mathrm{X})))$.

PROOF. (i) 1 vanishes nowhere, while 0 vanishes everywhere.

(ii) K is infinite (since algebraically closed), so any nonzero polynomial takes a nonzero value somewhere by [**Algebra I**, III.G.23]. This gives $J(K^n) = \{0\}$.

(iii) Given $\underline{a} \in V(\mathcal{T})$, every $f \in \mathcal{T}$ vanishes at $\underline{a}$; so every $f \in \mathcal{S}$ vanishes at $\underline{a}$, and $\underline{a} \in V(\mathcal{S})$.

(iv) Given $f \in J(\mathrm{Y})$, we have $f(\underline{a}) = 0$ ($\forall \underline{a} \in \mathrm{Y}$), hence $f(\underline{a}) = 0$ ($\forall \underline{a} \in \mathrm{X}$); thus $f \in J(\mathrm{X})$.

(v) If $f \in \mathcal{S}$, then $f(\underline{a}) = 0$ for every $\underline{a} \in V(\mathcal{S})$. If $\underline{a} \in \mathrm{X}$, then $f(\underline{a}) = 0$ for every $f \in J(\mathrm{X})$.

(vi) Begin with (v), and apply V and (iii) [resp. J and (iv)]. For instance, applying J to $\mathrm{X} \subset V(J(\mathrm{X}))$ gives $J(\mathrm{X}) \supset J(V(J(\mathrm{X})))$, and we have the other inclusion $J(\mathrm{X}) \subset J(V(J(\mathrm{X})))$ by applying the first part of (v) to $\mathcal{S} := J(\mathrm{X})$. $\square$

In view of (v), the obvious question is *when are* X *and* $\mathcal{S}$ ***closed***? — that is, when are these inclusions equalities? There is an obvious, again tautological, answer to half of this question:

IV.G.8. COROLLARY. X *is k-Zariski closed exactly when it is a k-variety:* $\mathrm{X} = \overline{\mathrm{X}} \iff \mathrm{X} \in \mathscr{V}$.

PROOF. $\underline{(\implies)}$: $\mathrm{X} = V(J(\mathrm{X})) \implies$ X is a k-variety (duh).

($\Longleftarrow$): Say $\mathrm{X} = V(\mathcal{S})$. By IV.G.7(vi), $V(\mathcal{S}) = V(J(V(\mathcal{S}))) \implies \mathrm{X} = V(J(\mathrm{X}))\ (= \overline{\mathrm{X}})$. □

But the answer for $\mathcal{S}$ is considerably deeper; indeed, it is a corollary of the famous

IV.G.9. HILBERT'S NULLSTELLENSATZ (1893). *For any $I \in \mathscr{I}$,*

$$J(V(I)) = \mathrm{Rad}(I).$$

We will prove this below after some preparation. Note that it implies $J(V(\mathcal{S})) = \mathrm{Rad}((\mathcal{S}))$ for any $\mathcal{S} \in \mathscr{S}$.

IV.G.10. COROLLARY. *$\mathcal{S} \in \mathscr{S}$ is closed precisely when it is a radical ideal: $\mathcal{S} = \overline{\mathcal{S}} \iff \mathcal{S} \in \mathscr{R}$.*

PROOF. ($\implies$): Use IV.G.4 and the hypothesis that $\mathcal{S} = J(V(\mathcal{S}))$. ($\Longleftarrow$): Write $\mathcal{S} = I$. By IV.G.9, $\overline{I} = J(V(I)) = \mathrm{Rad}(I) = I$ (since $I \in \mathscr{R}$). □

Using this result we obtain a clean parametrization of k-varieties in K^n by radical ideals in $k[x_1, \ldots, x_n]$:

IV.G.11. COROLLARY. *$\mathscr{R} \underset{J}{\overset{V}{\rightleftarrows}} \mathscr{V}$ is an inclusion-reversing bijection.*

PROOF. For $I \in \mathscr{R}$, $J(V(I)) = I$ by IV.G.10; and for $\mathrm{X} \in \mathscr{V}$, $V(J(\mathrm{X})) = \mathrm{X}$ by IV.G.8. □

In fact, the correspondence goes far beyond a bijection: for instance, in the HW you will show that

$$V(\cap_i I_i) = \cup_i V(I_i) \quad \text{and} \quad V(\textstyle\sum_i I_i) = \cap V(I_i) \tag{IV.G.12}$$

for any finite collection of ideals. Moreover, defining a k-variety to be **irreducible** if it cannot decompose as a union of two proper subsets which are both k-varieties, you will show the

IV.G.13. PROPOSITION. *V and J put the irreducible k-varieties in bijection with $\mathscr{P}$.*

The "rings of polynomial functions" we have been alluding to so far informally may now be codified as follows:

IV.G.14. DEFINITION. Let $\mathrm{X} = V(I) \subset K^n$ be an affine k-variety, and $\mathfrak{F}(\mathrm{X})$ the set of K-valued functions on X. Writing $|_{\mathrm{X}}$ for "restriction to X", the **ring of regular functions** on X or **coordinate ring** of X is defined by

$$\begin{aligned} k[\mathrm{X}] &:= \mathrm{im}\{k[x_1,\ldots,x_n] \overset{|_{\mathrm{X}}}{\to} \mathfrak{F}(\mathrm{X})\} \\ &\cong k[x_1,\ldots,x_n]/\ker(|_{\mathrm{X}}) \\ &\cong k[x_1,\ldots,x_n]/J(\mathrm{X}). \end{aligned}$$

By the Nullstellensatz, we see at once that

$$k[V(I)] \cong k[x_1,\ldots,x_n]/\mathrm{Rad}(I). \tag{IV.G.15}$$

If I is a radical ideal, with generators $f_1,\ldots,f_m$, and X is the variety described by $\cap_{i=1}^m \{\underline{a} \mid f_i(\underline{a}) = 0\}$, this takes the form

$$k[\mathrm{X}] = k[x_1,\ldots,x_n]/(f_1,\ldots,f_m).$$

It is left to you to describe what happens to X, and to this ring, when I has a nontrivial reduced primary decomposition.

Proving the Nullstellensatz.

We proceed by way of two lemmas which are of significant interest in their own right. Let R/k be a finitely generated ring extension. Write $\mathbb{F} := \mathfrak{F}\{R\}$ for its fraction field, and put $r := \mathrm{trdeg}(\mathbb{F}/k)$.

IV.G.16. NOETHER NORMALIZATION LEMMA. *There exists an algebraically independent subset $\{t_1,\ldots,t_r\} \subset R$ such that R is integral over $k[t_1,\ldots,t_r]$.*

IV.G.17. REMARK. Notice that by IV.F.19, this implies that the Krull dimension of R is r. If R is the coordinate ring of an affine variety $\mathrm{X} \subset K^n$, the result can be thought of as saying that there is a k-linear projection $K^n \twoheadrightarrow K^r$ whose restriction to X presents it as a finite cover of affine r-space, along which the embedding

$k[t_1, \ldots, t_r] \hookrightarrow k[\mathrm{X}] = R$ represents pullback of functions. In fact, as the first line of the proof demonstrates, we are always in this case:

PROOF. Let $u_1, \ldots, u_n$ denote generators of R/k (as a ring); that is, there is a homomorphism $\pi \colon k[x_1, \ldots, x_n] \twoheadrightarrow R$ sending $x_i \mapsto u_i$. If it is an isomorphism, then the $\{u_i\}$ are algebraically independent, and furnish a transcendence basis for $\mathbb{F}/k$ (and we are done).

Otherwise, $I := \ker(\theta)$ is a nonzero ideal, and $R \cong k[x_1, \ldots, x_n]/I$. Fix an element $\mathfrak{f}(\underline{x}) := \sum_{\underline{\jmath} \in \mathfrak{J}} \kappa_{\underline{\jmath}} \underline{x}^{\underline{\jmath}} \in I \backslash \{0\}$, with $\kappa_{\underline{\jmath}} \in k^*$ and $\mathfrak{J} \subset \mathbb{N}^n$ a finite index set, with all entries strictly bounded by some $c \in \mathbb{N}$. Writing $\sigma_{\underline{\jmath}} := \sum_{i=1}^n c^{i-1} \jmath_i$, the set $\{\sigma_{\underline{\jmath}} \mid \underline{\jmath} \in \mathfrak{J}\} \subset \mathbb{N}$ has the same cardinality[10] as $\mathfrak{J}$ and a maximal element $\sigma_{\underline{\jmath}^*}$.

Now $\mathfrak{f}(\underline{u}) = \pi(\mathfrak{f}(\underline{x})) = 0$. Writing $u_i =: v_i + u_1^{c^{i-1}}$ for $2 \leq i \leq n$, this becomes $\kappa_{\underline{\jmath}^*} u_1^{\sigma_{\underline{\jmath}^*}} + f(u_1, v_2, \ldots, v_n) = 0$, with $\deg_{u_1}(f) < \sigma_{\underline{\jmath}^*}$. Denoting $R_1 := k[v_2, \ldots, v_n] \subset R$, it follows that u_1 is integral over R_1 and (by IV.F.9(b)) that $R = R_1[u_1]$ is integral over R_1. Moreover, $\mathbb{F}$ is algebraic over $\mathbb{F}_1 := \mathfrak{F}\{R_1\}$ (why?).

At this point we repeat the argument from the beginning with R_1 and $v_2, \ldots, v_n$ replacing R and $u_1, \ldots, u_n$. This obviously must terminate at some $R_\ell = k[w_{\ell+1}, \ldots, w_n]$, with the $\{w_i\}$ algebraically independent. Applying IV.F.9(c) to the tower of ring extensions, we get that R/R_ℓ is integral; and by I.N.6 (and the tower law), the $\{w_i\}$ are a transcendence basis for $\mathbb{F}$. So $r = n - \ell$ and we are done. □

Before proving that the closure of a proper ideal (in the sense of IV.G.6(b)) is its radical, we first need to show that it remains proper. Equivalently, before we show that $V(I)$ is a variety with ring of functions $k[x_1, \ldots, x_n]/\sqrt{I}$, we need to show that it contains a point:

IV.G.18. WEAK NULLSTELLENSATZ. *Any proper ideal* $I \subsetneq k[x_1, \ldots, x_n]$ *has nonempty* $V(I) \subset K^n$.

PROOF. Let P be a prime of $k[x_1, \ldots, x_n]$ containing I, so that $V(P) \subset V(I)$ by IV.G.7(iii). It will suffice to show that $V(P) \neq \emptyset$.

[10] Suppose $\sigma_{\jmath} = \sigma_{\jmath'}$. Then going mod c gives $c \mid \jmath_1 - \jmath_1'$ hence $\jmath_1 = \jmath_1'$ and $\sum_{i=2}^n c^{i-2} \jmath_i = \sum_{i=2}^n c^{i-2} \jmath_i'$. Going mod c again gives $\jmath_2 = \jmath_2'$, and so on until $\underline{\jmath} = \underline{\jmath}'$.

Write $\pi\colon k[x_1,\ldots,x_n] \twoheadrightarrow k[x_1,\ldots,x_n]/P =: R$ and $u_i := \pi(x_i)$. Since $P \cap k = \{0\}$, we may identify k with its image. Noether normalization produces $t_1,\ldots,t_r \in R$, algebraically independent over k, such that R is integral over the polynomial ring $S := k[t_1,\ldots,t_r]$.

The kernel of the evaluation map $S \twoheadrightarrow k$ sending $t_i \mapsto 0$ is the ideal $\mathfrak{m} := (t_1,\ldots,t_r)$ consisting of polynomials with zero constant term. So $S/\mathfrak{m} \cong k$ and $\mathfrak{m}$ is maximal. By the Lying-over theorem IV.F.16, there is a prime $\mathfrak{n} \subset R$ with $\mathfrak{n} \cap S = \mathfrak{m}$; by IV.F.21, $\mathfrak{n}$ is maximal, and $R/\mathfrak{n} =: \tilde{k}$ a field. Using the diagram

$$\begin{array}{ccc} k \cong S/(\mathfrak{n}\cap S) & \hookrightarrow & R/\mathfrak{n} = \tilde{k} \\ \uparrow & & \uparrow {\scriptstyle =:\tau} \\ S & \hookrightarrow & R \end{array}$$

we see at once that $\tilde{k}/k$ is an algebraic extension: lift an element of $\tilde{k}$ to R, write down its monic equation over S, and apply the upward arrows. So there exists an embedding $\sigma\colon \tilde{k} \hookrightarrow \bar{k} \subset K$.

Writing ϕ for the composition

$$k[x_1,\ldots,x_n] \overset{\pi}{\twoheadrightarrow} R \overset{\tau}{\twoheadrightarrow} \tilde{k} \overset{\sigma}{\hookrightarrow} K,$$

we note that it kills P and is the identity on k. So for each $f \in P$, we have $f(\phi(x_1),\ldots,\phi(x_n)) = \phi(f(x_1,\ldots,x_n)) = 0$, whence $(\phi(x_1),\ldots,\phi(x_n)) \in V(P)$. □

IV.G.19. REMARK. Geometrically, one should think of R as the coordinate ring of the irreducible variety $\mathrm{X} \subset K^n$ defined by P. Homomorphisms from $k[x_1,\ldots,x_n]$ to K are evaluation maps at points of K^n, i.e. pullback maps along the inclusion of a point in K^n. To say that a homomorphism factors through $R = k[x_1,\ldots,x_n]/P$ is to say this point is in X.

The mechanism by which this proof produced a homomorphism from R to K was, in geometric terms, to present X as a finite branched cover $\beta\colon \mathrm{X} \twoheadrightarrow K^r$, and exhibit a point of $\beta^{-1}(\underline{0})$. The map from $\beta^{-1}(\underline{0})$ to $\underline{0}$ is "dual" to $k \hookrightarrow \tilde{k}$, and the choice of embedding $\tilde{k} \hookrightarrow K$ over k was the choice of a point in $\beta^{-1}(\underline{0})$.

Finally, turning to the Nullstellensatz itself:

PROOF OF IV.G.9. We may assume $I \subsetneq k[\underline{x}] := k[x_1, \ldots, x_n]$ is a proper ideal, since otherwise we are done by IV.G.7(i-ii). Moreover, it's easy to see that $\text{Rad}(I) \subset J(V(I))$: if $f^m \in I$, then since $I \subset J(V(I))$ (by IV.G.7(v)) and $J(V(I))$ is radical (by IV.G.4), we have $f \in J(V(I))$.

Suppose, conversely, that $f \in J(V(I)) \backslash \{0\}$. Consider the ideals $\tilde{I} := k[\underline{x}, y]I$ and $J := (yf - 1) + \tilde{I} \subset k[\underline{x}, y]$ in the polynomial ring in $(n+1)$ variables. Given $(\underline{a}, b) \in V(J) \subset K^{n+1}$, we have:

- $\underline{a} \in V(I)$, since $J \supset \tilde{I} \implies V(J) \subset V(\tilde{I}) = V(I) \times K$; and
- $(\underline{a}, b) \in V(yf - 1)$, since $J \supset (yf - 1)$.

This gives $0 = bf(\underline{a}) - 1 = b \cdot 0 - 1 = -1$, a contradiction. So $V(J) = \emptyset$. But then, by the weak Nullstellensatz, J cannot be a proper ideal! That is, $J = k[\underline{x}, y]$; so $1 \in J$, whence

(IV.G.20) $$1 = (yf - 1)g_0 + \textstyle\sum_{i=1}^{\ell} g_i f_i$$

for some $f_i \in I$ and $g_i \in k[\underline{x}, y]$.

Now define a homomorphism $\theta\colon k[\underline{x}, y] \to k(\underline{x})$ (over k) by sending $x_i \mapsto x_i$ and $y \mapsto \frac{1}{f(\underline{x})}$. Applying this to (IV.G.20) yields

$$1 = (\tfrac{1}{f} f - 1)g_0(\underline{x}, \tfrac{1}{f}) + \textstyle\sum_{i=1}^{\ell} g_i(\underline{x}, \tfrac{1}{f}) f_i(\underline{x}) = \sum_{i=1}^{\ell} g_i(\underline{x}, \tfrac{1}{f}) f_i(\underline{x}).$$

Taking $m := \max(\{\deg_y(g_i)\}_{i=1}^{\ell})$, so that $f^m(\underline{x}) g_i(\underline{x}, \frac{1}{f}) \in k[\underline{x}]$, we get

$$f^m = f^m \cdot 1 = \textstyle\sum_{i=1}^{\ell} f^m(\underline{x}) g_i(\underline{x}, \tfrac{1}{f}) f_i(\underline{x}) \in I.$$

Hence $f \in \text{Rad}(I)$ and the proof is complete. $\square$