# NOETHER NORMALIZATION, THE NULLSTELLENSATZ AND AFFINE VARIETIES

R. VIRK

## Contents

I suggest that at first reading you skip the proofs of Noether Normalization (Thm. 3.1) and the Nullstellensatz (Thm. 3.5). Come back to them later once you have a feel for the overall picture being sketched below.

## 1. Algebraic sets

1.1. From now on, unless explicitly stated otherwise, $k$ will denote an algebraically closed field, known as the *ground field.*

1.2. An *algebraic subset* of $k^n$ is a subset of the form

$$\mathrm{zeroes}(\Sigma) = \{(a_1, \dots, a_n) \in k^n \mid f(a_1, \dots, a_n) = 0 \text{ for all } f \in \Sigma\},$$

where $\Sigma$ is a subset of $k[x_1, \dots, x_n]$.

1.3. *Remark.* Note that $\mathrm{zeroes}(\Sigma) = \mathrm{zeroes}(\mathfrak{a}_\Sigma)$, where $\mathfrak{a}_\Sigma$ denotes the ideal generated by $\Sigma$. Now ideals in $k[x_1, \dots, x_n]$ are finitely generated, so an algebraic subset is the set of simultaneous solutions of a finite number of polynomial equations.

1.4. *Example.* $\mathrm{zeroes}(0) = k^n$, this algebraic set is denoted $\mathbf{A}^n$ and is called *affine $n$-space.* $\mathbf{A}^1$ is often called the *affine line* and $\mathbf{A}^2$ is often called the *affine plane.*

1.5. *Example.* Let $C = \{(t^2, t^3) \in k^2 \mid t \in k\}$. Then $C$ is an algebraic set, since it is the set of solutions (in $k^2$) to $x^3 - y^2 = 0$.

1.6. By definition, zeroes gives a map

$$\{\text{ideals of } k[x_1, \dots, x_n]\} \xrightarrow{\text{zeroes}} \{\text{algebraic subsets of } k^n\}.$$

There is a correspondence going the other way:

$$\{\text{algebraic subsets of } k^n\} \xrightarrow{I} \{\text{ideals of } k[x_1, \dots, x_n]\},$$

defined by

$$I(X) = \{f \in k[x_1, \dots, x_n] \mid f(a) = 0 \text{ for all } a \in X\}.$$

The correspondences $I$ and $V$ enjoy a number of useful properties that I will state in a moment. First, recall that if $\mathfrak{a}$ is an ideal in a ring $A$, then the *radical* of $\mathfrak{a}$ is

$$\sqrt{\mathfrak{a}} = \{f \in A \mid f^n \in \mathfrak{a} \text{ for some } n \in \mathbf{Z}_{\geq 0}\}.$$

1.7. **Proposition.** *We have*

(i) $\text{zeroes}(0) = k^n$ *and* $\text{zeroes}(1) = \emptyset$.

(ii) *For any family of ideals* $\mathfrak{a}_i \in k[x_1, \dots, x_n]$*,* $i \in I$*:*

$$\text{zeroes}(\bigcup_{i\in I} \mathfrak{a}_i) = \bigcap_{i \in I} \text{zeroes}(\mathfrak{a}_i).$$

(iii) $\text{zeroes}(\mathfrak{a} \cap \mathfrak{b}) = \text{zeroes}(\mathfrak{a}\mathfrak{b}) = \text{zeroes}(\mathfrak{a}) \cup \text{zeroes}(\mathfrak{b})$ *for any ideals* $\mathfrak{a}, \mathfrak{b} \subseteq k[x_1, \dots, x_n]$*.*

(iv) *Let* $\mathfrak{a}, \mathfrak{b} \subseteq k[x_1, \dots, x_n]$ *be ideals. If* $\mathfrak{a} \subseteq \mathfrak{b}$*, then* $\text{zeroes}(\mathfrak{b}) \subseteq \text{zeroes}(\mathfrak{a})$*.*

(v) *Let* $X, Y \subseteq k^n$ *be algebraic sets. If* $X \subseteq Y$*, then* $I(Y) \subseteq I(X)$*.*

(vi) $\text{zeroes}(I(X)) = X$ *for all algebraic sets* $X \subseteq k^n$*.*

(vii) $\sqrt{\mathfrak{a}} \subseteq I(\text{zeroes}(\mathfrak{a}))$ *for all ideals* $\mathfrak{a} \subseteq k[x_1, \dots, x_n]$*.*

*Proof.* Exercise! □

1.8. *Remark.* The containment in (vii) above can be upgraded to an equality. However, this is not quite trivial to show. We will do so in a bit.

## 2. Morphisms and the coordinate ring

2.1. Morphisms are fascinating! A *morphism* of algebraic sets $X \to Y$ is a polynomial map $X \to Y$. That is, if $X \subseteq k^n$ and $Y \subseteq k^m$ are algebraic sets (note that $X$ and $Y$ don't necessarily live in the same ambient space), then a map $f\colon X \to Y$ is a morphism if there exist polynomials $f_1, \dots, f_m \in k[x_1, \dots, x_m]$ such that

$$f(a) = (f_1(a_1, \dots, a_n), \dots, f_m(a_1, \dots, a_n))$$

for all points $a = (a_1, \dots, a_n) \in X$. A morphism $f\colon X \to Y$ is an isomorphism if there exists a morphism $g\colon Y \to X$ such that $gf$ and $fg$ are the identity on $X$ and $Y$ respectively.

2.2. **Warning.** A bijective morphism need not be an isomorphism: let $C \subset k^2$ be the algebraic set defined by the ideal $(x^3 - y^2) \in k[x, y]$. That is, $C$ is the set of solutions to the equation $x^3 - y^2 = 0$. Define a morphism $f\colon \mathbf{A}^1 \to C$ by $t \mapsto (t^2, t^3)$. This morphism is a bijection. However, it is not an isomorphism (why not?).

2.3. Let $X \subseteq k^n$ be an algebraic set. Then the quotient ring $k[x_1, \dots, x_n]/I(X)$ is in a natural way a ring of functions on $X$. In more detail, define a *polynomial function* on $X$ to be a map $f\colon X \to k$ of the form $(a_1, \dots, a_n) \mapsto F(a_1, \dots, a_n)$, with $F \in k[x_1, \dots, x_n]$. Equivalently, a polynomial function on $X$ is a morphism $X \to \mathbf{A}^1$. Regardless, all of this just means that $f$ is defined by a polynomial. Now two polynomials $f_1, f_2 \in k[x_1, \dots, x_n]$ define the same function on $X$ if and only if $f_1 - f_2$ vanishes on $X$, i.e., $f_1 - f_2 \in I(X)$. Thus, we define the *coordinate ring* $k[X]$ by

$$k[X] = \{\text{polynomial functions } X \to k\} = k[x_1, \dots, x_n]/I(X).$$

2.4. Let $f\colon X \to Y$ be a morphism of algebraic sets. Define

$$f^*\colon k[Y] \to k[X] \qquad \text{by} \qquad f^*g(x) = g(f(x)).$$

To clarify: suppose $f$ is given by

$$(x_1, \dots, x_n) \mapsto (f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n))$$

for some polynomials $f_i$. Then, for $g \in k[y_1, \dots, y_n]/I(Y)$,

$$f^*g \text{ evaluated at } (x_1, \dots, x_n) = g \text{ evaluated at } (f_1(x_1, \dots, x_n), \dots, f_m(x_1, \dots, x_n)).$$

2.5. *Example.* Let $C \subset k^2$ be the set of solutions of the polynomial $x^3 - y^2 = 0$, so that $k[C] = k[x,y]/(x^3 - y^2)$. Define $f\colon \mathbf{A}^1 \to C, t \mapsto (t^2, t^3)$. Then

$$f^*\colon k[x,y]/(x^3-y^2) \to k[\mathbf{A}^1] = k[z] \quad \text{is given by} \quad x \mapsto z^2, y \mapsto z^3.$$

Note that I haven't justified why $k[C] = k[x,y]/(x^3 - y^2)$. Nevertheless, it is true (exercise!). Do note that this is by no means an obvious fact, the necessary tools required to show this will be developed in the next section.

2.6. **Proposition.** *The assignment $f \mapsto f^*$ gives a canonical bijection*

$$\{\textit{morphisms } X \to Y\} \leftrightarrow \{k\textit{-algebra homomorphisms } k[Y] \to k[X]\}.$$

*Proof.* By the definition of an algebraic set: $X \subseteq k^n$, $Y \subseteq k^m$, and $k[X] = k[x_1,\dots,x_n]/I(X)$, $k[Y] = k[y_1,\dots,y_m]/I(Y)$. For a $k$-algebra homomorphism $g\colon k[Y] \to k[X]$, write $g_i$ for $g(y_i)$, $i = 1,\dots,m$. Define $g^\vee : X \to Y$ by

$$g^\vee(a_1,\dots,a_n) = (g_1(a_1,\dots,a_n),\dots,g_m(a_1,\dots,a_n)).$$

This is well defined: $g_i$ is uniquely defined modulo $I(X)$ and every element of $I(X)$ vanishes on $(a_1,\dots,a_n) \in X$. Certainly, $g^\vee$ is a morphism of algebraic sets. Further, if $f \in k[y_1,\dots,y_m]/I(Y)$, then

$$f(g_1(a_1,\dots,a_n),\dots,g_m(a_1,\dots,a_n)) = g(f) \text{ evaluated at } (a_1,\dots,a_n).$$

In particular, $g^\vee$ lands in $Y$ and $(g^\vee)^* = g$. Finally, if $h\colon X \to Y$ is a morphism given by $(a_1,\dots,a_n) \mapsto (h_1(a_1,\dots,a_n),\dots,h_m(a_1,\dots,a_n))$, then

$$\begin{aligned}(h^*)^\vee(a_1,\dots,a_n) &= (h_1^*(a_1,\dots,a_n),\dots,h_m^*(a_1,\dots,a_n))\\ &= (h_1(a_1,\dots,a_n),\dots,h_m(a_1,\dots,a_n))\\ &= h(a_1,\dots,a_n).\end{aligned}$$

Hence, $(h^*)^\vee = h$. To summarize, we have shown that the assignment $g \mapsto g^\vee$ is inverse to the assignment $f \mapsto f^*$. □

2.7. **Proposition.** *Let $X \xrightarrow{f} Y \xrightarrow{g} Z$ be morphisms of algebraic sets. Then*

$$(g \circ f)^* = f^* \circ g^*.$$

*Proof.* To avoid confusion, for a set $S$ and a function $F\colon S \to k$, write $\langle F, s\rangle$ for $F$ evaluated at $s \in S$. Let $p \in k[Z]$ and $x \in X$. Then

$$\langle (g\circ f)^* p, x\rangle = \langle p, gf(x)\rangle = \langle g^*p, f(x)\rangle = \langle f^*(g^*p), x\rangle.$$

That is, $(g \circ f)^* = f^* \circ g^*$. □

2.8. *Remark.* The result above is essentially just the fact that composition of maps is associative.

2.9. **Corollary.** *A morphism of algebraic sets $f\colon X \to Y$ is an isomorphism if and only if $f^*k[Y] \to k[X]$ is an isomorphism of $k$-algebras.*

*Proof.* Exercise! □

## 3. Noether Normalization and the Nullstellensatz

3.1. **Theorem** (Noether Normalization)**.** *Let $A$ be a finitely generated algebra over a field $k$ (not necessarily algebraically closed). Then there exist $x_1,\dots,x_n \in A$ algebraically independent over $k$ (this means that the homomorphism from the polynomial ring $k[t_1,\dots,t_n]$ to $A$ given by $t_i \mapsto x_i$ is injective) such that $A$ is finite over $B = k[z_1,\dots,z_m]$.*

*Proof.* As $A$ is a finitely generated algebra over $k$ we may assume that $A = k[y_1, \dots, y_m]/\mathfrak{p}$ for some ideal $\mathfrak{a}$. If $\mathfrak{a} = 0$, then there is nothing to prove so assume otherwise. Let $f(y_1, \dots, y_m) \in \mathfrak{a}$ be non-zero. Let $r_1, \dots, r_m$ be positive integers, and let

$$z_2 = y_2 - y_1^{r_2}, \quad z_3 = y_3 - y_1^{r_3}, \quad \cdots, \quad z_m = y_m - y_1^{r_m}.$$

Then $f(y_1, z_2 + y_1^{r_2}, \dots, z_m + y_1^{r_m}) = 0$ in $A$. Now the polynomial $f(y_1, \dots, y_m)$ is the sum of monomial terms of the form $ay_1^{b_1} \cdots y_m^{b_m}$, $a \in k - \{0\}$. Each of these terms gives rise to various new monomial terms in the polynomial $f(y_1, z_2 + y_1^{r_2}, \dots, z_m + y_1^{r_m}) = 0$, including some terms of the form $ay_1^{b_1 + r_2 b_2 + \cdots + r_m b_m}$ which may cancel each other out. However, a moment's reflection should convince you that if we pick the $r_i$'s large enough and increasingly rapidly enough: $0 \ll r_2 \ll r_3 \ll \cdots \ll r_m$, then these new terms $ay_1^{b_1 + r_2 b_2 + \cdots + r_m b_m}$ will have distinct degrees, and one of them will emerge as the term of highest degree in this new polynomial. Thus,

$$f(y_1, z_2 + y_1^{r_2}, \dots, z_m + y_1^{r_m}) = ay_1^N + \text{ terms of degree } < N,$$

with $a \neq 0$. Thus, $f(y_1, z_2 + y_1^{r_2}, \dots, z_m + y_1^{r_m}) = 0$ in $A$ gives an equation of integral dependence for $y_1$ over $k[z_2, \dots, z_m]$. Further, $A$ is integrally dependent on $k[y_1, z_2, \dots, z_m]$, since $y_i = z_i + y^{r_i}$. Hence, $A$ is integrally dependant on $k[z_2, \dots, z_m]$. Now repeat the procedure outlined above for $k[z_2, \dots, z_m]$. □

3.2. **Proposition.** *Let $B$ be an integral domain and let $A \subseteq B$ be a subring. Assume that $B$ is integral over $A$. Show that $A$ is a field if and only if $B$ is a field.*

*Proof.* Exercise! □

3.3. **Theorem** (Weak Nullstellensatz)**.** *Let $k$ be an algebraically closed field. Then the maximal ideals in the ring $k[x_1, \dots, x_n]$ are the ideals*

$$(x_1 - a_1, x_2 - a_2, \dots, x_n - a_n),$$

*where $a_1, \dots, a_n \in k$.*

*Proof.* Let $\mathfrak{m} \subset k[x_1, \dots, x_n]$ be a maximal ideal and set $k' = k[x_1, \dots, x_n]/\mathfrak{m}$. Then $k'$ is a field extension of $k$. We need to show that $k' = k$. As $k$ is algebraically closed, it suffices to show that $k'$ is a finite (and hence algebraic) extension of $k$. Certainly, $k'$ is a finitely generated $k$-algebra. So, by Noether Normalization, there exists a $k$-subalgebra $A \subseteq k'$ that is isomorphic to a polynomial ring and is such that $k'$ is finite over $A$ (and hence also integral over $A$, see Prop. 2.5 and Remark 2.6 in the previous week's notes). By Prop. 3.2, $A$ is a field. But, the only polynomial ring over $k$ that is a field is the ring of polynomials in zero variables! That is, we must have $A = k$. □

3.4. **Corollary.** *Let $\mathfrak{a} \subseteq k[x_1, \dots, x_n]$ be an ideal. Then* zeroes$(\mathfrak{a}) = \emptyset$ *if and only if $\mathfrak{a} = k[x_1, \dots, x_n]$.*

*Proof.* It is obvious that if $\mathfrak{a} = k[x_1, \dots, x_n]$, then zeroes$(\mathfrak{a}) = 1$ (see (i) of the previous proposition). The interesting part is to show that if $\mathfrak{a}$ is a proper ideal, then zeroes$(\mathfrak{a}) \neq \emptyset$. If $\mathfrak{a}$ is a proper ideal, then there exists some maximal ideal $\mathfrak{m}$ containing $\mathfrak{a}$. By the Weak Nullstellensatz, we have zeroes$(\mathfrak{m}) \neq \emptyset$. Using (iv) of the previous proposition we infer zeroes$(\mathfrak{m}) \subseteq$ zeroes$(\mathfrak{a})$. Hence, zeroes$(\mathfrak{a})$ is not empty. □

3.5. **Theorem** (Nullstellensatz)**.** *Let $\mathfrak{a} \subseteq k[x_1, \dots, x_n]$ be an ideal. Then*

$$I(\text{zeroes}(\mathfrak{a})) = \sqrt{\mathfrak{a}}.$$

*Proof.* Let $f_1(x_1,\dots,x_n),\dots,f_m(x_1,\dots,x_n)$ be generators of $\mathfrak{a}$. We need to show that if $g(x_1,\dots,x_n)$ is a polynomial satisfying $g(a_1,\dots,a_n)=0$ for every point $(a_1,\dots,a_n)\in k^n$ such that

$$f_1(a_1,\dots,a_n)=f_2(a_1,\dots,a_n)=\dots=f_m(a_1,\dots,a_n)=0,$$

then $g(x_1,\dots,x_n)^N\in\mathfrak{a}$ for some $N\in\mathbf{Z}_{\geq 0}$. This requires a clever trick (called the Rabinowitsch trick): we work in the polynomial ring $k[x_1,\dots,x_n,t]$ and consider the ideal $\mathfrak{b}\subseteq k[x_1,\dots,x_n,t]$ generated by $f_1(x_1,\dots,x_n),\dots,f_m(x_1,\dots,x_n)$ and $1-tg(x_1,\dots,x_n)$. I claim that $\mathfrak{b}=k[x_1,\dots,x_n,t]$. To see this consider $V(\mathfrak{b})\subseteq k^{n+1}$. This algebraic set is the intersection of the set

$$\{(a_0,\dots,a_n,b)\,|\,(a_0,\dots,a_n)\in \text{zeroes}(\mathfrak{a})\subseteq k^n, b\in k)\}$$

with the set

$$\{(a_0,\dots,a_n,\frac{1}{g(a_0,\dots,a_n)})\,|\,(a_0,\dots,a_n)\in k^n, g(a_0,\dots,a_n)\neq 0\}.$$

But, by assumption, $g(x_1,\dots,x_n)$ vanishes on zeroes($\mathfrak{a}$). Thus, this intersection is empty, i.e., zeroes($\mathfrak{b}$) $=\emptyset$. Hence, $\mathfrak{b}=k[x_1,\dots,x_n,t]$ by Cor. 3.4.

We now infer that there exist polynomials $p_1(x_1,\dots,x_n,t),\dots,p_{m+1}(x_1,\dots,x_n,t)$ such that

$$1=\sum_{i=1}^m p_i(x_1,\dots,x_n,t)f_i(x_1,\dots,x_n)+p_{m+1}(x_1,\dots,x_n,t)(1-tg(x_1,\dots,x_n)).$$

This gives us the following relation in the quotient ring $k[x_1,\dots,x_n,t]/(1-tg)$:

$$1=\sum_{i=1}^m p_i(x_1,\dots,x_n,t)f_i(x_1,\dots,x_n).$$

Multiplying by a sufficiently large power $N$ of $g(x_1,\dots,x_n)$ we obtain an relation, in $k[x_1,\dots,x_n,t]/(1-tg)$, of the form

$$g(x_1,\dots,x_n)^N=\sum_{i=1}^m r_i(x_1,\dots,x_n)f_i(x_1,\dots,x_n),$$

for some appropriate polynomials $r_i(x_1,\dots,x_n)$. We may and will assume that $g(x_1,\dots,x_n)$ is not the zero polynomial (otherwise there would have been nothing to prove in the first place). Then the map $k[x_1,\dots,x_n]\to k[x_1,\dots,x_n,t]/(1-tg)$, $h(x_1,\dots,x_n)\mapsto h(x_1,\dots,x_n)$, is injective (why?) and hence the expression above is valid in $k[x_1,\dots,x_n]$. In other words, $g(x_1,\dots,x_n)\in\sqrt{\mathfrak{a}}$. □

## 4. Affine varieties

4.1. Talking about algebraic sets can be a bit cumbersome, since we have to always refer to an ambient space $k^n$ that an algebraic set sits in. Don't get me wrong, this can be extremely convenient when we need to get our hands dirty and explicitly compute something. This is analogous to the tension between matrices and linear transformations (they are the same thing but sometimes it is convenient to not pick a basis and work with the abstract notion of a linear transformation as opposed to a matrix). I am about to free algebraic sets from the tyranny of an ambient space by defining an *affine variety.* But, for practical purposes, you will not miss much if you put 'affine variety = algebraic set'. Prop. 2.6 and Cor. 2.9 tell us that algebraic sets are determined up to isomorphism by their coordinate rings. So it makes sense to make the following definition:

4.2. An *affine variety* (over $k$) is a set $V$, together with a ring of $k$-valued functions $k[V]$ (addition and multiplication defined point wise), such that:

(i) $k[V]$ is a finitely generated algebra over $k$.

(ii) For some choice of generators $t_1, \dots, t_n \in k[V]$, called *coordinate functions*, the map
$$V \to k^n, \quad v \mapsto (t_1(v), \dots, t_n(v)),$$
embeds $V$ as an algebraic subset of $k^n$.

4.3. *Example.* Let $\mathbf{G}_m$ be the affine variety given as follows: as a set $\mathbf{G}_m$ consists of the non-zero elements in $k$, $k[\mathbf{G}_m] = k[t, t^{-1}]$, where $t(a) = a$ for all $a \in \mathbf{G}_m$. The coordinate functions are $t$ and $t^{-1}$, so that $a \mapsto (t(a), t^{-1}(a)) = (a, a^{-1})$ embeds $\mathbf{G}_m$ in $k^2$ as the set of solutions to the polynomial equation $xy - 1 = 0$.

4.4. *Remark.* The affine variety $\mathbf{G}_m$ is one of the simplest examples of an 'affine algebraic group'. Roughly, an affine algebraic group is an affine variety whose underlying points have a group structure compatible with the variety structure.

4.5. I should certainly also define a morphism of affine varieties. Of course, the definition is completely dictated by 'affine variety = algebraic set'. A morphism of affine varieties $V \to W$ is a map of sets $f \colon V \to W$ such that, for $p \in k[W]$, the assignment $p \mapsto f^*p$ defines a $k$-algebra homomorphism $k[W] \to k[V]$. As before, $f^*p(v) = p(f(v))$.

## 5. Commercial break

We have established a bridge between algebra and geometry:
$$\{\text{finitely generated } k\text{-algebras with no nilpotents}\} \leftrightarrow \{\text{affine varieties}\}.$$
The goal for the remainder of this course is to send some fairly lightweight traffic both ways across this bridge. The type of questions that we want to address are: what do injections/surjections on one side correspond to on the other? What type of geometry corresponds to an integral domain, PID, UFD, Dedekind domain? What type of ring corresponds to a curve or a hypersurface? What 'is' a curve/hypersurface? What is the geometry of integral/finite maps? What is the algebra of geometric notions like 'tangent', 'smooth' or 'dimension'? Of course, we are only going to have the time to discuss one or two of these questions. I hope you will find this synthesis of algebra and geometry amazing (and a bit overwhelming!) and at some point decide to learn more than can feasibly be tackled in what time we have left. I want to make one final remark that 'officially' has nothing to do with the course (and should probably be ignored).

We have defined varieties only with the adjective 'affine'. A *variety* is, roughly speaking, a space that locally looks like an affine variety (this is analogous to how a sphere locally looks like $\mathbf{R}^2$). Further, some of you may have heard of schemes (probably in dark corridors and in hushed tones). What we have called an affine variety is a reduced separated affine scheme of finite type over an algebraically closed field (is anyone actually reading this? prone to headaches much?). I mention this since for different authors 'affine variety' often means different things. Some authors define an affine variety to be an algebraic set $X$ such that $I(X)$ is a prime ideal. These will correspond to what we will call *irreducible* affine varieties. So, some care should be exercised when exploring the literature. Finally, with our definition of affine variety we are essentially studying rings with no nilpotents. An (affine) scheme is what you would get if you seriously pursued the (*a priori* absurd) point of view that *every* ring is the ring of functions on some geometric object.

Department of Mathematics, University of California, Davis, CA 95616
*E-mail address*: virk@math.ucdavis.edu