Chapter 12

Algebraic Varieties

12.1 Algebraic Varieties

Let K be a field, $n \geq 1$ a natural number, and let $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$ be polynomials with coefficients in K. Then

$$V = \{(a_1, \ldots, a_n) : f_1(a_1, \ldots, a_n) = \ldots = f_m(a_1, \ldots, a_n) = 0\}$$

is called an affine algebraic variety defined over K (we will later actually add more conditions; in the literature, the objects above are often called prevarieties or algebraic sets). If we replace the affine by projective spaces (and the polynomials by homogeneous polynomials) we get the notion of projective algebraic prevarieties.

Special cases include the space $\mathbb{A}^n K$ (or $\mathbb{P}^n K$) itself, which is the zero set of an empty set of polynomials (or, if you don't like this, of the zero polynomial) and the empty set (which is the zero set of the (homogeneous) equation $1 = 0$). Plane algebraic curves are zero sets in $\mathbb{A}^2 K$ of a single polynomial in two variables (or of a homogeneous polynomial in three variables in the case of the projective plane).

An important class of affine algebraic prevarieties are hypersurfaces: these are the zero sets of a single polynomial. Another well studied class consists of quadrics, the zero sets of polynomials of degree 2; conics are examples of quadrics in the plane. Examples of higher dimensional quadrics are the sphere $x^2 + y^2 + z^2 = 1$ or elliptic curves (!) given as the intersection of two quadrics $ax^2 + by^2 + cz^2 = 0$, $ey^2 + fz^2 + gw^2 = 0$ in $\mathbb{P}^3 K$ under suitable conditions guaranteeing smoothness.

As a first example, let us see how to find rational points on the sphere $S : x^2 + y^2 + z^2 = 1$ starting from the known point $P = (-1, 0, 0)$. The idea is clear: intersect lines through P with S. Lines through a point (u, v, w) are described by the equations $x = u + at$, $y = v + bt$, $z = w + ct$ (the constants a, b, c describe the "slopes" of the lines; of course they are not allowed to vanish simultaneously). For our P we get $x = -1 + at$, $y = bt$, $z = ct$; plugging this

into the equation for S we find $(-1+at)^2+b^2t^2+c^2t^2=1$. The value $t=0$ gives the known point P, so we should factor out t: we get $t(a^2t+b^2t+c^2t-2a)=0$. Thus the second point of intersection is given by $t=\frac{2a}{a^2+b^2+c^2}$, and we find the parametrization

$$x=\frac{a^2-b^2-c^2}{a^2+b^2+c^2},\quad y=\frac{2ab}{a^2+b^2+c^2},\quad z=\frac{2ac}{a^2+b^2+c^2}.$$

Geometrically it is clear that every point $\neq P$ on S is parametrized by these equations, and P itself is parametrized for $a=0$ and arbitrary values of b and c (not both zero).

We will have to deal with singular points on algebraic varieties; postponing the general definition for now, let us simply remark that for hypersurfaces, singular points are those in which all the partial derivatives vanish. In order to find the singular points of the cubic surface $X^2+Y^3-Y^2+Z^2=0$, let us homogenize. We find $F(X,Y,Z,W)=X^2W+Y^3-Y^2W+Z^2W$, hence

$$\begin{aligned}F_X&=2XW,\\F_Y&=3Y^2-2YW,\\F_Z&=2ZW,\\F_W&=X^2-Y^2+Z^2.\end{aligned}$$

If $w=0$, then $y=0$, and the partials all vanish if and only if $x^2+z^2=0$. Since $x\neq 0$, we can rescale and assume that $x=1$; then $z=pmi$, and we have exactly two singular points $[1:0:\pm i:0]$ at infinity.

In the affine space, we have $w=1$, and then we find $x=y=z=0$, hence the origin $[0:0:0:1]$ is the unique singular point in the affine part of the surface.

This singularity can be used to parametrize the cubic surface: the lines through the origin are given by $X=at$, $Y=bt$, $Z=ct$. Intersection with the affine surface gives $t^2(a^2+b^3t-b^2+c^2)=0$, hence the second point of intersection satisfies $t=\frac{b^2-a^2-c^2}{b^3}$. This provides us with the parametrization

$$x=\frac{a(b^2-a^2-c^2)}{b^3},\quad y=\frac{b^2-a^2-c^2}{b^2},\quad z=\frac{c(b^2-a^2-c^2)}{b^3}.$$

The point P is again parametrized infinitely often: just pick any rational numbers with $a^2+c^2=b^2$.

12.2 From Ideals to Varieties

To any ideal I in $K[X_1,\ldots,X_n]$ we can attach a variety

$$\mathcal{V}(I)=\{P\in\mathbb{A}^nK : f(P)=0 \text{ for all } f\in I\}.$$

In fact, this is a variety by Hilbert's basis theorem (see below), according to which every ideal in $K[X_1,\ldots,X_n]$ is finitely generated. Thus $\mathcal{V}(I)$ really can be written as the zero set of a finite list $f_1,\ldots,f_m$ of polynomials.

Proposition 12.2.1. *The map $\mathcal{V}$ from ideals in $R = K[X_1, \ldots, X_n]$ to affine varieties in $\mathbb{A}^n K$ has the following properties:*

1. $\mathcal{V}(0) = \mathbb{A}^n K$; $\mathcal{V}(R) = \varnothing$;
2. $I \subseteq J$ *implies* $\mathcal{V}(I) \supseteq \mathcal{V}(J)$;
3. $\mathcal{V}(I \cap J) = \mathcal{V}(I) \cup \mathcal{V}(J)$;
4. $\mathcal{V}(\sum I_\nu) = \bigcap \mathcal{V}(I_\nu)$.

Here I, J, I_ν are ideals in R, and $\sum I_\nu$ denotes the ideal consisting of finite R-linear combinations of elements in the I_ν.

Proof. 1. These properties are clear.

2. If $I \subseteq J$, then $\mathcal{V}(J) \subseteq \mathcal{V}(I)$.

3. We have $\mathcal{V}(I) \subset \mathcal{V}(I \cap J)$ since $I \cap J \subset I$. Similarly $\mathcal{V}(J) \subset \mathcal{V}(I \cap J)$, hence $\mathcal{V}(I) \cup \mathcal{V}(J) \subset \mathcal{V}(I \cap J)$.

   Now assume that $P \in \mathcal{V}(I \cap J)$. If P is not in $\mathcal{V}(I)$, then there is some $f \in I$ with $f(P) \neq 0$. Similarly, if P is not in $\mathcal{V}(J)$, then there is some $g \in J$ with $g(P) \neq 0$. Then $fg \in I \cap J$ and $fg(P) \neq 0$: contradiction.

4. Let $P \in \bigcap \mathcal{V}(I_\nu)$; then $f_\nu(P) = 0$ for all $f_\nu \in I_\nu$, hence $f(P) = 0$ for all finite linear combinations $f \in \sum I_\nu$. This shows that $\bigcap \mathcal{V}(I_\nu) \subseteq \mathcal{V}(\sum I_\nu)$.

   On the other hand, $I_\mu \subset \sum I_\nu$ for every μ, hence $\mathcal{V}(\sum I_\nu) \subseteq \mathcal{V}(I_\mu)$ for every μ, and therefore $\mathcal{V}(\sum I_\nu) \subseteq \bigcap \mathcal{V}(I_\mu)$.

□

Note that this proposition (in particular (1), (3) and (4)) implies that the algebraic varieties in $\mathbb{A}^n K$ form the closed sets of a topology on $\mathbb{A}^n K$; this topology is called the Zariski topology.

Lemma 12.2.2. *The Zariski-closed sets in $\mathbb{A}^1 K$ are the finite subsets (finite sets of points) and $\mathbb{A}^1 K$ itself.*

12.3 From Varieties to Ideals: The Vanishing Ideal

Assume that V is an affine algebraic variety, defined as the zero set of polynomials $f_1, \ldots, f_m \in K[X_1, \ldots, X_n]$. For any $P = (a_1, \ldots, a_n) \in V$ we have $f_j(P) = 0$. Thus $f(P) = 0$ for any K-linear combination f of the f_i. This shows that $f(a) = 0$ for all $f \in (f_1, \ldots, f_n)$. Thus we are led to define the vanishing ideal

$$\mathcal{I} = \{f \in K[X_1, \ldots, X_n] : f(P) = 0 \text{ for all } P \in V\}$$

of the variety V. Note that $\mathcal{I}(\varnothing) = K[X_1, \ldots, X_n]$. If K has infinitely many elements, then $\mathcal{I}(\mathbb{A}^n K) = (0)$.

Lemma 12.3.1. *For any variety V we have $\mathcal{V}(\mathcal{I}(V)) = V$.*

Proof. We clearly have $V \subseteq \mathcal{V}(\mathcal{I}(V))$: if $f \in \mathcal{I}(V)$, then $f(P) = 0$ for any $P \in V$, hence $P \in \mathcal{V}(\mathcal{I}(V))$.

Now assume that V is the zero set of polynomials $f_1, \dots, f_m \in K[X_1, \dots, X_n]$. Then $f_1, \dots, f_m \in \mathcal{I}(V)$, hence $(f_1, \dots, f_m) \subseteq \mathcal{I}(V)$, and therefore $\mathcal{V}(\mathcal{I}(V)) \subset \mathcal{V}(f_1, \dots, f_m) = V$. $\square$

We have seen that any ideal I in $K[X_1, \dots, X_n]$ gives rise to a variety $\mathcal{V}(I)$, and every variety V can be obtained this way. Conversely, does every ideal I have the form $I = \mathcal{I}(V)$ for some variety V? The answer is no: for example, the ideal $I = (X^2)$ in $K[X, Y]$ is not of the form $\mathcal{I}(V)$: in fact, assume that $\mathcal{I}(V) = I$. Then $V = \mathcal{V}(\mathcal{I}(V)) = \mathcal{V}(I)$, hence V consists of the y-axis. But then $\mathcal{I}(V) = (X)$, and this ideal is strictly larger than I.

There is a second problem: if we work in the affine plane over $K = \mathbb{R}$, then $\mathcal{V}(I) = \varnothing$ for $I = (X^2 + Y^2 + 1)$, whereas $\mathcal{I}(\mathcal{V}(I)) = \mathcal{I}(\varnothing) = \mathbb{R}[X, Y] \neq I$. Thus if we want a bijection between ideals and varieties, then we will have to assume that K is algebraically closed.

In order to clarify the first problem, let us introduce the radical $\operatorname{rad} I$ of an ideal I in any ring R by

$$\operatorname{rad} I = \{f \in R : f^m \in I \text{ for some } m \in \mathbb{N}\}.$$

It is an easy exercise to check that $\operatorname{rad} I$ is an ideal; the only difficulty consists in showing that $\operatorname{rad} I$ is closed under addition: assume that $f, g \in \operatorname{rad} I$. Then $f^n, g^m \in I$ for suitably chosen integers $n, m \geq 0$, hence $(f + g)^r = \sum \binom{r}{k} f^k g^{r-k} \in I$ as soon as $r \geq m + n - 1$.

Note that $I \subseteq \operatorname{rad} I$ for every ideal I. Moreover, $\operatorname{rad}(X^2) = (X)$. Note that if R is a UFD and $f = f_1^{a_1} \cdots f_n^{a_n}$, then $\operatorname{rad}(f) = (f_1 \cdots f_n)$. Compare this with our use of rad in Mason's theorem.

Proposition 12.3.2. *If V is an algebraic variety, then $\mathcal{I}(V) = \operatorname{rad} \mathcal{I}(V)$.*

Thus vanishing ideals have the property that they coincide with their radical. In particular, (X^2) can never be the vanishing ideal of a variety because $\operatorname{rad}(X^2) = (X)$.

Proof. Since $I \subseteq \operatorname{rad} I$ for any ideal I, we only have to show that $\operatorname{rad} \mathcal{I}(V) \subseteq \mathcal{I}(V)$. Assume therefore that $f \in \operatorname{rad} \mathcal{I}(V)$. Then $f^n \in \mathcal{I}(V)$ for some n, hence $f^n(P) = 0$ for all $P \in V$. But this implies $f(P) = 0$, hence $f \in \mathcal{I}(V)$. $\square$

Thus we only can hope to get a bijection between affine algebraic varieties and radical ideals (these are ideals that coincide with their radical). This is exactly what happens:

Proposition 12.3.3. *For any ideal I in R we have $\mathcal{I}(\mathcal{V}(I)) = \operatorname{rad} I$.*

The proof of this proposition is nontrivial; actually it is a consequence of Hilbert's Nullstellensatz, which we will prove below.

12.4 Hilbert's Basis Theorem

We start with the following result:

Proposition 12.4.1. *Let R be a ring. The following assertions are equivalent:*

1. *Every ideal I in R is finitely generated, i.e., can be written in the form $I = (a_1, \ldots, a_m)$ for $a_i \in R$.*
2. *R satisfies the ascending chain condition, i.e., every chain $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ becomes stationary: there is some index N such that $I_N = I_{N+1} = \ldots$.*

A ring R is called Noetherian if the conditions in Prop. 12.4.1 are satisfied.

Proof. (1) $\Longrightarrow$ (2). Let $I_1 \subseteq I_2 \subseteq \ldots$ be an ascending chain of ideals and put $I = \bigcup I_\nu$. Then I is an ideal, hence finitely generated: $I = (a_1, \ldots, a_m)$. We have $a_i \in I_{\nu(i)}$ for some $\nu(i)$; let $N = \max \nu(i)$. Then $a_1, \ldots, a_m \in I_\nu$ for every $\nu \geq N$, hence $I \subseteq I_\nu \subseteq I$, and we are done.

Conversely let I be a nonzero ideal in R, and let $a_1 \in I \setminus (0)$. If $I = (a_1)$, we are done, if not then pick $a_2 \in I \setminus (a_1)$ and continue. In this way we get a strictly increasing ascending chain of ideals $(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \ldots$. This shows that the process must terminate. $\square$

Clearly, every field K is Noetherian since K has only two ideals (0) and (1). Every principal ideal ring (such as $\mathbb{Z}$) is also Noetherian because in such rings every ideal is generated by a single element.

Proposition 12.4.2. *For every ideal I in some Noetherian ring R, the quotient R/I is also Noetherian.*

Hilbert's Basis Theorem is a method for constructing lots of Noetherian rings:

Theorem 12.4.3. *If R is Noetherian, then so is $R[X]$.*

In particular, the rings $K[X_1, \ldots, X_n]$ are Noetherian. In fact, $K[X]$ is Noetherian because K is, and then $K[X, Y]$ is Noetherian because $K[X]$ is etc.

Proof. Let I be an ideal in $R[X]$. We claim that I is finitely generated. Choose $f_1 \in I \setminus (0)$ with minimal degree; if $I \neq (f_1)$, choose $f_2 \in I \setminus (f_1)$ with minimal degree. If this process terminates, we are done. If not, let a_i be the leading coefficient of f_i, and form the ideal $J = (a_1, a_2, a_3, \ldots)$ in R. Since R is Noetherian, we have $J = (a_1, \ldots, a_N)$ for some N.

We now claim that $I = I_N := (f_1, \ldots, f_N)$. If not, then $f_{N+1} \in I \setminus I_N$. Moreover, $a_{N+1} = \sum_{i=1}^N r_i a_i$ since $a_{N+1} \in J$. Now set

$$g = \sum_{i=0}^{N} r_i f_i x^{\deg f_{N+1} - \deg f_i}.$$

Since g is a linear combination of the f_i, we have $g \in I_N$. Next $\deg g = \deg f_{N+1}$, and both polynomials have the same leading term. Thus $\deg(f_{N+1} - g) < \deg f_{N+1}$, hence $f_{N+1} - g \in I \setminus I_N$; but this contradicts the minimality of $\deg f_{N+1}$. $\square$

12.5 Hilbert's Nullstellensatz

Recall that an ideal $\mathfrak{p}$ in a ring is prime if $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$; it is then easily seen that $\mathfrak{p}$ is prime if and only if $R/\mathfrak{p}$ is a domain. In fact, assume that $R/\mathfrak{p}$ is a domain, and let $ab \in \mathfrak{p}$. Then $0 = ab + \mathfrak{p} = (a + \mathfrak{p})(b + \mathfrak{p})$, and since $R/\mathfrak{p}$ is a domain, we get $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$: thus $\mathfrak{p}$ is prime. Conversely, if $\mathfrak{p}$ is prime and $(a + \mathfrak{p})(b + \mathfrak{p}) = 0$, then $ab \in \mathfrak{p}$, hence $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$, and this shows that $R/\mathfrak{p}$ is a domain.

Moreover, an ideal $\mathfrak{m}$ is maximal if $\mathfrak{m} \subseteq \mathfrak{n} \subseteq R$ for some ideal $\mathfrak{n}$ implies that $\mathfrak{m} = \mathfrak{n}$ or $\mathfrak{n} = R$; again it is easy to see that $\mathfrak{m}$ is maximal if and only if $R/\mathfrak{m}$ is a field.

For the rest of this chapter, let K be an algebraically closed field.

Theorem 12.5.1 (Weak Nullstellensatz)**.** *Let K be an algebraically closed field. Then every maximal ideal in the polynomial ring $R = K[X_1, \ldots, X_n]$ has the form $M = (X_1 - a_1, \ldots, X_n - a_n)$ for some point $P = (a_1, \ldots, a_n) \in \mathbb{A}^n K$.*

Note that the weak Nullstellensatz gives us a bijection between maximal ideals in $K[X_1, \ldots, X_n]$ and points in $\mathbb{A}^n K$. Also observe that the theorem does not hold for arbitrary fields: in $\mathbb{R}[X]$, the ideal $M = (X^2 + 1)$ is maximal because $\mathbb{R}[X]/(X^2+1) \simeq \mathbb{C}$ is a field, yet M is not of the form $(X - a)$ for some $a \in \mathbb{R}$.

As a consequence we have

Corollary 12.5.2 (Nullstellensatz)**.** *Let K be an algebraically closed field and $I \neq (1)$ be an ideal in $K[X_1, \ldots, X_n]$. Then $\mathcal{V}(I) \neq \varnothing$.*

Proof. If $I \neq R = K[X_1, \ldots, X_n]$, then there is some maximal ideal M with $I \subseteq M$ (this follows from the ascending chain condition: if I is maximal, we are done; if not then there is some I_1 sandwiched between I and R; now repeat and observe that this process must end eventually). Now $M = (X_1 - a_1, \ldots, X_n - a_n)$ by the weak Nullstellensatz, hence $f(P) = 0$ for $P = (a_1, \ldots, a_n)$ and any $f \in I$. In particular, $P \in \mathcal{V}(I)$. $\square$

Another consequence is

Corollary 12.5.3. *For any ideal I in $R = K[X_1, \ldots, X_n]$ we have $\mathcal{I}(\mathcal{V}(I)) = \operatorname{rad} I$. In particular, if I is a radical ideal, then $\mathcal{I}(\mathcal{V}(I)) = I$.*

Thus $\mathcal{I}$ and $\mathcal{V}$ set up a one-to-one correspondence between radical ideals in $K[X_1, \ldots, X_n]$ and affine algebraic varieties in $\mathbb{A}^n K$.

Proof. Let $I = (f_1, \ldots, f_m)$. Then $g \in \mathcal{I}(\mathcal{V}(I))$ if $g(P) = 0$ for any $P \in \mathcal{V}(I)$. We have to prove that some power of g lies in I.

The following proof is called the trick of Rabinowitsch. Adjoin a new variable X_{n+1} to R, i.e., let $S = R[X_{n+1}]$. Then the polynomials $f_1, \ldots, f_m$ and $X_{n+1}g - 1$ have no common zeros in $\mathbb{A}^{n+1}K$, so by the weak Nullstellensatz we must have

$$1 = p_1 f_1 + \ldots + p_m f_m + p_{m+1}(X_{n+1}g - 1),$$

where $p_j \in S$. Now plug in $X_{n+1} = \frac{1}{g}$ (the result will be an element in $K(X_1, \ldots, X_n)$. This gives

$$1 = p_1(x_1, \ldots, x_n, 1/g)f_1 + \ldots + p_m(x_1, \ldots, x_n, 1/g)f_m.$$

Now multiply through by a power of g to clear denominators; the resulting equation then shows that this power of g is in I. $\square$

For the proof of the Nullstellensatz we need the following lemma (whose proof is due to D. Allcock):

Lemma 12.5.4. *Let k be a field and K/k an extension which is finitely generated as a k-algebra. Then K/k is algebraic.*

We will give the proof later; for now let me explain what this means. Recall that an algebra is, cum grano salis, a vector space in which vectors can be multiplied. For example, the polynomial ring $A = K[X_1, \ldots, X_n]$ is also a K-vector space and therefore a K-algebra: elements in A can be added (as vectors), multiplied by scalars from K, and can be multiplied as polynomials.

If K/k is a field extension, then we can interpret K as a k-vector space: we can add and subtract elements of K and multiply them by the "scalars" from k. Since the "vectors" in K can also be multiplied as elements of K, we see that K actually is a k-algebra.

A k-algebra K is now said to be finitely generated if there are elements α_1, $\ldots$, α_m such that every $\alpha \in K$ can be written as a k-linear combination of products of the α_i; in other words: if the k-algebra generated by the α_i is equal to K.

As an example, consider the $\mathbb{Q}$-algebra $\mathbb{Q}(X)$ of rational functions in one variable X. The $\mathbb{Q}$-algebra generated by $f = \frac{1}{X}$ and $g = \frac{X-1}{X+1}$ consists of all $\mathbb{Q}$-linear combinations of f, g, f^2, fg, g^2, $\ldots$. Note that all such elements have poles at most at $x = 0$ and $x = -1$.

Now we claim that $\mathbb{Q}(X)$ is not finitely generated as a $\mathbb{Q}$-algebra. If it were, then there would be rational functions $f_1, \ldots, f_n$ such that every rational function $f \in \mathbb{Q}(X)$ can be written as a linear combination of products of the f_j. But this is not possible: the f_i have finitely many poles, and by forming products and linear combinations no new poles are created. Thus if $a \in \mathbb{Q}$ is not one of the finitely many poles, then $\frac{1}{X-a}$ is not an element of the $\mathbb{Q}$-algebra generated by the f_i.

Proof of the Weak Nullstellensatz. Let $\mathfrak{m}$ be a maximal ideal in R. Then $R/\mathfrak{m}$ is a field. Moreover, it is obviously finitely generated as a k-algebra, namely by the elements $X_1+\mathfrak{m}, \ldots, X_n+\mathfrak{m}$: every element in R is a k-linear combination of products of the X_i, hence every element in $R/\mathfrak{m}$ is a k-linear combination of products of the $X_i+\mathfrak{m}$. Observe that $R/\mathfrak{m}$ contains k as a subfield: the map $\phi : k \longrightarrow R/\mathfrak{m}; a \longmapsto a+\mathfrak{m}$ is a ring homomorphism, and we have $\ker\phi = \{a \in k : a \in \mathfrak{m}\} = k \cap \mathfrak{m}$. If $\mathfrak{m}$ contains a nonzero element $a \in k$, then it contains 1 and is therefore equal to R. Since $\mathfrak{m}$ is maximal, this cannot happen, hence $k \cap \mathfrak{m} = (0)$, and ϕ is injective.

Thus $R/\mathfrak{m}$ is a field extension of k, and by Lemma 12.5.4 we find that it is algebraic over k. But k is algebraically closed, hence $R/\mathfrak{m} = k$.

Now consider the natural projection $\pi : R \longrightarrow R/\mathfrak{m} = k$ sending $f \in R$ to the coset $f+\mathfrak{m}$. Since $\pi(x_j) = a_j$ for $a_j \in k$, the elements $x_j - a_j$ are in the kernel of π, which is by definition just $\mathfrak{m}$. Thus $\mathfrak{m}$ contains $(X_1 - a_1, \ldots, X_n - a_n)$; this last ideal is maximal, and since $\mathfrak{m}$ is also maximal, we must have equality: $\mathfrak{m} = (X_1 - a_1, \ldots, X_n - a_n)$. $\square$

In order to get an idea for the proof of Lemma 12.5.4, let us first consider the special case where k is infinite and where $K = k(X)$ is a simple transcendental extension. Our claim is that if $f_1, \ldots, f_m \in K$, then the k-algebra A they generate is strictly smaller than K. In fact, choose $a \in k$ such that a is not a pole of any of the rational functions f_j; then no element of A can have a pole at a, hence $\frac{1}{X-a} \in K \setminus A$.

Now we complete the proof of the Nullstellensatz by proving the central lemma:

Proof of Lemma 12.5.4. In order to simplify the presentation, we will assume that k is algebraically closed, although the proof for general fields k is only slightly more complicated.

We first give the proof for fields K with transcendence degree 1 over k and then do the general case later. Recall that K/k has transcendence degree 1 if there is some $X \in K$ such that $K/k(X)$ is finite.

As before, let $f_1, \ldots, f_m \in K$, and let A be the k-algebra these rational functions generate. Since $K/k(X)$ is finite, there exist elements $e_1, \ldots, e_n \in K$ that form a basis for the vector space K over $k(X)$. The product $e_i e_j$ of two basis elements can be expressed as a $k(X)$-linear combination of the e_h, hence there exist polynomials $a_{ijh}, b_{ijh} \in k[X]$ with

$$e_i e_j = \sum_h \frac{a_{ijh}(X)}{b_{ijh}(X)}\, e_h.$$

We also can express our f_i in terms of this basis:

$$f_i = \sum_j \frac{c_{ij}(X)}{d_{ij}(X)}\, e_j$$

for polynomials $c_{ij}, d_{ij} \in k[X]$.

Now observe that the poles of the elements in A must come from the finitely many poles of the e_j, the roots of the finitely many polynomials d_{ij}, or the roots of the finitely many polynomials b_{ijh}. Thus there is some $a \in k$ (here we use that k is algebraically closed) that is not among these poles, and then $\frac{1}{X-a} \in K \setminus A$.

Now let us do the general case of fields K with arbitrary transcendence degree ≥ 1. Let F be a subextension of K such that K/F has transcendence degree 1. From what we have proved we know that K is not a finitely generated F-algebra; this immediately shows that it is not a finitely generated k-algebra. $\square$