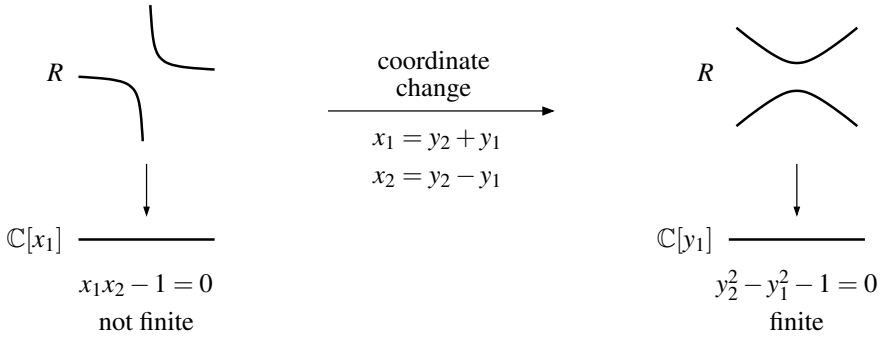
10. Noether Normalization and Hilbert's Nullstellensatz

In the last chapter we have gained much understanding for integral and finite ring extensions. We now want to prove an elementary but powerful theorem stating that every finitely generated algebra R over a field K (so in particular every coordinate ring of a variety by Remark 1.31) is a finite extension ring of a polynomial ring $K[z_1,\dots,z_r]$ — and hence of a very simple K-algebra that is easy to deal with. Let us start by giving the geometric idea behind this so-called Noether Normalization theorem, which is in fact very simple.

Example 10.1 (Idea of Noether Normalization)**.** Let $R = \mathbb{C}[x_1,x_2]/(x_1x_2-1)$ be the coordinate ring of the variety $X = V(x_1x_2-1) \subset \mathbb{A}^2_{\mathbb{C}}$ as in Example 9.4 (b). We know already that R is not integral (and hence not finite) over $\mathbb{C}[x_1]$; this is easily seen geometrically in the picture below on the left since this map does not satisfy the Lying Over property for the origin as in Example 9.19.



It is easy to change this however by a linear coordinate transformation: if we set e. g. $x_1 = y_2 + y_1$ and $x_2 = y_2 - y_1$ then we can write R also as $R = \mathbb{C}[y_1,y_2]/(y_2^2 - y_1^2 - 1)$, and this is now finite over $\mathbb{C}[y_1]$ by Proposition 9.5 since the polynomial $y_2^2 - y_1^2 - 1$ is monic in y_2. Geometrically, the coordinate transformation has tilted the space X as in the picture above on the right so that e. g. the Lying Over property now obviously holds. Note that this is not special to the particular transformation that we have chosen; in fact, "almost any" linear coordinate change would have worked to achieve this goal.

In terms of geometry, we are therefore looking for a change of coordinates so that a suitable coordinate projection to some affine space $\mathbb{A}^r_K$ then corresponds to a finite ring extension of a polynomial ring over K in r variables. Note that this number r can already be thought of as the "dimension" of X (a concept that we will introduce in Chapter 11) as finite ring extensions correspond to surjective geometric maps with finite fibers by Example 9.19, and thus should not change the dimension (we will prove this in Lemma 11.8).

As we have seen above already, the strategy to achieve our goal is to find a suitable change of coordinates so that the given relations among the variables become monic. The first thing we have to do is therefore to prove that such a change of coordinates is always possible. It turns out that a *linear* change of coordinates works in general only for infinite fields, whereas for arbitrary fields one has to allow more general coordinate transformations.

18

Lemma 10.2. *Let $f \in K[x_1,\dots,x_n]$ be a non-zero polynomial over an infinite field K. Assume that f is homogeneous, i. e. every monomial of f has the same degree (in the sense of Exercise 0.16).*

Then there are $a_1,\dots,a_{n-1} \in K$ such that $f(a_1,\dots,a_{n-1},1) \neq 0$.

Proof. We will prove the lemma by induction on n. The case $n = 1$ is trivial, since a homogeneous polynomial in one variable is just a constant multiple of a monomial.

So assume now that $n > 1$, and write f as $f = \sum_{i=0}^{d} f_i x_1^i$ where the $f_i \in K[x_2, \dots, x_n]$ are homogeneous of degree $d - i$. As f is non-zero, at least one f_i has to be non-zero. By induction we can therefore choose $a_2, \dots, a_{n-1}$ such that $f_i(a_2, \dots, a_{n-1}, 1) \neq 0$ for this i. But then $f(\cdot, a_2, \dots, a_{n-1}, 1) \in K[x_1]$ is a non-zero polynomial, so it has only finitely many zeroes. As K is infinite, we can therefore find $a_1 \in K$ such that $f(a_1, \dots, a_{n-1}, 1) \neq 0$. □

Lemma 10.3. *Let $f \in K[x_1, \dots, x_n]$ be a non-zero polynomial over an infinite field K. Then there are $\lambda \in K$ and $a_1, \dots, a_{n-1} \in K$ such that*

$$\lambda\, f(y_1 + a_1 y_n, y_2 + a_2 y_n, \dots, y_{n-1} + a_{n-1} y_n, y_n) \quad \in K[y_1, \dots, y_n]$$

is monic in y_n (i. e. as an element of $R[y_n]$ with $R = K[y_1, \dots, y_{n-1}]$).

Proof. Let d be the degree of f in the sense of Exercise 0.16, and write $f = \sum_{k_1,\dots,k_n} c_{k_1,\dots,k_n} x_1^{k_1} \cdots x_n^{k_n}$ with $c_{k_1,\dots,k_n} \in K$. Then the leading term of

$$\begin{aligned} &\lambda\, f(y_1 + a_1 y_n, y_2 + a_2 y_n, \dots, y_{n-1} + a_{n-1} y_n, y_n) \\ &\quad = \lambda \sum_{k_1,\dots,k_n} c_{k_1,\dots,k_n} (y_1 + a_1 y_n)^{k_1} \cdots (y_{n-1} + a_{n-1} y_n)^{k_{n-1}} y_n^{k_n} \end{aligned}$$

in y_n is obtained by always taking the second summand in the brackets and only keeping the degree-d terms, i. e. it is equal to

$$\lambda \sum_{\substack{k_1,\dots,k_n \\ k_1+\cdots+k_n = d}} c_{k_1,\dots,k_n} a_1^{k_1} \cdots a_{n-1}^{k_{n-1}} y_n^{k_1+\cdots+k_n} = \lambda\, f_d(a_1, \dots, a_{n-1}, 1)\, y_n^d,$$

where f_d is the (homogeneous) degree-d part of f. Now pick $a_1, \dots, a_{n-1}$ by Lemma 10.2 such that $f_d(a_1, \dots, a_{n-1}, 1) \neq 0$, and set $\lambda = f_d(a_1, \dots, a_{n-1}, 1)^{-1}$. □

Exercise 10.4. Let $f \in K[x_1, \dots, x_n]$ be a non-zero polynomial over an arbitrary field K. Prove that there are $\lambda \in K$ and $a_1, \dots, a_{n-1} \in \mathbb{N}$ such that

$$\lambda\, f(y_1 + y_n^{a_1}, y_2 + y_n^{a_2}, \dots, y_{n-1} + y_n^{a_{n-1}}, y_n) \quad \in K[y_1, \dots, y_n]$$

is monic in y_n.

Proposition 10.5 (Noether Normalization). *Let R be a finitely generated algebra over a field K, with generators $x_1, \dots, x_n \in R$. Then there is an injective K-algebra homomorphism $K[z_1, \dots, z_r] \to R$ from a polynomial ring over K to R that makes R into a finite extension ring of $K[z_1, \dots, z_r]$.*

Moreover, if K is an infinite field the images of $z_1, \dots, z_r$ in R can be chosen to be K-linear combinations of $x_1, \dots, x_n$.

Proof. We will prove the statement by induction on the number n of generators of R. The case $n = 0$ is trivial, as we can then choose $r = 0$ as well.

So assume now that $n > 0$. We have to distinguish two cases:

(a) There is no algebraic relation among the $x_1, \dots, x_n \in R$, i. e. there is no non-zero polynomial f over K such that $f(x_1, \dots, x_n) = 0$ in R. Then we can choose $r = n$ and the map $K[z_1, \dots, z_n] \to R$ given by $z_i \mapsto x_i$ for all i, which is even an isomorphism in this case.

(b) There is a non-zero polynomial f over K such that $f(x_1, \dots, x_n) = 0$ in R. Then we choose λ and $a_1, \dots, a_{n-1}$ as in Lemma 10.3 (if K is infinite) or Exercise 10.4 (for any K) and set

$$\begin{aligned} &y_1 := x_1 - a_1 x_n,\ \dots,\ y_{n-1} := x_{n-1} - a_{n-1} x_n,\ y_n := x_n \\ &\qquad \text{(so that } x_1 = y_1 + a_1 y_n,\ \dots,\ x_{n-1} = y_{n-1} + a_{n-1} y_n,\ x_n = y_n\text{)} \\ \text{or}\quad &y_1 := x_1 - x_n^{a_1},\ \dots,\ y_{n-1} := x_{n-1} - x_n^{a_{n-1}},\ y_n := x_n \\ &\qquad \text{(so that } x_1 = y_1 + y_n^{a_1},\ \dots,\ x_{n-1} = y_{n-1} + y_n^{a_{n-1}},\ x_n = y_n\text{)}, \end{aligned}$$

respectively. Note that in both cases these relations show that the K-subalgebra $K[y_1,\dots,y_n]$ of R generated by $y_1,\dots,y_n \in R$ is the same as that generated by $x_1,\dots,x_n$, i. e. all of R. Moreover, y_n is integral over the K-subalgebra $K[y_1,\dots,y_{n-1}]$ of R, since

$$\lambda f(y_1 + a_1 y_n, \dots, y_{n-1} + a_{n-1} y_n, y_n) \quad \text{or} \quad \lambda f(y_1 + y_n^{a_1}, \dots, y_{n-1} + y_n^{a_{n-1}}, y_n),$$

respectively, is monic in y_n and equal to $\lambda f(x_1,\dots,x_n) = 0$. Hence $R = K[y_1,\dots,y_n]$ is finite over $K[y_1,\dots,y_{n-1}]$ by Proposition 9.5. In addition, the subalgebra $K[y_1,\dots,y_{n-1}]$ of R is finite over a polynomial ring $K[z_1,\dots,z_r]$ by the induction hypothesis, and thus R is finite over $K[z_1,\dots,z_r]$ by Lemma 9.6 (a).

Moreover, if K is infinite we can always choose the coordinate transformation of Lemma 10.3, and thus $y_1,\dots,y_n$ (i. e. also the images of $z_1,\dots,z_r$ by induction) are linear combinations of $x_1,\dots,x_n$. □

Remark 10.6. Let $R = A(X)$ be the coordinate ring of a variety X over a field K.

(a) In the Noether Normalization of Proposition 10.5, the (images of) $z_1,\dots,z_r$ in R are algebraically independent functions on X in the sense that there is no polynomial relation among them with coefficients in K. On the other hand, every other element of R is algebraically dependent on $z_1,\dots,z_r$, i. e. it satisfies a (monic) polynomial relation with coefficients in $K[z_1,\dots,z_r]$. We can therefore think of r as the "number of parameters" needed to describe X, i. e. as the "dimension" of X as already mentioned in Example 10.1. In fact, we will see in Remark 11.10 that the number r in Proposition 10.5 is uniquely determined to be the dimension of X in the sense of Chapter 11.

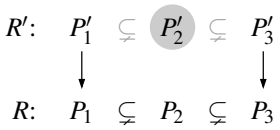
(b) As one would have guessed already from the geometric picture in Example 10.1, the proof of Lemma 10.2 shows that most choices of linear coordinate transformations are suitable to obtain a Noether normalization: in each application of this lemma, only finitely many values of $a_1 \in K$ have to be avoided. Hence we can translate Proposition 10.5 into geometry by saying that a sufficiently general projection to an r-dimensional linear subspace corresponds to a finite ring extension, and hence to a surjective map with finite fibers (where r is the dimension of X as in (a)).

Exercise 10.7. Find a Noether normalization of the $\mathbb{C}$-algebra $\mathbb{C}[x,y,z]/(xy+z^2, x^2y - xy^3 + z^4 - 1)$.

Exercise 10.8. Let $R \subset R'$ be an integral ring extension, and assume that R is a finitely generated algebra over some field K. Moreover, let $P_1 \subsetneq P_3$ be prime ideals in R and $P_1' \subsetneq P_3'$ be prime ideals in R' such that $P_1' \cap R = P_1$ and $P_3' \cap R = P_3$.

(a) Prove: If there is a prime ideal P_2 in R with $P_1 \subsetneq P_2 \subsetneq P_3$, then there is also a prime ideal P_2' in R' with $P_1' \subsetneq P_2' \subsetneq P_3'$.

(b) Can we always find P_2' in (a) such that in addition $P_2' \cap R = P_2$ holds?



As an important application of Noether Normalization we can now give rigorous proofs of some statements in our dictionary between algebra and geometry, namely of the correspondence between (maximal) ideals in the coordinate ring $A(X)$ of a variety X over an algebraically closed field and subvarieties (resp. points) of X. There are various related statements along these lines, and they are all known in the literature by the German name *Hilbert's Nullstellensatz* ("theorem of the zeroes").

Let us start with the simplest instance of this family of propositions. Still very algebraic in nature, it is the statement most closely related to Noether Normalization, from which the geometric results will then follow easily.

Corollary 10.9 (**Hilbert's Nullstellensatz**, version 1)**.** *Let K be a field, and let R be a finitely generated K-algebra which is also a field.*

Then $K \subset R$ is a finite field extension. In particular, if in addition K is algebraically closed then $R = K$.

Proof. By Noether Normalization as in Proposition 10.5 we know that R is finite over a polynomial ring $K[z_1,\dots,z_r]$, and thus also integral over $K[z_1,\dots,z_r]$ by Proposition 9.5. But R is a field, hence $K[z_1,\dots,z_r]$ must be a field as well by Corollary 9.21 (a). This is only the case for $r=0$, and so R is finite over K.

In particular, if K is algebraically closed then there are no algebraic extension fields of K since all zeroes of polynomials over K lie already in K. Hence by Proposition 9.5 there are no finite extensions either in this case, and we must have $R=K$. □

Corollary 10.10 (**Hilbert's Nullstellensatz**, version 2)**.** *Let K be an algebraically closed field. Then all maximal ideals of the polynomial ring $K[x_1,\dots,x_n]$ are of the form*

$$I(a) = (x_1-a_1,\dots,x_n-a_n)$$

for some $a=(a_1,\dots,a_n)\in\mathbb{A}^n_K$.

Proof. Let $P\trianglelefteq K[x_1,\dots,x_n]$ be a maximal ideal. Then $K[x_1,\dots,x_n]/P$ is a field by Lemma 2.3 (b), and in addition certainly a finitely generated K-algebra. Hence $K[x_1,\dots,x_n]/P=K$ by Corollary 10.9, i. e. the natural map $K\to K[x_1,\dots,x_n]/P$, $c\mapsto\overline{c}$ is an isomorphism. Choosing inverse images $a_1,\dots,a_n$ of $\overline{x_1},\dots,\overline{x_n}$ we get $\overline{x_i}=\overline{a_i}$ for all i, and thus $(x_1-a_1,\dots,x_n-a_n)\subset P$. But $(x_1-a_1,\dots,x_n-a_n)$ is a maximal ideal by Example 2.6 (c), and so we must already have $P=(x_1-a_1,\dots,x_n-a_n)=I(a)$. □

Remark 10.11 (Points of a variety correspond to maximal ideals)**.** It is easy to extend Corollary 10.10 to a statement about an arbitrary variety $X\subset\mathbb{A}^n_K$ over an algebraically closed field K: if $R=A(X)$ is the coordinate ring of X we claim that there is a one-to-one correspondence

$$\begin{array}{rcl}\{\text{points of } X\} & \overset{1:1}{\longleftrightarrow} & \{\text{maximal ideals in } A(X)\}\\ a & \longmapsto & I(a)\\ V(I) & \longmapsto & I.\end{array}$$

In fact, the maximal ideals of $A(X)=K[x_1,\dots,x_n]/I(X)$ are in one-to-one correspondence with maximal ideals $I\trianglelefteq K[x_1,\dots,x_n]$ such that $I\supset I(X)$ by Lemma 1.21 and Corollary 2.4. By Corollary 10.10 this is the same as ideals of the form $I(a)=(x_1-a_1,\dots,x_n-a_n)$ containing $I(X)$. But $I(a)\supset I(X)$ is equivalent to $a\in X$ by Lemma 0.9 (a) and (c), so the result follows.

Remark 10.12 (Zeroes of ideals in $K[x_1,\dots,x_n]$)**.** Another common reformulation of Hilbert's Nullstellensatz is that every proper ideal $I\trianglelefteq K[x_1,\dots,x_n]$ in the polynomial ring over an algebraically closed field K has a zero: by Corollary 2.17 we know that I is contained in a maximal ideal, which must be of the form $I(a)$ by Corollary 10.10. But $I\subset I(a)$ implies $a\in V(I)$ by Lemma 0.9 (a) and (c), and hence $V(I)\neq\emptyset$.

Note that this statement is clearly false over fields that are not algebraically closed, as e. g. (x^2+1) is a proper ideal in $\mathbb{R}[x]$ with empty zero locus in $\mathbb{A}^1_{\mathbb{R}}$.

19

In order to extend the correspondence between points and maximal ideals to arbitrary subvarieties we need another algebraic preliminary result first: recall that in any ring R the radical of an ideal I equals the intersection of all prime ideals containing I by Lemma 2.21. We will show now that it is in fact sufficient to intersect all maximal ideals containing I if R is a finitely generated algebra over a field.

Corollary 10.13 (**Hilbert's Nullstellensatz**, version 3)**.** *For every ideal I in a finitely generated algebra R over a field K we have*

$$\sqrt{I} = \bigcap_{\substack{P \text{ maximal}\\ P\supset I}} P.$$

Proof. The inclusion "$\subset$" follows immediately from Lemma 2.21, since every maximal ideal is prime.

For the opposite inclusion "$\supset$", let $f \in R$ with $f \notin \sqrt{I}$; we have to find a maximal ideal $P \supset I$ with $f \notin P$. Consider the multiplicatively closed set $S = \{f^n : n \in \mathbb{N}\}$. As $f \notin \sqrt{I}$ implies $I \cap S = \emptyset$, we get by Exercise 6.14 (a) a prime ideal $P \trianglelefteq R$ with $P \supset I$ and $P \cap S = \emptyset$, in particular with $f \notin P$. Moreover, we can assume by Exercise 6.14 (a) that $S^{-1}P$ is maximal. It only remains to show that P is maximal.

To do this, consider the ring extension $K \to R/P \to (R/P)_f = R_f/P_f$, where the subscript f denotes localization at S as in Example 6.5 (c). Note that the second map is in fact an inclusion since R/P is an integral domain, and the stated equality holds by Corollary 6.22 (b). Moreover, R_f/P_f is a field since P_f is maximal, and finitely generated as a K-algebra (as generators we can choose the classes of generators for R together with $\frac{1}{f}$). So $K \subset R_f/P_f$ is a finite field extension by Corollary 10.9, and hence integral by Proposition 9.5. But then $R/P \subset R_f/P_f$ is integral as well, which means by Corollary 9.21 (a) that R/P is a field since R_f/P_f is. Hence P is maximal by Lemma 2.3 (b). □

Corollary 10.14 (**Hilbert's Nullstellensatz**, version 4)**.** *Let $X \subset \mathbb{A}^n_K$ be a variety over an algebraically closed field K. Then for every ideal $I \trianglelefteq A(X)$ we have $I(V(I)) = \sqrt{I}$.*

In particular, there is a one-to-one correspondence

$$\begin{array}{ccc} \{\textit{subvarieties of } X\} & \overset{1:1}{\longleftrightarrow} & \{\textit{radical ideals in } A(X)\} \\ Y & \longmapsto & I(Y) \\ V(I) & \longmapsfrom & I. \end{array}$$

Proof. Let us first prove the equality $I(V(I)) = \sqrt{I}$.

"$\subset$": Assume that $f \notin \sqrt{I}$. By Corollary 10.13 there is then a maximal ideal $P \trianglelefteq A(X)$ with $P \supset I$ and $f \notin P$. But by Remark 10.11 this maximal ideal has to be of the form $I(a) = (x_1 - a_1, \dots, x_n - a_n)$ for some point $a \in X$. Now $I(a) \supset I$ implies $a \in V(I)$ by Lemma 0.9 (a) and (c), and $f \notin I(a)$ means $f(a) \neq 0$. Hence $f \notin I(V(I))$.

"$\supset$": Let $f \in \sqrt{I}$, i. e. $f^n \in I$ for some $n \in \mathbb{N}$. Then $(f(a))^n = 0$, and hence $f(a) = 0$, for all $a \in V(I)$. This means that $f \in I(V(I))$.

The one-to-one correspondence now follows immediately from what we already know: the two maps are well-defined since $I(Y)$ is always radical by Remark 1.10, and they are inverse to each other by Lemma 0.9 (c) and the statement $I(V(I)) = \sqrt{I}$ proven above. □