Chapter 4

The algebraic-geometric correspondence

4.1 The geometry of elimination

In Chapter 2 we have seen how Gröbner bases can be used for eliminating variables from algebraic equations. A general method for determining the solutions of a system of algebraic equations consists of two major steps:

- elimination: the goal is to "triangularize" the system, i.e. determine polynomials not containing x, and polynomials not containing x and y. Ideally, we would like to get a complete overview of these elimination polynomials.
- extension: after having solved the polynomials containing fewer variables, we would like to extend these partial solutions to solutions containing also coordinates for the other variables.

For the elimination step there are several methods available, such as resultants or Gröbner bases. Gröbner bases have particularly nice theoretical properties. Resultants, on the other hand, are faster to compute.

Def 4.1.1. Let I be an ideal in $K[x_1, \ldots, x_n]$. The *k-th elimination ideal* I_k of I is the ideal in $K[x_{k+1}, \ldots, x_n]$ defined by

$$I_k = I \cap K[x_{k+1}, \ldots, x_n]. \qquad \square$$

These elimination ideals can be determined via the elimination property of Gröbner bases, see Theorem 2.2.5.

So now that we have a complete overview of the elimination step, let us turn to the extension step. Let us first consider an example.

Example 4.1.1. Consider the system

$$\begin{aligned} xy - 1 &= 0, \\ xz - 1 &= 0. \end{aligned}$$

Let I be the ideal generated by these polynomials. A Gröbner basis for I w.r.t. the lexicographic ordering with $x > y > z$ has the form

$$\{\ xz - 1,\quad y - z\ \}.$$

So $I_1 = \langle y - z \rangle$, and $I_2 = \emptyset$. The partial solutions, i.e. the solutions of I_1, are

$$\{(a, a) | a \in \mathbb{C}\}.$$

Such a partial solution can be extended to a complete solution $(1/a, a, a)$ for all $a \in \mathbb{C}$, except for $a = 0$. Geometrically the situation is as follows:

We see that $V(I)$ has no point lying over the partial solution $(0, 0)$. □

The following theorem tells us when we can expect to be able to extend a partial solution.

Theorem 4.1.1. (Extension Theorem) *Let K be an algebraically closed field. Let $I = \langle f_1, \ldots, f_m \rangle$ be an ideal in $K[x_1, \ldots, x_n]$. For each $1 \le i \le m$ write f_i as a polynomial in the main variable x_1, i.e.*

$$f_i = g_i(x_2, \ldots, x_n) x_1^{d_i} + \text{terms of lower degree in } x_1,$$

where $d_i \ge 0$ and $g_i \in K[x_2, \ldots, x_n]$ is nonzero. (W.l.o.g. we assume that all the f_i are nonzero.) Let $(a_2, \ldots, a_n)$ be a partial solution, i.e. $(a_2, \ldots, a_n) \in V(I_1)$. If $(a_2, \ldots, a_n) \notin V(g_1, \ldots, g_m)$, then there exists $a_1 \in K$ such that $(a_1, a_2, \ldots, a_n) \in V(I)$.

Proof: we refer to [Win96], Theorem 4.3.3 for the case of $m = 2$ and to [CLO97], Theorem 3.6.5. □

Observe that the extension theorem is false over fields which are not algebraically closed, such as $\mathbb{R}$. This can be seen in the simple example $\{x^2 - y, x^2 - z\}$.

The elimination ideals of an ideal I loosely correspond to the geometric operation of projection applied to $V = V(I)$. For $1 \le i \le n$ let

$$\pi_i(V) = \{(a_{i+1}, \ldots, a_n) \mid (a_1, \ldots, a_i, a_{i+1}, \ldots, a_n) \in V \text{ for some } a_1, \ldots, a_i \in K\ \}.$$

elimination ideals:	projections:
I_1	$\pi_1(V)$
I_2	$\pi_2(V)$
$\vdots$	$\vdots$
I_n	$\pi_n(V)$

So, for instance, the first elimination ideal I_1 in Example 4.1.1 is $\langle y - z \rangle$, i.e. $V(I_1)$ is the line $y = z$ in the yz–plane. On the other hand, the first projection $\pi_1(V(I))$ is

$$\pi_1(V(I)) = \{(a, a) | a \in \mathbb{C} \setminus \{0\}\}.$$

The projection $\pi_1(V(I))$ is <u>not</u> an algebraic set, since the point $(0, 0)$ is missing. The relation between elimination ideals and projections is given in the following theorem.

Theorem 4.1.2. *Let K be algebraically closed, $V = V(f_1, \ldots, f_m)$ an algebraic set in $\mathbb{A}^n(K)$. Let $I = \langle f_1, \ldots, f_m \rangle$. Let the leading coefficients g_i be as in the Extension Theorem. Then in $\mathbb{A}^{n-1}(K)$ we have the equality*

$$V(I_1) = \pi_1(V) \cup (V(g_1, \ldots, g_m) \cap V(I_1)).$$

Proof: see [CLO97], Chap.3.2. □

Observe that in general $g_i \notin I_1$ (or in a prime component of it), so $V(g_1, \ldots, g_m) \cap V(I_1)$ will be a set of lower dimension than $V(I_1)$. At this point we cannot make this more precise, since we still have to introduce the notion of dimension. So in this case $V(I_1)$ and $\pi_1(V)$ agree "nearly everywhere".

Conversely, we have a theorem which tells us how much smaller than $V(I_1)$ the projection $\pi_1(V)$ could be.

Theorem 4.1.3. (Closure Theorem) *Let K be algebraically closed. Let $I = \langle f_1, \ldots, f_m \rangle$ be an ideal in $K[x_1, \ldots, x_n]$, $V = V(f_1, \ldots, f_m)$. Then:*
(a) *$V(I_k)$ is the smallest algebraic set containing $\pi_k(V)$.*
(b) *If $V \neq \emptyset$, then there is an algebraic set W properly contained in $V(I_k)$ such that $V(I_k) \setminus W \subset \pi_k(V)$.*

Proof: see [CLO97], Chap. 3.2. □

If $V(I_k)$ is irreducible, then W must be of strictly smaller dimension, so that we only have to take away "a few" points from $V(I_k)$ to get $\pi_k(V)$.

4.2 Hilbert's Nullstellensatz

We have already seen in previous chapters that for every polynomial ideal we have a corresponding algebraic set, and for every algebraic set we have a corresponding ideal.

$$\begin{array}{ccc} \text{polyn. ideals} & & \text{algebraic sets} \\ I & \longrightarrow & V(I) \\ I(V) & \longleftarrow & V \end{array}$$

In this section we will further investigate this correspondence. The key instrument for this investigation is Hilbert's Nullstellensatz.

Lemma 4.2.1. (Noether's normalization lemma) *Let K be infinite. Let $f \in K[x_1, \ldots, x_n]$ non-constant. There is a linear change of coordinates (i.e. an invertible linear map) L such that the leading coefficient of $L(f)$ w.r.t. x_1 is a nonzero constant.*

Proof: Let d be the total degree of f. Consider the linear change of coordinates

$$L: \quad \begin{array}{rcl} x_1 & = & \tilde{x}_1, \\ x_2 & = & \tilde{x}_2 + a_2\tilde{x}_1, \\ & \vdots & \\ x_n & = & \tilde{x}_n + a_n\tilde{x}_1, \end{array}$$

where the a_i are still to be determined constants. Then

$$\begin{aligned} L(f) &= f(\tilde{x}_1, \tilde{x}_2 + a_2\tilde{x}_1, \ldots, \tilde{x}_n + a_n\tilde{x}_1) \\ &= c(a_2, \ldots, a_n)\tilde{x}_1^d + \text{ terms in which } \tilde{x}_1 \text{ has degree } < d, \end{aligned}$$

where $c(a_2, \ldots, a_n)$ is a non-zero polynomial in the a_i. Thus, by Theorem 3.1.1, we can choose the a_i so that $c(a_2, \ldots, a_n) \neq 0$. $\square$

Theorem 4.2.2. (Weak Nullstellensatz) *Let K be an algebraically closed field. Let I be an ideal in $K[x_1, \ldots, x_n]$ satisfying $V(I) = \emptyset$. Then $I = K[x_1, \ldots, x_n]$.*

Proof: We proceed by induction on n. $K[x_1]$ is a principal ideal domain, so $I = \langle f \rangle$ for some $f \in K[x_1]$. Since K is algebraically closed, $V(I)$ can be empty only if f is a non-zero constant. So $I = K[x_1]$.

Now let $n > 1$. Let $I = \langle f_1, \ldots, f_m \rangle$, where none of these basis polynomials is 0. If any of the f_i is a constant, then obviously $I = K[x_1, \ldots, x_n]$. So let us assume that none of the f_i is a constant. Let $d \geq 1$ be the total degree of f_1. Because of Lemma 4.2.1 we can assume that f_1 is of the form

$$f_1 = cx_1^d + \text{ terms in which } x_1 \text{ has degree } < d.$$

If f_1 does not have this form to start with, we can apply a linear transformation L as in Lemma 4.2.1. The set $\tilde{I} = \{L(f) | f \in I\}$ is an ideal in $K[\tilde{x}_1, \ldots, \tilde{x}_n]$. Note that we still have $V(\tilde{I}) = \emptyset$ since if the transformed equations had solutions, so would the original ones. Moreover, if we can show that $1 \in \tilde{I}$, then also $f^{-1}(1) = 1 \in I$.

Since f_1 has this special form, from Theorem 4.1.2 we get

$$V(I_1) = \pi_1(V(I)).$$

This shows that $V(I_1) = \pi_1(V(I)) = \pi_1(\emptyset) = \emptyset$. By the induction hypothesis, it follows that $I_1 = K[x_2, \ldots, x_n]$. But this implies that $1 \in I_1 \subset I$. Thus, $I = K[x_1, \ldots, x_n]$. $\square$

Theorem 4.2.3. (Hilbert's Nullstellensatz) *Let K be an algebraically closed field, and I an ideal in $K[x_1, \ldots, x_n]$. Then*

$$I(V(I)) = \sqrt{I}.$$

(I.e., the ideal of an algebraic set is radical.)

Proof: Obviously $\sqrt{I} \subset I(V(I))$.

On the other hand, choose an arbitrary $g \in I(V(I))$. We have to show that $g \in \sqrt{I}$. Let $\{f_1, \ldots, f_m\}$ be a basis of I. Consider

$$J = \langle f_1, \ldots, f_m, x_{n+1}g - 1\rangle,$$

an ideal in $K[x_1, \ldots, x_n, x_{n+1}]$. Then $V(J) = \emptyset$, since g vanishes wherever all the f_i vanish. Applying the Weak Nullstellensatz to J, we see that $1 \in J$. So there is an equation

$$1 = \sum_{i=1}^{m} a_i(x_1, \ldots, x_{n+1})f_i \quad + \quad b(x_1, \ldots, x_{n+1})(x_{n+1}g - 1).$$

Let $y = 1/x_{n+1}$, and multiply the equation by a high power of y, so that an equation

$$y^k = \sum_{i=1}^{m} c_i(x_1, \ldots, x_n, y)f_i \quad + \quad d(x_1, \ldots, x_n, y)(g - y)$$

in $K[x_1, \ldots, x_n, y]$ results. Substituting g for y gives the required equation. $\square$

This idea of enlarging the ideal I by the polynomial $x_{n+1}g - 1$ is due to Rabinowitsch, and it is usually called the "Rabinowitsch trick".

Now the correspondence of ideals and algebraic sets can be expressed as a series of corollaries to Hilbert's Nullstellensatz. The field K is algebraically closed throughout this section.

Theorem 4.2.4. *If I is a radical ideal in $K[x_1, \ldots, x_n]$, then $I(V(I)) = I$. So there is a 1-1 correspondence between radical ideals and algebraic sets.*

Proof: this is an obvious consequence of the Nullstellensatz. $\square$

Theorem 4.2.5. *If I is a prime ideal, then $V(I)$ is irreducible. There is a 1-1 correspondence between prime ideals and irreducible algebraic sets. The maximal ideals correspond to points.*

Proof: The statement about irreducible sets was already proved.

Since the singleton set containing just one point is algebraic, any ideal I having a $V(I)$ properly containing this point cannot be maximal. The converse is also rather obvious. $\square$

The situation, in which the ideal I corresponds to a finite set of points, can be characterized via the vector space dimension of the polynomial ring modulo I.

Theorem 4.2.6. *Let I be an ideal in $K[x_1, \ldots, x_n]$. Then $V(I)$ is a finite set if and only if $K[x_1, \ldots, x_n]/I$ is a finite dimensional vector space over K. If this occurs, we have*

$$|V(I)| \;\leq\; \dim_K(K[x_1, \ldots, x_n]/I).$$

Proof: Let $P_1, \ldots, P_r \in V(I)$. Choose polynomials $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ such that

$$f_i(P_j) = \begin{cases} 1, & \text{if } i = j, \\ 0, & \text{if } i \neq j. \end{cases}$$

Such polynomials exist, see for instance [Win], Exercise 8.4.3. Let $\overline{f}_i$ be the equivalence class of f_i w.r.t. I. If $\sum \lambda_i \overline{f}_i = 0$ for some $\lambda_i \in K$, then $\sum \lambda_i f_i \in I$, so $\lambda_j = (\sum \lambda_i f_i)(P_j) = 0$. Thus, the $\overline{f}_i$ are linearly independent over K, so $r \leq \dim_K(K[x_1, \ldots, x_n]/I)$.

Conversely, if $V(I) = \{P_1, \ldots, P_r\}$ is finite, let $P_i = (a_{i1}, \ldots, a_{in})$, and let

$$f_j := \prod_{i=1}^{r} (x_j - a_{ij}),$$

for $j = 1, \ldots, n$. Then $f_j \in I(V(I))$, so, by the Nullstellensatz, $f_j^m \in I$ for some $m > 0$ (take m large enough to work for all f_j). $\overline{f}_j^m = 0$, so $\overline{x}_j^{rm}$ is a K–linear combination of $\overline{1}, \overline{x}_j, \ldots, \overline{x}_j^{rm-1}$. It follows by induction that $\overline{x}_j^s$ is a K–linear combination of $\overline{1}, \overline{x}_j, \ldots, \overline{x}_j^{rm-1}$ for all s. Hence,

$$\{\overline{x}_1^{e_1} \cdot \ldots \cdot \overline{x}_n^{e_n} \mid e_i < rm\}$$

generate $K[x_1, \ldots, x_n]/I$ as a vector space over K. $\square$

Example 4.2.1. We start with the ideal

$$I = \langle y^2 + x^2 - 1, (y - x)^2 \rangle \subseteq \mathbb{Q}[x, y].$$

The corresponding algebraic set, in $\overline{\mathbb{Q}}^2$ or $\mathbb{C}^2$, is

$$V(I) = \big\{ \big(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\big), \big(-\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2}\big) \big\}.$$

The polynomials

$$\begin{aligned} h_1 &= (y + \sqrt{2}/2)^2 + (x - \sqrt{2}/2)^2 - 2, \\ h_2 &= -17y - 6x^2 + 17x + 3, \\ h_3 &= -51y + 28x^3 - 102x^2 + 37x + 51 \end{aligned}$$

vanish on all the points in $V(I)$, so $h_1, h_2, h_3 \in I(V(I)) = \sqrt{I}$. However, none of these polynomials is in I itself. So, clearly, I is not radical. $\square$