

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 $K[x_1, \dots, x_n]$. The k -th elimination ideal I_k of I is the ideal in $K[x_{k+1}, \dots, x_n]$ defined by

$$I_k = I \cap K[x_{k+1}, \dots, x_n]. \quad \bullet$$

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 $(x_1 = x, x_2 = y, x_3 = z)$

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

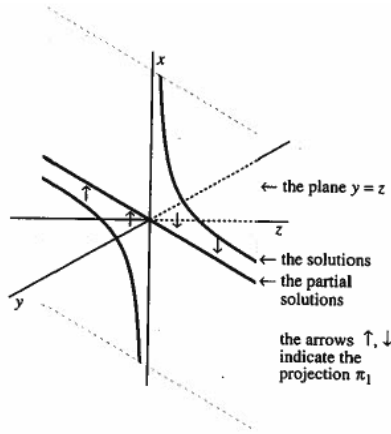
Let I be the ideal generated by these polynomials. A Gröbner basis for I w.r.t. the lexicographic ordering with $x > y > z$ has the form

$$\left\{ \begin{array}{l} xz - 1, \\ y - z \end{array} \right\}.$$

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

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

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 $I = \langle f_1, \dots, f_m \rangle$ be an ideal in $K[x_1, \dots, x_n]$. For each $1 \leq i \leq m$ write f_i as a polynomial in the main variable x_1 , i.e.*

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

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

Proof: We have already proven a simpler version of the Extension Theorem in Theorem 2.4.3. For the proof of this general theorem we refer 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 $1 \leq i \leq n$ let

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

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

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

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

Lemma 4.1.2. *Let I be an ideal in $K[x_1, \dots, x_n]$, and $V = V(I)$. Then in $\mathbb{A}^{n-l}(K)$ we have*

$$\pi_l(V) \subseteq V(I_l).$$

Proof: Consider $f \in I_l$. f is also in I , so for any point $(a_1, \dots, a_n) \in V$ we have

$$f(a_{l+1}, \dots, a_n) = f(\pi_l(a_1, \dots, a_n)) = 0.$$

This shows that f vanishes on all points of $\pi_l(V)$. •

Theorem 4.1.3. *Let K be algebraically closed, $V = V(f_1, \dots, f_m)$ an algebraic set in $\mathbb{A}^n(K)$. Let $I = \langle f_1, \dots, f_m \rangle$. Let the leading coefficients g_i be as in the Extension Theorem. Then in $\mathbb{A}^{n-1}(K)$ we have the equality*

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

Proof: This follows immediately from Lemma 4.1.2 and the Extension Theorem (Thm. 4.1.1). •

Theorem 4.1.3 will become important in the proof of Hilbert's Nullstellensatz (weak version).

Example 4.1.1. (continued) Theorem 4.1.2 tells us that $\pi_1(V)$ fills up the affine variety $V(I_1)$, except possibly for a part that lies in $V(g_1, \dots, g_m)$. Unfortunately, it is not clear how big this part is, and sometimes $V(g_1, \dots, g_m)$ is unnaturally large. For example, one can see that the equations

$$\begin{aligned} (y - z)x^2 + xy - 1 &= 0, \\ (y - z)x^2 + xz - 1 &= 0 \end{aligned} \tag{2}$$

generate the same ideal as equations (1). Since $g_1 = g_2 = y - z$ generate the elimination ideal I_1 , Theorem 4.1.3 tells us nothing about the size of $\pi_1(V)$ in this case. •

Observe that in general $g_i \notin I_1$ (or in a prime component of it), so $V(g_1, \dots, g_m) \cap V(I_1)$ 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”.

We finish with a theorem which tells us how much smaller than $V(I_1)$ the projection $\pi_1(V)$ could be.

Theorem 4.1.4. (Closure Theorem) *Let K be algebraically closed. Let $I = \langle f_1, \dots, f_m \rangle$ be an ideal in $K[x_1, \dots, x_n]$, $V = V(f_1, \dots, f_m)$. 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 $f \in K[x_1, \dots, x_n]$ 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

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

where the a_i are still to be determined constants. Then

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

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

Example 4.2.1. Consider the polynomial

$$f(x, y) = (2y^2 - 1)x^2 + y$$

in $\mathbb{Q}[x, y]$. Substituting $y + a_2x$ for y , we get

$$2a_2^2x^4 + 4a_2yx^3 + (2y^2 - 1)x^2 + a_2x + y .$$

So for $a_2 = 1$ we get

$$2x^4 + 4yx^3 + (2y^2 - 1)x^2 + x + y ,$$

having the constant leading coefficient 2. •

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

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 $I = \langle f_1, \dots, f_m \rangle$, where none of these basis polynomials is 0. If any of the f_i is a constant, then obviously $I = K[x_1, \dots, x_n]$. 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 $K[\tilde{x}_1, \dots, \tilde{x}_n]$. 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 $1 = L^{-1}(1) \in I$.

Since f_1 has this special form, from Theorem 4.1.3 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 $I_1 = K[x_2, \dots, x_n]$. But this implies that $1 \in I_1 \subset I$. Thus, $I = K[x_1, \dots, x_n]$. •

Theorem 4.2.3. (Hilbert's Nullstellensatz) *Let K be an algebraically closed field, and I an ideal in $K[x_1, \dots, x_n]$. 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 $\{f_1, \dots, f_m\}$ be a basis of I . Consider

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

an ideal in $K[x_1, \dots, x_n, x_{n+1}]$. 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

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

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

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

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

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 $K[x_1, \dots, x_n]$, 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. •

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. •

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

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

Proof: “ \Leftarrow ”: Let P_1, \dots, P_r be pairwise different points in $V(I)$. Choose polynomials $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ 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 \bar{f}_i be the equivalence class of f_i w.r.t. I . If $\sum \lambda_i \bar{f}_i = 0$ 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 \bar{f}_i are linearly independent over K , so $r \leq \dim_K(K[x_1, \dots, x_n]/I)$.

“ \Rightarrow ”: Conversely, if $V(I) = \{P_1, \dots, P_r\}$ is finite, let $P_i = (a_{i1}, \dots, a_{in})$, and let

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

for $j = 1, \dots, n$. 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). $\bar{f}_j^m = 0$, so \bar{x}_j^{rm} is a K -linear combination of $\bar{1}, \bar{x}_j, \dots, \bar{x}_j^{m-1}$. It follows by induction that \bar{x}_j^s is a K -linear combination of

$\bar{1}, \bar{x}_j, \dots, \bar{x}_j^{rm-1}$ for all s . Hence,

$$\{\bar{x}_1^{e_1} \cdot \dots \cdot \bar{x}_n^{e_n} \mid e_i < rm\}$$

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

Example 4.2.1. We start with the ideal

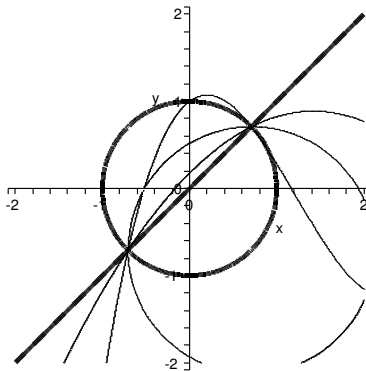
$$I = \langle y^2 + x^2 - 1, (y - x)^2 \rangle \subseteq \mathbb{Q}[x, y].$$

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

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

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. •

4.3 Primary decomposition of ideals

In Chapter 3 we have seen that every algebraic set V can be written as a finite non-trivial union of irreducible algebraic sets or varieties,

$$V = \bigcup V_i ,$$

(see Theorem 3.3.3). These algebraic sets correspond to polynomial ideals, $I = I(V), I_i = I(V_i)$, where the I_i are prime by Theorem 3.3.1. So we get that $I(V)$ can be represented as a finite non-trivial intersection of prime ideals

$$I(V) = \bigcap I(V_i) .$$

But what if we want to decompose a general non-radical ideal in this way? Let us give a short sketch of the general decomposition theory for ideals.

In this section we always consider R to be a commutative ring with 1.

Def 4.3.1. Let R be a commutative ring with 1, and let I be an ideal in R . I is *primary* iff for all $a, b \in R$:

$$ab \in I \implies (a \in I \text{ or } b^n \in I \text{ for some } n \in \mathbb{N}) .$$

I is *prime* iff for all $a, b \in R$:

$$ab \in I \implies (a \in I \text{ or } b \in I) . \quad \bullet$$

Theorem 4.3.1. (i) For every primary ideal I the radical \sqrt{I} is a prime ideal.

(ii) If I is prime and J is primary with $J \subseteq I$, then also $\sqrt{J} \subseteq I$.

Proof: (i) Suppose $a \cdot b \in \sqrt{I}$ and $a \notin \sqrt{I}$. Then for some n we have $(ab)^n \in I$ and $a^n \notin I$. So for some m we have $b^{nm} \in I$, which means $b \in \sqrt{I}$.

(ii) Exercise. •

Def 4.3.2. If I is a primary ideal then $J = \sqrt{I}$ is called the *associated prime ideal* of I ; I is called a *primary ideal belonging to J* . •

Def 4.3.3. An ideal I is called *irreducible* iff it cannot be represented as the intersection of two proper superideals; i.e. if J_1, J_2 are ideals and $I = J_1 \cap J_2$ then $I = J_1$ or $I = J_2$. •

Theorem 4.3.2. If R is Noetherian, then every ideal in R is the intersection of finitely many irreducible ideals.

Proof: We will apply the Principle of Divisor Induction (Theorem 3.2.4 or [Wae70] Chap. 15.1).

The statement is true for all irreducible ideals, so in particular for R . Suppose then that I is reducible, i.e. for J_1, J_2 we have

$$I = J_1 \cap J_2, \quad I \subset J_1, \quad I \subset J_2 .$$

If the statement is true for all proper divisors of I , then it is true in particular for J_1 and J_2 ; i.e. there are irreducible ideals s.t.

$$J_1 = \bigcap_{i=1}^r J_{1,i}, \quad J_2 = \bigcap_{i=1}^s J_{2,i} .$$

But this implies

$$I = \bigcap_{i=1}^r J_{1,i} \cap \bigcap_{i=1}^s J_{2,i} .$$

So the statement is also true for I . •

Theorem 4.3.3. *If R is Noetherian and I is an irreducible ideal in R , then I is primary.*

Proof: We show that if I is not primary, then it is also not irreducible. So assume that I is not primary. Then there are $a, b \in R$ s.t.

$$ab \in I, \quad a \notin I, \quad \text{and } b^n \notin I \forall n \in \mathbb{N} .$$

For every $n \in \mathbb{N}$ we consider the ideal $I : \langle b^n \rangle$. Clearly we have for all n :

$$I : \langle b^n \rangle \subseteq I : \langle b^{n+1} \rangle .$$

(Recall: $t \in I : \langle c \rangle \iff t \cdot c \in I$.)

Since R is Noetherian, there must be a $k \in \mathbb{N}$ s.t.

$$I : \langle b^k \rangle = I : \langle b^{k+1} \rangle = \dots .$$

Now consider the ideals

$$A := \langle a \rangle, \quad B := \langle b^k \rangle .$$

First we show that I is the intersection of two ideals:

$$I = (I + A) \cap (I + B) . \tag{*}$$

Obviously we have “ \subseteq ”, because $I \subseteq I + A$ and $I \subseteq I + B$.

For showing “ \supseteq ”, let $x \in (I + A) \cap (I + B)$. So there are $i_1, i_2 \in I$ and $r_1, r_2 \in R$ s.t.

$$i_1 + r_1 a = x = i_2 + r_2 b^k .$$

So $xb = i_1b + r_1ab$. Since $ab \in I$ we get $xb \in I$. Also $xb = i_2b + r_2b^{k+1}$, so we get $r_2b^{k+1} \in I$. This shows that $r_2 \in I : \langle b^{k+1} \rangle = I : \langle b^k \rangle$. So $r_2b^k \in I$, and also $x = i_2 + r_2b^k \in I$. This proves (*).

Now we show that $I + A$ and $I + B$ are proper divisors of I . Since $a \in I + A$ and $a \notin I$, we get $I \neq I + A$. Since $b^k \in I + B$ and $b^k \notin I$ we get $I \neq I + B$.

So we have shown that I is not irreducible. •

Theorems 4.3.2 and Theorem 4.3.3 together yield the following:

Corollary *If R is Noetherian, then every ideal in R is the intersection of finitely many primary ideals.*

This theorem can be made still sharper. First, all *redundant* ideals J_i in a *representation*

$$I = \bigcap_{i=1}^r J_i =: [J_1, \dots, J_r],$$

meaning all those J_i which contain the intersection of the other ideals, can be omitted. We thus arrive at an *irredundant* representation, that is, one in which no component J_i contains the intersection of the remaining ideals. In such a representation it is still possible that several of the primary components might be combined to form a primary ideal, that is, that their intersection is again a primary ideal; this is the case if these components all have the same associated prime ideal.

Theorem 4.3.4. ([Wae70] 15.4) *Every ideal in a Noetherian ring R admits an irredundant representation as the intersection of finitely many primary components. These primary components all have distinct associated prime ideals.*

This second decomposition theorem, proved for polynomial rings by E.Lasker and in general by E.Noether, is the most important result of general ideal theory (according to van der Waerden).

Example 4.3.1. ([Wae70] 15.5) The ideal

$$I = \langle x^2, xy \rangle$$

in $K[x, y]$ consists of all polynomials which are divisible by x and in which the linear and constant terms are absent. The set of all polynomials divisible by x is the prime ideal

$$J_1 = \langle x \rangle.$$

The set of all polynomials in which the linear and constant terms are absent is the primary ideal

$$J_2 = \langle x^2, xy, y^2 \rangle.$$

Hence

$$I = [J_1, J_2].$$

This is an irredundant representation, and the associated prime ideals, $\langle x \rangle$ and $\langle x, y \rangle$, of J_1 and J_2 are distinct. This is therefore also a representation by greatest primary ideals.

But in addition to this representation there is still another:

$$I = [J_1, J_3] ,$$

where

$$J_3 = \langle x^2, y \rangle ,$$

for in order that a polynomial lie in I , it is sufficient to require that the polynomial be divisible by x and that it contain no linear or constant term. If the field K is infinite, then there are even an infinite number of representations of this type:

$$I = [J_1, J_3^{(\lambda)}], \quad J_3^{(\lambda)} = \langle x^2, y + \lambda x \rangle .$$

All these decompositions of I have the common feature that the number of primary components and the associated prime ideals,

$$\langle x \rangle, \quad \langle x, y \rangle ,$$

are the same. •

Theorem 4.3.4. (Uniqueness Theorem, [Wae70] Chap. 15.5) *In two irredundant representations of an ideal I in R , a Noetherian commutative ring with 1, by primary components the number of components and the associated prime ideals are the same (although the components themselves need not be).*