Algebraic Geometry, Lecture 11

Frank-Olaf Schreyer

Saarland University, Perugia 2021

Overview

Today we prove the dimension criterion. A Key role is played by the concept of integral ring extensions.

1. Dimension criterion
2. Integral ring extensions
3. Proof of the dimension criterion
4. The lying over theorem
5. Krull's prime existence lemma
6. Krull dimension

The Gröbner basis criterion

Last time we formulated

Theorem. *Let* $I \subset K[x_1, \dots, x_c, y_1, \dots, y_d]$ *an ideal and* $A = V(I) \subset \mathbb{A}^{c+d}$ *the corresponding algebraic set. Let* $>$ *be a global monomial order. Suppose*

$$\operatorname{rad}(\operatorname{Lt}(I)) = (x_1, \dots, x_c).$$

Then $\dim A = d$ *and the projection*

$$\pi : A \to \mathbb{A}^d, \quad (a_1, \dots, a_c, b_1 \dots, b_d) \mapsto (b_1, \dots, b_d)$$

onto the last d *components is surjective.*

Moreover, if $\operatorname{Lt}(I)$ *is generated by monomials in the subring* $K[x_1, \dots, x_c]$, *then every associated prime of* I *defines a variety of dimension* d. *In particular every irreducible component of* A *has dimension* d.

The tower of projections

In the situation of the tower of projections theorem we get the desired dimension statement.

Theorem. *Suppose that* $I \subsetneq K[x_1, \ldots, x_n]$ *is a proper ideal. Let* $I_j = I \cap K[x_{j+1}, \ldots, x_n]$ *be the* j*-th elimination ideal. Set*

$$c = \min\{j \mid I_j = (0)\}$$

and suppose that for each j *with* $0 \leq j \leq c-1$ *the ideal* I_j *contains an* x_{j+1}*-monic polynomial of degree* d_j*. Then the projection* $\pi_c \colon V(I) \to \mathbb{A}^{n-c}$ *onto the last* $n-c$ *components is surjective, and each fiber*

$$\pi_c^{-1}(a_{c+1}, \ldots, a_n)$$

is finite of cardinality $\leq \prod_{j=0}^{c-1} d_j$*.*

Corollary. *With the assumption and notation of the tower theorem*

$$\dim V(I) = n - c$$

holds.

Proof of the corollary

The assumption of the Gröbner basis criterion is satisfied for $>_{lex}$ with $d = n - c$ and $y_1 = x_{c+1}, \ldots, y_d = x_n$. Indeed $I_c = 0$ implies

$$\operatorname{rad}(\mathrm{Lt}(I)) \subset (x_1, \ldots x_c)$$

by the key property of $>_{\mathrm{lex}}$. The existence of the x_j-monic polynomials in I_{j-1} for $j = 1, \ldots, c$ implies that equality holds.

The key concept for the proof of the dimension criterion is the notion of integral ring extensions. This played also the cruitial role in our proof of the Nullstellensatz.

Integral ring extensions

Definition. Let $R \subset S$ be an inclusion of rings and let $I \subset R$ be an ideal. An element $s \in S$ is **integral over** I if it satisfies a monic equation

$$s^n + r_1 s^{n-1} + \ldots + r_n = 0$$

with $r_i \in I$. s is **integral over** R if it is integral over the ideal $(1) = R$.
$R \subset S$ is called an **integral ring extension** if every element $s \in S$ is integral over R.
$R \subset S$ is called a **finite ring extension** if S as an R-module is finitely generated.

Example. Let $s \in S$ be integral over R. Then $R \subset R[s]$ is a finite ring extension. Indeed, from the monic equation above we see that $R[s]$ is generated by $1, s, \ldots, s^{n-1}$ as an R-module.

Integral elements

Proposition. *Let $R \subset S$ be a ring extension and $s \in S$ an element and $I \subset R$ an ideal. TFAE:*

1) *s is integral over R (over I).*
2) *$R[s]$ is finite over R (and $s \in \mathrm{rad}(IR[s])$).*
3) *$R[s]$ is contained in a subring $S' \subset S$ which is finite over R (and $s \in \mathrm{rad}(IS')$)*

Proof. 1) $\Rightarrow$ 2) was established above. If s is integral over I, then the equation says $s^n \in IR[s]$. 2) $\Rightarrow$ 3) is trivially true. 3) $\Rightarrow$ 1) is the essential direction. Suppose S' is generated by $m_1, \ldots, m_n$ as an R-module. Since $s \in \mathrm{rad}(IS')$ we may write for a suitable power N

$$s^N m_i = \sum_{j=1}^{n} r_{ij} m_j$$

with $r_{ij} \in I$. In matrix notation we obtain

$$(s^N E_n - B) \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0$$

Tower of extensions

Multiplying with the cofactor matrix we obtain

$$\det(s^N E_n - B) m_i = 0$$

for all i. Since $1 \in R \subset S'$ is a linear combination of $m_1, \ldots, m_n$ we obtain

$$\det(s^N E_n - B) = s^{nN} + r_1 s^{(n-1)N} + \ldots + r_n = 0,$$

i.e., s is integral over I. □

Proposition. *Let $R \subset S \subset T$ be a tower of finite or integral ring extensions. Then $R \subset T$ is a finite respectively integral ring extension as well.*

Proof

Suppose $s_1, \ldots, s_n$ generate S as an R-module and $t_1, \ldots, t_m$ generate T as an S-module. Then the nm products $s_i t_j$ generate T as an R-module. Every $t \in T$ has an expression $t = \sum a_j t_j$ with $a_j \in S$. Every a_j has an expression $a_j = \sum r_{ij} s_i$. Hence

$$t = \sum_{i=1}^{n} \sum_{j=1}^{m} r_{ij} s_i r_j.$$

For the second version consider an element $t \in T$. By assumption t is integral over S, i.e., t satisfies an equation

$$t^n + s_1 t^{n-1} + \ldots + s_n = 0 \text{ with } s_i \in S.$$

Since each s_i is integral over R the extension

$$R \subset R[s_1, \ldots, s_n]$$

is finite, hence $R \subset R[s_1, \ldots, s_n, t]$ is finite as well and t is integral over R by the conclusion 3) $\Rightarrow$ 1) above. □

Proof of the dimension criterion

Since $\mathrm{rad}(\mathrm{Lt}(I)) = (x_1, \ldots x_c)$ we have $I \cap K[y_1, \ldots, y_d] = 0$. Thus the induced map

$$K[y_1, \ldots, y_d] \to S = K[x_1, \ldots x_c, y_1, \ldots, y_d]/I$$

is injective. $K[y_1, \ldots, y_d] \subset S$ is a finite ring extension because for each x_i there exists an $x_i^{n_i} \in \mathrm{Lt}(I)$. Hence the $\overline{x}^\alpha$ with $\alpha_i < n_i$ generate S as a $K[y_1, \ldots, y_d]$-module by the division theorem. Consider now a minimal primary decomposition

$$I = \mathfrak{q}_1 \cap \ldots \cap \mathfrak{q}_r.$$

For at least one associated prime $\mathfrak{p}_j = \mathrm{rad}(\mathfrak{q}_j)$ we must have

$$\mathfrak{p}_j \cap K[y_1, \ldots, y_d] = 0.$$

Indeed, if there are non-zero elements $f_i \in \mathfrak{p}_i \cap K[y_1, \ldots, y_d]$ for every i, then their product $\prod f_i \in \mathrm{rad}(I) \cap K[y_1, \ldots, y_d]$ and a suitable power $(\prod f_i)^N \in I \cap K[y_1, \ldots, y_d]$ which contradicts $\mathrm{Lt}(I) \cap K[y_1, \ldots, y_d] = 0$.

Proof of the dimension criterion continued

For $A_j = V(\mathfrak{p}_j)$ with $\mathfrak{p}_j \cap K[y_1, \ldots, y_d] = 0$ we have that $K[y_1, \ldots, y_d] \subset K[A_j] = K[x_1, \ldots x_c, y_1, \ldots, y_d]/\mathfrak{p}_j$ is a finite extension. Hence

$$K(y_1, \ldots, y_d) \subset K(A_j)$$

is an algebraic field extension and

$$\dim A_j = \operatorname{trdeg}_K K(A_j) = \operatorname{trdeg}_K K(y_1, \ldots, y_d) = d.$$

For $\mathfrak{p}_i$ with $\mathfrak{p}_i^c = \mathfrak{p}_i \cap K[y_1, \ldots, y_d] \neq 0$ we have for $B_i = V(\mathfrak{p}_i^c) \subsetneq \mathbb{A}^d$ that

$$K[B_i] \subset K[A_i]$$

is a finite ring extension and

$$\dim A_i = \dim B_i = \operatorname{trdeg}_K K(B_i) < d$$

since $\overline{y}_1, \ldots, \overline{y}_d$ give algebraic dependent generators of $K(B_i)$ over K. Thus

$$\dim A = \max\{\dim A_j\} = d.$$

Proof of the unmixedness

In case that $\mathrm{Lt}(I)$ is $(x_1, \ldots, x_c)$-primary, $K[x_1, \ldots x_c, y_1, \ldots, y_d]/I$ is actually a free $K[y_1, \ldots, y_d]$-module: $\mathrm{Lt}(I)$ is generated by monomials in $K[x_1, \ldots, x_c]$ and the monomials $x^\alpha \in K[x_1, \ldots, x_c] \setminus \mathrm{Lt}(I)$ form a basis by the division theorem. If $\mathfrak{p}_i = \mathrm{ann}(m)$ for some $m \in K[x_1, \ldots x_c, y_1, \ldots, y_d]/I$ is an associated prime, then

$$\mathfrak{p}_i \cap K[y_1, \ldots, y_d] = \mathrm{ann}_{K[y_1,\ldots,y_d]}(m)$$

is an associated prime of $K[x_1, \ldots x_c, y_1, \ldots, y_d]/I$ as a $K[y_1, \ldots, y_d]$-module. But a free module has (0) as the only associated prime. Thus $\mathfrak{p}_i \cap K[y_1, \ldots, y_d] = 0$ for all i and every associated prime defines a variety $V(\mathfrak{p}_i)$ of dimension d.

It remains to prove that the map $\pi : A \to \mathbb{A}^d$ is surjective. We prove a more general result.

The lying over theorem

Let $R \subset S$ be a ring extension. If $\mathfrak{P}$ is a prime ideal in S, then $\mathfrak{p} = \mathfrak{P} \cap R$ is a prime ideal in R. One says $\mathfrak{P}$ **lies over** $\mathfrak{p}$.

Theorem. *Let $R \subset S$ be an integral ring extension and let $\mathfrak{p}$ be a prime ideal of R. Then:*

1) *There exists a prime ideal $\mathfrak{P}$ of S with $\mathfrak{p} = \mathfrak{P} \cap R$.*
2) *There are no strict inclusions between prime ideals lying over $\mathfrak{p}$.*
3) *If $\mathfrak{P}$ is a prime ideal lying over $\mathfrak{p}$, then $\mathfrak{P}$ is a maximal ideal iff $\mathfrak{p}$ is a maximal ideal.*
4) *If S is noetherian, then the prime ideals lying over $\mathfrak{p}$ are precisely the minimal primes of $\mathfrak{p}S$.*

The surjectivity of $\pi : A \to \mathbb{A}^d$ follows from 1) and 3) since maximal ideals in $K[x_1, \ldots, x_c, y_1, \ldots y_d]/I$ correspond to points $(a_1, \ldots, a_c, b_1, \ldots, b_d) \in A$, and maximal ideals of $K[y_1, \ldots, y_d]$ correspond to points $(b_1, \ldots, b_d) \in \mathbb{A}^d$.

Krull's prime existence Lemma

Lemma. *Let I be an ideal of the ring R and let $U \subset R$ be a multiplicative subset with $I \cap U = \emptyset$. Then there exists a prime ideal $\mathfrak{p}$ of R with $I \subset \mathfrak{p}$ and $U \cap \mathfrak{p} = \emptyset$.*

Proof. Consider the set

$$\mathcal{M} = \{J \subset R \mid J \text{ an ideal with } I \subset J \text{ and } J \subset U = \emptyset\}.$$

$\mathcal{M} \neq \emptyset$ because $I \in \mathcal{M}$ and consists of proper ideals because $1 \in U$. Let $\mathfrak{p}$ be a maximal element of $\mathcal{M}$ with respect to inclusion. Then:

Claim. $\mathfrak{p}$ *is a prime ideal.*

Indeed, suppose $r_1, r_2 \notin \mathfrak{p}$. Then $(\mathfrak{p} + (r_j)) \cap U \neq \emptyset$ because $\mathfrak{p}$ is maximal in $\mathcal{M}$. Thus there are $p_j \in \mathfrak{p}$ and $a_j \in R$ such that $a_j + a_j r_j \in U$. Since U is multiplicative we have

$$(p_1 + a_1 r_1)(p_2 + a_2 r_2) \in U = R \setminus \mathfrak{p}.$$

Hence $a_1 a_2 r_1 a_1 \notin \mathfrak{p}$. In particular $r_1 r_2 \notin \mathfrak{p}$ as desired.

Proof of Krull's prime existence lemma continued

The existence of a maximal element $\mathfrak{p}$ in $\mathcal{M}$ is clear if R is noetherian. For more general rings we apply Zorn's Lemma: $\mathcal{M}$ is partially ordered by inclusion. If $\{J_\lambda\}$ is a totally ordered subset set of $\mathcal{M}$, then $\bigcup_\lambda J_\lambda$ is an upper bound. Thus the assumptions of Zorn's Lemma are satisfied, and $\mathcal{M}$ contains maximal elements. □

Corollary. *Every proper ideal I in a ring R is contained in a maximal ideal.*

Proof. We apply Krull's Lemma to $I \subset R$ and $U = \{1\}$. □

Proof of part 1 of the lying over theorem

Consider the ideal $\mathfrak{p}S$ of S and the multiplicative subset $U = R \setminus \mathfrak{p}$ of S. Using that $R \subset S$ is an integral extension we verify that $\mathfrak{p}S \cap U = \emptyset$: Every $s \in \mathfrak{p}S$ has an expression $s = \sum_{i=1}^{n} a_i s_i$ with $a_i \in \mathfrak{p}$ and $s_i \in S$. Thus s is integral over $\mathfrak{p}R[s_1, \ldots, s_n]$. Consider an integral equation

$$s^d + r_1 s^{d-1} + \ldots + r_d = 0 \text{ with } r_i \in \mathfrak{p}.$$

We have to show that $s \notin U = R \setminus \mathfrak{p}$. Assume the contrary, then $s^d \in \mathfrak{p}$, hence $s \in \mathfrak{p}$ since $\mathfrak{p}$ is a prime ideal. This contradicts $s \in U = R \setminus \mathfrak{p}$.

We can now apply Krull's Lemma to the ideal $I = \mathfrak{p}S$ of S and the multiplicative subset U. There exists a prime ideal $\mathfrak{P}$ of S with $\mathfrak{p} \subset \mathfrak{p}S \subset \mathfrak{P}$ and $\mathfrak{P} \cap U = \emptyset$. Hence $\mathfrak{P} \cap R \subset \mathfrak{p}$ and equality holds.

Proof of part 2 of the lying over theorem

Consider prime ideals $\mathfrak{P}_1 \subset \mathfrak{P}_2$ of S, both lying over $\mathfrak{p}$. Then $\overline{R} = R/\mathfrak{p} \subset \overline{S} = S/\mathfrak{P}_1$ is an integral ring extensions of domains and $\mathfrak{P}_2/\mathfrak{P}_1 \subset \overline{S}$ is a prime ideal which lies over $(0) \subset \overline{R}$. We have to prove that $\mathfrak{P}_2/\mathfrak{P}_1 = (0)$. Suppose $\bar{s} \in \mathfrak{P}_2/\mathfrak{P}_1$ is non-zero. Let

$$\bar{s}^d + \bar{r}_1 \bar{s}^{d-1} + \ldots + \bar{r}_d = 0$$

be an integral equation of minimal degree. Then $\bar{r}_d \in \mathfrak{P}_2/\mathfrak{P}_1 \cap \overline{R} = (0)$. Thus $\bar{r}_d = 0$. If $d = 1$, then this says $s = 0$. If $d > 1$, then we can divide the integral equation by $\bar{s}$ since $\overline{S}$ is a domain, and we obtain an equation of smaller degree. Thus we get a contradiction in any case.

Proof of part 3 and 4 of the lying over theorem

3): If $\mathfrak{p}$ is a maximal ideal in R, then $\mathfrak{P}$ is a maximal ideal as well by part 2: Any prime ideal $\mathfrak{P}' \supset \mathfrak{P}$ lies over $\mathfrak{p}$ as well because $\mathfrak{p}$ is maximal. Hence $\mathfrak{P}' = \mathfrak{P}$ by part 2.

4): If $\mathfrak{P}$ lies over $\mathfrak{p}$, then $\mathfrak{p}S \subset \mathfrak{P}$ and $\mathfrak{P}$ is a minimal prime containing $\mathfrak{p}S$ by part 2. Since S is noetherian $\mathfrak{p}S$ has a primary decomposition

$$\mathfrak{p}S = \mathfrak{Q}_1 \cap \ldots \cap \mathfrak{Q}_r$$

and $\operatorname{rad}(\mathfrak{p}S) = \mathfrak{P}_1 \cap \ldots \cap \mathfrak{P}_r$ with $\mathfrak{P}_i = \operatorname{rad}(\mathfrak{Q}_i)$. Since $\mathfrak{p}S \subset \mathfrak{P}$ implies $\operatorname{rad}(\mathfrak{p}S) \subset \mathfrak{P}$ we conclude that $\mathfrak{P} \supset \mathfrak{P}_i$ for some i because otherwise the product of elements $f_j \in \mathfrak{P}_j \setminus \mathfrak{P}$ would be an element of $\operatorname{rad}(\mathfrak{p}S)$ whose factors do not lie in $\mathfrak{P}$, impossible since $\mathfrak{P}$ is prime. Since $\mathfrak{P}$ is a minimal prime over $\mathfrak{p}S$ we have $\mathfrak{P} = \mathfrak{P}_i$. Thus $\mathfrak{P}$ coincides with an associated prime of $\mathfrak{p}S$ which is minimal among the associated primes of $\mathfrak{p}S$.

Algebraic integers

Definition. Let $R \subset L$ be a ring extension. Then the **integral closure of R in L** is the set

$$S = \{s \in L \mid s \text{ is integral over } R\}$$

This is a ring because with $s_1, s_2 \in S$ the sum $s_1 + s_2 \in R[s_1, s_2]$ which is a finite extension of R. So $s_1 + s_2$ is integral over R as well. The same argument works for $s_1 s_2$.

The ring of **algebraic integers** is the integral closure of $\mathbb{Z}$ in $\mathbb{C}$. If $L = \mathbb{Q}(a_1, \ldots, a_n)$ is an algebraic number field, then $\mathbb{Z}_L$ denotes the integral closure of $\mathbb{Z}$ in L. This coincides with the ring of algebraic integers contained in L.
By the lying over theorem every non-zero prime ideal $\mathfrak{P} \subset \mathbb{Z}_L$ is a maximal ideal, since every prime ideal in $\mathbb{Z}$ is maximal.

If $\mathfrak{P} \subset \mathbb{Z}_L$ lies over (p) in $\mathbb{Z}$, then $\mathbb{F} = \mathbb{Z}_L/\mathfrak{P}$ is a finite extension field of $\mathbb{F}_p = \mathbb{Z}/(p)$.

Krull dimension

Definition. Let R be a ring. A **chain of prime ideals** in R is a sequence

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_\ell$$

of prime ideals. We call ℓ the **length** of the sequence.
The **Krull dimension** of R

$$\dim R = \sup\{\ell \mid \exists \text{ a chain of prime ideals of length } \ell \text{ in } R\}$$

is the maximal length of a chain of prime ideals in R.
Example. $\dim K[x_1, \ldots, x_n] = n$. Indeed

$$(0) \subsetneq (x_1) \subsetneq (x_1, x_2) \subsetneq \ldots \subsetneq (x_1, \ldots, x_n)$$

is a chain of prime ideals of length n. Thus

$$\dim K[x_1, \ldots, x_n] \geq n.$$

Proof of $\dim K[x_1, \ldots, x_n] = n$

To see equality, we note for prime ideals

$$\mathfrak{p} \subsetneq \mathfrak{p}' \subset K[x_1, \ldots, x_n] \implies d = \dim V(\mathfrak{p}) > \dim V(\mathfrak{p}').$$

Indeed, if we change coordinates such that the assumption of the tower of projections theorem is satisfied for $I = \mathfrak{p}$, then

$$K[x_{n-d+1}, \ldots x_n] \hookrightarrow K[x_1, \ldots, x_n]/\mathfrak{p}$$

is an integral ring extension. If $K[x_{n-d+1}, \ldots x_n] \cap \mathfrak{p}' = (0)$ then both $(0) \subsetneq \mathfrak{p}'/\mathfrak{p}$ would lie over $(0) \subset K[x_{n-d+1}, \ldots x_n]$ contradicting assertion 2) of the lying-over theorem. Thus

$$\mathfrak{q} = K[x_{n-d+1}, \ldots x_n] \cap \mathfrak{p}' \neq (0),$$

and $\dim V(\mathfrak{p}') = \dim V(\mathfrak{q}) < \dim \mathbb{A}^d$. □

Remark. Actually every maximal chain of prime ideals in $K[x_1, \ldots, x_n]$ has length n. This is usually proved with the so-called refined version of the Noether normalization.

Height of a prime ideal

More generally one has:

Theorem. *Let $A \subset \mathbb{A}^n$ be an irreducible algebraic set. Then every maximal chain of prime ideals in $K[A]$ has length* $\dim A$. □

This statement fails for algebraic sets which have components of different dimensions.

Definition. Let $\mathfrak{p}$ be a prime ideal in a ring R. The **height** of $\mathfrak{p}$ is

$$\text{height}(\mathfrak{p}) = \sup\{\ell \mid \exists \text{ a chain of prime ideals } \mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \ldots \subsetneq \mathfrak{p}_\ell \text{ with } \mathfrak{p}_\ell = \mathfrak{p}\}$$

Thus $\text{height}(\mathfrak{p}) = \dim R_{\mathfrak{p}}$. By the theorem above, we have for affine domains $R = K[A]$:

$$\text{height}(\mathfrak{p}) + \dim R/\mathfrak{p} = \dim R.$$