Outline

1. Filtrations and Rees Algebras
2. Krull Dimension
3. Rings of Polynomials
4. Homework
5. Finitely Generated Algebras
6. Noether Normalization
7. Associated Primes
8. Homework
9. Regular Sequences

Filtrations and Rees Algebras

Definition

A filtration of a ring R is a family $\mathcal{F}$ of subgroups F_i of R indexed by some set S. The most useful kinds are indexed by an ordered monoid S and are multiplicative

$$F_i \cdot F_j \subset F_{i+j}, \; i, j \in S.$$

They tend to be either *increasing* or *decreasing*, that is $F_i \subset F_j$ if $i < j$ or conversely.

Definition

The Rees algebra of $\mathcal{F}$ is the graded ring

$$R(\mathcal{F}) := \bigoplus_{i \in S} F_i,$$

with natural addition and multiplication. If the filtration is decreasing, there is another algebra attached to it, the associated graded ring

$$\mathrm{gr}_{\mathcal{F}}(R) := \bigoplus_{i \in S} F_i / F_{>i},$$

with $F_{>i} = \bigcup_{j>i} F_j$. If the filtration is increasing, the associated graded ring is defined similarly by changing the sign of i.

Some algebras of interest arise from special filtrations of a commutative ring, multiplicative decreasing $\mathbb{N}$–filtrations $\mathcal{F} = \{R_n,\ n \in \mathbb{N}\}$ of R where each R_n is an ideal of R, and

$$R_m \cdot R_n \subset R_{m+n}.$$

Its Rees algebra can be coded as a subring of the polynomial ring

$$R(\mathcal{F}) = \sum_{n \in \mathbb{N}} R_n t^n \subset R[t].$$

In addition to the associated graded ring as above, we also have the extended Rees algebra

$$R_e(\mathcal{F}) = R(\mathcal{F})[t^{-1}] = \sum_{n \in \mathbb{N}} R_n t^n \subset R[t, t^{-1}].$$

A major example is the I–adic filtration of an ideal I, $R_n = I^n,\ n \geq 0$. Its *Rees algebra*, which will be denoted by $R[It]$, has its significance centered on the fact that it provides an algebraic realization for the classical notion of blowing–up a variety along a subvariety, and plays an important role in the birational study of algebraic varieties, particularly in the study of desingularization.

Another filtration is the one associated to the symbolic powers $I^{(n)}$ of the ideal I. If I is a prime ideal, its nth symbolic power is the I–primary component of I^n. (There is a more general definition if I is not prime.) Its Rees algebra

$$\mathcal{R}(I) := \sum_{n \geq 0} I^{(n)} t^n,$$

the *symbolic Rees algebra* of I, also represents a blowup, inherits more readily the divisorial properties of R, but has its usefulness limited because it is not always Noetherian.
The presence of Noetherianess in $\mathcal{R}(I)$ is loosely linked to the number of equations necessary to define set–theoretically the subvariety $V(I)$. In turn, the lack of Noetherianess of certain cases has been used to construct counterexamples to Hilbert's 14th Problem.

Artin–Rees Lemma

This is a backbone of commutative algebra of nearly the same pedigree as Hilbert results in the 1870's papers.

Theorem (Artin-Rees Lemma)

Let R be a Noetherian ring and let I and J be two ideals. There exists an integer c such that for all $n \geq c$ the following equality holds

$$\boxed{J \cap I^n = I^{n-c}(J \cap I^c).} \tag{1}$$

Proof. Let $a_1, \ldots, a_n$ be a generating set of the ideal I and consider the R-subalgebra of the ring of polynomials $A = R[t]$,

$$B = R[a_1 t, \ldots, a_n t].$$

Since R is Noetherian and B is finitely generated, B is also Noetherian.
Grading A in the usual fashion, B is a graded subalgebra, the Rees algebra of I:

$$B = R + It + I^2 t^2 + \cdots + I^n t^n + \cdots .$$

Define $L_n = J \cap I^n$ and set

$$\mathcal{L} = L_0 + L_1 t + L_2 t^2 + \cdots + L_n t^n + \cdots .$$

$\mathcal{L}$ is clearly a homogeneous ideal of B, so there is a finite set of forms that generates it,

$$\mathcal{L} = (b_1 t^{d_1}, \ldots, b_s t^{d_s}).$$

In

$$\mathcal{L} = (b_1 t^{d_1}, \ldots, b_s t^{d_s}),$$

let $c = \sup\{d_1, \ldots, d_s\}$; for $n \geq c$, we must have

$$L_n = \sum_{i=1}^{s} I^{n-d_i} b_i,$$

from which the assertion

$$J \cap I^n = I^{n-c}(J \cap I^c)$$

follows.

Krull Intersection Theorem

Theorem

Let R be a Noetherian ring and let I be an ideal of R. If

$$L = \bigcap_{n \geq 1} I^n,$$

then $L = I \cdot L$. In particular, if I is contained in the Jacobson radical of R, then

$$\bigcap_{n \geq 1} I^n = 0.$$

Proof. It suffices to put $J = L$ in the Artin-Rees Lemma. The second assertion follows from Nakayama lemma:

Theorem (Nakayama Lemma)

Let M be a finitely generated R module and J its Jacobson radical. If $M = JM$, then $M = 0$.

Remark

Actually, using the Nakayama lemma one can give another description of L. Consider the multiplicative set $S = \{1 + a,\ a \in I\}$. In the ring $S^{-1}R$ the ideal $S^{-1}I$ is contained in the Jacobson radical. Thus the equality $S^{-1}L = S^{-1}I \cdot S^{-1}L$ implies (by Nakayama lemma) that $S^{-1}L = 0$. This means that there is $x \in I$ such that $(1 + x)L = 0$.

Remark

The theorem above applies equally to modules; more precisely, if M is a finitely generated R–module, then

$$L = \bigcap_{n \geq 1} I^n M,$$

satisfies $L = I \cdot L$.
This can be readily seen by making use of the idealization trick, *consisting in giving the direct sum $S = R \oplus M$ a ring structure by decreeing*

$$(a, x) \cdot (b, y) = (a \cdot b, a \cdot y + b \cdot x).$$

Now one applies the theorem to the ring S and its ideal $I \oplus M$.

Another important use of the Artin–Rees lemma is to the identification of two topologies defined by the powers of an ideal I. If M is a finitely generated module over a Noetherian ring R, then the family of submodules $\{I^n M \mid \forall n \geq 0\}$ defines a system of neighborhoods of $0 \in M$. If $N \subset M$ is a submodule, there are two topologies defined on N, the induced one, $\{I^n M \cap N\}$, and its own I-adic topology. The Artin-Rees lemma identifies them.

Outline

1. Filtrations and Rees Algebras
2. **Krull Dimension**
3. Rings of Polynomials
4. Homework
5. Finitely Generated Algebras
6. Noether Normalization
7. Associated Primes
8. Homework
9. Regular Sequences

Krull Dimension

The notion of dimension of a ring R is totally influenced by geometry, being given by lengths of chains of closed irreducible sets of its prime spectrum $\mathrm{Spec}(R)$. The great advantage here lies in the fact that such sets are each determined by a unique prime ideal,

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_n.$$

These are ideals that can be manipulated nicely, which will provide for many numerical estimates of lengths of chains of prime ideals.

- Codimension of ideals
- Systems of parameters
- Determinantal ideals

Codimension of Ideals

We introduce a measure of size for Noetherian rings and its ideals. Its justification lies on Theorem 10. A more numerical approach passes through the theory of Hilbert functions. There exists a method based on ordinary field theory that is good enough for most of our purposes that will be treated later. Some far-fetched arcane of homological algebra also serves this need to size up rings.

Definition

Let R be a Noetherian ring and let $\mathfrak{p}$ be a prime ideal.

- The *codimension* or *height* of $\mathfrak{p}$ is the supremum of the lengths of the chains of prime ideals contained in $\mathfrak{p}$.
- The height of an ideal I is the infimum of the heights of its minimal primes. The *Krull dimension* of R is the supremum of the heights of its prime ideals.

This definition can also be extended to modules. Given a finitely generated module M over a Noetherian R, its *dimension* $\dim M$ is the supremum of all $\dim R/\mathfrak{p}$, where $\mathfrak{p}$ runs through the set of associated primes of M.
This dimension equals the dimension of the ring R/I, where I is the annihilator of M. The height $\mathrm{codim}\, M$ of this ideal is called the *codimension* of M.

There is also a notion of *codimension of an algebra*, $A = k[x_1, \ldots, x_n]/I$: it is the codimension of the ideal I provided it does not contain any form of degree 1.

Krull Principal Ideal Theorem: PIT

The following result is central to the abstract theory of Noetherian rings. It is the bedrock on which many of its concepts are built. For its reach, its proofs tend to be surprisingly short. We will follow the treatment of Eisenbudbook.

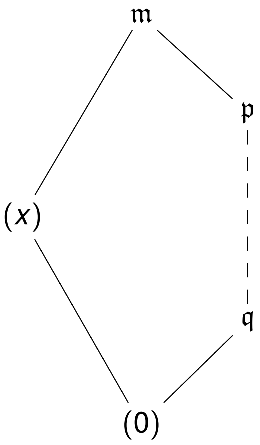
The reader is advised to read the lively discussion on dimension in Eisenbudbook.

Theorem

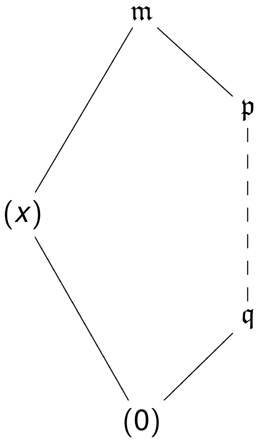
Let R be a Noetherian ring, x a non-unit of R and let $\mathfrak{m}$ be a minimal prime ideal over (x). Then $\operatorname{height} \mathfrak{m} \leq 1$.

Proof

We keep in mind the following diagram:



Our assumption says that there are no prime ideals between (x) and $\mathfrak{m}$.



- We will want to argue that if $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals, the situation described in the diagram cannot occur. By localizing R at $\mathfrak{m}$, we can assume R to be a local ring with $\mathfrak{m}$ as its maximal ideal.
- Consider the chain $(x) + \mathfrak{p}^{(n)}$, where $\mathfrak{p}$ is the prime ideal as in this diagram, and $\mathfrak{p}^{(n)}$ is the nth symbolic power of $\mathfrak{p}$. This is a descending chain of ideals, all of which contain (x). Since $R/(x)$ is a Noetherian ring with a single prime ideal, it must be Artinian.
- This means that for some $n \in \mathbb{Z}^+$ we have that

$$\mathfrak{p}^{(n)} \subset (x) + \mathfrak{p}^{(n+1)}.$$

- Therefore any $a \in \mathfrak{p}^{(n)}$ can be written as $a = rx + b$ where $r \in R$ and $b \in \mathfrak{p}^{(n+1)}$; since $\mathfrak{p}^{(n+1)} \subset \mathfrak{p}^{(n)}$ we have that $a - b = rx \in \mathfrak{p}^{(n)}$. However $x \notin \mathfrak{p}$ since $\mathfrak{m}$ is minimal over (x) and r is in $\mathfrak{p}^{(n)}$, and thus we have

$$\mathfrak{p}^{(n)} \subset x\mathfrak{p}^{(n)} + \mathfrak{p}^{(n+1)}. \tag{2}$$

- Since R is a local ring, we can apply Nakayama lemma to (2) and conclude that

$$\mathfrak{p}^{(n)} = \mathfrak{p}^{(n+1)}. \tag{3}$$

Localizing at $\mathfrak{p}$, this equality becomes

$$\mathfrak{p}_{\mathfrak{p}}^{n} = \mathfrak{p}_{\mathfrak{p}}^{n+1}. \tag{4}$$

We can apply Nakayama lemma to (4), and get that the maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$ of $R_{\mathfrak{p}}$ is nilpotent, and therefore $\mathfrak{p}$ cannot properly contain another prime. □

Krull Theorem

This theorem has the following fuller form.

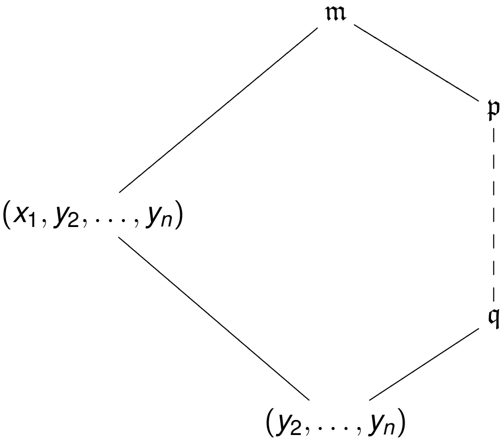
Theorem

Let R be a Noetherian ring and let $\mathfrak{m}$ *be a minimal prime ideal over* $(x_1, \ldots, x_n)$*. Then* $\operatorname{height} \mathfrak{m} \leq n$*.*

A consequence of this result is that prime ideals of Noetherian rings have finite height and thus $\operatorname{Spec}(R)$ satisfies the descending chain condition. In particular if R is a local ring then $\dim R < \infty$.

Proof

The picture the proof:



We may assume that R is a local ring with $\mathfrak{m}$ as its maximal ideal. Let $\mathfrak{p}$ be any prime ideal with no other prime between itself and $\mathfrak{m}$.
It will be enough to show that $\mathfrak{p}$ is a minimal prime over an ideal generated by $n-1$ elements.

We have that one of the x_i, say x_1, does not belong to $\mathfrak{p}$.
Consider the ideal $(\mathfrak{p}, x_1)$; the ring $R/(\mathfrak{p}, x_1)$ is Artinian, since the only maximal ideal is the image of $\mathfrak{m}$. Therefore there exists an integer s such that

$$\mathfrak{m}^s \subset (\mathfrak{p}, x_1).$$

In particular all the s-th powers of the x_i are contained in $(\mathfrak{p}, x_1)$; thus we can find $y_i \in \mathfrak{p}$ and $a_i \in R$ such that

$$x_i^s = y_i + a_i x_1,$$

for $i = 2, \ldots, n$. We claim that $\mathfrak{p}$ is minimal over $(y_2, \ldots, y_n)$. Note that $\mathfrak{m}$ is minimal over $(x_1, y_2, \ldots, y_n)$. Suppose there exists a prime ideal, say $\mathfrak{q}$, between $\mathfrak{p}$ and $(y_2, \ldots, y_n)$ and view this diagram in the ring $R/(y_2, \ldots, y_n)$, we have a situation that would contradict Krull's PIT. $\square$

Systems of Parameters

From the proof of Krull's theorem we restate what essentially is a converse:

Theorem

Let R be a Noetherian ring and let $\mathfrak{p}$ be a prime ideal of height r. Then $\mathfrak{p}$ is a minimal prime over an ideal $(x_1, \ldots, x_r)$ generated by r elements.

The set $\{x_1, \ldots, x_r\}$ is called a *system of parameters* for $\mathfrak{p}$. In the case of a local ring R, a system of parameters for its maximal ideal is also called a system of parameters of R.

Example

Let $\mathbf{R} = k[[x_1, \ldots, x_n]]$ be the ring of formal power series over the field k.

$$(0) \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, \ldots, x_n)$$

is a chain of prime ideals of $\mathbf{R}$,

$$\dim \mathbf{R} \geq n.$$

By Krull PIT, $\dim \mathbf{R} \leq n$.

Outline

1. Filtrations and Rees Algebras
2. Krull Dimension
3. **Rings of Polynomials**
4. Homework
5. Finitely Generated Algebras
6. Noether Normalization
7. Associated Primes
8. Homework
9. Regular Sequences

Rings of Polynomials

Proposition

Let R be a Noetherian ring and let $\mathfrak{P}$ be a prime ideal of the polynomial ring $R[x]$, and set $\mathfrak{p} = R \cap \mathfrak{P}$. Then

$$\operatorname{height} \mathfrak{P} = \begin{cases} \operatorname{height} \mathfrak{p}, & \text{if } \mathfrak{P} = \mathfrak{p}R[x], \\ \operatorname{height} \mathfrak{p} + 1, & \text{otherwise} \end{cases}$$

Proof

Proof. It is clear that if $\mathfrak{p}$ is a prime ideal of R, then $\mathfrak{p}R[x]$ is the kernel of the canonical homomorphism

$$\psi : R[x] \mapsto (R/\mathfrak{p})[x],$$

and is therefore a prime ideal of $R[x]$. If follows that if

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_s$$

is a chain of primes of R. Then

$$\mathfrak{p}_0 R[x] \subset \mathfrak{p}_1 R[x] \subset \cdots \subset \mathfrak{p}_s R[x]$$

is a chain of primes of $R[x]$ of the same length, which shows that

$$\text{height } \mathfrak{p} \leq \text{height } \mathfrak{p}R[x].$$

To prove the reverse inequality, we may localize at $\mathfrak{p}$ without affecting the height of the prime ideals $\mathfrak{p}$ and $\mathfrak{p}R[x]$. Let $(x_1, \ldots, x_s)$ be a system of parameters for $\mathfrak{p}$. By definition there exists an integer m such that $\mathfrak{p}^m R_{\mathfrak{p}} \subset (x_1, \ldots, x_s)R_{\mathfrak{p}}$, from which it is clear that $\mathfrak{p}^m R[x]_{\mathfrak{p}} \subset (x_1, \ldots, x_s)R[x]_{\mathfrak{p}}$, and thus by Krull's PIT, $\operatorname{height} \mathfrak{p}R[x]_{\mathfrak{p}} \leq s$, which takes care of the first assertion.

Suppose now $\mathfrak{P}$ is not an extended prime of $R[x]$, that is $\mathfrak{p} = \mathfrak{P} \cap R$, $\mathfrak{P} \neq \mathfrak{p}R[x]$. This means that $\operatorname{height} \mathfrak{P} \geq \operatorname{height} \mathfrak{p} + 1$. We may again localize at $\mathfrak{p}$, so that for simplicity of notation, assume that $(R, \mathfrak{p})$ is a local ring. We then have the embedding

$$\mathfrak{P}/\mathfrak{p}R[x] \hookrightarrow R[x]/\mathfrak{p}R[x] = (R/\mathfrak{p})[x]$$

into a principal ideal domain. Therefore $\mathfrak{P}/\mathfrak{p}R[x]$ is going to be generated by a single element, or equivalently

$$\mathfrak{P} = (f, \mathfrak{p}R[x]).$$

Clearly $\mathfrak{P}$ is minimal over $(x_1, \ldots, x_s, f)$, hence by Krull's PIT

$$\operatorname{height}_{R[x]} \mathfrak{P} \leq 1 + s = 1 + \operatorname{height}_R \mathfrak{p},$$

as desired. $\square$

Dimension of Polynomial Rings

Theorem

Let R be a Noetherian ring and let $x_1, \ldots, x_n$ be a set of independent indeterminates over R. Then

$$\dim R[x_1, \ldots, x_n] = \dim R + n.$$

In particular if R is a field k, then

$$\dim k[x_1, \ldots, x_n] = n.$$

Codimension of Determinantal Ideals

Let R be a Noetherian ring and let φ be a $m \times n$ matrix with entries in R:

$$\varphi = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}.$$

Estimating the sizes of the ideal $I_t(\varphi)$ generated by all $t \times t$ minors of φ is important for many of our constructions.

Krull PIT is the case of a matrix $[a_1, a_2, \ldots, a_n]$

Eagon-Northcott Formula

The classical bound for the sizes $EN(m, n; t)$ of these ideals is the theorem of Eagon and Northcott:

Theorem

The ideals $I_t(\varphi)$ satisfy

$$\boxed{\text{height } I_t(\varphi) \leq EN(m, n; t) = (m - t + 1)(n - t + 1),} \quad (5)$$

where equality is reached when φ is a generic matrix in $m \cdot n$ indeterminates.

Proof

We only prove the first assertion, leaving the rest to the reader. The case $t = 1$ is Krull's PIT, so that we may assume $t \geq 2$. Denote $I = I_t(\varphi)$ and let $\mathfrak{p}$ be a minimal prime of I. Localizing at $\mathfrak{p}$ we may assume that R is a local ring and denote still by $\mathfrak{p}$ its maximal ideal; it is enough to show that $\dim R \leq EN(m, n; t)$.

If one of the entries of φ is a unit, say a_{11} is an invertible element of R, through a series of elementary row and column operations the matrix φ can be transformed into a matrix

$$\left[\begin{array}{c|ccc} 1 & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & \varphi' & \\ 0 & & & \end{array}\right].$$

Since $t > 1$, it is clear that $I_t(\varphi) = I_{t-1}(\varphi')$. We induct on t, which means that all the entries of φ may be assumed to lie in the maximal ideal of R.

Consider now the matrix

$$\psi = \begin{bmatrix} a_{11} + x & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix},$$

where x is an indeterminate over R and let $L = I_t(\psi)$.

- Since $t > 1$, note that $L \subset \mathfrak{p}R[x]$, so in particular $\mathrm{height\ L} \leq \dim R$. On the other hand, $(L, x) = (I, x)$, from which we claim that L is $\mathfrak{p}R[x]$–primary.
- Otherwise there would exist a minimal prime $\mathfrak{Q}$ of L properly contained in $\mathfrak{p}R[x]$. But then, in the ring $R[x]/\mathfrak{Q}$, the image of $(\mathfrak{p}, x)$ would be a maximal ideal of codimension at least two, but minimal over the principal ideal generated by the image of x.
- This would contradict Krull PIT. We may now localize at $\mathfrak{p}R[x]$ and decrement t.

Outline

1. Filtrations and Rees Algebras
2. Krull Dimension
3. Rings of Polynomials
4. **Homework**
5. Finitely Generated Algebras
6. Noether Normalization
7. Associated Primes
8. Homework
9. Regular Sequences

Homework

1. Give an example of a Noetherian ring of infinite Krull dimension.
2. Give an example of a commutative ring R of dimension 1 such that $\dim R[x] = 3$.

Outline

1. Filtrations and Rees Algebras
2. Krull Dimension
3. Rings of Polynomials
4. Homework
5. **Finitely Generated Algebras**
6. Noether Normalization
7. Associated Primes
8. Homework
9. Regular Sequences

Finitely Generated Algebras

Let k be a field. A finitely generated k-algebra is a homomorphic image of a ring of polynomials over k,

$$\mathbf{R} = k[x_1, \ldots, x_n]/I$$

- Apply our theory of Krull dimension to **R** and relate it to another notion of dimension.
- This is connected to another topic.

Do polynomials have roots?

Let $\mathbf{f}(\mathbf{x}) = \mathbf{f}(x_1, \ldots, x_n)$ be a nonconstant polynomial of $R = \mathbb{C}[\mathbf{x}] = \mathbb{C}[x_1, \ldots, x_n]$, $n > 1$.

Fact: There is $\mathbf{c} \in \mathbb{C}^n$ such that $\mathbf{f}(\mathbf{c}) = 0$.
The answer is easy when

$$\mathbf{f}(x_1, \ldots, x_n) = x_n^d + \mathbf{g}(x_1, \ldots, x_n),$$

where $\mathbf{g}(\mathbf{x})$ is a polynomial of degree $< d$ in the variable x_n. So what is the solution for the general case? One seeks a change of variables (possibly linear)

$$\begin{aligned} \mathbf{x} &\rightarrow \mathbf{y}, \quad [\mathbf{x}] = [\mathbf{y}]\mathbf{A} \\ \mathbf{f}(\mathbf{x}) &= \mathbf{f}(\mathbf{y}\mathbf{A}) = \mathbf{g}(\mathbf{y}) \end{aligned}$$

so that $\mathbf{g}(\mathbf{y})$ has the appropriate form.

More generally, let $\mathbf{f}_1(\mathbf{x}), \ldots, \mathbf{f}_m(\mathbf{x})$ be a set of elements of $R = \mathbb{C}[\mathbf{x}]$.

Question: What are the obstructions to finding $\mathbf{c} \in \mathbb{C}^n$ such that

$$\mathbf{f}_1(\mathbf{c}) = \mathbf{f}_2(\mathbf{c}) = \cdots = \mathbf{f}_m(\mathbf{c}) = 0 \text{ ?}$$

Obviously one is: there exist $\mathbf{g}_1(\mathbf{x}), \ldots, \mathbf{g}_m(\mathbf{x})$ such that

$$\mathbf{g}_1(\mathbf{x})\mathbf{f}_1(\mathbf{x}) + \cdots + \mathbf{g}_m(\mathbf{x})\mathbf{f}_m(\mathbf{x}) = 1$$

What else?

Hilbert Nullstellensatz

Let k be a field and denote by $\overline{k}$ its algebraic closure. The Hilbert Nullstellensatz is about qualitative results about systems of polynomial equations.

Let $\mathbf{f}_i(x_1, \ldots, x_n) \in R = k[x_1, \ldots, x_n]$, $1 \leq i \leq m$, be a set of polynomials.

Definition

The algebraic variety defined by the $\mathbf{f}_i$ is the set

$$V(\mathbf{f}_1, \ldots, \mathbf{f}_m) = \{\mathbf{c} = (c_1, \ldots, c_n) \in \overline{k}^n : \mathbf{f}_i(\mathbf{c}) = 0, \quad 1 \leq i \leq m.\}$$

A hypersurface is a variety defined by a single equation $V(\mathbf{f})$.

Remark

If I is the ideal generated by the $\mathbf{f}_i$, then $V(I) = V(\mathbf{f}_1, \ldots, \mathbf{f}_m)$.

Hilbert Nullstellensatz

Theorem

If the ideal $I \subset R = k[x_1, \ldots, x_n]$ is proper, i.e. $I \neq R$, then $V(I) \neq \emptyset$.

Proof. We make two reductions.

1. Let $\mathfrak{m}$ be a maximal ideal of R containing I. Since $V(\mathfrak{m}) \subset V(I)$, ETA that I is maximal.
2. The ring of polynomials $S = \overline{k}[x_1, \ldots, x_n]$ is integral over $R = k[x_1, \ldots, x_n]$. By Lying-over, there is a maximal ideal M of S such that $M \cap R = \mathfrak{m}$. Since $V(M) \subset V(\mathfrak{m})$, ETA that I is a maximal ideal and k is algebraically closed.

Nullstellensatz

After these reductions the assertion is:

Theorem

If k is an algebraically closed field and M is a maximal ideal of $R = k[x_1, \ldots, x_n]$, then there is

$$\mathbf{c} = (c_1, \ldots, c_n) \in k^n$$

such that

$$\mathbf{f}(\mathbf{c}) = 0 \quad \forall \mathbf{f}(\mathbf{x}) \in M.$$

Special case: $\mathbb{C}$

Consider the field $\mathbf{F} = \mathbb{C}[x_1, \ldots, x_n]/M$.

Proposition

It is ETS that $\mathbf{F}$ *is isomorphic to* $\mathbb{C}$*.*

Proof. Indeed, if $\mathbf{F} \simeq \mathbb{C}$, for each indeterminate x_i its equivalence class in $k[x_1, \ldots, x_n]/M$ contains some element c_i of $\mathbb{C}$, that is $x_i - c_i \in M$. this means that

$$(x_1 - c_1, \ldots, x_n - c_n) \subset M.$$

But $(x_1 - c_1, \ldots, x_n - c_n)$ is also a maximal ideal, therefore it is equal to M. Clearly every polynomial of M vanishes at $\mathbf{c} = (c_1, \ldots, c_n)$. □

Proof of $\mathbb{C} = \mathbb{C}[x_1, \ldots, x_n]/M$

1. ETS that the extension $\mathbb{C} \to \mathbf{F} = \mathbb{C}[x_1, \ldots, x_n]/M$ is algebraic.
2. Observe that $[\mathbf{F} : \mathbb{C}]$ is countable, **F** being a homomorphic image of the countably generated vector space $\mathbb{C}[x_1, \ldots, x_n]$.
3. If **F** is not algebraic over $\mathbb{C}$, suppose $t \in \mathbf{F}$ is transcendental over $\mathbb{C}$.
4. Consider the uncountable set $\{1/(t - c), c \in \mathbb{C}\}$.

Since they cannot be linearly independent, there are distinct c_i, $1 \leq i \leq m$ and nonzero $r_i \in \mathbb{C}$ such that

$$r_1 \frac{1}{t - c_1} + \cdots + r_m \frac{1}{t - c_m} = 0.$$

Clearing denominators gives the equality of two polynomials of $\mathbb{C}[t]$:

$$r_1(t - c_2)(t - c_3) \cdots (t - c_m) = (t - c_1)\mathbf{g}(t),$$

which is a contradiction as the c_i are distinct.

Outline

1. Filtrations and Rees Algebras
2. Krull Dimension
3. Rings of Polynomials
4. Homework
5. Finitely Generated Algebras
6. **Noether Normalization**
7. Associated Primes
8. Homework
9. Regular Sequences

NNL: Noether Normalization Lemma

Definition

A finitely generated algebra R over a field k is a homomorphic image of a ring of polynomials over k,

$$k[x_1, \ldots, x_n]/I \simeq R = k[a_1, \ldots, a_n].$$

Theorem (NNL)

If R is finitely generated over k, there is a subalgebra

$$S = k[y_1, \ldots, y_r] \hookrightarrow R$$

such that the y_i are algebraically independent and R is integral over S. S is called a Noether Normalization of R.

From NNL to Nullstellensatz

1. Let M be a maximal ideal of $k[x_1, \ldots, x_n]$, $k = \overline{k}$. We will show that $M = (x_1 - c_1, \ldots, x_n - c_n)$, $c_i \in k$.
2. Using the NNL, let $S = k[y_1, \ldots, y_r] \hookrightarrow R = k[x_1, \ldots, x_n]/M$ be a Noether normalization. Since R is a field, S is also a field, thus $r = 0$.
3. This gives that $S = k \to R$ is a finite extension, so $k = R$.

Another version of the Nullstellensatz

Theorem

Let I be an ideal of $R = k[x_1, \ldots, x_n]$ and $\mathbf{f} \in R$ a polynomial. Then

$$V(I) \subset V(\mathbf{f}) \Leftrightarrow \mathbf{f} \in \sqrt{I}$$

that is, there is a power $\mathbf{f}^r \in I$.

Proof. In one direction it is clear.

Suppose $V(I) \subset V(\mathbf{f})$. Consider the ideal L in the polynomial ring with one extra variable

$$L = (I, 1 - t\mathbf{f}) \subset k[x_1, \ldots, x_n, t].$$

Since each zero of I is a zero of $\mathbf{f}$, $L = (I, 1 - t\mathbf{f})$ has no zeros. Thus by the Nullstellensatz $L = (1)$. This means that there is an equation

$$\sum \mathbf{g}_i \mathbf{f}_i + (1 - t\mathbf{f})\mathbf{g} = 1, \quad \mathbf{f}_i \in I, \mathbf{g}_i, \mathbf{g} \in R[t].$$

Replacing $t \to 1/\mathbf{f}$ and clearing denominators gives an equation

$$\mathbf{f}^r = \sum \mathbf{h}_i \mathbf{f}_i, \quad \mathbf{h}_i \in R$$

Example

Let

$$R = k[x, y]/(y^2 - 2xy + x^3)$$

Set $y_1 = \overline{x}$ and

$$S = k[y_1] \subset R$$

Note that $\overline{y}$ is integral over S, so R is integral over S. Finally,

$$S \simeq k[x]/(k[x] \cap (y^2 - 2xy + x^3)) = k[x]$$

Example

1. If $R = k[x, y]/(xy + x + y)$, need a preparation: change variables $x \to x_1$, $y \to x_1 + y_1$, so

$$xy + x + y \to x_1(x_1 + y_1) + x_1 + x_1 + y_1 = x_1^2 + x_1 y_1 + 2x_1 + y_1$$

2. Get the NN by choosing

$$S = k[y_1] \hookrightarrow R = k[x, y]/(xy + x + y).$$

Proof of NN

Let R be a commutative ring and B a finitely generated R-algebra, $B = R[x_1, \ldots, x_d]$. The expression *Noether normalization* usually refers to the search-as effectively as possible-of more amenable finitely generated R-subalgebras $A \subset B$ over which B is finite. This allows for looking at B as a finitely generated A-module and therefore applying to it methods from homological algebra or even from linear algebra.

When R is a field, two such results are: (i) the classical *Noether normalization lemma*, that asserts when it is possible to choose A to be a ring of polynomials, or (ii) how to choose A to be a hypersurface ring over which B is birational. We review these results since their constructive steps are very useful in our discussion of the integral closure of affine rings.

Affine Rings

Let $B = k[x_1, \dots, x_n]$ be a finitely generated algebra over a field k and assume that the x_i are algebraically dependent. Our goal is to find a new set of generators $y_1, \dots, y_n$ for B such that

$$k[y_2, \dots, y_n] \hookrightarrow B = k[y_1, \dots, y_n]$$

is an integral extension.

Let $k[X_1, \dots, X_n]$ be the ring of polynomials over k in n variables; to say that the x_i are algebraically dependent means that the map

$$\pi\colon\ k[X_1, \dots, X_n] \to B, \quad X_i \mapsto x_i$$

has non-trivial kernel, call it I.

Assume that f is a nonzero polynomial in I,

$$f(X_1, \ldots, X_n) = \sum_{\alpha} a_\alpha X_1^{\alpha_1} X_2^{\alpha_2} \cdots X_n^{\alpha_n},$$

where $0 \neq a_\alpha \in k$ and all the multi-indices $\alpha = (\alpha_1, \ldots, \alpha_n)$ are distinct. Our goal will be fulfilled if we can change the X_i into a new set of variables, the Y_i, such that f can be written as a monic (up to a scalar multiple) polynomial in Y_1 and with coefficients in the remaining variables, i.e.

$$f = aY_1^m + b_{m-1} Y_1^{m-1} + \cdots + b_1 Y_1 + b_0, \tag{6}$$

where $0 \neq a \in k$ and $b_i \in k[Y_2, \ldots, Y_n]$.

We are going to consider two changes of variables that work for our purposes: the first one, a clever idea of Nagata, does not assume anything about k; the second one assumes k to be infinite and has certain efficiencies attached to it.

The first change of variables replaces the X_i by Y_i given by

$$Y_1 = X_1,\ \ Y_i = X_i - {X_1}^{p^{i-1}} \text{for } i \geq 2,$$

where p is some integer yet to be chosen.
If we rewrite f using the Y_i instead of the X_i, it becomes

$$f = \sum_{\alpha} a_\alpha Y_1^{\alpha_1}(Y_2 + Y_1^{p})^{\alpha_2} \cdots (Y_n + Y_1^{p^{n-1}})^{\alpha_n}. \tag{7}$$

Expanding each term of this sum, there will be only one term pure in Y_1, namely

$$a_\alpha Y_1^{\alpha_1+\alpha_2 p+\cdots+\alpha_n p^{n-1}}.$$

Furthermore, from each term in (7) we are going to get one and only one such power of Y_1. Such monomials have higher degree in Y_1 than any other monomial in which Y_1 occurs. If we choose $p > \sup\{\alpha_i \mid a_\alpha \neq 0\}$, then the exponents $\alpha_1 + \alpha_2 p + \cdots + \alpha_n p^{n-1}$ are distinct since they have different p-adic expansions. This provides for the required equation.

If k is an infinite field, we consider another change of variables that preserves degrees. It will have the form

$$Y_1 = X_1,\ Y_i = X_i - c_i X_1 \text{ for } i \geq 2,$$

where the c_i are to be properly chosen. Using this change of variables in the polynomial f, we obtain

$$f = \sum_{\alpha} a_\alpha Y_1^{\alpha_1} (Y_2 + c_2 Y_1)^{\alpha_2} \cdots (Y_n + c_n Y_1)^{\alpha_n}. \tag{8}$$

We want to make choices of the c_i in such a way that when we expand (8) we achieve the same goal as before, i.e. a form like that in (6). For that, it is enough to work on the homogeneous component f_d of f of highest degree, in other words, we can deal with f_d alone. But

$$f_d(Y_1, \ldots, Y_n) = h_0(1, c_2, \ldots, c_n) Y_1^d + h_1 Y_1^{d-1} + \cdots + h_d,$$

where h_i are homogeneous polynomials in $k[Y_2, \ldots, Y_n]$, with $\deg h_i = i$, and we can view $h_0(1, c_2, \ldots, c_n)$ as a nontrivial polynomial function in the c_i. Since k is infinite, we can choose the c_i, so that $0 \neq h_0(1, c_2, \ldots, c_n) \in k$.

Theorem (Noether Normalization)

Let k be a field and $B = k[x_1, \ldots, x_n]$ a finitely generated k-algebra; then there exist algebraically independent elements $z_1, \ldots, z_d$ of B such that B is integral over the polynomial ring $A = k[z_1, \ldots, z_d]$.

Proof. We may assume that the x_i are algebraically dependent. From the preceding, we can find $y_1, \ldots, y_n$ in B such that

$$k[y_2, \ldots, y_n] \hookrightarrow k[y_1, \ldots, y_n] = B$$

is an integral extension, and if necessary we iterate. □

Corollary

Let k be a field and $\psi : A \mapsto B$ a k-homomorphism of finitely generated k-algebras. If $\mathfrak{P}$ is a maximal ideal of B then $\mathfrak{p} = \psi^{-1}(\mathfrak{P})$ is a maximal ideal of A.

Proof. Consider the embedding

$$A/\mathfrak{p} \hookrightarrow B/\mathfrak{P}$$

of k-algebras, where by the preceding $B/\mathfrak{P}$ is a finite dimensional k-algebra. It follows that the integral domain $A/\mathfrak{p}$ is also a finite dimensional k-vector space and therefore must be a field. □