Computer Algebra and Gröbner Bases

Frank-Olaf Schreyer

Saarland University WS 2020/21

Overview

Today's topics are decomposition into irreducible components, Noetherian rings and primary decomposition.

1. Component decomposition
2. Noetherian rings
3. Primary ideals and primary decomposition

Component decomposition

Last time we saw that

$$V(xy, yz) = V(y) \cup V(x, z)$$

is a decomposition into irreducible algebraic subsets.

Theorem. *Let K be an algebraically closed field, and let $A \subset \mathbb{A}^n$ be an algebraic subset. Then there exist finitely may irreducible algebraic subsets $C_j \subset \mathbb{A}^n$ such that*

$$A = C_1 \cup C_2 \cup \ldots \cup C_r.$$

Definition. A component decomposition $A = C_1 \cup C_2 \cup \ldots C_r$ is called **irredundant** if $C_i \not\subset C_j$ for $i \neq j$.

By deleting C_i which are contained in a C_j one can pass from a component decomposition to an irredundant one.

Uniqueness of the component decomposition

Theorem. *An irredundant decomposition* $A = C_1 \cup C_2 \cup \ldots \cup C_r$ *into irreducible algebraic sets* C_j *is unique up to the order.*

Proof. Suppose

$$A = C_1 \cup C_2 \cup \ldots \cup C_r = C_1' \cup C_2' \cup \ldots \cup C_s'$$

are two irredundant decompositions. Then each C_ℓ' is contained in some C_j because

$$C_\ell' = (C_\ell' \cap C_1) \cup (C_\ell' \cap C_2) \cup \ldots \cup (C_\ell' \cap C_r)$$

implies $C_\ell' = (C' \cap C_j)$ for some j since C_ℓ' is irreducible. Similarly each $C_j \subset C_k'$ for some k. So $C_\ell' \subset C_j \subset C_k'$ and we have equality because $C_1' \cup C_2' \cup \ldots \cup C_s'$ is irredundant. Thus each C_ℓ' a coincides with unique C_j and vice versa. In particular $r = s$. □

Towards the existence of a component decomposition

Suppose $A \subset \mathbb{A}^n$ is an algebraic set. If A is irreducible, we are done. Otherwise we can can decompose

$$A = A_1 \cup A_2$$

into proper algebraic subsets. If these are irreducible we are done, otherwise we decompose each reducible subset again. Thus we get a tree of smaller and smaller algebraic subsets.

The problem is to show that this process terminates. If we translate this with our algebra geometry dictionary, we get a tree of larger and larger radical ideals of $K[x_1, \ldots, x_n]$.

Noetherian rings

Theorem. *Let R be a ring. TFAE*

1) *Each ideal $I \subset R$ is finitely generated.*
2) *Every ascending chain of ideals*

$$I_1 \subset I_2 \subset \ldots \subset I_k \subset \ldots$$

becomes stationary, i.e., there exists an N such that $I_N = I_{N+1} = I_{N+2} = \ldots.$

3) *Every nonempty set $\mathcal{M}$ of ideals contains maximal elements with respect to inclusion, i.e.,*

$$\exists\, I \in \mathcal{M} \text{ such that } I \subset J \Rightarrow I = J\ \forall J \in \mathcal{M}.$$

It was Emmy Noether who noticed the importance of these conditions. To honor her we call rings which statisfy the equivalent conditions **noetherian**. By Hilbert's basis theorem $K[x_1, \ldots, x_n]$ is noetherian.

Proof of the theorem

1) $\Rightarrow$ 2): Let $I_1 \subset I_2 \subset \ldots$ be a chain of ideals. Then

$$J = \bigcup_{j=1}^{\infty} I_j$$

is an ideal as well:

$$f, g \in J \Rightarrow f \in I_k, g \in I_\ell \text{ for indices } \ell, k \in \mathbb{N}$$
$$\Rightarrow f + g \in I_{\max(k,\ell)} \subset J$$

By 1) the ideal J is finitely generated, say $J = (f_1, \ldots, f_r)$. Each $f_k \in I_{j(k)}$. If we take $N = \max\{j(k) \mid k = 1, \ldots, r\}$, then

$$J = (f_1, \ldots, f_r) \subset I_N \subset I_{N+1} \subset \ldots \subset J$$

and we have equality $I_k = I_{k+1}\ \forall k \geq N$.

Proof of the theorem, 2

2) $\Rightarrow$ 3): Let $\mathcal{M}$ be a non-empty set of ideals. Suppose there are no maximal elements in $\mathcal{M}$. Then for each $I \in \mathcal{M}$ we find a $J \in \mathcal{M}$ with $I \subsetneq J$. Inductively we find a chain

$$I_1 \subsetneq I_2 \subsetneq \dots$$

which does not become stationary in contradiction to 2).

3) $\Rightarrow$ 1): Let J be an ideal and consider the set

$$\mathcal{M} = \{I \subset J \mid I \text{ is finitely generated}\}.$$

$\mathcal{M} \neq \emptyset$ because $(0) \in \mathcal{M}$. Let $I = (f_1, \dots, f_r) \in \mathcal{M}$ be a maximal element. We have to prove $I = J$. Let $f \in J$ be an arbitrary element. Then also $(f_1, \dots, f_r, f)$ is finitely generated and $I \subset (f_1, \dots, f_r, f) \in \mathcal{M}$. By the maximality of I we get $I = (f_1, \dots, f_r, f)$, i.e., $f \in I$. This proves $J \subset I$ and equality holds. $\square$

Existence of the component decomposition

Using our dictionary we obtain

Corollary.

2') *Every descending chain of algebraic subsets*

$$A_1 \supset A_2 \supset \dots$$

becomes stationary.

3') *Every nonempty set $\mathcal{M}$ of algebraic subsets of $\mathbb{A}^n$ has a minimal element with respect to inclusion.* □

To prove the existence of a component composition is a typical proof by the so-called noetherian induction: Consider the set

$$\mathcal{M} = \{A \subset \mathbb{A}^n \,|A \text{ is an nonempty algebraic set, which is not a finite union of irreducible algebraic subsets}\}$$

We have to prove that $\mathcal{M} = \emptyset$.

Existence of the component decomposition, continued

Suppose $\mathcal{M} \neq \emptyset$. Then we can consider a minimal element $A \in \mathcal{M}$. A is not irreducible by the definition of $\mathcal{M}$. Thus there exists a decomposition

$$A = A_1 \cup A_2$$

in strictly smaller algebraic sets. By the minimality of A both A_1 and A_2 are finite unions of irreducible algebraic sets. But then so is A, a contradiction. We must have $\mathcal{M} = \emptyset$. □

The same argument shows

Theorem. *Let R be a noetherian ring. Every radical ideal $I \subset R$ is a finite intersection of prime ideals*

$$I = \mathfrak{p}_1 \cap \mathfrak{p}_2 \cap \ldots \cap \mathfrak{p}_r.$$

Remark. Note that a finite intersection of prime ideals in an arbitrary ring is always a radical ideal.

A natural appearance of non-radical ideals in geometry

Consider the intersection

$$V(xy, yz) \cap V(y-x-t) = V(xy, yz, y-x-t)$$

with a moving plane $H_t = V(y - x - t)$. For $t \neq 0$ the intersection consists of the line $L_t = V(y, x + t)$ and the point $p_t = V(x, z, y - t)$. For $t = 0$ the intersection is defined by the ideal

$$(xy, yz, y - x) = (x^2, xz, y - x).$$

This is not a radical ideal.

Continuation of the example

Definition. Let M be an R-module and $m \in M$. The **annihilator** of m is the ideal

$$\operatorname{ann}(m) = \{a \in R \mid am = 0 \in M\}.$$

The annihilator of $\overline{x} \in K[x, y, z]/(x^2, xz, y - x)$ as an $K[x, y, z]$-module is

$$\operatorname{ann}(\overline{x}) = (x, z, y - x) = (x, y, z).$$

The corresponding point $V(x, y, z)$ is the limit of the point $p_t = (0, t, 0)$ for $t \to 0$, which lies in the limit line $L_0 = V(y, z)$ of the L_t's.

Primary ideals

Definition. A **primary ideal** $\mathfrak{q}$ in a ring R is a proper ideal satisfying

$$fg \in \mathfrak{q} \Rightarrow f \in \mathfrak{q} \text{ or } g^n \in \mathfrak{q} \text{ for some } n \in \mathbb{N}$$

for all $f, g \in R$.

Proposition. *The radical* $\mathfrak{p} = \text{rad}(\mathfrak{q})$ *of a primary ideal* $\mathfrak{q}$ *is a prime ideal.* In this situation, $\mathfrak{q}$ is called a $\mathfrak{p}$-primary ideal.

Proof of the proposition. Suppose $fg \in \text{rad}(\mathfrak{q})$ and $g \notin \text{rad}(\mathfrak{q})$. Then a power $(fg)^n = f^n g^n \in \mathfrak{q}$. Since no power of g^n lies in $\mathfrak{q}$ we have $f^n \in \mathfrak{q}$ by the defining property of primary ideals. Thus $f^n \in \mathfrak{q}$ and $f \in \text{rad}(\mathfrak{q})$. □

Primary decomposition

Theorem. *Let $I \subsetneq R$ be a proper ideal in a noetherian ring R. Then I is a finite intersection*

$$I = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r.$$

of primary ideals $\mathfrak{q}_j$.

Remark. Emanuel Lasker proved this theorem for polynomial rings in 1905. Emmy Noether gave a simplified proof for arbitrary noetherian rings in 1921.

Emmy Noether's proof is another case of noetherian induction.

Existence of the primary decomposition

We proceed in two steps.

Definition. An ideal I statisfying

$$I = I_1 \cap I_2 \Rightarrow I_1 = I \text{ or } I_2 = I$$

for all ideal $I_1, I_2 \subset R$ is called **irreducible**.

Step 1. By property 3) in the definition of noetherian rings, the set of ideals which are not the intersection of finitely many irreducible ideals is empty by the same argument as in the component decomposition.

Step 2. *Irreducible ideals are primary ideals.*

Let $I \subsetneq$ be an irreducible ideal, $fg \in I$ and $f \notin I$. We have to prove that some power $g^m \in I$. Consider the ascending chain of ideals

$$I : g \subset I : g^2 \subset \ldots.$$

By property 2) in the definition of noetherian rings there exists an $m \in \mathbb{N}$ such that

$$I : g^m = I : g^{m+1}.$$

Existence of the primary decomposition continued

We first claim

$$I : g^m = I : g^{m+1} \implies (I : g^m) \cap ((I + (g^m)) = I.$$

Let $a + bg^m$ with $a \in I$ and $b \in R$ be an arbitrary element of the intersection. So $(a + bg^m)g^m \in I$ and hence $bg^{2m} \in I$. Writing $bg^{2m} = bg^{m-1}g^{m+1}$ the assumption gives $bg^{2m-1} \in I$. By the same argument

$$bg^k g^{m+1} \in I \Rightarrow bg^k g^m \in I$$

holds for every $k \geq 0$. So finally we obtain $bg^m \in I$ and hence $a + bg^m \in I$. This proves

$$I \subset (I : g^m) \cap ((I + (g^m)).$$

Since the other inclusion holds trivially we arrive at the claim. Now we use the irreducibility of I. Since $f \in I : g^m$ but $f \notin I$ we conclude

$$I + (g^m) = I, \text{ i.e., } g^m \in I.$$

Minimal primary decompositions

Lemma. *If $\mathfrak{q}_1$ and $\mathfrak{q}_2$ are $\mathfrak{p}$-primary, then $\mathfrak{q}_1 \cap \mathfrak{q}_2$ is $\mathfrak{p}$-primary as well.*

Proof. If $fg \in \mathfrak{q}_1 \cap \mathfrak{q}_2$ and $g \notin \mathfrak{p}$, we have to show $f \in \mathfrak{q}_1 \cap \mathfrak{q}_2$. This clear because $f \in \mathfrak{q}_j$ for all $j = 1, 2$ by the defining condition of primary ideals. □

A primary decomposition $I = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r$ is called **minmal** if

1. $\mathfrak{q}_j \not\supset \bigcap_{i \neq j} \mathfrak{q}_i$ for any j,
2. The prime ideals $\mathfrak{p}_j = \mathrm{rad}(\mathfrak{q}_j)$ are pairwise distinct.

By dropping superfluous terms and by collecting primary ideals with same radical into a single primary ideal one can always pass from an arbitrary primary decomposition to a minimal one.

Uniqueness of irredundant primary decompositions

Example. The ideal (x^2, xy) has many different minimal primary decomposions:

$$(x^2, xy) = (x) \cap (x^2, y) = (x) \cap (x^2, xy, y^n)$$

are different primary decompositions with associated primes (x) and (x, y). Thus minimal primary decompositions are not necessarily unique.

Theorem (First Uniqueness Theorem). The associated primes $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ of a minimal primary decomposition of

$$I = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r$$

are uniquely determined by I.

Definition. The minimal elements in the set of associated primes $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ are called **isolated primes** or **minimal primes** of I. The non-isolated primes are called **embedded primes**. The last notation is motivated by geometry: $\mathfrak{p}_i \subset \mathfrak{p}_j$ implies that $V(\mathfrak{p}_j)$ is embedded into $V(\mathfrak{p}_i)$ in case of $R = K[x_1, \ldots, x_n]$.

2^{nd} Uniqueness of theorem

Theorem. *The primary ideal $\mathfrak{q}_i$ corresponding to the isolated primes $\mathfrak{p}_i$ of a minimal primary decomposition*

$$I = \mathfrak{q}_1 \cap \mathfrak{q}_2 \cap \ldots \cap \mathfrak{q}_r$$

are uniquely determined by I.

Corollary. *Proper ideals I in a noetherian ring which have no embedded primes have a unique primary decomposition.*

Example. In our example above

$$(x^2, xy) = (x) \cap (x^2, y) = (x) \cap (x^2, xy, y^n),$$

$\mathfrak{p}_1 = (x)$ is an isolated prime and $\mathfrak{p}_2 = (x, y)$ an embedded prime. The primary ideal $\mathfrak{q}_1 = (x)$ is the same for each minimal decomposition.