Computational Algebraic Geometry

The Algebra-Geometry Dictionary

Kaie Kubjas

kaie.kubjas@aalto.fi

February 3, 2021

- We explore the correspondence between ideals and varieties.
- The Nullstellensatz characterizes which ideals correspond to varieties.
- This allows to build the algebra and geometry dictionary, where every statement about varieties translates into a statement about ideals (and vice versa).

The Algebra-Geometry Dictionary

- We explore the correspondence between ideals and varieties.
- The Nullstellensatz characterizes which ideals correspond to varieties.
- This allows to build the algebra and geometry dictionary, where every statement about varieties translates into a statement about ideals (and vice versa).

Topics:

1. Hilbert's Nullstellensatz
2. Radical ideals and the ideal-variety correspondence
3. Sums, products and intersections of ideals
4. Zariski closure and quotients of ideals
5. Irreducible varieties and prime ideals
6. Decomposition of a variety into irreducibles

Hilbert's Nullstellensatz

Correspondence between ideals and varieties

$$\begin{array}{ccc} \text{Varieties} & & \text{Ideals} \\ V & \longrightarrow & I(V) \end{array}$$

- a variety $V \subseteq k^n$ can be studied by passing to the ideal

$$\mathbb{I}(V) = \{f \in k[x_1, \ldots, x_n] : f(x) = 0 \text{ for all } x \in V\}$$

- hence we have a map from affine varieties to ideals

Correspondence between ideals and varieties

$$\begin{array}{ccc} \text{Ideals} & & \text{Varieties} \\ \text{I} & \longrightarrow & \text{V(I)} \end{array}$$

- conversely, an ideal $I \subseteq k[x_1, \ldots, x_n]$ defines the set

$$\mathbb{V}(I) = \{x \in k^n : f(x) = 0 \text{ for all } f \in I\}$$

- the Hilbert Basis Theorem assures that $\mathbb{V}(I)$ is an affine variety, i.e. there exist finitely many polynomials $f_1, \ldots, f_s \in I$ such that $I = \langle f_1, \ldots, f_s \rangle$
- $\mathbb{V}(f_1, \ldots, f_n) = \mathbb{V}(I)$
- hence we also have a map from ideals to affine varieties

Correspondence between ideals and varieties

- the correspondence is not one-to-one
- $\langle x \rangle, \langle x^2 \rangle \in k[x]$ give the same variety $\mathbb{V}(x) = \mathbb{V}(x^2) = \{0\}$

Correspondence between ideals and varieties

- the correspondence is not one-to-one
- $\langle x \rangle, \langle x^2 \rangle \in k[x]$ give the same variety $\mathbb{V}(x) = \mathbb{V}(x^2) = \{0\}$
- more serious problems when k is not algebraically closed: the varieties corresponding to

$$I_1 = \langle 1 \rangle = \mathbb{R}[x], I_2 = \langle 1 + x^2 \rangle, I_3 = \langle 1 + x^2 + x^4 \rangle,$$

  are all empty in $\mathbb{R}$

Correspondence between ideals and varieties

- the correspondence is not one-to-one
- $\langle x \rangle, \langle x^2 \rangle \in k[x]$ give the same variety $\mathbb{V}(x) = \mathbb{V}(x^2) = \{0\}$
- more serious problems when k is not algebraically closed: the varieties corresponding to

$$I_1 = \langle 1 \rangle = \mathbb{R}[x], I_2 = \langle 1 + x^2 \rangle, I_3 = \langle 1 + x^2 + x^4 \rangle,$$

  are all empty in $\mathbb{R}$
- does this problem of having different ideals represent the empty variety go away if the field k is algebraically closed?

The Weak Nullstellensatz

One variable and k is algebraically closed: $k[x]$ is the only ideal representing the empty variety:

- Every ideal I in $k[x]$ has the form $\langle f \rangle$
- $\mathbb{V}(I)$ is the set of roots of f
- Every nonconstant polynomial $f \in k[x]$ has a root
- If f is a nonzero constant, then $\langle f \rangle = k[x]$

One variable and k is algebraically closed: $k[x]$ is the only ideal representing the empty variety:

- Every ideal I in $k[x]$ has the form $\langle f \rangle$
- $\mathbb{V}(I)$ is the set of roots of f
- Every nonconstant polynomial $f \in k[x]$ has a root
- If f is a nonzero constant, then $\langle f \rangle = k[x]$

This observation generalizes to more variables:

Theorem (The Weak Nullstellensatz)

Let k be an algebraically closed field and let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal satisfying $\mathbb{V}(I) = \emptyset$. Then $I = k[x_1, \ldots, x_n]$.

"Fundamental Theorem of Algebra for multivariate polynomials"

Proof: Let I be s.t. $\mathbb{V}(I)=\emptyset$. We need to show that $1\in I$.

We will use induction on the number of variables.
Base case: (see above)
Induction step: Assume that the result is true for $n-1$ variables. Let $I=\langle f_1,\dots,f_s\rangle\subseteq k[x_1,\dots,x_n]$. Let $N:=\deg(f_1)\geq 1$ (if $N=0$, then f_1 is a constant and we are done).

Consider the linear change of variables:

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

where a_i are to be determined constants in k.

Then

$$f(x_1,\dots,x_n)=f_1(\tilde{x}_1,\tilde{x}_2+a_2\tilde{x}_1,\dots,\tilde{x}_n+a_n\tilde{x}_1)=$$
$$=c(a_2,\dots,a_n)\tilde{x}_1^N+\text{terms in which } \tilde{x}_1 \text{ has degree} < N.$$

- $c(a_2, \dots, a_n)$ is a nonzero polynomial
- an alg. closed field is infinite
- We can choose $a_2, \dots, a_n$ s.t. $c(a_2, \dots, a_n) \neq 0$

With this change of variables, every $f \in k[x_1, \dots, x_n]$ goes to a polynomial $\tilde{f} \in k[\tilde{x}_1, \dots, \tilde{x}_n]$.

- $\tilde{I} = \{\tilde{f} : f \in I\}$ is an ideal
- $\mathbb{V}(\tilde{I}) = \emptyset$
- if $1 \in \tilde{I}$, then $1 \in I$ (constants are unaffected)

We will show that $1 \in \tilde{I}$ using the Extension Theorem. Let $\tilde{I}_1 = \tilde{I} \cap k[\tilde{x}_2, \dots, \tilde{x}_n]$, then partial solutions in k^{n-1} always extend, i.e. $\mathbb{V}(\tilde{I}_1) = \pi_1(\mathbb{V}(\tilde{I}))$, because $g_1 = c(a_2, \dots, a_n)$ is a nonzero constant.

Hence $\mathbb{V}(\tilde{I}_1) = \pi_1(\mathbb{V}(\tilde{I})) = \pi_1(\emptyset) = \emptyset$.
By the induction hypothesis, $\tilde{I}_1 = k[\tilde{x}_2, \dots, \tilde{x}_n]$.
Hence $1 \in \tilde{I}_1 \subset \tilde{I}$ and $1 \in I$, which completes the proof. ∎

Consistency problem

The Weak Nullstellensatz allows us to solve the consistency problem: Does a system

$$\begin{aligned} f_1 &= 0, \\ f_2 &= 0, \\ &\vdots \\ f_s &= 0 \end{aligned}$$

of polynomial equations has a common solution in $\mathbb{C}^n$?

Consistency problem

The Weak Nullstellensatz allows us to solve the consistency problem: Does a system

$$\begin{aligned} f_1 &= 0, \\ f_2 &= 0, \\ &\vdots \\ f_s &= 0 \end{aligned}$$

of polynomial equations has a common solution in $\mathbb{C}^n$?

- fail to have a common solution if and only if $\mathbb{V}(f_1, \ldots, f_s) = \emptyset$

Consistency problem

The Weak Nullstellensatz allows us to solve the consistency problem: Does a system

$$\begin{aligned} f_1 &= 0, \\ f_2 &= 0, \\ &\vdots \\ f_s &= 0 \end{aligned}$$

of polynomial equations has a common solution in $\mathbb{C}^n$?

- fail to have a common solution if and only if $\mathbb{V}(f_1, \ldots, f_s) = \emptyset$
- the latter holds if and only if $1 \in \langle f_1, \ldots, f_s \rangle$

Consistency problem

The Weak Nullstellensatz allows us to solve the consistency problem: Does a system

$$
\begin{aligned}
f_1 &= 0, \\
f_2 &= 0, \\
&\vdots \\
f_s &= 0
\end{aligned}
$$

of polynomial equations has a common solution in $\mathbb{C}^n$?

- fail to have a common solution if and only if $\mathbb{V}(f_1, \ldots, f_s) = \emptyset$
- the latter holds if and only if $1 \in \langle f_1, \ldots, f_s \rangle$
- $\{1\}$ is the only reduced Groebner basis for the ideal $\langle 1 \rangle$

Hilbert's Nullstellensatz

In general, there is no one-to-one correspondence between ideals and varieties: $\mathbb{V}(x^2) = \mathbb{V}(x) = \{0\}$ works over any field

Theorem (Hilbert's Nullstellensatz)

Let k be an algebraically closed field. If $f, f_1, \ldots, f_s \in k[x_1, \ldots, x_n]$ are such that $f \in \mathbb{I}(\mathbb{V}(f_1, \ldots, f_s))$, then there exists an integer $m \geq 1$ such that

$$f^m \in \langle f_1, \ldots, f_s \rangle$$

(and conversely).

Proof: Given f that vanishes at every common zero of $f_1, \dots, f_s$, we want to show that there exists $m \geq 1$ s.t.

$$f^m = \sum_{i=1}^{s} A_i f_i, \quad \text{where } A_i \in k[x_1, \dots, x_n].$$

Consider $\tilde{I} = \langle f_1, \dots, f_s, 1 - yf \rangle \subseteq k[x_1, \dots, x_n, y]$.

CLAIM: $\mathbb{V}(\tilde{I}) = \emptyset$.

Proof: Let $(a_1, \dots, a_{n+1}) \in k^{n+1}$. Either
1) $(a_1, \dots, a_n) \in \mathbb{V}(f_1, \dots, f_s)$ or
2) $(a_1, \dots, a_n) \notin \mathbb{V}(f_1, \dots, f_s)$.

- In the first case $1 - y \cdot \underbrace{f(a_1, \dots, a_n)}_{0} = 1$, hence $(a_1, \dots, a_{n+1}) \notin \mathbb{V}(\tilde{I})$.

- In the second case, there is some f_i s.t. $f_i(a_1, \dots, a_n) \neq 0$, hence $(a_1, \dots, a_{n+1}) \notin \mathbb{V}(\tilde{I})$. ∎

By the Weak Nullstellensatz:

$$1 = \sum_{i=1}^{s} p_i(x_1,\dots,x_n,y)\cdot f_i + q(x_1,\dots,x_n,y)\cdot(1-yf)$$

for $p_i, q \in k[x_1,\dots,x_n,y]$.

Set $y = \dfrac{1}{f(x_1,\dots,x_n)}$. Then

$$1 = \sum_{i=1}^{s} p_i\left(x_1,\dots,x_n,\frac{1}{f}\right)\cdot f_i.$$

Multiply both sides of this equation by a large enough power of f. This gives

$$f^m = \sum_{i=1}^{s} A_i\cdot f_i, \qquad A_i \in k[x_1,\dots,x_n].$$

$\blacksquare$

Radical ideals and the ideal-variety correspondence

Radical ideals

Lemma

Let V be a variety. If $f^m \in \mathbb{I}(V)$, then $f \in \mathbb{I}(V)$.

Proof: Let f be s.t. $f^m \in I(V)$. Let $a \in V$. Then $(f(a))^m = 0$. This implies that $f(a) = 0$. ∎

Radical ideals

Lemma

Let V be a variety. If $f^m \in \mathbb{I}(V)$, then $f \in \mathbb{I}(V)$.

Definition

An ideal I is radical if $f^m \in I$ for some integer $m \geq 1$ implies that $f \in I$.

Radical ideals

Lemma

Let V be a variety. If $f^m \in \mathbb{I}(V)$, then $f \in \mathbb{I}(V)$.

Definition

An ideal I is radical if $f^m \in I$ for some integer $m \geq 1$ implies that $f \in I$.

Corollary

$\mathbb{I}(V)$ is a radical ideal.

Radical ideals

Lemma

Let V be a variety. If $f^m \in \mathbb{I}(V)$, then $f \in \mathbb{I}(V)$.

Definition

An ideal I is radical if $f^m \in I$ for some integer $m \geq 1$ implies that $f \in I$.

Corollary

$\mathbb{I}(V)$ is a radical ideal.

Definition

Let $I \subseteq k[x_1, \ldots, x_n]$ be an ideal. The radical of I, denoted $\sqrt{I}$, is the

$$\{f : f^m \in I \text{ for some integer } m \geq 1\}$$

Radical ideals

Example

Let $J = \langle x^2, y^3 \rangle \subseteq k[x, y]$. Then $x, y \in \sqrt{J}$. Show that $xy, x + y \in \sqrt{J}$.

Radical ideals

Example

Let $J = \langle x^2, y^3 \rangle \subseteq k[x, y]$. Then $x, y \in \sqrt{J}$. Show that $xy, x + y \in \sqrt{J}$.

Lemma

If I is an ideal in $k[x_1, \ldots, x_n]$, then $\sqrt{I}$ is an ideal in $k[x_1, \ldots, x_n]$ containing I. Furthermore, $\sqrt{I}$ is a radical ideal.

Proof: 1) We have $I \subseteq \sqrt{I}$, because $f \in I$ is the same as $f^1 \in I$, and hence $f \in \sqrt{I}$.

2) $\sqrt{I}$ is an ideal:

* Let $f, g \in \sqrt{I}$. This means that $\exists\, m, l \geq 1$ such that $f^m, g^l \in I$. In the expansion of $(f+g)^{m+l-1}$, every term is of the form $\binom{m+l-1}{i} f^i g^{m+l-1-i}$. Either $i \geq m$ or $j \geq l$ and hence every such term is in I. Hence $(f+g)^{m+l-1} \in I$ and $f+g \in \sqrt{I}$.

* Let $f \in \sqrt{I}$ and $h \in k[x_1, \ldots, x_n]$. Then $f^m \in I$ for some $m \geq 1$. Hence $h^m \cdot f^m \in I$ and $h \cdot f \in I$.

3) $\sqrt{I}$ is a radical ideal: Assume $f^m \in \sqrt{I}$ for some $m \geq 1$. By the definition of $\sqrt{I}$, $\exists\, l \geq 1$ s.t. $(f^m)^l \in I$. Using the definition again, since $f^{m \cdot l} \in I$, then $f \in \sqrt{I}$. Hence $\sqrt{I}$ is a radical ideal. $\boxtimes$

Radical ideals

Example

Let $J = \langle x^2, y^3 \rangle \subseteq k[x, y]$. Then $x, y \in \sqrt{J}$. Show that $xy, x + y \in \sqrt{J}$.

Lemma

If I is an ideal in $k[x_1, \ldots, x_n]$, then $\sqrt{I}$ is an ideal in $k[x_1, \ldots, x_n]$ containing I. Furthermore, $\sqrt{I}$ is a radical ideal.

Theorem (The Strong Nullstellensatz)

Let k be an algebraically closed field. If I is an ideal in $k[x_1, \ldots, x_n]$, then

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

The Nullstellensatz refers to the Strong Nullstellensatz.

Proof: "$\subseteq$" Let $f \in \mathbb{I}(\mathbb{V}(I))$. Then by the Hilbert's Nullstellensatz, $\exists m \geq 1$ s.t. $f^m \in I$. Hence $\mathbb{I}(\mathbb{V}(I)) \subseteq I \subseteq \sqrt{I}$.

"$\supseteq$" Let $f \in \sqrt{I}$. Then $f^m \in I$ for some $m \geq 1$. Hence f^m vanishes on $\mathbb{V}(I)$ and hence f vanishes on $\mathbb{V}(I)$. Hence $f \in \mathbb{I}(\mathbb{V}(I))$. ∎

The Ideal-Variety Correspondence

Theorem

Let k be an arbitrary field.

1. *The maps*

   $$\text{affine varieties} \longrightarrow \text{ideals}$$

   and

   $$\text{ideals} \longrightarrow \text{affine varieties}$$

   are inclusion-reversing. Furthermore, for any variety V, we have

   $$\mathbb{V}(\mathbb{I}(V)) = V,$$

   so that I is always one-to-one.

Theorem

Let k be an arbitrary field.

1. *The maps*
$$\text{affine varieties} \longrightarrow \text{ideals}$$
and
$$\text{ideals} \longrightarrow \text{affine varieties}$$
are inclusion-reversing. Furthermore, for any variety V, we have
$$\mathbb{V}(\mathbb{I}(V)) = V,$$
so that I is always one-to-one.
2. *If k is algebraically closed, and if we restrict to radical ideals, then the maps*
$$\text{affine varieties} \longrightarrow \text{radical ideals}$$
and
$$\text{radical ideals} \longrightarrow \text{affine varieties}$$
are inclusion-reversing bijections which are inverses of each-other.

Proof: 1) Inclusion-reversing: EXERCISE

* $\mathbb{V}(\mathbb{I}(V)) = V$. Let $V = \mathbb{V}(f_1, \dots, f_s)$. Let $a \in V$. Then $f(a) = 0$ for all $f \in \mathbb{I}(V)$. Hence $V \subseteq \mathbb{V}(\mathbb{I}(V))$.

Conversely, $\mathbb{I}(V) \supseteq \langle f_1, \dots, f_s \rangle$. Using inclusion reversion, we get $\mathbb{V}(\mathbb{I}(V)) \subseteq \underbrace{\mathbb{V}(f_1, \dots, f_s)}_{= V}$.

2) $\mathbb{I}(\mathbb{V}(I)) = I$. By Nullstellensatz $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$. Since I is radical, then $\sqrt{I} = I$. ☒

Radical Ideals

The Nullstellensatz motivates the study of radical ideals:

1. (Radical generators) Given an ideal I, is there an algorithm that computes a basis $\{g_1, \ldots, g_m\}$ of $\sqrt{I}$? [We will answer it for principal ideals.]
2. (Radical ideal) Is there an algorithm for checking whether I is radical? [Out of scope of this course.]
3. (Radical membership) Given $f \in k[x_1, \ldots, x_n]$, is there an algorithm to determine whether $f \in \sqrt{I}$? [We will answer it completely using the Hilbert's Nullstellensatz.]

Radical Membership

Proposition

Let k be an arbitrary field and let $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$ be an ideal. Then $f \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal $\tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq k[x_1, \ldots, x_n, y]$.

Proof: As in the proof of the Hilbert's Nullstellensatz, $1 \in \tilde{I}$ implies that $f^m \in I$ for some $m \geq 1$.

Conversely, assume that $f \in \sqrt{I}$. Then $f^m \in I \subset \tilde{I}$ for some $m \geq 1$. But also $1 - yf \in \tilde{I}$. Thus

$$1 = y^m f^m + (1 - y^m f^m) =$$
$$= y^m f^m + (1 - yf) \cdot (1 + yf + \dots + y^{m-1} f^{m-1}) \in \tilde{I}.$$

$\blacksquare$

Radical Membership

Proposition

Let k be an arbitrary field and let $I = \langle f_1, \ldots, f_s \rangle \subseteq k[x_1, \ldots, x_n]$ be an ideal. Then $f \in \sqrt{I}$ if and only if the constant polynomial 1 belongs to the ideal $\tilde{I} = \langle f_1, \ldots, f_s, 1 - yf \rangle \subseteq k[x_1, \ldots, x_n, y]$.

Example (Radical Membership Algorithm)

Consider $I = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1 \rangle \subseteq k[x, y]$. We want to test if $f = y - x^2 + 1$ lies in $\sqrt{I}$. Using lex order on $k[x, y, z]$, one checks that the ideal

$$\tilde{I} = \langle xy^2 + 2y^2, x^4 - 2x^2 + 1, 1 - z(y - x^2 + 1) \rangle \subseteq k[x, y, z]$$

has reduced Groebner basis $\{1\}$. It follows that $y - x^2 + 1 \in \sqrt{I}$.

Irreducible polynomials

Definition

Let k be a field. A polynomial $f \in k[x_1, \ldots, x_n]$ is irreducible over k if and only if it is nonconstant and it is not the product of two nonconstant polynomials in $k[x_1, \ldots, x_n]$.

Irreducible polynomials

Definition

Let k be a field. A polynomial $f \in k[x_1, \ldots, x_n]$ is irreducible over k if and only if it is nonconstant and it is not the product of two nonconstant polynomials in $k[x_1, \ldots, x_n]$.

Quiz: Is $x^2 + 1$ irreducible over $\mathbb{R}$? Over $\mathbb{C}$?

Irreducible polynomials

Definition

Let k be a field. A polynomial $f \in k[x_1, \ldots, x_n]$ is irreducible over k if and only if it is nonconstant and it is not the product of two nonconstant polynomials in $k[x_1, \ldots, x_n]$.

Quiz: Is $x^2 + 1$ irreducible over $\mathbb{R}$? Over $\mathbb{C}$?
Answer: It is irreducible over $\mathbb{R}$ but it factors as $(x - i)(x + i)$ over $\mathbb{C}$.

Irreducible polynomials

Definition

Let k be a field. A polynomial $f \in k[x_1, \dots, x_n]$ is irreducible over k if and only if it is nonconstant and it is not the product of two nonconstant polynomials in $k[x_1, \dots, x_n]$.

Quiz: Is $x^2 + 1$ irreducible over $\mathbb{R}$? Over $\mathbb{C}$?
Answer: It is irreducible over $\mathbb{R}$ but it factors as $(x - i)(x + i)$ over $\mathbb{C}$.

Proposition

Every nonconstant polynomial $f \in k[x_1, \dots, x_n]$ can be written as a product of polynomials which are irreducible over k.

Unique factorization

Theorem

Every nonconstant polynomial $f \in k[x_1, \ldots, x_n]$ can be written as a product $f = f_1 \cdot f_2 \cdots f_r$ of irreducible polynomials over l. Further, if $f = g_1 \cdot g_2 \cdots g_s$ is another factorization into irreducible polynomials over l, then $r = s$ and the g_i's can be permuted so that each f_i is a constant multiple of g_i.

Principal ideals

Proposition

Let $f \in k[x_1, \ldots, x_n]$ and $I = \langle f \rangle$ be the principal ideal generated by f. If $f = cf_1^{a_1} \cdots f_r^{a_r}$ is the factorization of f into a product of distinct irreducible polynomials, then

$$\sqrt{I} = \langle f_1 f_2 \cdots f_r \rangle.$$

Principal ideals

Proposition

Let $f \in k[x_1, \ldots, x_n]$ and $I = \langle f \rangle$ be the principal ideal generated by f. If $f = cf_1^{a_1} \cdots f_r^{a_r}$ is the factorization of f into a product of distinct irreducible polynomials, then

$$\sqrt{I} = \langle f_1 f_2 \cdots f_r \rangle.$$

Definition

If $f \in k[x_1, \ldots, x_n]$ is a polynomial, we define reduction of f, denoted f_{red}, to be the polynomial such that $\langle f_{red} \rangle = \sqrt{\langle f \rangle}$. A polynomial is said to be reduced (or square-free) if $f = f_{red}$.

Principal ideals

Proposition

Let $f \in k[x_1, \dots, x_n]$ and $I = \langle f \rangle$ be the principal ideal generated by f. If $f = cf_1^{a_1} \cdots f_r^{a_r}$ is the factorization of f into a product of distinct irreducible polynomials, then

$$\sqrt{I} = \langle f_1 f_2 \cdots f_r \rangle.$$

Definition

If $f \in k[x_1, \dots, x_n]$ is a polynomial, we define reduction of f, denoted f_{red}, to be the polynomial such that $\langle f_{red} \rangle = \sqrt{\langle f \rangle}$. A polynomial is said to be reduced (or square-free) if $f = f_{red}$.

Example

What is the reduction of $f = (x + y^2)^3(x - y)$?

Definition

Let $f, g \in k[x_1, \ldots, x_n]$. Then $h \in k[x_1, \ldots, x_n]$ is called a greatest common divisor of f and g, and denoted $h = \mathrm{GCD}(f, g)$, if

1. h divides f and g.
2. If p is any polynomial which divides both f and g, then p divides h.

Definition

Let $f, g \in k[x_1, \ldots, x_n]$. Then $h \in k[x_1, \ldots, x_n]$ is called a greatest common divisor of f and g, and denoted $h = \mathrm{GCD}(f, g)$, if

1. h divides f and g.
2. If p is any polynomial which divides both f and g, then p divides h.

- GCD exists and is unique up to multiplication by a nonzero constant k
- the Euclidean algorithm does not work in the case of several variables: $\mathrm{GCD}(xy, xz) = x$, but remainder is either xy or xz depending in which order we divide the monomials
- we will talk about an algorithm for computing GCD in the next lectures

Reduction

Proposition

Suppose that k is a field containing the rational numbers $\mathbb{Q}$ and let $I = \langle f \rangle$ be a principal ideal in $k[x_1, \ldots, x_n]$. Then $\sqrt{I} = \langle f_{red} \rangle$, where

$$f_{red} = \frac{f}{GCD(f, \frac{\partial f}{\partial x_1}, \cdots, \frac{\partial f}{\partial x_n})}.$$

Conclusion

Today:

- Hilbert's Nullstellensatz
- Radical ideals
- Ideal-variety correspondence

Next time:

- Sums, products and intersections of ideals
- Zariski closure and quotients of ideals