Solving Polynomial Equations and Primary Decomposition

Gerhard Pfister

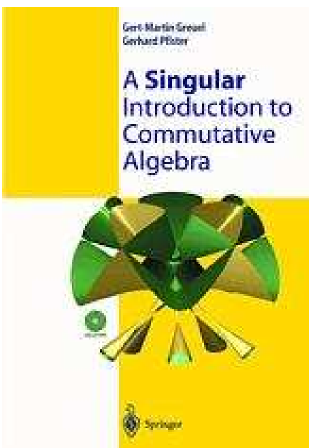
pfister@mathematik.uni-kl.de

Departement of Mathematics

University of Kaiserslautern

References

- Greuel, G.-M.; Pfister, G.:
  A SINGULAR Introduction to Commutative Algebra,
  Springer 2002, second edition 2007



References

- Gianni, P.; Trager, B.; Zacharias, G.: Gröbner Bases and Primary Decomposition of Polynomial Ideals. J. Symb. Comp. 6, 149–167 (1988).
- Eisenbud, D.; Huneke, C.; Vasconcelos, W.: Direct Methods for Primary Decomposition. Invent. Math. 110, 207–235 (1992).
- Shimoyama, T.; Yokoyama, K.: Localization and Primary Decomposition of Polynomial ideals. J. Symb. Comp. 22, 247–277 (1996).

References

- Gianni, P.; Trager, B.; Zacharias, G.: Gröbner Bases and Primary Decomposition of Polynomial Ideals. J. Symb. Comp. 6, 149–167 (1988).
- Eisenbud, D.; Huneke, C.; Vasconcelos, W.: Direct Methods for Primary Decomposition. Invent. Math. 110, 207–235 (1992).
- Shimoyama, T.; Yokoyama, K.: Localization and Primary Decomposition of Polynomial ideals. J. Symb. Comp. 22, 247–277 (1996).
- Decker, W.; Greuel, G.-M.; Pfister, G.: Primary Decomposition: Algorithms and Comparisons. In: Algorithmic Algebra and Number Theory, Springer, 187–220 (1998).

SINGULAR

SINGULAR

A Computer Algebra System for Polynomial Computations

with special emphasize on the needs of algebraic geometry, commutative algebra, and singularity theory

SINGULAR

SINGULAR

A Computer Algebra System for Polynomial Computations

with special emphasize on the needs of algebraic geometry, commutative algebra, and singularity theory

G.-M. Greuel, G. Pfister, H. Schönemann

Technische Universität Kaiserslautern

Fachbereich Mathematik; Zentrum für Computer Algebra

D-67663 Kaiserslautern

SINGULAR

A Computer Algebra System for Polynomial Computations

with special emphasize on the needs of algebraic geometry, commutative algebra, and singularity theory

G.-M. Greuel, G. Pfister, H. Schönemann

Technische Universität Kaiserslautern

Fachbereich Mathematik; Zentrum für Computer Algebra

D-67663 Kaiserslautern

The computer is not the philosopher's stone but the philosopher's whetstone

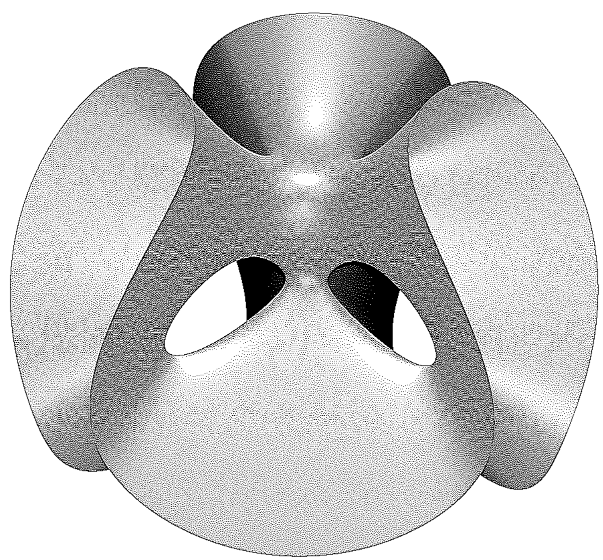
Hugo Battus, Rekenen op taal 1983

Motivation

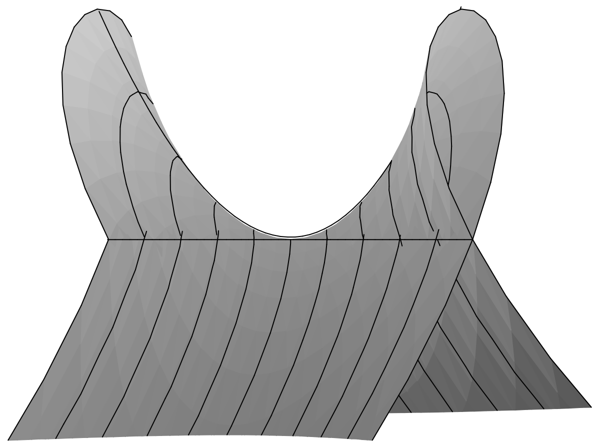
The basic problem of algebraic geometry is to understand the set of solutions $x = (x_1, \ldots, x_n) \in K^n$ of a system of polynomial equations

$$f_1(x_1, \ldots, x_n) = 0\,, \;\ldots\;, \; f_k(x_1, \ldots, x_n) = 0\,,$$

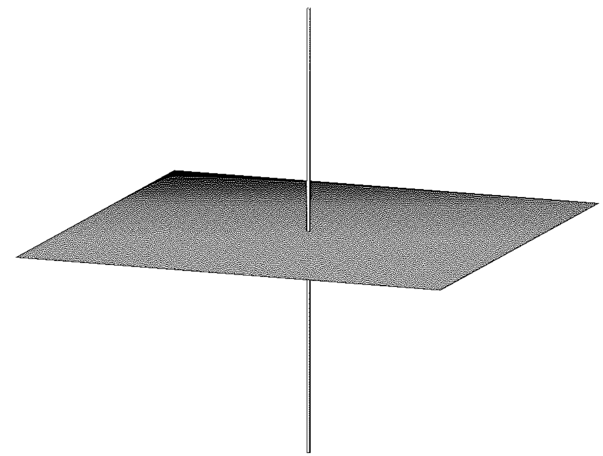
$f_i \in K[x] = K[x_1, \ldots, x_n]$ and K a field. The solution set is called an algebraic set or algebraic variety.



Motivation

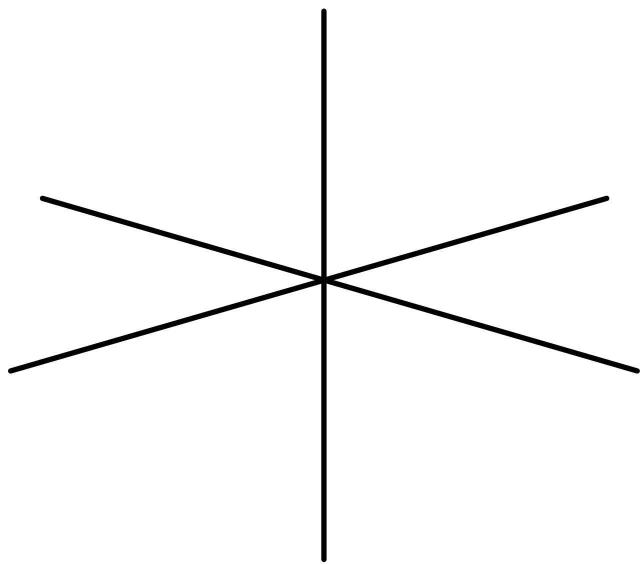


(A) The Hypersurface $V(x^2 + y^3 - z^2 y^2)$.

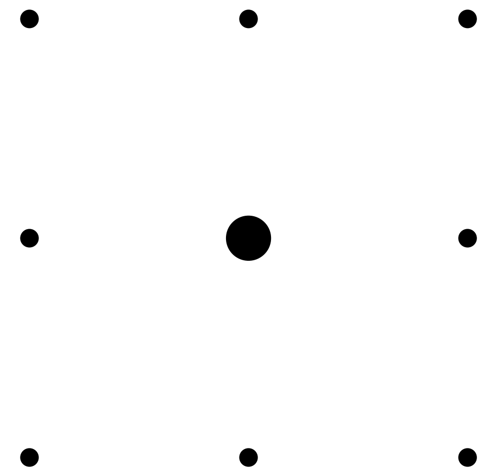


(B) The Variety $V(xz, yz)$.

Motivation



(C) The Space Curve $V(xy, xz, yz)$.



(D) The Set of Points $V(y^4 - y^2, xy^3 - xy, x^3y - xy, x^4 - x^2)$.

surfaces: http://www.imaginary2008.de/

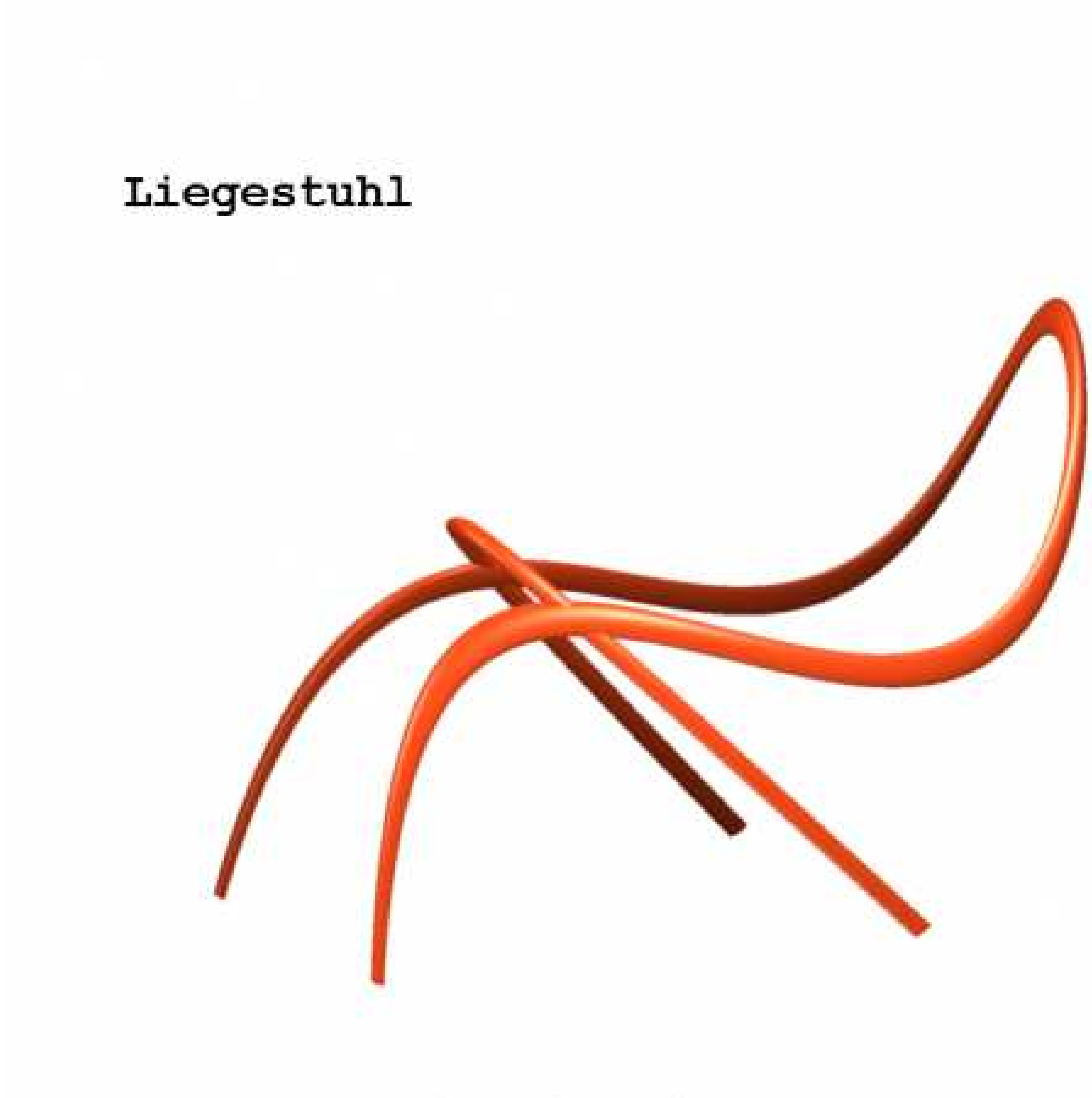
TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

- Consider the equation

$$((y-z)^2+(y-1-\tfrac{1}{2}x-\tfrac{1}{8}x^2+\tfrac{1}{16}x^3)^2-\tfrac{1}{50})((x-\tfrac{3}{5}y+1)^2+(y-z^2)^2-\tfrac{1}{100})=0$$

- defining a surface of degree 10 in $\mathbb{R}^3$.
- What do you expect from the real picture?

Nice algebraic surfaces



Motivation

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

- A set $X \subset \mathbb{A}^n_K$ is called an *affine algebraic variety* (over K) if there exist polynomials $f_\lambda \in K[x_1, \ldots, x_n]$, λ in some index set Λ, such that

$$X = V\big((f_\lambda)_{\lambda \in \Lambda}\big) = \{x \in \mathbb{A}^n_K \mid f_\lambda(x) = 0, \ \ \forall\, \lambda \in \Lambda\}\,.$$

Motivation

- A set $X \subset \mathbb{A}^n_K$ is called an *affine algebraic variety* (over K) if there exist polynomials $f_\lambda \in K[x_1, \ldots, x_n]$, λ in some index set Λ, such that

$$X = V\big((f_\lambda)_{\lambda \in \Lambda}\big) = \{x \in \mathbb{A}^n_K \mid f_\lambda(x) = 0, \;\; \forall\, \lambda \in \Lambda\}\,.$$

- Of course, X depends only on the ideal I generated by the f_λ, that is, $X = V(I)$ with $I = \langle f_\lambda \mid \lambda \in \Lambda \rangle_{K[x]}$.

Motivation

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

- A set $X \subset \mathbb{A}^n_K$ is called an *affine algebraic variety* (over K) if there exist polynomials $f_\lambda \in K[x_1, \ldots, x_n]$, λ in some index set Λ, such that

$$X = V\big((f_\lambda)_{\lambda\in\Lambda}\big) = \{x \in \mathbb{A}^n_K \mid f_\lambda(x) = 0, \ \ \forall\, \lambda \in \Lambda\}\,.$$

- Of course, X depends only on the ideal I generated by the f_λ, that is, $X = V(I)$ with $I = \langle f_\lambda \mid \lambda \in \Lambda\rangle_{K[x]}$.
- For any set $X \subset \mathbb{A}^n$ define

$$I(X) := \big\{ f \in K[x_1, \ldots, x_n] \,\big|\, f|_X = 0 \,\big\}\,,$$

the *(full vanishing) ideal of* X, where $f|_X : X \to K$ denotes the polynomial function of f restricted to X.

Motivation

Let $X \subset \mathbb{A}^n$ be a subset, $X_1, X_2 \subset \mathbb{A}^n$ affine varieties.

1. $I(X)$ is a radical ideal.
2. $V\big(I(X)\big) = \overline{X}$ the Zariski closure of X in $\mathbb{A}^n$.
3. If X is an affine variety, then $V\big(I(X)\big) = X$.
4. $I(\overline{X}) = I(X)$.

Motivation

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Let $X \subset \mathbb{A}^n$ be a subset, $X_1, X_2 \subset \mathbb{A}^n$ affine varieties.

1. $I(X)$ is a radical ideal.
2. $V\big(I(X)\big) = \overline{X}$ the Zariski closure of X in $\mathbb{A}^n$.
3. If X is an affine variety, then $V\big(I(X)\big) = X$.
4. $I(\overline{X}) = I(X)$.
5. $X_1 \subset X_2$ if and only if $I(X_2) \subset I(X_1)$,
   $X_1 = X_2$ if and only if $I(X_1) = I(X_2)$.
6. $I(X_1 \cup X_2) = I(X_1) \cap I(X_2)$.
7. $I(X_1 \cap X_2) = \sqrt{I(X_1) + I(X_2)}$.

Motivation

Let $X \subset \mathbb{A}^n$ be a subset, $X_1, X_2 \subset \mathbb{A}^n$ affine varieties.

1. $I(X)$ is a radical ideal.
2. $V\big(I(X)\big) = \overline{X}$ the Zariski closure of X in $\mathbb{A}^n$.
3. If X is an affine variety, then $V\big(I(X)\big) = X$.
4. $I(\overline{X}) = I(X)$.
5. $X_1 \subset X_2$ if and only if $I(X_2) \subset I(X_1)$,
   $X_1 = X_2$ if and only if $I(X_1) = I(X_2)$.
6. $I(X_1 \cup X_2) = I(X_1) \cap I(X_2)$.
7. $I(X_1 \cap X_2) = \sqrt{I(X_1) + I(X_2)}$.

Hilbert's Nullstellensatz: If $I \subset K[x_1, \ldots, x_n]$ is an ideal, K is algebraically closed, and $X = V(I)$, then

$$I(X) = \sqrt{I}\,.$$

Motivation

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

We obtain, for K algebraically closed, an inclusion reversing bijection (HN refers to Hilbert's Nullstellensatz)

$$\{\text{affine algebraic sets in } \mathbb{A}^n_K\} \overset{HN}{\longleftrightarrow} \{\text{radical ideals } I \subset K[x_1, \ldots, x_n]\}$$

$$X \longmapsto I(X)$$

$$V(I) \longleftarrow\!\shortmid \; I\,.$$

Motivation

For K an algebraically closed field, we have the following inclusion reversing bijections (with $K[x] = K[x_1, \ldots, x_n]$):

$$\begin{array}{rcl}
\{\text{algebraic sets in } \mathbb{A}^n_K\} & \overset{HN}{\longleftrightarrow} & \{\text{radical ideals in } K[x]\} \\
\bigcup & & \bigcup \\
\{\text{irreducible algebraic sets in } \mathbb{A}^n_K\} & \longleftrightarrow & \{\text{prime ideals in } K[x]\} \\
\bigcup & & \bigcup \\
\{\text{points of } \mathbb{A}^n_K\} & \longleftrightarrow & \{\text{maximal ideals in } K[x]\} .
\end{array}$$

How to solve polynomial systems?

Let > be the lexicographical ordering lp, i.e. $x_1 > \ldots, > x_n$.
A set of polynomials $F = \{f_1, \ldots, f_n\} \subset K[x_1, \ldots, x_n]$ is called a *triangular set* if for each i

(1) $f_i \in K[x_{n-i+1}, \ldots, x_n]$,

(2) $LM(f_i) = x_{n-i+1}^{m_i}$, for some $m_i > 0$.

Hence, f_1 depends only on x_n, f_2 on x_{n-1}, x_n and so on, until f_n which depends on all variables.

How to solve polynomial systems?

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Let > be the lexicographical ordering lp, i.e. $x_1 > \ldots, > x_n$.
A set of polynomials $F = \{f_1, \ldots, f_n\} \subset K[x_1, \ldots, x_n]$ is called a *triangular set* if for each i

(1) $f_i \in K[x_{n-i+1}, \ldots, x_n]$,

(2) $LM(f_i) = x_{n-i+1}^{m_i}$, for some $m_i > 0$.

Hence, f_1 depends only on x_n, f_2 on x_{n-1}, x_n and so on, until f_n which depends on all variables.

- A list of triangular sets $F_1, \ldots, F_s$ is called a *triangular decomposition* of the zero–dimensional ideal I if

$$\sqrt{I} = \sqrt{\langle F_1 \rangle} \cap \ldots \cap \sqrt{\langle F_s \rangle}.$$

How to solve polynomial systems?

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Let > be the lexicographical ordering lp, i.e. $x_1 > \ldots, > x_n$.
A set of polynomials $F = \{f_1, \ldots, f_n\} \subset K[x_1, \ldots, x_n]$ is called a *triangular set* if for each i

(1) $f_i \in K[x_{n-i+1}, \ldots, x_n]$,

(2) $LM(f_i) = x_{n-i+1}^{m_i}$, for some $m_i > 0$.

Hence, f_1 depends only on x_n, f_2 on x_{n-1}, x_n and so on, until f_n which depends on all variables.

- A list of triangular sets $F_1, \ldots, F_s$ is called a *triangular decomposition* of the zero–dimensional ideal I if

$$\sqrt{I} = \sqrt{\langle F_1 \rangle} \cap \ldots \cap \sqrt{\langle F_s \rangle}.$$

- A triangular set is a Gröbner basis.

How to solve polynomial systems?

- Let $M \subset K[x_1, \ldots, x_n]$ be a maximal ideal and $G = \{g_1, \ldots, g_r\}$ a minimal Gröbner basis of M such that $LM(g_1) < \ldots < LM(g_r)$. Then G is a triangular set, in particular $r = n$.

How to solve polynomial systems?

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

- Let $M \subset K[x_1, \ldots, x_n]$ be a maximal ideal and $G = \{g_1, \ldots, g_r\}$ a minimal Gröbner basis of M such that $LM(g_1) < \ldots < LM(g_r)$. Then G is a triangular set, in particular $r = n$.
- There is an algorithm to compute a triangular decomposition of the zero-dimensional ideal I without computing the associated maximal ideals using only Gröbner bases and no multivariate polynomial factorization.

How to solve polynomial systems?

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

- Let $M \subset K[x_1, \ldots, x_n]$ be a maximal ideal and $G = \{g_1, \ldots, g_r\}$ a minimal Gröbner basis of M such that $LM(g_1) < \ldots < LM(g_r)$. Then G is a triangular set, in particular $r = n$.
- There is an algorithm to compute a triangular decomposition of the zero-dimensional ideal I without computing the associated maximal ideals using only Gröbner bases and no multivariate polynomial factorization.
- This algorithm is implemented in SINGULAR: solve.lib .

How to solve polynomial systems?


```
ring  A=0,(x,y,z),lp;
ideal I=x2+y+z-1,
        x+y2+z-1,
        x+y+z2-1;

LIB"solve.lib";
list s1=solve(I,6);

[1]:            [2]:     [3]:                [4]:      [5]:
   [1]:            [1]:     [1]:                [1]:      [1]:
       0.414214       0          -2.414214         1         0
   [2]:            [2]:     [2]:                [2]:      [2]:
       0.414214       0          -2.414214         0         1
   [3]:            [3]:     [3]:                [3]:      [3]:
       0.414214       1          -2.414214         0         0
```

Sudoku

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

				5			8	
				6	2			5
6			4			7		
		7				9	6	
		5	2		6	1		
	3	6				4		
		3			7			4
1			5	8				
	6			1				

Sudoku

- the idea of a Sudoku goes back to Leonard Euler: Latin squares
- in our days invented by Howard Garns (USA): Number place

Sudoku

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

- the idea of a Sudoku goes back to Leonard Euler: Latin squares
- in our days invented by Howard Garns (USA): Number place

J.Gago-Vargas, I. Hartillo-Hermoso, J. Martin-Morales, J. Maria Ucha-Enriquez:
Sudokus and Gröbner bases: not only a Divertimento

Sudoku

- the idea of a Sudoku goes back to Leonard Euler: Latin squares
- in our days invented by Howard Garns (USA): Number place

J.Gago-Vargas, I. Hartillo-Hermoso, J. Martin-Morales, J. Maria Ucha-Enriquez:
Sudokus and Gröbner bases: not only a Divertimento

- associate to the places in a Sudoku the variables $x_1, \ldots, x_{81}$ and to each variable x_i the polynomial $F_i(x_i) = \prod_{j=1}^{9}(x_i - j)$
- Let $E = \{(i,j), i < j$ and i,j in the same row, column or $3 \times 3-$box$\}$
- For $(i,j) \in E$ let $G_{i,j} = \frac{F_i - F_j}{x_i - x_j}$.
- Let $I \subset \mathbb{Q}[x_1, \ldots, x_{81}]$ be the ideal generated by the 891 polynomials $\{G_{i,j}\}_{(i,j)\in E}$ and $\{F_i\}_{i=1,\ldots,9}$

Sudoku

- $a = (a_1, \ldots, a_{81}) \in V(I)$ iff $a_i \in \{1, \ldots, 9\}$ and $a_i \neq a_j$ for $(i, j) \in E$
- a well posed Sudoku has a unique solution.
- Let $L \subset \{1, \ldots, 81\}$ be the set of pre-assigned places and $\{a_i\}_{i \in L}$ the corresponding numbers of a concrete Sudoku S.
- Then $I_S = I + < \{x_i - a_i\}_{i \in L} >$ is the ideal associated to the Sudoku S. It has to be a maximal ideal if the Sudoku is well posed.

Sudoku

- $a = (a_1, \ldots, a_{81}) \in V(I)$ iff $a_i \in \{1, \ldots, 9\}$ and $a_i \neq a_j$ for $(i, j) \in E$
- a well posed Sudoku has a unique solution.
- Let $L \subset \{1, \ldots, 81\}$ be the set of pre-assigned places and $\{a_i\}_{i \in L}$ the corresponding numbers of a concrete Sudoku S.
- Then $I_S = I + < \{x_i - a_i\}_{i \in L} >$ is the ideal associated to the Sudoku S. It has to be a maximal ideal if the Sudoku is well posed.
- The reduced Gröbner basis of I_S with respect to the lexicographical ordering has the shape $x_1 - a_1, \ldots, x_{81} - a_{81}$ and $(a_1, \ldots, a_{81})$ is the solution of the Sudoku.

Models for economy

Felix Kubler and Karl Schmedders (University of Zürich)

General problem:

- Study a computer model of a national economy,
  a standard exchange economy with finitely many agents and goods
- especially study equilibria
  Walrasian equilibrium consists of prices and choices, such that household maximize utilities, firms maximize profits and markets clear

Models for economy

Felix Kubler and Karl Schmedders (University of Zürich)

General problem:

- Study a computer model of a national economy,
  a standard exchange economy with finitely many agents and goods
- especially study equilibria
  Walrasian equilibrium consists of prices and choices, such that household maximize utilities, firms maximize profits and markets clear

Mathematical problem:
Find the positive real roots of a given system of polynomial equations

equilibrium model with production

```
ring R = 0,x(1..22),dp;
ideal I = -1+x(1)^5*x(4)*x(13),      -1+x(2)^5*x(4)*x(14),
-1+x(3)^5*x(4)*x(15),     -1+x(5)^3*x(8)*x(13),        -1+x(6)^3*x(8)*x(14),
-1+x(7)^3*x(8)*x(15),                              -1+x(9)^4*x(12)*x(13),
-1+x(10)^4*x(12)*x(14),                         -1+x(11)^4*x(12)*x(15),
5+2*x(16)-x(1)*x(13)-x(2)*x(14)-x(3)*x(15),
3+5*x(16)-x(5)*x(13)-x(6)*x(14)-x(7)*x(15),
(x(1)+x(5)+x(9))^3-x(17)^2*x(18),
(x(2)+x(6)+x(10))^2-x(19)*x(20),
(x(3)+x(7)+x(11))^2-4*x(21)*x(22),
x(17)+x(19)+x(21)-10,                              x(18)+x(20)+x(22)-10,
8*x(13)^3*x(18)-27*x(16)^3*x(17),    x(13)^3*x(17)^2-27*x(18)^2,
x(14)^2*x(20)-4*x(16)^2*x(19),         x(14)^2*x(19)-4*x(20),
x(15)^2*x(22)-x(16)^2*x(21),             x(15)^2*x(21)-x(22);
```

Primary decomposition

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Let A be a Noetherian ring, and let $I \subsetneq A$ be an ideal.

1. The set of *associated primes* of I, denoted by $Ass(I)$, is defined as $Ass(I) = \{P \subset A \| P \text{ prime}, P = I : \langle b \rangle \text{ for some } b \in A\}$.
   Elements of $Ass(\langle 0 \rangle)$ are also called *associated primes* of A.

Primary decomposition

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Let A be a Noetherian ring, and let $I \subsetneq A$ be an ideal.

1. The set of *associated primes* of I, denoted by $Ass(I)$, is defined as $Ass(I) = \{P \subset A \| P$ prime, $P = I : \langle b \rangle$ for some $b \in A\}$.
   Elements of $Ass(\langle 0 \rangle)$ are also called *associated primes* of A.
2. Let $P, Q \in Ass(I)$ and $Q \subsetneq P$, then P is called an *embedded prime ideal* of I. $Ass(I, P) := \{Q \mid Q \in Ass(I), Q \subset P\}$.

Primary decomposition

Let A be a Noetherian ring, and let $I \subsetneq A$ be an ideal.

1. The set of *associated primes* of I, denoted by $Ass(I)$, is defined as $Ass(I) = \{P \subset A \| P \text{ prime}, P = I : \langle b \rangle \text{ for some } b \in A\}$.
   Elements of $Ass(\langle 0 \rangle)$ are also called *associated primes* of A.
2. Let $P, Q \in Ass(I)$ and $Q \subsetneq P$, then P is called an *embedded prime ideal* of I. $Ass(I, P) := \{Q \mid Q \in Ass(I), Q \subset P\}$.
3. I is called *equidimensional* or *pure dimensional* if all associated primes of I have the same dimension.

Primary decomposition

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Let A be a Noetherian ring, and let $I \subsetneq A$ be an ideal.

1. The set of *associated primes* of I, denoted by $Ass(I)$, is defined as $Ass(I) = \{P \subset A \| P$ prime, $P = I : \langle b \rangle$ for some $b \in A\}$. Elements of $Ass(\langle 0 \rangle)$ are also called *associated primes* of A.
2. Let $P, Q \in Ass(I)$ and $Q \subsetneq P$, then P is called an *embedded prime ideal* of I. $Ass(I, P) := \{Q \mid Q \in Ass(I), Q \subset P\}$.
3. I is called *equidimensional* or *pure dimensional* if all associated primes of I have the same dimension.
4. I is a *primary ideal* if, for any $a, b \in A$, $ab \in I$ and $a \notin I$ imply $b \in \sqrt{I}$. Let P be a prime ideal, then a primary ideal I is called P*–primary* if $P = \sqrt{I}$.

Primary decomposition

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Let A be a Noetherian ring, and let $I \subsetneq A$ be an ideal.

1. The set of *associated primes* of I, denoted by $Ass(I)$, is defined as $Ass(I) = \{P \subset A \| P$ prime, $P = I : \langle b \rangle$ for some $b \in A\}$. Elements of $Ass(\langle 0 \rangle)$ are also called *associated primes* of A.
2. Let $P, Q \in Ass(I)$ and $Q \subsetneq P$, then P is called an *embedded prime ideal* of I. $Ass(I, P) := \{Q \mid Q \in Ass(I), Q \subset P\}$.
3. I is called *equidimensional* or *pure dimensional* if all associated primes of I have the same dimension.
4. I is a *primary ideal* if, for any $a, b \in A$, $ab \in I$ and $a \notin I$ imply $b \in \sqrt{I}$. Let P be a prime ideal, then a primary ideal I is called *P–primary* if $P = \sqrt{I}$.
5. A *primary decomposition* of I, that is, a decomposition $I = Q_1 \cap \cdots \cap Q_s$ with Q_i primary ideals, is called *irredundant* if no Q_i can be omitted and if $\sqrt{Q_i} \neq \sqrt{Q_j}$ for all $i \neq j$.

Primary decomposition

- Let A be a Noetherian ring and $I \subsetneq A$ be an ideal, then there exists an irredundant decomposition $I = Q_1 \cap \cdots \cap Q_r$ of I as intersection of primary ideals $Q_1, \ldots, Q_r$.

Primary decomposition

- Let A be a Noetherian ring and $I \subsetneq A$ be an ideal, then there exists an irredundant decomposition $I = Q_1 \cap \cdots \cap Q_r$ of I as intersection of primary ideals $Q_1, \ldots, Q_r$.
- Let A be a ring and $I \subset A$ be an ideal with irredundant primary decomposition $I = Q_1 \cap \cdots \cap Q_r$. Then $r = \#Ass(I)$,

$$Ass(I) = \{\sqrt{Q_1}, \ldots, \sqrt{Q_r}\},$$

and if $\{\sqrt{Q_{i_1}}, \ldots, \sqrt{Q_{i_s}}\} = Ass(I, P)$ for $P \in Ass(I)$ then $Q_{i_1} \cap \cdots \cap Q_{i_s}$ is independent of the decomposition.

Primary decomposition

1. If $I = \langle f \rangle \subset K[x_1, \dots, x_n]$ is a principal ideal and $f = f_1^{n_1} \cdots f_s^{n_s}$ is the factorization of f into irreducible factors, then

$$I = \langle f_1^{n_1} \rangle \cap \cdots \cap \langle f_r^{n_r} \rangle$$

is the primary decomposition, and the $\langle f_i \rangle$ are the associated prime ideals which are all minimal.

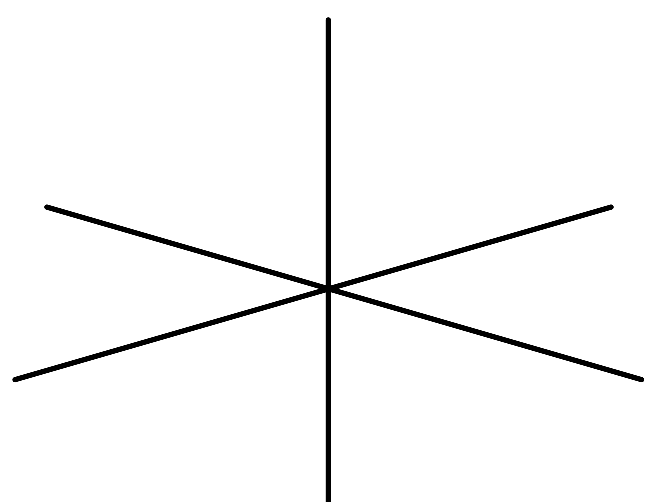
Primary decomposition

1. If $I = \langle f \rangle \subset K[x_1, \ldots, x_n]$ is a principal ideal and $f = f_1^{n_1} \cdots f_s^{n_s}$ is the factorization of f into irreducible factors, then

$$I = \langle f_1^{n_1} \rangle \cap \cdots \cap \langle f_r^{n_r} \rangle$$

   is the primary decomposition, and the $\langle f_i \rangle$ are the associated prime ideals which are all minimal.

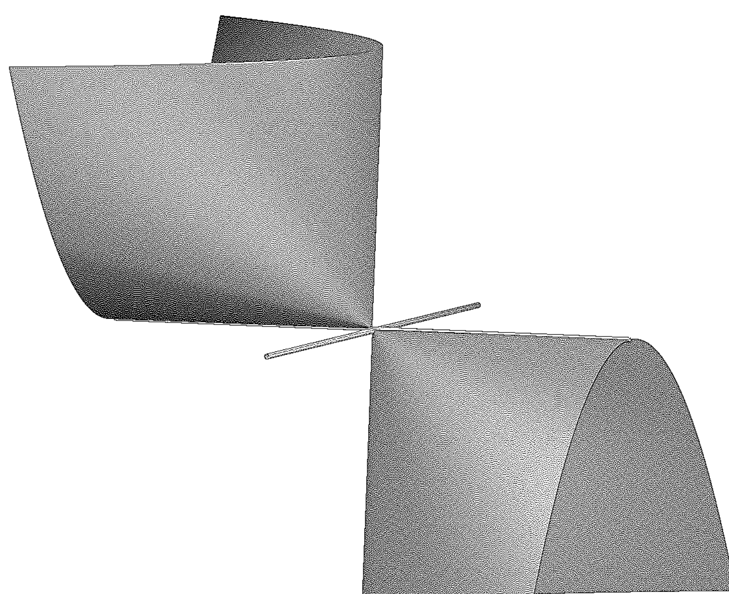
2. Let $I = \langle xy, xz, yz \rangle = \langle x, y \rangle \cap \langle x, z \rangle \cap \langle y, z \rangle \subset K[x, y, z]$. Then the zero–set $V(I)$ is the union of the coordinate axes .



Primary decomposition

Let $I = \langle (y^2 - xz)\cdot(z^2 - x^2y),\ (y^2 - xz)\cdot z\rangle \subset K[x,y,z]$.

- $I = \langle y^2 - xz\rangle \cap \langle x^2, z\rangle \cap \langle y, z^2\rangle$,
- $Ass(I) = \{\langle y^2 - xz\rangle, \langle x, z\rangle, \langle y, z\rangle\}$
- $minAss(I) = \{\langle y^2 - xz\rangle, \langle x, z\rangle\}$.
- $\langle y, z\rangle$ is an embedded prime $Ass(I, \langle y, z\rangle) = \{\langle y^2 - xz\rangle, \langle y, z\rangle\}$.



Gianni, Trager, Zacharias

Definition

- A maximal ideal $M \subset K[x_1, \ldots, x_n]$ is called in general position with respect to the lexicographical ordering with $x_1 > \cdots > x_n$, if there exist $g_1, \ldots, g_n \in K[x_n]$ with $M = \langle x_1 + g_1(x_n), \ldots, x_{n-1} + g_{n-1}(x_n), g_n(x_n)\rangle$.

Gianni, Trager, Zacharias

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Definition

- A maximal ideal $M \subset K[x_1, \dots, x_n]$ is called in general position with respect to the lexicographical ordering with $x_1 > \cdots > x_n$, if there exist $g_1, \dots, g_n \in K[x_n]$ with $M = \langle x_1 + g_1(x_n), \dots, x_{n-1} + g_{n-1}(x_n), g_n(x_n)\rangle$.
- A zero–dimensional ideal $I \subset K[x_1, \dots, x_n]$ is called in general position with respect to the lexicographical ordering with $x_1 > \cdots > x_n$, if all associated primes $P_1, \dots, P_k$ are in general position and if $P_i \cap K[x_n] \neq P_j \cap K[x_n]$ for $i \neq j$.

Proposition

Let K be a field of characteristic 0, and let $I \subset K[x]$, $x = (x_1, \dots, x_n)$, be a zero–dimensional ideal. Then there exists a non–empty, Zariski open subset $U \subset K^{n-1}$ such that for all $\underline{a} = (a_1, \dots, a_{n-1}) \in U$, the coordinate change $\varphi_{\underline{a}} : K[x] \to K[x]$ defined by $\varphi_{\underline{a}}(x_i) = x_i$ if $i < n$, and

$$\varphi_{\underline{a}}(x_n) = x_n + \sum_{i=1}^{n-1} a_i x_i$$

has the property that $\varphi_{\underline{a}}(I)$ is in general position with respect to the lexicographical ordering defined by $x_1 > \cdots > x_n$.

Proposition

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Let $I \subset K[x_1, \ldots, x_n]$ be a zero–dimensional ideal. Let $\langle g \rangle = I \cap K[x_n]$, $g = g_1^{\nu_1} \ldots g_s^{\nu_s}$, g_i monic and prime and $g_i \neq g_j$ for $i \neq j$. Then

- $I = \bigcap_{i=1}^{s} \langle I, g_i^{\nu_i} \rangle$.

Proposition

Let $I \subset K[x_1, \ldots, x_n]$ be a zero–dimensional ideal. Let $\langle g \rangle = I \cap K[x_n]$, $g = g_1^{\nu_1} \ldots g_s^{\nu_s}$, g_i monic and prime and $g_i \neq g_j$ for $i \neq j$. Then

- $I = \bigcap_{i=1}^{s} \langle I, g_i^{\nu_i} \rangle$.
- If I is in general position with respect to the lexicographical ordering with $x_1 > \cdots > x_n$, then

(2) $\langle I, g_i^{\nu_i} \rangle$ is a primary ideal for all i.

Criterion

Let $I \subset K[x_1, \ldots, x_n]$ be a proper ideal. Then the following conditions are equivalent:

- I is zero–dimensional, primary and in general position with respect to the lexicographical ordering with $x_1 > \cdots > x_n$.
- There exist $g_1, \ldots, g_n \in K[x_n]$ and positive integers $\nu_1, \ldots, \nu_n$ such that
  - $I \cap K[x_n] = \langle g_n^{\nu_n} \rangle$, g_n irreducible;
  - for each $j < n$, I contains the element $\left(x_j + g_j\right)^{\nu_j}$.

Criterion

Let $I \subset K[x_1, \ldots, x_n]$ be a proper ideal. Then the following conditions are equivalent:

- I is zero–dimensional, primary and in general position with respect to the lexicographical ordering with $x_1 > \cdots > x_n$.
- There exist $g_1, \ldots, g_n \in K[x_n]$ and positive integers $\nu_1, \ldots, \nu_n$ such that
  - $I \cap K[x_n] = \langle g_n^{\nu_n} \rangle$, g_n irreducible;
  - for each $j < n$, I contains the element $\left(x_j + g_j\right)^{\nu_j}$.
- Let S be a reduced Gröbner basis of I with respect to the lexicographical ordering with $x_1 > \ldots > x_n$. Then there exist $g_1, \ldots, g_n \in K[x_n]$ and positive integers $\nu_1, \ldots, \nu_n$ such that
  - $g_n^{\nu_n} \in S$ and g_n is irreducible;
  - $(x_j + g_j)^{\nu_j}$ is congruent to an element in $S \cap K[x_j, \ldots, x_n]$ modulo $\langle g_n, x_{n-1} + g_{n-1}, \ldots, x_{j+1} + g_{j+1} \rangle \subset K[x]$ for $j = 1, \ldots, n-1$.

primaryTest(I)

- Input: A zero–dimensional ideal $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$, $x = (x_1, \ldots, x_n)$.
- Output: $\sqrt{I}$ if I is primary and in general position or $< 0 >$ else.
  - compute a reduced Gröbner basis S of I with respect to the lexicographical ordering with $x_1 > \cdots > x_n$;
  - factorize $g \in S$, the element with smallest leading monomial;
  - if ($g = g_n^{\nu_n}$ with g_n irreducible) prim := $\langle g_n \rangle$
    else return $\langle 0 \rangle$.
  - $i := n$;
    while $(i > 1)$
    - $i := i - 1$;
    - choose $f \in S$ with $LM(f) = x_i^m$;
    - $b :=$ the coefficient of x_i^{m-1} in f considered as polynomial in x_i;
    - $q := x_i + b/m$;
    - if ($q^m \equiv f \mod$ prim) prim := prim + $\langle q \rangle$;
    - else return $\langle 0 \rangle$;
  - return prim.

zeroDecomp(I)

- Input: a zero-dimensional ideal $I := \langle f_1, \dots, f_k \rangle \subset K[x]$, $x = (x_1, \dots, x_n)$.
- Output: a set of pairs (Q_i, P_i) of ideals in $K[x]$, $i = 1, \dots, r$, such that
  - $I = Q_1 \cap \dots \cap Q_r$ is a primary decomposition of I, and
  - $P_i = \sqrt{Q_i}$, $i = 1, \dots, r$.

  - result $:= \emptyset$;
  - choose a random $\underline{a} \in K^{n-1}$, and apply the coordinate change $I' := \varphi_{\underline{a}}(I)$;
  - compute a Gröbner basis G of I' with respect to the lexicographical ordering with $x_1 > \dots > x_n$, let $g \in G$ be the element with smallest leading monomial.
  - factorize $g = g_1^{\nu_1} \cdot \ldots \cdot g_s^{\nu_s} \in K[x_n]$;
  - for $i = 1$ to s do

    set $Q_i' := \langle I', g_i^{\nu_i} \rangle$ and $Q_i := \langle I, \varphi_{\underline{a}}^{-1}(g_i)^{\nu_i} \rangle$;
    set $P_i' :=$ PRIMARYTEST(Q_i');
    if $P_i' \neq \langle 0 \rangle$
        set $P_i := \varphi_{\underline{a}}^{-1}(P_i')$;
        result := result $\cup \{(Q_i, P_i)\}$;
    else
        result := result $\cup$ ZERODECOMP (Q_i);
  - return result.

Example

```
ring R=0,(x,y),lp;
ideal I=(x2-2)^2,y2-2;

map phi=R,x,x+y;       //coordinate change
map psi=R,x,-x+y;      //the inverse map
I=std(phi(I));
I;
I[1]=y6-16y4+64y2
I[2]=32xy2+y5+8y3
I[3]=x2+2xy+y2-2

factorize(I[1]);
[1]:
   _[1]=1
   _[2]=y
   _[3]=y2-8
[2]:
   1,2,2
```

Example

```
ideal Q1=std(I,(y^2)); //the candidates for the
                             //primary ideals
ideal Q2=std(I,(y^2-8)^2);     //in general position
Q1; Q2;

Q1[1]=y2                    Q1[2]=x2+2xy-2

Q2[1]=y4-16y2+64            Q2[2]=32x+y3+8y

Q2=std(psi(Q2));
Q2;
Q2[1]=y2-2                   Q2[2]=x2+2xy+2
```

Example

```
> primdecGTZ(I);
[1]:
   [1]:
      _[1]=y2-2
      _[2]=x2-2xy+2
   [2]:
      _[1]=y2-2
      _[2]=x-y
[2]:
   [1]:
      _[1]=y2-2
      _[2]=x2+2xy+2
   [2]:
      _[1]=y2-2
      _[2]=x+y
```

Proposition

Let $I \subset K[x]$ be an ideal and $u \subset x = \{x_1, \ldots, x_n\}$ be a maximal independent set of variables with respect to I.
($I \cap K[u] = \{0\}$ and $\#(u) = dim(K[x]/I)$)

- $IK(u)[x \smallsetminus u] \subset K(u)[x \smallsetminus u]$ is a zero–dimensional ideal.
- Let $S = \{g_1, \ldots, g_s\} \subset I \subset K[x]$ be a Gröbner basis of $IK(u)[x \smallsetminus u]$, and let $h :=$ lcm$\big($LC$(g_1), \ldots,$ LC$(g_s)\big) \in K[u]$, then

$$IK(u)[x \smallsetminus u] \cap K[x] = I : \langle h^\infty \rangle\,,$$

and this ideal is equidimensional of dimension $\dim(I)$.

Proposition

Let $I \subset K[x]$ be an ideal and $u \subset x = \{x_1, \ldots, x_n\}$ be a maximal independent set of variables with respect to I.
($I \cap K[u] = \{0\}$ and $\#(u) = dim(K[x]/I)$)

- $IK(u)[x \smallsetminus u] \subset K(u)[x \smallsetminus u]$ is a zero–dimensional ideal.
- Let $S = \{g_1, \ldots, g_s\} \subset I \subset K[x]$ be a Gröbner basis of $IK(u)[x \smallsetminus u]$, and let $h := \text{lcm}\big(\text{LC}(g_1), \ldots, \text{LC}(g_s)\big) \in K[u]$, then

  $$IK(u)[x \smallsetminus u] \cap K[x] = I : \langle h^\infty \rangle \,,$$

  and this ideal is equidimensional of dimension $\dim(I)$.
- Let $IK(u)[x \smallsetminus u] = Q_1 \cap \cdots \cap Q_s$ be an irredundant primary decomposition, then also $IK(u)[x \smallsetminus u] \cap K[x] = (Q_1 \cap K[x]) \cap \cdots \cap (Q_s \cap K[x])$ is an irredundant primary decomposition.

reductionToZero(I)

- Input: $I := \langle f_1, \dots, f_k \rangle \subset K[x]$, $x = (x_1, \dots, x_n)$.
- Output: A list (u, G, h), where
  – $u \subset x$ is a maximal independent set with respect to I,
  – $G = \{g_1, \dots, g_s\} \subset I$ is a Gröbner basis of $IK(u)[x \smallsetminus u]$,
  – $h \in K[u]$ such that $IK(u)[x \smallsetminus u] \cap K[x] = I : \langle h \rangle = I : \langle h^\infty \rangle$.

  - compute a maximal independent set $u \subset x$ with respect to I;
  - compute a Gröbner basis $G = \{g_1, \dots, g_s\}$ of I with respect to the lexicographical ordering with $x \smallsetminus u > u$;
  - $h := \prod_{i=1}^{s} \mathrm{LC}(g_i) \in K[u]$, where the g_i are considered as polynomials in $x \smallsetminus u$ with coefficients in $K(u)$;
  - compute m such that $\langle g_1, \dots, g_s \rangle : \langle h^m \rangle = \langle g_1, \dots, g_s \rangle : \langle h^{m+1} \rangle$;
  - return $u, \{g_1, \dots, g_s\}, h^m$.

decomp(I)

- Input: $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$, $x = (x_1, \ldots, x_n)$.
- Output: a set of pairs (Q_i, P_i) of ideals in $K[x]$, $i = 1, \ldots, r$, such that
  - $I = Q_1 \cap \cdots \cap Q_r$ is a primary decomposition of I, and
  - $P_i = \sqrt{(}Q_i)$, $i = 1, \ldots, r$.

  - (u, G, h) := REDUCTIONTOZERO (I);
  - change ring to $K(u)[x \setminus u]$ and compute
    qprimary := ZERODECOMP $(\langle G \rangle_{K(u)[x \setminus u]})$;
  - change ring to $K[x]$ and compute
    primary := $\{(Q' \cap K[x],\ P' \cap K[x]) \mid (Q', P') \in$ qprimary$\}$;
  - primary := primary $\cup$ DECOMP $(\langle I, h^n \rangle)$;
  - return primary.

Definition

Let A be a Noetherian ring, let $I \subset A$ be an ideal, and let $I = Q_1 \cap \cdots \cap Q_s$ be an irredundant primary decomposition.

- The equidimensional part $E(I)$ is the intersection of all primary ideals Q_i with $\dim(Q_i) = \dim(I)$.

Definition

Let A be a Noetherian ring, let $I \subset A$ be an ideal, and let $I = Q_1 \cap \cdots \cap Q_s$ be an irredundant primary decomposition.

- The equidimensional part $E(I)$ is the intersection of all primary ideals Q_i with $\dim(Q_i) = \dim(I)$.
- The ideal I (respectively the ring A/I) is called equidimensional or pure dimensional if $E(I) = I$. In particular, the ring A is called equidimensional if $E(\langle 0 \rangle) = \langle 0 \rangle$.

equidimensional(I)

- Input: $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$, $x = (x_1, \ldots, x_n)$.
- Output: $E(I) \subset K[x]$, the equidimensional part of I.
  - set (u, G, h) := REDUCTIONTOZERO (I);
  - if $(\dim(\langle I, h \rangle) < \dim(I))$
    return $(\langle G \rangle : \langle h \rangle)$;
    else
    return $\big((\langle G \rangle : \langle h \rangle) \cap$ EQUIDIMENSIONAL $(\langle I, h \rangle)\big)$.

Proposition

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Let $I \subset K[x_1, \ldots, x_n]$ be a zero–dimensional ideal and $I \cap K[x_i] = \langle f_i \rangle$ for $i = 1, \ldots, n$. Moreover, let g_i be the squarefree part of f_i, then $\sqrt{I} = I + \langle g_1, \ldots, g_n \rangle$.

proof

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

- Obviously, $I \subset I + \langle g_1, \ldots, g_n \rangle \subset \sqrt{I}$. Hence, it remains to show that $a^n \in I$ implies that $a \in I + \langle g_1, \ldots, g_n \rangle$.

proof

- Obviously, $I \subset I + \langle g_1, \ldots, g_n \rangle \subset \sqrt{I}$. Hence, it remains to show that $a^n \in I$ implies that $a \in I + \langle g_1, \ldots, g_n \rangle$.
- Let $\overline{K}$ be the algebraic closure of K. We see that each g_i is the product of different linear factors of $\overline{K}[x_i]$. These linear factors of the g_i induce a splitting of the ideal $(I + \langle g_1, \ldots, g_n \rangle)\overline{K}[x]$ into an intersection of maximal ideals.

proof

Technische Universität Kaiserslautern

- Obviously, $I \subset I + \langle g_1, \ldots, g_n \rangle \subset \sqrt{I}$. Hence, it remains to show that $a^n \in I$ implies that $a \in I + \langle g_1, \ldots, g_n \rangle$.
- Let $\overline{K}$ be the algebraic closure of K. We see that each g_i is the product of different linear factors of $\overline{K}[x_i]$. These linear factors of the g_i induce a splitting of the ideal $(I + \langle g_1, \ldots, g_n \rangle)\overline{K}[x]$ into an intersection of maximal ideals.
- Hence, $(I + \langle g_1, \ldots, g_n \rangle)\overline{K}[x]$ is radical. Now consider $a \in K[x]$ with $a^n \in I + \langle g_1, \ldots, g_n \rangle$. We obtain
$a \in (I + \langle g_1, \ldots, g_n \rangle)\overline{K}[x] \cap K[x] = I + \langle g_1, \ldots, g_n \rangle$.

zeroradical(I)

- Input: a zero–dimensional ideal $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$, $x = (x_1, \ldots, x_n)$.
- Output: $\sqrt{I} \subset K[x]$, the radical of I.
  - for $i = 1, \ldots, n$, compute $f_i \in K[x_i]$ such that $I \cap K[x_i] = \langle f_i \rangle$;
  - return $I + \langle \text{SQUAREFREE}(f_1), \ldots, \text{SQUAREFREE}(f_n) \rangle$.

radical(I)

- Input: $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$, $x = (x_1, \ldots, x_n)$.
- Output: $\sqrt{I} \subset K[x]$, the radical of I.
  - (u, G, h) := REDUCTIONTOZERO (I);
  - change ring to $K(u)[x \setminus u]$ and compute $J :=$ ZERORADICAL $(\langle G \rangle)$;
  - compute a Gröbner basis $\{g_1, \ldots, g_\ell\} \subset K[x]$ of J;
  - set $p := \prod_{i=1}^{\ell}$ LC$(g_i) \in K[u]$;
  - change ring to $K[x]$ and compute $J \cap K[x] = \langle g_1, \ldots, g_\ell \rangle : \langle p^\infty \rangle$;
  - return $(J \cap K[x]) \cap$ RADICAL $(\langle I, h \rangle)$.