Primary Decomposition

Gerhard Pfister

pfister@mathematik.uni-kl.de

Departement of Mathematics

University of Kaiserslautern

Primary Decomposition: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).

Primary Decomposition: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).

Primary Decomposition:References

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

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

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 $x_1 > \dots > x_n$, 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 $x_1 > \dots > x_n$, 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 $I \subset K[x]$, $x = (x_1, \ldots, x_n)$, be a zero–dimensional ideal. Then there exists a non–empty, Zariski open subset $U \subset K^{n-1}$ such that for all $\underline{a} = (a_1, \ldots, a_{n-1}) \in U$, 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

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

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Let $I \subset K[x_1, \dots, x_n]$ 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 $g_1, \dots, g_n \in K[x_n]$ and positive integers $\nu_1, \dots, \nu_n$ 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 $g_1, \dots, g_n \in K[x_n]$ and positive integers $\nu_1, \dots, \nu_n$ 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 $S \cap K[x_j, \dots, x_n]$ modulo $\langle g_n, x_{n-1} + g_{n-1}, \dots, x_{j+1} + g_{j+1} \rangle \subset K[x]$ for $j = 1, \dots, n-1$.

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 coeffi cient 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)

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

- Input: a zero-dimensional ideal $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$, $x = (x_1, \ldots, x_n)$.
- 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
  – $P_i = \sqrt{Q_i}$, $i = 1, \ldots, r$.

  - 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 $x_1 > \cdots > x_n$, 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.

Proposition

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

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 $\dim(I)$.

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

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

decomp(I)

- Input: $I := \langle f_1, \dots, f_k \rangle \subset K[x]$, $x = (x_1, \dots, x_n)$.
- 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
  - $P_i = \sqrt{(}Q_i)$, $i = 1, \dots, r$.

  - (u, G, h) := REDUCTIONTOZERO (I);
  - change ring to $K(u)[x \smallsetminus u]$ and compute
    qprimary := ZERODECOMP $(\langle G \rangle_{K(u)[x \smallsetminus u]})$;
  - 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

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

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

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 $K(u)[x \smallsetminus u]$ 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 $(\langle I, h \rangle)$.

Hensel's Lemma

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

Let A be one of the following rings:
$\mathbb{Z}, \mathbb{Z}[x_1, \ldots, x_n], \mathbb{Q}[x_1, \ldots, x_n], \mathbb{C}[x_1, \ldots, x_n]$.

- Let $I \subseteq A$ be an ideal and $f(x) \in A[x]$ monic.
- Assume, $g_1(x), h_1(x) \in A/I[x]$ are relatively prime and monic, such that $f(x) = g_1(x) \cdot h_1(x) \mod I$.

Hensel's Lemma

Let A be one of the following rings:
$\mathbb{Z}, \mathbb{Z}[x_1, \ldots, x_n], \mathbb{Q}[x_1, \ldots, x_n], \mathbb{C}[x_1, \ldots, x_n]$.

- Let $I \subseteq A$ be an ideal and $f(x) \in A[x]$ monic.
- Assume, $g_1(x), h_1(x) \in A/I[x]$ are relatively prime and monic, such that $f(x) = g_1(x) \cdot h_1(x) \mod I$.
- Then there exist monic polynomials $g_n, h_n \in A/I^n[x]$ such that
  - $f = g_n \cdot h_n \mod I^n$
  - $g_n = g_1 \mod I\ ,\ h_n = h_1 \mod I$

Hensel's Lemma

Let A be one of the following rings:
$\mathbb{Z}, \mathbb{Z}[x_1, \dots, x_n], \mathbb{Q}[x_1, \dots, x_n], \mathbb{C}[x_1, \dots, x_n]$.

- Let $I \subseteq A$ be an ideal and $f(x) \in A[x]$ monic.
- Assume, $g_1(x), h_1(x) \in A/I[x]$ are relatively prime and monic, such that $f(x) = g_1(x) \cdot h_1(x) \mod I$.
- Then there exist monic polynomials $g_n, h_n \in A/I^n[x]$ such that
  - $f = g_n \cdot h_n \mod I^n$
  - $g_n = g_1 \mod I\ ,\ h_n = h_1 \mod I$
- Furthermore, there exist unique polynomials $\widehat{g}, \widehat{h} \in \widehat{A}_I[X]$ such that
  - $f = \widehat{g}\widehat{h}$
  - $\widehat{g} = g_1 \mod I\ ,\ \widehat{h} = h_1 \mod I$

Lifting a factorization

$f \in \mathbb{C}[x_1, \ldots, x_n] \quad I = \langle x_3 - a_3, \ldots, x_n - a_N \rangle$, $d_i = \deg_{x_i}(f)$
$\bar{f}^{(i)} = f(x_1, \ldots, x_i, a_4, \ldots, a_n)$

- $\bar{f}^{(2)} = g_1 \cdot h_1$
  Hensel's lemma in $A[x_1]$ $(A = \mathbb{C}[x_2, x_3]$, $I = \langle x_3 - a_3 \rangle)$

Lifting a factorization

$f \in \mathbb{C}[x_1, \ldots, x_n] \quad I = \langle x_3 - a_3, \ldots, x_n - a_N \rangle$, $d_i = \deg_{x_i}(f)$
$\bar{f}^{(i)} = f(x_1, \ldots, x_i, a_4, \ldots, a_n)$

- $\bar{f}^{(2)} = g_1 \cdot h_1$
  Hensel's lemma in $A[x_1]$ $(A = \mathbb{C}[x_2, x_3]\ ,\ I = \langle x_3 - a_3 \rangle)$
- $\bar{f}^{(3)} = g_{d_3+1} h_{d_3+1} \mod \langle x_3 - a_3 \rangle^{d_3+1}$
- if $f = f_1 \cdot f_2$ and
  $f_1(x_1, x_2, a_3, \ldots, a_n) = g_1, f_2(x_1, x_2, a_3, \ldots, a_n) = h_1$
  then

$$\begin{aligned} f_1(x_1, x_2, x_3, a_4 \ldots a_n) &= g_{d_3+1}(x_1, x_2, x_3) \\ f_2(x_1, x_2, x_3, a_4 \ldots a_n) &= h_{d_3+1}(x_1, x_2, x_3) \end{aligned}$$

  by unicity of Hensel's lemma.
- Restart with the next variable.

Gao's version of Bertini's Theorem

Let K be a field of characteristic 0 and $S \subset K$ a finite subset.

- Let $f \in K[x_1, \ldots, x_n]$, $\deg(f) = d$ and
  $f_0(x, y) = f(a_1 x + b_1 y + c_1, \ldots, a_n x + b_n y + c_n)$

Gao's version of Bertini's Theorem

Let K be a field of characteristic 0 and $S \subset K$ a finite subset.

- Let $f \in K[x_1, \ldots, x_n]$, $\deg(f) = d$ and $f_0(x, y) = f(a_1x + b_1y + c_1, \ldots, a_nx + b_ny + c_n)$
- Then, for random choices of a_i, b_i, c_i in S with probability at least $1 - \frac{2d^3}{|S|}$ all the absolute irreducible factors of f remain absolutely irreducible factors of f_0 in $K[x, y]$.

Irreducibility Testing

- Let $f \in \mathbb{Z}[x, y]$ be irreducible, if for some prime p
  - f is irreducible in $\mathbb{Z}/p\mathbb{Z}[x, y]$
  - there exists a simple point $(a, b) \in (\mathbb{Z}/p\mathbb{Z})^2$ of $V(f)$
  - the degree of $f \mod p$ is equal to the degree of f.

Irreducibility Testing

- Let $f \in \mathbb{Z}[x,y]$ be irreducible, if for some prime p
  - f is irreducible in $\mathbb{Z}/p\mathbb{Z}[x,y]$
  - there exists a simple point $(a,b) \in (\mathbb{Z}/p\mathbb{Z})^2$ of $V(f)$
  - the degree of $f \mod p$ is equal to the degree of f.
- The test is based on the following theorem:
  - Let k be a field and $(\alpha,\beta) \in \bar{k}^2$ be a simple point of $f \in k[x,y]$.
    Then one absolute irreducible factor belongs to $k[\alpha,\beta][x,y]$.

Splitting over $\mathbb{C}$

Theorem: Gao/Ruppert Let $f \in \mathbb{Q}[x,y]$ be irreducible of bidegree (m,n).

Let $G = \{g \in \mathbb{Q}[x,y] | (m-1,n) \geq deg(g), \exists h \in \mathbb{Q}[x,y], \frac{\partial(g/f)}{\partial y} = \frac{\partial(h/f)}{\partial x}\}$.

The vector space G has the following properties

Splitting over $\mathbb{C}$

Theorem: Gao/Ruppert Let $f \in \mathbb{Q}[x,y]$ be irreducible of bidegree (m,n).

Let $G = \{g \in \mathbb{Q}[x,y] | (m-1,n) \geq deg(g), \exists h \in \mathbb{Q}[x,y], \frac{\partial(g/f)}{\partial y} = \frac{\partial(h/f)}{\partial x}\}$.

The vector space G has the following properties

- f is irreducible in $\mathbb{C}[x,y]$ if and only if $dim_{\mathbb{Q}}(G) = 1$.

Splitting over $\mathbb{C}$

Theorem: Gao/Ruppert Let $f \in \mathbb{Q}[x,y]$ be irreducible of bidegree (m,n).

Let $G = \{g \in \mathbb{Q}[x,y] | (m-1,n) \geq deg(g), \exists h \in \mathbb{Q}[x,y], \frac{\partial(g/f)}{\partial y} = \frac{\partial(h/f)}{\partial x}\}$.

The vector space G has the following properties

- f is irreducible in $\mathbb{C}[x,y]$ if and only if $dim_{\mathbb{Q}}(G) = 1$.
- $gG \subset \frac{\partial f}{\partial x} G$ mod f for all $g \in G$.

Splitting over $\mathbb{C}$

Theorem: Gao/Ruppert Let $f \in \mathbb{Q}[x, y]$ be irreducible of bidegree (m, n).

Let $G = \{g \in \mathbb{Q}[x, y] | (m-1, n) \geq deg(g), \exists h \in \mathbb{Q}[x, y], \frac{\partial(g/f)}{\partial y} = \frac{\partial(h/f)}{\partial x}\}$.

The vector space G has the following properties

- f is irreducible in $\mathbb{C}[x, y]$ if and only if $dim_{\mathbb{Q}}(G) = 1$.
- $gG \subset \frac{\partial f}{\partial x} G$ mod f for all $g \in G$.
- Let $g_1, \ldots, g_a \in G$ be a basis and $g \in G \setminus \mathbb{Q}\frac{\partial f}{\partial x}$,

$$gg_i = \sum a_{ij} g_j \frac{\partial f}{\partial x} \mod f.$$

Let $\chi(t) = det(tE - (a_{ij}))$ be the characteristic polynomial. Then χ is irreducible in $\mathbb{Q}[t]$.

Splitting over $\mathbb{C}$

Theorem: Gao/Ruppert Let $f \in \mathbb{Q}[x,y]$ be irreducible of bidegree (m,n).

Let $G = \{g \in \mathbb{Q}[x,y] | (m-1,n) \geq deg(g), \exists h \in \mathbb{Q}[x,y], \frac{\partial(g/f)}{\partial y} = \frac{\partial(h/f)}{\partial x}\}$.

The vector space G has the following properties

- f is irreducible in $\mathbb{C}[x,y]$ if and only if $dim_{\mathbb{Q}}(G) = 1$.
- $gG \subset \frac{\partial f}{\partial x} G$ mod f for all $g \in G$.
- Let $g_1, \ldots, g_a \in G$ be a basis and $g \in G \setminus \mathbb{Q}\frac{\partial f}{\partial x}$,

  $$gg_i = \sum a_{ij} g_j \frac{\partial f}{\partial x} \mod f.$$

  Let $\chi(t) = det(tE - (a_{ij}))$ be the characteristic polynomial. Then χ is irreducible in $\mathbb{Q}[t]$.
- $f = \prod_{c \in \mathbb{C}, \chi(c)=0} gcd(f, g - c\frac{\partial f}{\partial x})$ is the decomposition of f into irreducible factors in $\mathbb{C}[x,y]$.

Splitting over $\mathbb{C}$: Example

- $f = x^2 + y^2$

Splitting over $\mathbb{C}$: Example

- $f = x^2 + y^2$
- $G = < x, y >_{\mathbb{Q}}$
- $$(a_{i,j}) = \begin{pmatrix} 0 & 1/2 \\ -1/2 & 0 \end{pmatrix}$$

Splitting over $\mathbb{C}$: Example

- $f = x^2 + y^2$
- $G = < x, y >_{\mathbb{Q}}$
- $$(a_{i,j}) = \begin{pmatrix} 0 & 1/2 \\ -1/2 & 0 \end{pmatrix}$$
- $\chi(t) = t^2 + 1/4$

Splitting over $\mathbb{C}$: Example

- $f = x^2 + y^2$
- $G = < x, y >_{\mathbb{Q}}$
- $$(a_{i,j}) = \begin{pmatrix} 0 & 1/2 \\ -1/2 & 0 \end{pmatrix}$$
- $\chi(t) = t^2 + 1/4$
- $gcd(x^2 + y^2, y - \frac{i}{2}2x)gcd(x^2 + y^2, y + \frac{i}{2}2x) = x^2 + y^2$

How to compute the normalization?

- Let A be a reduced ring, the normalization $\overline{A}$ is the integral closure of A in the total ring of fractions $Q(A)$.

How to compute the normalization?

- Let A be a reduced ring, the normalization $\overline{A}$ is the integral closure of A in the total ring of fractions $Q(A)$.
- Let A be a reduced Noetherian ring and $J \subset A$ an ideal containing a non–zerodivisor x of A. Then there are natural inclusions of rings

$$A \subset Hom_A(J, J) \cong \frac{1}{x} \cdot (xJ : J) \subset \overline{A}\,.$$

proof

- For $a \in A$, let $m_a : J \to J$ denote the multiplication with a. If $m_a = 0$, then $m_a(x) = ax = 0$ and, hence, $a = 0$, since x is a non–zerodivisor. Thus, $a \mapsto m_a$ defi nes an inclusion $A \subset Hom_A(J, J)$.

proof

- For $a \in A$, let $m_a : J \to J$ denote the multiplication with a. If $m_a = 0$, then $m_a(x) = ax = 0$ and, hence, $a = 0$, since x is a non–zerodivisor. Thus, $a \mapsto m_a$ defi nes an inclusion $A \subset Hom_A(J, J)$.
- It is easy to see that for $\varphi \in Hom_A(J, J)$ the element $\varphi(x)/x \in Q(A)$ is independent of x: for any $a \in J$ we have $\varphi(a) = (1/x) \cdot \varphi(xa) = a \cdot \varphi(x)/x$, since φ is A–linear.

proof

- For $a \in A$, let $m_a : J \to J$ denote the multiplication with a. If $m_a = 0$, then $m_a(x) = ax = 0$ and, hence, $a = 0$, since x is a non–zerodivisor. Thus, $a \mapsto m_a$ defi nes an inclusion $A \subset Hom_A(J, J)$.
- It is easy to see that for $\varphi \in Hom_A(J, J)$ the element $\varphi(x)/x \in Q(A)$ is independent of x: for any $a \in J$ we have $\varphi(a) = (1/x) \cdot \varphi(xa) = a \cdot \varphi(x)/x$, since φ is A–linear.
- Hence, $\varphi \mapsto \varphi(x)/x$ defi nes an inclusion $Hom_A(J, J) \subset Q(A)$ mapping $x \cdot Hom_A(J, J)$ into $xJ : J = \{b \in A \mid bJ \subset xJ\}$. The latter map is also surjective, since any $b \in xJ : J$ defi nes, via multiplication with b/x, an element $\varphi \in Hom_A(J, J)$ with $\varphi(x) = b$. Since x is a non–zerodivisor, we obtain the isomorphism $Hom_A(J, J) \cong (1/x) \cdot (xJ : J)$.

proof

- For $a \in A$, let $m_a : J \to J$ denote the multiplication with a. If $m_a = 0$, then $m_a(x) = ax = 0$ and, hence, $a = 0$, since x is a non–zerodivisor. Thus, $a \mapsto m_a$ defi nes an inclusion $A \subset Hom_A(J, J)$.
- It is easy to see that for $\varphi \in Hom_A(J, J)$ the element $\varphi(x)/x \in Q(A)$ is independent of x: for any $a \in J$ we have $\varphi(a) = (1/x) \cdot \varphi(xa) = a \cdot \varphi(x)/x$, since φ is A–linear.
- Hence, $\varphi \mapsto \varphi(x)/x$ defi nes an inclusion $Hom_A(J, J) \subset Q(A)$ mapping $x \cdot Hom_A(J, J)$ into $xJ : J = \{b \in A \mid bJ \subset xJ\}$. The latter map is also surjective, since any $b \in xJ : J$ defi nes, via multiplication with b/x, an element $\varphi \in Hom_A(J, J)$ with $\varphi(x) = b$. Since x is a non–zerodivisor, we obtain the isomorphism $Hom_A(J, J) \cong (1/x) \cdot (xJ : J)$.
- It follows that any $b \in xJ : J$ satisfi es an integral relation $b^p + a_1 b^{p-1} + \cdots + a_0 = 0$ with $a_i \in \langle x^i \rangle$. Hence, b/x is integral over A, showing $(1/x) \cdot (xJ : J) \subset \overline{A}$.

non-normal locus

- The non–normal locus of A is defined as

$$N(A) = \{P \in SpecA \mid A_P \text{ is not normal}\}\,.$$

Let $C = Ann_A(\overline{A}/A) = \{a \in A \mid a\overline{A} \subset A\}$ be the conductor of A in $\overline{A}$. Then

$$N(A) = V(C) = \{P \in SpecA \mid P \supset C\}\,.$$

non-normal locus

- The non–normal locus of A is defined as

$$N(A) = \{P \in SpecA \mid A_P \text{ is not normal}\}\,.$$

Let $C = Ann_A(\overline{A}/A) = \{a \in A \mid a\overline{A} \subset A\}$ be the conductor of A in $\overline{A}$. Then

$$N(A) = V(C) = \{P \in SpecA \mid P \supset C\}\,.$$

- In particular, $N(A)$ is closed in $SpecA$.

Let $J \subset A$ be an ideal containing a non–zerodivisor of A.

- There are natural inclusions of A–modules

$$Hom_A(J,J) \subset Hom_A(J,A) \cap \overline{A} \subset Hom_A(J,\sqrt{J})\,.$$

Let $J \subset A$ be an ideal containing a non–zerodivisor of A.

- There are natural inclusions of A–modules

$$Hom_A(J, J) \subset Hom_A(J, A) \cap \overline{A} \subset Hom_A(J, \sqrt{J}).$$

- If $N(A) \subset V(J)$ then $J^d\overline{A} \subset A$ for some d.

- The embedding of $Hom_A(J, A)$ in $Q(A)$ is given by $\varphi \mapsto \varphi(x)/x$, where x is a non–zerodivisor of J. With this identifi cation we obtain

$$Hom_A(J, A) = A :_{Q(A)} J = \{h \in Q(A) \mid hJ \subset A\}$$

and $Hom_A(J, J)$, respectively $Hom_A(J, \sqrt{J})$, is identifi ed with those $h \in Q(A)$ such that $hJ \subset J$, respectively $hJ \subset \sqrt{J}$. Then the fi rst inclusion follows.
For the second inclusion let $h \in \overline{A}$ satisfy $hJ \subset A$. Consider an integral relation $h^n + a_1 h^{n-1} + \cdots + a_n = 0$ with $a_i \in A$. Let $g \in J$ and multiply the above equation with g^n. Then

$$(hg)^n + ga_1(hg)^{n-1} + \cdots + g^n a_n = 0\,.$$

Since $g \in J$, $hg \in A$ and, therefore, $(hg)^n \in J$ and $hg \in \sqrt{J}$. This shows the second inclusion.

- The embedding of $Hom_A(J, A)$ in $Q(A)$ is given by $\varphi \mapsto \varphi(x)/x$, where x is a non–zerodivisor of J. With this identifi cation we obtain

$$Hom_A(J, A) = A :_{Q(A)} J = \{h \in Q(A) \mid hJ \subset A\}$$

  and $Hom_A(J, J)$, respectively $Hom_A(J, \sqrt{J})$, is identifi ed with those $h \in Q(A)$ such that $hJ \subset J$, respectively $hJ \subset \sqrt{J}$. Then the fi rst inclusion follows.
  For the second inclusion let $h \in \overline{A}$ satisfy $hJ \subset A$. Consider an integral relation $h^n + a_1 h^{n-1} + \cdots + a_n = 0$ with $a_i \in A$. Let $g \in J$ and multiply the above equation with g^n. Then

$$(hg)^n + ga_1(hg)^{n-1} + \cdots + g^n a_n = 0\,.$$

  Since $g \in J$, $hg \in A$ and, therefore, $(hg)^n \in J$ and $hg \in \sqrt{J}$. This shows the second inclusion.
- By assumption, we have $V(C) \subset V(J)$ and, hence, $J \subset \sqrt{C}$, that is, $J^d \subset C$ for some d which implies the claim.

Criterion for Normality

Let A be a Noetherian reduced ring and $J \subset A$ an ideal satisfying

- J contains a non–zerodivisor of A,
- J is a radical ideal,
- $N(A) \subset V(J)$.

Criterion for Normality

Let A be a Noetherian reduced ring and $J \subset A$ an ideal satisfying

- J contains a non–zerodivisor of A,
- J is a radical ideal,
- $N(A) \subset V(J)$.
- Then A is normal if and only if $A = Hom_A(J, J)$.

proof

- If $A = \overline{A}$ then $Hom_A(J, J) = A$. To see the converse, we choose $d \geq 0$ minimal such that $J^d\overline{A} \subset A$. If $d > 0$ then there exists some $a \in J^{d-1}$ and $h \in \overline{A}$ such that $ah \notin A$.

proof

- If $A = \overline{A}$ then $Hom_A(J, J) = A$. To see the converse, we choose $d \geq 0$ minimal such that $J^d\overline{A} \subset A$. If $d > 0$ then there exists some $a \in J^{d-1}$ and $h \in \overline{A}$ such that $ah \notin A$.
- But $ah \in \overline{A}$ and $ah \cdot J \subset hJ^d \subset A$, that is, $ah \in Hom_A(J, A) \cap \overline{A}$, which is equal to $Hom_A(J, J)$, since $J = \sqrt{J}$.

proof

- If $A = \overline{A}$ then $Hom_A(J, J) = A$. To see the converse, we choose $d \geq 0$ minimal such that $J^d\overline{A} \subset A$. If $d > 0$ then there exists some $a \in J^{d-1}$ and $h \in \overline{A}$ such that $ah \notin A$.
- But $ah \in \overline{A}$ and $ah \cdot J \subset hJ^d \subset A$, that is, $ah \in Hom_A(J, A) \cap \overline{A}$, which is equal to $Hom_A(J, J)$, since $J = \sqrt{J}$.
- By assumption $Hom_A(J, J) = A$ and, hence, $ah \in A$, which is a contradiction. We conclude that $d = 0$ and $A = \overline{A}$.

Let A be a reduced Noetherian ring, let $J \subset A$ be an ideal and $x \in J$ a non–zerodivisor. Then

- $A = Hom_A(J, J)$ if and only if $xJ : J = \langle x \rangle$.

Let A be a reduced Noetherian ring, let $J \subset A$ be an ideal and $x \in J$ a non–zerodivisor. Then

- $A = Hom_A(J, J)$ if and only if $xJ : J = \langle x \rangle$.
- Moreover, let $\{u_0 = x, u_1, \dots, u_s\}$ be a system of generators for the A–module $xJ : J$. Then we can write
  - $u_i \cdot u_j = \sum_{k=0}^{s} x\xi_k^{ij} u_k$ with suitable $\xi_k^{ij} \in A$, $1 \leq i \leq j \leq s$.

Let A be a reduced Noetherian ring, let $J \subset A$ be an ideal and $x \in J$ a non–zerodivisor. Then

- $A = Hom_A(J, J)$ if and only if $xJ : J = \langle x \rangle$.
- Moreover, let $\{u_0 = x, u_1, \ldots, u_s\}$ be a system of generators for the A–module $xJ : J$. Then we can write
  - $u_i \cdot u_j = \sum_{k=0}^{s} x\xi_k^{ij} u_k$ with suitable $\xi_k^{ij} \in A$, $1 \le i \le j \le s$.
- Let $(\eta_0^{(k)}, \ldots, \eta_s^{(k)}) \in A^{s+1}$, $k = 1, \ldots, m$, generate $syz(u_0, \ldots, u_s)$, and let $I \subset A[t_1, \ldots, t_s]$ be the ideal ($t_0 := 1$)

$$I := \left\langle \left\{ t_i t_j - \sum_{k=0}^{s} \xi_k^{ij} t_k \;\middle|\; 1 \le i \le j \le s \right\},\ \left\{ \sum_{\nu=0}^{s} \eta_\nu^{(k)} t_\nu \;\middle|\; 1 \le k \le m \right\} \right\rangle ,$$

  - $t_i \mapsto u_i / x$, $i = 1, \ldots, s$, defines an isomorphism

$$A[t_1, \ldots, t_s]/I \xrightarrow{\cong} Hom_A(J, J) \cong \frac{1}{x} \cdot (xJ : J)\,.$$

Example

- Let $A := K[x,y]/\langle x^2 - y^3\rangle$ and $J := \langle x, y\rangle \subset A$.
- Then $x \in J$ is a non–zerodivisor in A with $xJ : J = x\langle x,y\rangle : \langle x,y\rangle = \langle x, y^2\rangle$, therefore,
- $Hom_A(J,J) = \langle 1,\, y^2/x\rangle$.
- Setting $u_0 := x$, $u_1 := y^2$, we obtain $u_1^2 = y^4 = x^2 y$, that is, $\xi_0^{11} = y$. Hence, we obtain an isomorphism

Example

- Let $A := K[x,y]/\langle x^2 - y^3\rangle$ and $J := \langle x, y\rangle \subset A$.
- Then $x \in J$ is a non–zerodivisor in A with $xJ : J = x\langle x, y\rangle : \langle x, y\rangle = \langle x, y^2\rangle$, therefore,
- $Hom_A(J,J) = \langle 1,\, y^2/x\rangle$.
- Setting $u_0 := x$, $u_1 := y^2$, we obtain $u_1^2 = y^4 = x^2 y$, that is, $\xi_0^{11} = y$. Hence, we obtain an isomorphism
- $$A[t]/\langle t^2 - y,\, xt - y^2,\, yt - x\rangle \xrightarrow{\cong} Hom_A(J,J)\,.$$

  of A–algebras. Note that $A[t]/\langle t^2 - y,\, xt - y^2,\, yt - x\rangle \simeq K[t]$.

normalization(I)

TECHNISCHE UNIVERSITÄT KAISERSLAUTERN

- Input: $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$ a prime ideal, $x = (x_1, \ldots, x_n)$.
- Output: A polynomial ring $K[t]$, $t = (t_1, \ldots, t_N)$, a prime ideal $P \subset K[t]$ and $\pi : K[x] \to K[t]$ such that the induced map $\pi : K[x]/I \to K[t]/P$ is the normalization of $K[x]/I$.
  - if $I = \langle 0 \rangle$ then return $(K[x], \langle 0 \rangle, id_{K[x]})$;
  - compute $r := \dim(I)$;
  - if we know that the singular locus of I is $V(x_1, \ldots, x_n)$

    $J := \langle x_1, \ldots, x_n \rangle$;

    else

    compute $J :=$ the ideal of the $(n - r)$–minors of the Jacobian matrix I;
  - $J :=$ RADICAL$(I + J)$;
  - choose $a \in J \setminus \{0\}$;
  - if $aJ : J = \langle a \rangle$ return $(K[x], I, id_{K[x]})$;

normalization(I)

- compute a generating system $u_0 = a, u_1, \ldots, u_s$ for $aJ : J$;
- compute a generating system $\{(\eta_0^{(1)}, \ldots, \eta_s^{(1)}), \ldots, (\eta_0^{(m)}, \ldots, \eta_s^{(m)})\}$ for the module of syzygies $syz(u_0, \ldots, u_s) \subset (K[x]/I)^{s+1}$;
- compute ξ_k^{ij} such that $u_i \cdot u_j = \sum_{k=0}^{s} a \cdot \xi_k^{ij} u_k$, $i, j = 1, \ldots s$;
- change ring to $K[x_1, \ldots, x_n, t_1, \ldots, t_s]$, and set (with $t_0 := 1$) $I_1 := \left\langle \{t_i t_j - \sum_{k=0}^{s} \xi_k^{ij} t_k\}_{0 \le i \le j \le s}, \{\sum_{\nu=0}^{s} \eta_\nu^{(k)} t_\nu\}_{1 \le k \le m} \right\rangle + IK[x, t]$;
- return NORMALIZATION(I_1).

non-normal locus

The ideal $Ann_A\big(Hom_A(J,J)/A\big) \subset A$ defines the non–normal locus. Moreover,

$$Ann_A\big(Hom_A(J,J)/A\big) = \langle x \rangle : (xJ : J)$$

for any non–zerodivisor $x \in J$.

non–normalLocus(I)

- Input: $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$ a prime ideal, $x = (x_1, \ldots, x_n)$.
- Output: An ideal $N \subset K[x]$, defining the non–normal locus in $V(I)$.
  - If $I = \langle 0 \rangle$ then return $(K[x])$;
  - compute $r = \dim(I)$;
  - compute J the ideal of the $(n-r)$–minors of the Jacobian matrix of I;
  - $J =$ RADICAL $(I + J)$;
  - choose $a \in J \setminus \{0\}$;
  - return $\big(\langle a \rangle : (aJ : J)\big)$.