

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

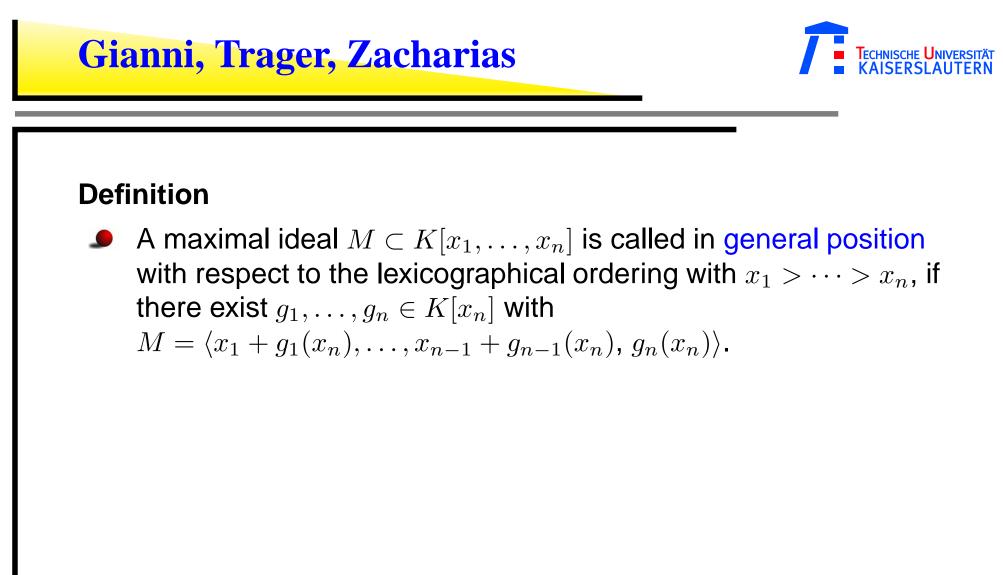


- Gianni, P.; Trager, B.; Zacharias, G.: Gröbner Bases and Primary Decomposition of Polynomial Ideals. J. Symb. Comp. 6, 149–167 (1988).
- Eisenbud, D.; Huneke, C.; Vasconcelos, W.: Direct Methods for Primary Decomposition. Invent. Math. 110, 207–235 (1992).
- Shimoyama, T.; Yokoyama, K.: Localization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



- 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





Definition

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



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 $x_1 > \cdots > x_n$.



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

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

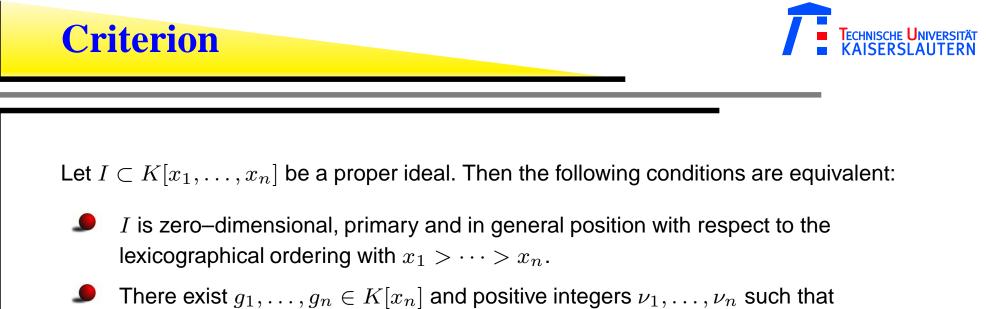


Let $I \subset K[x_1, \ldots, x_n]$ be a zero-dimensional ideal. Let $\langle g \rangle = I \cap K[x_n]$, $g = g_1^{\nu_1} \ldots g_s^{\nu_s}$, g_i monic and prime and $g_i \neq g_j$ for $i \neq j$. Then

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

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*.

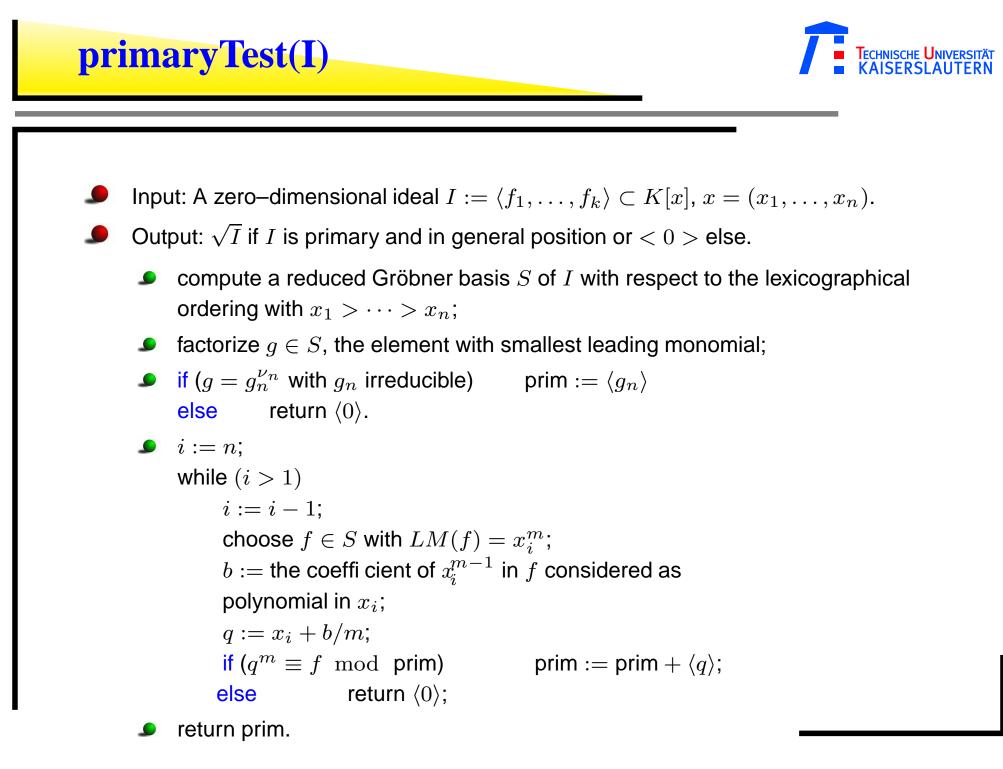


- There exist $g_1, \ldots, g_n \in \mathbb{R}[x_n]$ and positive integers ν_1, \ldots, ν_n
 - $I \cap K[x_n] = \langle g_n^{\nu_n} \rangle, g_n \text{ irreducible;}$
 - for each j < n, I contains the element $(x_j + g_j)^{\nu_j}$.



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 $u_1, \ldots,
 u_n$ such that
 - $I \cap K[x_n] = \langle g_n^{\nu_n} \rangle, g_n \text{ irreducible;}$
 - for each j < n, I contains the element $(x_j + g_j)^{\nu_j}$.
- 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 ν_1, \ldots, ν_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 $j = 1, \dots, n-1$.



EXERCIPENDED
Conserve Set
$$P_i^{(1)}$$

Conserve Set $P_i^{(1)}$
Conserve Set

Primary Decomposition - p.



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

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

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

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



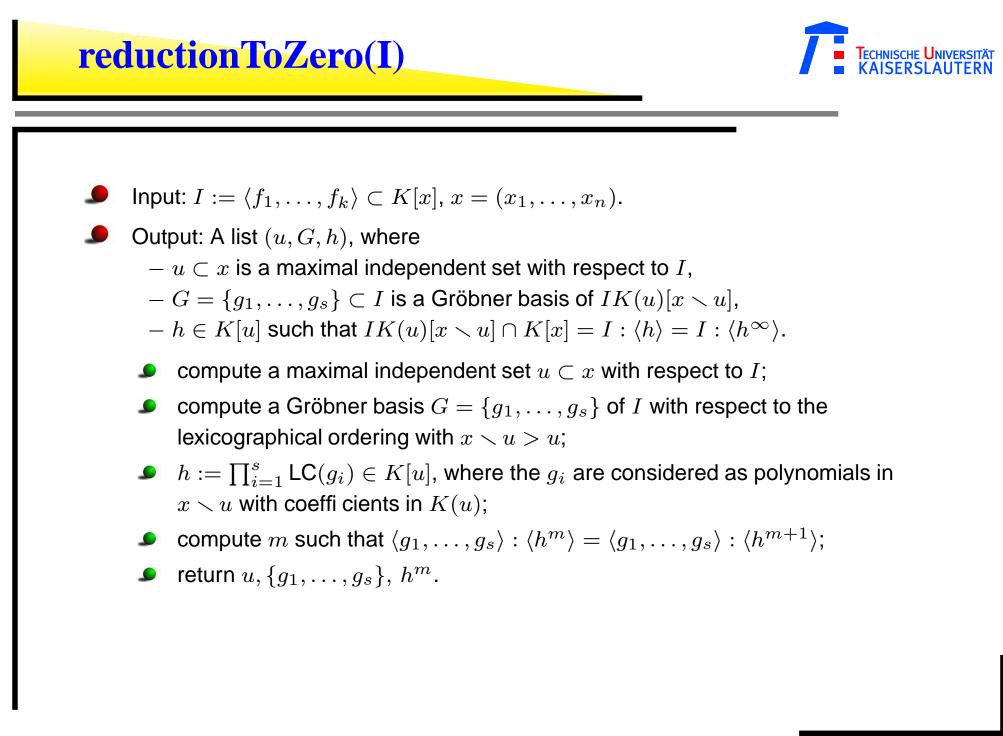
Let $I \subset K[x]$ be an ideal and $u \subset x = \{x_1, \dots, x_n\}$ be a maximal independent set of variables with respect to *I*. ($I \cap K[u] = \{0\}$ and #(u) = dim(K[x]/I))

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

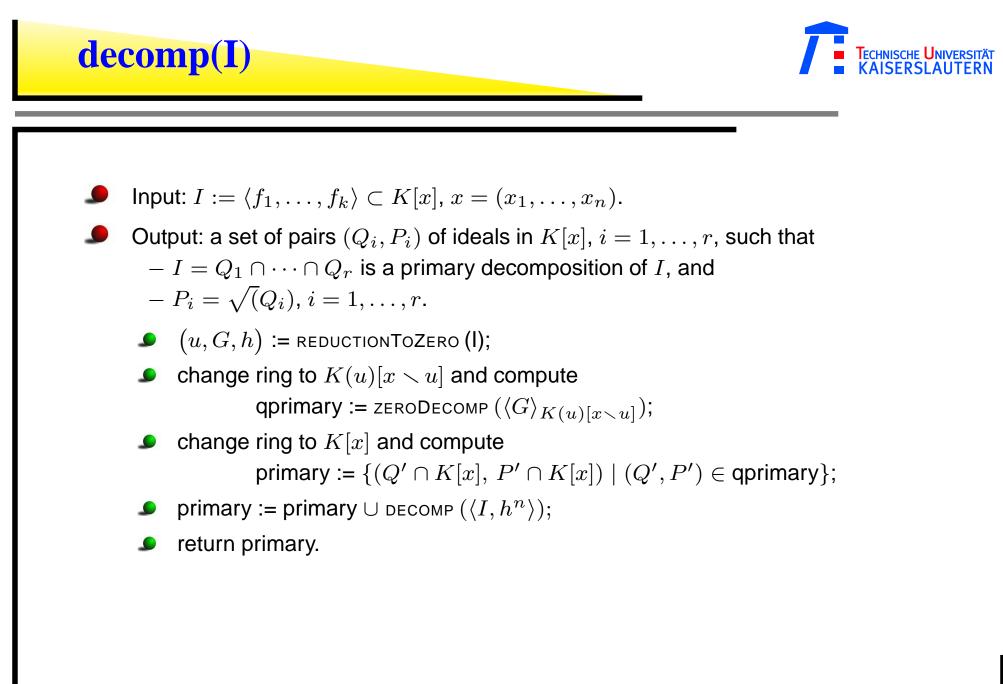
$$IK(u)[x \smallsetminus u] \cap K[x] = I : \langle h^{\infty} \rangle,$$

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

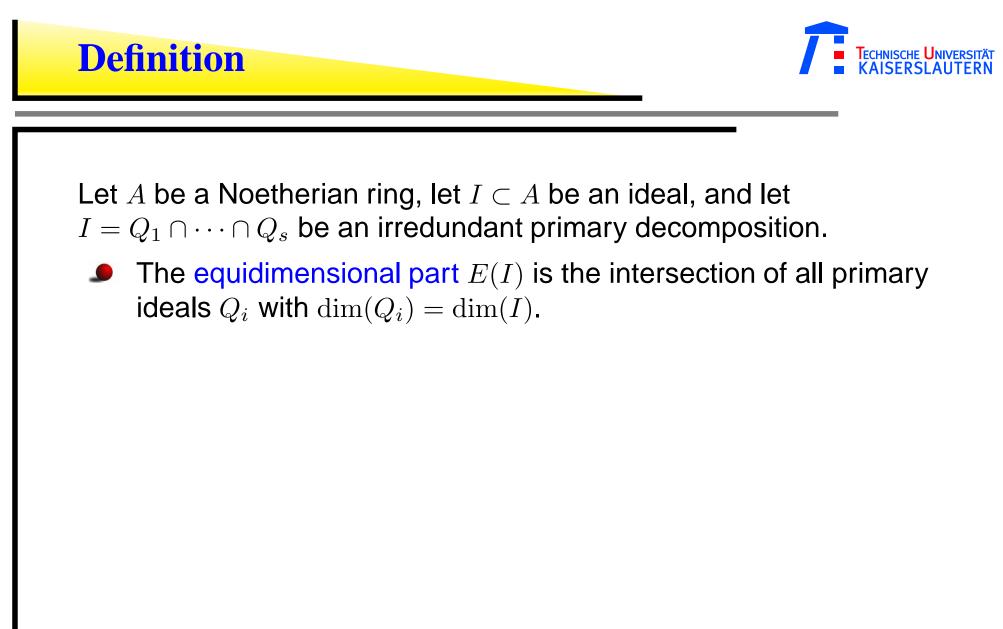
■ Let $IK(u)[x \setminus u] = Q_1 \cap \cdots \cap Q_s$ be an irredundant primary decomposition, then also $IK(u)[x \setminus u] \cap K[x] = (Q_1 \cap K[x]) \cap \cdots \cap (Q_s \cap K[x])$ is an irredundant primary decomposition.

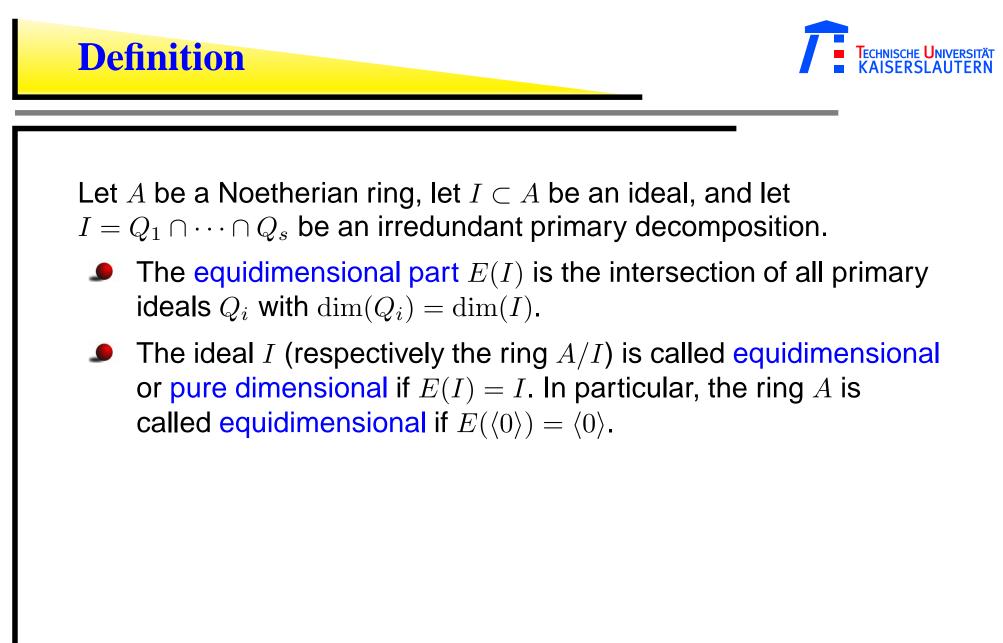


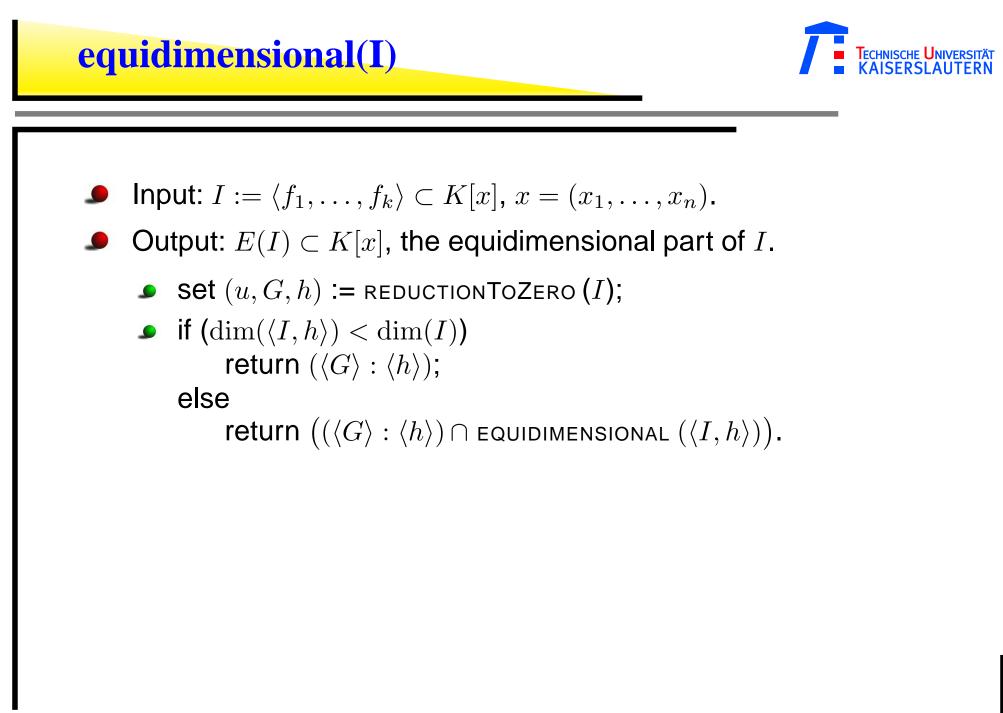
Primary Decomposition – p. 1



Primary Decomposition - p. 1



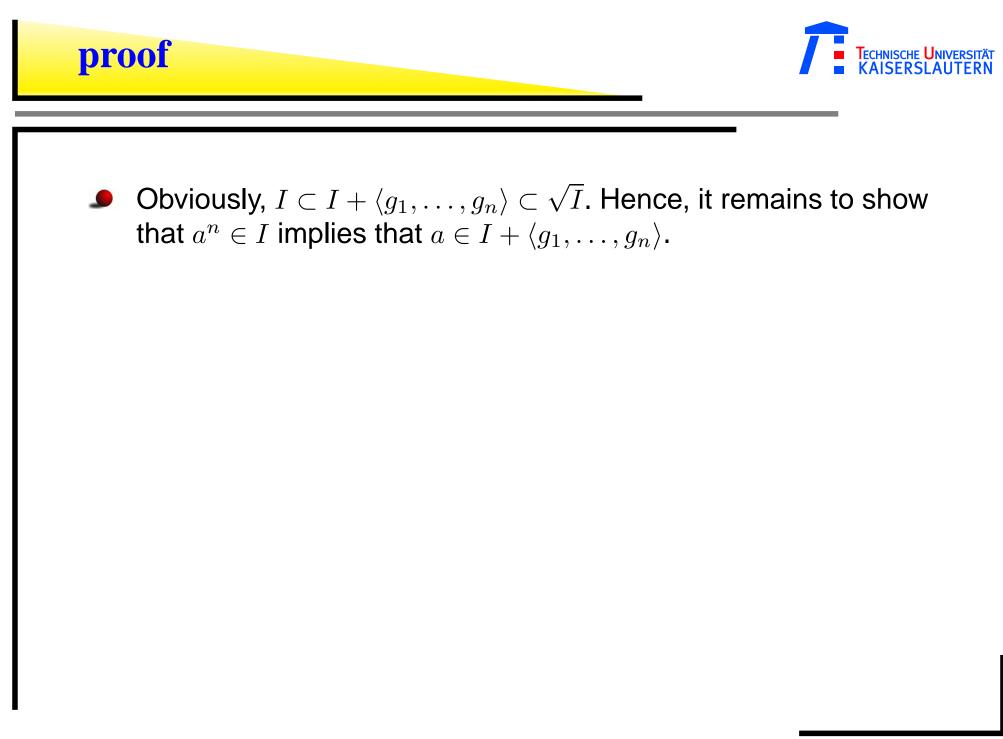


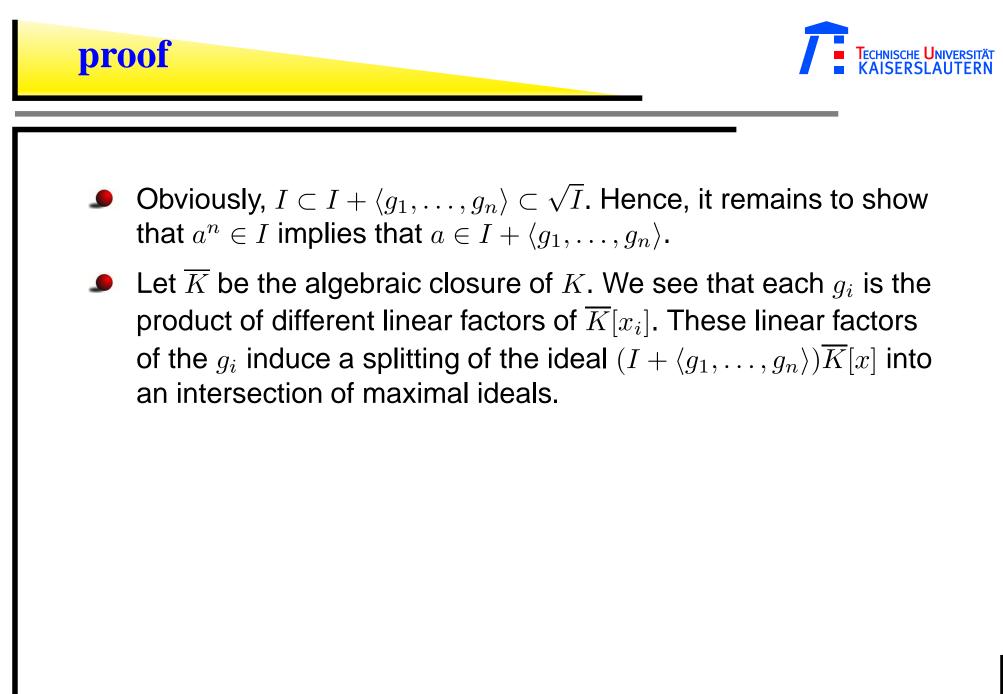


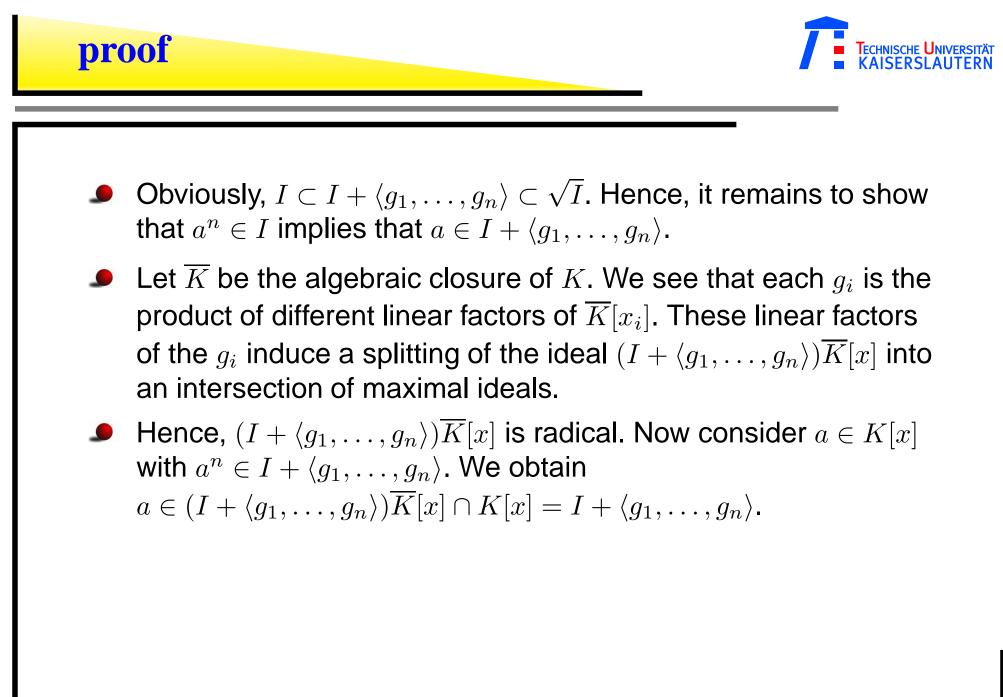
Primary Decomposition - p. 7

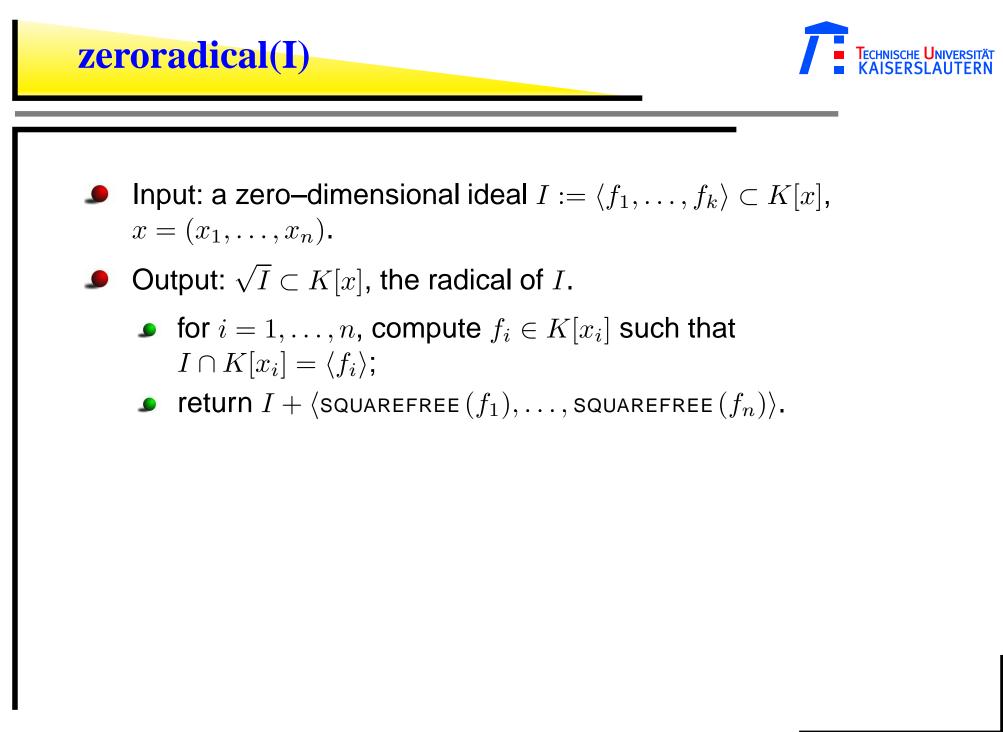


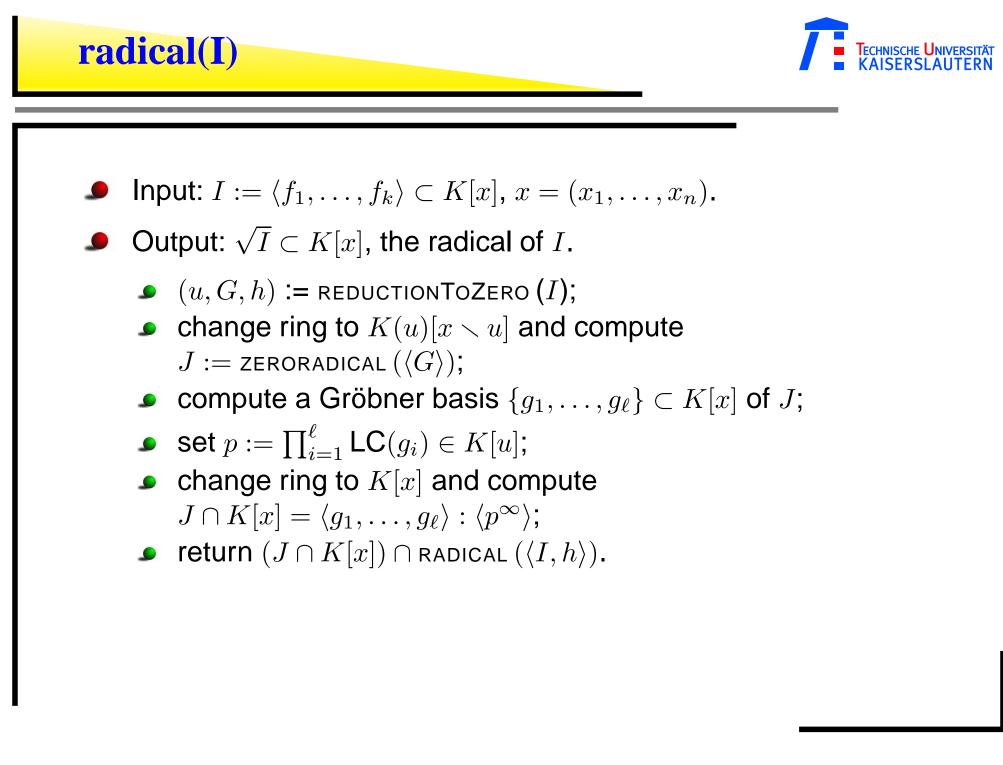
Let $I \subset K[x_1, \ldots, x_n]$ be a zero-dimensional ideal and $I \cap K[x_i] = \langle f_i \rangle$ for $i = 1, \ldots, n$. Moreover, let g_i be the squarefree part of f_i , then $\sqrt{I} = I + \langle g_1, \ldots, g_n \rangle$.

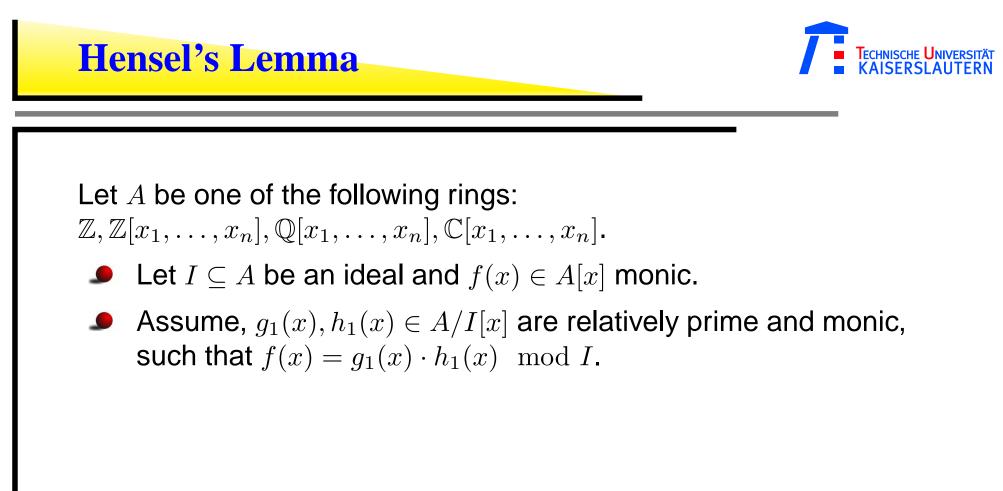


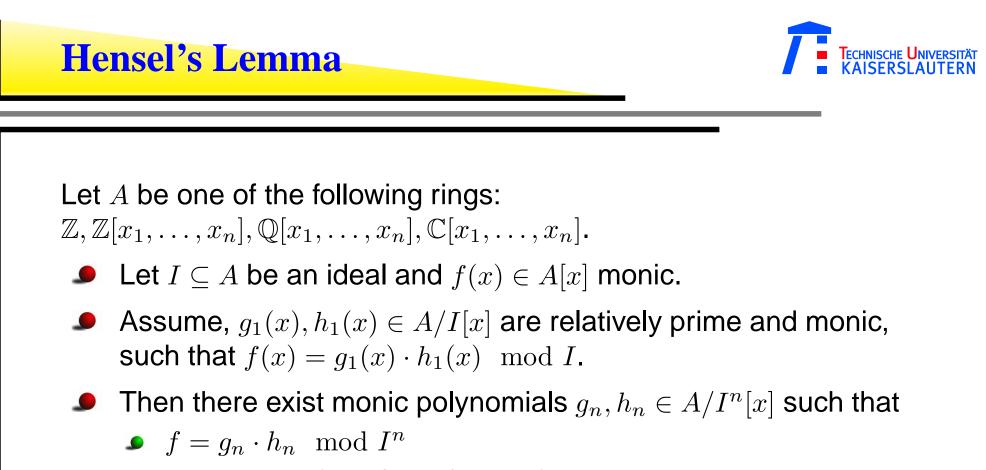


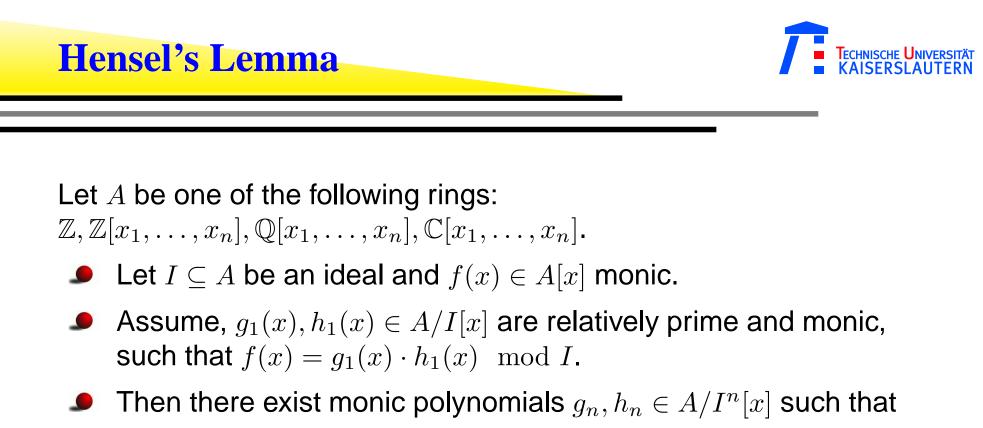












•
$$f = g_n \cdot h_n \mod I^n$$

Furthermore, there exist unique polynomials $\widehat{g}, \widehat{h} \in \widehat{A}_I[X]$ such that

•
$$f = \widehat{g}\widehat{h}$$

• $\widehat{g} = g_1 \mod I$, $\widehat{h} = h_1 \mod I$



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

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



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

•
$$\overline{f}^{(2)} = g_1 \cdot h_1$$

Hensel's lemma in $A[x_1] (A = \mathbb{C}[x_2, x_3], I = \langle x_3 - a_3 \rangle)$

•
$$\bar{f}^{(3)} = g_{d_{3+1}} h_{d_{3+1}} \mod \langle x_3 - a_3 \rangle^{d_3 + 1}$$

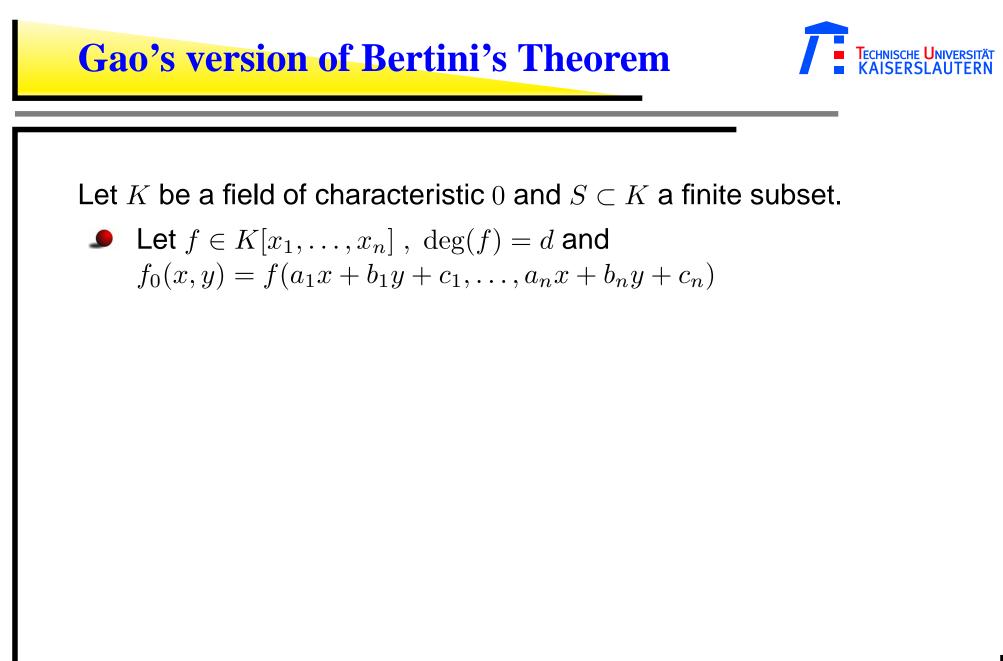
• if
$$f = f_1 \cdot f_2$$
 and
 $f_1(x_1, x_2, a_3, \dots, a_n) = g_1, f_2(x_1, x_2, a_3, \dots, a_n) = h_1$
then

$$f_1(x_1, x_2, x_3, a_4 \dots a_n) = g_{d_{3+1}}(x_1, x_2, x_3)$$

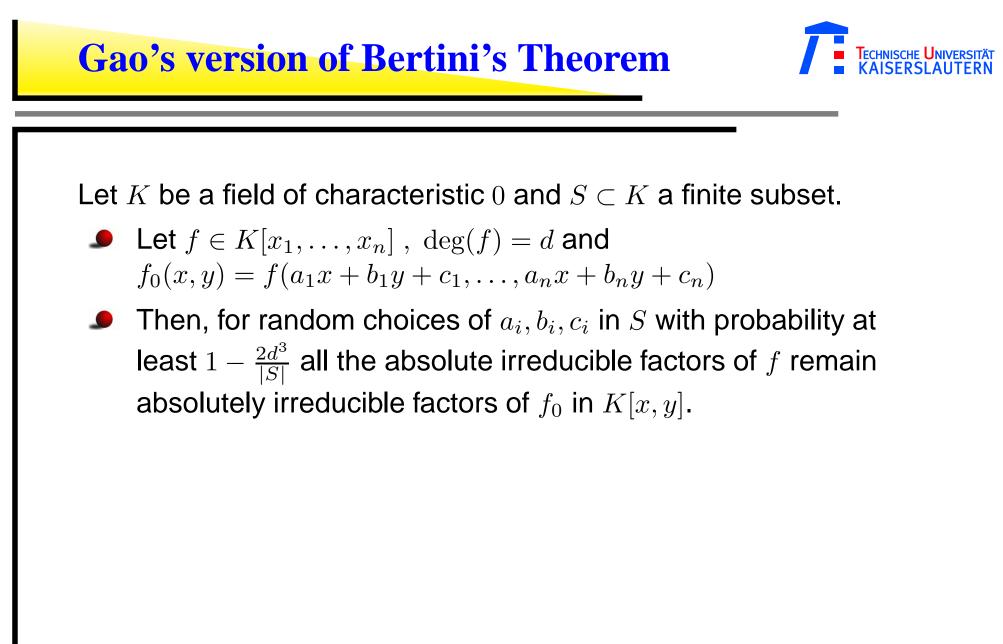
$$f_2(x_1, x_2, x_3, a_4 \dots a_n) = h_{d_{3+1}}(x_1, x_2, x_3)$$

by unicity of Hensel's lemma.

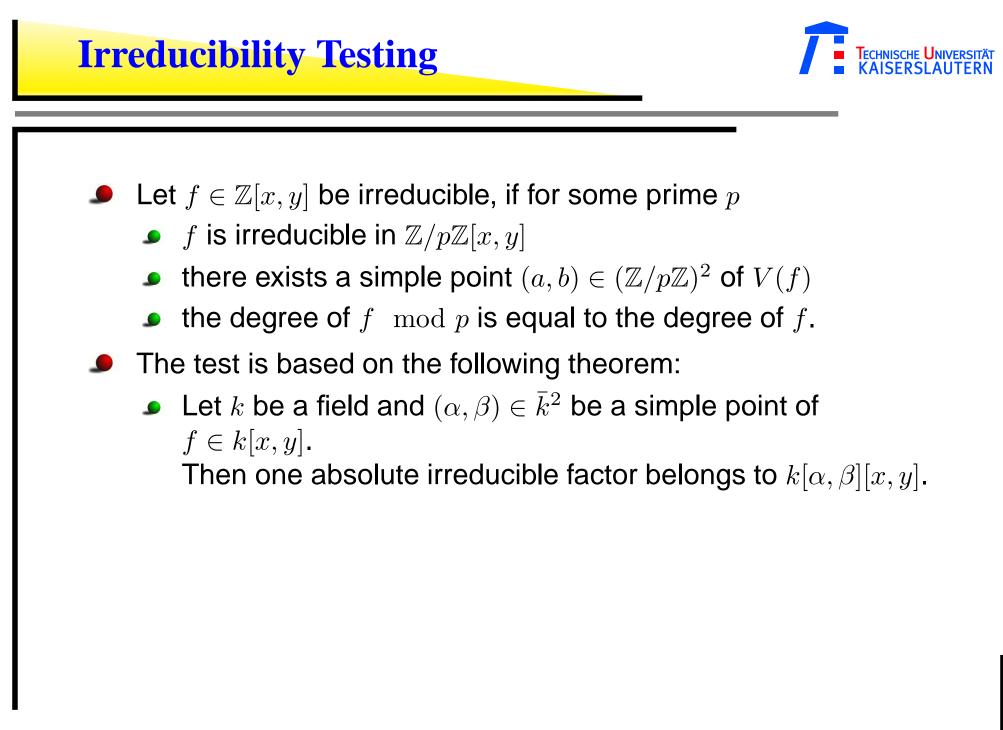
Restart with the next variable.

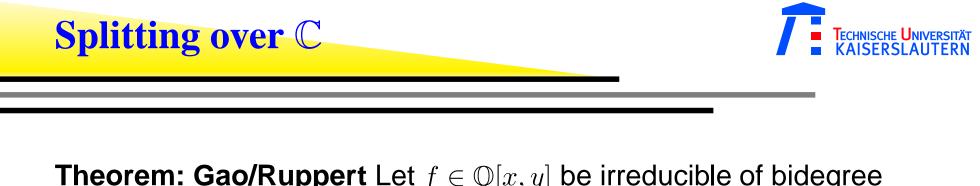


Primary Decomposition - p. 2



| Irreducibility Testing | TECHNISCHE UNIVERSITÄT KAISERSLAUTERN |
|--|--|
| Let f ∈ Z[x, y] be irreducible, if for some prime p f is irreducible in Z/pZ[x, y] there exists a simple point (a, b) ∈ (Z/pZ)² of V(f) the degree of f mod p is equal to the degree of f. | |
| | |

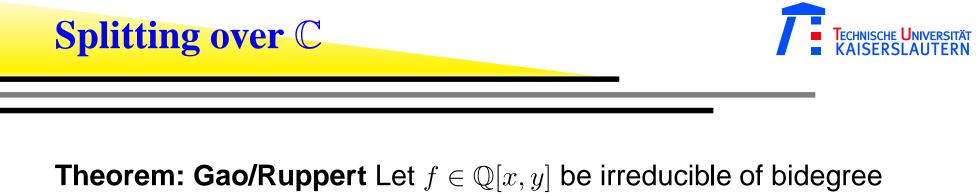




Theorem: Gao/Ruppert Let $f \in \mathbb{Q}[x, y]$ be irreducible of bidegree (m, n).

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

The vector space G has the following properties



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

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

The vector space G has the following properties

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



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

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

The vector space G has the following properties

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

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

Let $G = \{g \in \mathbb{Q}[x, y] | (m - 1, n) \ge deg(g), \exists h \in \mathbb{Q}[x, y], \frac{\partial(g/f)}{\partial y} = \frac{\partial(h/f)}{\partial x} \}.$ The vector space G has the following properties

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

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

Let $G = \{g \in \mathbb{Q}[x, y] | (m - 1, n) \ge deg(g), \exists h \in \mathbb{Q}[x, y], \frac{\partial(g/f)}{\partial y} = \frac{\partial(h/f)}{\partial x} \}.$ The vector space G has the following properties

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

$$gG \subset \frac{\partial f}{\partial x}G \text{ mod f for all } g \in G.$$

• 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 $\mathbb{Q}[t]$.



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



•
$$f = x^2 + y^2$$

• $G = \langle x, y \rangle_{\mathbb{Q}}$

$$(a_{i,j}) = \left(\begin{array}{cc} 0 & 1/2\\ -1/2 & 0 \end{array}\right)$$



•
$$f = x^2 + y^2$$

• $G = \langle x, y \rangle_{\mathbb{Q}}$

$$(a_{i,j}) = \left(\begin{array}{cc} 0 & 1/2\\ -1/2 & 0 \end{array}\right)$$

•
$$\chi(t) = t^2 + 1/4$$



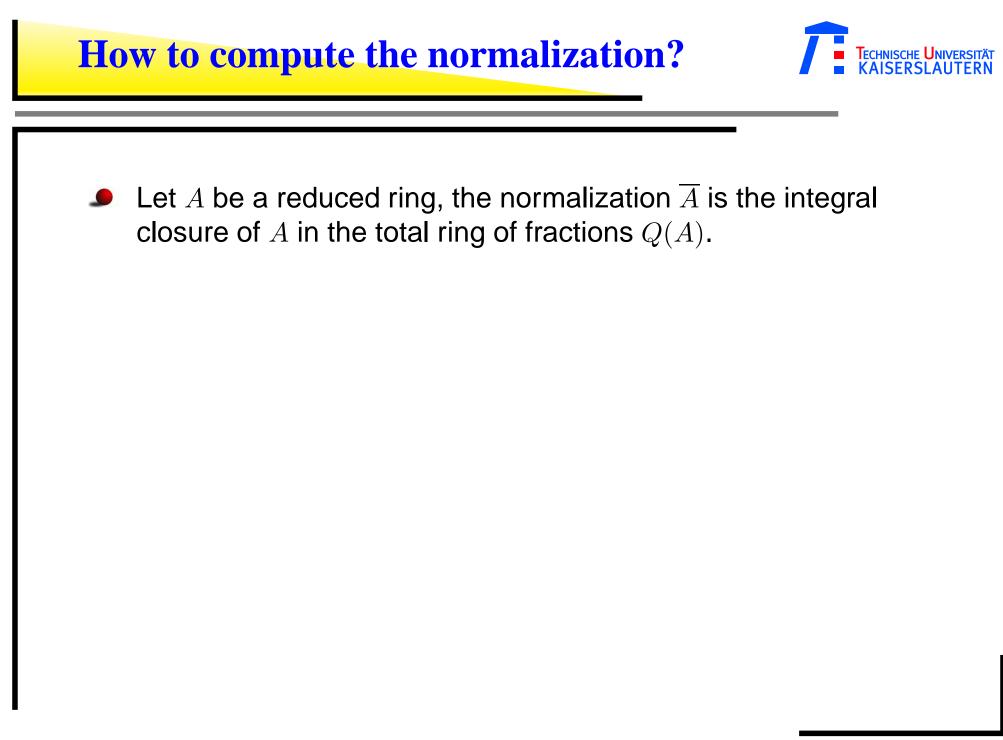
$$f = x^2 + y^2$$

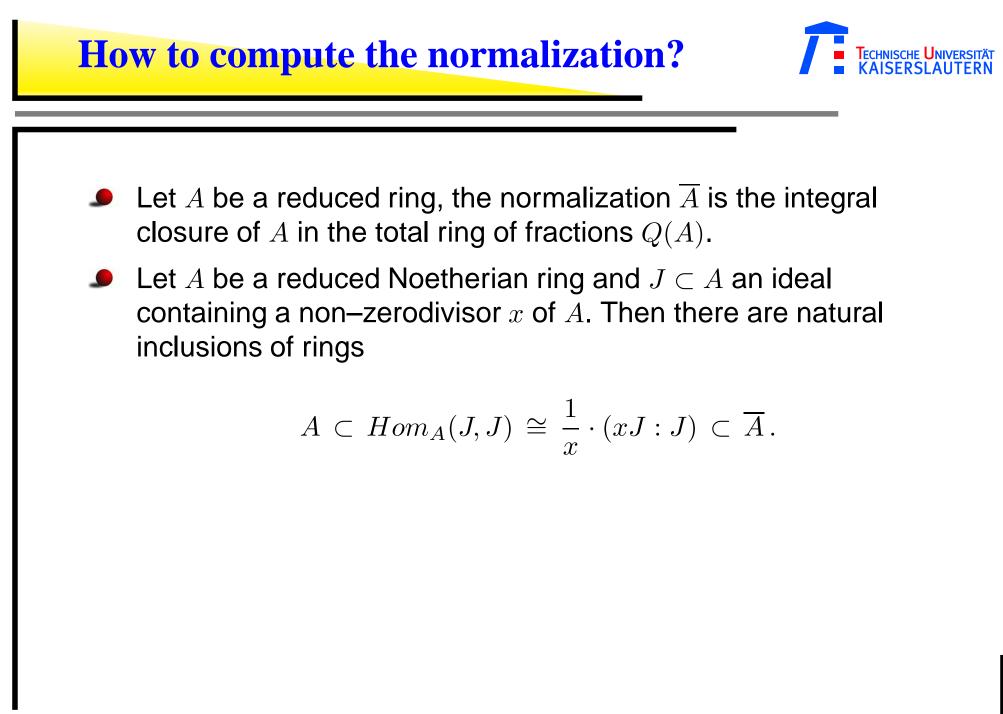
$$G = \langle x, y \rangle_{\mathbb{Q}}$$

$$(a_{i,j}) = \left(\begin{array}{cc} 0 & 1/2 \\ -1/2 & 0 \end{array} \right)$$

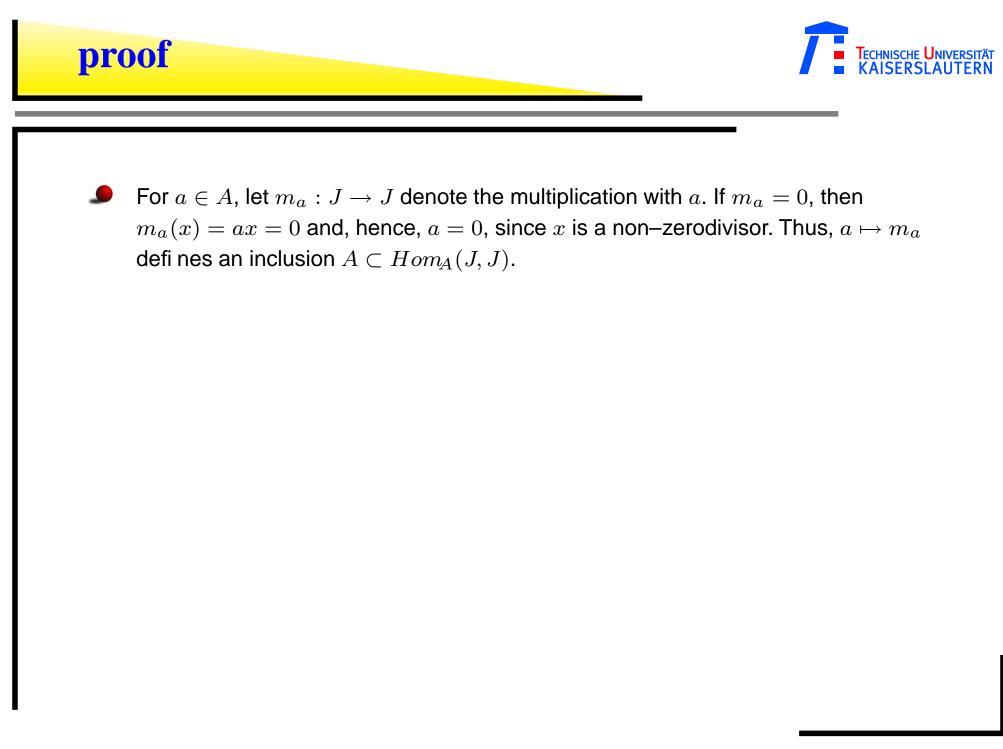
•
$$\chi(t) = t^2 + 1/4$$

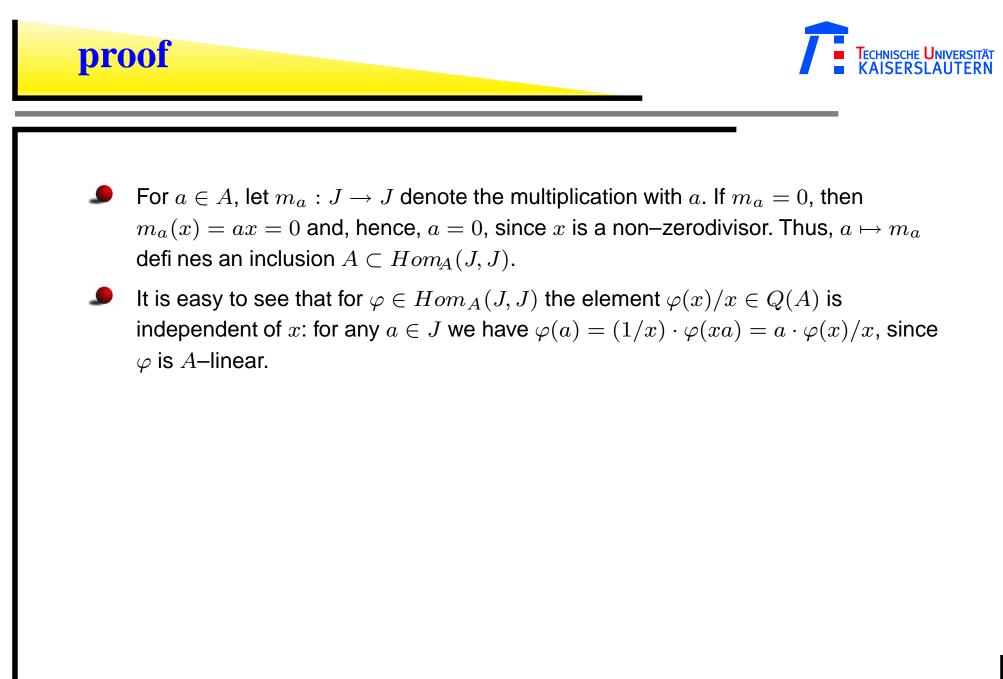
• $gcd(x^2 + y^2, y - \frac{i}{2}2x)gcd(x^2 + y^2, y + \frac{i}{2}2x) = x^2 + y^2$

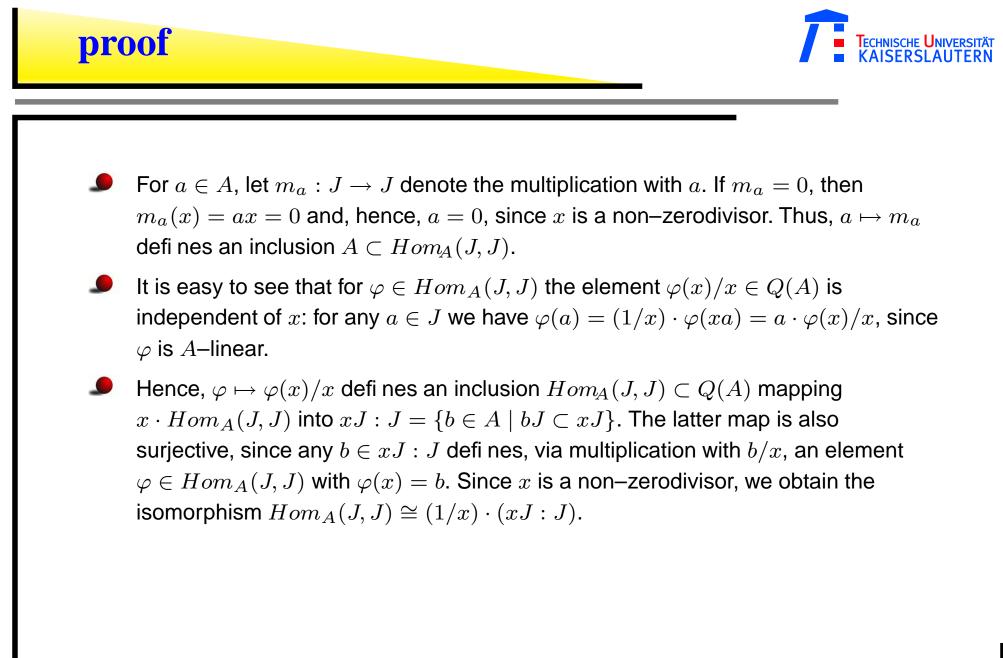




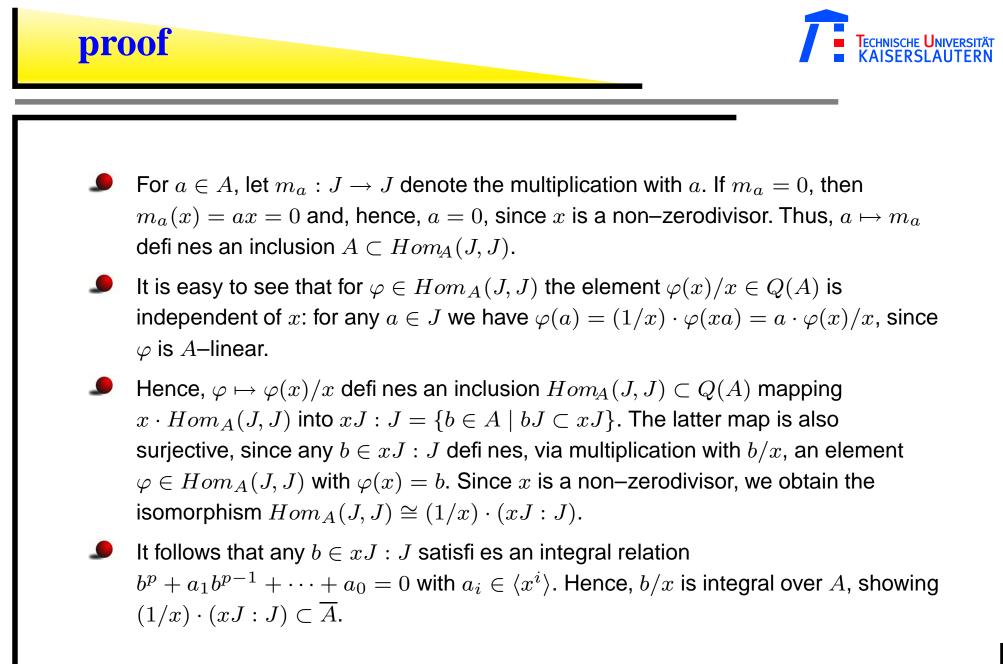
Primary Decomposition – p. 2



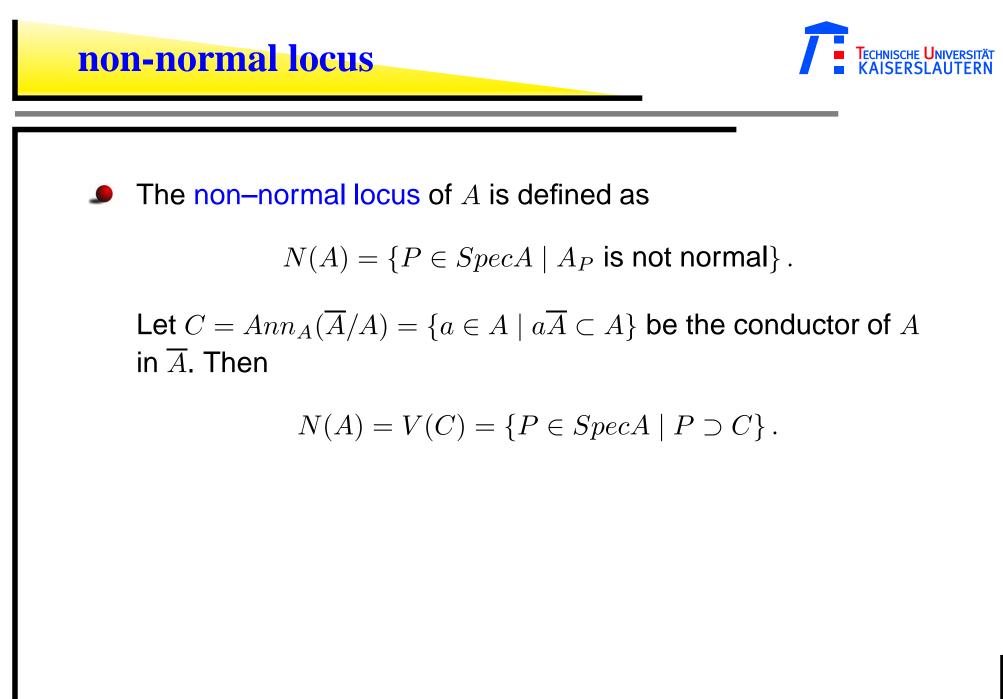




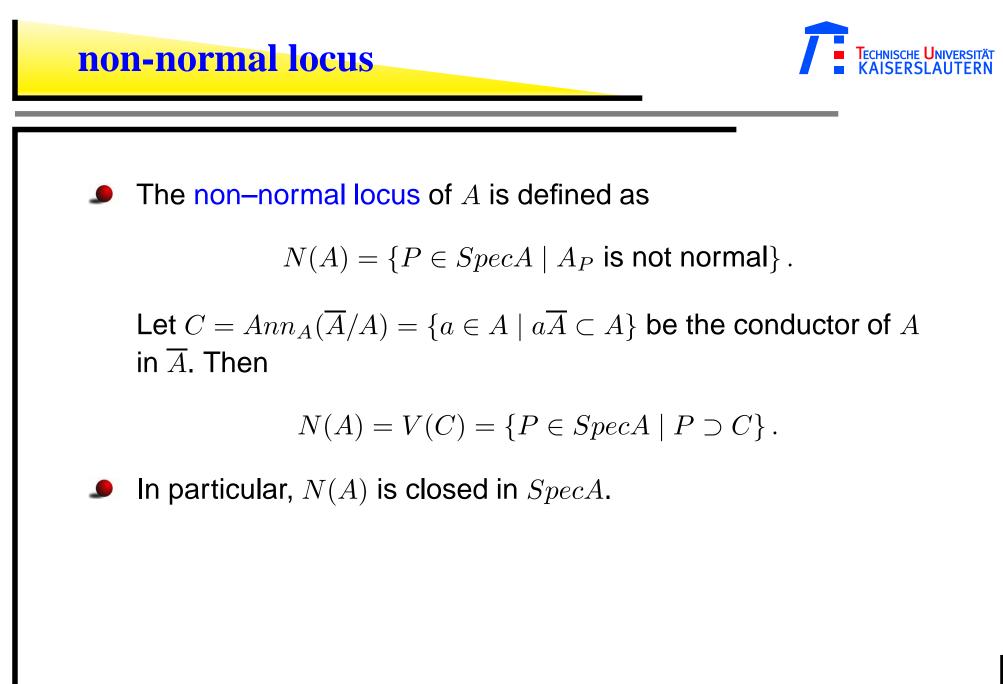
Primary Decomposition - p. 2



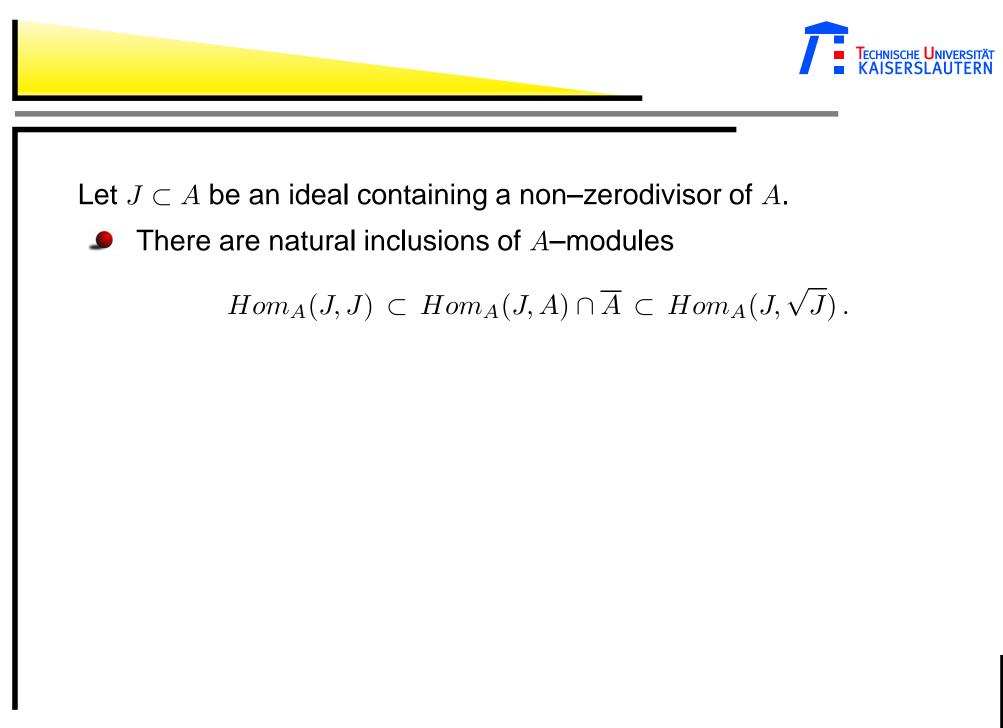
Primary Decomposition - p. 2

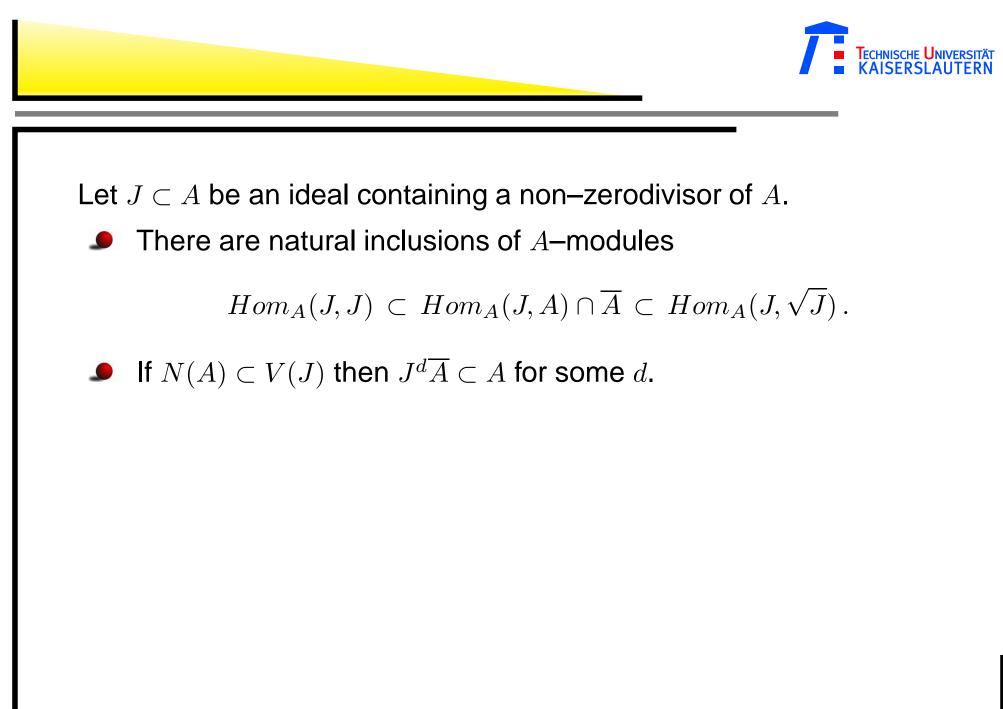


Primary Decomposition – p. 2



Primary Decomposition - p. 2







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 identification 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 identified with those $h \in Q(A)$ such that $hJ \subset J$, respectively $hJ \subset \sqrt{J}$. Then the first inclusion follows. For the second inclusion let $h \in \overline{A}$ satisfy $hJ \subset A$. Consider an integral relation $h^n + a_1h^{n-1} + \cdots + a_n = 0$ with $a_i \in A$. Let $g \in J$ and multiply the above equation with g^n . Then

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

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

Primary Decomposition – p. 2



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 identification we obtain

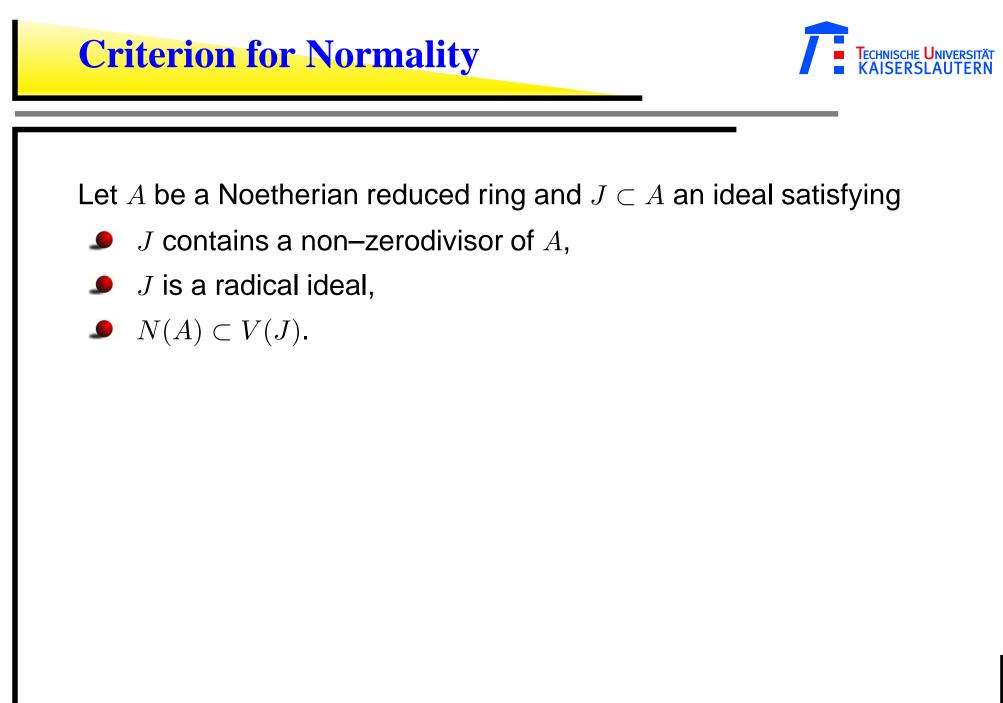
$$Hom_A(J,A) = A :_{Q(A)} J = \{h \in Q(A) \mid hJ \subset A\}$$

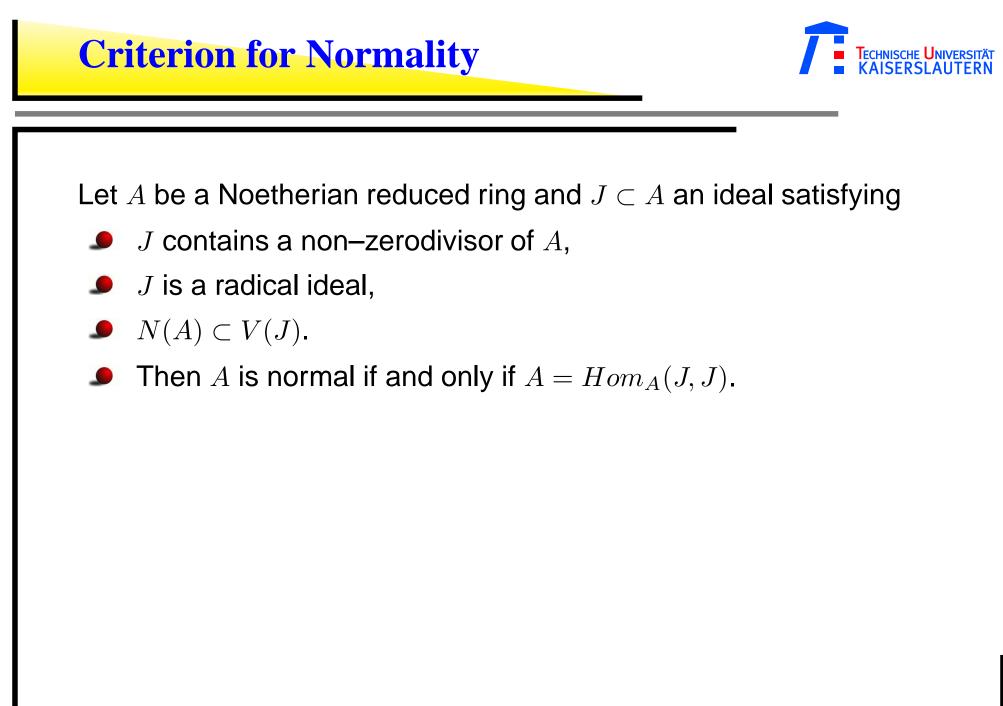
and $Hom_A(J, J)$, respectively $Hom_A(J, \sqrt{J})$, is identified with those $h \in Q(A)$ such that $hJ \subset J$, respectively $hJ \subset \sqrt{J}$. Then the first inclusion follows. For the second inclusion let $h \in \overline{A}$ satisfy $hJ \subset A$. Consider an integral relation $h^n + a_1h^{n-1} + \cdots + a_n = 0$ with $a_i \in A$. Let $g \in J$ and multiply the above equation with g^n . Then

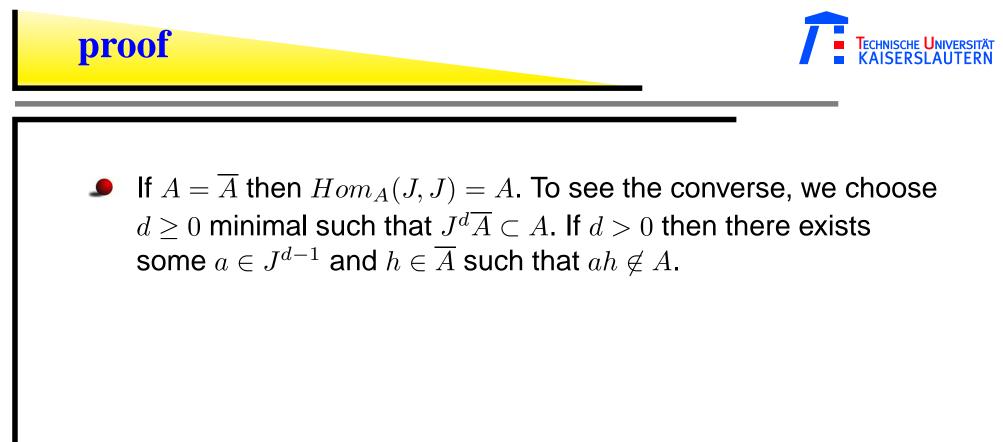
$$(hg)^n + ga_1(hg)^{n-1} + \dots + g^n a_n = 0.$$

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.









- If $A = \overline{A}$ then $Hom_A(J, J) = A$. To see the converse, we choose $d \ge 0$ 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 $J = \sqrt{J}$.



- If $A = \overline{A}$ then $Hom_A(J, J) = A$. To see the converse, we choose $d \ge 0$ 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

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

.



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 $xJ : J = \langle x \rangle$.

s

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

$$u_i \cdot u_j = \sum_{k=0}^{\circ} x \xi_k^{ij} u_k \text{ with suitable } \xi_k^{ij} \in A, \ 1 \le i \le j \le s.$$



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

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

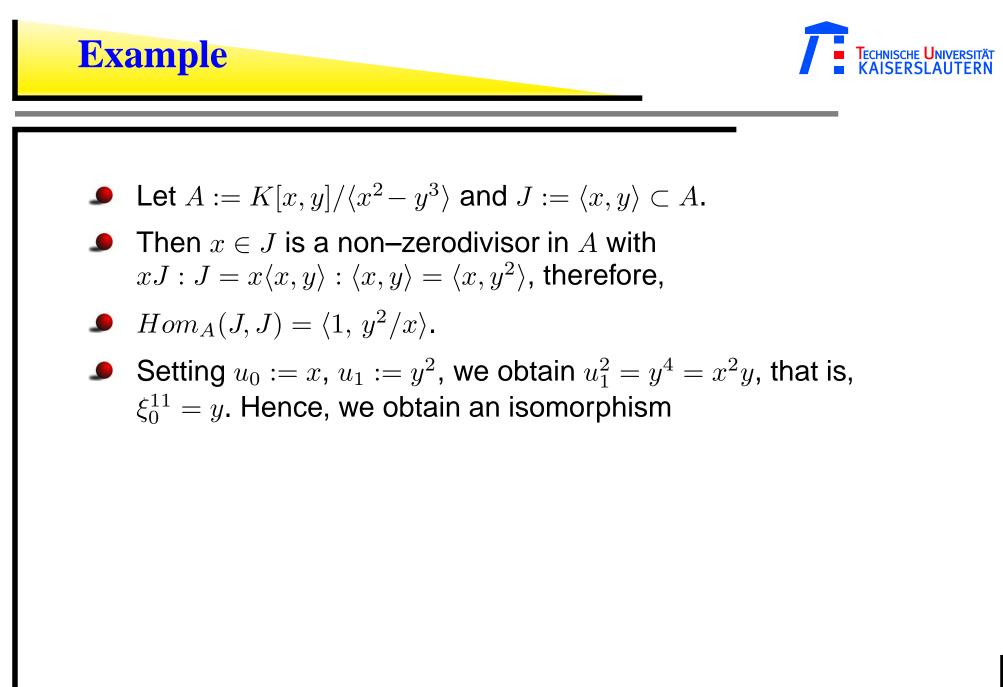
Moreover, let $\{u_0 = x, u_1, \dots, u_s\}$ be a system of generators for the *A*-module xJ : J. Then we can write

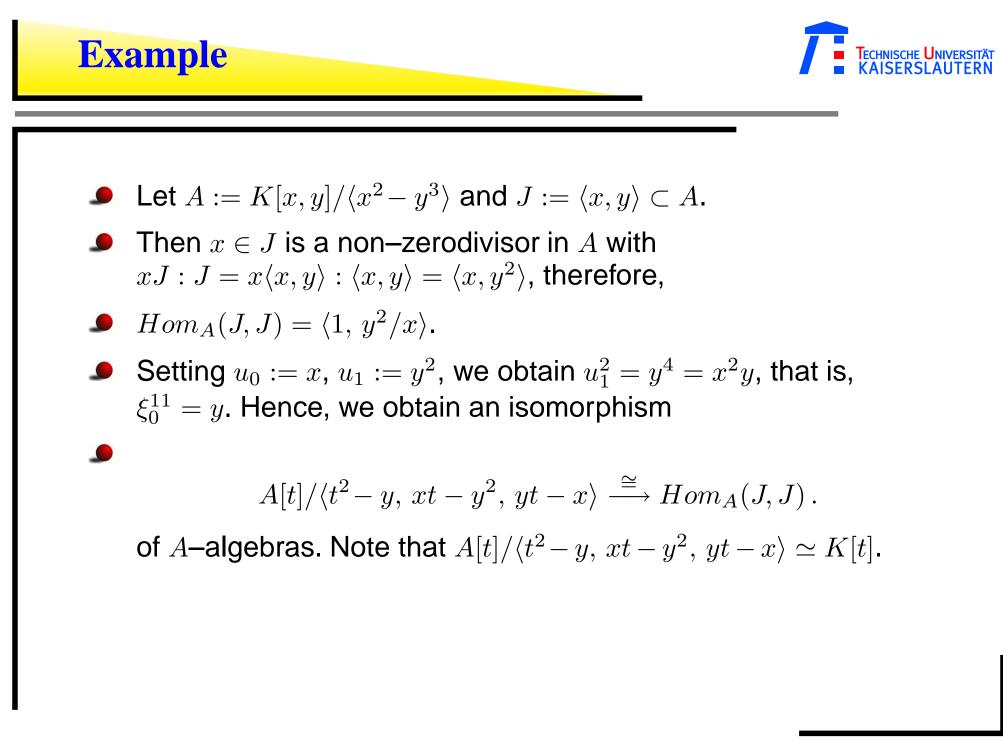
• Let $(\eta_0^{(k)}, \ldots, \eta_s^{(k)}) \in A^{s+1}$, $k = 1, \ldots, m$, generate $syz(u_0, \ldots, u_s)$, and let $I \subset A[t_1, \ldots, t_s]$ be the ideal ($t_0 := 1$)

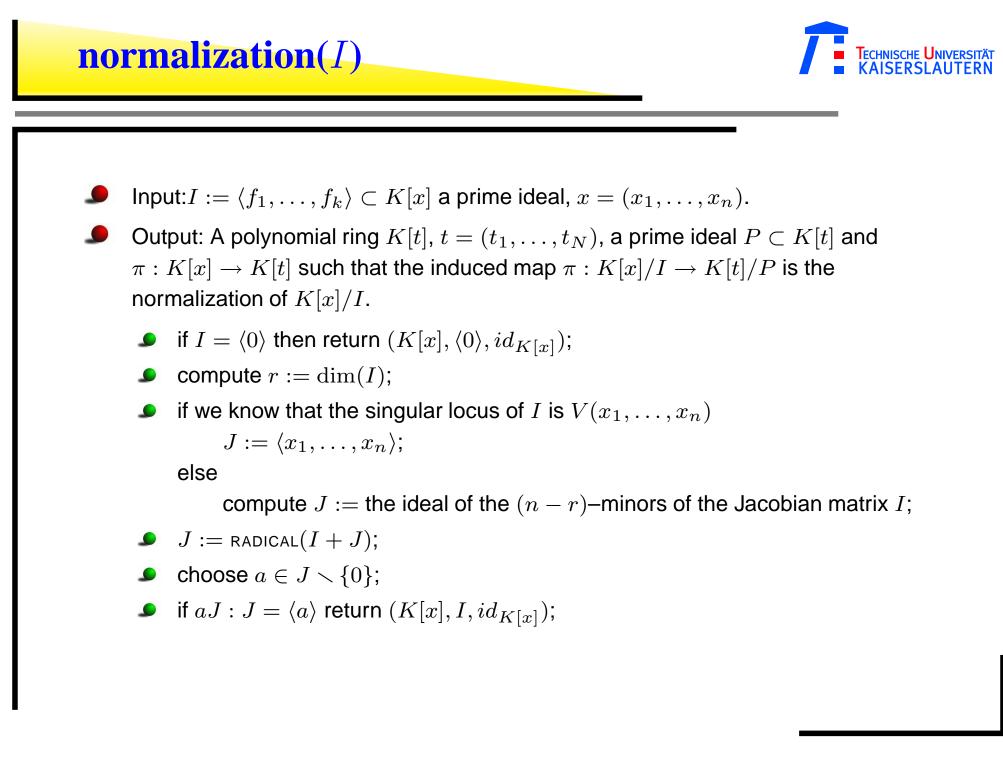
$$I := \left\langle \left\{ t_i t_j - \sum_{k=0}^s \xi_k^{ij} t_k \middle| 1 \le i \le j \le s \right\}, \left\{ \sum_{\nu=0}^s \eta_\nu^{(k)} t_\nu \middle| 1 \le k \le m \right\} \right\rangle,$$

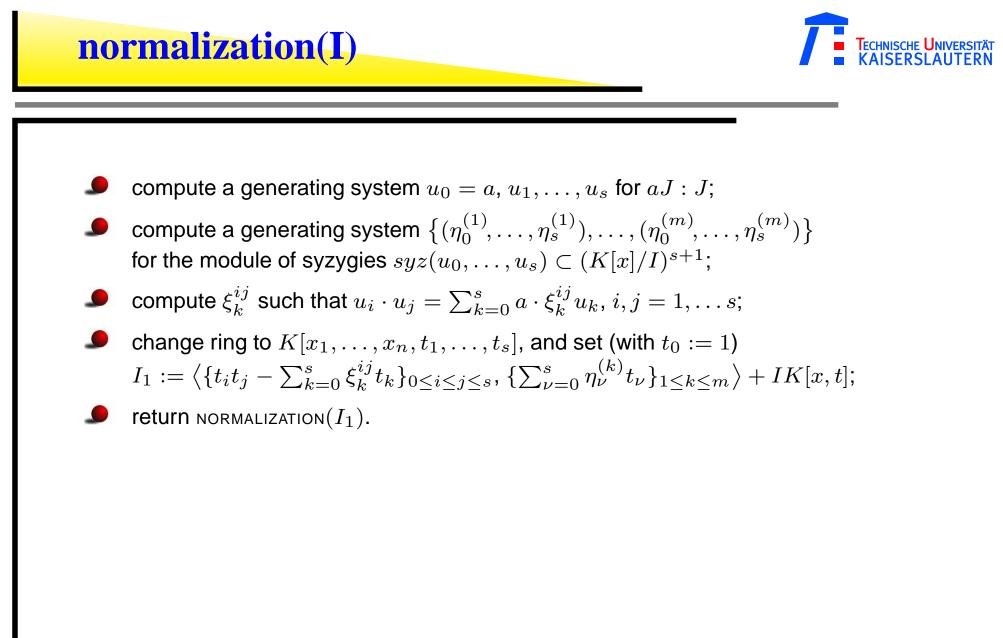
● $t_i \mapsto u_i/x$, i = 1, ..., s, defines an isomorphism

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





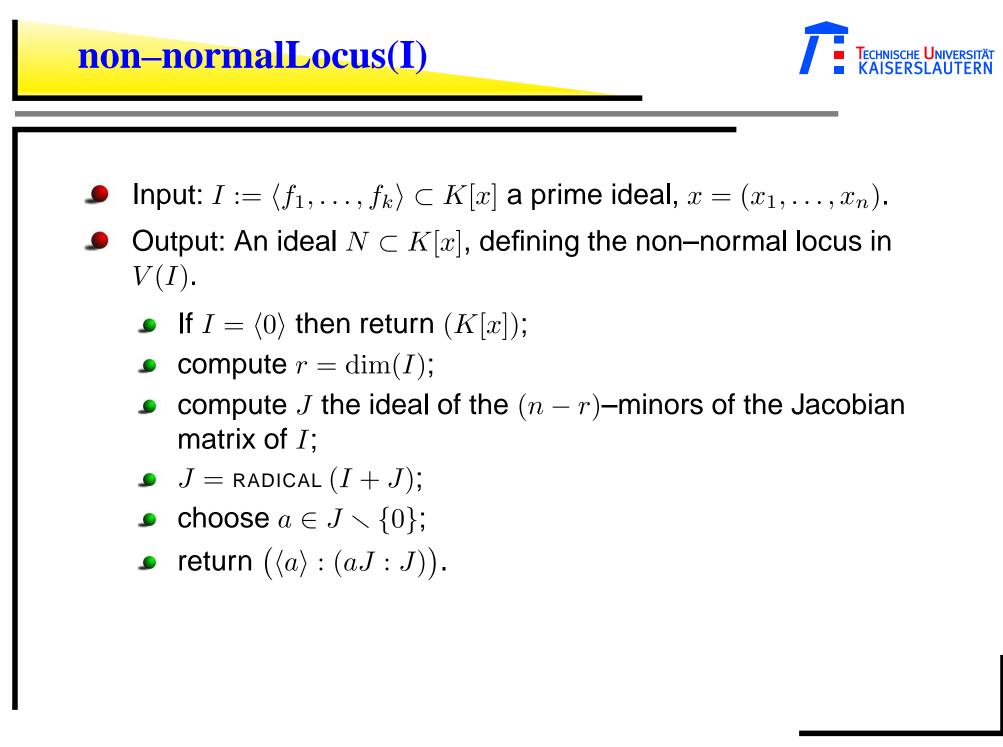




The ideal $Ann_A(Hom_A(J, J)/A) \subset A$ defines the non–normal locus. Moreover,

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

for any non–zerodivisor $x \in J$.



Primary Decomposition - p. 3