

COMPUTING IN COMMUTATIVE ALGEBRA

GERHARD PFISTER

1. STANDARD BASES AND SINGULAR

SINGULAR is available, free of charge, as a binary programme for most common hardware and software platforms. Release versions of SINGULAR can be downloaded through ftp from our FTP site

`ftp://www.mathematik.uni-kl.de/pub/Math/Singular/`,

or, using your favourite WWW browser, from

`http://www.singular.uni-kl.de/download.html`

The basis of SINGULAR is multivariate polynomial factorization and standard bases computations.

We explain first of all the notion of a Gröbner basis (with respect to any ordering) as the basis for computations in localizations of factorings of polynomial rings. The presentation of a polynomial as a linear combination of monomials is unique only up to an order of the summands, due to the commutativity of the addition. We can make this order unique by choosing a total ordering on the set of monomials. For further applications it is necessary, however, that the ordering is compatible with the semigroup structure on Mon_n .

We give here only the important definitions, theorems and examples. Proofs can be found in [7]. The SINGULAR examples can be found on the CD in [7].

Definition 1.1. A monomial ordering or semigroup ordering is a total (or linear) ordering $>$ on the set of monomials $\text{Mon}_n = \{x^\alpha \mid \alpha \in \mathbf{N}^n\}$ in n variables satisfying

$$x^\alpha > x^\beta : \implies : x^\gamma x^\alpha > x^\gamma x^\beta$$

for all $\alpha, \beta, \gamma \in \mathbf{N}^n$. We say also $>$ is a monomial ordering on $A[x_1, \dots, x_n]$, A any ring, meaning that $>$ is a monomial ordering on Mon_n .

Definition 1.2. Let $>$ be a fixed monomial ordering. Write $f \in K[x]$, $f \neq 0$, in a unique way as a sum of non-zero terms

$$f = a_\alpha x^\alpha + a_\beta x^\beta + \dots + a_\gamma x^\gamma, \quad x^\alpha > x^\beta > \dots > x^\gamma,$$

and $a_\alpha, a_\beta, \dots, a_\gamma \in K$. We define:

- (1) $LM(f) := \text{leadmonom}(f) := x^\alpha$, the leading monomial of f ,
- (2) $LE(f) := \text{leadexp}(f) := \alpha$, the leading exponent of f ,
- (3) $LT(f) := \text{lead}(f) := a_\alpha x^\alpha$, the leading term or head of f ,
- (4) $LC(f) := \text{leadcoef}(f) := a_\alpha$, the leading coefficient of f

- (5) $\text{tail}(f) := f - \text{lead}(f) = a_\beta x^\beta + \dots + a_\gamma x^\gamma$, the tail.
(6) $\text{ecart}(f) := \deg(f) - \deg(\text{LM}(f))$.

SINGULAR Example 1.

```
ring A = 0, (x,y,z), lp;
poly f = y4z3+2x2y2z2+3x5+4z4+5y2;
f; //display f in a lex-ordered way
//-> 3x5+2x2y2z2+y4z3+5y2+4z4
leadmonom(f); //leading monomial
//-> x5
leadexp(f); //leading exponent
//-> 5,0,0
lead(f); //leading term
//-> 3x5
leadcoef(f); //leading coefficient
//-> 3
f - lead(f); //tail
//-> 2x2y2z2+y4z3+5y2+4z4
```

Definition 1.3. Let $>$ be a monomial ordering on $\{x^\alpha \mid \alpha \in \mathbf{N}^n\}$.

- (1) $>$ is called a global ordering if $x^\alpha > 1$ for all $\alpha \neq (0, \dots, 0)$,
- (2) $>$ is called a local ordering if $x^\alpha < 1$ for all $\alpha \neq (0, \dots, 0)$,
- (3) $>$ is called a mixed ordering if it is neither global nor local.

Lemma 1.4. Let $>$ be a monomial ordering, then the following conditions are equivalent:

- (1) $>$ is a well-ordering.
- (2) $x_i > 1$ for $i = 1, \dots, n$.
- (3) $x^\alpha > 1$ for all $\alpha \neq (0, \dots, 0)$, that is, $>$ is global.

In the following examples we fix an enumeration x_1, \dots, x_n of the variables, any other enumeration leads to a different ordering.

%beginenumerate GLOBAL ORDERINGS

(i) *Lexicographical ordering $>_{lp}$* (also denoted by *lex*):

$$x^\alpha >_{lp} x^\beta : \iff \exists 1 \leq i \leq n : \alpha_1 = \beta_1, \dots, \alpha_{i-1} = \beta_{i-1}, \alpha_i > \beta_i.$$

(ii) *Degree reverse lexicographical ordering $>_{dp}$* (denoted by *degrevlex*):

$$x^\alpha >_{dp} x^\beta : \iff : \deg x^\alpha > \deg x^\beta$$

$$\text{or} : (\deg x^\alpha = \deg x^\beta \text{ and } \exists 1 \leq i \leq n : \alpha_n = \beta_n, \dots, \alpha_{i+1} = \beta_{i+1}, \alpha_i < \beta_i),$$

where $\deg x^\alpha = \alpha_1 + \dots + \alpha_n$.

%le i

LOCAL ORDERINGS

(i) *Negative lexicographical ordering* $>_{ls}$:

$$x^\alpha >_{ls} x^\beta : \iff \exists 1 \leq i \leq n, \alpha_1 = \beta_1, \dots, \alpha_{i-1} = \beta_{i-1}, \alpha_i < \beta_i.$$

(ii) *Negative degree reverse lexicographical ordering*:

$$\begin{aligned} x^\alpha >_{ds} x^\beta &: \iff: \deg x^\alpha < \deg x^\beta, \text{ where } \deg x^\alpha = \alpha_1 + \dots + \alpha_n, \\ &\text{or : } (\deg x^\alpha = \deg x^\beta \text{ and } \exists 1 \leq i \leq n : \\ &\quad \alpha_n = \beta_n, \dots, \alpha_{i+1} = \beta_{i+1}, \alpha_i < \beta_i). \end{aligned}$$

Let $>$ be a monomial ordering on the set of monomials $\text{Mon}(x_1, \dots, x_n) = \{x^\alpha \mid \alpha \in \mathbf{N}^n\}$, and $K[x] = K[x_1, \dots, x_n]$ the polynomial ring in n variables over a field K . Then the leading monomial function LM has the following properties for polynomials $f, g \in K[x] \setminus \{0\}$:

- (1) $\text{LM}(gf) = \text{LM}(g)\text{LM}(f)$.
- (2) $\text{LM}(g+f) \leq \max\{\text{LM}(g), \text{LM}(f)\}$ with equality if and only if the leading terms of f and g do not cancel.

In particular, it follows that

$$S_{>} := \{u \in K[x] \setminus \{0\} \mid \text{LM}(u) = 1\}$$

is a multiplicatively closed set.

Definition 1.5. For any monomial ordering $>$ on $\text{Mon}(x_1, \dots, x_n)$, we define

$$K[x]_{>} := S_{>}^{-1}K[x] = \left\{ \frac{f}{u} \mid f, u \in K[x], \text{LM}(u) = 1 \right\},$$

the localization of $K[x]$ with respect to $S_{>}$ and call $K[x]_{>}$ the ring associated to $K[x]$ and $>$.

Note that $S_{>} = K^*$ if and only if $>$ is global and $S_{>} = K[x] \setminus \langle x_1, \dots, x_n \rangle$ if and only if $>$ is local.

Definition 1.6. Let $>$ be any monomial ordering:

- (1) For $f \in K[x]_{>}$ choose $u \in K[x]$ such that $\text{LT}(u) = 1$ and $uf \in K[x]$. We define

$$\begin{aligned} \text{LM}(f) &:= \text{LM}(uf), \\ \text{LC}(f) &:= \text{LC}(uf), \\ \text{LT}(f) &:= \text{LT}(uf), \\ \text{LE}(f) &:= \text{LE}(uf), \end{aligned}$$

and $\text{tail}(f) = f - \text{LT}(f)$.

- (2) For any subset $G \subset K[x]_{>}$ define the ideal

$$L_{>}(G) := L(G) := \langle \text{LM}(g) \mid g \in G \setminus \{0\} \rangle_{K[x]}.$$

$L(G) \subset K[x]$ is called the leading ideal of G .

Definition 1.7. Let $I \subset R = K[x]_{>}$ be an ideal.

(1) A finite set $G \subset R$ is called a standard basis of I if

$$G \subset I, \text{ and } L(I) = L(G).$$

That is, G is a standard basis, if the leading monomials of the elements of G generate the leading ideal of I , or, in other words, if for any $f \in I \setminus \{0\}$ there exists a $g \in G$ satisfying $LM(g) \mid LM(f)$.

(2) If $>$ is global, a standard basis is also called a Gröbner basis.

(3) If we just say that G is a standard basis, we mean that G is a standard basis of the ideal $\langle G \rangle_R$ generated by G .

Standard bases can be characterized using the notion of the normal form. We need the following definitions:

Definition 1.8. Let $f, g \in R \setminus \{0\}$ with $LM(f) = x^\alpha$ and $LM(g) = x^\beta$, respectively. Set

$$\gamma := \text{lcm}(\alpha, \beta) := (\max(\alpha_1, \beta_1), \dots, \max(\alpha_n, \beta_n))$$

and let $\text{lcm}(x^\alpha, x^\beta) := x^\gamma$ be the least common multiple of x^α and x^β . We define the s -polynomial (spoly, for short) of f and g to be

$$\text{spoly}(f, g) := x^{\gamma-\alpha} f - \frac{LC(f)}{LC(g)} \cdot x^{\gamma-\beta} g.$$

If $LM(g)$ divides $LM(f)$, say $LM(g) = x^\beta$, $LM(f) = x^\alpha$, then the s -polynomial is particularly simple,

$$\text{spoly}(f, g) = f - \frac{LC(f)}{LC(g)} \cdot x^{\alpha-\beta} g,$$

and $LM(\text{spoly}(f, g)) < LM(f)$.

Definition 1.9. Let \mathcal{G} denote the set of all finite lists $G \subset R = K[x]_{>}$.

$$NF : R \times \mathcal{G} \rightarrow R, (f, G) \mapsto NF(f \mid G),$$

is called a normal form on R if, for all $G \in \mathcal{G}$,

$$(0) \quad NF(0 \mid G) = 0,$$

and, for all $f \in R$ and $G \in \mathcal{G}$,

$$(1) \quad NF(f \mid G) \neq 0 \implies LM(NF(f \mid G)) \notin L(G).$$

(2) If $G = \{g_1, \dots, g_s\}$, then f has a standard representation with respect to $NF(- \mid G)$, that is, there exists a unit $u \in R^*$ such that

$$uf - NF(f \mid G) = \sum_{i=1}^s a_i g_i, \quad a_i \in R, \quad s \geq 0,$$

satisfying $LM(\sum_{i=1}^s a_i g_i) \geq LM(a_i g_i)$ for all i such that $a_i g_i \neq 0$.

The existence of a normal form is given by the following algorithm:

Algorithm 1.10. $NF(f \mid G)$

Let $>$ be any monomial ordering.

Input: $f \in K[x]$, G a finite list in $K[x]$

Output: $h \in K[x]$ a polynomial normal form of f with respect to G .

- $h := f$;
- $T := G$;
- *while*($h \neq 0$ and $T_h := \{g \in T \mid LM(g) \mid LM(h)\} \neq \emptyset$)
 - choose* $g \in T_h$ with *ecart*(g) minimal;
 - if* (*ecart*(g) > *ecart*(h))
 - $T := T \cup \{h\}$;
 - $h := \text{spoly}(h, g)$;
- *return* h ;

Theorem 1.11. *Let $I \subset R$ be an ideal and $G = \{g_1, \dots, g_s\} \subset I$. Then the following are equivalent:*

- (1) G is a standard basis of I .
- (2) $NF(f \mid G) = 0$ if and only if $f \in I$.

We will explain now how to use standard bases to solve problems in algebra.

Ideal membership

Problem: Given $f, f_1, \dots, f_k \in K[x]$, and let $I = \langle f_1, \dots, f_k \rangle_R$. We wish to decide whether $f \in I$, or not.

Solution: We choose any monomial ordering $>$ such that $K[x]_> = R$ and compute a standard basis $G = \{g_1, \dots, g_s\}$ of I with respect to $>$. $f \in I$ if and only if $NF(f \mid G) = 0$.

SINGULAR Example 2.

```
ring A = 0, (x,y), dp;
ideal I = x10+x9y2, y8-x2y7;
ideal J = std(I);
poly f = x2y7+y14;
reduce(f, J, 1);          //3rd parameter 1 avoids tail reduction
//-> -xy12+x2y7          //f is not in I
      f = xy13+y12;
reduce(f, J, 1);
//-> 0                   //f is in I
```

Intersection with Subrings (Elimination of variables)

Problem: Given $f_1, \dots, f_k \in K[x] = K[x_1, \dots, x_n]$, $I = \langle f_1, \dots, f_k \rangle_{K[x]}$, we should like to find generators of the ideal

$$I' = I \cap K[x_{s+1}, \dots, x_n], \quad s < n.$$

Elements of the ideal I' are said to be obtained from f_1, \dots, f_k by *eliminating* x_1, \dots, x_s . The following lemma is the basis for solving the elimination problem.

Lemma 1.12. Let $>$ be an elimination ordering for x_1, \dots, x_s on the set of monomials $\text{Mon}(x_1, \dots, x_n)$, and let $I \subset K[x_1, \dots, x_n]_{>}$ be an ideal. If $S = \{g_1, \dots, g_k\}$ is a standard basis of I , then

$$S' := \{g \in S \mid LM(g) \in K[x_{s+1}, \dots, x_n]\}$$

is a standard basis of $I' := I \cap K[x_{s+1}, \dots, x_n]_{>'}$. In particular, S' generates the ideal I' .

SINGULAR Example 3.

```
ring A =0, (t,x,y,z), dp;
ideal I=t2+x2+y2+z2, t2+2x2-xy-z2, t+y3-z3;

eliminate(I,t);
//-> _[1]=x2-xy-y2-2z2      _[2]=y6-2y3z3+z6+2x2-xy-z2
```

Alternatively choose a product ordering:

```
ring A1=0, (t,x,y,z), (dp(1), dp(3));
ideal I=imap(A,I);
ideal J=std(I);
J;
//-> J[1]=x2-xy-y2-2z2      J[2]=y6-2y3z3+z6+2x2-xy-z2
//-> J[3]=t+y3-z3
```

Radical Membership

Problem: Let $f_1, \dots, f_k \in K[x]_{>}$, $>$ a monomial ordering on $\text{Mon}(x_1, \dots, x_n)$ and $I = \langle f_1, \dots, f_k \rangle_{K[x]_{>}}$. Given some $f \in K[x]_{>}$ we want to decide whether $f \in \sqrt{I}$. The following lemma, which is sometimes called *Rabinowich's trick*, is the basis for solving this problem.¹

Lemma 1.13. Let A be a ring, $I \subset A$ an ideal and $f \in A$. Then

$$f \in \sqrt{I} : \iff 1 \in \tilde{I} := \langle I, 1 - tf \rangle_{A[t]}$$

where t is an additional new variable.

SINGULAR Example 4.

```
ring A =0, (x,y,z), dp;
ideal I=x5,xy3,y7,z3+xyz;
poly f =x+y+z;

ring B =0, (t,x,y,z), dp; //need t for radical test
ideal I=imap(A,I);
poly f =imap(A,f);
I=I,1-t*f;
std(I);
//-> _[1]=1                //f is in the radical
```

¹We can even compute the full radical \sqrt{I} , but this is a much harder computation.

```
LIB"primdec.lib"; //just to see, we compute the radical
setring A;
radical(I);
//-> _[1]=z _[2]=y _[3]=x
```

Intersection of Ideals

Problem: Given $f_1, \dots, f_k, h_1, \dots, h_r \in K[x]$ and $>$ a monomial ordering. Let $I_1 = \langle f_1, \dots, f_k \rangle_{K[x]>}$ and $I_2 = \langle h_1, \dots, h_r \rangle_{K[x]>}$. We wish to find generators for $I_1 \cap I_2$.

Consider the ideal $J := \langle tf_1, \dots, tf_k, (1-t)h_1, \dots, (1-t)h_r \rangle_{(K[x]>)[t]}$.

Lemma 1.14. *With the above notations, $I_1 \cap I_2 = J \cap K[x]>$.*

SINGULAR Example 5.

```
ring A=0,(x,y,z),dp;
ideal I1=x,y;
ideal I2=y^2,z;
intersect(I1,I2); //the built-in SINGULAR command
//-> _[1]=y^2 _[2]=yz _[3]=xz
```

```
ring B=0,(t,x,y,z),dp; //the way described above
ideal I1=imap(A,I1);
ideal I2=imap(A,I2);
ideal J=t*I1+(1-t)*I2;
eliminate(J,t);
//-> _[1]=yz _[2]=xz _[3]=y^2
```

Quotient of Ideals

Problem: Let I_1 and $I_2 \subset K[x]>$. We want to compute

$$I_1 : I_2 = \{g \in K[x]> \mid gI_2 \subset I_1\}.$$

Since, obviously, $I_1 : \langle h_1, \dots, h_r \rangle = \bigcap_{i=1}^r (I_1 : \langle h_i \rangle)$, we can compute $I_1 : \langle h_i \rangle$ for each i . The next lemma shows a way to compute $I_1 : \langle h_i \rangle$.

Lemma 1.15. *Let $I \subset K[x]>$ be an ideal, and let $h \in K[x]>$, $h \neq 0$. Moreover, let $I \cap \langle h \rangle = \langle g_1 \cdot h, \dots, g_s \cdot h \rangle$. Then $I : \langle h \rangle = \langle g_1, \dots, g_s \rangle_{K[x]>}$.*

SINGULAR Example 6.

```
ring A=0,(x,y,z),dp;
ideal I1=x,y;
ideal I2=y^2,z;
quotient(I1,I2); //the built-in SINGULAR command
//-> _[1]=y _[2]=x
```

Kernel of a Ring Map

Let $\varphi : R_1 := (K[x]_{>_1})/I \rightarrow (K[y]_{>_2})/J =: R_2$ be a ring map defined by polynomials $\varphi(x_i) = f_i \in K[y] = K[y_1, \dots, y_m]$ for $i = 1, \dots, n$ (and assume that the monomial orderings satisfy $1 >_2 \text{LM}(f_i)$ if $1 >_1 x_i$).

Define $J_0 := J \cap K[y]$, and $I_0 := I \cap K[x]$. Then φ is induced by

$$\tilde{\varphi} : K[x]/I_0 \rightarrow K[y]/J_0, \quad x_i \mapsto f_i,$$

and we have a commutative diagram

$$\begin{array}{ccc} K[x]/I_0 & \xrightarrow{\tilde{\varphi}} & K[y]/J_0 \\ \downarrow & & \downarrow \\ R_1 & \xrightarrow{\varphi} & R_2. \end{array}$$

Problem: Let I, J and φ be as above. Compute generators for $\text{Ker}(\varphi)$.

Solution: Assume that $J_0 = \langle g_1, \dots, g_s \rangle_{K[y]}$ and $I_0 = \langle h_1, \dots, h_t \rangle_{K[x]}$.

Set $H := \langle h_1, \dots, h_t, g_1, \dots, g_s, x_1 - f_1, \dots, x_n - f_n \rangle \subset K[x, y]$, and compute $H' := H \cap K[x]$ by eliminating y_1, \dots, y_m from H . Then H' generates $\text{Ker}(\varphi)$ by the following lemma.

Lemma 1.16. *With the above notations, $\text{Ker}(\varphi) = \text{Ker}(\tilde{\varphi})R_1$ and*

$$\text{Ker}(\tilde{\varphi}) = (I_0 + \langle g_1, \dots, g_s, x_1 - f_1, \dots, x_n - f_n \rangle_{K[x,y]} \cap K[x]) \text{ mod } I_0.$$

In particular, if $>_1$ is global, then $\text{Ker}(\varphi) = \text{Ker}(\tilde{\varphi})$.

SINGULAR Example 7.

```
ring A=0, (x,y,z), dp;
ring B=0, (a,b), dp;
map phi=A, a2, ab, b2;
ideal zero; //compute the preimage of 0
setring A;
preimage(B, phi, zero); //the built-in SINGULAR command
//-> _[1]=y2-xz

ring C=0, (x,y,z,a,b), dp; //the method described above
ideal H=x-a2, y-ab, z-b2;
eliminate(H, ab);
//-> _[1]=y2-xz
```

2. LECTURE: POLYNOMIAL SOLVING AND PRIMARY DECOMPOSITION

Solvability of Polynomial Equations

Problem: Given $f_1, \dots, f_k \in K[x_1, \dots, x_n]$, we want to assure whether the system of polynomial equations

$$f_1(x) = \dots = f_k(x) = 0$$

has a solution in \bar{K}^n , where \bar{K} is the algebraic closure of K .

Let $I = \langle f_1, \dots, f_k \rangle_{K[x]}$, then the question is whether the algebraic set $V(I) \subset \bar{K}^n$ is empty or not.

Solution: By Hilbert's Nullstellensatz, $V(I) = \emptyset$ if and only if $1 \in I$. We compute a Gröbner basis G of I with respect to any global ordering on $\text{Mon}(x_1, \dots, x_n)$ and normalize it (that is, divide every $g \in G$ by $\text{LC}(g)$). Since $1 \in I$ if and only if $1 \in L(I)$, we have $V(I) = \emptyset$ if and only if 1 is an element of a normalized Gröbner basis of I . Of course, we can avoid normalizing, which is expensive in rings with parameters. Since $1 \in I$ if and only if G contains a non-zero constant polynomial, we have only to look for an element of degree 0 in G .

SINGULAR Example 8.

```
ring A=0,(x,y,z),lp;
ideal I=x2+y+z-1,
      x+y2+z-1,
      x+y+z2-1;
ideal J=groebner(I); //the lexicographical Groebner basis
J;
//-> J[1]=z6-4z4+4z3-z2      J[2]=2yz2+z4-z2
//-> J[3]=y2-y-z2+z         J[4]=x+y+z2-1
```

We use the multivariate solver based on triangular sets.

```
LIB"solve.lib";
list s1=solve(I,6);
//-> // name of new current ring: AC
s1;
//-> [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
```

If we want to compute the zeros with multiplicities then we use 1 as a third parameter for the command:

```

setring A;
list s2=solve(I,6,1);
s2;
//-> [1]: [2]:
//-> [1]: [1]:
//-> [1]: [1]:
//-> -2.414214 0
//-> [2]: [2]:
//-> -2.414214 1
//-> [3]: [3]:
//-> -2.414214 0
//-> [2]: [2]:
//-> [1]: [1]:
//-> 0.414214 1
//-> [2]: [2]:
//-> 0.414214 0
//-> [3]: [3]:
//-> 0.414214 0
//-> [2]: [3]:
//-> 1 [1]:
//-> 0
//-> [2]:
//-> 0
//-> [3]:
//-> 1
//-> [2]:
//-> 2

```

The output has to be interpreted as follows: there are two zeros of multiplicity 1 and three zeros $((0, 1, 0), (1, 0, 0), (0, 0, 1))$ of multiplicity 2.

Definition 2.1.

- (1) 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 $M = \langle x_1 + g_1(x_n), \dots, x_{n-1} + g_{n-1}(x_n), g_n(x_n) \rangle$.
- (2) 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 2.2. 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 $\varphi_{\underline{a}} : K[x] \rightarrow K[x]$ 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 $x_1 > \dots > x_n$.

Proposition 2.3. Let $I \subset K[x_1, \dots, x_n]$ be a zero-dimensional ideal. Let $\langle g \rangle = I \cap K[x_n]$, $g = g_1^{v_1} \dots g_s^{v_s}$, g_i monic and prime and $g_i \neq g_j$ for $i \neq j$. Then

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

If I is in general position with respect to the lexicographical ordering with $x_1 > \dots > x_n$, then

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

SINGULAR Example 9 (zero-dim primary decomposition).

We give an example for a zero-dimensional primary decomposition.

```
option(redSB);
ring R=0, (x,y), lp;
ideal I=(y^2-1)^2, x^2-(y+1)^3;
```

The ideal I is not in general position with respect to lp , since the minimal associated prime $\langle x^2 - 8, y - 1 \rangle$ is not.

```
map phi=R,x,x+y; //we choose a generic coordinate change
map psi=R,x,-x+y; //and the inverse map
I=std(phi(I));
I;
//-> I[1]=y^7-y^6-19y^5-13y^4+99y^3+221y^2+175y+49
//-> I[2]=112xy+112x-27y^6+64y^5+431y^4-264y^3-2277y^2-2520y-847
//-> I[3]=56x^2+65y^6-159y^5-1014y^4+662y^3+5505y^2+6153y+2100
factorize(I[1]);
//-> [1]:
//-> _[1]=1
//-> _[2]=y^2-2y-7
//-> _[3]=y+1
//-> [2]:
//-> 1,2,3

ideal Q1=std(I,(y^2-2y-7)^2); //the candidates for the
//primary ideals
ideal Q2=std(I,(y+1)^3); //in general position
Q1; Q2;

//-> Q1[1]=y^4-4y^3-10y^2+28y+49 Q2[1]=y^3+3y^2+3y+1
```

```

//-> Q1[2]=56x+y3-9y2+63y-7      Q2[2]=2xy+2x+y2+2y+1
                                   Q2[3]=x2

factorize(Q1[1]); //primary and general position test
                //for Q1

//-> [1]:
//->   _[1]=1
//->   _[2]=y2-2y-7
//-> [2]:
//->   1,2

factorize(Q2[1]); //primary and general position test
                //for Q2

//-> [1]:
//->   _[1]=1
//->   _[2]=y+1
//-> [2]:
//->   1,3

```

Both ideals are primary and in general position.

```

Q1=std(psi(Q1)); //the inverse coordinate change
Q2=std(psi(Q2)); //the result
Q1; Q2;

//-> Q1[1]=y2-2y+1      Q2[1]=y2+2y+1
//-> Q1[2]=x2-12y+4     Q2[2]=x2

```

We obtain that I is the intersection of the primary ideals Q_1 and Q_2 with associated prime ideals $\langle y-1, x^2-8 \rangle$ and $\langle y+1, x \rangle$.

The following proposition reduces the higher dimensional case to the zero-dimensional case:

Proposition 2.4. *Let $I \subset K[x]$ be an ideal and $u \subset x = \{x_1, \dots, x_n\}$ be a maximal independent set of variables² with respect to I .*

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

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

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

²It is maximal such that $I \cap K[u] = \langle 0 \rangle$.

- (3) 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.

Finally we explain how to compute the radical.

Proposition 2.5. Let $I \subset K[x_1, \dots, x_n]$ be a zero-dimensional ideal and $I \cap K[x_i] = \langle f_i \rangle$ for $i = 1, \dots, n$. Moreover, let g_i be the squarefree part of f_i , then $\sqrt{I} = I + \langle g_1, \dots, g_n \rangle$.

The higher dimensional case can be reduced similarly to the primary decomposition to the zero-dimensional case.

3. LECTURE: INVARIANTS

The computation of the Hilbert function will be discussed and explained. Let K be a field.

Definition 3.1. Let $A = \bigoplus_{v \geq 0} A_v$ be a Noetherian graded K -algebra, and let $M = \bigoplus_{v \in \mathbb{Z}} M_v$ be a finitely generated graded A -module. The Hilbert function $H_M : \mathbb{Z} \rightarrow \mathbb{Z}$ of M is defined by

$$H_M(n) := \dim_K(M_n),$$

and the Hilbert–Poincaré series HP_M of M is defined by

$$HP_M(t) := \sum_{v \in \mathbb{Z}} H_M(v) \cdot t^v \in \mathbb{Z}[[t]][t^{-1}].$$

Theorem 3.2. Let $A = \bigoplus_{v \geq 0} A_v$ be a graded K -algebra, and assume that A is generated, as K -algebra, by $x_1, \dots, x_r \in A_1$. Then, for any finitely generated (positively) graded A -module $M = \bigoplus_{v \geq 0} M_v$,

$$HP_M(t) = \frac{Q(t)}{(1-t)^r} \text{ for some } Q(t) \in \mathbb{Z}[t].$$

Note that SINGULAR has a command which computes the numerator $Q(t)$ for the Hilbert–Poincaré series:

SINGULAR Example 10.

```
ring A=0, (t,x,y,z), dp;
ideal I=x5y2,x3,y3,xy4,xy7;
intvec v = hilb(std(I),1);
v;
//-> 1,0,0,-2,0,0,1,0
```

We obtain $Q(t) = t^6 - 2t^3 + 1$.

The latter output has to be interpreted as follows: if $v = (v_0, \dots, v_d, 0)$ then $Q(t) = \sum_{i=0}^d v_i t^i$.

Theorem 3.3. *Let $>$ be any monomial ordering on $K[x] := K[x_1, \dots, x_r]$, and let $I \subset K[x]$ be a homogeneous ideal. Then*

$$HP_{K[x]/I}(t) = HP_{K[x]/L(I)}(t),$$

where $L(I)$ is the leading ideal of I with respect to $>$.

Examples how to compute the Hilbert polynomial, the Hilbert–Samuel function, the degree respectively and the multiplicity and the dimension of an ideal can be found in [7]. As above all computations are reduced to compute the corresponding invariants for the leading ideal.

4. LECTURE: HOMOLOGICAL ALGEBRA

Here we will show different approaches how to test Cohen–Macaulayness using SINGULAR. More details about the underlying theory can be found in [7].

SINGULAR Example 11 (first test for Cohen–Macaulayness).

Let (A, \mathfrak{m}) be a local ring, $\mathfrak{m} = \langle x_1, \dots, x_n \rangle$. Let M be an A -module given by a presentation $A^\ell \rightarrow A^s \rightarrow M \rightarrow 0$. To check whether M is Cohen–Macaulay we use that the equality

$$\begin{aligned} \dim(A/\text{Ann}(M)) &= \dim(M) = \text{depth}(M) \\ &= n - \sup\{i \mid H_i(x_1, \dots, x_n, M) \neq 0\}. \end{aligned}$$

is necessary and sufficient for M to be Cohen–Macaulay. The following procedure computes $\text{depth}(\mathfrak{m}, M)$, where $\mathfrak{m} = \langle x_1, \dots, x_n \rangle \subset A = K[x_1, \dots, x_n]_{>}$ and M is a finitely generated A -module with $\mathfrak{m}M \neq M$.

The following procedures use the procedures Koszul Homology from `homolog.lib` and `Ann` from `primdec.lib` to compute the Koszul Homology $H_i(x_1, \dots, x_n, M)$ and the annihilator $\text{Ann}(M)$. They have to be loaded first.

```
LIB "homolog.lib";
proc depth(module M)
{
  ideal m=maxideal(1);
  int n=size(m);
  int i;
  while(i<n)
  {
    i++;
    if(size(KoszulHomology(m,M,i))==0){return(n-i+1);}
  }
  return(0);
}
```

Now the test for Cohen–Macaulayness is easy.

```
LIB "primdec.lib";
proc CohenMacaulayTest(module M)
{
  return(depth(M)==dim(std(Ann(M))));
}
```

The procedure returns 1 if M is Cohen–Macaulay and 0 if not.

As an application, we check that a complete intersection is Cohen–Macaulay and that $K[x, y, z]_{\langle x, y, z \rangle} / \langle xz, yz, z^2 \rangle$ is not Cohen–Macaulay.

```
ring R=0, (x, y, z), ds;
ideal I=xz, yz, z2;
module M=I*freemodule(1);
CohenMacaulayTest(M);
//-> 0
```

```
I=x2+y2, z7;
M=I*freemodule(1);
CohenMacaulayTest(M);
//-> 1
```

SINGULAR Example 12 (second test for Cohen–Macaulayness).

Let $A = K[x_1, \dots, x_n]_{\langle x_1, \dots, x_n \rangle} / I$. Using Noether normalization, we may assume that $A \supset K[x_{s+1}, \dots, x_n]_{\langle x_{s+1}, \dots, x_n \rangle} =: B$ is finite. We choose a monomial basis $m_1, \dots, m_r \in K[x_1, \dots, x_s]$ of $A|_{x_{s+1}=\dots=x_n=0}$.

Then m_1, \dots, m_r is a minimal system of generators of A as B -module. A is Cohen–Macaulay if and only if A is a free B -module, that is, there are no B -relations between m_1, \dots, m_r , in other words, $\text{syz}_A(m_1, \dots, m_r) \cap B^r = \langle 0 \rangle$. This test can be implemented in SINGULAR as follows:

```
proc isCohenMacaulay(ideal I)
{
  def A = basering;
  list L = noetherNormal(I);
  map phi = A, L[1];
  I = phi(I);
  int s = nvars(basering)-size(L[2]);
  execute("ring B="+charstr(A)+", x(1..s), ds;");
  ideal m = maxideal(1);
  map psi = A, m;
  ideal J = std(psi(I));
  ideal K = kbase(J);
  setring A;
  execute("
    ring C="+charstr(A)+", (" + varstr(A) + "), (dp(s), ds);");
```

```

ideal I = imap(A,I);
qring D = std(I);
ideal K = fetch(B,K);
module N = std(syz(K));
intvec v = leadexp(N[size(N)]);
int i=1;
while((i<s)&&(v[i]==0)){i++;}
setring A;
if(!v[i]){return(0);}
return(1);
}

```

As the above procedure uses `noetherNormal` from `algebra.lib`, we first have to load this library.

```

LIB"algebra.lib";
ring r=0,(x,y,z),ds;
ideal I=xz,yz;
isCohenMacaulay(I);
//-> 0

```

```

I=x2-y3;
isCohenMacaulay(I);
//-> 1

```

SINGULAR Example 13 (3rd test for Cohen–Macaulayness).

We use the Auslander–Buchsbaum formula to compute the depth of M and then check if $\text{depth}(M) = \dim(M) = \dim(A/\text{Ann}(M))$.

We assume that $A = K[x_1, \dots, x_n]_{\langle x_1, \dots, x_n \rangle} / I$ and compute a minimal free resolution. Then $\text{depth}(A) = n - \text{pd}_{K[x_1, \dots, x_n]_{\langle x_1, \dots, x_n \rangle}}(A)$. If M is a finitely generated A -module of finite projective dimension, then we compute a minimal free resolution of M and obtain $\text{depth}(M) = \text{depth}(A) - \text{pd}_A(M)$.

```

proc projdim(module M)
{
  list l=mres(M,0);          //compute the resolution
  int i;
  while(i<size(l))
  {
    i++;
    if(size(l[i])==0){return(i-1);}
  }
}

```

Now it is easy to give another test for Cohen–Macaulayness.

```

proc isCohenMacaulay1(ideal I)

```

```

{
  int de=nvars(basering)-projdim(I*freemodule(1));
  int di=dim(std(I));
  return(de==di);
}

```

```

ring R=0,(x,y,z),ds;
ideal I=xz,yz;
isCohenMacaulay1(I);
//-> 0

```

```

I=x2-y3;
isCohenMacaulay1(I);
//-> 1

```

```

I=xz,yz,xy;
isCohenMacaulay1(I);
//-> 1
kill R;

```

The following procedure checks whether the depth of M is equal to d . It uses the procedure `Ann` from `primdec.lib`.

```

proc CohenMacaulayTest1(module M, int d)
{
  return((d-projdim(M))==dim(std(Ann(M))));
}

```

```

LIB"primdec.lib";
ring R=0,(x,y,z),ds;
ideal I=xz,yz;
module M=I*freemodule(1);
CohenMacaulayTest1(M,3);
//-> 0

```

```

I=x2+y2,z7;
M=I*freemodule(1);
CohenMacaulayTest1(M,3);
//-> 1

```

REFERENCES

- [1] Cox, D.; Little, J.; O'Shea, D.: Ideals, Varieties and Algorithms. Springer (1992).
- [2] Decker, W.; Lossen, Chr.: Computing in Algebraic Geometry; A quick start using SINGULAR. Springer, (2006).
- [3] Decker, W.; Greuel, G.-M.; Pfister, P.: Primary Decomposition: Algorithms and Comparisons. In: Algorithmic Algebra and Number Theory, Springer, 187–220 (1998).

- [4] Decker, W.; Greuel, G.-M.; de Jong, T.; Pfister, G.: The Normalization: a new Algorithm, Implementation and Comparisons. In: Proceedings EUROCONFERENCE Computational Methods for Representations of Groups and Algebras (1.4. – 5.4.1997), Birkhäuser, 177–185 (1999).
- [5] Dickenstein, A.; Emiris, I.Z.: Solving Polynomial Equations; Foundations, Algorithms, and Applications. Algorithms and Computations in Mathematics, Vol. 41, Springer, (2005).
- [6] Eisenbud, D.; Grayson, D.; Stillman, M., Sturmfels, B.: Computations in Algebraic Geometry with Macaulay2. Springer, (2001).
- [7] Greuel, G.-M.; Pfister G.: A Singular Introduction to Commutative Algebra. Springer 2008.
- [8] Greuel, G.-M.; Pfister, G.: SINGULAR and Applications, Jahresbericht der DMV 108 (4), 167-196, (2006).
- [9] Kreuzer, M.; Robbiano, L.: Computational Commutative Algebra 1. Springer (2000).
- [10] Vasconcelos, W.V.: Computational Methods in Commutative Algebra and Algebraic Geometry. Springer (1998).

Computer Algebra Systems

- [11] ASIR (Noro, M.; Shimoyama, T.; Takeshima, T.): <http://www.asir.org/>.
- [12] CoCoA (Robbiano, L.): A System for Computation in Algebraic Geometry and Commutative Algebra. Available from cocoa.dima.unige.it/cocoa
- [13] Macaulay 2 (Grayson, D.; Stillman, M.): A Computer Software System Designed to Support Research in Commutative Algebra and Algebraic Geometry. Available from <http://math.uiuc.edu/Macaulay2>.
- [14] SINGULAR (Greuel, G.-M.; Pfister, G.; Schönemann, H.): A Computer Algebra System for Polynomial Computations. Centre for Computer Algebra, University of Kaiserslautern, free software under the GNU General Public Licence (1990-2007). <http://www.singular.uni-kl.de>.