Advanced Studies in Pure Mathematics 68, 2016
School on Real and Complex Singularities in São Carlos, 2012
pp. 171–190

# Algorithms for primary decomposition in Singular

**Hans Schönemann**

**Abstract.**

Gröbner bases are the main computational tool available for algebraic geometry. Building on top of Gröbner bases algorithms for ideal theoretical operations (intersection, quotient, saturation, free resolution,...) will be presented. Combining these algorithms with (multivariate) factorization leads to several algorithms for primary decomposition of ideals.

## §1. Algebraic Sets and Ideals

### 1.1. Ideals in Polynomial Rings

Consider the polynomial ring $R = K[x_1, \dots, x_n]$.

If $T \subset R$ is any subset, all linear combinations $g_1 f_1 + \cdots + g_r f_r$, with $g_1, \dots .g_r \in R$ and $f_r \in T$, form an ideal $\langle T \rangle$ of $R$, called the ideal **generated by** $T$. We also say that $T$ is a **set of generators** for the ideal.

**Hilbert's Basis Theorem** Every ideal of the polynomial ring $K[x_1, \dots, x_n]$ has a finite set of generators.

### 1.2. Algebraic Sets

The **affine** $n$**-space** over $K$ is the set

$$\mathbb{A}^n(K) = \big\{(a_1, \dots, a_n) \mid a_1, \dots, a_n \in K\big\}.$$

**Definition.** If $T \subset R$ is any set of polynomials, its **vanishing locus** in $\mathbb{A}^n(K)$ is the set

$$V(T) = \{p \in \mathbb{A}^n(K) \mid f(p) = 0 \forall f \in T\}.$$

Every such set is called an **affine algebraic set**.

Received January 29, 2013.
Revised July 18, 2013.
2010 *Mathematics Subject Classification.* 14Q99, 13P10, 68W30.

The vanishing locus of a subset $T \subset R$ coincides with that of the ideal $\langle T \rangle$ generated by $T$. So every algebraic set in $\mathbb{A}^n(K)$ is of type $V(I)$ for some ideal $I$ of $R$. By Hilbert's basis theorem, it is the vanishing locus of a set of finitely many polynomials.

The vanishing locus of a single non-constant polynomial is called a **hypersurface** of $\mathbb{A}^n(K)$. According to our definitions, every algebraic set is the intersection of finitely many hypersurfaces.

**Example.** The **twisted cubic curve** in $\mathbb{A}^3(\mathbb{R})$ is obtained by intersecting the hypersurfaces $V(y - x^2)$ and $V(xy - z)$:

Taking vanishing loci defines a map $V$ which sends sets of polynomials to algebraic sets. We summarize the properties of $V$:

**Proposition.**

(i) The map $V$ reverses inclusions: If $I \subset J$ are subsets of $R$, then $V(I) \supset V(J)$.

(ii) Affine space and the empty set are algebraic:

$$V(0) = \mathbb{A}^n(K). \quad V(1) = \emptyset.$$

(iii) The union of finitely many algebraic sets is algebraic: If $I_1, \ldots, I_s$ are ideals of $R$, then

$$\bigcup_{k=1}^{s} V(I_k) = V(\bigcap_{k=1}^{s} I_k).$$

(iv) The intersection of any family of algebraic sets is algebraic: If $\{I_\lambda\}$ is a family of ideals of $R$, then

$$\bigcap_{\lambda} V(I_\lambda) = V\left(\sum_{\lambda} I_\lambda\right).$$

(v) A single point is algebraic: If $a_1, \ldots, a_n \in K$, then

$$V(x_1 - a_1, \ldots, x_n - a_n) = \{(a_1, \ldots, a_n)\}.$$

This proposition allows to deal with ideals of polynomials instead of algebraic sets. The key idea behind Gröbner bases is to reduce problems concerning arbitrary ideals in polynomial rings to problems concerning monomial ideals.

## §**2. Basic definitions for Gröbner bases**

### 2.1. Monomial orderings

The basis ingredient for all Gröbner basis algorithms is the ordering of the monomials (and the concept of the leading term: the term with the highest monomial).

A **monomial ordering** (term ordering) on $K[x_1,\dots,x_n]$ is a total ordering $<$ on the set of monomials (power products) $\{x^\alpha | \alpha \in \mathbf{N}^n\}$ which is compatible with the natural semigroup structure, i.e. $x^\alpha < x^\beta$ implies $x^\gamma x^\alpha < x^\gamma x^\beta$ for any $\gamma \in \mathbf{N^n}$.

An ordering $<$ is called a **wellordering** iff 1 is the smallest monomial. Most of the algorithms work for general orderings.

Robbiano (cf.[R]) proved that any semigroup ordering can be defined by a matrix $A \in GL(n,\mathbf{R})$ as follows (**matrix ordering**):

Let $a_1,\dots,a_k$ be the rows of $A$, then $x^\alpha < x^\beta$ if and only if there is an $i$ with $a_j\alpha = a_j\beta$ for $j < i$ and $a_i\alpha < a_i\beta$. Thus, $x^\alpha < x^\beta$ if and only if $A\alpha$ is smaller than $A\beta$ with respect to the lexicographical ordering of vectors in $\mathbf{R}^n$.

We call an ordering a **degree ordering** if it is given by a matrix with coefficients of the first row either all positive or all negative.

Let $K$ be a field; for $g \in K[\underline{x}]$, $g \neq 0$, let $\mathbf{L(g)}$ be the **leading monomial** with respect to the ordering $<$[1] and $\mathbf{c(g)}$ the coefficient of $L(g)$ in $g$, that is $g = c(g)L(g)+$ smaller terms with respect to $<$.

An ordering $<$ is an **elimination ordering** for $x_{r+1},\dots,x_n$ iff $L(g) \in K[x_1,\dots,x_r]$ implies $g \in K[x_1,\dots,x_r]$).

### 2.2. Examples for monomial orderings

Important orderings for applications are:

- The **lexicographical ordering** *lp*, given by the matrix:

$$\begin{pmatrix} 1 & & & \\ & 1 & & 0 \\ & & \ddots & \\ & 0 & & 1 \end{pmatrix}$$

[1] we write the terms of a polynomial in decreasing order

resp. *ls*:

$$\begin{pmatrix} -1 & & & \\ & -1 & & 0 \\ & & \ddots & \\ & 0 & & -1 \end{pmatrix}$$

**Remark 2.1.** *The positive lexicographic ordering lp on* $K[x_1, \dots, x_n]$ *is an elimination ordering for* $x_1, \dots, x_i$

$$\forall 1 \le i \le n.$$

The definition of rings with these orderings in Singular: (Each line starting with // is a comment in Singular.)

```
ring R1=0,(x(1..5)),lp;
ring R2=0,(x(1..5)),ls;
```

- The **weighted degree reverse lexicographical ordering**, given by the matrix

$$wp : \begin{pmatrix} w_1 & w_2 & \dots & w_n \\ & & & -1 \\ & & \diagup & \\ 0 & -1 & & \end{pmatrix}$$

$w_i > 0 \forall i$, (resp. $ws : w_1 \neq 0, w_i \in \mathbf{Z}\ \forall i$).

If $w_i = 1$ (respectively $w_i = -1$) for all $i$ we obtain the **degree reverse lexicographical ordering, dp** (respectively **ds**).

The definition of rings with these orderings in Singular:

```
ring R3=0,(x(1..5)),wp(2,3,4,5,6);
// correspond to w_i:2,3,4,5,6
ring R4=0,(x(1..5)),ws(2,3,4,5,6);
// correspond to w_i:-2,-3,-4,-5,-6
ring R5=0,(x(1..4)),dp;
ring R6=0,(x(1..4)),ds;
```

- An example for an **elimination ordering** for $x_{r+1}, \dots, x_n$ in $K[\underline{x}] =$ $\mathrm{Loc}_< K[\underline{x}]$ is given by the matrix

$$\begin{pmatrix}
0 & 0 & \dots & 0 & w_{r+1} & w_{r+2} & \dots & w_n \\
w_1 & w_2 & \dots & w_r & 0 & 0 & \dots & 0 \\
 & & & & & & & -1 \\
 & & & & & & \diagup & \\
 & & & & 0 & -1 & & \\
 & & & -1 & & & & \\
 & & \diagup & & & & & \\
0 & -1 & & & & & &
\end{pmatrix}$$

with $w_1 > 0, \dots, w_n > 0$. In $K[x_1, \dots, x_r]_{(x_1, \dots, x_r)}[x_{r+1}, \dots, x_n]$ $=$ $\mathrm{Loc}_< K[\underline{x}]$ it is given by the same matrix with $w_1 < 0, \dots,$ $w_r < 0$ and $w_{r+1} > 0, \dots, w_n > 0$.

The definition of a polynomial ring with an elimination ordering for $x_3$ and $x_4$ in SINGULAR:

```
ring E=0,(x(1..4)),(a(0,0,1,1),a(1,1),dp);
// correspond to w_i=1 for all i, r=2
// or simpler:
ring EE=0,(x(1..4)),(a(0,0,1,1),dp);
```

- The **product ordering**, given by the matrix

$$\begin{pmatrix}
A_1 & & & 0 \\
 & A_2 & & \\
 & & \ddots & \\
0 & & & A_k
\end{pmatrix}$$

if the $A_i$ define orderings on monomials given by the corresponding subsets of $\{x_1, \dots, x_n\}$. Such an ordering can be used to compute in

– $K(\underline{y})[\underline{x}]$ ($A_1$ : dp *on* $\underline{x}$, $A_2$ : dp *on* $\underline{y}$)
– $(K[\underline{y}]_{(\underline{y})})[\underline{x}]$ ($A_1$ : dp *on* $\underline{x}$, $A_2$ : ds *on* $\underline{y}$)
– $(K[\underline{y}])[\underline{x}]_{(\underline{x})}$ ($A_1$ : ds *on* $\underline{x}$, $A_2$ : dp *on* $\underline{y}$)

(See [GTZ], [GP], definition 3.1).

The definition of a ring with this ordering in SINGULAR:

```
ring P=0,(x(1..6)),(dp(4),ds(2));
// correspond to
// a first block of 4 variables with ordering dp
// and a 2nd block of 2 variables with ordering ds
```

## §3. Gröbner bases

**Definition 3.1.** *We define* $\mathbf{Loc_<K[\underline{x}]} := S_<^{-1}K[\underline{x}]$ *to be the localization of* $K[\underline{x}]$ *with respect to the multiplicative closed set* $S_< = \{1+g \mid g = 0$ *or* $g \in K[\underline{x}]\backslash\{0\}$ *and* $1 > L(g)\}$.

**Remark 3.2.** 1) $K[\underline{x}] \subseteq \mathrm{Loc}_< K[\underline{x}] \subseteq K[\underline{x}]_{(\underline{x})}$, where $K[\underline{x}]_{(\underline{x})}$ denotes the localization of $K[\underline{x}]$ with respect to the maximal ideal $(x_1, \dots, x_n)$. In particular, $\mathrm{Loc}_< K[\underline{x}]$ is noetherian, $\mathrm{Loc}_< K[\underline{x}]$ is $K[\underline{x}]$–flat and $K[\underline{x}]_{(\underline{x})}$ is $\mathrm{Loc}_< K[\underline{x}]$–flat.

2) If $<$ is a wellordering then $x^0 = 1$ is the smallest monomial and $\mathrm{Loc}_< K[\underline{x}] = K[\underline{x}]$ . If $1 > x_i$ for all $i$, then $\mathrm{Loc}_< K[\underline{x}] = K[\underline{x}]_{(\underline{x})}$.

3) If, in general, $x_1, \dots, x_r < 1$ and $x_{r+1}, \dots, x_n > 1$ then

$$1 + (x_1, \dots, x_r)K[x_1, \dots, x_r] \subseteq S_< \subseteq 1 + (x_1, \dots, x_r)K[\underline{x}] =: S,$$

hence

$$K[x_1, \dots, x_r]_{(x_1,\dots,x_r)}[x_{r+1}, \dots, x_n] \subseteq \mathrm{Loc}_< K[\underline{x}] \subseteq S^{-1}K[\underline{x}].$$

### 3.1. Definition

**Definition 3.3.** 1) $\mathbf{L}(I)$ *denotes the ideal of* $K[\underline{x}]$ *generated by* $\{L(f) | f \in I\}$.

2) $f_1, \dots, f_s \in I$ *is called a* **Gröbner basis** *of* $I$ *if* $\{L(f_1), \dots, L(f_s)\}$ *generates the ideal* $L(I) \subset K[\underline{x}]$.

**Remark 3.4.** *The term Gröbner basis is usually only in the case of well-orderings used, for more general monomial orderings, especially for local orderings,* $f_1, \dots, f_s \in I$ *is called a* **standard basis** *of* $I$

Singular example: A Gröbner basis computation:

```
// define a ring R= (Z/32003)[x,y,z]
ring R = 32003, (x,y,z), dp ;
// define 3 polynomials
poly s1 =x^3*y^2 + 151*x^5*y + 169*x^2*y4
        + 151*x^2*y*z3 + 186*x*y^6 + 169*y^9;
poly s2 =x^2*y^2*z^2 + 3*z^8;
poly s3 =5*x^4*y^2 + 4*x*y^5 + 2x^2*y^2*z^3 + y^7 + 11*x^10;
// define the ideal i generated by s1,s2,s3
ideal i = s1, s2, s3;
// compute standard basis j of i
ideal j = std(i);
// display j;
j;
```

```
=> j[1]=z8+10668x2y2z2
=> j[2]=y9-567xy6+6250x5y+x2y4+6250x2yz3-5681x3y2
=> j[3]=x10-8728y7-2909x2y2z3-11637x4y2-2909xy5
```

### 3.2. Gröbner Bases for Submodules of Free Modules

We consider also **module orderings** $<_m$ on the set of "monomials" $\{x^\alpha e_i\}$ of $K[\underline{x}]^r = \sum_{i=1,\dots,r} K[\underline{x}]e_i$ which are compatible with the ordering $<$ on $K[\underline{x}]$. That is for all monomials $f, f' \in K[\underline{x}]^r$ and $p, q \in K[\underline{x}]$ we have: $f <_m f'$ implies $pf <_m pf'$ and $p < q$ implies $pf <_m qf$.

We now fix an ordering $<_m$ on $K[\underline{x}]^r$ compatible with $<$ and denote it also with $<$. Again we have the notion of coefficient $c(f)$ and leading monomial $L(f)$. $<$ has the important property:

$$\begin{array}{ll} L(qf) = L(q)L(f) & \text{for } q \in K[\underline{x}] \text{ and } f \in K[\underline{x}]^r, \\ L(f+g) \leq \max(L(f), L(g)) & \text{for } f, g \in K[\underline{x}]^r. \end{array}$$

**Definition 3.5.** 1) $\mathbf{L}(I)$ *denotes the submodule of* $K[\underline{x}]^r$ *generated by* $\{L(f) | f \in I\}$.

2) $f_1, \dots, f_s \in I$ *is called a* **Gröbner basis** *of* $I$ *if* $\{L(f_1), \dots, L(f_s)\}$ *generates the submodule* $L(I) \subset K[\underline{x}]^r$.

In SINGULAR submodules of free modules are defined by a set of generators. These sets are of type `module`.

### 3.3. Basic properties of Gröbner Bases

3.3.1. *Ideal membership*

**Definition 3.6.** *A function* $NF : K[\underline{x}]^r \times \{G | G \text{ standardbasis}\} \to K[\underline{x}]^r, (p, G) \mapsto NF(p|G)$, *is called a* **normal form** *if for any* $p \in K[\underline{x}]^r$ *and any* $G$ *the following holds: if* $NF(p|G) \neq 0$ *then* $L(g) \nmid L(NF(p|G))$ *for all* $g \in G$. $NF(g|G)$ *is called the* **normal form of p with respect to G**.

**Lemma 3.7.** $f \in I$ *iff* $NF(f, std(I)) = 0$.

SINGULAR example:

```
//f defines a trimodal singularity for generic moduli
ring R = 0,(x,y),ds;
int a1,a2,a3=random(1,100),random(-100,1),random(1,100);
poly f = (x^2-y^3)*(y+a1*x)*(y+a2*x)*(y+a3*x);
ideal J = jacob(f);
ideal I = f;
// J:I, ideal of the closure of V(J) \ V(I)
ideal Q = quotient(J,I);
//the Hessian of f
```

```
poly Hess = det(jacob(jacob(f)));
//Hess is contained in Q iff NF is 0
reduce(Hess,std(Q));
=> 0
```

3.3.2. *Elimination*

**Lemma 3.8.** *Let $<$ be an elimination order for $y_1, \ldots, y_n$, $R = K[x_1, \ldots, x_r, y_1, \ldots, y_n]$.*
*Then $std(I) \cap K[x_1, \ldots, x_r] = std(I \cap K[x_1, \ldots, x_r])$.*

Singular example:

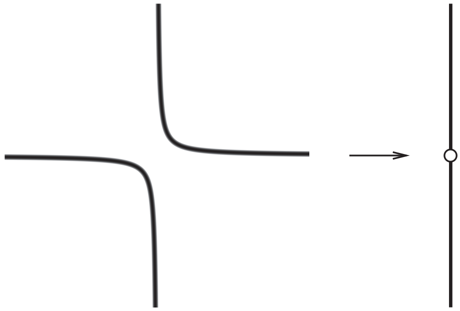
```
//find the equations from a parametrization t->(t^3,t^4,t^5)
ring R=0,(x,y,z,t),dp;
ideal i=x-t^3,
        y-t^4,
        z-t^5;
ideal j=eliminate(i,t);
j;
=> j[1]=y2-xz
=> j[2]=x2y-z2
=> j[3]=x3-yz
```

3.3.3. *Geometry of Elimination* Elimination means geometrically to compute the projection $\pi : V(I) \subset K^n \longrightarrow K^{n-k+1}$.

**Definition.** Let $A \subset \mathbb{A}^n(K)$ and $B \subset \mathbb{A}^m(K)$ be (nonempty) algebraic sets. A map $\varphi : A \to B$ is a **polynomial map**, or a **morphism**, if its components are polynomial functions on $A$. That is, there exist polynomials $f_1, \ldots, f_m \in R$ such that $\varphi(p) = (f_1(p), \ldots, f_m(p))$ for all $p \in A$.

The image of a morphism needs not be an algebraic set.

**Example.** Let $\pi : A^2(R) \to A^1(R)$, $(a, b) \mapsto b$, be projection of the $xy$-plane onto the $y$-axis. Then $\pi$ maps the hyperbola $C = V(xy-1)$ onto the punctured line $\pi(C) = A^1(R) \setminus \{0\}$ which is not an algebraic set.



### 3.3.4. *Hilbert Series*

**Definition 3.9.** *Let $M$ be a graded module over $K[\underline{x}]$. The* **Hilbert series** *of $M$ is the power series*

$$H(M)(t) = \sum_{t=-\infty}^{\infty} dim_K M_i t^i.$$

**Lemma 3.10.** *Let $<$ be a (positive or negative) degree ordering and $H(M)$ the Hilbert function of (the homogenization of) $I$. Then $H(M) = H(L(M))$.*

**Remark 3.11.** *It turns out that $H(M)(t)$ can be written in two useful ways:*

(1) *$H(M)(t) = Q(t)/(1-t)^n$, where $Q(t)$ is a polynomial in $t$ and $n$ its the number of variables in $K[\underline{x}]$.*

(2) *$H(M)(t) = P(t)/(1-t)^{dimM}$ where $P(t)$ is a polynomial and $degM = P(1)$.*

(3) *vector space dimension $dim_K(M) = dim_K(L(M))$.*

**Remark 3.12.** *Let $<$ be a degree ordering.*

- *Krull dimension: $dim(M) = dim(L(M))$.*
- *degree (for a positive degree ordering) resp. multiplicity (for a negative degree ordering) is equal for $M$ and $L(M)$.*

SINGULAR example:

```
// the rational quartic curve J in P^3:
ring R=0,(a,b,c,d),dp;
ideal J=c3-bd2,bc-ad,b3-a2c,ac2-b2d;
// the output of hilb is Q, then P:
hilb(J);
=>// ** J is no standard basis
=>//         1 t^0
=>//        -1 t^2
=>//        -3 t^3
=>//         4 t^4
=>//        -1 t^5
=>
=>//         1 t^0
=>//         2 t^1
=>//         2 t^2
=>//        -1 t^3
=>// dimension (proj.)  = 1
=>// degree (proj.)   = 4
```

### 3.3.5. *Submodule Membership*

**Lemma 3.13.** $(F) \subseteq (G)$ *iff* $NF(F, std(G)) = 0$.

Singular example:

```
ring r=0,(x,y,z),dp;
module F=[x,y],[0,y];
module G=[x,0],[0,y],[0,z];
reduce(F,std(G));
=> _[1]=0
=> _[2]=0
```

### 3.3.6. *Euclidean Algorithm*

**Lemma 3.14.** *If* $<$ *is a wellordering and* $I = \{f, g\} \subseteq K[x]$ *then the computation of the Gröbner basis of* $I$ *yields the greatest common divisor of* $f$ *and* $g$*.*

Singular example:

```
ring R=32003,x,dp;
poly f=(x^3+5)^2*(x-2)*(x^2+x+2)^4;
poly g=(x^3+5)*(x^2-3)*(x^2+x+2);
ideal I=f,g;
std(I);
=>_[1]=x5+x4+2x3+5x2+5x+10
// and the expected result:
(x^3+5)*(x^2+x+2);
=>x5+x4+2x3+5x2+5x+10
```

### 3.3.7. *Gaussian Algorithm*

**Lemma 3.15.** *If* $<$ *is a wellordering and the generators of* `I` *are linear then the computation of the Gröbner basis of* `I` *is a Gaussian algorithm with the columns of* `matrix(I)`*.*

Singular example:

```
ring R=32003,(x,y,z),dp;
ideal I=22*x+77*y+z-3,
         0*x+ 1*y+z-77,
         1*x+ 0*y+z+11;
std(I);
=> _[1]=z-58
=> _[2]=y+z-77
=> _[3]=x+z+11
```

3.3.8. *Kernel of a Ring Homomorphism*

**Lemma 3.16.** *Let $\Phi$ be an affine ring homomorphism*

$$\Phi : R = K[x_1, \dots, x_m]/I \longrightarrow K[y_1, \dots, y_n]/(g_1, \dots, g_s)$$

*given by $f_i = \Phi(x_i) \in K[y_1, \dots, y_n]/(g_1, \dots, g_s)$ , $i = 1, \dots, m$ . Then $Ker(\Phi)$ is generated by*

$$(g_1(\underline{y}), \dots, g_s(\underline{y}) \, , \, (x_1 - f_1(\underline{y})), \dots, (x_m - f_m(\underline{y}))) \cap K[x_1, \dots, x_m]$$

*in $K[x_1, \dots, x_m]/I$ .*

**Remark 3.17.** *For $std(H) \cap R$ use lemma 3.8.*

SINGULAR example:

```
ring r1=32003,(x,y,z,w),lp;
ring r=32003,(x,y,z),dp;
ideal i=x,y,z;
ideal i1=x,y;
ideal i0=0;
map f=r1,i;
setring r1;
ideal i1=preimage(r,f,i1);
i1;
==> i1[1]=w
==> i1[2]=y
==> i1[3]=x
// the kernel of f
preimage(r,f,i0);
==> _[1]=w
// or, use:
kernel(r,f);
==> _[1]=w
```

3.3.9. *Radical Membership*

**Lemma 3.18.** *Let $I \subseteq R = Loc_< K[x_1, \dots, x_n]$, $I$ generated by $F$. $f \in \sqrt{I}$ iff $1 \in std(F + (yf - 1) \subseteq R[y]$.*

3.3.10. *Principal Ideal*

**Lemma 3.19.** *$I = (F)$ is principal (i.e. has a one-element ideal basis) iff $std(F)$ has exactly one element.*

3.3.11. *Trivial Ideal*

**Lemma 3.20.** *$(F)$ is the whole ring $R$ iff $std(F) = \{1\}$.*

3.3.12. *Module Intersection 1*

**Lemma 3.21.** *Let $(F) \subseteq R$ and $(G) \subseteq R$.
Then $std((F) \cap (G)) = std(y(F) + (1-y)(G)) \cap R$ in $R[y]$.*

**Remark 3.22.** *For $std(H) \cap R$ use lemma 3.8.*

Singular example:

```
ring r1 = 32003,(x,y,z),(c,ds);
poly s1=x2y3+45x6y3+68x4z5+80y6x8;
poly s2=6x5+3y6+8z6;
poly s3=12xyz3+2y3z6;
ideal i1=s1,s2,s3;
ideal i2=s1+s2,s2,s1;
intersect(i1,i2);
=>_[1]=6x5+x2y3+3y6+8z6+45x6y3+68x4z5+80x8y6
=>_[2]=6x5+3y6+8z6
=>_[3]=x2y3+45x6y3+68x4z5+80x8y6
```

## §4. Syzygies

### 4.1. Definition

**Definition 4.1.** *Let $I = \{g_1, \ldots, g_q\} \subseteq K[\underline{x}]^r$.
The* **module of syzygies syz***(I) is ker $(K[\underline{x}]^q \to K[\underline{x}]^r, \sum w_i e_i \mapsto \sum w_i g_i)$.*

**Lemma 4.2.** *The module of syzygies of I is*

$$(g_1(\underline{x}) - e_{r+1}, \ldots, g_q(\underline{y}) - e_{r+q}) \cap \{0\}^r \times K[\underline{x}]^q$$

*in $(K[x_1, \ldots, x_m]/J)^q$ .*

**Remark 4.3.** *Use a module ordering with $e_i > e_j \forall i \leq r < j$ and the elimination property of lemma 3.8.*

Singular example:

```
ring R=0,(x,y,z),(c,dp);
ideal I=maxideal(1);
// the syzygies of the (x,y,z)
syz(I);
=>_[1]=[0,z,-y]
=>_[2]=[z,0,-x]
=>_[3]=[y,-x]
// syz yields a generating set for the module of syzygies
// but may not be a standard basis !
```

### 4.2. Free Resolutions

Iterating the `syz` command yields a free resolution of a module or ideal. SINGULAR does this if the `res` or `mres` command is used.

Another algorithm due to Schreyer is presented in [S]. It is be used by the `sres` command.
SINGULAR example:

```
ring r=0,(x,y,z),dp;
ideal I=x,y,z;
list Ir=res(I,0);
// print the results:
Ir;
=>[1]:
=>   _[1]=z
=>   _[2]=y
=>   _[3]=x
=>[2]:
=>   _[1]=-y*gen(1)+z*gen(2)
=>   _[2]=-x*gen(1)+z*gen(3)
=>   _[3]=-x*gen(2)+y*gen(3)
=>[3]:
=>   _[1]=x*gen(1)-y*gen(2)+z*gen(3)
```

### 4.3. Kernel of a Module Homomorphism

**Definition 4.4.** *Let* $R = K[x_1, \dots, x_n]/(h_1, \dots, h_p)$ , $A \in Mat(m \times r, R)$ *and* $B \in Mat(m \times s, R)$ *then define*

$$\mathbf{modulo}(\mathbf{A}, \mathbf{B}) := ker(R^r \xrightarrow{A} R^m/Im(B))$$

*(*$modulo(A, B)$ *is the preimage of* $B$ *under the homomorphism given by* $A$*.)*

**Lemma 4.5.** *Let* $\{\, (\underline{\alpha}_i, \underline{\beta}_i, \underline{\gamma}_i) \mid i = 1, \dots, k \,\} \subset R^{r+s+p} =: R^N$ *be a generating set of* $syz(D)$ *where*

$$C = \begin{pmatrix} h_1 & \cdots & h_p & 0 & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & h_1 & \cdots & h_p & 0 & \cdots & \cdots \\ \vdots & & & & & & & & \vdots \\ 0 & \cdots & \cdots & \cdots & \cdots & \cdots & h_1 & \cdots & h_p \end{pmatrix}$$

$$\in Mat(m \times pm, R)$$

*and*

$$D = \left(\begin{array}{ccc|ccc|ccc} a_{11} & \cdots & a_{1r} & b_{11} & \cdots & b_{1s} & c_{11} & \cdots & c_{1,pm} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ a_{m1} & \cdots & a_{mr} & b_{m1} & \cdots & b_{ms} & c_{m1} & \cdots & c_{m,pm} \end{array}\right)$$

$$\in Mat(m \times r + s + pm, R)$$

*Then*

$$modulo\,(A, B) := (\,\alpha_1 \ldots \alpha_k\,) \in Mat(r \times k, R)$$

*(see Lemma 4.2.)*

**Remark 4.6.** *In practice, one need not compute the entire syzygy module of D: it is better to find modulo(A,B) as:*

$$\left(\begin{array}{ccc|ccc|ccc} a_{11} & \cdots & a_{1r} & b_{11} & \cdots & b_{1s} & c_{11} & \cdots & c_{1,pm} \\ \vdots & & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ a_{m1} & \cdots & a_{mr} & b_{m1} & \cdots & b_{ms} & c_{m1} & \cdots & c_{m,pm} \\ 1 & & 0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & \ldots & 0 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & & 1 & 0 & \cdots & \cdots & \cdots & \cdots & 0 \end{array}\right) \cap \begin{pmatrix} 0 \\ \vdots \\ 0 \\ R \\ \vdots \\ R \end{pmatrix}$$

*(see Sections 4.2, 3.8.)*

### 4.4. Module intersection 2

Let $R$ be an affine ring, and let $I, J, K \subseteq R$ be ideals. One can compute generators for the intersection $L = I \cap J \cap K$ in the following way: $L$ is the kernel of the $R$-module homomorphism $\phi : R \to R/I \oplus R/J \oplus R/K$ which sends 1 to (1,1,1).

**Lemma 4.7.**

$$I \cap J \cap K = modulo(\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} I & 0 & 0 \\ 0 & J & 0 \\ 0 & 0 & K \end{pmatrix}).$$

### 4.5. Ideal Quotient

**Lemma 4.8.** *The quotient $(I : J)$ of two ideals $I = (a_1, \ldots, a_r)$ and $J = (b_1, \ldots, b_s)$ in $R$ is the kernel of the map*

$$\begin{array}{ccc} R & \longrightarrow & R/I \oplus \ldots \oplus R/I \\ 1 & \longmapsto & (b_1, \ldots, b_s) \end{array}$$

*It can be computed as*

$$(I : J) = modulo\left((b_1|\ldots|b_s)^T,\ (a_1|\ldots|a_r) \oplus \ldots \oplus (a_1|\ldots|a_r)\right)$$

### 4.6. Saturation

The saturation $(I : J)^\infty$ of I with respect J can be computed by computing $(I : J), ((I : J) : J), \ldots$ until it stabilizes.

### 4.7. Annihilator of a Module

**Lemma 4.9.** *Let* $R = Loc_< K[x_1, \ldots, x_n]/(h_1, \ldots, h_p)$ , $M \subseteq R^m$. $Ann_R(R^m/M) := \{\, g \in R \,|\, gR^m \subset M \,\}$ *is generated by first entries of syzygies of the module*

$$\left(\begin{array}{c|c|c|c|c} e_1 & M & 0 & \cdots & 0 \\ e_2 & 0 & M & \ddots & \vdots \\ \vdots & \vdots & \ddots & \ddots & 0 \\ e_m & 0 & \cdots & 0 & M \end{array}\right)$$

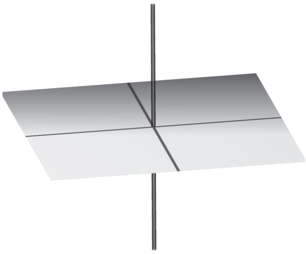
*where* $e_i$ *is the i-th unit vector in* $R^m$*.*
*(We identify a matrix with the module generated by it columns.)*

## §5. Primary Decomposition

### 5.1. Motivation: Decomposition of Algebraic Sets

**Example**

```
ring R=0,(x,y,z),dp;
ideal K=yz,xz;
LIB "primdec.lib";
primdecGTZ(K);
=>_[1][1]=z
=>_[1][2]=z
=>_[2][1]=x,y
=>_[2][2]=x,y
```



### 5.2. Definition.

A proper ideal $Q$ of a ring $R$ is said to be **primary** if $f, g \in R$, $fg \in Q$ and $f \notin Q$ implies $g \in \sqrt{Q}$. In this case, $P = \sqrt{Q}$ is a prime ideal, and $Q$ is also said to be a $P$**-primary ideal**. Given any ideal $I$ of $R$, a **primary decomposition** of $I$ is an expression of $I$ as an intersection of finitely many primary ideals.

Now suppose that $R$ is Noetherian. Then every proper ideal $I$ of $R$ has a primary decomposition. We can always achieve that such a decomposition $I = \bigcap_{i=1}^r Q_i$ is **minimal**. That is, the prime ideals $P_i = \sqrt{Q_i}$ are all distinct and none of the $Q_i$ can be left out. In this case, the $P_i$ are uniquely determined by $I$ and are referred to as the **associated primes** of $I$. If $P_i$ is minimal among $P_1, \ldots, P_r$ with respect to inclusion, it is called a **minimal associated prime** of $I$.

The minimal associated primes of $I$ are precisely the minimal prime ideals containing $I$. Their intersection is equal to $\sqrt{I}$. Every primary ideal occurring in a minimal primary decomposition of $I$ is called a **primary component** of $I$. The component is said to be **isolated** if its radical is a minimal associated prime of $I$. Otherwise, it is said to be **embedded**. The isolated components are uniquely determined by $I$, the others are far from being unique.

From the definitions, it is clear that there is a number of different tasks coming with primary decomposition. These range from computing radicals via computing the minimal associated primes to computing a full primary decomposition. A variety of corresponding algorithms is implemented in the SINGULAR library `primdec.lib`. The two main algorithms for computing a full primary decomposition are `primdecSY` and `primdecGTZ`. A detailed description is given in [DGP].

### 5.3. Computational Primary Decomposition: History of Algorithms

First approaches for algorithms to compute the primary decomposition of polynomial ideals were given by Grete Herrmann (1926): generic projections, computed via resultants, reduce the task to the case of hypersurfaces (i.e. the case of principal ideals). The case of principal ideals was handled by factoring polynomials.

A more modern algorithm was proposed by Wu in Maple (Wu-Ritt-process, 1989): compute the set of all minimal associated primes via characteristic sets, and use Gröbner base techniques for saturation steps (see "Algorithm of Shimoyama-Yokoyama" (SY) below).

The algorithm by Gianni,Trager,Zacharias in AXIOM (1988) via factorization is the basis of `primdecGTZ` in SINGULAR, which reduces to the zerodimensional case (via Gröbner bases for projection) and handles this case by polynomial factorization.

The algorithm by Eisenbud, Huneke, Vasconcelos (1992) avoids the time consuming elimination and decomposes into equidimensional parts.

Singular implements GTZ, SY (1998), EHV (2001) in the libraries `primdec.lib` and `ehv.lib`.

### 5.4. Computational Primary Decomposition by the Algorithm of Gianni, Trager, Zacharias

The starting point of the GTZ-algorithm is the following simple observation:

**Lemma (Splitting Tool).** If $I \subset R$ is an ideal, if $h \in R$ is a polynomial, and if $m \geq 1$ is an integer such that $I : \langle h \rangle^\infty = I : \langle h \rangle^m$, then

$$I = \big(I : \langle h \rangle^m\big) \cap \langle I, h^m \rangle \,.$$

The key result on which the algorithm is based specifies which polynomials $h$ are considered:
If $I : f = I : f^2$ for some $f$, then $I = (I : f) \cap (I, f)$.
If $fg \in I$ and $(f, g) = R$, then $I = (I, f) \cap (I, g)$.
If $fg \in I$, then $\sqrt{I} = \sqrt{(I, f)} \cap \sqrt{(I, g)}$.
If $f^r \in I$, then $\sqrt{I} = \sqrt{(I, f)}$.
If $J \subseteq R$ an ideal, then $\sqrt{I} = \sqrt{I : J} \cap \sqrt{I + J} = \sqrt{I : J} \cap \sqrt{I : (I : J)}$.

5.4.1. *Primary Decomposition: Reduction to Dimension 0*

**Proposition** Let $I \subsetneq K[\underline{x}] = R$ be a proper ideal, and let $\underline{u} \subset \underline{x}$ be a subset of maximal cardinality such that $I \cap K[\underline{u}] = \{0\}$. Then:

- The ideal $I\,K(\underline{u})[\underline{x} \setminus \underline{u}] \subset K(\underline{u})[\underline{x} \setminus \underline{u}]$ is zero-dimensional.
- Let $> = (>_{\underline{x} \setminus \underline{u}}, >_{\underline{u}})$ be a global product ordering on $K[\underline{x}]$, and let $G$ be a Gröbner basis for $I$ with respect to $>$. Then $G$ is a Gröbner basis for $I\,K(\underline{u})[\underline{x} \setminus \underline{u}]$ with respect to the monomial ordering obtained by restricting $>$ to the monomials in $K[\underline{x} \setminus \underline{u}]$. Further, if $h \in K[\underline{u}]$ is the least common multiple of the leading coefficients of the elements of $G$ (regarded as polynomials in $K(\underline{u})[\underline{x} \setminus \underline{u}]$), then

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

- All primary components of the ideal $I\,K(\underline{u})[\underline{x} \setminus \underline{u}] \cap K[\underline{x}]$ have the same dimension, namely $\dim I$.
  Further, if $I\,K(\underline{u})[\underline{x} \setminus \underline{u}] = Q_1 \cap \ldots \cap Q_r$ is the minimal primary decomposition, then

$$I\,K(\underline{u})[\underline{x} \setminus \underline{u}] \cap K[\underline{x}] = (Q_1 \cap K[\underline{x}]) \cap \ldots \cap (Q_r \cap K[\underline{x}])$$

  is the minimal primary decomposition, too.

If $>$ is a global monomial ordering on $K[\underline{x}]$, then every subset $\underline{u} \subset \underline{x}$ of maximal cardinality satisfying $L_>(I) \cap K[\underline{u}] = \{0\}$ is also a subset of maximal cardinality such that $I \cap K[\underline{u}] = \{0\}$.

By recursion, the proposition allows us to reduce the general case of primary decomposition to the zero-dimensional case. In turn, if $I \subset K[\underline{x}]$ is a zero-dimensional ideal “in general position” (with respect to the lexicographic order satisfying $x_1 > \cdots > x_n$), and if $h_n$ is a generator for $I \cap K[x_n]$, the minimal primary decomposition of $I$ is obtained by factorizing $h_n$. In characteristic zero, the condition that $I$ is in general position can be achieved by means of a generic linear coordinate transformation

5.4.2. *Zero-dimensional Primary Decomposition* The lexicographical Gröbner basis of a zero-dimensional ideal $I$ contains one polynomial $f$ of only the last variable. Let $f_1^{\alpha_1} .... f_r^{\alpha_r} = f$ the decomposition of $f$ in irreducible factors.

Then the minimal primary decomposition of $I$ is given by

$$I = \cap_{k=1}^{r} (I, f_k^{\alpha_k})$$

### 5.5. Computational Primary Decomposition by the Algorithm of Eisenbud, Huneke, Vasconcelos

The algorithm by Eisenbud, Huneke, Vasconcelos avoids the time consuming elimination and decomposes into equidimensional parts Its main splitting tools is (cf. [EHV])

**Proposition.** If $I \subseteq R = K[x_1, ..x_n]$ is an ideal, then the equidimensional hull of $I$ $E(I)$ is $AnnExt_R^{n-d}(R/I, R)$, where $d = dim(I)$.

### 5.6. Computational Primary Decomposition by Characteristic Series

5.6.1. *Characteristic Series* Let $<$ be the lexicographical ordering on $R = K[x_1, ..., x_n]$ with $x_1 < ... < x_n$. For $f \in R$ let lvar$(f)$ (the leading variable of $f$) be the largest variable in $f$, i.e., if $f = a_s(x_1, ..., x_{k-1})x_k^s + ... + a_0(x_1, ..., x_{k-1})$ for some $k \leq n$ then lvar$(f) = x_k$.

Moreover, let ini$(f) := a_s(x_1, ..., x_{k-1})$. The pseudo remainder $r =$ prem$(g, f)$ of $g$ with respect to $f$ is defined by the equality ini$(f)^a \cdot g = qf + r$ with $\deg_{lvar(f)}(r) < \deg_{lvar(f)}(f)$ and $a$ minimal. A set $T = \{f_1, ..., f_r\} \subset R$ is called triangular if lvar$(f_1) < ... <$ lvar$(f_r)$. Moreover, let $U \subset T$, then $(T, U)$ is called a triangular system, if $T$ is a triangular set such that ini$(T)$ does not vanish on $V(T) \setminus V(U) (=: V(T \setminus U))$.

$T$ is called irreducible if for every $i$ there are no $d_i$,$f_i'$,$f_i''$ such that

$$\text{lvar}(d_i) < \text{lvar}(f_i) = \text{lvar}(f_i') = \text{lvar}(f_i''),$$

$$0 \notin \text{prem}(\{d_i, \text{ini}(f_i'), \text{ini}(f_i'')\}, \{f_1, ..., f_{i-1}\}),$$

$$\text{prem}(d_i f_i - f_i' f_i'', \{f_1, ..., f_{i-1}\}) = 0.$$

Furthermore, $(T, U)$ is called irreducible if $T$ is irreducible.

The main result on triangular sets is the following:

Let $G = \{g_1, ..., g_s\} \subset R$, then there are irreducible triangular sets $T_1, ..., T_l$ such that $V(G) = \bigcup_{i=1}^{l} (V(T_i \setminus I_i))$ where $I_i = \{\text{ini}(f) \mid f \in T_i\}$.

Such a set $\{T_1, ..., T_l\}$ is called an **irreducible characteristic series** of the ideal $(G)$.
SINGULAR example:

```
ring R= 0,(x,y,z,u),dp;
ideal i=-3zu+y2-2x+2,
        -3x2u-4yz-6xz+2y2+3xy,
        -3z2u-xu+y2z+y;
print(char_series(i));
=>_[1,1],3x2z-y2+2yz,3x2u-3xy-2y2+2yu,
=>x,     -y+2z,      -2y2+3yu-4
char_series(i);
=>_[1,1]=-9x4y2+18x5-12x2y3-18x4+24x3y+9xy3+2y4
         -24x2y+8xy2-8y2
=>_[1,2]=3x2z-y2+2yz
=>_[1,3]=3x2u-3xy-2y2+2yu
=>_[2,1]=x
=>_[2,2]=-y+2z
=>_[2,3]=-2y2+3yu-4
```

5.6.2. *Algorithm of Shimoyama-Yokoyama* The SY algorithm (cf [SY])

- computes the set of all minimal associated primes $\{P_1, ..., P_l\}$ of the ideal $I$,
- computes pseudo primary components $Q'_i$ and a remaining ideal $(f_1^{e_1}, ..., f_l^{e_l})$ with $\sqrt{Q'_i} = P_i$ and $I = Q'_1 \cap ... \cap Q'_l \cap (I + (f_1^{e_1}, ..., f_l^{e_l}))$,
- decomposes all pseudo primary components $Q'_i$ into a primary component $Q_i$ and a remaining ideal $I'_i$, s.t. $Q'_i = Q_i \cap I'_i$,
- decomposes the remaining ideals $I'_i, I + (f_1^{e_1}, ..., f_l^{e_l})$ by applying SY recursively.

### 5.7. Preprocessing: Factorizing Buchberger Algorithm

The factorizing Buchberger algorithm is the combination of Buchberger algorithm with factorization: each new element for the Gröbner basis will be factorized, and, if reducible, used to split the computation into several branches corresponding to the factors. Applied to an ideal $I = (f_1, ..., f_s)$ it computes a list of Gröbner bases $G_1, ..., G_r$ such that

$$V(I) = V(G_1) \cup ... \cup V(G_r).$$

The $V(G_i)$ need not be irreducible, so this algorithm is mainly used as a preprocessing step. See [C].

## References

[BW] Becker, T.; Weispfenning, V.: Gröbner Bases. A computational approach to commutative algebra. Springer–Verlag GTM 141 (1991).

[B1] Buchberger, B.: Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal. Thesis, Univ. Innsbruck, 1965.

[CLO] Cox, D; Little, J.; O'Shea, D.: Ideals, Varieties and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra. Springer 1992.

[C] Czapor, S.R.: Solving algebraic equations: Combining Buchberger's algorithm with multivariate factorization. J. Symb. Comp. 7(1), 49-53, 1998.

[DGP] Decker, W.; Greuel, G.-M.;Pfister, G.: Primary decomposition: algorithms and comparisons. Gert-Martin Greuel, B. H. Matzat, G. Hiss: Algorithmic Algebra and Number Theory (Springer), 187-220, 1998.

[DGPS] Decker, W.; Greuel, G.-M.; Pfister, G.; Schönemann, H.: SINGULAR 3-1-6 — A computer algebra system for polynomial computations. http://www.singular.uni-kl.de (2012).

[DL] Decker, W.;Lossen, C.: Computing in Algebraic Geometry - A Quick Start using Singular Springer Verlag, 2005, ACM 16.

[E] Eisenbud, D.: Commutative Algebra with a view toward Algebraic Geometry. GTM 150 Springer, 1995.

[EHV] Eisenbud, D.; Huneke, C.; Vasconcelos, W.: Direct Methods for Primary Decomposition. Invent. Math. 110, 207-235 (1992).

[GTZ] Gianni, P.; Trager, B.;Zacharias, G.: Gröbner bases and Primary Decomposition of Polynomial Ideals. Journal of Symbolic Computation. 1985.

[GP] Greuel, G.-M.; Pfister, G.: A Singular Introduction to Commutative Algebra. with contributions by Olaf Bachmann, Christoph Lossen, and Hans Schönemann. Springer Verlag, 2002, Second edition 2007

[R] Robbiano, L.: Termorderings on the polynomial ring. Proceedings of EUROCAL 85, Lecture Notes in Computer Science **204**, 513–517 (1985).

[S] Schreyer, F.-O.: A standard basis approach to syzygies of canonical curves. J. reine angew. Math. **421**, 83-123 (1991).

[SY] Shimoyama, T.; Yokoyama, K.: Localization and Primary Decomposition of Polynomial ideals. J. Symb. Comp. 22, 247-277 (1996).

[St1] Stillman, M.: Methods for computing in algebraic geometry and commutative algebra. Acta Applicandae Mathematicae 21(77-103) 1990.

*University of Kaiserslautern*
*Department of Mathematics*
*D-67653 Kaiserslautern*
*Germany*
*E-mail address*: hannes@mathematik.uni-kl.de