4. Primary Decomposition and Related Topics

4.1 The Theory of Primary Decomposition

It is well–known that every integer is a product of prime numbers, for instance $10 = 2 \cdot 5$. This equation can also be written as an equality of ideals, $\langle 10 \rangle = \langle 2 \rangle \cap \langle 5 \rangle$ in the ring $\mathbb{Z}$. The aim of this section is to generalize this fact to ideals in arbitrary Noetherian rings.

Ideals generated by prime elements are prime ideals. Therefore, $\langle 10 \rangle$ is the intersection of finitely many prime ideals. In Proposition 3.3.5 this is generalized to radical ideals: in a Noetherian ring every radical ideal I, that is, $I = \sqrt{I}$, is the intersection of finitely many prime ideals. However, what can we expect if the ideal is not radical? For example, $20 = 2^2 \cdot 5$, respectively $\langle 20 \rangle = \langle 2 \rangle^2 \cap \langle 5 \rangle$; in the ring of integers $\mathbb{Z}$ every ideal is the intersection of finitely many ideals which are powers of prime ideals. This is, for arbitrary Noetherian rings, no longer true. A generalization of the powers of prime ideals are the so–called primary ideals. We shall prove in this section that, in a Noetherian ring, every ideal is the intersection of finitely many primary ideals.

Definition 4.1.1. Let A be a Noetherian ring, and let $I \subset A$ be an ideal.

(1) The set of *associated primes* of I, denoted by $\mathrm{Ass}(I)$, is defined as

$$\mathrm{Ass}(I) = \big\{ P \subset A \;\big|\; P \text{ prime}, P = I : \langle b \rangle \text{ for some } b \in A \big\} \,.$$

Elements of $\mathrm{Ass}(\langle 0 \rangle)$ are also called *associated primes* of A.

(2) Let $P, Q \in \mathrm{Ass}(I)$ and $Q \subsetneq P$, then P is called an *embedded prime ideal* of I. We define $\mathrm{Ass}(I, P) := \{Q \mid Q \in \mathrm{Ass}(I), Q \subset P\}$.

(3) I is called *equidimensional* or *pure dimensional* if all associated primes of I have the same dimension.

(4) I is a *primary ideal* if, for any $a, b \in A$, $ab \in I$ and $a \notin I$ imply $b \in \sqrt{I}$. Let P be a prime ideal, then a primary ideal I is called P*–primary* if $P = \sqrt{I}$.

(5) A *primary decomposition* of I, that is, a decomposition $I = Q_1 \cap \cdots \cap Q_s$ with Q_i primary ideals, is called *irredundant* if no Q_i can be omitted in the decomposition and if $\sqrt{Q_i} \neq \sqrt{Q_j}$ for all $i \neq j$.

Example 4.1.2.

(1) Let A be a ring, and let $I \subset A$ be an ideal such that $\sqrt{I}$ is a maximal ideal, then I is primary (cf. Exercise 4.1.4).
(2) Let $A = K[x, y]$ and $I = \langle x^2, xy\rangle = \langle x\rangle \cap \langle x, y\rangle^2 = \langle x\rangle \cap \langle x^2, y\rangle$. Then $\langle x\rangle$, $\langle x, y\rangle^2$, $\langle x^2, y\rangle$ are primary ideals, and $\mathrm{Ass}(I) = \{\langle x\rangle, \langle x, y\rangle\}$. In particular, $\langle x, y\rangle$ is an embedded prime of I with $\mathrm{Ass}(I, \langle x, y\rangle) = \{\langle x\rangle, \langle x, y\rangle\}$, while $\mathrm{Ass}(I, \langle x\rangle) = \{\langle x\rangle\}$. Note that both decompositions are irredundant primary decompositions of I, which shows that an irredundant primary decomposition might be *not unique*.
(3) $\mathrm{minAss}(I) \subset \mathrm{Ass}(I)$ and $\mathrm{minAss}(I) = \mathrm{Ass}(I)$ if and only if I has no embedded primes (Exercise 4.1.5), showing that $\mathrm{minAss}(I)$ is the set of minimal elements (with respect to inclusion) of $\mathrm{Ass}(I)$.

The following lemma collects the properties of primary ideals needed for the primary decomposition.

Lemma 4.1.3. *Let A be a Noetherian ring and $Q \subset A$ a P–primary ideal.*

(1) The radical of a primary ideal is a prime ideal.
(2) Let Q' be a P–primary ideal, then $Q \cap Q'$ is a P–primary ideal.
(3) Let $b \in A$, $b \notin Q$, then $Q : \langle b\rangle$ is P–primary. If $b \in P$ then $Q \subsetneq Q : \langle b\rangle$.
(4) Let $P' \supset Q$ be a prime ideal, then $QA_{P'} \cap A = Q$.
(5) There exists $d \in A$ such that $P = Q : \langle d\rangle$. Especially, $P \in \mathrm{Ass}(Q)$.

Proof. (1) and (2) are left as exercises. To prove (3), let $b \in A$, $b \notin Q$. If $b \notin P$, then $Q : \langle b\rangle = Q$ because $ab \in Q$, $a \notin Q$ implies $b \in P$ by definition of a primary ideal. If $b \in P$ then $b^n \in Q$ for a suitable n. We may assume $n \geq 2$ and $b^{n-1} \notin Q$. Then $b^{n-1} \in Q : \langle b\rangle$ and, therefore, $Q \subsetneq Q : \langle b\rangle$. Let $xy \in Q : \langle b\rangle$ and $x \notin Q : \langle b\rangle$. This implies $bxy \in Q$ and $bx \notin Q$. By definition of a primary ideal, we obtain $y^n \in Q$ for a suitable n. This implies that $Q : \langle b\rangle$ is a primary ideal. Finally, $\sqrt{Q : \langle b\rangle} \supset \sqrt{Q} = P$. Let $x \in \sqrt{Q : \langle b\rangle}$, that is, $bx^n \in Q$ for some n but $b \notin Q$ and, therefore, $x^n \in P$. Now P is prime and we obtain $x \in P$ which proves $\sqrt{Q : \langle b\rangle} = P$.

To prove (4), let $x \in QA_{P'} \cap A$. This means that $sx \in Q$ for a suitable $s \notin P'$. If $x \notin Q$, then, by definition of a primary ideal, $s \in \sqrt{Q} \subset P'$ in contradiction to the choice of s. We obtain $QA_{P'} \cap A \subset Q$. The other inclusion is trivial.

To prove (5), we consider first the case $Q = P$. In this case, we can use $d = 1$ and are finished. If $Q \subsetneq P$ we choose $g_1 \in P \setminus Q$ and obtain, using (3), that $Q : \langle g_1\rangle \supsetneq Q$ is P–primary and $\sqrt{Q : \langle g_1\rangle} = P$. Again, if $Q : \langle g_1\rangle \subsetneq P$ we can choose $g_2 \in P \setminus (Q : \langle g_1\rangle)$ such that $(Q : \langle g_1\rangle) : \langle g_2\rangle \supsetneq Q : \langle g_1\rangle$. Now $(Q : \langle g_1\rangle) : \langle g_2\rangle = Q : \langle g_1 g_2\rangle$ (Exercise 4.1.2), and continuing in this way we obtain an increasing chain of ideals $Q \subsetneq Q : \langle g_1\rangle \subsetneq Q : \langle g_1 g_2\rangle \subsetneq \dots$. The ring A is Noetherian and, therefore, this chain has to stop, that is, we find n and $g_1, \dots, g_n \in P$ such that $Q : \langle g_1 \cdots g_n\rangle = P$. $\square$

Theorem 4.1.4. *Let A be a Noetherian ring and $I \subset A$ be an ideal, then there exists an irredundant decomposition $I = Q_1 \cap \cdots \cap Q_r$ of I as intersection of primary ideals $Q_1, \ldots, Q_r$.*

Proof. Because of Lemma 4.1.3 (2) it is enough to prove that every ideal is the intersection of finitely many primary ideals. Suppose this is not true, and let $\mathfrak{M}$ be the set of ideals which are not an intersection of finitely many primary ideals. The ring A is Noetherian and, by Proposition 1.3.6, $\mathfrak{M}$ has a maximal element with respect to the inclusion. Let $I \in \mathfrak{M}$ be maximal. Since I is not primary, there exist $a, b \in A$, $a \notin I$, $b^n \notin I$ for all n and $ab \in I$. Now consider the chain $I : \langle b \rangle \subset I : \langle b^2 \rangle \subset \cdots$. As A is Noetherian, there exists an n with $I : \langle b^n \rangle = I : \langle b^{n+1} \rangle = \cdots$. Using Lemma 3.3.6, we obtain $I = (I : \langle b^n \rangle) \cap \langle I, b^n \rangle$. Since $b^n \notin I$ we have $I \subsetneq \langle I, b^n \rangle$. Since $a \notin I$ and $ab^n \in I$ we have $I \subsetneq I : \langle b^n \rangle$. As I is maximal in $\mathfrak{M}$, $I : \langle b^n \rangle$ and $\langle I, b^n \rangle$ are not in $\mathfrak{M}$. This implies that both ideals are intersections of finitely many primary ideals and, therefore, I is an intersection of finitely many primary ideals, too, in contradiction to the assumption. □

Theorem 4.1.5. *Let A be a ring and $I \subset A$ be an ideal with irredundant primary decomposition $I = Q_1 \cap \cdots \cap Q_r$. Then $r = \# \operatorname{Ass}(I)$,*

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

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

Proof. Let $I = Q_1 \cap \cdots \cap Q_r$ be an irredundant primary decomposition. If $P \in \operatorname{Ass}(I)$, $P = I : \langle b \rangle$ for a suitable b, then $P = (Q_1 : \langle b \rangle) \cap \cdots \cap (Q_r : \langle b \rangle)$ (Exercise 4.1.3). In particular, $\bigcap_{i=1}^{r}(Q_i : \langle b \rangle) \subset P$, hence, $Q_j : \langle b \rangle \subset P$ for a suitable j (Lemma 1.3.12). On the other hand, since $P = I : \langle b \rangle \subset Q_j : \langle b \rangle$, we obtain $P = Q_j : \langle b \rangle$. Now $Q_j : \langle b \rangle \subset \sqrt{Q_j}$ (Lemma 4.1.3 (3)), which implies $P = \sqrt{Q_j}$. This proves that $\{\sqrt{Q_1}, \ldots, \sqrt{Q_r}\} \supset \operatorname{Ass}(I)$.

It remains to prove that $\sqrt{Q_i} = I : \langle b_i \rangle$ for a suitable b_i. But this is a consequence of Lemma 4.1.3 (5): let $J = Q_1 \cap \cdots \cap Q_{i-1} \cap Q_{i+1} \cap \cdots \cap Q_r$, then $J \not\subset Q_i$, since the decomposition is irredundant. We can choose $d \in J \setminus Q_i$ and obtain, using Exercise 4.1.3, $I : \langle d \rangle = Q_i : \langle d \rangle$. By Lemma 4.1.3 (3), (5), respectively Exercise 4.1.2, $\sqrt{Q_i} = \sqrt{Q_i : \langle d \rangle} = (Q_i : \langle d \rangle) : \langle g \rangle = I : \langle dg \rangle$ for a suitable g. We obtain $\operatorname{Ass}(I) = \{\sqrt{Q_1}, \ldots, \sqrt{Q_r}\}$.

Now let $\operatorname{Ass}(I, P) = \{\sqrt{Q_{i_1}}, \ldots, \sqrt{Q_{i_s}}\}$, then Lemma 4.1.3 (4) gives that $Q_{i_\nu} A_P \cap A = Q_{i_\nu}$. If $j \notin \{i_1, \ldots, i_s\}$ then $Q_j \not\subset P$, therefore, $Q_j A_P = A_P$. This implies that $IA_P \cap A = \bigcap_{j=1}^{r}(Q_j A_P \cap A) = Q_{i_1} \cap \cdots \cap Q_{i_s}$ is independent of the decomposition, since $\operatorname{Ass}(I, P)$ is. □

Example 4.1.6.

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

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

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

(2) Let $I = \langle xy, xz, yz \rangle = \langle x, y \rangle \cap \langle x, z \rangle \cap \langle y, z \rangle \subset K[x, y, z]$. Then the zero–set $V(I)$ (cf. A.1) is the union of the coordinate axes (cf. Figure 4.1).

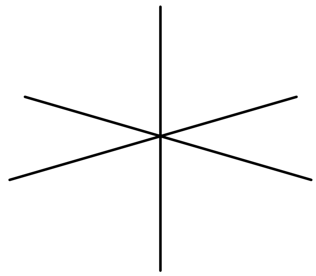

Fig. 4.1. The zero–set of $\langle xy, xz, yz \rangle$.

(3) Let $I = \langle (y^2 - xz) \cdot (z^2 - x^2 y),\ (y^2 - xz) \cdot z \rangle \subset K[x, y, z]$. Then we obtain the irredundant primary decomposition $I = \langle y^2 - xz \rangle \cap \langle x^2, z \rangle \cap \langle y, z^2 \rangle$, $\mathrm{Ass}(I) = \{\langle y^2 - xz \rangle, \langle x, z \rangle, \langle y, z \rangle\}$ and $\mathrm{minAss}(I) = \{\langle y^2 - xz \rangle, \langle x, z \rangle\}$. $\langle y, z \rangle$ is an embedded prime with $\mathrm{Ass}(I, \langle y, z \rangle) = \{\langle y^2 - xz \rangle, \langle y, z \rangle\}$. The zero–set of I (cf. A.1) is displayed in Figure 4.2.

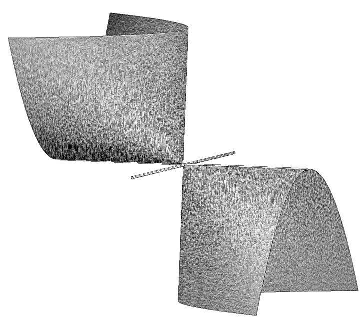

Fig. 4.2. The zero–set of $I = \langle y^2 - xz \rangle \cap \langle x^2, z \rangle \cap \langle y, z^2 \rangle$.

Remark 4.1.7.

(1) Primary decomposition does not hold, in general, in non–Noetherian rings, even if we allow infinite intersections.
(2) There exists a concept of primary decomposition for finitely generated modules over Noetherian rings (Exercise 4.1.13). Primary decomposition of modules has been implemented in the SINGULAR library `mprimdec.lib`.

Exercises

For these exercises let A be a Noetherian ring, K a field and I, J ideals in A.

4.1.1. Prove that $\sqrt{I}$ is prime if I is primary.

4.1.2. Prove that, for $a, b \in A$, $(I : \langle a\rangle) : \langle b\rangle = I : \langle ab\rangle$.

4.1.3. Prove that, for any $b \in A$, $(I \cap J) : \langle b\rangle = (I : \langle b\rangle) \cap (J : \langle b\rangle)$.

4.1.4. Prove that I is primary if $\sqrt{I}$ is a maximal ideal.

4.1.5. Prove that $\mathrm{minAss}(I) \subset \mathrm{Ass}(I)$ with equality if and only if I has no embedded primes.

4.1.6. Let $P \subset A$ be a prime ideal, and let $Q_1, Q_2 \subset A$ be P–primary. Prove that $Q_1 \cap Q_2$ is a P–primary ideal.

4.1.7. Let $f_1, f_2 \in A$ such that $f = f_1 \cdot f_2 \in I$ and $\langle f_1, f_2\rangle = A$. Prove that $I = \langle I, f_1\rangle \cap \langle I, f_2\rangle$.

4.1.8. Let $I \subset K[x_1, \dots, x_n]$ be a *homogeneous* ideal (that is, generated by homogeneous polynomials). Prove that the ideals in $\mathrm{Ass}(I)$ are homogeneous.

4.1.9. Let $w = (w_1, \dots, w_n) \in \mathbb{Z}^n$, $w_i \neq 0$ for all i, and let $I \subset K[x_1, \dots, x_n]$ be an ideal. Moreover, let $I^h \subset K[x_1, \dots, x_n, t]$ be the ideal generated by the weighted homogenizations of the elements of I with respect to t (see Exercise 1.7.5). Prove the following statements:

(1) I^h is primary (prime) if and only if I is primary (prime).
(2) Let $I = Q_1 \cap \ldots \cap Q_r$ be an irredundant primary decomposition, then $I^h = Q_1^h \cap \ldots \cap Q_r^h$ is an irredundant primary decomposition, too.

(Hint: to show (1), first prove the analogue of Exercise 2.2.5 for primary instead of prime ideals. For (2), prove that $(I_1 \cap I_2)^h = I_1^h \cap I_2^h$.)

4.1.10. Let $\mathrm{Ass}(\langle 0\rangle) = \{P_1, \dots, P_s\}$. Prove that $\bigcup_{i=1}^s P_i$ is the set of zerodivisors of A.

4.1.11. Let $I = Q_1 \cap \dots \cap Q_m$ be an irredundant primary decomposition, and let $J := Q_2 \cap \dots \cap Q_m$. Prove that $\dim\big(A/(Q_1 + J)\big) < \dim(A/J)$.

4.1.12. Use SINGULAR to show the following equality of ideals in $K[x,y,z]$:

$$\langle y^2 - xz\rangle \cap \langle x^2, z\rangle \cap \langle y, z^2\rangle = \big\langle (y^2 - xz)(z^2 - x^2y),\, (y^2 - xz)\cdot z\big\rangle\,.$$

4.1.13. Let M be a finitely generated A–module and $N \subset M$ a submodule. Then N is called *primary* in M if $N \neq M$ and for every zerodivisor x of M/N there exists ρ such that $x^\rho \in \mathrm{Ann}(M/N)$. Prove the following statements:

(1) If $N \subset M$ is primary then $N : M$ is a primary ideal ($\sqrt{N : M}$ is called the *associated prime* to N).
(2) N has an irredundant primary decomposition and the associated primes are uniquely determined.
(3) If P is an associated prime of N, then $P = N : \langle m\rangle$ for some $m \in M$.
(4) Let $P_1, \dots, P_s$ be the set of associated primes of N, then the zerodivisors of M/N are $\bigcup_{i=1}^{s} P_i$.

(Hint: recall that $\sqrt{N : M} = \sqrt{\mathrm{Ann}(M/N)} = \sqrt[M]{N}$, see Exercise 2.8.6.)

4.1.14. Let M be a finitely generated A–module. Let $\mathrm{Ass}(M)$ be the set of *associated prime ideals* to $\langle 0\rangle \subset M$ in the sense of Exercise 4.1.13, that is,

$$\mathrm{Ass}(M) := \big\{P \subset A \text{ prime} \;\big|\; P = \mathrm{Ann}(m),\ m \in M \smallsetminus \{0\}\big\}\,.$$

Let $\mathcal{M} := \{\mathrm{Ann}(m) \mid 0 \neq m \in M\}$. Prove that the maximal elements in $\mathcal{M}$ are associated prime ideals.

4.1.15. Let A be a Noetherian ring and $M \neq \langle 0\rangle$ a finitely generated A–module. Prove that there exists a chain $M = M_0 \supset M_1 \supset \dots \supset M_n = \langle 0\rangle$ of submodules of M such that $M_i/M_{i+1} \cong A/P_i$ for a suitable prime ideal $P_i \subset A$, $i = 0, \dots, n-1$.

(Hint: choose an associated prime $P_1 \in \mathrm{Ass}(M)$, and let $P_1 = \mathrm{Ann}(m_1)$. If $M = \langle m_1\rangle$ then $M \cong A/P_1$, otherwise continue with $M/\langle m_1\rangle$.)

4.2 Zero–dimensional Primary Decomposition

In this section we shall give an algorithm to compute a primary decomposition for zero–dimensional ideals in a polynomial ring over a field of characteristic 0. This algorithm was published by Gianni, Trager, and Zacharias ([72]). Let K be a field of characteristic 0. In the case of one variable x, any ideal $I \subset K[x]$ is a principal ideal and the primary decomposition is given by the factorization of a generator of I: let $I = \langle f\rangle$, $f = f_1^{n_1} \dots f_r^{n_r}$ with f_i irreducible and $\langle f_i, f_j\rangle = K[x]$ for $i \neq j$, then $I = \langle f_1\rangle^{n_1} \cap \dots \cap \langle f_r\rangle^{n_r}$ is the primary decomposition of I. In the case of n variables, the univariate polynomial factorization is also an essential ingredient. We shall see that, after a generic coordinate change, the factorization of a polynomial in one variable leads to a primary decomposition. By definition, all associated prime ideals of a zero–dimensional ideal are maximal. We need the concept for an ideal in general position.

Definition 4.2.1.

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

Proposition 4.2.2. *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 $x_1 > \cdots > x_n$.

Proof. We consider first the case that $I \subset K[x_1, \ldots, x_n]$ is a maximal ideal. The field $K[x_1, \ldots, x_n]/I$ is a finite extension of K (Theorem 3.5.1), and there exists a dense, Zariski open subset $U \subset K^{n-1}$ such that for $\underline{a} \in U$ the element $z = x_n + \sum_{i=1}^{n-1} a_i x_i$ is a primitive element for the field extension (Primitive Element Theorem, cf. [190], here it is necessary that K is a perfect, infinite field).

Since $\varphi_{\underline{a}+\underline{b}} = \varphi_{\underline{b}} \circ \varphi_{\underline{a}}$, we may assume that $\underline{0} \in U$, that is,

$$K[x_1, \ldots, x_n]/I \cong K[x_n]/\langle f_n(x_n)\rangle$$

for some irreducible polynomial $f_n(x_n)$. Via this isomorphism $x_i \mod I$ corresponds to some $f_i(x_n) \mod \langle f_n(x_n)\rangle$ and we obtain

$$\langle x_1 - f_1(x_n), \ldots, x_{n-1} - f_{n-1}(x_n),\ f_n(x_n)\rangle = I\ .$$

The set of these generators is obviously a Gröbner basis with the required properties.

Now let I be an arbitrary zero–dimensional ideal and let $P_1, \ldots, P_s$ be the associated primes of I, then $\varphi_{\underline{a}}(P_j)$ are in general position with respect to the lexicographical ordering $x_1 > \cdots > x_n$ for almost all $\underline{a} \in K^{n-1}$. It remains to prove that $\varphi_{\underline{a}}(P_i) \cap K[x_n] \neq \varphi_{\underline{a}}(P_j) \cap K[x_n]$ for $i \neq j$ and almost all $\underline{a}$. We may assume that the P_i's are already in general position with respect to the lexicographical ordering $x_1 > \cdots > x_n$. We study the behaviour of a maximal ideal $P = \langle x_1 - g_1(x_n), \ldots, x_{n-1} - g_{n-1}(x_n),\ g_n(x_n)\rangle$ under the automorphism $\varphi_{\underline{a}}$.

If $\varphi_{\underline{a}}(P)$ is again in general position with respect to the lexicographical ordering $x_1 > \cdots > x_n$, then $\varphi_{\underline{a}}(P) \cap K[x_n] = \langle h^{(\underline{a})} \rangle$ for a monic polynomial $h^{(\underline{a})}$ of degree

$$r := \dim_K K[x_n]/\langle h^{(\underline{a})} \rangle = \dim_K K[x]/\varphi_{\underline{a}}(P) = \dim_K K[x]/P = \deg(g_n)\,.$$

To compute $h^{(\underline{a})}$, we consider the algebraic closure $\overline{K}$ of K. Let $\alpha_1, \ldots, \alpha_r \in \overline{K}$ be the roots of $g_n(x_n)$. Because of Exercise 4.2.1 (b), $g_n(x_n)$ is squarefree in $\overline{K}[x_n]$. Then $g_n(x_n) = c(x_n - \alpha_1) \cdot \ldots \cdot (x_n - \alpha_r)$, $c \in K$ and, because of Exercise 4.1.7,

$$P\overline{K}[x] = \bigcap_{i=1}^{r} \langle x_1 - g_1(\alpha_i), \ldots, x_{n-1} - g_{n-1}(\alpha_i), x_n - \alpha_i \rangle\,.$$

Now

$$\begin{aligned} &\varphi_{\underline{a}}\big(\langle x_1 - g_1(\alpha_i), \ldots, x_{n-1} - g_{n-1}(\alpha_i), x_n - \alpha_i \rangle\big) \\ &\qquad = \Big\langle x_1 - g_1(\alpha_i), \ldots, x_{n-1} - g_{n-1}(\alpha_i), x_n - \alpha_i + \sum_{\nu=1}^{n-1} a_\nu g_\nu(\alpha_i) \Big\rangle\,. \end{aligned}$$

This implies that $\varphi_{\underline{a}}(P\overline{K}[x]) \cap \overline{K}[x_n] \supset \langle \prod_{i=1}^{r} \big(x_n - \alpha_i + \sum_{\nu=1}^{n-1} a_\nu g_\nu(\alpha_i)\big) \rangle$.

Since $\langle h^{(\underline{a})} \rangle = \varphi_{\underline{a}}(P) \cap K[x_n] = \varphi_{\underline{a}}(P\overline{K}[x]) \cap K[x_n]$ (Exercise 4.2.1 (a)), and since $h^{(\underline{a})}$, as well as $\prod_{i=1}^{r} \big(x_n - \alpha_i + \sum_{\nu=1}^{n-1} a_\nu g_\nu(\alpha_i)\big)$, are monic polynomials in $K[x_n]$[1] of degree r, it follows that

$$h^{(\underline{a})} = \prod_{i=1}^{r} \left(x_n - \alpha_i + \sum_{\nu=1}^{n-1} a_\nu g_\nu(\alpha_i) \right)\,.$$

Now let $\varphi_{\underline{a}}(P_1) \cap K[x_n] = \langle h_1^{(\underline{a})} \rangle$, $\ldots$, $\varphi_{\underline{a}}(P_s) \cap K[x_n] = \langle h_s^{(\underline{a})} \rangle$ with monic polynomials $h_i^{(\underline{a})} \in K[x_n]$, and assume that the prime ideals $\varphi_{\underline{a}}(P_i)$ are in general position with respect to the lexicographical ordering $x_1 > \cdots > x_n$. The condition $\varphi_{\underline{a}}(P_i) \cap K[x_n] = \varphi_{\underline{a}}(P_j) \cap K[x_n]$, that is, $h_i^{(\underline{a})} = h_j^{(\underline{a})}$ leads, because of $P_i \neq P_j$, to a non–trivial polynomial system of equations for $\underline{a}$. This implies that for almost all $\underline{a}$, $\varphi_{\underline{a}}(P_i) \cap K[x_n] \neq \varphi_{\underline{a}}(P_j) \cap K[x_n]$ if $i \neq j$. □

Proposition 4.2.3. *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*

[1] $\prod_{i=1}^{r} \big(x_n - \alpha_i + \sum_{\nu=1}^{n-1} a_\nu g_\nu(\alpha_i)\big) \in K[x_n]$ is a consequence of Galois theory, since the product is invariant under the action of the Galois group (the K–automorphisms of $K(\alpha_1, \ldots, \alpha_r)$ are given by permutations of the roots $\alpha_1, \ldots, \alpha_r$).

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

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.

Proof. To prove (1) note that, obviously, $I \subset \bigcap_{i=1}^{s} \langle I, g_i^{\nu_i} \rangle$. To prove the other inclusion let $g^{(i)} := g/g_i^{\nu_i}$ for $i = 1, \ldots, s$. Then the univariate polynomials $g^{(1)}, \ldots, g^{(s)} \in K[x_n]$ have the greatest common divisor 1. Hence, we can find $a_1, \ldots, a_s \in K[x_n]$ with $\sum_{i=1}^{s} a_i g^{(i)} = 1$. Now let $f \in \bigcap_{i=1}^{s} \langle I, g_i^{\nu_i} \rangle$, in particular, there exist $f_i \in I$, $\xi_i \in R$ such that $f = f_i + \xi_i g_i^{\nu_i}$, $i = 1, \ldots, s$. Hence,

$$f = \sum_{i=1}^{s} a_i g^{(i)} (f_i + \xi_i g_i^{\nu_i}) = \sum_{i=1}^{s} (a_i g^{(i)} f_i + a_i \xi_i g) \in I\,,$$

which proves (1).

(2) First note that $\langle I, g_i^{\nu_i} \rangle \subsetneq K[x]$ and $\operatorname{Ass}(\langle I, g_i^{\nu_i} \rangle) \subset \operatorname{Ass}(I)$. This can be seen as follows: if we could write $1 = f + a g_i^{\nu_i}$ for some $f \in I$, $a \in K[x]$, then $g/g_i^{\nu_i} \in \langle f, g \rangle \subset I$, contradicting the assumption $I \cap K[x_n] = \langle g \rangle$. Moreover, $I \subset \langle I, g_i^{\nu_i} \rangle$ and the uniqueness of associated primes implies that each associated prime of $\langle I, g_i^{\nu_i} \rangle$ has to contain some associated prime of I. But, since I is zero–dimensional, its associated primes are maximal ideals.

Now, let $P_1, \ldots, P_\ell$ be the associated primes of I and let $P_i \cap K[x_n] = \langle p_i \rangle$. Then, by assumption, the polynomials $p_1, \ldots, p_\ell$ are pairwise coprime and, therefore, $\bigcap_{i=1}^{\ell} (P_i \cap K[x_n]) = \bigcap_{i=1}^{\ell} \langle p_i \rangle = \big\langle \prod_{i=1}^{\ell} p_i \big\rangle$. On the other hand, we have $\bigcap_{i=1}^{\ell} (P_i \cap K[x_n]) = \big(\bigcap_{i=1}^{\ell} P_i \big) \cap K[x_n] = \sqrt{I} \cap K[x_n]$. Hence, the assumption $I \cap K[x_n] = \langle g \rangle$ implies that $\prod_{i=1}^{\ell} p_i$ divides g and g divides a power of $\prod_{i=1}^{\ell} p_i$. The latter implies $\ell = s$, and we may assume $g_i = p_i$ for $i = 1, \ldots, s$. It follows that P_i is the unique associated prime of I containing $g_i^{\nu_i}$, and, by the above, we can conclude that $\operatorname{Ass}(\langle I, g_i^{\nu_i} \rangle) = \{P_i\}$. Hence, $\langle I, g_i^{\nu_i} \rangle$ is a primary ideal. □

Proposition 4.2.3 shows how to obtain a primary decomposition of a zero–dimensional ideal in general position by using the factorization of g. In the algorithm for the zero–dimensional decomposition we try to put I in general position via a map $\varphi_{\underline{a}}$, $\underline{a} \in K^{n-1}$ chosen randomly. But we cannot be sure, in practice, that for a random choice of $\underline{a}$ made by the computer, $\varphi_{\underline{a}}(I)$ is in general position. We need a test to decide whether $\langle I, g_i^{\nu_i} \rangle$ is primary and in general position. Using Definition 4.2.1 we obtain the following criterion:

Criterion 4.2.4. *Let* $I \subset K[x_1, \ldots, x_n]$ *be a proper ideal. Then the following conditions are equivalent:*

(1) I *is zero–dimensional, primary and in general position with respect to the lexicographical ordering with* $x_1 > \cdots > x_n$.

(2) *There exist* $g_1, \ldots, g_n \in K[x_n]$ *and positive integers* $\nu_1, \ldots, \nu_n$ *such that*
   a) $I \cap K[x_n] = \langle g_n^{\nu_n} \rangle$, g_n *irreducible;*
   b) *for each* $j < n$, I *contains the element* $\big(x_j + g_j\big)^{\nu_j}$.

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

Proof. To prove (3) ⇒ (2), let $M := \sqrt{I}$. Then $g_n \in M$, and, inductively, we obtain $x_j + g_j \in M$ for all j. This implies

$$M = \langle x_1 + g_1, \ldots, x_{n-1} + g_{n-1}, g_n \rangle \,,$$

because g_n is irreducible and, therefore, $\langle x_1 - g_1, \ldots, x_{n-1} - g_{n-1}, g_n \rangle \subset K[x]$ is a maximal ideal. Finally, $M = \sqrt{I}$ implies now a) and b) in (2).

(2) ⇒ (1) is clear because $M = \langle x_1 + g_1, \ldots, x_{n-1} + g_{n-1}, g_n \rangle \subset \sqrt{I}$ is a maximal ideal and, by definition, in general position with respect to the lexicographical ordering with $x_1 > \cdots > x_n$.

To prove (1) ⇒ (3), let $M := \sqrt{I}$. Since I is in general position and primary, $M = \langle x_1 + g_1, \ldots, x_{n-1} + g_{n-1}, g_n \rangle$ with $g_n \in K[x_n]$ irreducible and $g_1, \ldots, g_{n-1} \in K[x_n]$. We may assume that g_n is monic. Now, let S be a reduced Gröbner basis of I (in particular, all elements are supposed to be monic, too). Then, due to the elimination property of $>_{lp}$, $S \cap K[x_n] = \{g\}$ generates $I \cap K[x_n]$, which is a primary ideal with $\sqrt{I \cap K[x_n]} = \langle g_n \rangle$. This implies $g = g_n^{\nu_n}$ for a suitable ν_n.

Now let $j \in \{1, \ldots, n-1\}$. Since I is zero-dimensional and S is a reduced Gröbner basis of I, there exists a unique $h \in S$ such that $\mathrm{LM}(h)$ is a power of x_j, $\mathrm{LM}(h) = x_j^m$ (Theorem 3.5.1 (7)). Note that the latter implies, in particular, that $h \in K[x_j, \ldots, x_n]$ (again due to the elimination property of $>_{lp}$). We set $M' := M \cap K[x_{j+1}, \ldots, x_n]$, $K' := K[x_{j+1}, \ldots, x_n]/M' \cong K[x_n]/\langle g_n \rangle$, and consider the canonical projection

$$\Phi : K[x_1, \ldots, x_n] = (K[x_{j+1}, \ldots, x_n])[x_1, \ldots, x_j] \longrightarrow K'[x_1, \ldots, x_j] \,.$$

Step 1. We show $\Phi(S \cap K[x_j, \ldots, x_n]) = \{\Phi(h), 0\}$. Since $S \cap K[x_j, \ldots, x_n]$ is a standard basis (w.r.t. $>_{lp}$) of $I \cap K[x_j, \ldots, x_n]$, this implies

$$I \cap K[x_j, \ldots, x_n] \equiv \langle h \rangle_{K[x_j, \ldots, x_n]} \mod M' \cdot K[x_j, \ldots, x_n] \,.$$

Let $K[x'] := K[x_{j+1}, \ldots, x_n]$ and consider

$$L := \left\langle f_s \in K[x'] \;\middle|\; \exists\, f_0, \ldots, f_{s-1} \in K[x'], s < m, \text{ such that } \sum_{i=0}^{s} f_i x_j^i \in I \right\rangle .$$

Then, clearly, $I \cap K[x'] \subset L \subsetneq K[x']$. Since $I \cap K[x']$ is primary and zero-dimensional, $\sqrt{I \cap K[x']}$ is the unique associated prime of $I \cap K[x']$ (Theorem 4.1.5) and a maximal ideal in $K[x']$. Hence, $L \subset \sqrt{I \cap K[x']} \subsetneq K[x']$, and there exists some $a \in K[x'] \smallsetminus I$ such that $\sqrt{I \cap K[x']} = (I \cap K[x']) : \langle a \rangle$.

Now, let $f \in S \cap K[x_j, \dots, x_n] \subset I$, $f \neq h$. We write $f = \sum_{i=0}^{s} f_i x_j^i$, with $f_i \in K[x']$. Since S is reduced and $\mathrm{LM}(h) = x_j^m$, we have $s < m$, hence $f_s \in L$. Moreover, $f' := x_j^{m-s} f - f_s h \in I$, and, writing $f' = \sum_{i=0}^{m-1} f_i' x_j^i$, we obtain $f_{m-1}' \in L$ and $f_i' \equiv f_{i+s-m} \mod L$, $i = m-s, \dots, m-1$. Therefore, $f_{s-1} \in L$, and proceeding inductively we obtain $f_i \in L$, $i = 0, \dots, s$.

The above implies now $a f_i \in I \cap K[x']$, and, since $I \cap K[x']$ is primary, it follows that $f_i \in \sqrt{I \cap K[x']} = M'$ for $i = 0, \dots, s$. Thus, $\Phi(f) = 0$.

Step 2. On the other hand, $\sqrt{\Phi(I)} = \Phi\big(\sqrt{I + \mathrm{Ker}(\Phi)}\,\big) = \Phi(M)$. It follows that $\sqrt{\Phi(I)} \cap K'[x_j] = \langle x_j + \overline{g}_j \rangle_{K'[x_j]}$, where $\overline{g}_j := g_j \mod M'$, and we conclude that $\Phi(I \cap K[x_j, \dots, x_n]) \cap K'[x_j] = \Phi(I) \cap K'[x_j] = \big\langle (x_j + \overline{g}_j)^\ell \big\rangle_{K'[x_j]}$ for a positive integer ℓ. Together with the result of Step 1, this implies that $h \equiv (x_j + g_j)^\ell \mod M' \cdot K[x_j, \dots, x_n]$, in particular, $\ell = m =: \nu_j$. □

Criterion 4.2.4 is the basis of the following algorithm to test whether a zero–dimensional ideal is primary and in general position.

Algorithm 4.2.5 (PRIMARYTEST(I)).

Input: A zero–dimensional ideal $I := \langle f_1, \dots, f_k \rangle \subset K[x]$, $x = (x_1, \dots, x_n)$.
Output: $\langle 0 \rangle$ if I is either not primary or not in general position, or $\sqrt{I}$ if I is primary and in general position.

- compute a reduced Gröbner basis S of I with respect to the lexicographical ordering with $x_1 > \dots > x_n$;
- factorize $g \in S$, the element with smallest leading monomial;
- if ($g = g_n^{\nu_n}$ with g_n irreducible)
  prim := $\langle g_n \rangle$
  else
  return $\langle 0 \rangle$.
- $i := n$;
  while ($i > 1$)
  $i := i - 1$;
  choose $f \in S$ with $\mathrm{LM}(f) = x_i^m$;
  $b :=$ the coefficient of x_i^{m-1} in f considered as polynomial in x_i;
  $q := x_i + b/m$;
  if ($q^m \equiv f \mod \text{prim}$)
  prim := prim + $\langle q \rangle$;
  else
  return $\langle 0 \rangle$;
- return prim.

SINGULAR Example 4.2.6 (primary test).

```
option(redSB);
ring R=0,(x,y),lp;
ideal I=y4-4y3-10y2+28y+49,x3-6x2y+3x2+12xy2-12xy+3x-8y3
+13y2-8y-6;
//the generators are a Groebner basis
```

We want to check whether the ideal I is primary and in general position.

```
factorize(I[1]);   //to test if Criterion 4.2.4 (3) a) holds
//-> [1]:
//->    _[1]=1
//->    _[2]=y2-2y-7
//-> [2]:
//->    1,2  //I[1] is the square of an irreducible element
ideal prim=std(y2-2y-7);
poly q=3x-6y+3;
poly f2=I[2];
reduce(q^3-27*f2,prim);

//-> 0
```

The ideal is primary and in general position and $\langle y^2-2y-7,\ x-2y+1\rangle$ is the associated prime ideal.

Now we are ready to give the procedure for the zero–dimensional decomposition. We describe first the main steps:

Algorithm 4.2.7 (zeroDecomp(I)).

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

- result $:= \emptyset$;
- choose a random $\underline{a}\in K^{n-1}$, and apply the coordinate change $I' := \varphi_{\underline{a}}(I)$ (cf. Proposition 4.2.2);
- compute a Gröbner basis G of I' with respect to the lexicographical ordering with $x_1>\dots>x_n$, and let $g\in G$ be the element with smallest leading monomial.
- factorize $g=g_1^{\nu_1}\cdot\ldots\cdot g_s^{\nu_s}\in K[x_n]$;
- for $i=1$ to s do
  set $Q_i' := \langle I', g_i^{\nu_i}\rangle$ and $Q_i := \langle I, \varphi_{\underline{a}}^{-1}(g_i)^{\nu_i}\rangle$;
  set $P_i' :=$ primaryTest(Q_i');
  if $P_i' \neq \langle 0\rangle$

set $P_i := \varphi_{\underline{a}}^{-1}(P_i')$;
result := result $\cup\{(Q_i, P_i)\}$;
else
result := result $\cup$ ZERODECOMP (Q_i);

- return result.

In the programming language of SINGULAR the procedure can be found in Section 4.6.

SINGULAR Example 4.2.8 (zero–dim primary decomposition).
We give an example for a zero-dimensional primary decomposition.

```
option(redSB);
ring R=0,(x,y),lp;
ideal I=(y2-1)^2,x2-(y+1)^3;
```

The ideal I is not in general position with respect to `lp` as y^2-1 is reducible.

```
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]=y7-y6-19y5-13y4+99y3+221y2+175y+49
//-> I[2]=112xy+112x-27y6+64y5+431y4-264y3-2277y2-2520y-847
//-> I[3]=56x2+65y6-159y5-1014y4+662y3+5505y2+6153y+2100
factorize(I[1]);
//-> [1]:
//->    _[1]=1
//->    _[2]=y2-2y-7
//->    _[3]=y+1
//-> [2]:
//->    1,2,3

ideal Q1=std(I,(y2-2y-7)^2); //the candidates for the
                             //primary ideals
ideal Q2=std(I,(y+1)^3);     //in general position
Q1; Q2;

//-> Q1[1]=y4-4y3-10y2+28y+49   Q2[1]=y3+3y2+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 $\langle y+1, x\rangle$.

Exercises

4.2.1. Let K be a field of characteristic 0, $\overline{K}$ the algebraic closure of K and $I \subset K[x]$ an ideal. Prove that

(1) $I\overline{K}[x] \cap K[x] = I$;
(2) if $f \in K[x]$ is squarefree, then $f \in \overline{K}[x]$ is squarefree.

Condition (1) says that $\overline{K}[x]$ is a flat $K[x]$–module (cf. Chapter 7).

4.2.2. Let $I \subset K[x] = K[x_1, \dots, x_n]$ be a zero–dimensional, and $J \subset K[x]$ a homogeneous ideal with $I \subset J \subset \sqrt{I}$. Prove that $\sqrt{I} = \langle x_1, \dots, x_n\rangle$.

4.2.3. Let $I \subset K[x_1, \dots, x_n]$ be a zero–dimensional ideal, and let $f \in K[x_n]$ be irreducible such that $I \cap K[x_n] = \langle f\rangle$. Let $\dim_K K[x_1, \dots, x_n]/I = \deg(f)$. Prove that I is a prime ideal in general position with respect to the lexicographical ordering with $x_1 > \dots > x_n$.

4.2.4. Compute a primary decomposition of $\langle x^2+1, y^2+1\rangle \subset \mathbb{Q}[x,y]$, by following Algorithm 4.2.7 (without using SINGULAR).

4.2.5. Let K be a field of characteristic 0 and $M \subset K[x_1, \dots, x_n]$ a maximal ideal. Prove that $K[x_1, \dots, x_n]_M \cong K[x_1, \dots, x_n]_{\langle x_1, \dots, x_{n-1}, f\rangle}$ for a suitable $f \in K[x_n]$.

4.2.6. Give an example for a zero–dimensional ideal in $\mathbb{F}_2[x, y]$ which is not in general position with respect to the lexicographical ordering with $x > y$.

4.3 Higher Dimensional Primary Decomposition

In this section we show how to reduce the primary decomposition of an arbitrary ideal in $K[x]$ to the zero–dimensional case. We use the following idea:

Let K be a field and $I \subset K[x]$ an ideal. Let $u \subset x = \{x_1, \dots, x_n\}$ be a maximal independent set with respect to the ideal I (cf. Definition 3.5.3) then $\emptyset \subset x \setminus u$ is a maximal independent set with respect to $IK(u)[x \setminus u]$ and, therefore, $IK(u)[x \setminus u] \subset K(u)[x \setminus u]$ is a zero–dimensional ideal (Theorem 3.5.1 (6)). Now, let $Q_1 \cap \dots \cap Q_s = IK(u)[x \setminus u]$ be an irredundant primary decomposition (which we can compute as we are in the zero–dimensional case), then also $IK(u)[x \setminus u] \cap K[x] = (Q_1 \cap K[x]) \cap \dots \cap (Q_s \cap K[x])$ is an irredundant primary decomposition. It turns out that $IK(u)[x \setminus u] \cap K[x]$ is equal to the saturation $I : \langle h^\infty \rangle = \bigcup_{m>0} I : \langle h^m \rangle$ for some $h \in K[u]$ which can be read from an appropriate Gröbner basis of $IK(u)[x \setminus u]$. Assume that $I : \langle h^\infty \rangle = I : \langle h^m \rangle$ for a suitable m (the ring is Noetherian). Then, using Lemma 3.3.6, we have $I = (I : \langle h^m \rangle) \cap \langle I, h^m \rangle$. Because we computed already the primary decomposition for $I : \langle h^m \rangle$ (an equidimensional ideal of dimension $\dim(I)$) we can use induction, that is, apply the procedure again to $\langle I, h^m \rangle$.

This approach terminates because either $\dim(\langle I, h^m \rangle) < \dim(I)$ or the number of maximal independent sets with respect to $\langle I, h^m \rangle$ is smaller than the number of maximal independent sets with respect to I (since u is not an independent set with respect to $\langle I, h^m \rangle$). The basis of this reduction procedure to the zero–dimensional case is the following proposition:

Proposition 4.3.1. *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.*

(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 $h := \text{lcm}\big(\text{LC}(g_1), \dots, \text{LC}(g_s)\big) \in K[u]$, then

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

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

Proof. (1) is obvious by definition of u and Theorem 3.5.1 (6).

(2) Obviously, $I : \langle h^\infty \rangle \subset IK(u)[x \setminus u]$. To prove the inverse inclusion, let $f \in IK(u)[x \setminus u] \cap K[x]$. S being a Gröbner basis, we obtain $\text{NF}(f \mid S) = 0$,

where NF denotes the Buchberger normal form in $K(u)[x \smallsetminus u]$. But the Buchberger normal form algorithm requires only to divide by the leading coefficients $\mathrm{LC}(g_i)$ of the g_i, $i = 1, \dots, s$. Hence, we obtain a standard representation $f = \sum_{i=1}^{s} \xi_i g_i$ with $\xi_i \in K[x]_h$. Therefore, $h^N f \in K[x]$ for some N. This proves $IK(u)[x \smallsetminus u] \cap K[x] \subset I : \langle h^\infty \rangle$.

To show that $I : \langle h^\infty \rangle \subset K[x]$ is an equidimensional ideal, suppose that $I = Q_1 \cap \dots \cap Q_r$ is a primary decomposition of I with $Q_i \cap K[u] = \langle 0 \rangle$ for $i = 1, \dots, s$ and $Q_i \cap K[u] \neq \langle 0 \rangle$ for $i = s+1, \dots, r$. Then $IK(u)[x \smallsetminus u] = \bigcap_{i=1}^{s} Q_i K(u)[x \smallsetminus u]$ is a primary decomposition (Exercise 4.3.3). Since u is an independent set w.r.t. the ideals $\sqrt{Q_i K(u)[x \smallsetminus u]}$, $i = 1, \dots, s$, it follows that all associated primes of $IK(u)[x \smallsetminus u]$ have at least dimension $\dim(I) = \#u$ (cf. Theorem 3.5.1 (6)).

(3) Obviously $Q_i \cap K[x]$ is primary and $\sqrt{Q_i \cap K[x]} \neq \sqrt{Q_j \cap K[x]}$ for $i \neq j$. Namely, $f \in \sqrt{Q_i}$ implies $f^m \in Q_i$ for a suitable m. It follows that $hf^m \in Q_i \cap K[x]$ for a suitable $h \in K[u]$, in particular, $(hf)^m \in Q_i \cap K[x]$. This implies $hf \in \sqrt{Q_i \cap K[x]}$. Assuming $\sqrt{Q_i \cap K[x]} = \sqrt{Q_j \cap K[x]}$, we would obtain $(hf)^\ell \in Q_j \cap K[x]$ for a suitable ℓ, that is, $f \in \sqrt{Q_j}$. This, together with the same reasoning applied to (j,i) in place of (i,j), would give $\sqrt{Q_i} = \sqrt{Q_j}$, contradicting the irredundance assumption. Similarly, we obtain a contradiction if we assume that $Q_i \cap K[x]$ can be omitted in the decomposition. □

Now we are prepared to give the algorithms. We start with a "universal" algorithm to compute all the ingredients we need for the reduction to the zero–dimensional case, as described above. We need this procedure for the primary decomposition and also for the computation of the equidimensional decomposition and the radical.

Algorithm 4.3.2 (REDUCTIONTOZERO(I)).

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

- compute a maximal independent set $u \subset x$ with respect to I; [2]
- compute a Gröbner basis $G = \{g_1, \dots, g_s\}$ of I with respect to the lexicographical ordering with $x \smallsetminus u > u$;
- $h := \prod_{i=1}^{s} \mathrm{LC}(g_i) \in K[u]$, where the g_i are considered as polynomials in $x \smallsetminus u$ with coefficients in $K(u)$;
- compute m such that $\langle g_1, \dots, g_s \rangle : \langle h^m \rangle = \langle g_1, \dots, g_s \rangle : \langle h^{m+1} \rangle$; [3]
- return $u, \{g_1, \dots, g_s\}, h^m$.

[2] For the computation of a maximal independent set, cf. Exercises 3.5.1 and 3.5.2.
[3] For the computation of the saturation exponent m, cf. Section 1.8.9.

Note that G is, indeed, a Gröbner basis of $IK(u)[x \smallsetminus u]$ (with respect to the induced lexicographical ordering), since, for each $f \in IK(u)[x \smallsetminus u]$, we obtain $\mathrm{LM}(f) \in L(I) \cdot K(u)$.

SINGULAR Example 4.3.3 (reduction to zero–dimensional case).

```
option(redSB);
ring R=0,(x,y),lp;
ideal a1=x;                //preparation of the example
ideal a2=y2+2y+1,x-1;
ideal a3=y2-2y+1,x-1;
ideal I=intersect(a1,a2,a3);
I;
//-> I[1]=xy4-2xy2+x
//-> I[2]=x2-x

ideal G=std(I);
indepSet(G);
//-> 0,1                  //the independent set is u={y}

ring S=(0,y),(x),lp;      //the ring K(u)[x\u]
ideal G=imap(R,G);
G;
//-> G[1]=(y4-2y2+1)*x
//-> G[2]=x2-x
```

This ideal in $K(y)[x]$ is obviously the prime ideal generated by x.

```
setring R;
poly h=y4-2y2+1;  //the lcm of the leading coefficients

ideal I1=quotient(I,h);
I1;
//-> I1[1]=x
```

Therefore, we obtain $I : \langle h \rangle = I : \langle h^\infty \rangle = G \cap K[x,y] = \langle x \rangle$, as predicted by Proposition 4.3.1 (2).

Combining everything so far, we obtain the following algorithm to compute a higher dimensional primary decomposition:

Algorithm 4.3.4 (DECOMP(I)).

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

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

The intersection $Q' \cap K[x]$ may be computed by saturation: let Q' be given by a Gröbner basis $\{g'_1, \ldots, g'_m\} \subset K[x]$, and let $g' := \prod_{i=1}^m \mathrm{LC}(g'_i) \in K[u]$, then $Q' \cap K[x] = \langle g'_1, \ldots, g'_m\rangle : \langle g'^\infty\rangle \subset K[x]$ (Exercise 4.3.4).

The procedure in the SINGULAR programming language can be found in Section 4.6.[4]

SINGULAR Example 4.3.5 (primary decomposition).
Use the results of Example 4.3.3.

```
ideal I2=std(I+ideal(h));
//we compute now the decomposition of I2
indepSet(I2);
//-> 0,0       // we are in the zero-dimensional case now

list fac=factorize(I2[1]);
fac;
//-> [1]:
//->    _[1]=1
//->    _[2]=y+1
//->    _[3]=y-1
//-> [2]:
//->    1,2,2

ideal J1=std(I2,(y+1)^2);       // the two candidates
ideal J2=std(I2,(y-1)^2);       // for primary ideals

J1; J2;
//-> J1[1]=y2+2y+1     J2[1]=y2-2y+1
//-> J1[2]=x2-x        J2[2]=x2-x
```

J1 and J2 are not in general position with respect to lp. We choose a generic coordinate change.

```
map phi=R,x,x+y;                // coordinate change
map psi=R,x,-x+y;               // and the inverse map
```

[4] Note that the algorithm described above computes a primary decomposition which is not necessarily irredundant. Check this using Example 4.1.6 (3).

```
ideal K1=std(phi(J1));
ideal K2=std(phi(J2));
factorize(K1[1]);
//-> [1]:
//->    _[1]=1
//->    _[2]=y+2
//->    _[3]=y+1
//-> [2]:
//->    1,2,2

ideal K11=std(K1,(y+1)^2);      // the new candidates
                                // for primary ideals
ideal K12=std(K1,(y+2)^2);      // coming from K1
factorize(K2[1]);
//-> [1]:
//->    _[1]=1
//->    _[2]=y
//->    _[3]=y-1
//-> [2]:
//->    1,2,2

ideal K21=std(K2,(y-1)^2);      // the new candidates
                                // for primary ideals
ideal K22=std(K2,y2);           // coming from K2
K11=std(psi(K11));              // the inverse coordinate
                                // transformation
K12=std(psi(K12));
K21=std(psi(K21));
K22=std(psi(K22));

K11; K12; K21; K22;             // the result
//-> K11[1]=y2+2y+1    K12[1]=y2+2y+1
//-> K11[2]=x          K12[2]=x-1

//-> K21[1]=y2-2y+1    K22[1]=y2-2y+1
//-> K21[2]=x          K22[2]=x-1
```

$K_{11}, \ldots, K_{22}$ are now primary and in general position with respect to `lp`. K_{11} and K_{21} are redundant, because they contain I_1. We obtain $a_1 = I_1$, $a_2 = K_{12}$, $a_3 = K_{22}$ for the primary decomposition of I, as it should be, from the definition of I in Example 4.3.3.

Exercises

4.3.1. Compute the primary decomposition of the ideals $\langle xy, xz\rangle$ and $\langle x^2, xy\rangle$ in $\mathbb{Q}[x,y]$ using the algorithm `decomp`.

4.3.2. Let $I \subset K[x_1,\dots,x_n]$ be an ideal, and let $u \subset x = \{x_1,\dots,x_n\}$ be an independent set with respect to I. Prove that $IK(u)[x \smallsetminus u]$ is primary (respectively prime) if I is primary (respectively prime).

4.3.3. Let $I \subset K[x_1,\dots,x_n]$ be an ideal, and let $I = Q_1 \cap \dots \cap Q_r$ be an irredundant primary decomposition. Moreover, let $u \subset x = \{x_1,\dots,x_n\}$ be an independent set with respect to I. Assume that $Q_i \cap K[u] = \langle 0\rangle$ for $i = 1,\dots,s$ and $Q_i \cap K[u] \neq \langle 0\rangle$ for $i = s+1,\dots,r$.

Prove that $IK(u)[x \smallsetminus u] = \bigcap_{i=1}^{s} Q_i K(u)[x \smallsetminus u]$ is an irredundant primary decomposition.

4.3.4. Let $u \subset x = \{x_1,\dots,x_n\}$ be a subset, $J \subset K(u)[x \smallsetminus u]$ an ideal, and let $\{g_1,\dots,g_s\} \subset K[x_1,\dots,x_n]$ be a Gröbner basis of J with respect to any global monomial ordering on $K(u)[x \smallsetminus u]$. Let $\widetilde{h} \in K[u]$ be the least common multiple of the leading coefficients of the g_i and h the squarefree part of $\widetilde{h}$. Prove that $I \cap K[x] = \langle g_1,\dots,g_s\rangle : \langle h^\infty\rangle$.

4.3.5. Follow Examples 4.3.3 and 4.3.5 to compute an irredundant primary decomposition of the intersection of the Clebsch cubic (Figure A.1) and the Cayley cubic (Figure A.2).

4.4 The Equidimensional Part of an Ideal

In this section we shall compute the equidimensional part of an ideal and an equidimensional decomposition.

Definition 4.4.1. Let A be a Noetherian ring, let $I \subset A$ be an ideal, and let $I = Q_1 \cap \dots \cap Q_s$ be an irredundant primary decomposition. The *equidimensional part* $E(I)$ is the intersection of all primary ideals Q_i with $\dim(Q_i) = \dim(I)$.[5] The ideal I (respectively the ring A/I) is called *equidimensional* or *pure dimensional* if $E(I) = I$. In particular, the ring A is called *equidimensional* if $E(\langle 0\rangle) = \langle 0\rangle$.

Example 4.4.2.

(1) Let $I = \langle x^2, xy\rangle = \langle x\rangle \cap \langle x,y\rangle^2 \subset K[x,y]$, K any field. Then $E(I) = \langle x\rangle$.
(2) Let $A = K[x,y,z]$ and $I = \langle xy, xz\rangle = \langle x\rangle \cap \langle y,z\rangle$ then $E(I) = \langle x\rangle$. The zero–set of I is shown in Figure 4.3, the plane being the zero–set of the equidimensional part.

[5] Note that because of Theorem 4.1.5 the definition is independent of the choice of the irredundant primary decomposition.

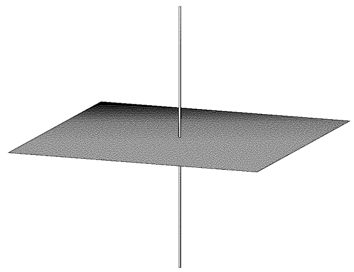

Fig. 4.3. The zero–set of $\langle xy, xz\rangle \subset K[x,y,z]$

Using Proposition 4.3.1 (2) we obtain the following algorithm to compute the equidimensional part of an ideal:

Algorithm 4.4.3 (EQUIDIMENSIONAL(I)).

Input: $I := \langle f_1,\dots,f_k\rangle \subset K[x]$, $x = (x_1,\dots,x_n)$.
Output: $E(I) \subset K[x]$, the equidimensional part of I.

- set $(u, G, h) :=$ REDUCTIONTOZERO (I);
- if $(\dim(\langle I,h\rangle) < \dim(I))$
  return $(\langle G\rangle : \langle h\rangle)$;
  else
  return $\big((\langle G\rangle : \langle h\rangle) \cap$ EQUIDIMENSIONAL $(\langle I,h\rangle)\big)$.

SINGULAR Example 4.4.4 (equidimensional part).
We compute $E(I)$ for $I = \langle xy^4 - 2xy^2 + x,\ x^2 - x\rangle \subset K[x,y]$ (cf. SINGULAR Example 4.3.3). As seen above, REDUCTIONTOZERO(I) returns $u = \{y\}$, $G = \{xy^4 - 2xy^2 + x,\ x^2 - x\}$ and $h = y^4 - 2y^2 + 1$. Using the results of Example 4.3.3, we compute the dimension of $\langle I,h\rangle$:

```
dim(std(I+ideal(h)));
//-> 0
```

Since $\dim(I) = \#u = 1$ and $\dim(\langle I,h\rangle) = 0$ as computed, we can stop here. The equidimensional part is $I_1 = \langle x\rangle$.

A little more advanced algorithm, returning the equidimensional part $E(I)$ and an ideal $J \subset K[x]$ with $I = E(I) \cap J$, written in the SINGULAR programming language, can be found in Section 4.6.

We should just like to mention another method to compute the equidimensional part of an ideal (cf. [52]). Let $A = K[x_1,\dots,x_n]$, K a field, and $I \subset A$ be an ideal. Then

$$E(I) = \mathrm{Ann}\big(\mathrm{Ext}_A^{n-d}(A/I, A)\big)\,, \quad d = \dim(A/I)$$

(for the definition of Ext see Chapter 7).

Definition 4.4.5. Let A be a Noetherian ring, and let $I \subset A$ be an ideal without embedded prime ideals. Moreover, let $I = \bigcap_{i=1}^s Q_i$ be an irredundant primary decomposition. For $\nu \le d = \dim(I)$ we define the *ν–th equidimensional part* $E_\nu(I)$ to be the intersection of all Q_i with $\dim(Q_i) = \nu$.[6]

Example 4.4.6. Let $I = \langle xy, xz\rangle = \langle x\rangle \cap \langle y, z\rangle \subset K[x,y,z]$, then $E_2(I) = \langle x\rangle$ and $E_1(I) = \langle y, z\rangle$.

Lemma 4.4.7. *Let A be a Noetherian ring and $I \subset A$ be an ideal without embedded prime ideals. Let $I = \bigcap_{i=1}^s Q_i$ be an irredundant primary decomposition such that $E(I) = \bigcap_{i=1}^k Q_i$. Then*

$$I : E(I) = \bigcap_{i=k+1}^{s} \big(Q_i : E(I)\big)\,.$$

In particular, $I = E(I) \cap \big(I : E(I)\big)$.

Proof. $I : E(I) = \bigcap_{i=1}^s \big(Q_i : E(I)\big) = \bigcap_{i=k+1}^s \big(Q_i : E(I)\big)$. Now $E(I) \not\subset \sqrt{Q_i}$ for $i = k+1, \dots, s$, because the primary decomposition is irredundant and all associated primes are minimal by assumption. This implies $Q_i : E(I) = Q_i$, since otherwise $E(I) \subset Q_i : \langle f\rangle$ for some $f \notin Q_i$ and, by Lemma 4.1.3 (3), $E(I) \subset \sqrt{Q_i : \langle f\rangle} = \sqrt{Q_i}$. □

Remark 4.4.8. Let A be a Noetherian ring, let $I \subset A$ be an ideal, and let $I = \bigcap_{i=1}^s Q_i$ be an irredundant primary decomposition with $E(I) = \bigcap_{i=1}^k Q_i$. Then $I : E(I) = \bigcap_{i=k+1}^s \widetilde{Q}_i$ for some primary ideals $\widetilde{Q}_i$ with $Q_i \subset \widetilde{Q}_i \subset \sqrt{Q_i}$, but $I = E(I) \cap \big(I : E(I)\big)$ need not be true. Just consider the following example: $I = \langle x^2, xy\rangle = \langle x\rangle \cap \langle x^2, y\rangle$, $E(I) = \langle x\rangle$ and $I : E(I) = \langle x, y\rangle$.

The following algorithm, based on Lemma 4.4.7, computes, for a given ideal I without embedded primes, all equidimensional parts.[7]

Algorithm 4.4.9 (EQUIDIMENSIONALDECOMP(I)).

Input: $I := \langle f_1, \dots, f_k\rangle \subset K[x]$, $x = (x_1, \dots, x_n)$.
Output: A list of ideals $I_1, \dots, I_n \subset K[x]$ such that $I_1 = E(I)$, $I_2 = E(I : I_1)$, $\dots$, $I_n = E(I_{n-2} : I_{n-1})$, and $\sqrt{I} = \bigcap_{j=1}^n \sqrt{I_j}$. If I is radical then the I_j are radical, too. for all j.

[6] The $E_\nu(I)$ are well-defined, because, under the above assumptions, the primary decomposition is uniquely determined (Theorem 4.1.5).

[7] If we apply the algorithm to an arbitrary ideal then we obtain a set of equidimensional ideals such that the intersection of their radicals is the radical of the given ideal. In case of $\langle x^2, xy\rangle$ we obtain $\langle x\rangle, \langle x, y\rangle$.

- $E :=$ EQUIDIMENSIONAL (I);
- return $\{E\} \cup$ EQUIDIMENSIONALDECOMP $(I : E)$.

SINGULAR Example 4.4.10 (equidimensional decomposition).
We use the results of SINGULAR Example 4.3.3:

```
ideal I2=quotient(I,I1);
I2;
//-> I2[1]=y4-2y2+1
//-> I2[2]=x-1
```

$I_2 = E(I_2)$, because I_2 is zero–dimensional (SINGULAR Example 4.4.4). Therefore, we obtain $E_1(I) = I_1 = \langle x \rangle$ and $E_0(I) = I_2 = \langle y^4 - 2y^2 + 1,\, x - 1\rangle$ as the equidimensional components of I.

Exercises

4.4.1. Write a SINGULAR procedure to compute the equidimensional decomposition using Procedure 4.6.6.

4.4.2. Use the algorithm EQUIDIMENSIONAL to compute the equidimensional part of $\langle xy, xz\rangle \subset K[x, y, z]$.

4.4.3. Let $I \subset K[x_1, \dots, x_n]$ be an ideal and assume that $K[x_1, \dots, x_r] \subset K[x_1, \dots, x_n]/I$ is a Noether normalization. Prove that I is equidimensional if and only if every non–zero $f \in K[x_1, \dots, x_r]$ is a non–zerodivisor in $K[x_1, \dots, x_n]/I$.

4.4.4. Use Exercise 4.4.3 to check whether $\langle x^2 + xy, xz\rangle$ is equidimensional.

4.4.5. Follow the SINGULAR Examples of this section to compute an equidimensional decomposition of the ideal

$$\langle x^3 + x^2y + x^2z - x^2 - xz - yz - z^2 + z,\ x^2xz + x^2y - yz^2 - yz,\\ x^2y^2 - x^2y - y^2z + yz\rangle\ ,$$

and verify it by using the procedure EQUIDIMENSIONAL.

4.5 The Radical

In this section we describe the algorithm of Krick and Logar (cf. [110]) to compute the radical of an ideal. Similarly to the algorithm for primary decomposition, using maximal independent sets, the computation of the radical is reduced to the zero–dimensional case.

Proposition 4.5.1. *Let $I \subset K[x_1, \ldots, x_n]$ be a zero–dimensional ideal and $I \cap K[x_i] = \langle f_i \rangle$ for $i = 1, \ldots, n$. Moreover, let g_i be the squarefree part of f_i, then $\sqrt{I} = I + \langle g_1, \ldots, g_n \rangle$.*

Proof. Obviously, $I \subset I + \langle g_1, \ldots, g_n \rangle \subset \sqrt{I}$. Hence, it remains to show that $a^n \in I$ implies that $a \in I + \langle g_1, \ldots, g_n \rangle$. Let $\overline{K}$ be the algebraic closure of K. Using Exercise 4.2.1 we see that each g_i is the product of different linear factors of $\overline{K}[x_i]$. Due to Exercise 4.1.7, these linear factors of the g_i induce a splitting of the ideal $(I + \langle g_1, \ldots, g_n \rangle)\overline{K}[x]$ into an intersection of maximal ideals. Hence, $(I + \langle g_1, \ldots, g_n \rangle)\overline{K}[x]$ is radical (Exercise 4.5.7). Now consider $a \in K[x]$ with $a^n \in I + \langle g_1, \ldots, g_n \rangle$. Using Exercise 4.2.1 again, we obtain $a \in (I + \langle g_1, \ldots, g_n \rangle)\overline{K}[x] \cap K[x] = I + \langle g_1, \ldots, g_n \rangle$. □

This leads to the following algorithm:

Algorithm 4.5.2 (ZERORADICAL(I)).

Input: a zero–dimensional ideal $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$, $x = (x_1, \ldots, x_n)$.
Output: $\sqrt{I} \subset K[x]$, the radical of I.

- for $i = 1, \ldots, n$, compute $f_i \in K[x_i]$ such that $I \cap K[x_i] = \langle f_i \rangle$;
- return $I + \langle \text{SQUAREFREE}(f_1), \ldots, \text{SQUAREFREE}(f_n) \rangle$.

To reduce the computation of the radical for an arbitrary ideal to the zero–dimensional case we proceed as in Section 4.3. Let $u \subset x$ be a maximal independent set for the ideal $I \subset K[x]$, $x = (x_1, \ldots, x_n)$, and let $h \in K[u]$ satisfy

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

(cf. Proposition 4.3.1 (2)). Then $I = (I : \langle h \rangle) \cap \langle I, h \rangle$ (Lemma 3.3.6), which implies that $\sqrt{I} = \sqrt{I : \langle h \rangle} \cap \sqrt{\langle I, h \rangle}$ (Exercise 4.5.7). Now $IK(u)[x \smallsetminus u]$ is a zero–dimensional ideal (Theorem 3.5.1 (6)), hence, we may compute its radical by applying ZERORADICAL. Clearly,

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

and it remains to compute the radical of the ideal $\langle I, h \rangle \subset K[x]$. This inductive approach terminates similarly to the corresponding approach for the primary decomposition.

We obtain the following algorithm for computing the radical of an arbitrary ideal:

Algorithm 4.5.3 (RADICAL(I)).

Input: $I := \langle f_1, \ldots, f_k \rangle \subset K[x]$, $x = (x_1, \ldots, x_n)$.
Output: $\sqrt{I} \subset K[x]$, the radical of I.

- $(u, G, h) :=$ REDUCTIONTOZERO(I);

- change ring to $K(u)[x \smallsetminus u]$ and compute $J :=$ ZERORADICAL $(\langle G \rangle)$;
- compute a Gröbner basis $\{g_1, \dots, g_\ell\} \subset K[x]$ of J;
- set $p := \prod_{i=1}^{\ell} \mathrm{LC}(g_i) \in K[u]$;
- change ring to $K[x]$ and compute $J \cap K[x] = \langle g_1, \dots, g_\ell \rangle : \langle p^\infty \rangle$;
- return $(J \cap K[x]) \cap$ RADICAL $(\langle I, h \rangle)$.

SINGULAR Example 4.5.4 (radical).
Use the results of Example 4.3.3.

```
ideal rad=I1;
ideal I2=std(I+ideal(h));
dim(I2);
//-> 0        //we are in the zero-dimensional case now

ideal u=finduni(I2);    //finds univariate polynomials
                        //in each variable in I2
u;
//-> u[1]=x2-x
//-> u[2]=y4-2y2+1

I2=I2,x2-1,y2-1;        //the squarefree parts of
                        //u[1],u[2] are added to I2
rad=intersect(rad,I2);
rad;
//-> rad[1]=xy2-x
//-> rad[2]=x2-x
```

From the output, we read $\sqrt{I} = \langle xy^2 - x, x^2 - x \rangle$.

Exercises

4.5.1. Let K be a field of characteristic 0, $\overline{K}$ its algebraic closure and $P \subset K[x_1, \dots, x_n]$ a maximal ideal. Prove that $P\overline{K}[x_1, \dots, x_n]$ is a radical ideal.

4.5.2. Let K be a field of characteristic 0, let $\overline{K}$ be its algebraic closure, and let $I \subset K[x_1, \dots, x_n]$ be a zero–dimensional radical ideal. Prove that $\dim_K K[x_1, \dots, x_n]/I$ is equal to the number of associated prime ideals of $I\overline{K}[x_1, \dots, x_n]$. This means, geometrically, that the number of points of the zero–set $V(I) \subset \overline{K}^n$ is equal to the dimension of the factor ring.

4.5.3. Let A be a ring, $I \subset A$ an ideal. Prove that

(1) $\sqrt{\langle I, fg\rangle} = \sqrt{\langle I, f\rangle} \cap \sqrt{\langle I, g\rangle}$,
(2) $\sqrt{I} = \sqrt{IA_f \cap A} \cap \sqrt{\langle I, f\rangle}$.

4.5.4 (Factorizing Gröbner basis algorithm). The idea of the *factorizing Gröbner basis algorithm* is to factorize, during Algorithm 1.7.1, a new polynomial when it occurs and then split the computations. A simple version is described in the following algorithm (we use the notations of Chapter 1).

Algorithm (FACSTD(G,NF)).
Let $>$ be a well–ordering.

Input: $G \in \mathcal{G}$, NF an algorithm returning a weak normal form.
Output: $S_1, \dots, S_r \in \mathcal{G}$ such that $\sqrt{\langle S_1\rangle} \cap \dots \cap \sqrt{\langle S_r\rangle} = \sqrt{\langle G\rangle}$ and S_i is a standard basis of $\langle S_i\rangle$.

- $S := G$;
- if there exist non–constant polynomials g_1, g_2 with $g_1 g_2 \in S$
    return FACSTD($S \cup \{g_1\}$,NF) $\cup$ FACSTD($S \cup \{g_2\}$,NF);
- $P := \{(f,g) \mid f, g \in S,\ f \neq g\}$, the pair–set;
- while ($P \neq \emptyset$)
    choose $(f,g) \in P$;
    $P := P \smallsetminus \{(f,g)\}$;
    $h := \mathrm{NF}(\mathrm{spoly}(f,g) \mid S)$;
    if ($h \neq 0$)
        if ($h = h_1 h_2$ with non–constant polynomials h_1, h_2)
            return FACSTD($S \cup \{h_1\}$,NF) $\cup$ FACSTD($S \cup \{h_2\}$,NF);
        $P := P \cup \{(h,f) \mid f \in S\}$;
        $S := S \cup \{h\}$;
- return S.

Prove that the output of FACSTD has the required properties. Moreover, use the command `facstd` of SINGULAR to compute a decomposition of the ideal I of Example 4.3.3.

Note that FACSTD can be used for the computation of the radical.

4.5.5. Let I_1 be primary and $I_2 \not\subset \sqrt{I_1}$. Prove that $\sqrt{I_1 : I_2^i} = \sqrt{I_1}$ for $i \geq 1$.

4.5.6. Let I be a radical ideal. Prove that, for every $h \notin I$, the ideal quotient $I : \langle h\rangle$ is a radical ideal.

4.5.7. Prove that $\sqrt{I \cap J} = \sqrt{I} \cap \sqrt{J}$.

4.6 Procedures

We collect the main procedures of this section as fully functioning SINGULAR procedures. However, since they are in no way optimized, one cannot expect them to be very fast. Each procedure has a small example to test it. This section demonstrates that it is not too difficult to implement a full primary decomposition, the equidimensional part and the radical.

4.6.1. We begin with a procedure to test whether a zero–dimensional ideal is primary and in general position.

proc primaryTest (ideal i, poly p)

```
"USAGE:   primaryTest(i,p); i standard basis with respect to
          lp, p irreducible polynomial in K[var(n)],
          p^a=i[1] for some a;
ASSUME:   i is a zero-dimensional ideal.
RETURN:   an ideal, the radical of i if i is primary and in
          general position with respect to lp,
          the zero ideal else.
"
{
   int m,e;
   int n=nvars(basering);
   poly t;
   ideal prm=p;

   for(m=2;m<=size(i);m++)
   {
     if(size(ideal(leadexp(i[m])))==1)
     {
       n--;
//----------------i[m] has a power of var(n) as leading term
       attrib(prm,"isSB",1);
//--- ?? i[m]=(c*var(n)+h)^e modulo prm for h
//     in K[var(n+1),...], c in K ??
       e=deg(lead(i[m]));
       t=leadcoef(i[m])*e*var(n)+(i[m]-lead(i[m]))
       /var(n)^(e-1);
       i[m]=poly(e)^e*leadcoef(i[m])^(e-1)*i[m];
//---if not (0) is returned, else c*var(n)+h is added to prm
       if (reduce(i[m]-t^e,prm,1) !=0)
       {
         return(ideal(0));
       }
       prm = prm,cleardenom(simplify(t,1));
```

```
      }
    }
    return(prm);
  }

  ring s=(0,x),(d,e,f,g),lp;
  ideal i=g^5,(x*f-g)^3,5*e-g^2,x*d^3;
  primaryTest(i,g);
```

4.6.2. The next procedure computes the primary decomposition of a zero–dimensional ideal.

proc zeroDecomp (ideal i)

```
  "USAGE:  zeroDecomp(i); i zero-dimensional ideal
  RETURN:  list l of lists of two ideals such that the
           intersection(l[j][1], j=1..)=i, the l[i][1] are
           primary and the l[i][2] their radicals
  NOTE:    algorithm of Gianni/Trager/Zacharias
  "
  {
    def  BAS = basering;
  //----the ordering is changed to the lexicographical one
    changeord("R","lp");
    ideal i=fetch(BAS,i);
    int n=nvars(R);
    int k;
    list result,rest;
    ideal primary,prim;
    option(redSB);

  //------the random coordinate change and its inverse
    ideal m=maxideal(1);
    m[n]=0;
    poly p=(random(100,1,n)*transpose(m))[1,1]+var(n);
    m[n]=p;
    map phi=R,m;
    m[n]=2*var(n)-p;
    map invphi=R,m;
    ideal j=groebner(phi(i));
  //-------------factorization of the first element in i
    list fac=factorize(j[1],2);
  //-------------computation of the primaries and primes
    for(k=1;k<=size(fac[1]);k++)
    {
      p=fac[1][k]^fac[2][k];
```

```
      primary=groebner(j+p);
      prim=primaryTest(primary,fac[1][k]);
//---test whether all ideals were primary and in general
//   position
      if(prim==0)
      {
        rest[size(rest)+1]=i+invphi(p);
      }
      else
      {
        result[size(result)+1]=
          list(std(i+invphi(p)),std(invphi(prim)));
      }
    }
//-------treat the bad cases collected in the rest again
   for(k=1;k<=size(rest);k++)
   {
     result=result+zeroDecomp(rest[k]);
   }
   option(noredSB);
   setring BAS;
   list result=imap(R,result);
   kill R;
   return(result);
}

ring  r = 32003,(x,y,z),dp;
poly  p = z2+1;
poly  q = z4+2;
ideal i = p^2*q^3,(y-z3)^3,(x-yz+z4)^4;
list pr = zeroDecomp(i);
pr;
```

4.6.3. Procedure to define for an independent set $u \subset x$ the ring $K(u)[x \smallsetminus u]$.

proc prepareQuotientring(ideal i)

```
"USAGE:   prepareQuotientring(i); i standard basis
RETURN:   a list l of two strings:
          l[1] to define K[x\u,u ], u a maximal independent
          set for i
          l[2] to define K(u)[x\u ], u a maximal independent
          set for i
          both rings with lexicographical ordering
"
{
```

```
  string va,pa;
//v describes the independent set u: var(j) is in
//u iff v[j]!=0
  intvec v=indepSet(i);
  int k;

  for(k=1;k<=size(v);k++)
  {
    if(v[k]!=0)
    {
      pa=pa+"var("+string(k)+"),";
    }
    else
    {
      va=va+"var("+string(k)+"),";
    }
  }

  pa=pa[1..size(pa)-1];
  va=va[1..size(va)-1];

  string newring="
  ring nring=("+charstr(basering)+"),("+va+","+pa+"),lp;";
  string quotring="
  ring quring=("+charstr(basering)+","+pa+"),("+va+"),lp;";
  return(newring,quotring);
}

ring s=(0,x),(a,b,c,d,e,f,g),dp;
ideal i=x*b*c,d^2,f-g;
i=std(i);
def Q=basering;
list l= prepareQuotientring(i);
l;
execute (l[1]);
basering;
execute (l[2]);
basering;
setring Q;
```

4.6.4. A procedure to collect the leading coefficients of a standard basis of an ideal in $K(u)[x \smallsetminus u]$. They are needed to compute $IK(u)[x \smallsetminus u] \cap K[x]$ via saturation.

proc prepareSat(ideal i)

```
{
   int k;
   poly p=leadcoef(i[1]);
   for(k=2;k<=size(i);k++)
   {
     p=p*leadcoef(i[k]);
   }
   return(p);
}
```

4.6.5. Using the above procedures, we can now present our procedure to compute a primary decomposition of an ideal.

proc decomp (ideal i)

```
"USAGE:  decomp(i); i ideal
RETURN:  list l of lists of two ideals such that the
         intersection(l[j][1], j=1..)=i, the l[i][1] are
         primary and the l[i][2] their radicals
NOTE:    algorithm of Gianni/Trager/Zacharias
"
{
   if(i==0)
   {
     return(list(i,i));
   }
   def  BAS = basering;
   ideal j;
   int n=nvars(BAS);
   int k;

   ideal SBi=std(i);
   int d=dim(SBi);
//---the trivial case and the zero-dimensional case
   if ((d==0)||(d==-1))
   {
      return(zeroDecomp(i));
   }
//---prepare the quotient ring with respect to a maximal
//   independent set
   list quotring=prepareQuotientring(SBi);
   execute (quotring[1]);
//---used to compute a standard basis of i*quring
//   which is in i
```

```
   ideal i=std(imap(BAS,i));
//---pass to the quotient ring with respect to a maximal
//   independent set
   execute (quotring[2]);
   ideal i=imap(nring,i);
   kill nring;
//---computation of the zero-dimensional decomposition
   list ra=zeroDecomp(i);
//---preparation for saturation
   list p;
   for(k=1;k<=size(ra);k++)
   {
     p[k]=list(prepareSat(ra[k][1]),prepareSat(ra[k][2]));
   }
   poly q=prepareSat(i);
//---back to the original ring
   setring BAS;
   list p=imap(quring,p);
   list ra=imap(quring,ra);
   poly q=imap(quring,q);
   kill quring;
//---compute the intersection of ra with BAS
   for(k=1;k<=size(ra);k++)
   {
     ra[k]=list(sat(ra[k][1],p[k][1])[1],
                sat(ra[k][2],p[k][2])[1]);
   }
   q=q^sat(i,q)[2];
//---i=intersection((i:q),(i,q)) and ra is the primary
//   decomposition of i:q
   if(deg(q)>0)
   {
     ra=ra+decomp(i+q);
   }
   return(ra);
}

ring  r = 0,(x,y,z),dp;
ideal i = intersect(ideal(x,y,z)^3,ideal(x-y-z)^2,
          ideal(x-y,x-z)^2);
list pr = decomp(i);
pr;
```

4.6.6. We pass to the computation of the equidimensional part of an ideal.

proc equidimensional (ideal i)

```
"USAGE:  equidimensional(i); i ideal
RETURN:  list l of two ideals such that intersection(l[1],
         l[2])=i if there are no embedded primes
         l[1] is equidimensional and dim(l[1])>dim(l[2])
"
{
   def  BAS = basering;

   ideal SBi=std(i);
   int d=dim(SBi);
   int n=nvars(BAS);
   int k;
   list result;

//----the trivial cases
   if ((d==-1)||(n==d)||(n==1)||(d==0))
   {
      result=i,ideal(1);
      return(result);
   }
//----prepare the quotient ring with respect to a maximal
//     independent set
   list quotring=prepareQuotientring(SBi);
   execute (quotring[1]);
//----we use this ring to compute a standard basis of
//     i*quring which is in i
   ideal eq=std(imap(BAS,i));
//----pass to the quotient ring with respect to a maximal
//     independent set
   execute (quotring[2]);
   ideal eq=imap(nring,eq);
   kill nring;
//----preparation for saturation
   poly p=prepareSat(eq);
//----back to the original ring
   setring BAS;
   poly p=imap(quring,p);
   ideal eq=imap(quring,eq);
   kill quring;
//----compute the intersection of eq with BAS
   eq=sat(eq,p)[1];
   SBi=std(quotient(i,eq));
```

```
    if(d>dim(SBi))
    {
      result=eq,SBi;
      return(result);
    }
    result=equidimensional(i);
    result=intersect(result[1],eq),result[2];
    return(result);
}

ring  r = 0,(x,y,z),dp;
ideal i = intersect(ideal(x,y,z)^3,ideal(x-y-z)^2,
          ideal(x-y,x-z)^2);
list pr = equidimensional(i);
pr;
dim(std(pr[1]));
dim(std(pr[2]));
option(redSB);
std(i);
std(intersect(pr[1],pr[2]));
```

4.6.7. Compute the squarefree part of a univariate polynomial f over a field of characteristic 0, depending on the i–th variable.

proc squarefree (poly f, int i)

```
{
  poly h=gcd(f,diff(f,var(i)));
  poly g=lift(h,f)[1][1];
  return(g);
}
```

4.6.8. Finally, a procedure to compute the radical of an ideal.

proc radical(ideal i)

```
"USAGE:  radical(i); i ideal
RETURN:  ideal = the radical of i
NOTE:    algorithm of Krick/Logar
"
{
   def  BAS = basering;
   ideal j;
   int n=nvars(BAS);
   int k;

   option(redSB);
```

```
   ideal SBi=std(i);
   option(noredSB);
   int d=dim(SBi);

//-----the trivial cases
   if ((d==-1)||(n==d)||(n==1))
   {
      return(ideal(squarefree(SBi[1],1)));
   }
//-----the zero-dimensional case
   if (d==0)
   {
      j=finduni(SBi);
      for(k=1;k<=size(j);k++)
      {
         i=i,squarefree(cleardenom(j[k]),k);
      }
      return(std(i));
   }
//-----prepare the quotientring with respect to a maximal
//     independent set
   list quotring=prepareQuotientring(SBi);
   execute (quotring[1]);
//-----we use this ring to compute a standardbasis of
//     i*quring which is in i
   ideal i=std(imap(BAS,i));
//-----pass to the quotientring with respect to a maximal
//     independent set
   execute( quotring[2]);
   ideal i=imap(nring,i);
   kill nring;
//-----computation of the zerodimensional radical
   ideal ra=radical(i);
//-----preparation for saturation
   poly p=prepareSat(ra);
   poly q=prepareSat(i);
//-----back to the original ring
   setring BAS;
   poly p=imap(quring,p);
   poly q=imap(quring,q);
   ideal ra=imap(quring,ra);
   kill quring;
//-----compute the intersection of ra with BAS
   ra=sat(ra,p)[1];
```

```
//----now we have radical(i)=intersection(ra,radical((i,q)))
   return(intersect(ra,radical(i+q)));
}

ring  r = 0,(x,y,z),dp;
ideal i =
intersect(ideal(x,y,z)^3,ideal(x-y-z)^2,ideal(x-y,x-z)^2);
ideal pr= radical(i);
pr;
```

The algorithms and, hence, the procedures work in characteristic 0. However, by our experience, the procedures in the library `primdec.lib`, distributed with SINGULAR, do also work for prime fields of finite characteristic provided that it is not too small. In fact, the procedures, although designed for characteristic 0, give a correct result for finite prime field whenever they terminate.