For example, let $S_1 = K[x_1, x_2]$, $S_2 = K[y_1, y_2, y_3]$, $S = K[x_1, x_2, y_1, y_2, y_3]$. Let $<_1$ be the lexicographic order on S_1, $<_2$ the reverse lexicographic order on S_2 and $<$ the product order of $<_1$ and $<_2$. Then

$$x_1x_2^2y_2^2 > x_1x_2^2y_1y_3 > x_1x_2y_2^5.$$

Let $<$ be any monomial order. We choose a vector $\mathbf{w} = (w_1, \ldots, w_n) \in \mathbb{R}^n$ with nonnegative entries, called **weight vector**. Then we define the new monomial order $<_{\mathbf{w}}$ as follows:

$$\mathbf{x^a} <_{\mathbf{w}} \mathbf{x^b}, \quad \text{if} \quad \mathbf{a}\cdot\mathbf{w} < \mathbf{b}\cdot\mathbf{w}, \quad \text{or else} \quad \mathbf{a}\cdot\mathbf{w} = \mathbf{b}\cdot\mathbf{w} \quad \text{and} \quad \mathbf{x^a} < \mathbf{x^b}.$$

Here $\mathbf{c}\cdot\mathbf{d} = \sum_{i=1}^n c_id_i$ is the standard scalar product on $\mathbb{R}^n$.

For example, if $<$ is the pure lexicographic order and we choose $\mathbf{w} = (1, 1, \ldots, 1)$ as weight vector, then $<_{\mathbf{w}}$ is the lexicographic order.

For later applications the following example is important.

Proposition 2.3. *Let $<$ be any monomial order on $K[x_1, \ldots, x_n]$. Fix an integer $1 \le t \le n$ and choose the weight vector $\mathbf{w} = (1, 1, \ldots, 1, 0, 0, \ldots, 0)$ with the first t entries being 1 and the remaining last entries being 0. Then the order $<_{\mathbf{w}}$ has the following property: if u, v are monomials such that $x_j|u$ for some $j \le t$, and x_j does not divide v for any $j \le t$, then $v <_{\mathbf{w}} u$.*

Proof. Let $u = \mathbf{x^a}$ and $v = \mathbf{x^b}$. Then $a_j \ne 0$ for some $j \le t$, hence $\mathbf{a}\cdot\mathbf{w} > 0$, while on the other hand, $b_j = 0$ for all $j \le t$. Therefore, $\mathbf{b}\cdot\mathbf{w} = 0$. This yields the desired conclusion. □

2.2. Initial ideals and Gröbner bases

2.2.1. The basic definitions. We now come to the main topic of this book. Let as before $S = K[x_1, \ldots, x_n]$ be the polynomial ring over the field K, and let $<$ be a monomial order on S.

If $f \ne 0$ is a polynomial in S, we set $\mathtt{in}_<(f)$ to be the largest monomial $u \in \operatorname{supp}(f)$ with respect to $<$, and call it the **initial monomial** of f. The coefficient c of $\mathtt{in}_<(f)$ in f is called the **leading coefficient** of f with respect to $<$, and $c\,\mathtt{in}_<(f)$ is called the **leading term** of f.

For convenience we set $\mathtt{in}_<(0) = 0$ and let $\mathtt{in}_<(0) < \mathtt{in}_<(f)$ for all $f \ne 0$.

For example, let $f = 2x_1^2x_3 + 3x_1x_2^2$. Then $\mathtt{in}_<(f) = x_1^2x_3$, if $<$ is the lexicographic order, and $\mathtt{in}_<(f) = x_1x_2^2$, if $<$ is the reverse lexicographic order.

For the initial monomial of a product or a sum of polynomials we have the following rules.

Lemma 2.4. *Let $<$ be a monomial order on S and let $f_1, \ldots, f_r$ be nonzero polynomials in S. Then*

(i) $\mathtt{in}_<(f_1 f_2 \cdots f_r) = \mathtt{in}_<(f_1)\,\mathtt{in}_<(f_2)\cdots\mathtt{in}_<(f_r)$;

(ii) $\mathtt{in}_<(f_1 + f_2 + \cdots + f_r) \leq \max\{\mathtt{in}_<(f_1), \mathtt{in}_<(f_2), \ldots, \mathtt{in}_<(f_r)\}$;

(iii) *Let c_j be the leading coefficient of f_j. Equality holds in* (ii) *if and only if $\sum_j c_j \neq 0$, where the sum is taken only over those j for which $\mathtt{in}_<(f_j) \geq \mathtt{in}_<(f_i)$ for all i.*

Proof. (i) Since for all $u \in \operatorname{supp}(f_i)$ we have $\mathtt{in}_<(f_i) \geq u$, it follows that

$$\mathtt{in}_<(f_1)\,\mathtt{in}_<(f_2)\cdots\mathtt{in}_<(f_r) \geq u_1 u_2 \cdots u_r$$

for all $u_i \in \operatorname{supp}(f_i)$. Equality holds if and only if $u_i = \mathtt{in}_<(f_i)$ for $i = 1, \ldots, r$. Since all monomials in $\operatorname{supp}(f_1 f_2 \cdots f_r)$ are of the form $u_1 u_2 \cdots u_r$ with $u_i \in \operatorname{supp}(f_i)$, and since $\mathtt{in}_<(f_1)\,\mathtt{in}_<(f_2)\cdots\mathtt{in}_<(f_r)$ belongs to the support of $f_1 f_2 \cdots f_r$, the assertion follows.

(ii) Observe that $\operatorname{supp}(f_1 + \cdots + f_r) \subseteq \bigcup_{i=1}^r \operatorname{supp}(f_i)$. This implies that

$$\begin{aligned} \mathtt{in}_<(f_1 + \cdots + f_r) &\leq \max\{u : u \in \bigcup_{i=1}^r \operatorname{supp}(f_i)\} \\ &= \max\{\mathtt{in}_<(f_1), \mathtt{in}_<(f_2), \ldots, \mathtt{in}_<(f_r)\}. \end{aligned}$$

(iii) Let u be the maximal initial monomial appearing among the f_i. Assuming that $\sum_j c_j \neq 0$, where the sum is taken over those j for which $\mathtt{in}_<(f_j) = u$, it follows that $u \in \operatorname{supp}(f_1 + \cdots + f_r)$. Therefore,

$$\mathtt{in}_<(f_1 + \cdots + f_r) \geq u = \max\{\mathtt{in}_<(f_1), \mathtt{in}_<(f_2), \ldots, \mathtt{in}_<(f_r)\}.$$

Thus, by (ii), equality holds.

Conversely, if $\sum_{j=1}^k c_j = 0$, then $u \notin \operatorname{supp}(f_1 + f_2 + \cdots + f_r)$, and hence $\mathtt{in}_<(f_1 + f_2 + \cdots + f_r) \neq \max\{\mathtt{in}_<(f_1), \mathtt{in}_<(f_2), \ldots, \mathtt{in}_<(f_r)\}$. □

Let $I \subset S$ be a nonzero ideal. The **initial ideal** of I is the monomial ideal

$$\mathtt{in}_<(I) = (\mathtt{in}_<(f) : f \in I,\ f \neq 0).$$

If $I = (0)$, then we set $\mathtt{in}_<(I) = (0)$.

Notice that $\mathtt{in}_<(I)$ is generated by the initial monomials of *all* nonzero polynomials in I. In general the initial monomials of a set of generators do *not* generate $\mathtt{in}_<(I)$. Consider, for example, the ideal

$$I = (f, g) \quad \text{with} \quad f = x_1x_2 - x_3x_4,\ g = -x_2^2 + x_1x_3.$$

With respect to the reverse lexicographic order $<$ we have $\mathtt{in}_<(f) = x_1x_2$ and $\mathtt{in}_<(g) = x_2^2$. On the other hand, $h = x_2 f + x_1 g = x_1^2x_3 - x_2x_3x_4 \in I$ and $\mathtt{in}_<(h) = x_1^2x_3$. Thus we see that $\mathtt{in}_<(h) \notin (\mathtt{in}_<(f), \mathtt{in}_<(g))$.

A priori $\mathtt{in}_<(I)$ is generated by infinitely many initial monomials. Nevertheless, since $\mathtt{in}_<(I)$ is a monomial ideal, as we know from Corollary 1.10, there exists $g_1, \ldots, g_m \in I$ such that

$$\mathtt{in}_<(I) = (\mathtt{in}_<(g_1), \ldots, \mathtt{in}_<(g_m)).$$

The observation leads to the most important concept studied in this book.

Definition 2.5. *Let $I \subset S$ be an ideal, and let $<$ be a monomial order on S. A sequence $g_1, \ldots, g_m$ of elements in I with $\mathtt{in}_<(I) = (\mathtt{in}_<(g_1), \ldots, \mathtt{in}_<(g_m))$ is called a **Gröbner basis** of I with respect to the monomial order $<$.*

The argument that we used to see that a Gröbner basis of I always exist does not tell us how to actually find a Gröbner basis. In case that I is a principal ideal, say $I = (g)$, one sees immediately that g is a Gröbner basis of I.

The Buchberger algorithm, which will be discussed in the next chapter, gives an efficient method to compute a Gröbner basis of an ideal. For many abstract arguments, however, it just suffices to know that a Gröbner basis always exists. First remarkable examples of such reasoning are the next theorems.

2.2.2. Macaulay's theorem. The following theorem is fundamental in Gröbner basis theory and it will be used several times later in the book.

Theorem 2.6 (Macaulay)**.** *Let $<$ be a monomial order on S, and let $I \subset S$ an ideal. Then the monomials in S which do not belong to $\mathtt{in}_<(I)$ form a K-basis of S/I.*

Proof. Suppose the monomials in S which do not belong to $\mathtt{in}_<(I)$ are K-linearly dependent modulo I. Then there exists a nonzero polynomial $f \in I$ with $\operatorname{supp}(f) \cap \operatorname{Mon}(\mathtt{in}_<(I)) = \emptyset$, where $\operatorname{Mon}(\mathtt{in}_<(I))$ denotes the set of monomials in $\mathtt{in}_<(I)$. This contradicts the fact that $\mathtt{in}_<(f) \in \mathtt{in}_<(I)$.

It remains to be shown that residue classes of the monomials in S which do not belong to $\mathtt{in}_<(I)$ generate the K-vector space S/I. To this end we will show that for any $f \in S$ there exists $g \in S$ with $f + I = g + I$ and $\operatorname{supp}(g) \cap \operatorname{Mon}(\mathtt{in}_<(I)) = \emptyset$. Suppose this is not the case, and let $f \in S$ be a polynomial with smallest initial monomial for which we cannot find a polynomial g as above. Let c be the leading coefficient of f. Then $f - c\,\mathtt{in}_<(f)$ has a smaller initial monomial, and hence there exists $g \in S$ with $\operatorname{supp}(g) \cap \operatorname{Mon}(\mathtt{in}_<(I)) = \emptyset$ and such that $(f - c\,\mathtt{in}_<(f)) + I = g + I$. Thus $f + I = (c\,\mathtt{in}_<(f) + g) + I$. If $\mathtt{in}_<(f) \notin \mathtt{in}_<(I)$, we may replace g by $c\,\mathtt{in}_<(f) + g$, contradicting the choice of f. If $\mathtt{in}_<(f) \in \mathtt{in}_<(I)$, then there exists $h \in I$ with leading coefficient 1 and $\mathtt{in}_<(h) = \mathtt{in}_<(f)$. It follows that $f - ch$ has a smaller initial monomial than f. Thus we can find a polynomial

$g \in S$ with $\operatorname{supp}(g) \cap \operatorname{Mon}(\mathtt{in}_<(I)) = \emptyset$ and $(f - ch) + I = g + I$. Since $f + I = (f - ch) + I$, this contradicts again the choice of f. □

On a polynomial ring with more than one variable there exist infinitely many different monomial orders; see Problem 2.4. However, as an application of Macaulay's theorem we show

Proposition 2.7. *Every ideal $I \subset S$ has only finitely many distinct initial ideals.*

Proof. Let $I \subset S$ be an ideal, and let $\mathcal{S}_0$ be the set of initial ideals of I. Assume that $\mathcal{S}_0$ is an infinite set. Let $0 \neq f_1 \in I$. To each initial ideal $J \in \mathcal{S}_0$ belongs a monomial $u \in \operatorname{supp}(f_1)$ with $u \in J$. Since $\operatorname{supp}(f_1)$ is a finite set, there exists $u_1 \in \operatorname{supp}(f_1)$ such that the set $\mathcal{S}_1 = \{J \in \mathcal{S}_0 \colon\ u_1 \in J\}$ is infinite. In particular, $J \neq (u_1)$ for at least one (in fact, infinitely many) $J \in \mathcal{S}_1$. Thus Theorem 2.6 implies that the monomials which do not belong to (u_1) are linearly dependent modulo I. Hence there exists $0 \neq f_2 \in I$ with $\operatorname{supp}(f_2) \cap (u_1) = \emptyset$. As before there exists $u_2 \in \operatorname{supp}(f_2)$ such that $\mathcal{S}_2 = \{J \in \mathcal{S}_1 \colon\ u_2 \in J\}$ is an infinite set. Since $u_2 \notin (u_1)$ it follows that (u_1) is strictly contained in (u_1, u_2). Again, since $\mathcal{S}_2$ is infinite, $J \neq (u_1, u_2)$ for some $J \in \mathcal{S}_2$, and as before we can construct an element $u_3 \notin (u_1, u_2)$. Proceeding in this way we construct an infinite strictly ascending sequence $(u_1) \subset (u_1, u_2) \subset (u_1, u_2, u_3) \subset \cdots$ of monomial ideals, contradicting Proposition 1.12. □

2.2.3. Hilbert's basis theorem. In the previous section we have seen that a system of generators of an ideal I need not to be a Gröbner basis of I. However, we have

Theorem 2.8. *Let $I \subset S$ be an ideal and let $g_1, \ldots, g_m$ be a Gröbner basis of I with respect to a monomial order $<$. Then $g_1, \ldots, g_m$ is a system of generators of I.*

Proof. If $f \in I$, then $\mathtt{in}_<(f) \in \mathtt{in}_<(I) = (\mathtt{in}_<(g_1), \ldots, \mathtt{in}_<(g_m))$. Therefore there exists an integer $1 \leq i \leq m$ and a monomial w such that $\mathtt{in}_<(f) = w\,\mathtt{in}_<(g_i)$. Let c be the coefficient of $\mathtt{in}_<(f)$ in f and d the coefficient of $\mathtt{in}_<(g_i)$ in g_i, and let $h = f - cd^{-1}wg_i$. Then $h \in I$. If $h = 0$, then $f = cd^{-1}wg_i \in (g_1, \ldots, g_m)$. Now assume $h \neq 0$. Since $\mathtt{in}_<(f) > \mathtt{in}_<(h)$ and since by Proposition 2.2 each strictly descending chain of monomials terminates, we may apply an induction argument and hence may assume that h is a linear combination of the g_i with coefficients in S. Since $f = h + cd^{-1}wg_i$, the same is true for f. □

Since each ideal has a Gröbner basis, and each Gröbner basis contains finitely many elements, we get

Corollary 2.9 (Hilbert's basis theorem)**.** *Each ideal in the polynomial ring $S = K[x_1, \ldots, x_n]$ is finitely generated.*

Hilbert's basis theorem says that the polynomial ring $S = K[x_1, \ldots, x_n]$ is Noetherian. It is known from general Commutative Algebra that a Noetherian ring is also characterized by the property that each ascending chain of ideals terminates. We will give a direct proof of this property for polynomial rings.

Proposition 2.10. *Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals in S. Then there exists an integer k such that $I_j = I_k$ for all $j \geq k$.*

Proof. Fix some monomial order $<$ on S. The given chain of ideals induces the following chain $\mathtt{in}_<(I_1) \subseteq \mathtt{in}_<(I_2) \subseteq \cdots$ of monomial ideals. By Proposition 1.12, there exists an integer k such that $\mathtt{in}_<(I_j) = \mathtt{in}_<(I_k)$ for all $j \geq k$. It follows from Problem 2.8 that $I_j = I_k$ for all $j \geq k$. □

2.3. The division algorithm

As announced in the introduction of this chapter we now discuss an extension of the classical division algorithm. The extension will be two-fold. On the one hand, the polynomials in one variable will be replaced by polynomials in several variables, and on the other hand, we may "divide" not only by one but if we wish by several polynomials at the same time. The precise statement is formulated in the next

Theorem 2.11. *Let f and $g_1, \ldots, g_m$ be polynomials in S with $g_i \neq 0$. Given a monomial order $<$, there exist polynomials $q_1, \ldots, q_m$ and a polynomial r in S with*

$$f = q_1 g_1 + q_2 g_2 + \cdots + q_m g_m + r$$

such that the following conditions are satisfied:

(i) *no element of* $\mathrm{supp}(r)$ *is contained in the ideal* $(\mathtt{in}_<(g_1), \ldots, \mathtt{in}_<(g_m))$;

(ii) $\mathtt{in}_<(f) \geq \mathtt{in}_<(q_i g_i)$ *for all i.*

An equation $f = q_1 g_1 + q_2 g_2 + \cdots + q_m g_m + r$ satisfying the conditions (i) and (ii) is called a **standard expression** of f, and r is called a **remainder** of f with respect to $g_1, \ldots, g_m$. The polynomial f may have different standard expressions and different remainders with respect to $g_1, \ldots, g_m$ as the following example demonstrates. Let $f = x_1 x_2 + x_2^2$, $g_1 = x_1 + x_2$ and $g_2 = x_1$. We let $<$ be the lexicographic order. Then

$$f = x_2 g_1 \quad \text{as well as} \quad f = x_2 g_2 + x_2^2$$

are standard expressions of f. In the first case the remainder is 0, in the second case the remainder is x_2^2.

4.4.2. Systems of linear equations over the polynomial ring. Consider the system of linear equations

$$\begin{aligned} a_{11}y_1 + a_{12}y_2 + \cdots + a_{1s}y_s &= b_1 \\ a_{21}y_1 + a_{22}y_2 + \cdots + a_{2s}y_s &= b_2 \\ \vdots \qquad\qquad\quad & \vdots \quad \vdots \\ a_{r1}y_1 + a_{r2}y_2 + \cdots + a_{rs}y_s &= b_r, \end{aligned} \tag{4.6}$$

where the a_{ij} and b_k are elements of the polynomial ring $S = K[x_1, \ldots, x_n]$. An element $(h_1, \ldots, h_s) \in S^s$ is called a solution of (4.6) if $\sum_{j=1}^{s} a_{ij}h_j = b_i$ for $i = 1, \ldots, r$. We denote by $\mathcal{L}$ the set of all solutions of (4.6). If we replace in (4.6) all b_i by 0, then we obtain the **homogeneous** system of linear equations associated to (4.6). Its set of solutions will be denoted by $\mathcal{L}_0$.

We will now show how $\mathcal{L}$ can be computed. From a theoretical point of view this is easy. Let G be the free module S^s with canonical basis $g_1, \ldots, g_s$, and F the free module S^r with the canonical basis $f_1, \ldots, f_r$.

1. *Existence of a solution.* Set $a_j = \sum_{i=1}^{r} a_{ij}f_i$ for $j = 1, \ldots, s$ and $b = \sum_{i=1}^{r} b_i f_i$, and let $U \subset F$ be the submodule generated by the elements $a_1, \ldots, a_s$. Then $\mathcal{L} \neq \emptyset$ if and only if $b \in U$.

Indeed, if $(h_1, \ldots, h_s) \in \mathcal{L}$, then

$$\begin{aligned} b &= \sum_{i=1}^{r} b_i f_i = \sum_{i=1}^{r} (\sum_{j=1}^{s} a_{ij}h_j) f_i \\ &= \sum_{j=1}^{s} h_j (\sum_{i=1}^{r} a_{ij} f_i) = \sum_{j=1}^{s} h_j a_j. \end{aligned}$$

Reading these equalities backwards we see that if $b = \sum_{j=1}^{s} h_j a_j$, then $(h_1, \ldots, h_s) \in \mathcal{L}$.

2. *Description of* $\mathcal{L}$. Let $\epsilon\colon G \to U$ be the epimorphism with $\epsilon(g_j) = a_j$ for $j = 1, \ldots, s$. Then $V = \mathrm{Syz}(a_1, \ldots, a_s)$ is the kernel of ϵ. Thus $h_1g_1 + h_2g_2 + \cdots + h_sg_s \in V$, if and only if $\sum_{j=1}^{s} h_j a_j = 0$. This is equivalent to saying that $\sum_{j=1}^{s} a_{ij}h_j = 0$ for $i = 1, \ldots, r$. In other words, the syzygies of $a_1, \ldots, a_s$ correspond to the elements of $\mathcal{L}_0$.

Now, if $\mathcal{L} \neq \emptyset$ and $(h_1, \ldots, h_s) \in \mathcal{L}$ is a **particular solution**, then

$$\mathcal{L} = (h_1, \ldots, h_s) + \mathcal{L}_0 = \{(h_1 + h'_1, \ldots, h_s + h'_s)\colon \sum_{j=1}^{s} h'_j g_j \in V\}.$$

It follows from this discussion that in order to describe the elements of $\mathcal{L}$ explicitly we have to proceed as follows:

(i) Decide whether $b \in U$. If yes, then $\mathcal{L} \neq \emptyset$;

(ii) If $b \in U$, then express b as a linear combination of the generators $a_1, \ldots, a_s$. The coefficients of this linear combination give us a particular solution;

(iii) Compute a system of generators of $V = \mathrm{Syz}(a_1, \ldots, a_s)$. Then any element in $\mathcal{L}$ can be expressed as a sum of the particular solution and a linear combination of the generators of V.

For Step (iii) we have to find an algorithm to compute $\mathrm{Syz}(a_1, \ldots, a_s)$ for the given set of generators $a_1, \ldots, a_s$ of $U \subset F$ (which is not necessarily a Gröbner basis of U, as is assumed in Theorem 4.12). The following two lemmata tell us how we can do this.

Lemma 4.14. *Let W be the submodule of $F \oplus G$ generated by the elements $a_j + g_j$ for $j = 1, \ldots, s$. Then*

$$\mathrm{Syz}(a_1, \ldots, a_s) = W \cap G.$$

Proof. Let $w \in W$; then $w = \sum_{j=1}^{s} h_j(a_j + g_j)$ for suitable $h_j \in S$. It follows that $w \in W \cap G$ if and only if $\sum_{j=1}^{s} h_j a_j = 0$, which is the case if and only if $w \in \mathrm{Syz}(a_1, \ldots, a_s)$. □

The intersection $W \cap G$ can be easily computed by using Gröbner bases.

Lemma 4.15. *Let H be a free S-module with basis $e_1, \ldots, e_n$ and W a submodule of H. Let $1 \leq m \leq n$ be an integer and G be the free submodule of H with basis $e_m, \ldots, e_n$, and let $<$ be the lexicographic order on H with $e_1 > e_2 > \cdots > e_n$. Furthermore, let $\mathcal{G} = w_1, \ldots, w_r$ be a Gröbner basis of W with respect to $<$. We may assume that $\mathtt{in}_<(w_i) \in G$ if and only if $i \in \{1, \ldots, s\}$. Then $w_1, \ldots, w_s$ is a Gröbner basis of $W \cap G$.*

Proof. Let $w \in W \cap G$. Then $w = \sum_{i=k}^{n} c_i e_i$ with $c_i \in S$, $c_k \neq 0$ and $k \geq m$. Since $\mathcal{G}$ is Gröbner basis of W, we have $\mathtt{in}_<(w) = u\,\mathtt{in}_<(w_j)$ for some j and some monomial u. Since $\mathtt{in}_<(w) = \mathtt{in}(c_k)e_k$ it follows that $\mathtt{in}_<(w_j) = \mathtt{in}_<(d_k)e_k$ for some nonzero polynomial $d_k \in S$. The definition of the lexicographic order implies that $w_j = \sum_{i=k}^{n} d_i e_i$ with certain polynomials $d_i \in S$. In particular, $w_j \in G$ and $j \leq s$. This proves the assertion. □

Now we are ready to describe the algorithm to compute the set of solutions $\mathcal{L}$ of the system (4.6) of linear equations.

For Step (iii) we proceed as described in Lemma 4.14 and Lemma 4.15. For the Steps (i) and (ii) we apply again Lemma 4.14 and Lemma 4.15 to first compute $\mathrm{Syz}(a_1, \ldots, a_s, b)$. In other words, we compute the Gröbner basis

$\mathcal{G}'$ of $W' \subset F \oplus G'$, where G' is the free S-module with basis $g_1, g_2, \ldots, g_{s+1}$ and where W' is generated by the elements $a_j + g_j$ for $j = 1, \ldots, s$ and the element $b + g_{s+1}$. Let $w_1, \ldots, w_t$ be those elements of $\mathcal{G}'$ with $\mathtt{in}_<(w_i) \in G'$. Then these elements form a Gröbner basis of $\mathrm{Syz}(a_1, \ldots, a_s, b)$. Hence if $w_i = \sum_{j=1}^{s+1} h_{ij} g_j$, then $h_{i,s+1} b = -\sum_{j=1}^{s} h_{ij} a_j$. It follows that $b \in (a_1, \ldots, a_s)$ if and only if one of the $h_{i,s+1}$ is a nonzero constant polynomial. If this is the case and, say, $h_{i,s+1} = c$ with $c \in K \setminus \{0\}$, then we get the following presentation of b as the linear combination of the a_j, namely

$$b = -c^{-1} h_{i1} a_1 - c^{-1} h_{i2} a_2 - \cdots - c^{-1} h_{is} a_s.$$

The following example demonstrates this algorithm. We want to find the set of solutions $\mathcal{L}$ of the system of linear equations

$$\begin{aligned} x_1 y_1 + x_2 y_2 + x_3 y_3 &= -x_1^2 + x_2^2 + x_3^2 \\ (x_2 + x_3) y_1 + (x_1 + x_3) y_2 + (x_1 + x_2) y_3 &= 2 x_2 x_3 \end{aligned}$$

with coefficients in $S = K[x_1, x_2, x_3]$.

Let $a_1 = x_1 e_1 + (x_2 + x_3) e_2$, $a_2 = x_2 e_1 + (x_1 + x_3) e_2$, $a_3 = x_3 e_1 + (x_1 + x_2) e_2$ and $b = (-x_1^2 + x_2^2 + x_3^2) e_1 + 2 x_2 x_3 e_2$. For the Steps (i) and (ii) we have to compute (with respect to the lexicographic order) the Gröbner basis of the submodule $W' \subset \bigoplus_{i=1}^{6} S e_i$ generated by

$$a_1 + e_3, a_2 + e_4, a_3 + e_5, b + e_6.$$

The calculation shows that the Gröbner basis of W' consists of the above generators and the additional elements

$$\begin{aligned} (x_1^2 - x_2^2 - x_1 x_3 + x_2 x_3) e_4 + (x_1^2 + x_1 x_2 - x_2 x_3 + x_3^2) e_5 + (x_2 - x_3) e_6, \\ (x_2 - x_3) e_3 + (-x_1 + x_3) e_4 + (x_1 - x_2) e_5, \\ x_1 e_3 - x_2 e_4 - x_3 e_5 + e_6, \\ (x_1 x_2 + x_2^2 - x_1 x_3 - x_3^2) e_2 - x_3 e_4 + x_2 e_5, \\ (x_1^2 - x_2^2 + x_1 x_3 - x_2 x_3) e_2 - x_3 e_3 + x_3 e_4 + (x_1 - x_2) e_5. \end{aligned}$$

The element $x_1 e_3 - x_2 e_4 - x_3 e_5 + e_6$ tells us that the linear system of equations is solvable and that $(-x_1, x_2, x_3)$ is a particular solution.

For Step (iii) it is required to compute the Gröbner basis of the submodule $W \subset \bigoplus_{i=1}^{5} S e_i$ generated by

$$a_1 + e_3, a_2 + e_4, a_3 + e_5.$$

The Gröbner basis consists of these generators and the additional elements

$$\begin{aligned} (x_2 - x_3) e_3 + (-x_1 + x_3) e_4 + (x_1 - x_2) e_5, \\ (x_1 x_2 + x_2^2 - x_1 x_3 - x_3^2) e_2 - x_3 e_4 + x_2 e_5, \\ (x_1^2 - x_2^2 + x_1 x_3 - x_2 x_3) e_2 - x_3 e_3 + x_3 e_4 + (x_1 - x_2) e_5. \end{aligned}$$

From this we see that $\mathrm{Syz}(a_1, a_2, a_3)$ is generated by

$$(x_2 - x_3)e_3 + (-x_1 + x_3)e_4 + (x_1 - x_2)e_5.$$

Thus we obtain as the final result that the set of solutions of our linear system of equations is given by

$$\mathcal{L} = \{(-x_1, x_2, x_3) + f \cdot (x_2 - x_3, -x_1 + x_3, x_1 - x_2) \colon\ f \in S\}.$$

4.4.3. Schreyer's theorem. Our next goal is to show that each finitely generated S-module has a free resolution of length at most n, where n is the number of variables of the polynomial ring S. This is the celebrated **syzygy theorem** of Hilbert. We prove this theorem by using Gröbner bases following the arguments given by Schreyer [**Sc80**], who found this new proof of Hilbert's syzygy theorem. The essential idea is to choose suitable monomial orders in the computation of the syzygies.

Let F be a free S-module with basis $e_1, \ldots, e_r$ and $<$ a monomial order on F. Let $U \subset F$ be generated by $f_1, \ldots, f_m$, G a free S-module with basis $g_1, \ldots, g_m$, and $\epsilon \colon G \to U$ the epimorphism with $\epsilon(g_j) = f_j$ for $j = 1, \ldots, m$. We define a monomial order on G, again denoted $<$, as follows. Let ug_i and vg_j be monomials in G. Then we set

$$ug_i < vg_j \iff \mathtt{in}_<(uf_i) < \mathtt{in}_<(vf_j), \text{ or } \mathtt{in}_<(uf_i) = \mathtt{in}_<(vf_j) \text{ and } j < i.$$

Let us verify that $<$ is a monomial order on G. In order to see that $<$ is a total order on the monomials of G, we have to show that either $ug_i < vg_j$ or $ug_i \geq vg_j$.

Assume that we have $ug_i \not< vg_j$. Then $\mathtt{in}_<(uf_i) \not< \mathtt{in}_<(vf_j)$, and either $\mathtt{in}_<(uf_i) \neq \mathtt{in}_<(vf_j)$ or $j \geq i$. In the first case $\mathtt{in}_<(uf_i) > \mathtt{in}_<(vf_j)$, since $<$ is a total order on F. It follows in this case that $ug_i > vg_j$. In the second case $\mathtt{in}_<(uf_i) = \mathtt{in}_<(vf_j)$ and $j \geq i$. In this case $ug_i \geq vg_j$, by the definition of $<$ on G.

Next we check conditions (1) and (2) for monomial orders as defined before:

(1) Let $w \in \mathrm{Mon}(S)$, $w \neq 1$. Then $\mathtt{in}_<(uf_i) < w\,\mathtt{in}_<(uf_i) = \mathtt{in}_<(wuf_i)$, therefore $ug_i < wug_i$.

(2) Let $ug_i < vg_j$ and $w \in \mathrm{Mon}(S)$. If $\mathtt{in}_<(uf_i) < \mathtt{in}_<(vf_j)$, then $\mathtt{in}_<(wuf_i) = w\,\mathtt{in}_<(uf_i) < w\,\mathtt{in}_<(vf_j) = \mathtt{in}_<(wvf_j)$, and so $wug_i < wvg_j$. On the other hand, if $\mathtt{in}_<(uf_i) = \mathtt{in}_<(vf_j)$, then $j < i$ and $\mathtt{in}_<(wuf_i) = \mathtt{in}_<(wvf_j)$. So again, $wug_i < wvg_j$.

We call this monomial order defined on G the monomial order induced by $f_1, \ldots, f_m$ (and the monomial order $<$ on F).

The crucial result [**Sc80**] is now the following:

6.3. Generalized Hibi rings

In 1985 Hibi [**Hi87**] introduced a class of algebras which nowadays are called **Hibi rings**. They are semigroup rings attached to finite posets, and may be viewed as natural generalizations of polynomial rings. Indeed, a polynomial ring in n variables over a field K is just the Hibi ring of the poset $[n] = \{1, 2, \ldots, n\}$.

Hibi rings appear naturally in various combinatorial and algebraic contexts, for example, in invariant theory.

Let $P = \{p_1, \ldots, p_n\}$ be a finite poset. A **poset ideal** I of P is a subset of P which satisfies the following condition. For every $p \in I$, if $q \in P$ and $q \leq p$, then $q \in I$. Let $\mathcal{I}(P)$ be the set of the poset ideals of P. It is easily seen that $\mathcal{I}(P)$ is a sublattice of the power set of P, hence it is a distributive lattice. By Birkhoff's theorem any finite distributive lattice arises in this way. Let K be a field. Then the Hibi ring over K attached to P is the toric ring $K[\mathcal{I}(P)]$ generated by the set of monomials $\{x_I t\colon\ I \in \mathcal{I}(P)\}$ where $x_I = \prod_{p_i \in I} x_i$. Let $T = K[\{t_I\colon\ t_I \in \mathcal{I}(P)\}]$ be the polynomial ring in the variables t_I over K, and $\varphi\colon T \to K[\mathcal{I}(P)]$ the K-algebra homomorphism with $t_I \mapsto x_I t$. One fundamental result concerning Hibi rings is that the toric ideal $L_P = \operatorname{Ker} \varphi$ has a reduced Gröbner basis consisting of the so-called **Hibi relations**:

$$t_I t_J - t_{I \cap J} t_{I \cup J} \quad \text{with} \quad I \not\subseteq J \quad \text{and} \quad J \not\subseteq I.$$

Hibi showed [**Hi87**] that any Hibi ring is a normal Cohen–Macaulay domain, and that it is Gorenstein if and only if the attached poset P is pure, that is, all maximal chains of P have the same cardinality.

More generally, for any lattice $\mathcal{L}$, not necessarily distributive, one may consider the K algebra $K[\mathcal{L}]$ with generators y_α, $\alpha \in \mathcal{L}$, and relations $y_\alpha y_\beta = y_{\alpha \wedge \beta} y_{\alpha \vee \beta}$ where $\wedge$ and $\vee$ denote meet and join in $\mathcal{L}$. Hibi showed that $K[\mathcal{L}]$ is a domain if and only if $\mathcal{L}$ is distributive, in other words, if $\mathcal{L}$ is an ideal lattice of a poset.

Hibi ideals were first introduced in [**HH05**]. To each finite poset $P = \{p_1, \ldots, p_n\}$, one may attach the **Hibi ideal** H_P as the monomial ideal in the polynomial ring with $2n$ indeterminates $K[x_1, \ldots, x_n, y_1, \ldots, y_n]$ generated by the monomials $x_I y_{P \setminus I}$ with $I \in \mathcal{I}(P)$. Note that the toric ring generated over K by these monomials is isomorphic to the Hibi ring attached to P.

We now present the theory of generalized Hibi rings as introduced in [**EHM10**].

Let $\mathcal{I}(P)$ be the set of poset ideals of P and r a positive integer. An **r-multichain** of $\mathcal{I}(P)$ is a chain of poset ideals of length r,

$$\mathcal{I} : I_1 \subseteq I_2 \subseteq \cdots \subseteq I_r = P.$$

We define a partial order on the set $\mathcal{I}_r(P)$ of all r-multichains of $\mathcal{I}(P)$ by setting $\mathcal{I} \leq \mathcal{I}'$ if $I_k \subseteq I'_k$ for $k = 1, \ldots, r$. Observe that the partially ordered set $\mathcal{I}_r(P)$ is a distributive lattice, if we define the meet of $\mathcal{I}\colon I_1 \subseteq \cdots \subseteq I_r$ and $\mathcal{I}'\colon I'_1 \subseteq \cdots \subseteq I'_r$ as $\mathcal{I} \cap \mathcal{I}'$ where $(\mathcal{I} \cap \mathcal{I}')_k = I_k \cap I'_k$ for $k = 1, \ldots, r$, and the join as $\mathcal{I} \cup \mathcal{I}'$ where $(\mathcal{I} \cup \mathcal{I}')_k = I_k \cup I'_k$ for $k = 1, \ldots, r$.

With each r-multichain of $\mathcal{I}_r(P)$ we associate a monomial $u_{\mathcal{I}}$ in the polynomial ring $S = K[\{x_{ij} : 1 \leq i \leq r, 1 \leq j \leq n\}]$ in rn indeterminates which is defined as

$$u_{\mathcal{I}} = x_{1J_1} x_{2J_2} \cdots x_{rJ_r},$$

where $x_{kJ_k} = \prod_{p_\ell \in J_k} x_{k\ell}$ and $J_k = I_k \setminus I_{k-1}$ for $k = 1, \ldots, r$.

Lemma 6.18. *Let $\mathcal{I}$ and $\mathcal{I}'$ be two r-multichains of $\mathcal{I}(P)$. Then*

$$u_{\mathcal{I}} u_{\mathcal{I}'} = u_{\mathcal{I} \cup \mathcal{I}'} u_{\mathcal{I} \cap \mathcal{I}'}.$$

Proof. Indeed, the equality holds if and only if

$$\frac{x_{tI_t}}{x_{tI_{t-1}}} \cdot \frac{x_{tI'_t}}{x_{tI'_{t-1}}} = \frac{x_{tI_t \cap I'_t}}{x_{tI_{t-1} \cap I'_{t-1}}} \cdot \frac{x_{tI_t \cup I'_t}}{x_{tI_{t-1} \cup I'_{t-1}}}$$

for $t = 1, \ldots, r$.

In order to see that this identity holds, just observe that

$$x_{tI_t \cap I'_t} = \gcd\{x_{tI_t}, x_{tI'_t}\}, \quad x_{tI_{t-1} \cap I'_{t-1}} = \gcd\{x_{tI_{t-1}}, x_{tI'_{t-1}}\},$$

and

$$x_{tI_t \cup I'_t} = \frac{x_{tI_t} \cdot x_{tI'_t}}{\gcd\{x_{tI_t}, x_{tI'_t}\}} \quad x_{tI_{t-1} \cup I'_{t-1}} = \frac{x_{tI_{t-1}} \cdot x_{tI'_{t-1}}}{\gcd\{x_{tI_{t-1}}, x_{tI'_{t-1}}\}}.$$

□

Theorem 6.19. *The set of monomials $\{u_{\mathcal{I}} : \mathcal{I} \in \mathcal{I}_r(P)\} \subset S_{rn}$ is sorted with respect to $x_{11} > x_{21} > \cdots > x_{r1} > x_{12} > \cdots > x_{r2} > \cdots > x_{1n} > \cdots > x_{rn}$.*

Proof. Let $\mathcal{I}, \mathcal{I}' \in \mathcal{I}_r(P)$ be two r-multichains. We show that, with respect to the given order of the indeterminates, $\operatorname{sort}(u_{\mathcal{I}}, u_{\mathcal{I}'}) = (u_{\mathcal{I} \cup \mathcal{I}'}, u_{\mathcal{I} \cap \mathcal{I}'})$. By Lemma 6.18, we have $u_{\mathcal{I}} u_{\mathcal{I}'} = u_{\mathcal{I} \cup \mathcal{I}'} u_{\mathcal{I} \cap \mathcal{I}'}$. Next, we notice that for every $1 \leq j \leq n$, there exist uniquely determined $1 \leq k, \ell \leq r$ such that $p_j \in I_k \setminus I_{k-1}$ and $p_j \in I'_\ell \setminus I'_{\ell-1}$. Therefore, $x_{\ell j}$ and x_{kj} are the unique indeterminates with second index j which divide the product $u_{\mathcal{I}} u_{\mathcal{I}'}$. If $k = \ell$, then obviously x_{kj} divides $u_{\mathcal{I} \cup \mathcal{I}'}$ and $u_{\mathcal{I} \cap \mathcal{I}'}$. Let $k < \ell$. By the definition of the sorting and the chosen order of indeterminates, the conclusion follows once we show that $x_{kj} | u_{\mathcal{I} \cup \mathcal{I}'}$ and $x_{\ell j} | u_{\mathcal{I} \cap \mathcal{I}'}$. Since $k < \ell$ and $p_j \in I_k$, we obtain $p_j \in I_\ell$ as well. Therefore, we get $p_j \in (I_\ell \cap I'_\ell) \setminus (I_{\ell-1} \cap I'_{\ell-1})$ since $p_j \notin I'_{\ell-1}$. We thus have $x_{\ell j} | u_{\mathcal{I} \cap \mathcal{I}'}$. On the other hand, as $p_j \notin I'_{\ell-1}$ and $k < \ell$, it follows that $p_j \notin I'_{k-1}$, thus $p_j \in (I_k \cup I'_k) \setminus (I_{k-1} \cup I'_{k-1})$. Therefore, $x_{kj} | u_{\mathcal{I} \cup \mathcal{I}'}$ and the proof is completed. □

Let $R_r(P)$ be the K-subalgebra of S generated by the set $\{u_{\mathcal{I}} : \mathcal{I} \in \mathcal{I}_r(P)\}$. The ring $R_r(P)$ is called a **generalized Hibi ring**. This naming is justified by the fact that for $r = 2$ one obtains the classical Hibi ring. Let T be the polynomial ring over K in the set of indeterminates $\{t_{\mathcal{I}} : \mathcal{I} \in \mathcal{I}_r(P)\}$. Furthermore, let $\varphi\colon T \to R_r(P)$ be the surjective K-algebra homomorphism with $\varphi(t_{\mathcal{I}}) = u_{\mathcal{I}}$ for all $\mathcal{I} \in \mathcal{I}_r(P)$.

By applying Theorem 6.16 and Theorem 6.19 we get the following

Theorem 6.20. *The set*

$$\mathcal{G} = \{t_{\mathcal{I}}t_{\mathcal{I}'} - t_{\mathcal{I}\cup\mathcal{I}'}t_{\mathcal{I}\cap\mathcal{I}'} \in T : \mathcal{I}, \mathcal{I}' \in \mathcal{I}_r(P) \text{ incomparable}\},$$

is a reduced Gröbner basis of the ideal $L_r = \operatorname{Ker}\varphi$ with respect to the sorting order on T induced by $x_{11} > x_{21} > \cdots > x_{r1} > x_{12} > \cdots > x_{r2} > \cdots > x_{1n} > \cdots > x_{rn}$.

Corollary 6.21. *For any poset P and all integers $r \geq 1$, the toric ring $R_r(P)$ is a normal Cohen–Macaulay domain.*

It is interesting that the set of binomials which gives the reduced Gröbner basis of L_r with respect to the sorting order coincides with the reduced Gröbner basis with respect to the reverse lexicographic order induced by a total order of indeterminates with the property that $\mathcal{I} < \mathcal{I}'$ implies that $t_{\mathcal{I}} > t_{\mathcal{I}'}$.

Theorem 6.22. *The set*

$$\mathcal{G} = \{t_{\mathcal{I}}t_{\mathcal{I}'} - t_{\mathcal{I}\cup\mathcal{I}'}t_{\mathcal{I}\cap\mathcal{I}'} \in T : \mathcal{I}, \mathcal{I}' \in \mathcal{I}_r(P) \text{ incomparable}\},$$

is a reduced Gröbner basis of the ideal $L_r = \operatorname{Ker}\varphi$ with respect to the reverse lexicographic order induced by the given order of the variables $t_{\mathcal{I}}$.

Proof. Let $\prod_{s=1}^{q} t_{\mathcal{I}_s} - \prod_{s=1}^{q} t_{\mathcal{I}'_s}$ be a primitive binomial in L_r with initial monomial $\prod_{s=1}^{q} t_{\mathcal{I}_s}$. We are going to show that there are two indices k and ℓ such that $\mathcal{I}_k$ and $\mathcal{I}_\ell$ are incomparable r-multichains of ideals, and that $t_{\mathcal{I}_k}t_{\mathcal{I}_\ell}$ is the leading monomial of $t_{\mathcal{I}_k}t_{\mathcal{I}_\ell} - t_{\mathcal{I}_k\cup\mathcal{I}_\ell}t_{\mathcal{I}_k\cap\mathcal{I}_\ell}$. This will then show that $\mathcal{G}$ is Gröbner basis of L_r. It is obvious that $\mathcal{G}$ is actually reduced.

Suppose to the contrary that $\mathcal{I}_1 \leq \mathcal{I}_2 \leq \ldots \leq \mathcal{I}_q$. We will show that $\mathcal{I}'_s < \mathcal{I}_q$ for all s. Indeed, since $\prod_{s=1}^{q} t_{\mathcal{I}_s} - \prod_{s=1}^{q} t_{\mathcal{I}'_s} \in L_r$ we see that $\prod_{s=1}^{q} u_{\mathcal{I}_s} = \prod_{s=1}^{q} u_{\mathcal{I}'_s}$. It follows that

$$\prod_{s=1}^{q}\Big(\prod_{k=1}^{\ell} x_{kI_{sk}\setminus I_{sk-1}}\Big) = \prod_{s=1}^{q}\Big(\prod_{k=1}^{\ell} x_{kI'_{sk}\setminus I'_{sk-1}}\Big) \quad \text{for all } \ell = 1, \ldots, r.$$

Here $\mathcal{I}_s$ is the r-multichain of ideals $I_{s1} \subseteq I_{s2} \subseteq \cdots \subseteq I_{sr} = P$, and $\mathcal{I}'_s$ the r-multichain of ideals $I'_{s1} \subseteq I'_{s2} \subseteq \cdots \subseteq I'_{sr} = P$.

Now for all j and k we apply the substitution $x_{kj} \mapsto x_j$, and obtain

$$\prod_{s=1}^{q} x_{I_{s\ell}} = \prod_{s=1}^{q} x_{I'_{s\ell}}, \quad \ell = 1, \ldots, r,$$

where $x_J = \prod_{j \in J} x_j$ for $J \subset [n]$.

Since $\mathcal{I}_1 \leq \mathcal{I}_2 \leq \cdots \leq \mathcal{I}_q$, it follows that $\operatorname{supp}(\prod_{s=1}^{q} x_{I_{s\ell}}) = I_{q\ell}$. Thus the equation $\prod_{s=1}^{q} x_{I_{s\ell}} = \prod_{s=1}^{q} x_{I'_{s\ell}}$ implies that $x_{I'_{s\ell}} | x_{I_{q\ell}}$ for all ℓ and all s. It follows that $\mathcal{I}'_s \leq \mathcal{I}_q$. We cannot have equality, since $\prod_{s=1}^{q} t_{\mathcal{I}_s} - \prod_{s=1}^{q} t_{\mathcal{I}'_s}$ is a primitive binomial. This contradicts the fact that $\prod_{s=1}^{q} t_{\mathcal{I}_s}$ is the initial monomial of $\prod_{s=1}^{q} t_{\mathcal{I}_s} - \prod_{s=1}^{q} t_{\mathcal{I}'_s}$.

Finally, $t_{\mathcal{I}_k} t_{\mathcal{I}_\ell}$ is the leading monomial of $t_{\mathcal{I}_k} t_{\mathcal{I}_\ell} - t_{\mathcal{I}_k \cup \mathcal{I}_\ell} t_{\mathcal{I}_k \cap \mathcal{I}_\ell}$ thanks to the monomial order on T. □

6.4. Gröbner bases for Rees rings

6.4.1. The ℓ-exchange property. This subsection is devoted to the study of the Gröbner bases of presentation ideals of Rees rings defined by monomial ideals.

Let $I \subset S = K[x_1, \ldots, x_n]$ be a graded ideal. Recall from Example 3.10 that the Rees ring of $I = (f_1, \ldots f_m)$, denoted by $\mathcal{R}(I)$, is the graded subring of $S[t]$ given by

$$\mathcal{R}(I) = \bigoplus_{j \geq 0} I^j t^j = S[f_1 t, \ldots, f_m t].$$

The Rees ring $\mathcal{R}(I)$ has the presentation

$$\varphi : R = S[y_1, \ldots, y_m] \longrightarrow \mathcal{R}(I),$$

defined by

$$x_i \mapsto x_i \quad \text{for} \quad 1 \leq i \leq n \quad \text{and} \quad y_j \mapsto f_j t \quad \text{for} \quad 1 \leq j \leq m.$$

The ideal $J = \operatorname{Ker}(\varphi) \subset S[y_1, \ldots, y_m]$ is called **the presentation ideal** of $\mathcal{R}(I)$.

In the following we concentrate on the case that $I = (u_1, \ldots, u_m)$ is a monomial ideal generated in one degree. In this case R is a polynomial ring which admits a natural bigraded K-algebra structure which is given by setting $\deg(x_i) = (1, 0)$ for $i = 1, \ldots, n$ and $\deg(y_j) = (0, 1)$ for $j = 1, \ldots, m$.

On the other hand, let $T = K[y_1, \ldots, y_m]$ and L be the toric ideal of $K[u_1, \ldots, u_m]$ which is the kernel of the surjective homomorphism

$$\psi : T \to K[u_1, \ldots, u_m]$$

defined by $\psi(y_i) = u_i$ for all i.