2. Involution I: Algebraic Theory

By the help of God and with His precious assistance, I say that Algebra is a scientific art.

Omar Khayyam

The first chapter was mainly concerned with the geometry behind the formal theory. For many problems a purely geometric approach is not sufficient and some additional algebraic ingredients are needed. These lead us to the title concept of this book: involution. We use in this chapter a rather abstract presentation that at first sight has no relations at all to differential equations but is rooted in commutative algebra. Only in the next chapter we will see how these algebraic ingredients appear in the analysis of the (geometric) symbol of a differential equation.

In the first section we introduce the notion of an involutive division, a restriction of the usual divisibility relation of power products. As we are interested in applications beyond the commutative case, we introduce the theory not for power products but more abstractly for the monoid of multi indices. Similarly, we proceed not just to the usual polynomial ring but to a more general class of not necessarily commutative algebras: the polynomial algebras of solvable types. They are introduced with many examples like rings of linear differential or difference operators or universal enveloping algebras of Lie algebras in Section 2.2.

In the following section we introduce involutive bases for arbitrary algebras of solvable type. It turns out that they may be understood as a special kind of Gröbner bases with additional combinatorial properties. The question of their existence and construction is postponed to Chapter 6; here we are only concerned with some elementary consequences of the definition. The fourth section studies in more details Pommaret bases which are for us the most important involutive bases. In particular, the problem of δ-regularity requires some scrutiny.

In Section 2.5 we motivate our approach to involution by discussing combinatorial decompositions of polynomial modules. It is a trivial fact that any involutive basis allows us to identify the submodule it generates with the direct sum of some free modules. Arbitrary polynomial modules may be presented as the quotient of a free module by one of its submodule. Any Gröbner basis of this submodule induces a Stanley decomposition, i. e. a vector space isomorphism between the module and a direct sum of free modules. A trivial application is the straightforward determination of the Hilbert function of the module. Pommaret bases lead to a special kind of decompositions, namely Rees decompositions, and thus provide us with a simple realisation of Hironaka's criterion for Cohen-Macaulay modules.

In the final section we study as a further application of involutive bases syzygies and free resolutions. Again Pommaret bases possess special properties. Given a Pommaret basis of a module, it is straightforward to construct a Pommaret basis of its syzygy module. By iteration, we easily obtain the full syzygy resolution and a stronger form of Hilbert's Syzygy Theorem. Finally, we show that the degree of a Pommaret basis is nothing but the Castelnuovo–Mumford regularity.

This chapter requires some familiarity with basic concepts in commutative algebra, in particular with Gröbner bases. Our introduction of involutive bases is closely modelled on a classical approach to Gröbner bases. A brief review of the most important points of this approach in the form we need is contained in Appendix B.

2.1 Involutive Divisions

As we will use involution in different contexts, we need a fairly general and flexible approach. For this reason we do not define it in terms of power products or differential operators or something similar but in terms of multi indices (introduced in Appendix A.1). We study the Abelian monoid $(\mathbb{N}_0^n, +)$ with the addition defined componentwise. The multi indices may be identified in a natural way with the vertices of an n-dimensional integer lattice, so that we can easily visualise subsets of $\mathbb{N}_0^n$.

For a multi index $\nu \in \mathbb{N}_0^n$ we introduce its *cone* $\mathcal{C}(\nu) = \nu + \mathbb{N}_0^n$, i. e. the set of all multi indices that can be reached from ν by adding another multi index. We say that ν *divides* μ, written $\nu \mid \mu$, if $\mu \in \mathcal{C}(\nu)$. It might appear strange to speak here of a "division", as the operation in $\mathbb{N}_0^n$ is an addition, but if we think of the power products x^ν and x^μ, then $\mu \in \mathcal{C}(\nu)$ is equivalent to $x^\nu \mid x^\mu$. Given a finite subset $\mathcal{N} \subset \mathbb{N}_0^n$, we define its *span* as the monoid ideal generated by $\mathcal{N}$:

$$\langle \mathcal{N} \rangle = \bigcup_{\nu \in \mathcal{N}} \mathcal{C}(\nu) \ . \tag{2.1}$$

Again this is easy to interpret for power products. The set $\{x^\nu \mid \nu \in \mathcal{N}\}$ generates a monomial ideal $\mathcal{I}$. We have $\mu \in \langle \mathcal{N} \rangle$, if and only if $x^\mu \in \mathcal{I}$.

The basic idea of an involutive division is to introduce a restriction of the cone of a multi index, the involutive cone: it is only allowed to add multi indices certain entries of which vanish. This is equivalent to a restriction of the above defined divisibility relation. The final goal will be having a *disjoint* union in (2.1) by using only these involutive cones on the right hand side. This will naturally lead to the combinatorial decompositions discussed in Section 2.5.

In order to finally give the definition of an involutive division, we need one more notation: let $N \subseteq \{1, \dots, n\}$ be an arbitrary subset of the set of the first n integers; then we write $\mathbb{N}_N^n = \{\nu \in \mathbb{N}_0^n \mid \nu_j = 0, \ \forall j \notin N\}$ for the set of all multi indices where the only entries who may be non-zero are those whose indices are contained in N.

Definition 2.1.1. *An* involutive division L *is defined on* $(\mathbb{N}_0^n, +)$*, if a subset* $N_{L,\mathcal{N}}(\nu) \subseteq \{1, \dots, n\}$ *of* multiplicative indices *is associated to every multi index* ν *in a finite subset* $\mathcal{N} \subset \mathbb{N}_0^n$ *such that the following two conditions on the* involutive cones $\mathcal{C}_{L,\mathcal{N}}(\nu) = \nu + \mathbb{N}^n_{N_{L,\mathcal{N}}(\nu)} \subseteq \mathbb{N}_0^n$ *of the multi indices* $\nu \in \mathcal{N}$ *are satisfied.*

1. *If there exist two elements* $\mu, \nu \in \mathcal{N}$ *with* $\mathcal{C}_{L,\mathcal{N}}(\mu) \cap \mathcal{C}_{L,\mathcal{N}}(\nu) \neq \emptyset$*, either* $\mathcal{C}_{L,\mathcal{N}}(\mu) \subseteq \mathcal{C}_{L,\mathcal{N}}(\nu)$ *or* $\mathcal{C}_{L,\mathcal{N}}(\nu) \subseteq \mathcal{C}_{L,\mathcal{N}}(\mu)$ *holds.*
2. *If* $\mathcal{N}' \subset \mathcal{N}$*, then* $N_{L,\mathcal{N}}(\nu) \subseteq N_{L,\mathcal{N}'}(\nu)$ *for all* $\nu \in \mathcal{N}'$*.*

An arbitrary multi index $\mu \in \mathbb{N}_0^n$ *is* involutively divisible *by* $\nu \in \mathcal{N}$*, written* $\nu \mid_{L,\mathcal{N}} \mu$*, if* $\mu \in \mathcal{C}_{L,\mathcal{N}}(\nu)$*.*

Before we discuss the precise meaning of this definition and in particular of the two conditions contained in it, we should stress the following important point: as indicated by the notation, involutive divisibility is always defined with respect to both an involutive division L and a fixed finite set $\mathcal{N} \subset \mathbb{N}_0^n$; only an element of $\mathcal{N}$ can be an involutive divisor. Obviously, involutive divisibility $\nu \mid_{L,\mathcal{N}} \mu$ implies ordinary divisibility $\nu \mid \mu$.

The involutive cone $\mathcal{C}_{L,\mathcal{N}}(\nu)$ of an element $\nu \in \mathcal{N}$ is a subset of the full cone $\mathcal{C}(\nu)$. We are not allowed to add arbitrary multi indices to ν but may increase only certain entries of ν determined by the multiplicative indices. The first condition in the above definition says that involutive cones can intersect only trivially: if two intersect, one must be a subset of the other.

The *non-multiplicative indices* form the complement of $N_{L,\mathcal{N}}(\nu)$ in N and are denoted by $\bar{N}_{L,\mathcal{N}}(\nu)$. If we remove some elements from the set $\mathcal{N}$ and determine the multiplicative indices of the remaining elements with respect to the subset $\mathcal{N}'$, we will obtain in general a different result than before. The second condition for an involutive division says now that while it may happen that a non-multiplicative index becomes multiplicative for some $\nu \in \mathcal{N}'$, the converse cannot happen.

Example 2.1.2. An important example of an involutive division is the *Janet division* J. In order to define it, we must introduce certain subsets of the given set $\mathcal{N} \subset \mathbb{N}_0^n$:

$$(d_k, \dots, d_n) = \left\{ \nu \in \mathcal{N} \mid \nu_i = d_i\,,\ k \leq i \leq n \right\}. \tag{2.2}$$

The index n is multiplicative for $\nu \in \mathcal{N}$, if $\nu_n = \max_{\mu \in \mathcal{N}}\{\mu_n\}$, and $k < n$ is multiplicative for $\nu \in (d_{k+1}, \dots, d_n)$, if $\nu_k = \max_{\mu \in (d_{k+1}, \dots, d_n)}\{\mu_k\}$.

Let us consider for $n = 2$ the set $\mathcal{N} = \left\{\nu^{(1)} = [2, 0], \nu^{(2)} = [0, 2]\right\}$. As $\nu_2^{(2)} > \nu_2^{(1)}$, the index 2 is multiplicative only for $\nu^{(2)}$. In order to decide whether 1 is multiplicative, we must look at the subsets (0) and (2), respectively. As each of these subsets consists of only one element, the index 1 is multiplicative for both multi indices and we obtain that $N_{J,\mathcal{N}}(\nu^{(1)}) = \{1\}$ and $N_{J,\mathcal{N}}(\nu^{(2)}) = \{1, 2\}$. ◁

Lemma 2.1.3. *The Janet division is an involutive division.*

Proof. The second condition of Definition 2.1.1 is easy to verify. If k is a multiplicative index for $\nu \in \mathcal{N}$, then ν_k is maximal in a certain subset $(d_{k+1}, \dots, d_n) \subseteq \mathcal{N}$. If we remove some elements of the set $\mathcal{N}$, this maximality is unchanged. Thus all multiplicative indices remain multiplicative. It may happen that some non-multiplicative indices become multiplicative, but this is allowed.

Concerning the first condition we will prove an even stronger result: if $\mathcal{C}_{J,\mathcal{N}}(\mu) \cap \mathcal{C}_{J,\mathcal{N}}(\nu) \neq \emptyset$ for two multi indices $\mu, \nu \in \mathcal{N}$, then μ and ν must in fact be identical. So assume there exists a multi index $\rho \in \mathcal{C}_{J,\mathcal{N}}(\mu) \cap \mathcal{C}_{J,\mathcal{N}}(\nu)$. Then there must exist two multi indices $\bar{\mu} \in \mathbb{N}^n_{N_{J,\mathcal{N}}(\mu)}$ and $\bar{\nu} \in \mathbb{N}^n_{N_{J,\mathcal{N}}(\nu)}$ such that $\rho = \mu + \bar{\mu} = \nu + \bar{\nu}$. We look first at ρ_n. If $\bar{\mu}_n > 0$ and $\bar{\nu}_n > 0$, n is multiplicative for both μ and ν. But by the definition of the Janet division this requires $\mu_n = \nu_n$. It is not possible that $\bar{\mu}_n > 0$ and $\bar{\nu}_n = 0$, as then $\mu_n < \nu_n$ and nevertheless $n \in N_{J,\mathcal{N}}(\mu)$ contradicting the definition of the Janet division. The same holds of course for $\bar{\mu}_n = 0$ and $\bar{\nu}_n > 0$. Thus we may conclude that $\mu_n = \nu_n$.

We proceed now to ρ_{n-1}. By the considerations above we know already that $\mu, \nu \in (\mu_n)$. But this implies that we can repeat the same argument for the next entry. For $n-1$ to be a multiplicative index for μ, we must have $\mu_{n-1} \geq \nu_{n-1}$ and vice versa. Hence $\mu_{n-1} = \nu_{n-1}$ and $\mu, \nu \in (\mu_{n-1}, \mu_n)$. Iterating this argument, we get $\mu = \nu$. □

We have stressed above that involutive divisibility is always defined with respect to a given set $\mathcal{N}$. However, there exist some involutive divisions where the multiplicative variables are independent of $\mathcal{N}$. Such divisions are very convenient in concrete computations and they have got a special name.

Definition 2.1.4. *An involutive division* L *is* globally defined*, if the assignment of the multiplicative indices is independent of the set* $\mathcal{N}$*; in this case we write simply* $N_L(\nu)$*.*

Example 2.1.5. An involutive division that will become very important for us in the sequel is the *Pommaret division* P. It assigns the multiplicative indices according to the following simple rule: if $1 \leq k \leq n$ is the smallest index such that $\nu_k > 0$ for some multi index $\nu \in \mathbb{N}_0^n \setminus \{[0, \dots, 0]\}$, then we call k the *class* of ν, written $\operatorname{cls} \nu$, and set $N_P(\nu) = \{1, \dots, k\}$. Finally, we define $N_P([0, \dots, 0]) = \{1, \dots, n\}$. Thus P is globally defined. ◁

Lemma 2.1.6. *The Pommaret division is an involutive division.*

Proof. The second condition of Definition 2.1.1 obviously holds for *any* globally defined division, as the set $\mathcal{N}$ does not influence the multiplicative indices. For the first condition assume that there is a multi index $\rho \in \mathcal{C}_P(\mu) \cap \mathcal{C}_P(\nu)$. As in the proof of Lemma 2.1.3 we write $\rho = \mu + \bar{\mu} = \nu + \bar{\nu}$ with multi indices $\bar{\mu} \in \mathbb{N}^n_{N_P(\mu)}$ and $\bar{\nu} \in \mathbb{N}^n_{N_P(\nu)}$. Without loss of generality, we may assume that $\operatorname{cls} \mu \leq \operatorname{cls} \nu = k$. By definition of the Pommaret division this implies $\rho_i = \mu_i = \nu_i$ for all $i > k$. We must distinguish two cases. If $\operatorname{cls} \mu = k$, too, then either $\nu_k \leq \mu_k$ and consequently $\mu \in \mathcal{C}_P(\nu)$ or $\nu_k > \mu_k$ and $\nu \in \mathcal{C}_P(\mu)$. If $\operatorname{cls} \mu < k$ and $\nu_k \leq \mu_k$, then again $\mu \in \mathcal{C}_P(\nu)$. This finishes the proof, as it is not possible that $\operatorname{cls} \mu < k$ and $\nu_k > \mu_k$: because of $\rho_k \geq \nu_k$ this would require that k is a multiplicative index for μ contradicting $\operatorname{cls} \mu < k$. □

Above we introduced the span of a set $\mathcal{N} \subset \mathbb{N}_0^n$ as the union of the cones of its elements. Given an involutive division it appears natural to consider also the union of the involutive cones. Obviously, this yields in general only a subset of the monoid ideal $\langle \mathcal{N} \rangle$.

Definition 2.1.7. *The* involutive span *of a finite set* $\mathcal{N} \subset \mathbb{N}_0^n$ *is*

$$\langle \mathcal{N} \rangle_L = \bigcup_{\nu \in \mathcal{N}} \mathcal{C}_{\mathcal{N},L}(\nu) \,. \tag{2.3}$$

The set $\mathcal{N}$ *is called* weakly involutive *for the division* L *or a* weak involutive basis *of the monoid ideal* $\langle\mathcal{N}\rangle$*, if* $\langle\mathcal{N}\rangle_L = \langle\mathcal{N}\rangle$*. The set* $\mathcal{N}$ *is a* strong involutive basis *or for short an* involutive basis*, if the union in* (2.3) *is disjoint, i. e. the intersections of the involutive cones are empty. We call any finite set* $\mathcal{N} \subseteq \bar{\mathcal{N}} \subset \mathbb{N}_0^n$ *such that* $\langle\bar{\mathcal{N}}\rangle_L = \langle\mathcal{N}\rangle$ *a* (weak) involutive completion *of* $\mathcal{N}$*. An* obstruction to involution *for the set* $\mathcal{N}$ *is a multi index* $\nu \in \langle\mathcal{N}\rangle \setminus \langle\mathcal{N}\rangle_L$*.*

Remark 2.1.8. An obvious necessary condition for a strong involutive basis is that no multi indices $\mu, \nu \in \mathcal{N}$ exist such that $\mu\,|_{L,\mathcal{N}}\,\nu$. Sets with this property are called *involutively autoreduced.* ◁

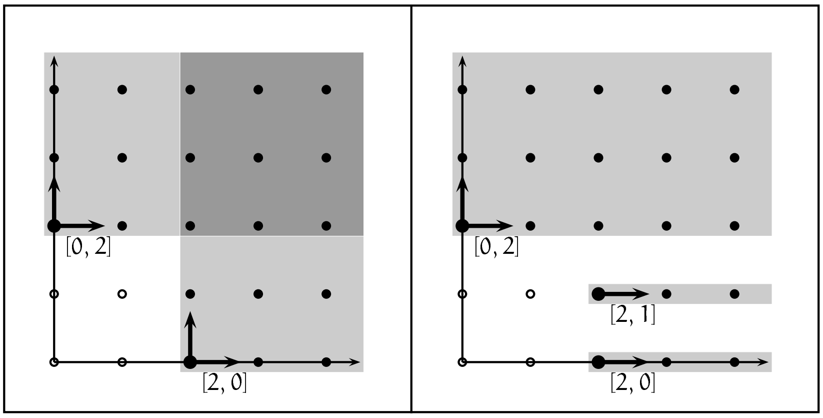

Fig. 2.1. *Left:* intersecting cones. *Right:* involutive cones.

Example 2.1.9. Figure 2.1 demonstrates the geometric interpretation of involutive divisions for $n = 2$. In both diagrams one can see the monoid ideal generated by the set $\mathcal{N} = \{[0,2],[2,0]\}$; the vertices belonging to it are marked by dark points. The arrows represent the multiplicative indices, i. e. the "allowed directions". The full cones of the two elements of $\mathcal{N}$ intersect in the darkly shaded area. The right diagram shows an involutive basis of $\langle\mathcal{N}\rangle$ for both the Janet and the Pommaret division. We must add to $\mathcal{N}$ the multi index $[2,1]$ and both for it and for $[2,0]$ only the index 1 is multiplicative. One can clearly see how $\langle\mathcal{N}\rangle$ is decomposed into three disjoint involutive cones: one of dimension 2, two of dimension 1. ◁

We are particularly interested in *strong* involutive bases, as only these lead to direct sums. The following result shows that in the "monomial" case any weak involutive basis can be reduced to a strong one by simply eliminating some elements.

Proposition 2.1.10. *If $\mathcal{N}$ is a weakly involutive set, a subset $\mathcal{N}' \subseteq \mathcal{N}$ exists such that $\mathcal{N}'$ is a strong involutive basis of $\langle\mathcal{N}\rangle$.*

Proof. The proof represents a nice motivation for the two conditions in Definition 2.1.1 of an involutive division. If $\mathcal{N}$ is not yet a strong involutive basis, the union in (2.3) cannot be disjoint. Thus there must exist involutive cones which intersect. By the first condition, this implies that some cones are contained in other ones; no other form of intersection is possible. If we eliminate the corresponding elements of $\mathcal{N}$, we get a subset $\mathcal{N}' \subset \mathcal{N}$ which has by the second condition the same involutive span, as the remaining elements may only gain additional multiplicative indices. Thus after a finite number of such eliminations we arrive at a strong involutive basis. $\square$

Remark 2.1.11. For the Janet division any weakly involutive set is also strongly involutive. This is a simple consequence of the proof of Lemma 2.1.3 where we showed that with respect to the Janet division two involutive cones only intersect, if they are identical. $\triangleleft$

The explicit construction of (strong) involutive completions for a given set $\mathcal{N} \subset \mathbb{N}_0^n$ will be discussed in detail in Section 6.4. For the moment we only note that we cannot expect that for an arbitrary set $\mathcal{N}$ and an arbitrary involutive division L an involutive basis $\mathcal{N}'$ of $\langle\mathcal{N}\rangle$ exists.

Example 2.1.12. We take the Pommaret division and the set $\mathcal{N} = \{[1,1]\}$. As $\operatorname{cls}[1,1] = 1$, we get $N_P([1,1]) = \{1\}$. So $\mathcal{C}_P([1,1]) \subset \mathcal{C}([1,1])$. But any multi index contained in $\langle\mathcal{N}\rangle$ has also class 1. Hence there does not exist a *finite* involutive basis of $\langle\mathcal{N}\rangle$ for the Pommaret division. We can generate it involutively only with the infinite set $\{[1,k] \mid k \in \mathbb{N}\}$. $\triangleleft$

Definition 2.1.13. *An involutive division L is called* Noetherian*, if any finite subset $\mathcal{N} \subset \mathbb{N}_0^n$ has a finite involutive completion with respect to L.*

Lemma 2.1.14. *The Janet division is Noetherian.*

Proof. Let $\mathcal{N} \subset \mathbb{N}_0^n$ be an arbitrary finite set. We will explicitly construct a Janet basis for $\langle\mathcal{N}\rangle$. Let μ be the multi index defined by $\mu_i = \max_{\nu\in\mathcal{N}} \nu_i$. We claim that the set

$$\bar{\mathcal{N}} = \{\bar{\nu} \in \mathbb{N}_0^n \cap \langle\mathcal{N}\rangle \mid \mu \in \mathcal{C}(\bar{\nu})\} \tag{2.4}$$

is an involutive completion of $\mathcal{N}$ with respect to the Janet division. Obviously, $\mathcal{N} \subseteq \bar{\mathcal{N}}$ and $\bar{\mathcal{N}} \subset \langle\mathcal{N}\rangle$. Let $\rho \in \langle\mathcal{N}\rangle$ be an arbitrary element. If $\rho \in \bar{\mathcal{N}}$, then trivially $\rho \in \langle \bar{\mathcal{N}} \rangle_J$. Otherwise set $I = \{i \mid \rho_i > \mu_i\}$ and define the multi index $\bar{\rho}$ by $\bar{\rho}_i = \rho_i$ for $i \notin I$ and $\bar{\rho}_i = \mu_i$ for $i \in I$, i.e. $\bar{\rho}_i = \min\{\rho_i, \mu_i\}$. By construction of the set $\bar{\mathcal{N}}$ and the definition of μ we have that $\bar{\rho} \in \bar{\mathcal{N}}$ and that $I \subseteq N_{J,\bar{\mathcal{N}}}(\bar{\rho})$. But this implies that $\rho \in \mathcal{C}_{J,\bar{\mathcal{N}}}(\bar{\rho})$ and thus $\bar{\mathcal{N}}$ is a finite Janet basis for $\langle \mathcal{N} \rangle$. □

2.2 Polynomial Algebras of Solvable Type

We introduced in the last section involutive bases in $\mathbb{N}_0^n$. We could interpret the multi indices as monomials and proceed to define involutive bases for polynomial ideals. But we are also interested in other rings containing linear differential or difference operators. As the basic ideas remain unchanged in many different situations, we need an algebraic structure within which all interesting cases can be handled in a unified manner. Slightly generalising a concept introduced by Kandry-Rody and Weispfenning [88], we use *polynomial algebras of solvable type*.

Let $\mathcal{P} = \Bbbk[x^1, \dots, x^n]$ be a polynomial ring over the field $\Bbbk$ of characteristic zero. $\mathcal{P}$ is a commutative ring with unit with respect to the usual multiplication. We equip the vector space $\mathcal{P}$ with alternative multiplications, in particular with non-commutative ones. We allow that both the variables x^i do not commute any more and that they operate on the coefficients. The usual multiplication is denoted either by a dot $\cdot$ or by no symbol at all. Alternative multiplications $\mathcal{P} \times \mathcal{P} \to \mathcal{P}$ are always denoted by $f \star g$.

Like Gröbner bases, involutive bases are defined with respect to a *term order*. It selects in each polynomial $f \in \mathcal{P}$ a *leading term* $\operatorname{lt}_\prec f = x^\mu$ with *leading exponent* $\operatorname{le}_\prec f = \mu$. Based on these leading exponents we can associate to each finite set $\mathcal{F}$ of polynomials a finite set $\operatorname{le}_\prec \mathcal{F} \subset \mathbb{N}_0^n$ to which we can apply the theory developed in the last section. But in order for this approach to make sense, we need a kind of compatibility between the multiplication $\star$ and the chosen term order.

Definition 2.2.1. *$(\mathcal{P}, \star, \prec)$ is a* polynomial algebra of solvable type *for the term order $\prec$, if the multiplication $\star : \mathcal{P} \times \mathcal{P} \to \mathcal{P}$ satisfies the following three axioms.*

(i) *$(\mathcal{P}, \star)$ is a ring with unit 1.*
(ii) $\forall a \in \Bbbk,\ f \in \mathcal{P}:\ a \star f = af$.
(iii) $\forall f, g \in \mathcal{P}:\ \operatorname{le}_\prec(f \star g) = \operatorname{le}_\prec f + \operatorname{le}_\prec g$.

Condition (i) ensures that the arithmetics in $(\mathcal{P}, \star, \prec)$ obeys the usual associative and distributive laws. Because of Condition (ii), $(\mathcal{P}, \star, \prec)$ is still a left $\mathbb{k}$-module. We do not require that it is a right $\mathbb{k}$-module, as this would exclude the possibility that the variables x^i operate on the coefficients. Condition (iii) relates the leading exponent of a product to the leading exponents of the factors. If $f, g \in \mathcal{P}$ are two arbitrary polynomials, a field element $c \in \mathbb{k}$ and a polynomial $h \in \mathcal{P}$ with $\mathrm{le}_\prec h \prec \mathrm{le}_\prec(f \cdot g)$ exist such that

$$f \star g = c\,(f \cdot g) + h\ . \tag{2.5}$$

We say that the multiplication $\star$ *respects the term order* $\prec$.

Since $\star$ is associative and distributive, the multiplication is fixed, as soon as the following data are given. We need for $1 \leq i, j \leq n$ constants $c_{ij} \in \mathbb{k}\setminus\{0\}$, polynomials $h_{ij} \in \mathcal{P}$ and maps $c_i : \mathbb{k} \to \mathbb{k}$, $h_i : \mathbb{k} \to \mathcal{P}$ such that

$$x^i \star a = c_i(a)x^i + h_i(a)\ , \quad \forall a \in \mathbb{k}\ , \tag{2.6a}$$

$$x^i \star x^j = c_{ij}x^ix^j + h_{ij}\ . \tag{2.6b}$$

Besides the conditions on the leading exponents of the polynomials h_{ij} and $h_i(a)$ imposed by (iii), each map c_i must be an injective field endomorphism and each map h_i must satisfy $h_i(a+b) = h_i(a)+h_i(b)$ and a kind of Leibniz rule $h_i(ab) = c_i(a)h_i(b) + h_i(a)b$.

Because of (iii) we can define Gröbner bases for ideals in algebras of solvable type. In case we endow $\mathcal{P}$ with a non-commutative multiplication, we must in principle distinguish left, right and two-sided ideals. However, we will exclusively work with left ideals and thus do not make this distinction. Recall that the left ideal generated by a finite subset $\mathcal{F} \subset \mathcal{P}$ is given by

$$\langle \mathcal{F} \rangle = \sum_{f \in \mathcal{F}} \mathcal{P} \star f\ . \tag{2.7}$$

Definition 2.2.2. *Let $(\mathcal{P}, \star, \prec)$ be a polynomial algebra of solvable type and $\mathcal{I} \subseteq \mathcal{P}$ a left ideal. A finite set $\mathcal{G} \subset \mathcal{P}$ is a* Gröbner basis *of the ideal $\mathcal{I}$, if $\langle \mathrm{le}_\prec \mathcal{G} \rangle = \mathrm{le}_\prec \mathcal{I}$.*

For the ordinary multiplication this definition reduces to the classical Definition B.2.3 of Gröbner bases. The decisive point, explaining the conditions imposed in Definition 2.2.1, is that *normal forms* with respect to a finite set $\mathcal{F} \subset \mathcal{P}$ can be computed in algebras of solvable type in precisely the same way as in the ordinary polynomial ring. Assume we are given a polynomial $f \in \mathcal{P}$ such that $\mathrm{le}_\prec g \mid \mathrm{le}_\prec f$ for some $g \in \mathcal{G}$ and set $\mu = \mathrm{le}_\prec f - \mathrm{le}_\prec g$. If we consider $g_\mu = x^\mu \star g$, then by (iii) $\mathrm{le}_\prec g_\mu = \mathrm{le}_\prec f$. Setting $d = \mathrm{lc}_\prec f / \mathrm{lc}_\prec g_\mu$, we find by (ii) that $\mathrm{lt}_\prec(f - dg_\mu) \prec \mathrm{lt}_\prec f$. Hence we may use the simple Algorithm B.1 for computing normal form; in particular, it always terminates by the same argument as in the ordinary case. Note that in general $d \neq \mathrm{lc}_\prec f / \mathrm{lc}_\prec g$, if $c \neq 1$

in (2.5), and that normal form computations are typically more expensive due to the appearance of the additional polynomial h in (2.5).

The Gröbner basis theory of Appendix B.2 can be extended straightforwardly to algebras of solvable type, as most proofs are based on the computation of normal forms. The remaining arguments mostly take place in $\mathbb{N}_0^n$ and thus can be applied without changes. In particular, we get the following result crucial for the termination of Buchberger's Algorithm B.2.

Proposition 2.2.3. *Let* $(\mathcal{P}, \star, \prec)$ *be a polynomial algebra of solvable type. Then* $\mathcal{P}$ *is a (left) Noetherian ring.*

Proof. For the ordinary multiplication this is Hilbert's Basis Theorem. There exist many different proofs of it; we present here one that can handle our more general situation. Let $\mathcal{I} \subseteq \mathcal{P}$ be a (left) ideal. By Dickson's Lemma the monoid ideal $\mathrm{le}_\prec \mathcal{I}$ has a finite basis. So we can choose a finite set $\mathcal{G} \subset \mathcal{I}$ such that $\mathrm{le}_\prec \mathcal{G}$ is a finite basis of $\mathrm{le}_\prec \mathcal{I}$. It follows from a simple normal form argument that $\mathcal{G}$ generates $\mathcal{I}$. □

Note that we have in fact proven more than required by the proposition. The set $\mathcal{G}$ is obviously a Gröbner basis of $\mathcal{I}$, so that we have shown the existence of a Gröbner basis for arbitrary ideals in a polynomial algebra of solvable type. We stop here and do not give more details on extending the Gröbner basis theory to these algebras, as we will use in the next section a completely different approach leading to involutive bases. For the remainder of this section we consider a number of important examples of algebras of solvable type in order to make this abstract concept better understandable. They demonstrate the wide range of applicability of these algebras. Further examples can be found in [88] (and references therein).

Example 2.2.4. Obviously, the most trivial example of an algebra of solvable type is the usual polynomial ring, i.e. we set $f \star g = fg$. Its multiplication respects any term order, as by definition a term order is compatible with the monoid structure of the terms.

In contrast to Kandry-Rody and Weispfenning [88], we allow that the terms operate on the coefficients. The most important example for us are rings of *linear differential operators*. We take for the coefficients some function field $\mathbb{F}$, say the rational functions $\mathbb{Q}(x^1, \dots, x^n)$, and consider the polynomial ring $\mathcal{D} = \mathbb{F}[\partial_1, \dots, \partial_n]$ where $\partial_i = \partial/\partial x^i$. More generally, we may take any differential field $\mathbb{F}$ with commuting derivations ∂_i. The product of two monomial operators $a(x)\partial^\mu$ and $b(x)\partial^\nu$ is given by

$$a(x)\partial^\mu \star b(x)\partial^\nu = \sum_{\sigma+\rho=\mu} \binom{\mu}{\sigma} a(x) \frac{\partial^{|\sigma|} b(x)}{\partial x^\sigma} \partial^{\rho+\nu} \tag{2.8}$$

where $\binom{\mu}{\sigma}$ is a shorthand for $\prod_{i=1}^{n}\binom{\mu_i}{\sigma_i}$. By the properties of a term order

$$\mathrm{le}_{\prec}\big(a(x)\partial^{\mu}\star b(x)\partial^{\nu}\big)=\mu+\nu=\mathrm{le}_{\prec}\big(a(x)\partial^{\mu}\big)+\mathrm{le}_{\prec}\big(b(x)\partial^{\nu}\big)\ , \tag{2.9}$$

as any term $\partial^{\rho+\nu}$ appearing on the right hand side of (2.8) divides $\partial^{\mu+\nu}$ and thus $\partial^{\rho+\nu}\preceq\partial^{\mu+\nu}$ for any term order $\prec$. Hence $\mathcal{D}$ is a polynomial algebra of solvable type for all term orders. ◁

This example can be considerably extended to a rather general class of non-commutative polynomials originally introduced by Ore [130]; our exposition follows [26].

Example 2.2.5. Let $\mathbb{F}$ be any field of characteristic zero and $\sigma:\mathbb{F}\to\mathbb{F}$ an injective endomorphism. A *pseudo-derivation* with respect to σ is a map $\delta:\mathbb{F}\to\mathbb{F}$ such that (i) $\delta(f+g)=\delta(f)+\delta(g)$ and (ii) $\delta(f\cdot g)=\sigma(f)\cdot\delta(g)+\delta(f)\cdot g$ for all $f,g\in\mathbb{F}$. If $\sigma=\mathrm{id}_{\mathbb{F}}$, the identity map, (ii) is the standard Leibniz rule for derivations. If $\sigma\neq\mathrm{id}_{\mathbb{F}}$, one can show that there exists an $h\in\mathbb{F}$ such that $\delta=h(\sigma-\mathrm{id}_{\mathbb{F}})$. And conversely, if $\delta\neq0$, there exists an $h\in\mathbb{F}$ such that $\sigma=h\delta+\mathrm{id}_{\mathbb{F}}$. Ore called $\sigma(f)$ the *conjugate* and $\delta(f)$ the *derivative* of f.

Given σ and δ, the ring $\mathbb{F}[\partial;\sigma,\delta]$ of univariate *Ore polynomials* consists of all formal polynomials in ∂ with coefficients in $\mathbb{F}$, i.e. of expressions of the form $\theta=\sum_{i=0}^{q}f_i\partial^i$ with $f_i\in\mathbb{F}$ and $q\in\mathbb{N}_0$. The addition is defined as usual. The "variable" ∂ operates on an element $f\in\mathbb{F}$ according to the rule

$$\partial\star f=\sigma(f)\partial+\delta(f) \tag{2.10}$$

which is extended associatively and distributively to define the multiplication in $\mathbb{F}[\partial;\sigma,\delta]$: given two elements $\theta_1,\theta_2\in\mathbb{F}[\partial;\sigma,\delta]$, we can transform the product $\theta_1\star\theta_2$ to the above normal form by repeatedly applying (2.10). The product of two linear polynomials evaluates then to

$$\begin{aligned}(f_1+f_2\partial)\star(g_1+g_2\partial)=f_1g_1+f_2\delta(g_1)+&\\ \big[f_1g_2+f_2\sigma(g_1)+f_2\delta(g_2)\big]\partial+&\\ f_2\sigma(g_2)\partial^2\ .&\end{aligned} \tag{2.11}$$

The condition that σ is injective ensures that $\deg(\theta_1\star\theta_2)=\deg\theta_1+\deg\theta_2$. We call $\mathbb{F}[\partial;\sigma,\delta]$ the *Ore algebra* generated by σ and δ.

A simple familiar example is given by $\mathbb{F}=\mathbb{Q}(x)$, $\delta=\frac{d}{dx}$ and $\sigma=\mathrm{id}_{\mathbb{F}}$ yielding linear ordinary differential operators with rational functions as coefficients. Similarly, we obtain *recurrence* and *difference operators*. We set $\mathbb{F}=\mathbb{C}(n)$, the field of sequences with complex elements, and take for σ the shift operator, i.e. the automorphism mapping s_n to s_{n+1}. Then $\Delta=\sigma-\mathrm{id}_{\mathbb{F}}$ is a pseudo-derivation. $\mathbb{F}[E;\sigma,0]$ consists of linear ordinary recurrence operators, $\mathbb{F}[E;\sigma,\Delta]$ of linear ordinary difference operators.

Note that so far it is not yet clear why we call the elements of these classical examples "operators". In fact, the elements of any Ore algebra $\mathbb{F}[\partial;\sigma,\delta]$ can be interpreted as operators on vector spaces over $\mathbb{F}$. Let $\mathcal{V}$ be such a vector space and L an $\mathbb{F}$-*pseudo-linear map* $L:\mathcal{V}\to\mathcal{V}$, i.e. $L(u+v)=L(u)+L(v)$ and $L(fu)=\sigma(f)L(u)+\delta(f)u$ for all $f\in\mathbb{F}$ and $u,v\in\mathcal{V}$. Then we introduce an action $\mathcal{L}:\mathbb{F}\times\mathcal{V}\to\mathcal{V}$ mapping $(\theta=\sum f_i\partial^i,u)$ to $L_\theta u=\sum f_iL^i(u)$. For $\mathcal{V}=\mathbb{F}^m$ a natural choice for L is $L(v_1,\dots,v_m)=\bigl(\delta(v_1),\dots,\delta(v_m)\bigr)$. If $\delta=0$ as for the recurrence operators, we may also take $L(v_1,\dots,v_m)=\bigl(\sigma(v_1),\dots,\sigma(v_m)\bigr)$. With these definitions the above Ore algebras contain linear operators in the familiar sense.

For multivariate Ore polynomials we take a set $\Sigma=\{\sigma_1,\dots,\sigma_n\}$ of injective $\mathbb{F}$-endomorphisms and a set $\Delta=\{\delta_1,\dots,\delta_n\}$ where each δ_i is a pseudo-derivation with respect to σ_i. For each pair (σ_i,δ_i) we introduce a "variable" ∂_i satisfying a commutation rule of the form (2.10). If we require that all the maps σ_i,δ_j commute with each other, i.e. $\sigma_i\circ\sigma_j=\sigma_j\circ\sigma_i$, $\delta_i\circ\delta_j=\delta_j\circ\delta_i$ and $\sigma_i\circ\delta_j=\delta_j\circ\sigma_i$ for all $i\neq j$, one easily checks that $\partial_i\star\partial_j=\partial_j\star\partial_i$, i.e. the "variables" ∂_i commute.

Setting $\mathcal{D}=\{\partial_1,\dots,\partial_n\}$, we denote by $\mathbb{F}[\mathcal{D};\Sigma,\Delta]$ the ring of multivariate Ore polynomials. Because of the commutativity of the ∂_i we can write the terms as ∂^μ with multi indices $\mu\in\mathbb{N}_0^n$, so that it indeed makes sense to speak of a polynomial ring. The proof that $\bigl(\mathbb{F}[\mathcal{D};\Sigma,\Delta],\star\bigr)$ is an algebra of solvable type for any term order goes completely analogously to the case of linear differential operators treated explicitly in Example 2.2.4 because of the great similarity of (2.10) and (2.8) (for $\mu=1_j$ and $\nu=0$). $\lhd$

Ore algebras are the special case where the maps h_i in (2.6a) take their values in $\Bbbk$ and not in $\mathcal{P}$ and where the variables commute. We consider now an example with non-commutative variables. By the same construction principle, factorisation of a free tensor algebra by a suitable quadratic ideal, one can generate many interesting algebras like Clifford algebras.

Example 2.2.6. Let $\mathfrak{A}$ be a finite-dimensional *Lie algebra* over a field $\Bbbk$. As usual we denote the product in $\mathfrak{A}$ by brackets: $[X,Y]$. Readers unfamiliar with Lie algebras should think of a subalgebra of $\mathfrak{gl}(m,\Bbbk)$, the algebra of all $m\times m$ matrices with entries from $\Bbbk$. The bracket is then the well-known commutator $[X,Y]=XY-YX$. Note that the multiplication in our algebra is the commutator and *not* the ordinary matrix multiplication!

As an algebra over a field, $\mathfrak{A}$ is in particular a vector space and we can choose a basis $\{X_1,\dots,X_n\}$. The structure of the Lie algebra is defined by the commutation relations of the generators X_i

$$[X_i,X_j]=C_{ij}^kX_k \tag{2.12}$$

where the $C^k_{ij} \in \Bbbk$ are the *structure constants* of the algebra $\mathfrak{A}$.

We construct now the *universal enveloping algebra* of $\mathfrak{A}$, an important tool in the representation theory of Lie algebras (see e. g. [185, Chapt. 3]). We start with the tensor algebra $\mathfrak{T}(\mathfrak{A})$ over $\mathfrak{A}$; a basis of it is given by all formal tensor products $X_{i_1} \otimes X_{i_2} \otimes \cdots \otimes X_{i_q}$ with $q \in \mathbb{N}_0$. As $X_i \otimes X_j \neq X_j \otimes X_i$, we cannot identify such "terms" with multi indices in $\mathbb{N}_0^n$. So we factor by the two-sided ideal generated by the quadratic elements $X_i \otimes X_j - X_j \otimes X_i - [X_i, X_j]$ in order to obtain the universal enveloping algebra $\mathfrak{U}(\mathfrak{A})$.

One can show that $\mathfrak{U}(\mathfrak{A})$ is an associative algebra and has the following universal property. Let $\pi : \mathfrak{A} \to \mathfrak{U}(\mathfrak{A})$ be the canonical linear map defined by $X_i \mapsto [X_i]$, i. e. each generator X_i is mapped on its equivalence class in the factor algebra $\mathfrak{U}(\mathfrak{A})$. The map π satisfies $\pi([X, Y]) = [\pi(X), \pi(Y)]$ for all $X, Y \in \mathfrak{A}$. Let $\mathfrak{B}$ be another associative algebra with a linear map $\phi : \mathfrak{A} \to \mathfrak{B}$ such that $\phi([X, Y]) = [\phi(X), \phi(Y)]$ for all $X, Y \in \mathfrak{A}$. Then there exists a unique homomorphism $\tilde{\phi} : \mathfrak{U}(\mathfrak{A}) \to \mathfrak{B}$ such that $\phi = \tilde{\phi} \circ \pi$.

In each equivalence class there is exactly one representative containing only terms of the form $X_{i_1} \otimes X_{i_2} \otimes \cdots \otimes X_{i_q}$ where now the indices form an ascending sequence $i_1 \leq i_2 \leq \cdots \leq i_q$. Given an arbitrary element $t \in \mathfrak{T}(\mathfrak{A})$ this representative can be constructed by substituting each product $X_i \otimes X_j$ with $i > j$ by $X_j \otimes X_i + [X_i, X_j]$ until no more such products appear. This leads to a normal form which can be identified with an element of $\Bbbk[X_1, \dots, X_n]$. Thus as vector spaces $\mathfrak{U}(\mathfrak{A})$ and $\Bbbk[X_1, \dots, X_n]$ are isomorphic (this is the *Poincaré–Birkhoff–Witt Theorem*).

As the right hand side of (2.12) is of lower degree than the left hand side, $\mathfrak{U}(\mathfrak{A})$ is a polynomial algebra of solvable type for any degree compatible term order. Kandry-Rody and Weispfenning [88] showed that if $\mathfrak{A}$ is a *solvable* Lie algebra, one can find bases $\{X_1, \dots, X_n\}$ such that $\mathfrak{U}(\mathfrak{A})$ is also of solvable type with respect to the lexicographic order.

As a concrete example we study the three-dimensional Lie algebra $\mathfrak{so}(3)$. Its commutation relations are $[X_i, X_j] = \epsilon_{ijk} X_k$ where ϵ_{ijk} is the totally antisymmetric tensor and we obtain for the multiplication in $\mathfrak{U}\bigl(\mathfrak{so}(3)\bigr)$

$$\begin{aligned} x^1 \star x^2 &= x^1x^2\,, & x^2 \star x^1 &= x^1x^2 - x^3\,, \\ x^1 \star x^3 &= x^1x^3\,, & x^3 \star x^1 &= x^1x^3 + x^2\,, \\ x^2 \star x^3 &= x^2x^3\,, & x^3 \star x^2 &= x^2x^3 - x^1\,. \end{aligned} \tag{2.13}$$

It is obvious that while the multiplication respects any degree compatible term order it does not respect the lexicographic order. ◁

Example 2.2.7. Non-commuting variables also occur in the *Weyl algebra* consisting of linear differential operators with polynomial coefficients. We may consider it as a polynomial ring $\mathcal{W}_n = \Bbbk[x^1, \dots, x^n, \partial_1, \dots, \partial_n]$ where the unknowns satisfy the commutation rules

$$[x^i, x^j] = 0\,, \quad [\partial_i, \partial_j] = 0\,, \quad [x^i, \partial_j] = \delta^i_j\,. \tag{2.14}$$

In fact, adding the "variable" $\mathbb{1}$ commuting which all other ones and writing the right hand side of (2.14) as $\delta^i_j\mathbb{1}$, we see that (2.14) defines a $(2n+1)$-dimensional Lie algebra, the *Heisenberg algebra*, which forms the basis of quantum mechanics. The Weyl algebra is a factor algebra of its enveloping algebra; we must factor in addition by the relations $\mathbb{1} \cdot x^i = x^i$ and $\mathbb{1} \cdot \partial_i = \partial_i$.

Modules over the Weyl algebra, often called $\mathcal{D}$-*modules*, are used in many different fields, in particular in singularity theory and in the representation theory of algebraic groups. An introduction into their theory may be found in [39]; more advanced material is contained in [19, 22]. Gröbner bases in the Weyl algebra are discussed in [154].

With respect to the solvability the Weyl algebra behaves like a ring of differential operators with polynomial coefficients. By the same argument as in Example 2.2.4 one can show that it is an algebra of solvable type for any term order. The difference to the there studied rings of differential operators lies in the different definition of terms. A term in the Weyl algebra has the form $x^\mu\partial^\nu$ where $\mu, \nu \in \mathbb{N}_0^n$. Thus the leading exponent of an element of $\mathcal{W}_n$ is a multi index with $2n$ entries. Terms in $\mathcal{D}$ are of the form ∂^μ with $\mu \in \mathbb{N}_0^n$ so that exponents have only n entries. $\triangleleft$

2.3 Involutive Bases

We proceed to define involutive bases for left ideals of polynomial algebras of solvable type. Our approach closely follows the introduction of Gröbner bases in Appendix B.2. In principle, we could at once consider submodules of free modules over such an algebra. But this only complicates the notation. So we start with the ideal case and the extension to submodules goes as for Gröbner bases.

Let $(\mathcal{P}, \star, \prec)$ be an algebra of solvable type for some term order $\prec$ and $\mathcal{F} \subset \mathcal{P}$ a finite subset. Furthermore, we choose on $\mathbb{N}_0^n$ an involutive division L. With the help of the leading exponents in $\operatorname{le}_\prec\mathcal{F}$, we may assign each element $f \in \mathcal{F}$ a set of *multiplicative variables*

$$X_{L,\mathcal{F},\prec}(f) = \left\{x^i \mid i \in N_{L,\operatorname{le}_\prec\mathcal{F}}(\operatorname{le}_\prec f)\right\}\,. \tag{2.15}$$

This leads naturally to the following extension of Definition 2.1.7 of the involutive span.

Definition 2.3.1. *Let $\mathcal{F} \subset \mathcal{P}$ be a finite set. Its* involutive span *for a given involutive division* L *and the term order* $\prec$ *is*

$$\langle \mathcal{F} \rangle_{L,\prec} = \sum_{f \in \mathcal{F}} \mathbb{k}[X_{L,\mathcal{F},\prec}(f)] \star f \,. \tag{2.16}$$

The definition of an obstruction to involution is more involved than in the monomial case. We need two central notions in the theory of Gröbner bases: reduction and normal form. We introduce variants adapted to the context of involutive bases.

Definition 2.3.2. *Let $\mathcal{F} \subset \mathcal{P}$ be a finite set and L an involutive division. A polynomial $g \in \mathcal{P}$ is* involutively reducible *with respect to $\mathcal{F}$, if it contains a term $x^\mu \in \operatorname{supp} g$ such that $\operatorname{le}_\prec f \,|_{L,\operatorname{le}_\prec \mathcal{F}}\, \mu$ for some $f \in \mathcal{F}$. The polynomial g is in* involutive normal form *with respect to $\mathcal{F}$, if it is not involutively reducible. The set $\mathcal{F}$ is* involutively autoreduced, *if no polynomial $f \in \mathcal{F}$ contains a term $x^\mu \in \operatorname{supp} f$ such that another polynomial $f' \in \mathcal{F} \setminus \{f\}$ exists with $\operatorname{le}_\prec f' \,|_{L,\operatorname{le}_\prec \mathcal{F}}\, \mu$.*

Remark 2.3.3. The definition of an involutively autoreduced set *cannot* be formulated more concisely by saying that each $f \in \mathcal{F}$ is in involutive normal form with respect to $\mathcal{F} \setminus \{f\}$. If we are not dealing with a global division, the removal of f from $\mathcal{F}$ will generally change the assignment of the multiplicative indices and thus affect the involutive divisibility. $\lhd$

Involutive reducibility is obviously a restriction of ordinary reducibility. An *obstruction to involution* is a polynomial $g \in \langle \mathcal{F} \rangle \setminus \langle \mathcal{F} \rangle_{L,\prec}$ possessing a standard representation (B.9) with respect to $\mathcal{F}$; i. e. $g = \sum_{f \in \mathcal{F}} g_f \star f$ for polynomials g_f satisfying $\operatorname{le}_\prec(g_f \star f) \preceq \operatorname{le}_\prec g$. We will later see that these elements make the difference between an involutive and a Gröbner basis.

In a differential equations context, elements of $\langle \mathcal{F} \rangle$ which do not possess a standard representation with respect to $\mathcal{F}$ are called *integrability conditions*. Note that this notion depends on the chosen term order $\prec$; only for degree compatible term orders it coincides with the informal definition of integrability conditions used in Section 1.4. By Proposition B.2.7, $\mathcal{F}$ is a Gröbner basis, if and only if no "integrability conditions" exist.

Example 2.3.4. Consider the set $\mathcal{F} = \{f_1, f_2, f_3\} \subset \mathbb{k}[x, y, z]$ with the polynomials $f_1 = z^2 - xy$, $f_2 = yz - x$ and $f_3 = y^2 - z$. For any degree compatible term order, the leading terms of f_2 and f_3 are unique. For f_1 we have two possibilities: if we use the degree lexicographic order[1] (i. e. for $x \prec y \prec z$), it is z^2, for the degree inverse lexicographic order (i. e. for $x \succ y \succ z$) the

[1] All used term orders are introduced in Example B.2.1.

leading term is xy. In the first case, neither "integrability conditions" nor obstructions to involution for the Janet division exist, as $\langle\mathcal{F}\rangle_{J,\prec_{\text{deglex}}} = \langle\mathcal{F}\rangle$. In the second case, $f_4 = z^3 - x^2 = zf_3 + xf_1$ is an "integrability condition". Adding it to $\mathcal{F}$ yields a Gröbner basis $\mathcal{G}$ of $\langle\mathcal{F}\rangle$, as one can easily check using Proposition B.2.12. But now $f_5 = zf_4$ is an obstruction to involution of $\mathcal{G}$, as it is not involutively reducible with respect to the Janet division. ◁

It often suffices, if one does not consider all terms in $\operatorname{supp} g$ but only the leading term $\operatorname{lt}_\prec g$: the polynomial g is *involutively head reducible*, if $\operatorname{le}_\prec f\,|_{L,\operatorname{le}_\prec\mathcal{F}}\operatorname{le}_\prec g$ for some $f \in \mathcal{F}$. Similarly, the set $\mathcal{F}$ is *involutively head autoreduced*, if no leading exponent of an element $f \in \mathcal{F}$ is involutively divisible by the leading exponent of another element $f' \in \mathcal{F}\setminus\{f\}$.

Example 2.3.5. In the case of the Janet division, a set $\mathcal{F}$ is involutively head autoreduced as soon as all elements have different leading terms. Indeed, we have seen in the proof of Lemma 2.1.3 that with respect to the Janet division two involutive cones only intersect, if they are identical. ◁

As involutive reducibility is a restriction of ordinary reducibility, involutive normal forms can be determined with trivial adaptions of the familiar algorithms like for example Algorithm B.1. The termination follows by the same argument as usual, namely that $\prec$ is a well-order. If g' is an involutive normal form of $g \in \mathcal{P}$ with respect to $\mathcal{F}$ for the division L, then we write $g' = \mathrm{NF}_{\mathcal{H},L,\prec}(g)$, although involutive normal forms are in general not unique (like ordinary normal forms – see Example B.2.6). Depending on the order in which reductions are applied different results are obtained.

The ordinary normal form is unique, if and only if it is computed with respect to a Gröbner basis (Proposition B.2.7). In fact, this property is often used to define Gröbner bases. For the involutive normal form, the situation is somewhat different.

Lemma 2.3.6. *If the finite set $\mathcal{F} \subset \mathcal{P}$ is involutively head autoreduced with respect to the involutive division* L*, the sum in* (2.16) *is direct.*

Proof. Let f_1, f_2 be two distinct elements of $\mathcal{F}$ and $X_i = X_{L,\mathcal{F},\prec}(f_i)$ their sets of multiplicative variables. Assume two polynomials $P_i \in \Bbbk[X_i]$ exist such that $P_1 \star f_1 = P_2 \star f_2$ implying in particular that $\operatorname{le}_\prec(P_1 \star f_1) = \operatorname{le}_\prec(P_2 \star f_2)$. As the multiplication $\star$ respects the term order $\prec$, this can only happen, if $\mathcal{C}_{L,\operatorname{le}_\prec\mathcal{F}}(\operatorname{le}_\prec f_1) \cap \mathcal{C}_{L,\operatorname{le}_\prec\mathcal{F}}(\operatorname{le}_\prec f_2) \neq \emptyset$. Thus one of the involutive cones is completely contained in the other one and either $\operatorname{le}_\prec f_1\,|_{L,\operatorname{le}_\prec\mathcal{F}}\operatorname{le}_\prec f_2$ or $\operatorname{le}_\prec f_2\,|_{L,\operatorname{le}_\prec\mathcal{F}}\operatorname{le}_\prec f_1$ contradicting that $\mathcal{F}$ is involutively head autoreduced. □

Proposition 2.3.7. *If the finite set $\mathcal{F} \subset \mathcal{P}$ is involutively head autoreduced, each polynomial $g \in \mathcal{P}$ has a unique involutive normal form $\mathrm{NF}_{\mathcal{F},L,\prec}(g)$.*

Proof. If 0 is an involutive normal form of g, then obviously $g \in \langle \mathcal{F} \rangle_{L,\prec}$. Conversely, assume that $g \in \langle \mathcal{F} \rangle_{L,\prec}$, i. e. the polynomial g can be written in the form $g = \sum_{f \in \mathcal{F}} P_f \star f$ with $P_f \in \Bbbk[X_{L,\mathcal{F},\prec}(f)]$. As $\mathcal{F}$ is involutively head autoreduced, the leading terms of the summands can never cancel (see the proof of Lemma 2.3.6). Thus $\operatorname{lt}_\prec g = \operatorname{lt}_\prec(P_f \star f)$ for some $f \in \mathcal{F}$ and any polynomial $g \in \langle \mathcal{F} \rangle_{L,\prec}$ is involutively head reducible with respect to $\mathcal{F}$. Each reduction step in an involutive normal form algorithm leads to a new polynomial $g' \in \langle \mathcal{F} \rangle_{L,\prec}$ with $\operatorname{lt}_\prec g' \preceq \operatorname{lt}_\prec g$. If the leading term is reduced, we even get $\operatorname{lt}_\prec g' \prec \operatorname{lt}_\prec g$. As each terminating normal form algorithm must sooner or later reduce the leading term, we eventually obtain 0 as unique involutive normal form of any $g \in \langle \mathcal{F} \rangle_{L,\prec}$.

Let g_1 and g_2 be two involutive normal forms of the polynomial g. Obviously, $g_1 - g_2 \in \langle \mathcal{F} \rangle_{L,\prec}$. By definition of a normal form both $\operatorname{supp} g_1$ and $\operatorname{supp} g_2$ do not contain any term involutively reducible with respect to $\mathcal{F}$ and the same holds for $\operatorname{supp}(g_1 - g_2) \subseteq \operatorname{supp} g_1 \cup \operatorname{supp} g_2$. Hence $g_1 - g_2$ is also in involutive normal form and by our considerations above we must have $g_1 - g_2 = 0$. □

Finally, we define involutive bases. As in the monomial case, we distinguish weak and strong bases. Although a strong involutive basis always induces a direct sum decomposition of the ideal $\mathcal{I}$ by Lemma 2.3.6, we cannot use this for the definition but must require a stronger property.

Definition 2.3.8. *Let $\mathcal{I} \subseteq \mathcal{P}$ be a (left) ideal. A* weak involutive basis *of $\mathcal{I}$ with respect to L and $\prec$ is a finite set $\mathcal{H}$ with $\langle \mathcal{H} \rangle_{L,\prec} = \mathcal{I}$. The set $\mathcal{H}$ is a* strong involutive basis *or shortly* involutive basis*, if it is in addition involutively head autoreduced.*

Example 2.3.9. We continue with Example 2.3.4. The set $\mathcal{F}$ is a Janet basis, i. e. an involutive basis with respect to the Janet division, of the ideal $\mathcal{I} = \langle \mathcal{F} \rangle$ for the term order $\prec_{\text{deglex}}$, although we have not yet the necessary tools to prove this fact. If we use $\prec_{\text{deginvlex}}$ as term order, a Janet basis is given by $\mathcal{F}' = \{f_1, f_2, f_3, f_4, f_5\}$; in fact, this is the smallest Janet basis of $\mathcal{I}$ for this term order, as it is not possible to remove an element. By Example 2.3.5, both $\mathcal{F}$ and $\mathcal{F}'$ are involutively head autoreduced for the respective term order. Note that for $\prec_{\text{deginvlex}}$ the basis is not only larger but also contains polynomials of higher degree. ◁

We postpone the question of existence and actual construction of involutive bases to Chapter 6. There we will also provide effective tools for checking whether a given set is an involutive basis. For the remainder of this section we concentrate instead on some important properties of these bases and especially on their relation to Gröbner bases. We start with an involutive form of

Proposition B.2.7. It is in so far stronger, as the involutive standard representation (2.17) is *unique* in contrast to the ordinary one (cf. Example B.2.8).

Proposition 2.3.10. *Let $\mathcal{I} \subseteq \mathcal{P}$ be a non-zero ideal and $\mathcal{H} \subset \mathcal{P}$ a finite set involutively head autoreduced with respect to the involutive division L. Then the following statements are equivalent.*

(i) *The set $\mathcal{H}$ is an involutive basis for the involutive division L and the term order $\prec$.*
(ii) *Every polynomial $f \in \mathcal{I}$ can be uniquely written in the form*

$$f = \sum_{h \in \mathcal{H}} P_h \star h \tag{2.17}$$

where the coefficients $P_h \in \Bbbk[X_{L,\mathcal{H},\prec}(h)]$ satisfy $\mathrm{lt}_\prec(P_h \star h) \preceq \mathrm{lt}_\prec f$ for all polynomials $h \in \mathcal{H}$.

Proof. As $\mathcal{H}$ is involutively head autoreduced, involutive normal forms are unique and $\mathrm{NF}_{\mathcal{H},L,\prec}(f) = 0$ for any $f \in \mathcal{I}$. Applying the division algorithm corresponding to the involutive form of Algorithm B.1 yields a representation in the form (2.17) satisfying the conditions on the leading terms. Its uniqueness follows from Lemma 2.3.6. Thus (i) implies (ii).

The converse is simple, too. Obviously, (ii) implies that $\langle \mathcal{H} \rangle_{L,\prec} = \mathcal{I}$. As by assumption $\mathcal{H}$ is furthermore involutively head autoreduced, it is an involutive basis of $\mathcal{I}$. □

Any monomial basis of a monomial ideal is trivially a Gröbner basis. Thus we can rephrase the definition of Gröbner bases as follows: a finite set $\mathcal{G}$ is a Gröbner basis of the ideal $\mathcal{I}$, if and only if $\mathrm{lt}_\prec \mathcal{G}$ is a Gröbner basis of $\mathrm{lt}_\prec \mathcal{I}$. Involutive bases satisfy a similar characterisation theorem.

Theorem 2.3.11. *Let $\mathcal{I} \subseteq \mathcal{P}$ be an ideal and $\mathcal{H} \subset \mathcal{P}$ a finite set. If $\mathrm{le}_\prec \mathcal{H}$ is a (weak) involutive basis of $\mathrm{le}_\prec \mathcal{I}$ for a given involutive division L, then $\mathcal{H}$ is a (weak) involutive basis of $\mathcal{I}$. If $\mathcal{H}$ is a strong involutive basis, the converse holds, too.*

Proof. For the first assertion take an arbitrary polynomial $f \in \mathcal{I}$. According to our assumption, its leading exponent $\mathrm{le}_\prec f$ lies in the involutive cone $\mathcal{C}_{L,\mathrm{le}_\prec \mathcal{H}}(h)$ of some element $h \in \mathcal{H}$. Let $\mu = \mathrm{le}_\prec f - \mathrm{le}_\prec h$ and set $f_1 = f - cx^\mu \star h$ where the coefficient $c \in \Bbbk$ is chosen such that the leading terms cancel. Obviously, $f_1 \in \mathcal{I}$ and $\mathrm{lt}_\prec f_1 \prec \mathrm{lt}_\prec f$. Thus we can iterate the procedure obtaining a sequence of polynomials $f_i \in \mathcal{I}$. After a finite number of steps we must reach $f_N = 0$, as the leading terms are always decreasing and by assumption *any* polynomial $f \in \mathcal{I}$ is involutively head reducible with respect to $\mathcal{H}$. But this implies that $f \in \langle \mathcal{H} \rangle_{L,\prec}$.

Thus we have proved that if $\mathrm{le}_{\prec}\mathcal{H}$ is a weak involutive basis of $\mathrm{le}_{\prec}\mathcal{I}$, then $\mathcal{H}$ is a weak involutive basis of $\mathcal{I}$. If $\mathrm{le}_{\prec}\mathcal{H}$ is a strong involutive basis of $\mathrm{le}_{\prec}\mathcal{I}$, then $\mathcal{H}$ is obviously involutively head autoreduced so that in this case it is in fact a strong involutive basis of $\mathcal{I}$.

For the converse we invoke Proposition 2.3.10. If the set $\mathcal{H}$ is a strong involutive basis, any polynomial f has a standard representation $f = \sum_{h\in\mathcal{H}} P_h \star h$ with $P_h \in \Bbbk[X_{L,\mathcal{H},\prec}(h)]$ and $\mathrm{lt}_{\prec}(P_h \star h) \preceq \mathrm{lt}_{\prec} f$ for all $h \in \mathcal{H}$. Thus we must have $\mathrm{le}_{\prec} f = \mathrm{le}_{\prec}(P_h \star h)$ for some $h \in \mathcal{H}$ and $\mathrm{le}_{\prec}\mathcal{H}$ is at least a weak involutive basis of the monoid ideal $\mathrm{le}_{\prec}\mathcal{I}$. But as $\mathcal{H}$ is involutively head autoreduced, it is in fact a strong involutive basis. $\square$

Corollary 2.3.12. *Let $\mathcal{H}$ be an involutive basis of the ideal $\mathcal{I} \subseteq \mathcal{P}$. Then $\mathcal{H}$ is a Gröbner basis of $\mathcal{I}$. Furthermore, the involutive and the ordinary normal form of any polynomial $f \in \mathcal{P}$ are identical.*

Proof. The first assertion follows at once from Theorem 2.3.11. As $\mathrm{le}_{\prec}\mathcal{H}$ is even an involutive basis of $\mathrm{le}_{\prec}\mathcal{I}$, it satisfies of course $\langle \mathrm{le}_{\prec}\mathcal{H}\rangle = \mathrm{le}_{\prec}\mathcal{I}$ so that $\mathcal{H}$ is a Gröbner basis of $\mathcal{I}$ by Definition 2.2.2.

The second assertion is a trivial consequence of the first. If $\mathcal{H}$ is an involutive basis, it is involutively head autoreduced. Thus by Proposition 2.3.7 involutive normal forms with respect to $\mathcal{H}$ are unique. As $\mathcal{H}$ is also a Gröbner basis, ordinary normal forms are unique, too. Finally, any polynomial in ordinary normal form is trivially in involutive normal form. Hence the two normal forms must coincide. $\square$

Remark 2.3.13. If $\mathcal{G}$ is a Gröbner basis of the ideal $\mathcal{I}$, then $\mathcal{I}$ cannot contain "integrability conditions" in the sense defined above, as any element of $\mathcal{I}$ has a standard representation by Proposition B.2.7. But this does not imply that for a given division L the ideal $\mathcal{I}$ is free of obstructions to involution. In order to obtain at least a weak involutive basis, we must add further elements of $\mathcal{I}$ to $\mathcal{G}$ until $\langle \mathrm{le}_{\prec}\mathcal{G}\rangle_L = \mathrm{le}_{\prec}\mathcal{I}$. Obviously, this observation allows us to reduce the construction of polynomial involutive bases to the monomial case. But we will see in Section 6.4 that better possibilities exist.

It follows from these considerations that in general involutive bases are not reduced Gröbner bases, as we already observed in Example 2.3.9. For $\prec_{\mathrm{deglex}}$ the set $\mathcal{F}$ was simultaneously a Janet basis and a reduced Gröbner basis. But for $\prec_{\mathrm{deginvlex}}$ the reduced Gröbner basis is $\mathcal{F} \cup \{f_4\}$, whereas a Janet basis requires in addition the polynomial f_5. We will see in the next sections that this "redundancy" in involutive bases is the key for their use in the structure analysis of polynomial ideals and modules. $\triangleleft$

Finally, we discuss the generalisation of Proposition 2.1.10 to the polynomial case. It turns out that only under additional assumptions, it is easily possible to obtain a strong involutive basis from a weak one.

Proposition 2.3.14. *Let $\mathcal{I} \subseteq \mathcal{P}$ be an ideal and $\mathcal{H} \subset \mathcal{P}$ a finite set such that $\mathrm{le}_\prec\mathcal{H}$ is a weak involutive basis of $\mathrm{le}_\prec\mathcal{I}$ for the involutive division L. Then there exists a subset $\mathcal{H}' \subseteq \mathcal{H}$ that is a strong involutive basis of $\mathcal{I}$.*

Proof. If the set $\mathcal{H}$ is involutively head autoreduced, it is already a strong involutive basis and we are done. Otherwise $\mathcal{H}$ contains polynomials h_1, h_2 such that $\mathrm{le}_\prec h_1 \mid_{L,\mathrm{le}_\prec\mathcal{H}} \mathrm{le}_\prec h_2$. Consider $\mathcal{H}' = \mathcal{H} \setminus \{h_2\}$. By the same arguments as in the proof of Proposition 2.1.10 one easily shows that $\mathrm{le}_\prec\mathcal{H}' = \mathrm{le}_\prec\mathcal{H} \setminus \{\mathrm{le}_\prec h_2\}$ is still a weak involutive basis of $\mathrm{le}_\prec\mathcal{I}$ and thus by Theorem 2.3.11 the set $\mathcal{H}'$ is still a weak involutive basis of $\mathcal{I}$. We can repeat such eliminations, until we reach a strong involutive basis. □

Example 2.3.15. In order to demonstrate why we really need in Proposition 2.3.14 the additional assumption on the leading exponents of the basis, we consider in the ordinary polynomial ring $\Bbbk[x, y]$ the ideal $\mathcal{I}$ generated by the two polynomials $f_1 = y^2$ and $f_2 = y^2 + x^2$. If we order the variables as $x^1 = x$ and $x^2 = y$, then $\mathcal{H} = \{f_1, f_2\}$ is a weak Janet basis of $\mathcal{I}$, as all variables are multiplicative for each generator. However, $\mathrm{le}_\prec\mathcal{H} = \{[0, 2]\}$ does *not* generate $\mathrm{le}_\prec\mathcal{I}$, as obviously $[2, 0] \in \mathrm{le}_\prec\mathcal{I} \setminus \langle\{[0, 2]\}\rangle$.

Thus the assumption of Proposition 2.3.14 is not satisfied. Indeed, elimination of one of the generators leads to a set which no longer generates $\mathcal{I}$. One could hope that an involutive autoreduction of $\mathcal{H}$ might lead to a strong involutive basis, but this is not the case. We obtain the set $\mathcal{H}' = \{x^2, y^2\}$ which is not even a weak involutive basis of $\mathcal{I}$, as y is not multiplicative for x^2 and $x^2y \notin \langle\mathcal{H}'\rangle_{J,\prec}$. ◁

2.4 Pommaret Bases and δ-Regularity

We have seen in Example 2.1.12 that not every monoid ideal in $\mathbb{N}_0^n$ possesses a finite Pommaret basis: the Pommaret division is not Noetherian. This phenomenon is known under the name δ*-regularity*. We study it in this section for (ordinary) polynomial ideals; the extension to differential equations is straightforward. But before, we prove two technical lemmata.

Lemma 2.4.1. *Let $\mathcal{H}$ be a homogeneous Pommaret basis of the homogeneous ideal $\mathcal{I} \subseteq \mathcal{P}$. If $q \geq \max_{h\in\mathcal{H}} \deg h$, then a Pommaret basis of the truncation $\mathcal{I}_{\geq q} = \bigoplus_{p\geq q} \mathcal{I}_p$ is given by*

$$\mathcal{H}_q = \left\{x^\mu h \mid h \in \mathcal{H},\ |\mu| + \deg h = q,\ \mu_j = 0\ \forall j > \operatorname{cls} h\right\}. \tag{2.18}$$

Conversely, if $\mathcal{I}_{\geq q}$ possesses a Pommaret basis, then so does $\mathcal{I}$.

Proof. By the conditions in (2.18), any polynomial $h \in \mathcal{H}$ is multiplied by terms x^μ containing only variables multiplicative for it. Thus trivially $\operatorname{cls}(x^\mu h) = \operatorname{cls}\mu$. Furthermore, $\mathcal{H}_q$ is involutively head autoreduced, as $\mathcal{H}$ is. Now let $f \in \mathcal{I}_{\geq q}$ be an arbitrary homogeneous polynomial. As $\mathcal{H}$ is a Pommaret basis of $\mathcal{I}$, it has a standard representation $f = \sum_{h\in\mathcal{H}} P_h h$ with $P_h \in \mathbb{k}[x^1,\dots,x^{\operatorname{cls} h}]$. Hence f can be written as a linear combination of polynomials $x^\nu h$ where $|\nu| = \deg f - \deg h \geq q - \deg h$ and where x^ν contains only multiplicative variables. We decompose $\nu = \mu + \rho$ with $|\mu| = q - \deg h$ and $\rho_j = 0$ for all $j > \operatorname{cls}\mu$. Thus $x^\nu h = x^\rho(x^\mu h)$ with $x^\mu h \in \mathcal{H}_q$ and x^ρ contains only variables multiplicative for it. But this trivially implies the existence of a standard representation $f = \sum_{h'\in\mathcal{H}_q} P_{h'} h'$ with $P_{h'} \in \mathbb{k}[x^1,\dots,x^{\operatorname{cls} h'}]$ and thus $\mathcal{H}_q$ is a Pommaret basis of $\mathcal{I}_{\geq q}$.

The converse is also very simple. Let $\mathcal{H}_q$ be a Pommaret basis of $\mathcal{I}_{\geq q}$ and $\mathcal{H}_p$ bases of $\mathcal{I}_p$ as a vector space for $0 \leq p < q$. If we set $\mathcal{H} = \bigcup_{p=0}^{q} \mathcal{H}_q$, then $\operatorname{le}_\prec \mathcal{H}$ is obviously a weak Pommaret basis of $\operatorname{le}_\prec \mathcal{I}$ and by Proposition 2.3.14 an involutive head autoreduction yields a strong basis. □

We call the number $q = \max_{h\in\mathcal{H}} \deg h$ the *degree* of the basis $\mathcal{H}$ and write $\deg \mathcal{H} = q$.

Lemma 2.4.2. *With the same notations as in Lemma 2.4.1, let $\mathcal{N} = \operatorname{le}_\prec \mathcal{H}_q$. If $\nu \in \mathcal{N}$ with $\operatorname{cls}\nu = k$, then $\nu - 1_k + 1_j \in \mathcal{N}$ for all $j > k$.*

Proof. j is non-multiplicative for ν. As $\mathcal{N}$ is an involutive basis of $\operatorname{le}_\prec \mathcal{I}_{\geq q}$, it must contain a multi index μ with $\mu \mid_P \nu + 1_j$. Obviously, $\operatorname{cls}(\nu + 1_j) = k$ and thus $\operatorname{cls}\mu \geq k$. Because of $|\mu| = |\nu|$, the only possibility is $\mu = \nu + 1_j - 1_k$. □

The basic observation is that δ-regularity is a question of the used coordinates. With the help of a linear coordinate transformation, any ideal can be mapped into another one that has a finite Pommaret basis. The first problem is to detect that one is using "bad" coordinates and the second problem to find "good" ones. A number of different solutions exist; most of them tend to be computationally rather expensive. We present here a new one; its main advantage is that it is very cheap.

We start with an algebraic definition of δ-regularity. Let as always $\mathcal{P} = \mathbb{k}[x^1,\dots,x^n]$ be the polynomial ring and $\prec$ a term order. A linear change of variables $\tilde{x} = Ax$ with a regular matrix $A \in \mathbb{k}^{n\times n}$ transforms any polynomial in $\mathcal{P}$ into a polynomial of the same degree in $\tilde{\mathcal{P}} = \mathbb{k}[\tilde{x}^1,\dots,\tilde{x}^n]$. We use on $\tilde{\mathcal{P}}$ the same term order as on $\mathcal{P}$; i. e. if we ordered, say, degree reverse lexicographically on $\mathcal{P}$, we order again degree reverse lexicographically on $\tilde{\mathcal{P}}$. In other words, we are actually using an order defined on $\mathbb{N}_0^n$; performing a variable transformation only changes the multi indices appearing as exponents.

Let $\mathcal{F} \subset \mathcal{P}$ be a finite subset which is involutively head autoreduced with respect to an involutive division L. We call the total number of multiplicative variables of its elements its *involutive size* and denote it by

$$|\mathcal{F}|_{L,\prec} = \sum_{f \in \mathcal{F}} |X_{L,\prec,\mathcal{F}}(f)| \ . \tag{2.19}$$

Applying the above transformation yields a set $\tilde{\mathcal{F}} \subset \tilde{\mathcal{P}}$. In general, $\tilde{\mathcal{F}}$ is no longer involutively head autoreduced, but we can easily perform an involutive head autoreduction obtaining a set $\tilde{\mathcal{F}}^{\triangle}$. The leading exponents of $\tilde{\mathcal{F}}^{\triangle}$ may be very different from those of $\mathcal{F}$ and thus $|\mathcal{F}|_{L,\prec}$ may differ from $|\tilde{\mathcal{F}}^{\triangle}|_{L,\prec}$.

Definition 2.4.3. *Let the finite set $\mathcal{F} \subset \mathcal{P}$ be involutively head autoreduced with respect to the Pommaret division. The coordinates $\mathbf{x}$ are* δ-regular *for $\mathcal{F}$, if after any linear change of coordinates $\tilde{\mathbf{x}} = A\mathbf{x}$ the inequality $|\mathcal{F}|_{P,\prec} \geq |\tilde{\mathcal{F}}^{\triangle}|_{P,\prec}$ holds.*

Example 2.4.4. Let us reconsider Example 2.1.12 in terms of polynomials. Thus we take the set $\mathcal{F} = \{xy\} \subset \Bbbk[x,y]$. Independent of how we order the variables, the class of xy is 1. After the change of coordinates $x = \tilde{x} + \tilde{y}$ and $y = \tilde{y}$, we obtain the set $\tilde{\mathcal{F}} = \{\tilde{y}^2 + \tilde{x}\tilde{y}\} \subset \Bbbk[\tilde{x},\tilde{y}]$. If we use the degree reverse lexicographic order, the leading term is $\tilde{y}^2$ which is of class 2. Thus it is possible to enlarge the involutive size of $\mathcal{F}$ and the original coordinates are not δ-regular. The new coordinates obviously are, as a higher class than 2 is not possible. ◁

Proposition 2.4.5. *Let $\mathcal{H}$ be a Pommaret basis of an ideal $\mathcal{I} \subseteq \mathcal{P}$. Then the coordinates $\mathbf{x}$ are δ-regular for $\mathcal{H}$.*

Proof. By Theorem 2.3.11, $\mathrm{le}_\prec \mathcal{H}$ is a Pommaret basis of $\mathrm{le}_\prec \mathcal{I}$. Thus it suffices to consider homogeneous ideals and, by Lemma 2.4.1, we may further reduce to the case that all generators are of the same degree q. The involutive size of $\mathcal{H}_q$ is then the vector space dimension of $\mathcal{I}_{q+1}$. This value is independent of the chosen coordinates and no involutively head autoreduced set may lead to a larger involutive size. Thus our coordinates are δ-regular. □

Thus δ-regularity is necessary for the existence of Pommaret bases and for the termination of the completion algorithms discussed in Chapter 6. From an algorithmic point of view, δ-singular coordinates are "bad". Fortunately, there are not many of them. Choosing an arbitrary coordinate system as reference, we may identify every coordinate system with the regular matrix $A \in \Bbbk^{n\times n}$ defining the transformation from our reference system to it.

Proposition 2.4.6. *Those coordinate systems that are δ-singular for a given finite involutively head autoreduced set $\mathcal{F} \subset \mathcal{P}$ form a Zariski closed set in $\Bbbk^{n\times n}$.*

Proof. Let us first perform a coordinate transformation with an undetermined matrix A, i. e. we are treating its entries as parameters. This obviously leads to a δ-regular coordinate system, as each polynomial in $\tilde{\mathcal{F}}^{\triangle}$ will get its maximally possible class. δ-singular coordinates are defined by the vanishing of certain (leading) coefficients. These coefficients are polynomials in the entries of A. Thus the set of all δ-singular coordinate systems can be described as the zero set of an ideal. □

By definition of the Zariski topology, this means that hardly any coordinate system is δ-singular. More precisely, they form a subset of dimension less than n^2 in an n^2-dimensional space. Thus if we randomly choose a coordinate system, it is δ-regular with probability 1! Nevertheless, δ-singular coordinate systems exist for most sets $\mathcal{F}$; exceptions are sets like $\mathcal{F} = \{x^2+y^2\}$ where one easily shows that any coordinate system is δ-regular. We will see below in the proof of Theorem 2.4.10 that it suffices for the construction of δ-regular coordinates to consider only transformations $\mathbf{x} \mapsto A\mathbf{x}$ where the matrix A satisfies $A_{ii} = 1$ and $A_{ij} = 0$ for $j > i$.

Our goal is to find a simple criterion for δ-singular coordinates. The basic idea is to compare the multiplicative variables assigned by the Pommaret and by the Janet division, respectively. The definitions of these two divisions are very different. Somewhat surprisingly, they yield very similar results.

Proposition 2.4.7. *Let the finite set $\mathcal{N} \subset \mathbb{N}_0^n$ be involutively autoreduced with respect to the Pommaret division. Then for all $\nu \in \mathcal{N}$ the inclusion $N_P(\nu) \subseteq N_{J,\mathcal{N}}(\nu)$ holds.*

Proof. Let $\nu \in \mathcal{N}$ with $\operatorname{cls}\nu = k$. Thus $\nu = [0, \dots, 0, \nu_k, \dots, \nu_n]$ with $\nu_k > 0$. We must show that the indices $1, \dots, k$ are multiplicative for ν with respect to the Janet division. In order to decide whether $k \in N_{J,\mathcal{N}}(\nu)$, we study the set $(\nu_{k+1}, \dots, \nu_n) \subseteq \mathcal{N}$. If it contained a multi index μ with $\mu_k > \nu_k$, the set $\mathcal{N}$ would not be involutively autoreduced with respect to the Pommaret division, as $\nu \mid_P \mu$. Thus k is multiplicative for the Janet division, too. The same argument can be applied for $k-1, \dots, 1$ where sets of the form $(0, \dots, 0, \nu_k, \dots, \nu_n)$ with an increasing number of zeros are considered. Hence $N_P(\nu) \subseteq N_{J,\mathcal{N}}(\nu)$. □

For later use, we note the following simple corollaries which further study the relationship between the Janet and the Pommaret division. Recall that by Remark 2.1.11 any set $\mathcal{N} \subset \mathbb{N}_0^n$ is involutively autoreduced with respect to the Janet division. We show first that by an involutive autoreduction of $\mathcal{N}$ with respect to the *Pommaret* division its *Janet* span can become only larger but not smaller.

Corollary 2.4.8. *Let $\mathcal{N} \subset \mathbb{N}_0^n$ be an arbitrary finite set of multi indices and $\mathcal{N}_P = \mathcal{N} \setminus \{\nu \in \mathcal{N} \mid \exists \mu \in \mathcal{N} : \mu \,|_P\, \nu\}$, i. e. we eliminate all multi indices possessing a Pommaret divisor in $\mathcal{N}$. Then $\langle \mathcal{N} \rangle_J \subseteq \langle \mathcal{N}_P \rangle_J$.*

Proof. If $\mu^{(1)} \,|_P\, \mu^{(2)}$ and $\mu^{(2)} \,|_P\, \nu$, then trivially $\mu^{(1)} \,|_P\, \nu$. Thus for each eliminated multi index $\nu \in \mathcal{N} \setminus \mathcal{N}_P$ another multi index $\mu \in \mathcal{N}_P$ exists with $\mu \,|_P\, \nu$. Let $\operatorname{cls}\mu = k$. By the proposition above $\{1, \dots, k\} \subseteq N_{J,\mathcal{N}_P}(\mu)$. Assume that an index $j > k$ exists with $j \in N_{J,\mathcal{N}}(\nu)$. By definition of the Pommaret division, $\mu_i = \nu_i$ for all $i > k$. Thus $\mu \in (\nu_{j+1}, \dots, \nu_n)$ and $j \in N_{J,\mathcal{N}}(\mu)$. As by the second condition on an involutive division $N_{J,\mathcal{N}}(\mu) \subseteq N_{J,\mathcal{N}_P}(\mu)$ for all $\mu \in \mathcal{N}_P$, we conclude that $j \in N_{J,\mathcal{N}_P}(\mu)$ and $\mathcal{C}_{J,\mathcal{N}}(\nu) \subset \mathcal{C}_{J,\mathcal{N}_P}(\mu)$. But this immediately implies $\langle \mathcal{N} \rangle_J \subseteq \langle \mathcal{N}_P \rangle_J$. □

The second corollary implies that any Pommaret basis is simultaneously a Janet basis. Thus if $\mathcal{H}$ is a Pommaret basis, then $X_{P,\prec}(h) = X_{J,\mathcal{H},\prec}(h)$ for all polynomials $h \in \mathcal{H}$.

Corollary 2.4.9. *Let the finite set $\mathcal{H} \subset \mathcal{P}$ be involutive with respect to the Pommaret division (and some term order). Then $\mathcal{H}$ is also involutive with respect to the Janet division.*

Proof. By the proposition above, it is obvious that the set $\mathcal{H}$ is at least weakly involutive with respect to the Janet division. For the Janet division any weakly involutive set is strongly involutive, as soon as no two elements have the same leading terms (recall Example 2.3.5). But as $\mathcal{H}$ is a Pommaret basis, this cannot happen. □

We show now that for δ-regular coordinate systems the inclusions in Proposition 2.4.7 must be equalities. In other words, if a variable x^ℓ exists which is multiplicative for an element of $\mathcal{F}$ with respect to the Janet division but non-multiplicative with respect to the Pommaret division, then the used coordinates are δ-singular. Our proof is constructive in the sense that it shows us how to find coordinates leading to a larger involutive span.

Theorem 2.4.10. *Let the finite set $\mathcal{F} \subset \mathcal{P}$ be involutively head autoreduced with respect to the Pommaret division and a class respecting term order. If $|\mathcal{F}|_{J,\prec} > |\mathcal{F}|_{P,\prec}$, the coordinates $\mathbf{x}$ are δ-singular for $\mathcal{F}$.*

Proof. By the proposition above, we have $X_P(f) \subseteq X_{J,\mathcal{F}}(f)$ for all $f \in \mathcal{F}$. Assume that for a polynomial $h \in \mathcal{F}$ the strict inclusion $X_P(h) \subset X_{J,\mathcal{F}}(h)$ holds. Thus a variable $x^\ell \in X_{J,\mathcal{F}}(h)$ with $\ell > k = \operatorname{cls} h$ exists. We perform the linear change of variables $x^i = \tilde{x}^i$ for $i \neq k$ and $x^k = \tilde{x}^k + a\tilde{x}^\ell$ with a yet arbitrary parameter $a \in \mathbb{k} \setminus \{0\}$. This induces the following transformation of the terms $x^\mu \in \mathbb{T}$:

$$x^\mu = \sum_{j=0}^{\mu_k} \binom{\mu_k}{j} a^j \tilde{x}^{\mu - j_k + j_\ell} \,. \tag{2.20}$$

Let $\operatorname{le}_\prec h = \mu$. Thus $\mu = [0, \dots, 0, \mu_k, \dots, \mu_n]$ with $\mu_k > 0$. We define $\nu = \mu - (\mu_k)_k + (\mu_k)_\ell$; obviously, $\operatorname{cls} \nu > k$ by construction. Applying our transformation to the polynomial h leads to a polynomial $\tilde{h}$ containing the term $\tilde{x}^\nu$. Note that ν cannot be an element of $\operatorname{le}_\prec \mathcal{F}$. Indeed, if it was, it would be an element of the same set $(\mu_{\ell+1}, \dots, \mu_n)$ as μ. But this contradicts our assumption that ℓ is multiplicative for the multi index μ with respect to the Janet division, as $\nu_\ell > \mu_\ell$.

Applying the transformation to all polynomials $f \in \mathcal{F}$ yields the set $\tilde{\mathcal{F}}$ on which we perform an involutive head autoreduction in order to obtain the set $\tilde{\mathcal{F}}^\triangle$. We are interested in its involutive size with respect to the Pommaret division. We can choose the parameter a such that after the transformation each polynomial $\tilde{f} \in \tilde{\mathcal{F}}$ has at least the same class as the corresponding polynomial $f \in \mathcal{F}$, as our term order respects classes. This is a simple consequence of (2.20): only for a finite number of values of a cancellations of terms may occur. It follows from the definition of the Pommaret division that if $\operatorname{le}_\prec f_2 \,|_P\, \operatorname{le}_\prec f_1$, then $\operatorname{cls} \operatorname{le}_\prec f_2 \geq \operatorname{cls} \operatorname{le}_\prec f_1$. Hence even after the involutive head autoreduction the involutive size of $\tilde{\mathcal{F}}^\triangle$ cannot be smaller than that of $\mathcal{F}$.

Now consider again the polynomial h. The leading term of the transformed polynomial $\tilde{h}$ must be greater than or equal to $\tilde{x}^\nu$. Thus its class is greater than k. This remains true even after an involutive head autoreduction with all those polynomials $\tilde{f} \in \tilde{\mathcal{F}}$ that are of class greater than k, as $x^\nu \notin \operatorname{lt}_\prec \mathcal{F}$. Hence the only possibility to obtain a leading term of class less than or equal to k consists of an involutive reduction with respect to a polynomial $\tilde{f} \in \tilde{\mathcal{F}}$ with $\operatorname{cls} f \leq k$. But this implies that $\operatorname{cls} \operatorname{le}_\prec \tilde{f} > k$. So we may conclude that after the transformation we have at least one polynomial more whose class is greater than k. So the coordinates $\mathbf{x}$ cannot be δ-regular. □

Corollary 2.4.11. *If the coordinates $\mathbf{x}$ are δ-regular for the Pommaret head autoreduced set $\mathcal{F}$, then $\langle \mathcal{F} \rangle_{J,\prec} = \langle \mathcal{F} \rangle_{P,\prec}$ for any class respecting term order $\prec$.*

It is important to note that this corollary provides us only with a necessary but *not* with a sufficient criterion for δ-regularity. In other words, even if the Janet and the Pommaret size are equal for a given set $\mathcal{F} \subset \mathcal{P}$, this does not imply that the used coordinates are δ-regular.

Example 2.4.12. Let $\mathcal{F} = \{\underline{z^2} + yz - x^2,\ \underline{xz} + xy - z,\ \underline{yz} + y^2 + x^2 - x\}$. The underlined terms are the leaders with respect to the degree reverse lexicographic order. One easily checks that the Janet and the Pommaret division yield the same multiplicative variables. If we perform the transformation $\tilde{x} = z$, $\tilde{y} = y + z$ and $\tilde{z} = x$, then after an autoreduction we obtain the set $\tilde{\mathcal{F}}^{\triangle} = \{\underline{\tilde{z}^2} - \tilde{x}\tilde{y},\ \underline{\tilde{y}\tilde{z}} - \tilde{x},\ \underline{\tilde{y}^2} - \tilde{z}\}$. Again the Janet and the Pommaret division yield the same multiplicative variables, but $|\tilde{\mathcal{F}}^{\triangle}|_{P,\prec} > |\mathcal{F}|_{P,\prec}$. Thus the coordinates (x, y, z) are not δ-regular for $\mathcal{F}$. $\triangleleft$

While we have defined δ-regularity as a problem of the Pommaret division, this example shows that in fact other divisions "feel" it, too. Usually they yield in δ-singular coordinates a lower number of multiplicative variables and thus larger involutive bases. δ-regularity is a typical phenomenon in commutative algebra. Many results are valid only in "generic" coordinates, i. e. for coordinates in a Zariski open set.

Besides being necessary for the mere existence of a finite Pommaret basis, a second application of δ-regular coordinates is the construction of $\mathcal{I}$-regular sequences for a homogeneous ideal $\mathcal{I} \subseteq \mathcal{P}$.

Proposition 2.4.13. *Let $\mathcal{I} \subseteq \mathcal{P}$ be a homogeneous ideal and $\mathcal{H}$ a homogeneous Pommaret basis for it with respect to the degree reverse lexicographic order. Let $d = \min_{h\in\mathcal{H}} \operatorname{cls} h$. Then $(x^1, \dots, x^d)$ is a maximal $\mathcal{I}$-regular sequence and* $\operatorname{depth} \mathcal{I} = d$.

Proof. A Pommaret basis $\mathcal{H}$ induces a decomposition of $\mathcal{I}$ of the form

$$\mathcal{I} = \bigoplus_{h\in\mathcal{H}} \Bbbk[x^1, \dots, x^{\operatorname{cls} h}] \cdot h\,. \tag{2.21}$$

If $d = \min_{h\in\mathcal{H}} \operatorname{cls} h$ denotes the minimal class of a generator in $\mathcal{H}$, then (2.21) trivially implies that the sequence $(x^1, \dots, x^d)$ is $\mathcal{I}$-regular.

Let us try to extend this sequence by a variable x^k with $k > d$. We set $\mathcal{H}_d = \{h \in \mathcal{H} \mid \operatorname{cls} h = d\}$ and choose an element $\bar{h} \in \mathcal{H}_d$ of maximal degree. As we use the degree reverse lexicographic order, $\bar{h} \in \langle x^1, \dots, x^d\rangle$ by Lemma B.2.2. Consider the product $x^k\bar{h}$; by construction x^k is non-multiplicative for $\bar{h}$. For each $h \in \mathcal{H}$ a polynomial $P_h \in \Bbbk[x^1, \dots, x^{\operatorname{cls} h}]$ exists such that $x^k\bar{h} = \sum_{h\in\mathcal{H}} P_h h$. No polynomial h with $\operatorname{cls} h > d$ lies in $\langle x^1, \dots, x^d\rangle$ (obviously $\operatorname{lt}_\prec h \notin \langle x^1, \dots, x^d\rangle$). As the leading terms cannot cancel in the sum, $P_h \in \langle x^1, \dots, x^d\rangle$ for all $h \in \mathcal{H} \setminus \mathcal{H}_d$. Thus $x^k\bar{h} = \sum_{h\in\mathcal{H}_d} c_h h + g$ with $c_h \in \Bbbk$ and $g \in \langle x^1, \dots, x^d\rangle\mathcal{I}$. As $\mathcal{I}$ is a homogeneous ideal and as the degree of $\bar{h}$ is maximal in $\mathcal{H}_d$, all constants c_h must vanish.

It is not possible that $\bar{h} \in \langle x^1, \dots, x^d\rangle\mathcal{I}$, as otherwise $\bar{h}$ would be involutively head reducible by some other element of $\mathcal{H}$. Hence we have shown that any variable x^k with $k > d$ is a zero divisor in $\mathcal{I}/\langle x^1, \dots, x^d\rangle\mathcal{I}$ and the $\mathcal{I}$-regular sequence $(x^1, \dots, x^d)$ cannot be extended by any x^k with $k > d$.

Finally, assume that $y^1, \dots, y^{d+1} \in \mathcal{P}_1$ form an $\mathcal{I}$-regular sequence of length $d+1$. We extend them to a basis $\{y^1, \dots, y^n\}$ of $\mathcal{P}_1$ and perform a coordinate transformation $\mathbf{x} \mapsto \mathbf{y}$. Our basis $\mathcal{H}$ transforms into the set $\mathcal{H}_{\mathbf{y}}$ and after an involutive head autoreduction we obtain the set $\mathcal{H}_{\mathbf{y}}^{\triangle}$. In general, the coordinates $\mathbf{y}$ are not δ-regular for $\mathcal{H}_{\mathbf{y}}^{\triangle}$. But there exist coordinates $\tilde{\mathbf{y}}$ of the form $\tilde{y}^k = y^k + \sum_{i=1}^{k-1} a_i^k y^i$ with $a_i^k \in \Bbbk$ such that if we transform $\mathcal{H}$ to them and perform afterwards an involutive head autoreduction, they are δ-regular for the obtained set $\tilde{\mathcal{H}}_{\mathbf{y}}^{\triangle}$.

This implies that $\tilde{\mathcal{H}}_{\mathbf{y}}^{\triangle}$ is a Pommaret basis of the ideal it generates.[2] Thus $\min_{\tilde{h} \in \tilde{\mathcal{H}}_{\mathbf{y}}^{\triangle}} \operatorname{cls} \tilde{h} = d$ and by the same argument as above $\tilde{y}^{d+1}$ is a zero divisor in $\mathcal{I}/\langle \tilde{y}^1, \dots, \tilde{y}^d \rangle \mathcal{I}$. Because of the special form of the transformation from $\mathbf{y} \mapsto \tilde{\mathbf{y}}$, we have $\langle \tilde{y}^1, \dots, \tilde{y}^d \rangle = \langle y^1, \dots, y^d \rangle$ and y^{d+1} must be a zero divisor in $\mathcal{I}/\langle y^1, \dots, y^d \rangle \mathcal{I}$. But this contradicts the assumption that $(y^1, \dots, y^{d+1})$ is an $\mathcal{I}$-regular sequence and $\operatorname{depth} \mathcal{I} = d$. □

Remark 2.4.14. One may wonder to what extent this result really requires the Pommaret division. Given an arbitrary involutive basis $\mathcal{H}$ of $\mathcal{I}$, we may introduce the set $X_{\mathcal{I}} = \bigcap_{h \in \mathcal{H}} X_{L,\mathcal{H},\prec}(h)$; obviously, for a Pommaret basis $\mathcal{X}_{\mathcal{I}} = \{x^1, \dots, x^d\}$ with $d = \operatorname{depth} \mathcal{I}$. Again it is trivial to conclude from the induced decomposition that any sequence formed by elements of $\mathcal{X}_{\mathcal{I}}$ is $\mathcal{I}$-regular. But in general we cannot claim that these are *maximal* $\mathcal{I}$-regular sequences. Thus only a lower bound for the depth is obtained.

As a simple example we consider the ideal $\mathcal{I}$ generated by $f_1 = z^2 - xy$, $f_2 = yz - x$ and $f_3 = y^2 - z$. If we set $x^1 = x$, $x^2 = y$ and $x^3 = z$, then the set $\mathcal{F} = \{f_1, f_2, f_3\}$ is a Pommaret basis of $\mathcal{I}$ with respect to the degree reverse lexicographic order. By Proposition 2.4.13, (x, y) is a maximal $\mathcal{I}$-regular sequence and $\operatorname{depth} \mathcal{I} = 2$.

If we set $x^1 = z$, $x^2 = y$ and $x^3 = x$ (i.e. we invert the ordering of the variables), then no finite Pommaret basis exists; these coordinates are not δ-regular. In order to obtain a Janet basis $\mathcal{F}_J$ of $\mathcal{I}$ (for the degree reverse lexicographic order with respect to the new ordering of the variables), we must enlarge $\mathcal{F}$ by $f_4 = z^3 - x^2$ and $f_5 = z^3x - x^3$. We find $X_{\mathcal{I}} = \{z\}$, as

$$\begin{aligned} &X_{J,\mathcal{F}_J,\prec_{\text{deglex}}}(f_1) = \{z, y, x\}\,, \quad X_{J,\mathcal{F}_J,\prec_{\text{deglex}}}(f_2) = \{z\}\,, \\ &X_{J,\mathcal{F}_J,\prec_{\text{deglex}}}(f_3) = \{z, y\}\,, \qquad X_{J,\mathcal{F}_J,\prec_{\text{deglex}}}(f_4) = \{z\}\,, \\ &X_{J,\mathcal{F}_J,\prec_{\text{deglex}}}(f_5) = \{z, x\}\,. \end{aligned} \tag{2.22}$$

The minimal number of multiplicative variables for a generator is 1 which is less than $\operatorname{depth} \mathcal{I}$. Thus no obvious way exists to deduce $\operatorname{depth} \mathcal{I}$ or a maximal

[2] The involutive sizes of $\mathcal{H}$ and $\tilde{\mathcal{H}}_{\mathbf{y}}^{\triangle}$ are equal. Thus local involution of $\mathcal{H}$ implies local involution of $\tilde{\mathcal{H}}_{\mathbf{y}}^{\triangle}$ and for the Pommaret division local involution is equivalent to involution (cf. Proposition 6.4.5 and Lemma 6.3.5).

$\mathcal{I}$-regular sequence. In particular, it is not possible to extend (z) to a longer $\mathcal{I}$-regular sequence: x is a zero divisor for $\mathcal{I}/z\mathcal{I}$, as $x(xf_2 - f_4) \in z\mathcal{I}$; similarly y, as $y(yf_2 - f_1) \in z\mathcal{I}$; and even for an arbitrary linear combination $ax + by$ with $a, b \in \Bbbk$ we find $(ax + by)\big[b(yf_2 - f_1) - a(xf_2 - f_4)\big] \in z\mathcal{I}$. ◁

2.5 Applications I: Combinatorial Decompositions

In the proof of Proposition 2.4.13 we could already see the power of the direct sum decompositions induced by (strong) involutive bases. In this section we want to study this aspect in more details. All results apply to arbitrary finitely generated polynomial modules. But for notational simplicity, we restrict to graded $\Bbbk$-algebras $\mathcal{A} = \mathcal{P}/\mathcal{I}$ for some homogeneous ideal $\mathcal{I} \subseteq \mathcal{P}$ where $\mathcal{P} = \Bbbk[x^1, \dots, x^n]$ is the ordinary polynomial ring. If we speak of a basis of the ideal $\mathcal{I}$, we always assume that it is homogeneous, too.

Recall that the main motivation of Buchberger for the introduction of Gröbner bases was to be able to compute effectively in such factor spaces. Indeed given a Gröbner basis $\mathcal{G}$ of the ideal $\mathcal{I}$, the normal form with respect to $\mathcal{G}$ distinguishes a unique representative in each equivalence class (cf. Remark B.2.9). Our goal in this and the next section is to show that Pommaret bases yield in addition a lot of structural information about the algebra $\mathcal{A}$. More precisely, we want to compute fundamental invariants like the Hilbert polynomial (which immediately yields the Krull dimension and the multiplicity), the depth or the Castelnuovo–Mumford regularity. Our basic tools are combinatorial decompositions of $\mathcal{A}$ into a direct sum of polynomial rings.

Definition 2.5.1. *A* Stanley decomposition *of the graded $\Bbbk$-algebra $\mathcal{A} = \mathcal{P}/\mathcal{I}$ consists of an isomorphism as $\Bbbk$-vector spaces*

$$\mathcal{A} \cong \bigoplus_{t \in \mathcal{T}} \Bbbk[X_t] \cdot t \tag{2.23}$$

with a finite set $\mathcal{T} \subset \mathbb{T}$ and sets $X_t \subseteq \{x^1, \dots, x^n\}$.

We call the elements of X_t again multiplicative variables. As a first, almost trivial application of such decompositions we determine the Hilbert series and the (Krull) dimension.

Proposition 2.5.2. *Let the graded algebra $\mathcal{A}$ possess the Stanley decomposition* (2.23)*. Then its Hilbert series is*

$$\mathcal{H}_{\mathcal{A}}(\lambda) = \sum_{t \in \mathcal{T}} \frac{\lambda^{q_t}}{(1-\lambda)^{k_t}} \tag{2.24}$$

where $q_t = \deg t$ *and* $k_t = |X_t|$. *Thus the (Krull) dimension of* $\mathcal{A}$ *is given by* $D = \max_{t\in\mathcal{T}}\{k_t\}$ *and the multiplicity (or degree) by the number of terms* $t \in \mathcal{T}$ *with* $k_t = D$.

Proof. The Hilbert series of a polynomial ring $\Bbbk[y^1, \dots, y^d]$ is given by $\mathcal{H}(\lambda) = 1/(1-\lambda)^d$. Indeed, the Taylor coefficient of order q of this function is $\binom{d+q-1}{q}$, the number of monomials of degree q in the ring by (A.4a). If the generator t is of degree q_t, we must shift all coefficients by q_t which is easily achieved by a multiplication with λ^{q_t}. Finally, we may simply add the contributions of the individual generators, as the right hand side of (2.23) is a direct sum. Thus we arrive at (2.24). The statements about the dimension and the multiplicity are simple corollaries. □

Vasconcelos [186, p. 23] calls Stanley decompositions *"an approach that is not greatly useful computationally but it is often nice theoretically"*. One reason for this assessment is surely that so far the main algorithms for their construction work only for monomial ideals $\mathcal{I}$. Thus one must first compute a Gröbner basis of $\mathcal{I}$ for some term order $\prec$ and then, exploiting that as vector spaces $\mathcal{P}/\mathcal{I} \cong \mathcal{P}/\mathrm{lt}_\prec\mathcal{I}$, one determines a Stanley decomposition. Its existence is guaranteed by the following result.

Proposition 2.5.3. *Let* $\mathcal{I} \subseteq \mathbb{N}_0^n$ *be a monoid ideal and* $\bar{\mathcal{I}} = \mathbb{N}_0^n \setminus \mathcal{I}$ *its complementary set. There exists a finite set* $\bar{\mathcal{N}} \subset \bar{\mathcal{I}}$ *and for each multi index* $\nu \in \bar{\mathcal{N}}$ *a set* $\emptyset \subseteq N_\nu \subseteq \{1, \dots, n\}$ *such that*

$$\bar{\mathcal{I}} = \bigcup_{\nu\in\bar{\mathcal{N}}} \left(\nu + \mathbb{N}^n_{N_\nu}\right) \tag{2.25}$$

and $(\nu + \mathbb{N}^n_{N_\nu}) \cap (\mu + \mathbb{N}^n_{N_\mu}) = \emptyset$ *for all* $\mu, \nu \in \bar{\mathcal{N}}$.

Proof. The assertion is trivial for the zero ideal, so we exclude this case and proceed by an induction on the number n. The case $n = 1$ is trivial, as any monoid ideal in $\mathbb{N}_0$ is of the form $\mathcal{I} = \langle [q] \rangle$ for some $q \in \mathbb{N}_0$ and hence $\bar{\mathcal{I}} = \{[0], [1], \dots, [q-1]\}$ which is obviously of the form (2.25) with $N_\nu = \emptyset$ for all ν.

Suppose now that the assertion is true for $n-1$. We want to show that it holds for n, too. But before we must introduce some notations. Primed letters always refer to multi indices $\nu' \in \mathbb{N}_0^{n-1}$; unprimed ones to multi indices $\nu \in \mathbb{N}_0^n$. For a given $\nu \in \mathbb{N}_0^n$, we define $\nu' = [\nu_1, \dots, \nu_{n-1}] \in \mathbb{N}_0^{n-1}$, i. e. we simply drop the last entry. Finally, we write $[\nu', q]$ for the multi index $[\nu_1, \dots, \nu_{n-1}, q] \in \mathbb{N}_0^n$.

Given a monoid ideal $\mathcal{I} \subseteq \mathbb{N}_0^n$, we define for all $q \in \mathbb{N}_0$ the monoid ideals $\mathcal{I}'_q = \left\{\nu' \in \mathbb{N}_0^{n-1} \mid [\nu', q] \in \mathcal{I}\right\}$ in $\mathbb{N}_0^{n-1}$. Thus we "slice" $\mathcal{I}$ by intersecting it with the "hyperplanes" $\nu_n = \mathit{Const}$. Obviously, for $q < r$ we have $\mathcal{I}'_q \subseteq \mathcal{I}'_r$ so that these ideals form an ascending chain. As $\mathbb{N}_0^{n-1}$ is a Noetherian monoid, an integer $q_0 \in \mathbb{N}$ exists such that $\mathcal{I}'_q = \mathcal{I}'_{q_0}$ for all $q \geq q_0$.

According to our inductive hypothesis, the complements $\bar{\mathcal{I}}'_q$ of each of these monoid ideals for $0 \leq q \leq q_0$ can be disjointly decomposed in the form

$$\bar{\mathcal{I}}'_q = \bigcup_{\nu' \in \bar{\mathcal{N}}_q^{(n-1)}} \left(\nu' + \mathbb{N}^{n-1}_{N_{\nu'}}\right) \tag{2.26}$$

with some subsets $\bar{\mathcal{N}}_q^{(n-1)} \subset \mathbb{N}_0^{n-1}$ and $N_{\nu'} \subseteq \{1,\dots,n-1\}$. We set now $\bar{\mathcal{N}}_q^{(n)} = \left\{[\nu', q] \mid \nu' \in \bar{\mathcal{N}}_q^{(n-1)}\right\}$ and $\bar{\mathcal{N}} = \bigcup_{q=0}^{q_0} \bar{\mathcal{N}}_q^{(n)}$. Furthermore, we choose $N_{[\nu',q]} = N_{\nu'}$ for $q < q_0$ and $N_{[\nu',q]} = N_{\nu'} \cup \{n\}$ for $q = q_0$.

Setting $\mathcal{U} = \bigcup_{\nu \in \bar{\mathcal{N}}} (\nu + \mathbb{N}^n_{N_\nu})$, the union is obviously disjoint. We claim that $\mathcal{U} = \bar{\mathcal{I}}$ which implies our proposition. Let $\mu \in \mathcal{U}$, then by construction of the set $\bar{\mathcal{N}}$ we have that $\mu' \in \bar{\mathcal{I}}'_q$ for some $0 \leq q \leq q_0$ and hence by definition of the ideals $\mathcal{I}'_q$, the multi index μ cannot be an element of $\mathcal{I}$. Thus $\mathcal{U} \subseteq \bar{\mathcal{I}}$. Conversely, $\mu \in \bar{\mathcal{I}}$ implies $\mu' \in \bar{\mathcal{I}}'_{\mu_n}$. If $\mu_n \geq q_0$, then $\mathcal{I}'_{\mu_n} = \mathcal{I}'_{q_0}$ and a multi index $\nu' \in \bar{\mathcal{N}}_{q_0}^{(n-1)}$ exists such that $\mu' \in \nu' + \mathbb{N}^{n-1}_{N_{\nu'}}$. Thus $\mu \in \nu + \mathbb{N}^n_\nu$ with $\nu = [\nu', q_0]$. If $\mu_n < q_0$, then a multi index $\nu' \in \bar{\mathcal{N}}_{\mu_n}^{(n-1)}$ exists such that $\mu' \in \nu' + \mathbb{N}^{n-1}_{N_{\nu'}}$ and in this case $\mu \in \nu + \mathbb{N}^n_\nu$ with $\nu = [\nu', \mu_n]$. Thus we have $\bar{\mathcal{I}} \subseteq \mathcal{U}$ and consequently $\mathcal{U} = \bar{\mathcal{I}}$ as claimed. □

One must stress that the decomposition (2.25) is not unique and different decompositions may use sets $\bar{\mathcal{N}}$ of different sizes. The elements in the sets N_ν are again called *multiplicative indices*. The proof above is not completely constructive, as the number q_0 was defined by a Noetherian argument. But it is not difficult to see that we may take $q_0 = \max_{\nu \in \mathcal{N}} \nu_n$ where $\mathcal{N}$ is the minimal basis of the monoid ideal $\mathcal{I}$. Now one can straightforwardly transform our proof into a recursive algorithm for the construction of Stanley decompositions. If a Janet basis of $\mathcal{I}$ is known, an alternative algorithm exists.

Proposition 2.5.4. *Let $\mathcal{N}_J$ be a Janet basis of the monoid ideal $\mathcal{I} \subseteq \mathbb{N}_0^n$. Then the set $\bar{\mathcal{N}} \subset \mathbb{N}_0^n$ in* (2.25) *may be chosen such that for all $\nu \in \bar{\mathcal{N}}$ the equality $N_\nu = N_{J,\mathcal{N}_J \cup \{\nu\}}(\nu)$ holds.*

Proof. We explicitly construct such a set $\bar{\mathcal{N}}$. Let $q_n = \max_{\mu \in \mathcal{N}_J} \mu_n$. Then we put into $\bar{\mathcal{N}}$ all multi indices $\nu = [0,\dots,0,q]$ such that $0 \leq q < q_n$ and such that $\mathcal{N}_J$ does not contain any multi index μ with $\mu_n = q$. We set $N_\nu = \{1,\dots,n-1\}$ which obviously is just $N_{J,\mathcal{N}_J \cup \{\nu\}}(\nu)$ according to the definition of the Janet division given in Example 2.1.2.

Let $(d_k,\dots,d_n) \subseteq \mathcal{N}_J$ be one of the subsets (2.2) considered in the assignment of the multiplicative variables to the elements of $\mathcal{N}_J$ according to the definition of the Janet division and set $q_{k-1} = \max_{\mu \in (d_k, \dots, d_n)} \mu_{k-1}$. We enlarge the set $\bar{\mathcal{N}}$ by all those multi indices $\nu = [0, \dots, 0, q, d_k, \dots, d_n]$ where $0 \leq q < q_{k-1}$ and where $(d_k, \dots, d_n)$ does not contain any multi index μ with $\mu_{k-1} = q$. The corresponding sets N_ν of multiplicative indices contain the indices $1, \dots, k-1$ and all those indices greater than k that are multiplicative for the elements of $(d_k, \dots, d_n)$. Again it is easy to verify that this entails $N_\nu = N_{J, \mathcal{N}_J \cup \{\nu\}}(\nu)$.

We claim that the thus constructed set $\bar{\mathcal{N}}$ (together with the sets N_ν) defines a disjoint decomposition (2.25) of the complementary set $\bar{\mathcal{I}}$. Like in the proof of the previous proposition we proceed by an induction on n and use again the notations introduced there. The case $n = 1$ is trivial. Suppose that our assertion is true for $n-1$. Let $\rho \in \mathbb{N}_0^n$ be an arbitrary multi index and let $q_1 < q_2 < \cdots < q_r$ represent all values that occur for the entry μ_n in the multi indices $\mu \in \mathcal{N}_J$. We must distinguish three cases depending on the value of ρ_n: (i) $\rho_n < q_r$ but $\rho_n \notin \{q_1, \dots, q_{r-1}\}$, (ii) $\rho_n \in \{q_1, \dots, q_{r-1}\}$, and (iii) $\rho_n \geq q_r$.

In the first case, $\bar{\mathcal{N}}$ contains the multi index $\nu = [0, \dots, 0, \rho_n]$ and, as $N_\nu = \{1, \dots, n-1\}$, obviously $\rho \in \nu + \mathbb{N}^n_{N_\nu}$. It is easy to see that ρ cannot be an element of $\mathcal{I}$ or of the cone $\bar{\nu} + \mathbb{N}^n_{N_{\bar{\nu}}}$ of any other multi index $\bar{\nu} \in \bar{\mathcal{N}}$.

In the second case, we "slice" the sets $\mathcal{N}_J$ and $\bar{\mathcal{N}}$ at degree ρ_n and obtain thus the two sets $\mathcal{N}'_J = \{\mu' \in \mathbb{N}_0^{n-1} \mid \mu \in \mathcal{N}_J,\ \mu_n = \rho_n\} \subset \mathbb{N}_0^{n-1}$ and $\bar{\mathcal{N}}' = \{\nu' \in \mathbb{N}_0^{n-1} \mid \nu \in \bar{\mathcal{N}},\ \nu_n = \rho_n\} \subset \mathbb{N}_0^{n-1}$, respectively. If we compute the sets $N_{J, \mathcal{N}'_J}(\mu')$ of multiplicative indices for the elements $\mu' \in \mathcal{N}'_J$, it is straightforward to verify that they are just $N_{J, \mathcal{N}_J}(\mu)$, as μ_n is not maximal and $\mu \in (\rho_n)$, if and only if $\mu' \in \mathcal{N}'_J$. Furthermore, $\mathcal{N}'_J$ is a Janet basis of the monoid ideal $\mathcal{I}'_{\rho_n}$. If we apply the procedure above to this ideal in $\mathbb{N}_0^{n-1}$, we obtain $\bar{\mathcal{N}}'$ as complementary basis and the sets of multiplicative variables remain unchanged.

By our inductive hypothesis, $\bar{\mathcal{N}}'$ defines a disjoint decomposition of the sought form of the set $\bar{\mathcal{I}}'_{\rho_n}$. If $\rho \in \bar{\mathcal{I}}$, then $\rho' \in \bar{\mathcal{I}}'_{\rho_n}$ and a multi index $\nu' \in \bar{\mathcal{N}}'$ exists such that $\rho' \in \nu' + \mathbb{N}^{n-1}_{N_{\nu'}}$. By construction, $\nu = [\nu', \rho_n] \in \bar{\mathcal{N}}$ and $\rho \in \nu + \mathbb{N}^n_{N_\nu}$. If $\rho \in \mathcal{I}$, then $\rho' \in \mathcal{I}'_{\rho_n}$, and it is not possible to find a multi index $\nu' \in \bar{\mathcal{N}}'$ such that $\rho' \in \nu' + \mathbb{N}^{n-1}_{N_{\nu'}}$. Hence $\rho \notin \nu + \mathbb{N}^n_{N_\nu}$ for any $\nu \in \bar{\mathcal{N}}$.

The third case is very similar to the second one. For the definition of $\mathcal{N}'_J$ and $\bar{\mathcal{N}}'$ we consider only multi indices where the value of the last entry is q_r. Note that for all multi indices $\nu \in \bar{\mathcal{N}}$ that contribute to $\bar{\mathcal{N}}'$ the index n is multiplicative. If $\rho \in \bar{\mathcal{I}}$, then $\rho' \in \bar{\mathcal{I}}'_{\rho_n}$ and a multi index $\nu' \in \bar{\mathcal{N}}'$ exists such that $\rho' \in \nu' + \mathbb{N}^{n-1}_{N_{\nu'}}$ and we conclude as above that $\rho \in \nu + \mathbb{N}^n_{N_\nu}$ for $\nu = [\nu', q_r] \in \bar{\mathcal{N}}$. Again it is obvious that for a multi index $\rho \in \mathcal{I}$, it is not possible to find such a $\nu \in \bar{\mathcal{N}}$. □

We have formulated this proposition only for the case that $\mathcal{N}_J$ is a Janet basis, but our proof yields an even stronger result. Let $\mathcal{N}_J$ be an *arbitrary* subset of $\mathbb{N}_0^n$ and construct the corresponding set $\bar{\mathcal{N}}$. Then we may substitute everywhere in the proof $\mathcal{I}$ by the involutive span $\langle\mathcal{N}_J\rangle_J$ and still obtain that any multi index $\rho \in \mathbb{N}_0^n$ either lies in $\langle\mathcal{N}_J\rangle_J$ or in exactly one of the cones defined by $\bar{\mathcal{N}}$ and the sets N_ν.

Example 2.5.5. Consider the simple example $\mathcal{N}_J = \{[1,1]\}$. Our construction yields $\nu^{(1)} = [0,0]$ with $N_{\nu^{(1)}} = \{1\}$ and $\nu^{(2)} = [0,1]$ with $N_{\nu^{(2)}} = \{2\}$. Obviously, the corresponding cones disjointly decompose the complementary set $\bar{\mathcal{I}} = \{[i,j] \in \mathbb{N}_0^2 \mid ij = 0\}$. ◁

According to Corollary 2.4.9, we may apply the same construction to Pommaret bases. But as the Pommaret division is globally defined, it is very simple to give an alternative decomposition.

Proposition 2.5.6. *Let $\mathcal{N}_P \subset \mathbb{N}_0^n$ be a Pommaret basis of the monoid ideal $\mathcal{I} \subseteq \mathbb{N}_0^n$ and $q = \max_{\nu\in\mathcal{N}_P}|\nu|$. If we introduce $\bar{\mathcal{N}}_0 = \{\nu \in \bar{\mathcal{I}} \mid |\nu| < q\}$ and $\bar{\mathcal{N}}_1 = \{\nu \in \bar{\mathcal{I}} \mid |\nu| = q\}$, then*

$$\bar{\mathcal{I}} = \bar{\mathcal{N}}_0 \cup \bigcup_{\nu\in\bar{\mathcal{N}}_1} \mathcal{C}_P(\nu)\ . \tag{2.27}$$

Proof. The definition of the Pommaret division implies the identity

$$(\mathbb{N}_0^n)_{\geq q} = \bigcup_{|\nu|=q} \mathcal{C}_P(\nu) \tag{2.28}$$

from which the proposition follows trivially. Here $(\mathbb{N}_0^n)_{\geq q}$ denotes the set of all multi indices of length greater than or equal to q. By the definition of an involutive division, the union on the right hand side is disjoint. □

Example 2.5.7. The decomposition (2.27) is usually redundant. Considering for $\bar{\mathcal{N}}_1$ only multi indices of length q makes the formulation much easier but it is not optimal. Consider the trivial example $\mathcal{N}_P = \{[0,1]\}$. According to Proposition 2.5.6 we should set $\bar{\mathcal{N}}_0 = \{[0,0]\}$ and $\bar{\mathcal{N}}_1 = \{[1,0]\}$. But obviously $\bar{\mathcal{I}} = [0,0] + \mathbb{N}_{\{1\}}^2$. Applying the construction used in the proof of Proposition 2.5.4 yields directly this more compact form. ◁

A very interesting special type of Stanley decompositions are *Rees decompositions*. Here the sets X_t are of the form $X_t = \{x^1, \dots, x^{\operatorname{cls} t}\}$ where the number $\operatorname{cls} t$ is called the *class*[3] of the generator t. It is no coincidence that we use here the same terminology as in the Pommaret division. By Proposition 2.5.6, a Pommaret basis of the ideal $\mathcal{I} \subseteq \mathcal{P}$ immediately induces a Rees

[3] Some authors also use the term *level*.

decomposition of the algebra $\mathcal{P}/\mathcal{I}$. If $t = x^\mu$ with $\mu \in \bar{\mathcal{N}}_1$, then indeed its class is just the usual one of its multi index. As an application, we show that given a Pommaret basis of $\mathcal{I}$, we can easily read off the dimension and the depth of $\mathcal{A} = \mathcal{P}/\mathcal{I}$.

Proposition 2.5.8. *Let $\mathcal{H}$ be a Pommaret basis of degree q of the homogeneous ideal $\mathcal{I} \subseteq \mathcal{P}$. The dimension of the algebra $\mathcal{A} = \mathcal{P}/\mathcal{I}$ is given by $D = \min\{i \mid \langle \mathcal{H}, x^1, \dots, x^i\rangle_q = \mathcal{P}_q\}$.*

Proof. The Hilbert polynomials of $\mathcal{A}$ and the truncation $\mathcal{A}_{\geq q}$ coincide. Thus it suffice to consider the latter algebra. By Lemma 2.4.1, a Pommaret basis of $\mathcal{I}_{\geq q}$ is given by the set $\mathcal{H}_q$ determined in (2.18). If D is the smallest number such that $\langle \mathcal{H}_q, x^1, \dots, x^D\rangle_q = \mathcal{P}_q$, then all multi indices $\nu \in \mathbb{N}_0^n$ with $|\nu| = q$ and $\operatorname{cls}\nu > D$ lie in $\operatorname{le}_\prec \mathcal{H}_q$ but a multi index $\mu \in \mathbb{N}_0^n$ exists such that $|\mu| = q$, $\operatorname{cls}\mu = D$ and $\mu \neq \operatorname{le}_\prec \mathcal{H}_q$. By Proposition 2.5.6 this entails that μ is a generator of class D of the decomposition (2.27) and that the decomposition does not contain a generator of higher class. But this trivially implies that $\dim \mathcal{A} = D$. □

In a terminology apparently introduced by Gröbner [65, Section 131], a subset $X_\mathcal{I} \subseteq \{x^1, \dots, x^n\}$ is *independent modulo* $\mathcal{I}$, if $\mathcal{I} \cap \Bbbk[X_\mathcal{I}] = \{0\}$ and $\dim \mathcal{I}$ is the maximal size of an independent set. This approach to the dimension of an ideal has been taken up again by Kredel and Weispfenning [97] using Gröbner bases (see also [15, Sections 6.3 and 9.3]).

Corollary 2.5.9. *Under the assumptions of Proposition 2.5.8, $\{x^1, \dots, x^D\}$ is a maximal independent set modulo the ideal $\mathcal{I}$.*

Proof. Let $d = \min_{h\in\mathcal{H}} \operatorname{cls} h$. Then $\{x^1, \dots, x^{d-1}\}$ is trivially an independent set. Indeed, since $\operatorname{lt}_\prec \mathcal{H} \subset \Bbbk[x^d, \dots, x^n]$ and $\operatorname{lt}_\prec \mathcal{I} = \langle \operatorname{lt}_\prec \mathcal{H}\rangle$, no non-zero element of $\mathcal{I}$ has a leading term in $\Bbbk[x^1, \dots, x^{d-1}]$. Obviously, $D \geq d$.

As above, it suffices to consider the truncation $\mathcal{I}_{\geq q}$. Assume a non-zero polynomial $f \in \mathcal{I}_{\geq q} \cap \Bbbk[x^1, \dots, x^D]$ exists. As $\mathcal{H}_q$ is a Pommaret basis of the ideal $\mathcal{I}_{\geq q}$, it must contain a polynomial h such that $\operatorname{le}_\prec h \mid_P \operatorname{le}_\prec f$; this implies $\operatorname{lt}_\prec h \in \Bbbk[x^d, \dots, x^D]$. Repeated applications of Lemma 2.4.2 to $\operatorname{le}_\prec h$ with $j = D$ yields that $\nu = q_D \in \operatorname{le}_\prec \mathcal{H}_q$. Further applications of Lemma 2.4.2 to ν with $k = D$ show that in fact any multi index of length q and class D is contained in $\operatorname{le}_\prec \mathcal{H}_q$. But thus already $\langle \mathcal{H}, x^1, \dots, x^{D-1}\rangle_q = \mathcal{P}_q$ in contradiction to the characterisation of D in Proposition 2.5.8. □

As our proof is solely based on an analysis of the leading terms, we showed in fact that $\{x^1, \dots, x^D\}$ is a *strongly* independent set modulo $\mathcal{I}$ and the term order $\prec$, i. e. that $\Bbbk[x^1, \dots, x^D] \cap \operatorname{lt}_\prec \mathcal{I} = \{0\}$ [15, Definition 9.22].

Proposition 2.5.10. *Let $\mathcal{H}$ be a Pommaret basis of the homogeneous ideal $\mathcal{I} \subseteq \mathcal{P}$ for the degree reverse lexicographic order and $d = \min_{h\in\mathcal{H}} \operatorname{cls} h$. The depth of $\mathcal{A} = \mathcal{P}/\mathcal{I}$ is $d-1$.*

Proof. We claim that $(x^1, \dots, x^{d-1})$ is a maximal $\mathcal{A}$-regular sequence. Let $f \in \mathcal{P}$ be an arbitrary polynomial. If $x^j f \in \mathcal{I}$ for an index $1 \leq j < d$, then we must have $f \in \mathcal{I}$, as no $h \in \mathcal{H}$ is divisible by x^j because of the condition on the classes. Indeed, in the involutive standard representation $x^j f = \sum_{h\in\mathcal{H}} P_h h$ all polynomials P_h must lie in $\langle x^j\rangle$ and dividing by x^j we obtain the standard representation of f. Hence none of the variables in $(x^1, \dots, x^{d-1})$ is a zero divisor for $\mathcal{A}$. The same argument shows that $x^j f \in \langle x^1, \dots, x^k\rangle\mathcal{I}$ for an index $k < j < d$ implies that $f \in \langle x^1, \dots, x^k\rangle\mathcal{I}$ and none of the variables in $(x^{k+1}, \dots, x^{d-1})$ is a zero divisor in $\mathcal{A}/\langle x^1, \dots, x^k\rangle\mathcal{A}$, as we may identify $\langle x^1, \dots, x^k\rangle\mathcal{A} \cong \langle x^1, \dots, x^k\rangle/\langle x^1, \dots, x^k\rangle\mathcal{I}$. Hence $(x^1, \dots, x^{d-1})$ is an $\mathcal{A}$-regular sequence.

Now we show that it is not possible to extend this sequence by any x^k with $k \geq d$. We identify $\mathcal{A}/\langle x^1, \dots, x^{d-1}\rangle\mathcal{A}$ with $\Bbbk[x^d, \dots, x^n]/\bar{\mathcal{I}}$ where the homogeneous ideal $\bar{\mathcal{I}} = \{f \in \Bbbk[x^d, \dots, x^n] \mid \exists g \in \langle x^1, \dots, x^{d-1}\rangle : f + g \in \mathcal{I}\}$ is isomorphic to $\mathcal{I}/\langle x^1, \dots, x^{d-1}\rangle$. If we drop in each element of $\mathcal{H}$ all terms contained in $\langle x^1, \dots, x^{d-1}\rangle$, we obtain a basis $\bar{\mathcal{H}}$ of $\bar{\mathcal{I}}$. As this operation does not affect the leading terms of the generators, $\bar{\mathcal{H}}$ is still a Pommaret basis.

Let $\bar{h}_d \in \bar{\mathcal{H}}$ be a polynomial of class d and of maximal degree among all generators of this class. As the degree reverse lexicographic order respects classes, it is of the form $\bar{h}_d = x^d\hat{h}_d$. It is not possible that $\hat{h}_d \in \bar{\mathcal{I}}$, as otherwise $\bar{\mathcal{H}}$ would not be involutively head autoreduced. Thus x^d is a zero divisor in $\mathcal{A}/\langle x^1, \dots, x^{d-1}\rangle\mathcal{A}$, as $x^d\hat{h}_d \in \bar{\mathcal{I}}$.

Now consider x^k with $k > d$. Obviously, it is a non-multiplicative variable for $\bar{h}_d$. Thus for each generator $\bar{h} \in \bar{\mathcal{H}}$ a polynomial $P_{\bar{h}} \in \Bbbk[x^d, \dots, x^{\operatorname{cls}\bar{h}}]$ exists such that $x^k\bar{h}_d = \sum_{\bar{h}\in\bar{\mathcal{H}}} P_{\bar{h}}\bar{h}$. As in the proof of Proposition 2.4.13, one easily deduces from the fact that the leading terms cannot cancel that $P_{\bar{h}} \in \langle x^d\rangle$ for all $\bar{h}$ with $\operatorname{cls}\bar{h} > d$. If $\operatorname{cls}\bar{h} = d$, then $P_{\bar{h}} \in \Bbbk[x^d]$. As $\bar{h}_d$ is of maximal degree among all generators of class d and $\bar{\mathcal{I}}$ is a homogeneous ideal, we must have $P_{\bar{h}} \in \langle x^d\rangle$, too. Thus we may divide by x^d and obtain $x^k\hat{h}_d = \sum_{\bar{h}\in\bar{\mathcal{H}}}(P_{\bar{h}}/x^d)\bar{h} \in \bar{\mathcal{I}}$. But this implies that x^k is a zero divisor in $\mathcal{A}/\langle x^1, \dots, x^{d-1}\rangle\mathcal{A}$.

Finally, assume that $y^1, \dots, y^d \in \mathcal{P}_1$ form an $\mathcal{A}$-regular sequence. We extend to a basis $\{y^1, \dots, y^n\}$ of $\mathcal{P}_1$ and perform a change of coordinates $\mathbf{x} \mapsto \mathbf{y}$. This transforms $\mathcal{H}$ into $\tilde{\mathcal{H}}$ and after an involutive head autoreduction we obtain the set $\tilde{\mathcal{H}}^{\triangle}$. Let $c = \min_{\tilde{h}\in\tilde{\mathcal{H}}^{\triangle}} \operatorname{cls}\tilde{h}$. One proves in the same manner as above that y^c is a zero divisor in $\mathcal{A}/\langle y^1, \dots, y^{c-1}\rangle\mathcal{A}$ and thus that $c > d$. This implies that the original coordinates $\mathbf{x}$ are not δ-regular for $\mathcal{H}$ contradicting Proposition 2.4.5. Hence $\operatorname{depth}\mathcal{A} = d-1$. □

As a trivial corollary we obtain that for any graded algebra $\mathcal{A} = \mathcal{P}/\mathcal{I}$ the inequality $\operatorname{depth}\mathcal{A} \leq \dim\mathcal{A}$ holds. In the limit case $\operatorname{depth}\mathcal{A} = \dim\mathcal{A}$, the algebra is by definition *Cohen–Macaulay*. Thus we obtain the following characterisation of algebras of this type.

Theorem 2.5.11. *Let $\mathcal{H}$ be a Pommaret basis of degree q of the homogeneous ideal $\mathcal{I} \subseteq \mathcal{P}$ with respect to the degree reverse lexicographic order and $d = \min_{h\in\mathcal{H}} \operatorname{cls} h$. The algebra $\mathcal{A} = \mathcal{P}/\mathcal{I}$ is Cohen–Macaulay, if and only if $\langle \mathcal{H}, x^1, \dots, x^{d-1}\rangle_q = \mathcal{P}_q$.*

Proof. By the results above, $\operatorname{depth}\mathcal{A} = \dim\mathcal{A} = d - 1$. □

Corollary 2.5.12 (Hironaka criterion). *$\mathcal{A} = \mathcal{P}/\mathcal{I}$ is a Cohen–Macaulay algebra, if and only if a Rees decomposition of $\mathcal{A}$ exists where all generators have the same class.*

Proof. One direction is trivial. If such a special decomposition exists with d the common class of all generators, then obviously both the dimension and the depth of $\mathcal{A}$ is d and thus $\mathcal{A}$ is Cohen–Macaulay.

For the converse, let us assume that $\mathcal{A}$ is Cohen–Macaulay and that $\dim\mathcal{A} = \operatorname{depth}\mathcal{A} = d$. Let $\mathcal{H}$ be a Pommaret basis of $\mathcal{I}$ with respect to the degree reverse lexicographic order. We will show later that in suitably chosen variables $\mathbf{x}$ such a basis always exists (Corollary 6.4.7). By our results above, this implies that $\min_{h\in\mathcal{H}} \operatorname{cls} h = d + 1$. We introduce the set $\bar{\mathcal{N}} = \{\nu \in \mathbb{N}_0^n \setminus \langle \operatorname{le}_\prec \mathcal{H}\rangle \mid \operatorname{cls}\nu > d\}$ (recall that by convention we defined $\operatorname{cls}[0,\dots,0] = n$ so that $[0,\dots,0] \in \bar{\mathcal{N}}$ whenever $\mathcal{I} \neq \mathcal{P}$). $\bar{\mathcal{N}}$ is finite, as all its elements satisfy $|\nu| < \deg\mathcal{H}$, and we claim that

$$\mathcal{A} \cong \bigoplus_{\nu\in\bar{\mathcal{N}}} \Bbbk[x^1,\dots,x^d]\cdot x^\nu\,. \tag{2.29}$$

In fact, (2.29) is just the decomposition obtained by applying the algorithm implicitly contained in the proof of Proposition 2.5.4. Consider an element $\nu \in \bar{\mathcal{N}}$; obviously, it is of the form $\nu = [0,\dots,0,\nu_{d+1},\dots,\nu_n]$ with $\sum_{i=d+1}^n \nu_i < q = \deg\mathcal{H}$. If we set $q' = q - \sum_{i=d+2}^n \nu_i$, then by Theorem 2.5.11 the multi index $[0,\dots,0,q',\nu_{d+2},\dots,\nu_n]$ lies in the monoid ideal $\langle \operatorname{le}_\prec\mathcal{H}\rangle$. But this implies the existence of a multi index $\nu' \in \operatorname{le}_\prec\mathcal{H}$ with $\nu' = [0,\dots,0,\nu'_{d+1},\nu_{d+2},\dots,\nu_n]$ with $\nu_{d+1} < \nu'_{d+1} \leq q'$. Hence the set $(\nu_{d+2},\dots,\nu_n)$ is considered in the assignment of multiplicative variables to the elements of $\mathcal{H}$ with respect to the Janet division and it consists only of the multi index ν', as $\mathcal{H}$ is involutively head autoreduced (with respect to the Pommaret division). But this implies that our algorithm chooses ν as an element of $\bar{\mathcal{N}}$ and assigns to it the multiplicative variables $x^1,\dots,x^d$.

The algorithm cannot lead to a larger set $\bar{\mathcal{N}}$, as any further multi index would be of class less than or equal to d and thus be contained in $\mathbb{k}[x^1, \dots, x^d] \cdot 1$. But we know that the sets are disjoint, so that this cannot happen and we get the decomposition (2.29). □

Example 2.5.13. Consider the ideal $\mathcal{I} = \langle z^3, yz^2 - xz^2, y^2 - xy \rangle \subset \mathbb{k}[x, y, z]$. A Pommaret basis of $\mathcal{I}$ for the degree reverse lexicographic order is given by $\mathcal{H} = \{z^3, yz^2 - xz^2, y^2z - xyz, y^2 - xy\}$ and thus both the depth and the dimension of $\mathcal{P}/\mathcal{I}$ is 1. Following the proof of Proposition 2.5.4 we obtain $\mathcal{T} = \{1, y, z, yz, z^2\}$ and the Hironaka decomposition is

$$\mathcal{P}/\mathcal{I} \cong \mathbb{k}[x] \oplus \mathbb{k}[x] \cdot y \oplus \mathbb{k}[x] \cdot z \oplus \mathbb{k}[x] \cdot yz \oplus \mathbb{k}[x] \cdot z^2 \,. \tag{2.30}$$

The term z^2 comes from the set $(2) = \{[0, 1, 2]\}$. The terms yz and z arise from $(1) = \{[0, 2, 1]\}$ and finally 1 and y stem from $(0) = \{[0, 2, 0]\}$. The set $(3) = \{[0, 0, 3]\}$ does not contribute to the decomposition. ◁

2.6 Applications II: Syzygies and Free Resolutions

Appendix B.3 shows that Gröbner bases are very useful in syzygy theory; the Schreyer Theorem B.3.3 gives us even directly a Gröbner basis of the first syzygy module. In this section we want to consider the use of involutive bases for this problem. In particular, Pommaret bases allow us to make statements about the whole syzygy resolution. We consider only the ordinary polynomial ring $\mathcal{P} = \mathbb{k}[x^1, \dots, x^n]$ and free modules $\mathcal{P}^m$ over it.

In this section we cannot avoid the explicit use of modules and we use the vector notation introduced in the Appendices B.2 and B.3. Let $\mathcal{H} \subset \mathcal{P}^m$ be a finite set, $\prec$ a term order on $\mathbb{T}_m$ and L an involutive division on $\mathbb{N}_0^n$. We divide $\mathcal{H}$ into m disjoint sets $\mathcal{H}_\alpha = \{\mathbf{h} \in \mathcal{H} \mid \mathrm{lt}_\prec \mathbf{h} = t\boldsymbol{e}_\alpha,\ t \in \mathbb{T}\}$. This leads naturally to m sets $\mathcal{N}_\alpha = \{\mu \in \mathbb{N}_0^n \mid x^\mu \boldsymbol{e}_\alpha \in \mathrm{lt}_\prec \mathcal{H}_\alpha\}$. If $\mathbf{h} \in \mathcal{H}_\alpha$, we assign the multiplicative variables $X_{L,\mathcal{H},\prec}(\mathbf{h}) = \{x^i \mid i \in N_{L,\mathcal{N}_\alpha}(\mathrm{le}_\prec \mathbf{h})\}$. The involutive span $\langle \mathcal{H} \rangle_{L,\prec}$ is defined by an obvious generalisation of (2.16).

Let $\mathcal{M} \subseteq \mathcal{P}^m$ be a submodule and $\mathcal{H}$ an involutive basis of $\mathcal{M}$, i.e. $\langle \mathcal{H} \rangle_L = \mathcal{M}$ and $\mathcal{H}$ is involutively head autoreduced. Take an arbitrary element $\mathbf{h}_\alpha \in \mathcal{H}$ and choose a non-multiplicative variable $x^k \in \bar{X}_{L,\mathcal{H},\prec}(\mathbf{h}_\alpha)$. By Proposition 2.3.10, we can determine for each $\mathbf{h}_\beta \in \mathcal{H}$ with an involutive normal form algorithm a unique polynomial $P_\beta^{(\alpha;k)} \in \mathbb{k}[X_{L,\mathcal{H},\prec}(\mathbf{h}_\beta)]$ such that $x^k \mathbf{h}_\alpha = \sum_{\beta=1}^s P_\beta^{(\alpha;k)} \mathbf{h}_\beta$. The corresponding syzygy is

$$\mathbf{S}_{\alpha;k} = x^k \boldsymbol{e}_\alpha - \sum_{\beta=1}^s P_\beta^{(\alpha;k)} \boldsymbol{e}_\beta \in \mathcal{P}^s \,. \tag{2.31}$$

We claim now that the set of all these syzygies $\mathbf{S}_{\alpha;k}$ generates the syzygy module $\mathrm{Syz}(\mathcal{H})$. Before the proof, we need a simple technical lemma.

Lemma 2.6.1. *Let* $\mathbf{S} = \sum_{\beta=1}^{s} S_\beta \boldsymbol{e}_\beta$ *be an arbitrary syzygy in* $\mathrm{Syz}(\mathcal{H})$. *Then* $S_\beta \in \mathbb{k}[X_{L,\mathcal{H},\prec}(\mathbf{h}_\beta)]$ *for all* $1 \le \beta \le s$, *if and only if* $\mathbf{S} = 0$.

Proof. By definition of a syzygy, $\sum_{\beta=1}^{s} S_\beta \mathbf{h}_\beta = 0$. As $\mathcal{H}$ is involutively head autoreduced, each element $\mathbf{f} \in \langle\mathcal{H}\rangle$ possesses a unique involutive normal form by Proposition 2.3.7. In particular, this holds for $0 \in \langle\mathcal{H}\rangle$. Thus either $S_\beta \notin \mathbb{k}[X_{L,\mathcal{H},\prec}(\mathbf{h}_\beta)]$ for at least one β or $\mathbf{S} = 0$. $\square$

We recall from Appendix B.3 the definition of the term order $\prec_{\mathcal{F}}$ on $\mathbb{T}_s$ induced by an arbitrary finite set $\mathcal{F} = \{\mathbf{f}_1, \dots, \mathbf{f}_s\} \subset \mathcal{P}^m$ and an arbitrary term order $\prec$ on $\mathbb{T}_m$. Given two terms $\mathbf{s} = s\boldsymbol{e}_\sigma$ and $\mathbf{t} = t\boldsymbol{e}_\tau$, we set $\mathbf{s} \prec_{\mathcal{F}} \mathbf{t}$, if either $\mathrm{lt}_\prec(s\mathbf{f}_\sigma) \prec \mathrm{lt}_\prec(t\mathbf{f}_\tau)$ or $\mathrm{lt}_\prec(s\mathbf{f}_\sigma) = \mathrm{lt}_\prec(t\mathbf{f}_\tau)$ and $\tau < \sigma$.

Proposition 2.6.2. *The set* $\mathcal{H}_{\mathrm{Syz}} = \{\mathbf{S}_{\alpha;k} \mid 1 \le \alpha \le s;\ x^k \in \bar{X}_{L,\mathcal{H},\prec}(\mathbf{h}_\alpha)\}$ *is a generating set of the syzygy module* $\mathrm{Syz}(\mathcal{H})$.

Proof. This result is a simple corollary to Schreyer's Theorem and Buchberger's second criterion in the form of Lemma B.3.4. Without loss of generality, we assume that $\mathcal{H}$ is a monic basis, i. e. all leading coefficients are 1. Let $\mathbf{S}_{\alpha;k} \in \mathcal{H}_{\mathrm{Syz}}$. By Proposition 2.3.10 the polynomials $P_\beta^{(\alpha;k)}$ in (2.31) satisfy $\mathrm{lt}_\prec(P_\beta^{(\alpha;k)}\mathbf{h}_\beta) \preceq \mathrm{lt}_\prec(x^k\mathbf{h}_\alpha)$. By Lemma 2.3.6 there exists one and only one index $\bar\beta$ such that $\mathrm{lt}_\prec(P_{\bar\beta}^{(\alpha;k)}\mathbf{h}_{\bar\beta}) = \mathrm{lt}_\prec(x^k\mathbf{h}_\alpha)$.

Set $\mathbf{t}_\alpha = \mathrm{lt}_\prec\mathbf{h}_\alpha$ and $\mathbf{t}_{\alpha\beta} = \mathrm{lcm}(\mathbf{t}_\alpha, \mathbf{t}_\beta)$. As an involutive basis is simultaneously a Gröbner basis, we may write all S-polynomials in the form $\mathbf{S}_\prec(\mathbf{h}_\alpha, \mathbf{h}_\beta) = \sum_{\gamma=1}^{s} f_{\alpha\beta\gamma}\mathbf{h}_\gamma$ with some polynomials $f_{\alpha\beta\gamma} \in \mathcal{P}$. In particular, we can choose these polynomials such that $\mathrm{lt}_\prec\bigl(\mathbf{S}_\prec(\mathbf{h}_\alpha, \mathbf{h}_\beta)\bigr) \succeq \mathrm{lt}_\prec(f_{\alpha\beta\gamma}\mathbf{h}_\gamma)$ for $1 \le \gamma \le s$. As in Appendix B.3, we introduce for $\alpha \ne \beta$ the syzygies

$$\mathbf{S}_{\alpha\beta} = \frac{\mathbf{t}_{\alpha\beta}}{\mathbf{t}_\alpha}\boldsymbol{e}_\alpha - \frac{\mathbf{t}_{\alpha\beta}}{\mathbf{t}_\beta}\boldsymbol{e}_\beta - \mathbf{f}_{\alpha\beta}\ . \tag{2.32}$$

The set $\mathcal{H}_{\mathrm{Schreyer}} = \{\mathbf{S}_{\alpha\beta} \mid 1 \le \alpha < \beta \le s\}$ of all these syzygies generates the syzygy module $\mathrm{Syz}(\mathcal{H})$ by the Schreyer Theorem B.3.3. It is easy to see that $\mathbf{S}_{\alpha;k} = \mathbf{S}_{\alpha\bar\beta}$. Thus $\mathcal{H}_{\mathrm{Syz}} \subseteq \mathcal{H}_{\mathrm{Schreyer}}$.

Let $\mathbf{S}_{\alpha\beta} \in \mathcal{H}_{\mathrm{Schreyer}} \setminus \mathcal{H}_{\mathrm{Syz}}$ be an arbitrary syzygy. We prove first that $\mathcal{H}_{\mathrm{Schreyer}} \setminus \{\mathbf{S}_{\alpha\beta}\}$ is still a generating set of $\mathrm{Syz}(\mathcal{H})$. Any syzygy in $\mathcal{H}_{\mathrm{Schreyer}}$ has the form $\mathbf{S}_{\alpha\beta} = x^\mu\boldsymbol{e}_\alpha - x^\nu\boldsymbol{e}_\beta + \mathbf{R}_{\alpha\beta}$. By construction, one of the monomials x^μ and x^ν must contain a non-multiplicative variable x^k for $\mathbf{h}_\alpha$ or $\mathbf{h}_\beta$, respectively. Without loss of generality, we assume that $x^k \in \bar{X}_{L,\mathcal{H},\prec}(\mathbf{h}_\alpha)$ and $\mu_k > 0$. This implies that $\mathcal{H}_{\mathrm{Syz}}$ contains the syzygy $\mathbf{S}_{\alpha;k}$. As shown above, a unique index $\gamma \ne \beta$ exists such that $\mathbf{S}_{\alpha;k} = \mathbf{S}_{\alpha\gamma}$.

Let $\mathbf{S}_{\alpha\gamma} = x^k \mathbf{e}_\alpha - x^\rho \mathbf{e}_\gamma + \mathbf{R}_{\alpha\gamma}$. By construction, $x^\rho \mathbf{t}_\gamma = x^k \mathbf{t}_\alpha$ divides $x^\mu \mathbf{t}_\alpha = \mathbf{t}_{\alpha\beta}$. Thus $\mathbf{t}_\gamma \mid \mathbf{t}_{\alpha\beta}$ and by Lemma B.3.4 the set $\mathcal{H}_{\text{Schreyer}} \setminus \{\mathbf{S}_{\alpha\beta}\}$ still generates $\operatorname{Syz}(\mathcal{H})$. If we try to iterate this argument, we encounter the following problem. In order to be able to eliminate $\mathbf{S}_{\alpha\beta}$ we need both $\mathbf{S}_{\alpha\gamma}$ and $\mathbf{S}_{\beta\gamma}$ in the remaining set. For $\mathbf{S}_{\alpha\gamma} \in \mathcal{H}_{\text{Syz}}$, this is always guaranteed. But we know nothing about $\mathbf{S}_{\beta\gamma}$ and, if it is not an element of $\mathcal{H}_{\text{Syz}}$, it could have been removed in an earlier iteration.

We claim that with respect to the term order $\prec_{\mathcal{H}}$ the term $\operatorname{lt}_{\prec_{\mathcal{H}}} \mathbf{S}_{\alpha\beta}$ is greater than both $\operatorname{lt}_{\prec_{\mathcal{H}}} \mathbf{S}_{\alpha\gamma}$ and $\operatorname{lt}_{\prec_{\mathcal{H}}} \mathbf{S}_{\beta\gamma}$. Without loss of generality, we may assume for simplicity that $\alpha < \beta < \gamma$, as the syzygies $\mathbf{S}_{\alpha\beta}$ and $\mathbf{S}_{\beta\alpha}$ differ only by a sign. Thus $\operatorname{lt}_{\prec_{\mathcal{H}}} \mathbf{S}_{\alpha\beta} = \frac{\mathbf{t}_{\alpha\beta}}{\mathbf{t}_\alpha} \mathbf{e}_\alpha$ and similarly for $\mathbf{S}_{\alpha\gamma}$ and $\mathbf{S}_{\beta\gamma}$. Furthermore, $\mathbf{t}_\gamma \mid \mathbf{t}_{\alpha\beta}$ trivially implies $\mathbf{t}_{\alpha\gamma} \mid \mathbf{t}_{\alpha\beta}$ and hence $\mathbf{t}_{\alpha\gamma} \prec \mathbf{t}_{\alpha\beta}$ for any term order $\prec$. Obviously, the same holds for $\mathbf{t}_{\beta\gamma}$. Now a straightforward application of the definition of the term order $\prec_{\mathcal{H}}$ proves our claim.

Thus if we always remove a syzygy $\mathbf{S}_{\alpha\beta} \in \mathcal{H}_{\text{Schreyer}} \setminus \mathcal{H}_{\text{Syz}}$ whose leading term is maximal with respect to the term order $\prec_{\mathcal{H}}$, it can never happen that the syzygy $\mathbf{S}_{\beta\gamma}$ required for the application of Lemma B.3.4 has already been eliminated earlier and $\mathcal{H}_{\text{Syz}}$ is indeed a generating set of $\operatorname{Syz}(\mathcal{H})$. □

This result is weaker than Schreyer's Theorem, as it only yields a generating set of the syzygy module and not a Gröbner basis for it. However, if $\mathcal{H}$ is not any involutive basis but a Pommaret basis, then $\mathcal{H}_{\text{Syz}}$ is again a Pommaret basis for $\operatorname{Syz}(\mathcal{H})$ with respect to $\prec_{\mathcal{H}}$.

Theorem 2.6.3. *Let $\mathcal{H}$ be a Pommaret basis of $\mathcal{M}$. If we order its elements according to their class, i. e. if we assume that $\operatorname{cls} \mathbf{h}_\alpha < \operatorname{cls} \mathbf{h}_\beta$ implies $\alpha < \beta$, then $\mathcal{H}_{\text{Syz}}$ is a Pommaret basis of $\operatorname{Syz}(\mathcal{H})$ with respect to the term order $\prec_{\mathcal{H}}$.*

Proof. Our ordering of $\mathcal{H}$ implies that $\operatorname{lt}_{\prec_{\mathcal{H}}} \mathbf{S}_{\alpha;k} = x^k \mathbf{e}_\alpha$. Indeed, as mentioned above $\operatorname{lt}_\prec(P_\beta^{(\alpha;k)} \mathbf{h}_\beta) \preceq \operatorname{lt}_\prec(x^k \mathbf{h}_\alpha)$ for all β and only one index $\bar\beta$ exists with $\operatorname{lt}_\prec(P_{\bar\beta}^{(\alpha;k)} \mathbf{h}_{\bar\beta}) = \operatorname{lt}_\prec(x^k \mathbf{h}_\alpha)$. But as $P_{\bar\beta}^{(\alpha;k)} \in \Bbbk[X_{P,\prec}(\mathbf{h}_{\bar\beta})]$ this equality implies that $\operatorname{cls} \mathbf{h}_{\bar\beta} > \operatorname{cls} \mathbf{h}_\alpha$. Hence $\bar\beta > \alpha$ and according to the definition of the term order $\prec_{\mathcal{H}}$ we find $\operatorname{lt}_{\prec_{\mathcal{H}}} \mathbf{S}_{\alpha;k} = x^k \mathbf{e}_\alpha$.

In order to show that $\mathcal{H}_{\text{Syz}}$ is a Pommaret basis, we must express every non-multiplicative product $x^\ell \mathbf{S}_{\alpha;k}$ with $\ell > k$ as a linear combination of multiplicative products. As x^ℓ is obviously non-multiplicative for $\mathbf{h}_\alpha$, the set $\mathcal{H}_{\text{Syz}}$ also contains the syzygy $\mathbf{S}_{\alpha;\ell}$ and x^k is multiplicative for it. Let us study the difference

$$x^\ell \mathbf{S}_{\alpha;k} - x^k \mathbf{S}_{\alpha;\ell} = \sum_{\beta=1}^{s} \left(x^\ell P_\beta^{(\alpha;k)} - x^k P_\beta^{(\alpha;\ell)} \right) \mathbf{e}_\beta \ . \tag{2.33}$$

If all coefficients on the right hand side are multiplicative, we know by Lemma 2.6.1 that it must actually be zero and we are done.

While the polynomials $P_\beta^{(\alpha;k)}$ and $P_\beta^{(\alpha;\ell)}$ depend only on multiplicative variables, it is possible that either x^ℓ or x^k is non-multiplicative for one or more $\mathbf{h}_\beta$ where $P_\beta^{(\alpha;k)}$ or $P_\beta^{(\alpha;\ell)}$, respectively, is not zero. If this is the case, we choose the pair (β, k) or (β, ℓ) for that $\mathrm{lt}_{\prec_{\mathcal{H}}}(x^\ell P_\beta^{(\alpha;k)} \boldsymbol{e}_\beta)$ (or $\mathrm{lt}_{\prec_{\mathcal{H}}}(x^k P_\beta^{(\alpha;\ell)} \boldsymbol{e}_\beta)$, respectively) is maximal with respect to $\prec_{\mathcal{H}}$. Without loss of generality we assume that this pair is of the form (β, k); the following argument remains true for pairs of the form (β, ℓ).

As x^k is assumed to be non-multiplicative for $\mathbf{h}_\beta$, the set $\mathcal{H}_{\mathbf{Syz}}$ contains the syzygy $\mathbf{S}_{\beta;k}$ and we can eliminate $\mathrm{lt}_{\prec_{\mathcal{H}}}(x^k P_\beta^{(\alpha;\ell)} \boldsymbol{e}_\beta)$ by subtracting $P_\beta^{(\alpha;\ell)} \mathbf{S}_{\beta;k}$. Note that the polynomial $P_\beta^{(\alpha;\ell)}$ depends only on variables x^i with $i \leq \mathrm{cls}\, \mathbf{h}_\beta$. By assumption $\mathrm{cls}\, \mathbf{h}_\beta < k$; hence this is a multiplicative product. All terms introduced by this operation are less than $\mathrm{lt}_{\prec_{\mathcal{H}}}(x^k P_\beta^{(\alpha;\ell)} \boldsymbol{e}_\beta)$. It follows that continuing this way we can eliminate all terms with non-multiplicative coefficients in a finite number of steps. As soon as this has happened, it follows from Lemma 2.6.1 that the remainder is zero and we have expressed $x^\ell \mathbf{S}_{\alpha;k}$ as a linear combination of multiplicative products. □

Note that this proof makes extensive use of the definition of the Pommaret division and cannot easily be extended to other divisions. In particular, it is decisive that we can trivially determine first the leading terms and then the multiplicative variables of each syzygy $\mathbf{S}_{\alpha;k}$. As a simple corollary we obtain the following stronger version of Hilbert's Syzygy Theorem B.3.6.

Corollary 2.6.4. *Let $\mathcal{H}$ be a Pommaret basis of the polynomial module $\mathcal{M}$. Denote by $\beta_0^{(k)}$ the number of generators $\mathbf{h} \in \mathcal{H}$ such that $\mathrm{cls}\, \mathrm{le}_\prec \mathbf{h} = k$ and set $d = \min\{k \mid \beta_0^{(k)} > 0\}$. Then $\mathcal{M}$ possesses a free resolution*

$$0 \longrightarrow \mathcal{P}^{t_{n-d}} \longrightarrow \cdots \longrightarrow \mathcal{P}^{t_1} \longrightarrow \mathcal{M} \longrightarrow 0 \tag{2.34}$$

where the ranks of the free modules are given by

$$t_i = \sum_{k=1}^{n-i} \binom{n-k}{i} \beta_0^{(k)} \,. \tag{2.35}$$

Proof. By Theorem 2.6.3, $\mathcal{H}_{\mathbf{Syz}}$ is a Pommaret basis of $\mathrm{Syz}(\mathcal{H})$. Applying Theorem 2.6.3 again, we can construct a Pommaret basis of the second syzygy module $\mathrm{Syz}^2(\mathcal{H})$ and so on. It follows from the definition (2.31) of the generators $\mathbf{S}_{\alpha;k}$ that $\mathrm{cls}\, \mathbf{S}_{\alpha;k} = k > \mathrm{cls}\, \mathbf{h}_\alpha$. If d is the minimal class appearing in $\mathcal{H}$, the minimal class in $\mathcal{H}_{\mathbf{Syz}}$ is $d+1$. This yields the length of the resolution (2.34), as a Pommaret basis with $d = n$ generates a free module.

The ranks of the modules follow from a rather straightforward combinatorial calculation. Let $\beta_i^{(k)}$ denote the number of generators of class k of the ith syzygy module $\mathrm{Syz}^i(\mathcal{H})$. By definition of the generators $\mathbf{S}_{\alpha;k}$, we find $\beta_i^{(k)} = \sum_{j=1}^{k-1} \beta_{i-1}^{(j)}$, as each generator of class less than k in the Pommaret basis of $\mathrm{Syz}^{i-1}(\mathcal{H})$ contributes one generator of class k in the basis of $\mathrm{Syz}^i(\mathcal{H})$. A simple induction allows us to express the $\beta_i^{(k)}$ in terms of the $\beta_0^{(k)}$:

$$\beta_i^{(k)} = \sum_{j=1}^{k-i} \binom{k-j-1}{i-1} \beta_0^{(j)} . \tag{2.36}$$

The ranks of the modules in (2.34) are given by $t_i = \sum_{k=1}^{n} \beta_i^{(k)}$; entering (2.36) yields via a classical identity for binomial coefficients (2.35). □

A natural question is when the resolution (2.34) is *minimal* in the sense of Definition B.3.7, as in this case t_i are the Betti numbers of the module $\mathcal{M}$. In general, (2.34) is not minimal, as the generators $\mathbf{S}_{\alpha;k}$ may contain constant coefficients. But (2.34) is at least a resolution of minimal length, i. e. $\operatorname{proj\,dim} \mathcal{M} = n - d$. Indeed, by Proposition 2.4.13, $\operatorname{depth} \mathcal{M} = d$ and the Auslander–Buchsbaum formula (graded form [47, Exercise 19.8]) for a $\mathcal{P}$-module asserts that $\operatorname{proj\,dim} \mathcal{M} + \operatorname{depth} \mathcal{M} = n$.

In the case of monomial modules, Eliahou and Kervaire [49] identified a class of modules for which (2.34) is a minimal resolution: stable modules. Their result is readily derived using Pommaret bases; in fact, implicitly they used such bases.

Definition 2.6.5. *A (possibly infinite) set $\mathcal{N} \subseteq \mathbb{N}_0^n$ is* stable*, if for each multi index $\nu \in \mathcal{N}$ all multi indices $\nu - 1_k + 1_j$ with $k = \operatorname{cls} \nu < j \leq n$ are also elements of $\mathcal{N}$. A monomial submodule $\mathcal{M} \subseteq \mathcal{P}^m$ is called* stable*, if each of the sets $\mathcal{N}_\alpha = \{\mu \mid x^\mu \mathbf{e}_\alpha \in \mathcal{M}\} \subset \mathbb{N}_0^n$ with $1 \leq \alpha \leq m$ is stable.*

Any monomial submodule has a unique minimal basis. For stable submodules it must coincide with its Pommaret basis. This represents a very simple and effective characterisation of stable submodules.

Proposition 2.6.6. *Let $\mathcal{M} \subseteq \mathcal{P}^m$ be a monomial submodule. $\mathcal{M}$ is stable, if and only if its minimal basis $\mathcal{H}$ is also a Pommaret basis.*

Proof. Let us assume first that $\mathcal{M}$ is stable; we have to show that $\langle \mathcal{H} \rangle_P = \mathcal{M}$. For every term $\mathbf{s} \in \mathcal{M}$ a unique term $\mathbf{t}_1 \in \mathcal{H}$ exists such that $\mathbf{s} = s_1 \mathbf{t}_1$ for some term $s_1 \in \mathbb{T}$. If $s_1 \in \mathbb{k}[X_P(\mathbf{t}_1)]$, we are done. Otherwise there exists an index $j > k = \operatorname{cls} \mathbf{t}_1$ such that $x^j \mid s_1$ and we rewrite

$$\mathbf{s} = \left(\frac{x^k}{x^j} s_1\right) \left(\frac{x^j}{x^k} \mathbf{t}_1\right) . \tag{2.37}$$

Since, by assumption, $\mathcal{M}$ is stable, $(x^j/x^k)\mathbf{t}_1 \in \mathcal{M}$. Thus a term $\mathbf{t}_2 \in \mathcal{H}$ exists such that $(x^j/x^k)\mathbf{t}_1 = s_2\mathbf{t}_2$ for some term $s_2 \in \mathbb{T}$. We are done, if $\mathbf{t}_2 \mid_P \mathbf{s}$. Otherwise we iterate this construction. By the continuity of the Pommaret division, this cannot go on infinitely, i. e. after a finite number of steps we must reach a term $\mathbf{t}_N \in \mathcal{H}$ such that $\mathbf{t}_N \mid_P \mathbf{s}$ and thus $\mathbf{s} \in \langle\mathcal{H}\rangle_P$.

For the converse, assume that the minimal basis $\mathcal{H}$ is a Pommaret basis. Then a unique $\mathbf{t} \in \mathcal{H}$ exists for each $\mathbf{s} \in \mathcal{M}$ such that $\mathbf{t} \mid_P \mathbf{s}$. We must show that with $k = \operatorname{cls}\mathbf{s} \leq \operatorname{cls}\mathbf{t}$ for all $i > k$ the terms $(x^i/x^k)\mathbf{s}$ are also elements of $\mathcal{M}$. We distinguish two cases. If $\mathbf{s} = \mathbf{t}$, a $\bar{\mathbf{t}} \in \mathcal{H}$ exists with $\bar{\mathbf{t}} \mid_P (x^i\mathbf{t})$. As $\mathcal{H}$ is a minimal basis, it cannot be that $\bar{\mathbf{t}} = x^i\mathbf{t}$. Instead we must have that $\bar{\mathbf{t}} \mid (x^i/x^k)\mathbf{t} = (x^i/x^k)\mathbf{s}$ and we are done. If $\mathbf{s} \neq \mathbf{t}$, we write $\mathbf{s} = s\mathbf{t}$ with $s \in \mathbb{T}$. If $k < \operatorname{cls}\mathbf{t}$, then $x^k \mid s$ which implies that we can divide by x^k and thus $(x^i/x^k)\mathbf{s} \in \mathcal{M}$. Otherwise, $\operatorname{cls}\mathbf{s} = \operatorname{cls}\mathbf{t}$ and we know from the first case that $(x^i/x^k)\mathbf{t} \in \mathcal{M}$. But $(x^i/x^k)\mathbf{s} = (x^i/x^k)s\mathbf{t}$. □

Example 2.6.7. It follows from Lemma 2.4.2, that if $\mathcal{H}$ is a Pommaret basis of the submodule $\mathcal{M} \subseteq \mathcal{P}^m$ of degree q, then $(\operatorname{lt}_{\prec}\mathcal{M})_{\geq q}$ is a stable monomial submodule, as $\operatorname{lt}_{\prec}\mathcal{H}_q$ is obviously its minimal basis and simultaneously a Pommaret basis. ◁

Theorem 2.6.8. *Let $\mathcal{M} \subseteq \mathcal{P}^m$ be a monomial module. Then the syzygy resolution* (2.34) *is minimal, if and only if $\mathcal{M}$ is stable.*

Proof. The proof is rather simple but notationally messy. We denote the elements of the Pommaret basis of $\operatorname{Syz}^i(\mathcal{H})$ by $\mathbf{S}_{\alpha;k_1,\dots,k_i}$ where the inequalities $k_i > \cdots > k_1 > \operatorname{cls}\mathbf{h}_\alpha$ hold. Similarly, we denote the standard basis of the free module $\mathcal{P}^{t_i}$ by $\mathbf{e}_{\alpha;k_1,\dots,k_{i-1}}$ with the same inequalities for the indices. The ith syzygies have the form

$$\mathbf{S}_{\alpha;k_1,\dots,k_i} = x^{k_i}\mathbf{e}_{\alpha;k_1,\dots,k_{i-1}} - \sum P^{(\alpha;k_1,\dots,k_i)}_{\beta;\ell_1,\dots,\ell_{i-1}}\mathbf{e}_{\beta;\ell_1,\dots,\ell_{i-1}} \tag{2.38}$$

with polynomials $P^{(\alpha;k_1,\dots,k_i)}_{\beta;\ell_1,\dots,\ell_{i-1}} \in \mathbb{k}[x^1,\dots,x^{\ell_{i-1}}]$ and where the summation is over all $1 \leq \beta \leq p$ and $\ell_{i-1} > \cdots > \ell_1 > \operatorname{cls}\mathbf{h}_\beta$. By definition, the resolution is minimal, if and only if all polynomials $P^{(\alpha;k_1,\dots,k_i)}_{\beta;\ell_1,\dots,\ell_{i-1}}$ are elements of the ideal $\mathcal{P}_+ = \langle x^1,\dots,x^n\rangle$.

We proceed by an induction over the resolution. If $\mathcal{M}$ is stable, by Proposition 2.6.6 the Pommaret basis $\mathcal{H}$ is the minimal basis of $\mathcal{M}$. To each element $\mathbf{h}_\alpha \in \mathcal{H}$ and each non-multiplicative index $k > \operatorname{cls}\mathbf{h}_\alpha$ there exists precisely one $\mathbf{h}_\beta \in \mathcal{H}$ such that $x^k\mathbf{h}_\alpha = m\mathbf{h}_\beta$ where the term $m \in \mathbb{T}$ contains only multiplicative variables of $\mathbf{h}_\beta$. As $\mathcal{H}$ is the minimal basis of $\mathcal{M}$, it is not possible that $m = 1$, as otherwise $\mathbf{h}_\alpha \mid \mathbf{h}_\beta$. This proves our claim for the case $i = 1$, as $P^{(\alpha;k)}_\beta \in \mathcal{P}_+$ for all possible values of α, β and k.

Assume now that $P^{(\alpha;k_1,\dots,k_i)}_{\beta;\ell_1,\dots,\ell_{i-1}} \in \mathcal{P}_+$ for all possible values of the indices. For the induction we must show that all coefficients $P^{(\alpha;k_1,\dots,k_{i+1})}_{\beta;\ell_1,\dots,\ell_i} \in \mathcal{P}_+$. For this purpose, we rewrite

$$\begin{aligned} x^{k_{i+1}} \mathbf{S}_{\alpha;k_1,\dots,k_i} = x^{k_i}(x^{k_{i+1}} \mathbf{e}_{\alpha;k_1,\dots,k_{i-1}}) - \\ \sum P^{(\alpha;k_1,\dots,k_i)}_{\beta;\ell_1,\dots,\ell_{i-1}}(x^{k_{i+1}} \mathbf{e}_{\beta;\ell_1,\dots,\ell_{i-1}}) \end{aligned} \tag{2.39}$$

and proceed as in the proof of Theorem 2.6.3: we compute a normal form with respect to the Pommaret basis of $\mathrm{Syz}^{i+1}(\mathcal{H})$. We solve each syzygy (2.38) for its initial term, the first term on the right hand side, and substitute the result in (2.39) whenever there is a non-multiplicative product of a basis vector $\mathbf{e}_{\beta;\ell_1,\dots,\ell_{i-1}}$. As all $P^{(\alpha;k_1,\dots,k_i)}_{\beta;\ell_1,\dots,\ell_{i-1}}$ lie in $\mathcal{P}_+$, such a substitution can never decrease the degree of a coefficient. Thus $P^{(\alpha;k_1,\dots,k_{i+1})}_{\beta;\ell_1,\dots,\ell_i} \in \mathcal{P}_+$ for all possible values of the indices.

This proves that for a stable module the resolution (2.34) is minimal. Assume that $\mathcal{M}$ is not stable. By Proposition 2.6.6 the Pommaret basis $\mathcal{H}$ cannot be the minimal basis. In this case, $\mathcal{H}$ contains elements $\mathbf{h}_\alpha$, $\mathbf{h}_\beta$ with $\mathbf{h}_\beta = x^k \mathbf{h}_\alpha$ for some $x^k \in \bar{X}_P(\mathbf{h}_\alpha)$. So the syzygy $\mathbf{S}_{\alpha;k} = x^k \mathbf{e}_\alpha - \mathbf{e}_\beta$ contains a constant coefficient and the resolution is not minimal. □

We return to the general, polynomial, case but restrict for notational simplicity again to ideals instead of submodules. In many situations it is of interest to obtain an estimate on the degree of an ideal basis, in particular for the complexity analysis of completion algorithms. Up to date, no simple answer is known to this question. Somewhat surprisingly, the stronger problem of bounding not only the degree of a basis of $\mathcal{I}$ but also of its syzygies can be treated effectively.

Definition 2.6.9. *Let $\mathcal{I} \subseteq \mathcal{P}$ be a homogeneous ideal. $\mathcal{I}$ is* q-regular*, if the jth syzygy module is generated by elements of degree less than or equal to $q + j$. The* Castelnuovo–Mumford regularity $\operatorname{reg}\mathcal{I}$ *of the ideal $\mathcal{I}$ is the least q for which $\mathcal{I}$ is q-regular.*

We show in the remainder of this section that $\operatorname{reg}\mathcal{I}$ can be trivially read off a Pommaret basis of $\mathcal{I}$. Our basic tool is the following theorem combining results from Bayer and Stillman [14] and Eisenbud and Goto [48], respectively. These works also contain proofs of it.

Theorem 2.6.10. *The following statements are equivalent.*

(i) *The homogeneous module $\mathcal{I} \subseteq \mathcal{P}$ is q-regular.*
(ii) *The truncation $\mathcal{I}_{\geq q}$ admits a linear free resolution, i. e. $\mathcal{I}_{\geq q}$ is generated by elements of degree q and all maps in the resolution are linear.*

(iii) *For some* $0 \leq d \leq n$ *elements* $y^1, \dots, y^d \in \mathcal{P}_1$ *exist such that*

$$\big(\langle \mathcal{I}, y^1, \dots, y^{j-1}\rangle : y^j\big)_q = \big(\langle \mathcal{I}, y^1, \dots, y^{j-1}\rangle\big)_q\ , \quad 1 \leq j \leq d\ , \tag{2.40a}$$

$$\big(\langle \mathcal{I}, y^1, \dots, y^d\rangle\big)_q = \mathcal{P}_q\ . \tag{2.40b}$$

Recall that the truncation is defined by $\mathcal{I}_{\geq q} = \bigoplus_{p \geq q} \mathcal{I}_p$. The notation $\mathcal{I} : g$ refers to the quotient of the ideal $\mathcal{I}$ by the principal ideal generated by $g \in \mathcal{P}$, i. e. $\mathcal{I} : g = \{f \in \mathcal{P} \mid gf \in \mathcal{I}\}$.

Theorem 2.6.11. *Let* $\mathcal{I} \subseteq \mathcal{P}$ *be a homogeneous ideal. The Castelnuovo–Mumford regularity of* $\mathcal{I}$ *is* q*, if and only if* $\mathcal{I}$ *has (in suitable coordinates) a Pommaret basis of degree* q *with respect to the degree reverse lexicographic order.*

Proof. One direction is trivial. If $\mathcal{I}$ has a Pommaret basis $\mathcal{H}$ of degree q, then the set $\mathcal{H}_q$ defined by (2.18) is a Pommaret basis of the truncation $\mathcal{I}_{\geq q}$ according to Lemma 2.4.1. Now it follows easily from Theorem 2.6.3 that $\mathcal{I}_{\geq q}$ possesses a linear free resolution, as all syzygies of $\mathcal{H}_q$ are homogeneous of degree 1. Thus the ideal $\mathcal{I}$ is q-regular by Part (ii) of Theorem 2.6.10.

For the converse we apply Part (iii) of Theorem 2.6.10. We use coordinates x such that $x^i = y^i$ for $1 \leq i \leq d$. By Part (ii) of Theorem 2.6.10, $\mathcal{I}_{\geq q}$ can be generated by elements of degree q. Let $\mathcal{H}_q$ be a basis of $\mathcal{I}_q$ as a vector space in triangular form, i. e. $\operatorname{lt}_\prec h_1 \neq \operatorname{lt}_\prec h_2$ for all $h_1, h_2 \in \mathcal{H}_q$. We claim that $\mathcal{H}_q$ is a Pommaret basis of $\mathcal{I}_{\geq q}$.

Let us write $\mathcal{H}_q = \{h_{k,\ell} \mid 1 \leq k \leq n,\ 1 \leq \ell \leq \ell_k\}$ where $\operatorname{cls} h_{k,\ell} = k$. This implies that a minimal basis of the ideal $\langle \mathcal{I}_{\geq q}, x^1, \dots, x^j\rangle$ is given by $\{h \in \mathcal{H}_q \mid \operatorname{cls} h > j\} \cup \{x^1, \dots, x^j\}$. We show now that

$$\mathcal{H}_{q+1} = \{x^j h_{k,\ell} \mid 1 \leq j \leq k,\ 1 \leq k \leq n,\ 1 \leq \ell \leq \ell_k\} \tag{2.41}$$

is a basis of $\mathcal{I}_{q+1}$ as a vector space. We will prove in Chapter 6 that this implies that $\mathcal{H}_q$ is a Pommaret basis of $\mathcal{I}_{\geq q}$ ($\mathcal{H}_q$ is then locally involutive, cf. Proposition 6.4.5 and Lemma 6.3.5).

Let $f \in \mathcal{I}_{q+1}$ and $\operatorname{cls} f = j$. By the properties of the degree reverse lexicographic order this implies that $f = x^j \hat{f} + g$ with $\hat{f} \in \big(\mathbb{k}[x^j, \dots, x^n] \setminus \{0\}\big)_q$ and $g \in \big(\langle x^1, \dots, x^{j-1}\rangle\big)_{q+1}$ (cf. Lemma B.2.2). We distinguish two cases. By (2.40b) we have $\big(\langle \mathcal{I}, x^1, \dots, x^d\rangle\big)_q = \mathcal{P}_q$. Thus if $j > d$, we may write $\hat{f} = \sum_{k=d+1}^n \sum_{\ell=1}^{\ell_k} c_{k,\ell} h_{k,\ell} + \hat{g}$ with $c_{k,\ell} \in \mathbb{k}$ and $\hat{g} \in \big(\langle x^1, \dots, x^d\rangle\big)_q$. We set $\hat{f}_0 = \sum_{k=j}^n \sum_{\ell=1}^{\ell_k} c_{k,\ell} h_{k,\ell}$ and $\hat{f}_1 = \sum_{k=d+1}^{j-1} \sum_{\ell=1}^{\ell_k} c_{k,\ell} h_{k,\ell} + \hat{g}$. Obviously, $\hat{f} \in \big(\langle \mathcal{I}, x^1, \dots, x^{j-1}\rangle : x^j\big)_q$. Thus if we have $j \leq d$, then (2.40a) implies that $\hat{f} \in \big(\langle \mathcal{I}, x^1, \dots, x^{j-1}\rangle\big)_q$. Hence in this case we may write $\hat{f} = \hat{f}_0 + \hat{f}_1$ with $\hat{f}_0 = \sum_{k=j}^n \sum_{\ell=1}^{\ell_k} c_{k,\ell} h_{k,\ell}$ and $\hat{f}_1 \in \big(\langle x^1, \dots, x^{j-1}\rangle\big)_q$.

It is trivial that $\langle \mathcal{H}_{q+1} \rangle \subseteq \mathcal{I}_{q+1}$ (here we mean the span over $\Bbbk$ and not over $\mathcal{P}$). We show by an induction over j that $\mathcal{I}_{q+1} \subseteq \langle \mathcal{H}_{q+1} \rangle$. If $j = 1$, then $f = x^1 \hat{f}$ with $\hat{f} \in \mathcal{I}_q$. Thus $f \in \langle \mathcal{H}_{q+1} \rangle$. If $j > 1$, we write $f = f_0 + f_1$ with $f_0 = x^j \hat{f}_0$ and $f_1 = x^j \hat{f}_1 + g$ where $\hat{f}_0$ and $\hat{f}_1$ have been defined above. By construction, $f_0 \in \langle \mathcal{H}_{q+1} \rangle$, as x^j is multiplicative for all generators contained in $\hat{f}_0$, and $f_1 \in \mathcal{I}_{q+1}$ with $\operatorname{cls} f_1 < j$. According to our inductive hypothesis this implies that $f_1 \in \langle \mathcal{H}_{q+1} \rangle$, too. Hence $\langle \mathcal{H}_{q+1} \rangle = \mathcal{I}_{q+1}$. □

Remark 2.6.12. Again it is a natural question whether this result holds only for Pommaret bases. And again we may simply take the example already used in Remark 2.4.14. In δ-regular coordinates, the ideal $\mathcal{I}$ considered there possesses a Pommaret basis of degree 2. Hence the Castelnuovo–Mumford regularity $\operatorname{reg} \mathcal{I}$ is 2. But we saw that a simple permutation of the variables yields a Janet basis of degree 4 for the same term order. Thus we may conclude that arbitrary involutive bases contain no information on the Castelnuovo–Mumford regularity. ◁

2.7 Notes

Combinatorial decompositions of polynomial modules and involutive bases are implicitly contained in the *Janet–Riquier Theory* of linear systems of differential equations developed in the late 19th, early 20th century by a number of authors (see e. g. [83, 84, 150, 177, 180]). In this theory, the term *passive* introduced by Méray and Riquier [122] is more common than *involutive*; the latter one seems to go back to Lie. The idea of assigning multiplicative variables is apparently due to Janet. In this context, one should mention that the distinction into parametric and principal derivatives used in Chapter 1 goes back to Riquier.

The results of this theory remained more or less unknown in commutative algebra until fairly recently. Rees [145] introduced much later the special decomposition now carrying his name. The concept was generalised by Stanley [169, 170] who was interested in a simple way to determine Hilbert functions; Proposition 2.5.2 is due to him. In recent years, a number of authors have picked up these ideas and applied them in various fields; see e. g. [12, 18, 54, 172, 173] and references therein.

Concrete algorithms for their construction have been proposed by Sturmfels and White [173]. They presented a simple recursive algorithm to determine a Stanley decomposition for arbitrary monomial modules which is essentially equivalent to our proof of Proposition 2.5.3 (a related algorithm was designed by Reid [147] in the context of initial value problems for overdetermined systems of differential equations). Thus its extension to polynomial modules $\mathcal{P}^m/\mathcal{N}$ requires that one must first compute a Gröbner basis of $\mathcal{N}$ for some term order $\prec$ in order to obtain a basis of $\operatorname{lt}_\prec \mathcal{N}$. They further developed a special method for determining Rees decompositions. However, it is rather expensive, as it needs repeated computations of Gröbner bases. Our approach via Pommaret bases is more direct and efficient.

Proposition 2.5.3 on the decomposition of the complementary set is a classical result in commutative algebra [40, pp. 417–418] and is sometimes used to prove the existence of the Hilbert polynomial. We slightly modified the proof in order to obtain a disjoint decomposition. Gerdt [55, Lemma 24] proposed a version of this result that relates the form of the cones to an involutive division. However, his proof is not correct, as the there constructed set $\mathcal{U}$ (in the notation of our proof of Proposition 2.5.3) may also contain elements of $\mathcal{I}$. Indeed, it is trivial to provide examples for this effect using the Janet division. Proposition 2.5.4 was already proven by Janet [84, Section 15].

Involutive divisions were introduced by Gerdt and Blinkov [56]. They also defined all examples of divisions appearing in this chapter. One should note a slight difference in conventions. We always analyse multi indices from the right, i. e. we start with the last entry μ_n and not with the first entry μ_1. Thus for the Janet division we first check whether n is multiplicative and then continue with the lower values;[4] for the Pommaret division multi indices of the form $[0, \dots, 0, \mu_n]$ possess the most multiplicative indices. In [56], it is exactly the other way round: they start the analysis of a multi index with μ_1 and not μ_n; for the Janet division they first check whether 1 is multiplicative and for the Pommaret division multi indices $[\mu_1, 0, \dots, 0]$ possess the most multiplicative indices. Obviously, the two conventions become identical, if one simply inverts the order of the variables.

A weaker notion of an involutive division was introduced by Apel [8]. One could say that he uses a "local" approach whereas ours is "global". He defines an involutive division only with respect to a *single* set $\mathcal{N} \subseteq \mathbb{N}_0^n$ and hence does not need the second condition in Definition 2.1.1 relating the set of multiplicative indices for subsets. We will discuss the effect of this in more detail at the end of Chapter 6 in the context of completion algorithms.

The term "algebra of solvable type" was coined by Kandry-Rody and Weispfenning [88], when they tried to introduce Gröbner bases for non-commutative rings. Their definition is more restrictive than ours, as it does not allow that the terms operate on the coefficients and requires a stronger form of compatibility between the multiplication $\star$ and the term order $\prec$. It automatically implies that $\star$ respects $\prec$. For our purposes this is the decisive property and thus we have used it instead of the more technical axioms in [88] for Definition 2.2.1.

In the application sections we restricted to the ordinary polynomial ring $\mathcal{P}$. In fact, many of the results presented there do not hold in arbitrary polynomial algebras of solvable type. For example, in all our proofs concerning the depth of a module we implicitly assumed that if $f \in \langle x^i \rangle$, then each term in $\operatorname{supp} f$ is divisible by x^i. In case of the universal enveloping algebra of $\mathfrak{so}(3)$ this is obviously not the case according to (2.13). In fact, we find even that $\langle x^1, x^2 \rangle = \langle x^1, x^2, x^3 \rangle$.

The definition of a Stanley decomposition for a module over a polynomial algebra of solvable type is identical to the definition in the case of the ordinary polynomial ring, as it is based on an isomorphism as vector spaces. Thus the multiplication does not matter and it is important to note that on the right hand side of (2.23) the $\cdot$ is *not* replaced by a $\star$. If the multiplication $\star$ preserves the natural grading of the polynomial ring, Proposition 2.5.2 remains valid.

[4] In fact, this is the way the division was introduced by Janet [84, pp. 16–17].

Our syzygy theory can be generalised under certain conditions. In particular, the proof of Theorem 2.6.3 depends mainly on normal form arguments that work in any polynomial algebra of solvable type. We must require that $\star$ respects term orders of the form $\prec_{\mathcal{H}}$ in order for the theorem to make sense. In addition, we must take care of the arguments on multiplicative variables. In arbitrary polynomial algebras of solvable type $(ax^i) \star (bx^j) = cx^i x^j + h$ where in general the polynomial h may depend on any variables x^k. We need that if x^i and x^j are both multiplicative for some other polynomial, then the product $(ax^i) \star (bx^j)$ should also be multiplicative. This implies that h may depend only on variables with $k \leq \max\{i, j\}$. All these conditions are for example satisfied by rings of differential operators.

The notion of an involutive basis is also due to Gerdt and Blinkov [56]; the special case of a Pommaret basis was already earlier introduced by Zharkov and Blinkov [195]. But as already mentioned, such bases are implicitly contained in many articles, even in rather old ones. The main credit of the three mentioned authors is that, inspired by the work of Janet, they were the first to give a rigorous algebraic formulation of the theory and to relate it to the modern theory of Gröbner bases. In particular, they introduced involutive reductions and normal forms, two concepts missing in the classical Janet–Riquier Theory.

One may wonder why we have introduced weak involutive bases. This concept is indeed very weak: a weak involutive basis does not define a Stanley decomposition, it is not necessarily a Gröbner basis and so on. All interesting properties hold only for strong bases; indeed, we will exclusively work with strong bases. One simple reason for the introduction of weak bases is that in our approach to involutive bases their definition appears very naturally. In some proofs it is convenient to show first that one has a weak basis and later that it can be reduced to a strong one.

In a recent preprint [73] on involutive bases in the Weyl algebra, weak bases played a more prominent role. There bases with respect to a larger class of orders, so-called *multiplicative monomial orders*, are studied. In general, these orders are not well-orders and normal form computations do not always terminate. It was not possible to show the existence of strong involutive bases for such orders but a constructive proof of the existence of weak involutive bases which are simultaneously Gröbner bases could be given. This work showed that normal form arguments are even more important for involutive bases than for Gröbner bases.

δ-regularity is often considered as a purely technical nuisance. It is of course unpleasant that for some ideals no finite Pommaret basis exists. In particular, the completion algorithms discussed in Chapter 6 do not terminate in this case. However, δ-singularity is often related to important properties of the ideal considered. For example, in applications to differential equations it is related to characteristics; if the hyperplane $x^n = 0$ is a characteristic surface, then the coordinates are δ-singular (see Section 3.3).

Several solutions to the problem of δ-regularity have been proposed in the literature; mainly in the context of differential equations. Most of them are based on the proof of Proposition 2.4.6. Pommaret [139] advocates the brute force method of computing in a generic coordinate system. As it requires the introduction of n^2 additional parameters which are considered as algebraically independent transcendentals over $\mathbb{k}$, this approach is only of theoretical value. Even for small examples computations in generic coordinates very quickly blow up. An advantage is that one obtains an explicit characterisation of all δ-singular coordinate systems which is sometimes of interest (see e. g. [173, Proposition 5.3])

[159] contains an improvement on this approach. If k is the lowest class present in the set $\mathcal{F}$, it requires only the introduction of $n(n-k)$ parameters. Furthermore, it is not necessary to explicitly perform the coordinate transformation. As the ranks of several parametric matrices must be determined, this solution is still computationally rather expensive. It also yields all genericity conditions.

Another possibility consists of relying on Proposition 2.4.6 and performing a random coordinate transformation. This approach is, for example, used by Hartley and Tucker [69] in their implementation of the Cartan–Kähler theory (and also by Sturmfels and White [173] in their above mentioned method for the construction of Rees decompositions). As we have seen, it leads with probability 1 to a δ-regular coordinate system. Besides the possibility that we still might get a δ-singular system, the main disadvantage of this approach is that it destroys any sparsity that might be present in the original set $\mathcal{F}$. In particular, in applications to differential equations the elements of $\mathcal{F}$ are very often sparse, i. e. not every derivative p^α_μ up to a given length q of the multi indices μ does actually appear. Of course, this is a great advantage in any concrete computations which one would like to preserve.

The approach presented in Section 2.4 was developed in [71] only very recently. It has two interesting aspects for computations. On one hand it provides us with a very cheap method to detect termination problems in the completion; this will be discussed in more detail in Section 6.4. On the other hand, the proof indicates a concrete coordinate transformation that brings us closer to δ-regularity. It preserves comparatively much of the sparsity of $\mathcal{F}$, as it only affects terms containing x^ℓ.

We have seen that (strong) involutive bases are a special form of Gröbner bases. Very often they are reduced to this one aspect. Much of the (not very extensive) literature on involutive bases treats them solely as an alternative approach to compute Gröbner bases. It is completely overlooked that the combinatorial decompositions defined by involutive bases reveal a lot of structural information not contained in arbitrary Gröbner bases. This holds in particular for Pommaret bases where e. g. Proposition 2.4.13 and Corollary 2.6.4 yield the depth and the projective dimension together with a simple proof of Hilbert's Syzygy Theorem.

The characterisation of stable monomial modules in terms of Pommaret bases is due to Mall [111] (but see also the remark after Lemma 1.2 in [49]). Eliahou and Kervaire [49] provide an explicit representation of their minimal free resolution. It is based on some manipulations of a Koszul complex. Unfortunately, it is not possible to extend their results to the polynomial case. The main reason is very simple. Assume we are given a stable monomial module with basis $\{\mathbf{t}_\alpha\}$. If we multiply the generator $\mathbf{t}_\alpha$ with a term s, there exists a unique generator $\mathbf{t}_\beta$ such that $s\mathbf{t}_\alpha \in \mathcal{C}_P(\mathbf{t}_\beta)$. The estimate $\operatorname{cls}\mathbf{t}_\beta \geq \operatorname{cls}\mathbf{t}_\alpha$ is completely trivial but essential for the construction of the differential of Eliahou and Kervaire. In the polynomial case with a basis $\{\mathbf{h}_\alpha\} \subset \mathcal{P}^m$, the standard representation of a product $s\mathbf{h}_\alpha$ consists of a sum involving in general many generators $\mathbf{h}_\beta$. In particular, it is no longer possible to provide a lower bound for the classes of the $\mathbf{h}_\beta$. This prevents the construction of a complex along the lines of Eliahou and Kervaire.

Of course, based on the Schreyer Theorem, any Gröbner basis may be used to construct a syzygy resolution. And in many textbooks this resolution is used for a proof of Hilbert's Syzygy Theorem. However, the special structures induced by Pommaret basis does not only yield a stronger estimate on the length of the minimal resolution (in fact, we have seen that it always yields a resolution of minimal length) but even a closed formula for the ranks of the modules contained in the resolution. At the moment, it is still an open question to what extent this result may be exploited for obtaining tight estimates on the Betti numbers or even for computing them directly.

A number of different approaches to the Castelnuovo–Mumford regularity exists. A few notes on the history of this concept can be found in [47, pp. 514–515]. Often it is defined using local cohomology. In view of Theorem 2.6.11, this should be closely related to the definition of involution via the Spencer cohomology. To our knowledge, this relation has not yet been worked out. Our approach exploits the more constructive criteria provided by [14, 48].

Among other applications, the Castelnuovo–Mumford regularity $\operatorname{reg}\mathcal{I}$ is a useful measure for the complexity of Gröbner basis computations [13]. Roughly speaking, only for ideals $\mathcal{I}$ with a not too high value of $\operatorname{reg}\mathcal{I}$ one has a good chance to determine a Gröbner basis in a reasonable time. Bayer and Stillman [14] proved that in generic coordinates it is not possible to find a Gröbner basis of degree less than $\operatorname{reg}\mathcal{I}$. This estimate is sharp, as it is realised by bases with respect to the degree reverse lexicographic order. As by Theorem 2.6.11, any Pommaret basis for the degree reverse lexicographic order has this very degree, we obtain as a trivial corollary an estimate how much larger a Pommaret basis may become in comparison to the corresponding reduced Gröbner basis.