Pommaret Bases and Rees Decomposition

Orn Arnaldsson

Abstract

We define involutive bases for polynomial ideals and demonstrate their use in calculating direct decompositions of polynomial modules, focusing on the so-called Pommaret bases. The resulting decomposition is the well known Rees decomposition. An overview of other important applications of Pommaret bases is given.

1 Introduction

The objective of this note is to give a solid introduction to involutive bases. Rather than introduce too many of the wonderful applications of involutive bases, making this short note cluttered, we focus on the underpinnings of the theory, only giving their application to a direct decomposition of factor algebras $\mathcal{P}/\mathcal{I}$, named after Rees [5]. The reader of this note will then hopefully be well equipped, and motivated, to pursue the applications further.

Much of the theory of Groebner bases (and the more refined involutive bases) originated in the study of partial differential equations in the late 19th and early 20th centuries. Gjunter, see [2] for an overview of his work, even anticipated the Buchberger algorithm in his study of integrability of PDEs. The combinatorial decompositions of polynomial modules appeared in the Janet-Riquier theory of systems of PDEs ([3], [6]). It was much later that Rees introduced the decomposition now bearing his name. These ideas were then generalized by Stanley [8] who was interested in a simple way to determine Hilbert functions.

We will focus on a certain type of involutive bases, namely the Pommaret bases. Among the algebraic application of these are the calculation of many important invariants of polynomial modules, such as the Hilbert function, depth, dimension and Castaelnuovo-Mumford regularity. They can also be used to calculate primary decompositions, minimal free resolutions and syzygys. For details and more applications, see Chapter 5 of [7].

The applications of Pommaret bases to PDE theory culminate in the Cartan-Kahler theorem and the Cartan-Kuranishi theorem (conjectured by Cartan and proven by Kuranishi [4]) on integrability of (analytic) PDEs. The latter theorem is especially hard in the framework of exterior differential systems in which it was originally formulated. It is a testament to the power of the involutive theory how easy it becomes in the involutive framework, where it is a simple Noetherian argument. For details see Chapters 7 and 9 in [7].
2 The Abelian Monoid

In this section, we give the definition of an involutive division, which will enable us to decompose polynomial ideals into direct sums. We shall start out by working with \((\mathbb{N}_0^n, +)\), the abelian monoid of \(n\)-tuples with component-wise addition, where \(\mathbb{N}_0\) is the set of non-negative integers. We refer to the elements of \(\mathbb{N}_0^n\) as multi-indices. For \(\nu \in \mathbb{N}_0^n\) we define its cone as the set \(C(\nu) := \nu + \mathbb{N}_0^n\). An ideal in \(\mathbb{N}_0^n\) is a set \(\mathcal{I} \subset \mathbb{N}_0^n\) such that \(\mathcal{I} + \mathbb{N}_0^n = \mathcal{I}\). For a subset \(\mathcal{B} \subset \mathbb{N}_0^n\), its span is the ideal

\[
\langle \mathcal{B} \rangle := \bigcup_{\nu \in \mathcal{B}} C(\nu).
\]

By Dixon’s lemma [1], every ideal, \(\mathcal{I}\), in \(\mathbb{N}_0^n\) has a finite basis, i.e. a finite set \(\mathcal{B}\) such that \(\langle \mathcal{B} \rangle = \mathcal{I}\). Note that we can associate to every multi-index \(\nu = (\nu_1, \ldots, \nu_m) \in \mathbb{N}_0^n\) a monomial \(x^\nu \in \mathbb{P} := \mathbb{k}[x_1, \ldots, x_n]\), where \(x^\nu = x_{\nu_1} \cdots x_{\nu_m}\), and the monoid operation corresponds to regular multiplication: \(x^\nu x^\mu = x^{\nu + \mu}\). The sum of the indices of an element \(\nu \in \mathbb{N}_0^n\), denoted \(|\nu|\), is called the length of \(\nu\), and it corresponds to the total degree of \(x^\nu\).

Remark 1. For a set \(\mathcal{B} \subset \mathbb{N}_0^n\), we can define the monomial ideal, \(\mathcal{J}\), spanned by the set \(\{x^\nu \mid \nu \in \mathcal{B}\}\). It is easy to see that \(x^\nu \in \mathcal{J}\) if and only if \(\mu \in \mathcal{B}\). To translate our results to the polynomial realm we take a term order that designates leading order terms of polynomials and consequently, the monomial ideal spanned by those terms.

Let \(\mathcal{B}\) be a basis for the monoid ideal \(\mathcal{I}\). In general, the union in (1) is certainly not disjoint, and so an element \(\mu \in \mathcal{I}\) may belong to many different basis cones. We are interested in decomposing monoid ideals into disjoint unions of so-called involutive cones. Before discussing this idea in more detail, we give the fundamental definition of our subject, due to Seiler (see [7], page 65 and the notes at the end of Chapter 3 for a historical account of involution.)

Definition 1. An involutive division \(L\) is defined on the abelian monoid \((\mathbb{N}_0^n, +)\), if for any finite subset \(\mathcal{B} \subset \mathbb{N}_0^n\) and every \(\nu \in \mathcal{B}\), a set \(N_{L, \mathcal{B}}(\nu) \subset \{1, \ldots, n\}\) of multiplicative indices is defined and consequently a submonoid \(M(\nu, \mathcal{B}) := \{\mu \mid \forall j \notin N_{L, \mathcal{B}}(\nu) : \mu_j = 0\}\) such that the following hold for the involutive cones \(C_{L, \mathcal{B}}(\nu) := \nu + M(\nu, \mathcal{B})\):

(i) For any two elements, \(\nu, \mu \in \mathcal{B}\) such that \(C_{L, \mathcal{B}}(\nu) \cap C_{L, \mathcal{B}}(\mu) \neq \emptyset\), then \(C_{L, \mathcal{B}}(\nu) \subset C_{L, \mathcal{B}}(\mu)\) or \(C_{L, \mathcal{B}}(\mu) \subset C_{L, \mathcal{B}}(\nu)\).

(ii) If \(\mathcal{B}' \subset \mathcal{B}\), then \(N_{L, \mathcal{B}} \subset N_{L, \mathcal{B}'}\).

In words, the involutive division \(L\) is a rule that assigns to every pair \(\mathcal{B} \subset \mathbb{N}_0^n\) and \(\nu \in \mathbb{N}_0^n\) the set \(N_{L, \mathcal{B}}(\nu)\). It is not obvious how this rather technical definition is related to our interest in decomposing monoid ideals into disjoint cones, but it is in fact tailor-made for such a decomposition. Here’s how. For a finite basis, \(\mathcal{B}\), for an ideal \(\mathcal{I}\), and an involutive division \(L\) on \(\mathbb{N}_0^n\), we define the involutive span of \(\mathcal{B}\) with respect to the division \(L\) to be the union of the involutive cones of the elements of \(\mathcal{B}\),

\[
\langle \mathcal{B} \rangle_L := \bigcup_{\nu \in \mathcal{B}} C_{L, \mathcal{B}}(\nu).
\]

2
If the involutive span of $\mathcal{B}$ happens to equal the whole ideal $\mathcal{I}$ (warning: for a given set $\mathcal{B}$, finding an involutive basis for $\langle \mathcal{B} \rangle$ is in general not an easy problem), then we say that $\mathcal{B}$ is a weak involutive basis for $\mathcal{I}$. Now, thanks to conditions (i) and (ii) in Definition 1, we can actually reduce the (weak) basis $\mathcal{B}$ to a strong involutive basis $\mathcal{B}'$ where all the involutive cones in $\langle \mathcal{B}' \rangle_L$ are disjoint. To see this, assume that two cones in $(2), C_{L,B}(\nu)$ and $C_{L,B}(\nu')$, intersect. By condition (i) above, one is included in the other, say $C_{L,B}(\nu') \subset C_{L,B}(\nu)$. Now simply drop $\nu'$ from the weak basis $\mathcal{B}$ to obtain the set $\mathcal{B}_1 := \mathcal{B} \setminus \{\nu\}$. By condition (ii) above, in the involutive span $\langle \mathcal{B}_1 \rangle_L$, the involutive cones have all increased and so $\langle \mathcal{B}_1 \rangle_L \subset \langle \mathcal{B}' \rangle_L$. But both are included in the ideal $\mathcal{I}$ so $\mathcal{B}'$ is indeed a weak basis for $\mathcal{I}$. We easily see that $\langle \mathcal{B} \rangle = \langle \mathcal{B}' \rangle$, so continuing this process will eventually lead to a set $\mathcal{B}'$, whose involutive span is still $\mathcal{I}$, and all of whose involutive cones are disjoint.

The most important involutive division for our purposes, both in algebraic applications and partial differential equations, is the Pommaret division, denoted by $P$, and defined as follows. For a multi-index $\nu$, define its set of multiplicative variables $N_P(\nu) := \{1, 2, \ldots, \text{cls}(\nu)\}$, where $\text{cls}(\nu) := \min\{i \mid \nu_i \neq 0\}$, is the class of the multi-index $\nu$. Proving that this actually gives a division is an easy exercise. Notice how $P$ does not depend on a set $\mathcal{B}$ which $\nu$ belongs to. Such divisions are called global. This property is part of the reason the Pommaret division is appealing: In the process of determining a Pommaret basis, we do not need to constantly calculate the change in multiplicative indices as we add or eliminate elements from our potential basis (cf. condition (ii) in Definition 1.)

We mention here another division, the Janet division, denoted by $J$, whose surprising connection to the Pommaret division facilitates the existence theory of Pommaret bases (see Chapter 4.3 in [7]). It is defined as follows. Let $\mathcal{B} \subset \mathbb{N}^n_0$, and $\nu \in \mathcal{B}$. For $(d_k, d_{k+1}, \ldots, d_n) \in \mathbb{N}^{n-k+1}_0$ define the set

$$(d_k, d_{k+1}, \ldots, d_n)_B := \{\nu \in \mathcal{B} \mid \nu_i = d_i, \; k \leq i \leq n\}.$$ 

We declare the index $l$ to be multiplicative for $\nu$ in $\mathcal{B}$ if $\nu_l = \max\{\mu_l \mid \mu \in \mathcal{B}, \; \mu \in (\nu_{l+1}, \ldots, \nu_n)_B\}$.

Example 1. Let $\mathcal{B} = \{(1, 0), (0, 1)\} \subset \mathbb{N}^2_0$. Then $N_P(1, 0) = \{1\}$, $N_P(0, 1) = \{1, 2\}$, $N_{J,B}(1, 0) = \{1\}$ and $N_{J,B}(0, 1) = \{2\}$. We easily see that $\langle \mathcal{B} \rangle_P = \langle \mathcal{B} \rangle$, while $\langle \mathcal{B} \rangle_J \neq \langle \mathcal{B} \rangle$, so $\mathcal{B}$ is a Pommaret basis for $\langle \mathcal{B} \rangle$, while it is not a Janet basis. A Janet basis for $\langle \mathcal{B} \rangle$ would be $\mathcal{B} \cup \{(1, 1)\}$.

An involutive division, $L$, is called Noetherian if every ideal in $\mathbb{N}^n_0$ has an involutive basis with respect to $L$. The Janet division is Noetherian (see [7], page for a proof), while the same is not true for the Pommaret division, as the next example shows.

Example 2. The ideal $\mathcal{I} = \{(1, 1)\} \subset \mathbb{N}^2_0$ does not have a finite Pommaret basis, since every element in $\mathcal{I}$ has class equal to 1.

In order to apply the above to general polynomial ideals $\mathcal{I} \subset \mathcal{P} = \mathbb{k}[x_1, \ldots, x_n]$ (for $\mathbb{k}$ a field of characteristic 0), we need a term order. It turns out that since we are primarily interested in the Pommaret division, a class respecting term order is desirable. This means that if $\nu$ and $\mu$ have the same length then $\nu \leq \mu$ if and only if $\text{cls}(\nu) \leq \text{cls}(\mu)$. There is essentially only one class respecting term order (see [7], page 514), the degree reverse lexicographic order, and we shall simply denote it by $\prec$. For a polynomial $f \in \mathcal{P}$, the
leading order term is denoted by $\text{lt}_<(f)$ and the exponent of $\text{lt}_<(f)$ by $\text{le}_<(f)$. In general, for a subset $\mathcal{H} \subset \mathcal{P}$, the collection of leading order terms of $\mathcal{H}$ is denoted $\text{lt}_<(\mathcal{H})$. For an ideal $\mathcal{I} \subset \mathcal{P}$, we define the leading term ideal, as $(\text{lt}_<(\mathcal{I}))$, the monomial ideal spanned by all the leading terms of the elements of $\mathcal{I}$. By Remark 1 this monomial ideal corresponds to an ideal in $\mathbb{N}_0^n$ and we can thus speak of an involutive basis for $\text{lt}_<(\mathcal{I})$ and hence $\mathcal{I}$.

The popular Groebner bases from computational algebra provide a systematic way of writing elements of $\mathcal{I}$ in terms of the basis elements. The crucial difference between general Groebner bases and involutive bases is that the latter provide a direct decomposition of the ideal as each element can be written as a combination of basis elements in a unique way. The proof of the following theorem requires only checking the conditions of Definition 1.

**Theorem 2.** Let $\mathcal{H}$ be a finite subset of $\mathcal{P}$, $\mathcal{I}$ an ideal in $\mathcal{P}$ and let $L$ be an involutive division on $\mathbb{N}_0^n$. The following are equivalent.

(i) $\text{lt}_<(\mathcal{H})$ is an involutive basis for $\text{lt}_<(\mathcal{P})$.

(ii) $\mathcal{I}$ can be decomposed as a direct sum in the following way

$$\mathcal{I} = \bigoplus_{h \in \mathcal{H}} \mathbb{k}[X_{h,<,L}] \cdot h,$$

where $X_{h,<,L} \subset \{x_1, \ldots, x_n\}$ correspond to the multiplicative indices of $\text{le}_<(h)$ according to the division $L$.

For a homogeneous polynomial ideal $\mathcal{I} = \bigoplus q \mathcal{I}_q$ and an involutive basis $\mathcal{H}$ for $\mathcal{I}$, this result immediately gives a simple way of calculating the dimension of the $q^{th}$ degree component $\mathcal{I}_q$. We have (where $k_h := |X_{h,<,L}|$ is the number of multiplicative indices of $h$ and $d_h$ is the degree of $h$)

$$\dim \mathcal{I}_q = \sum_{h \in \mathcal{H}} \left( q - d_h + k_h - 1 \right).$$

### 3 Rees Decomposition

As a nice application of the above we present a result on Rees decompositions of the factor algebra $\mathcal{P}/\mathcal{I}$, where $\mathcal{I}$ is an ideal. By a decomposition, we mean a $\mathbb{k}$-vector space isomorphism

$$\mathcal{P}/\mathcal{I} \cong \bigoplus_{t \in \mathcal{T}} \mathbb{k}[X_t] \cdot t,$$

where $\mathcal{T}$ is a finite set of elements of $\mathcal{P}$, whose elements are called the generators of the decomposition, and $X_t \subset \{x_1, \ldots, x_n\}$ are, again, called the multiplicative indices of $t$. A Rees decomposition is one where $X_t = \{x_1, \ldots, x_{\text{cls}(\text{le}_<(t))}\}$. Note that, as $\mathbb{k}$-vector spaces, $\mathcal{P}/\mathcal{I} \cong \mathcal{P}/\text{lt}_<(\mathcal{I})$ and so without loss of generality, we can assume that $\mathcal{I}$ is a monomial
ideal. We denote the corresponding ideal in \( \mathbb{N}_n^0 \) also by \( \mathcal{I} \), and its complement by \( \bar{\mathcal{I}} \subset \mathbb{N}_n^0 \). Notice that if we manage to decompose \( \bar{\mathcal{I}} \subset \mathbb{N}_n^0 \) into disjoint sets

\[
\bar{\mathcal{I}} = \bigoplus_{t \in \mathcal{T}} M_t \cdot t, \quad M_t \text{ a sub-monoid of } \mathbb{N}_n^0,
\]

then this decomposition immediately descends to a decomposition of \( \mathcal{P}/\mathcal{I} \cong \bigoplus_{t \in \mathcal{T}} \mathbb{K}[X_t] \cdot t \). Where, of course, \( X_t \) is the sub-algebra of \( \mathcal{P} \) corresponding to \( M_t \). The result that connects Pommaret bases and decompositions is the following.

**Theorem 3.** The monoid ideal \( \mathcal{I} \subset \mathbb{N}_n^0 \) has a Pommaret basis with maximal degree \( q \), if and only if the sets \( \bar{\mathcal{B}}_0 = \{ \nu \in \bar{\mathcal{I}} \mid |\nu| < q \} \) and \( \bar{\mathcal{B}}_1 = \{ \nu \in \bar{\mathcal{I}} \mid |\nu| = q \} \) yield the following disjoint decomposition

\[
\bar{\mathcal{I}} = \bar{\mathcal{B}}_0 \uplus \bigcup_{\nu \in \bar{\mathcal{B}}_1} \mathcal{C}_P(\nu).
\]

**Proof.** Notice that \( (\mathbb{N}_n^0)_{\geq q} = \bigcup_{|\nu|=q} \mathcal{C}_P(\nu) \), where \( (\mathbb{N}_n^0)_{\geq q} \) are the monoids of length at least \( q \). The result now follows from the fact (see [7], page 124) that \( \mathcal{I} \subset \mathbb{N}_n^0 \) has a Pommaret basis if and only if \( (\mathcal{I})_{\geq q} := \mathcal{I} \cap (\mathbb{N}_n^0)_{\geq q} \) has a Pommaret basis all of whose elements have length \( q \).

The disjoint union in (3) may well have some redundancies. In fact, cleaning them up results in the following surprising result (see [7], page 175 for proof.)

**Theorem 4.** Let \( \mathcal{I} \) be a polynomial ideal possessing a Pommaret basis \( \mathcal{H} \), with \( \min_{h \in \mathcal{H}} \text{cls}(h) = d \). Then the factor algebra has a Rees decomposition where the minimal class of generators is \( d - 1 \).

**References**


