4

An Algebraist's View on Border Bases

Achim Kehrein[1], Martin Kreuzer[1], and Lorenzo Robbiano[2]

[1] Universität Dortmund, Fachbereich Mathematik, 44221 Dortmund, Germany
achim.kehrein@mathematik.uni-dortmund.de
martin.kreuzer@mathematik.uni-dortmund.de
[2] Dipartimento di Matematica, Via Dodecaneso 35, 16146 Genova, Italy
robbiano@dima.unige.it

Summary. This chapter is devoted to laying the algebraic foundations for border bases of ideals. Using an order ideal $\mathcal{O}$, we describe a zero-dimensional ideal *from the outside*. The first and higher borders of $\mathcal{O}$ can be used to measure the distance of a term from $\mathcal{O}$ and to define $\mathcal{O}$-border bases. We study their existence and uniqueness, their relation to Gröbner bases, and their characterization in terms of commuting matrices. Finally, we use border bases to solve a problem coming from statistics.

4.1 Introduction

El infinito tango me lleva hacia todo
[The infinite tango takes me towards everything]
(Jorge Luis Borges)

The third author was invited to teach a course at the CIMPA school in July 2003. When the time came to write a contribution to the present volume, he was still inspired by the tunes of classical tango songs which had been floating in his mind since his stay in Buenos Aires. He had the idea to create some variations on one of the themes of his lectures. Together with the first and second authors, he formed a *trio* of algebraists. They started to collect scattered phrases and tunes connected to the main theme, and to rework them into a survey on border bases. Since the idea was welcomed by the organizers, you have now the opportunity to enjoy their composition.

In the last few years it has become increasingly evident how Gröbner bases are changing the mathematical landscape. To use a lively metaphor, we can say that by considering a Gröbner basis of an ideal I in the polynomial ring $P = K[x_1, \ldots, x_n]$, we are looking at I *from the inside*, i.e. by describing a special set of generators. But a Gröbner basis grants us another perspective. We can look at I *from the outside*, i.e. by describing a set of polynomials which form a K-vector space basis of P/I, namely the set of terms outside $\mathrm{LT}_\sigma(I)$ for some term ordering σ. However, Gröbner bases are not optimal from the latter point of view, for instance, because the bases they provide tend to be numerically ill-behaved.

This leads us to one of the main ideas behind the concept of a border basis. We want to find more "general" systems of generators of I which give rise to a K-basis of P/I. Quotation marks are in order here, since so far the generalization only works for the subclass of zero-dimensional ideals I. In the zero-dimensional case, the theory of border bases is indeed an extension of the theory of Gröbner bases, because there are border bases which cannot be associated to Gröbner bases. Moreover, border bases do not require the choice of a term ordering. Our hope is that the greater freedom they provide will make it possible to construct bases of P/I having additional good properties such as numerical stability or symmetry.

Even if these considerations convince you that studying border bases is useful, you might still ask why we want to add this survey to the current literature on that topic? Our main reason is that we believe that the algebraic foundations of border bases have not yet been laid out solidly enough. Important contributions are scattered across many publications (some in less widely distributed journals), and do not enjoy a unified terminology or a coherent set of hypotheses. We hope that this paper can be used as a first solid foundation of a theory which will surely expand quickly.

Now let us look at the content more closely. In Section 4.2 we describe some techniques for treating pairwise commuting endomorphisms of finitely generated vector spaces. In particular, we describe a Buchberger-Möller type algorithm (see Theorem 4.2.7) for computing the defining ideal of a finite set of commuting matrices. Given pairwise commuting endomorphisms $\varphi_1, \dots, \varphi_n$ of a finite dimensional K-vector space V, we can view V as a P-module via $f \cdot v = f(\varphi_1, \dots, \varphi_n)(v)$ for $f \in P$ and $v \in V$. Then Theorem 4.2.9 yields an algorithm for checking whether V is a cyclic P-module, i.e. whether it is isomorphic to P/I for some zero-dimensional ideal $I \subseteq P$.

Section 4.3 is a technical interlude where order ideals, borders, indices, and marked polynomials have their solos. An order ideal is a finite set of terms which is closed under taking divisors. We use order ideals to describe a zero-dimensional ideal "from the outside". The first and higher borders of an order ideal can be used to measure the "distance" of a term from the order ideal. The main tune in Section 4.3 is played by the Border Division Algorithm 4.3.10. It imitates the division algorithm in Gröbner basis theory and allows us to divide a polynomial by a border prebasis, i.e. by a list of polynomials which are "marked" by the terms in the border of an order ideal.

And then, as true stars, border bases appear late in the show. They enter the stage in Section 4.4 and solve the task of finding a system of generators of a zero-dimensional polynomial ideal having good properties. After we discuss the existence and uniqueness of border bases (see Theorem 4.4.4), we study their relation to Gröbner bases (see for instance Propositions 4.4.6 and 4.4.9). Then we define normal forms with respect to an order ideal, and use border bases to compute them. Many useful properties of normal forms are collected in Proposition 4.4.13.

In the final part of Section 4.4, we explain the connection between border bases and commuting matrices. This variation leads to the fundamental Theorem 4.4.17 which characterizes border bases in terms of commuting matrices and opens the door for our main application. Namely, we use border bases to solve a problem coming from statistics. This application is presented in Section 4.5, where we discuss the statistical background and explain the role of border bases in this field.

Throughout the text, we have tried to provide a generous number of examples. They are intended to help the reader master the basics of the theory of border bases. Moreover, we have tried to keep this survey as self-contained and elementary as possible. When we had to quote "standard results" of computer algebra, we preferred to rely on the book by the second and third authors [KR00]. This does not mean that those results are not contained in other books on the subject; we were merely more familiar with it.

Albert Einstein is said to have remarked that the secret of creativity was to know how to hide ones sources. Since none of us is Albert Einstein, we try to mention all sources of this survey. We apologize if we are unaware of some important contribution to the topic. First and foremost, we would like to acknowledge the work of Hans J. Stetter (see [AS88], [AS89], and [Ste04]) who used border bases in connection with problems arising in numerical analysis. Later H. Michael Möller recognized the usefulness of these results for computer algebra (see [Möl93], [MS95], and [MT01]). These pioneering works triggered a flurry of further activities in the area, most notably by Bernard Mourrain (see for instance [Mou99]) from the algorithmic point of view. A good portion of the material presented here is taken from the papers [CR97], [CR01], [KK03a], [Rob98], [Rob00], and [RR98]. Moreover, many results we discuss are closely related to other surveys in this volume.

Naturally, much work still has to be done; or, as we like to put it, there is still a huge `TODO`-list. A path which deserves further attention is the connection between border bases and numerical computation. Many ideas about the interplay of numerical and symbolic computation were proposed by Stetter, but we believe that there remains a large gap between the two areas which has to be addressed by algebraists. What about the algorithmic aspects? Almost no computer algebra system has built-in facilities for computing border bases. Naive algorithms for computing border bases, e.g. algorithms based on Gröbner basis computations, require substantial improvements in order to be practically feasible. This is an area of ongoing research. Some results in this direction are contained in Chapter 3. On the theoretical side we can ask whether the analogy between border bases and Gröbner bases can be further extended. First results in this direction are contained in [KK03a], but there appears to be ample scope for extending the algebraic theory of border bases.

Finally, wouldn't it be wonderful to remove the hypothesis that I is zero-dimensional, i.e. to develop a theory of border bases for the case when P/I is an infinite dimensional vector space? At the moment, despite the *infinite tango*, we are unfortunately lacking the inspiration to achieve this goal. Some ideas are presented in [Ste04], Ch. 11.

As for our notation, we refer the readers to [KR00]. In particular, throughout this paper we let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K. A polynomial of the form $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$, where $\alpha_1, \ldots, \alpha_n \in \mathbb{N}$, is called a **term** (or a **power product**). The monoid of all terms in P is denoted by $\mathbb{T}^n$.

4.2 Commuting endomorphisms

Tango has the habit of waiting
(Aníbal Troilo, virtuoso bandeoneonist)

Every polynomial ideal I is accompanied by the quotient algebra P/I. A zero-dimensional ideal I corresponds to an algebra P/I of finite vector space dimension over K. The first part of this section reviews how the K-algebra P/I is characterized by its P-module structure and how the latter is given by n pairwise commuting multiplication endomorphisms of the K-vector space P/I. In particular, for zero-dimensional ideals these endomorphisms can be represented by pairwise commuting multiplication matrices. Then we address the converse realization problem: Which collections of n pairwise commuting matrices can be preassigned as multiplication matrices corresponding to a zero-dimensional ideal? A necessary and sufficient condition is that these matrices induce a cyclic P-module structure. Whether a P-module structure on a finite dimensional K-vector space is cyclic can be checked effectively – an algorithm is presented in the second part.

4.2.1 Multiplication endomorphisms

Given a K-vector space V which carries a P-module structure, there exist endomorphisms of V which are associated to the multiplications by the indeterminates.

Definition 4.2.1. *For $i = 1, \ldots, n$, the P-linear map*

$$\varphi_i : V \longrightarrow V \qquad \text{defined by} \qquad v \mapsto x_i v$$

is called the $\mathbf{i^{th}}$ **multiplication endomorphism** *of V.*

The multiplication endomorphisms of V are pairwise commuting, i.e. we have $\varphi_i \circ \varphi_j = \varphi_j \circ \varphi_i$ for $i, j \in \{1, \ldots, n\}$. The prototype of such a vector space is given by the following example.

Example 4.2.2. Let $I \subseteq P$ be an ideal. The quotient algebra P/I possesses a natural P-module structure $P \times P/I \to P/I$ given by $(f, g+I) \mapsto fg + I$. Hence there are canonical multiplication endomorphisms $X_i : P/I \longrightarrow P/I$ such that $X_i(f+I) = x_i f + I$ for $f \in P$ and $i = 1, \ldots, n$. Note that P/I is a cyclic P-module with generator $1 + I$.

Remark 4.2.3. Let $\varphi_1, \ldots, \varphi_n$ be pairwise commuting endomorphisms of a vector space V. The following three constructions will be used frequently.

1. There is a natural way of equipping V with a P-module structure such that φ_i is the i^{th} multiplication endomorphism of V, namely the structure defined by
$$P \times V \longrightarrow V \qquad \text{such that} \qquad (f, v) \mapsto f(\varphi_1, \ldots, \varphi_n)(v)$$
2. There is a ring homomorphism
$$\eta : P \longrightarrow \mathrm{End}_K(V) \qquad \text{such that} \qquad f \mapsto f(\varphi_1, \ldots, \varphi_n)$$
3. Every ring homomorphism $\eta : P \longrightarrow \mathrm{End}_K(V)$ induces a P-module structure on V via the rule $f \cdot v = \eta(f)(v)$.

The following result allows us to compute the **annihilator** of V, i.e. the ideal $\mathrm{Ann}_P(V) = \{f \in P \mid f \cdot V = 0\}$.

Proposition 4.2.4. *Let V be a K-vector space equipped with a P-module structure corresponding to a ring homomorphism $\eta : P \longrightarrow \mathrm{End}_K(V)$. Then we have $\mathrm{Ann}_P(V) = \ker(\eta)$.*

Proof. By Remark 4.2.3, we have $f \cdot V = 0$ if and only if $\eta(f) = 0$. □

Of particular interest are P-module structures on V for which V is a cyclic P-module. The following proposition shows that such structures are essentially of the type given in Example 4.2.2.

Proposition 4.2.5. *Let V be a K-vector space and a cyclic P-module. Then there exist an ideal $I \subseteq P$ and a P-linear isomorphism*
$$\Theta : P/I \longrightarrow V$$
such that the multiplication endomorphisms of V are given by the formula $\varphi_i = \Theta \circ X_i \circ \Theta^{-1}$ for $i = 1, \ldots, n$.

Proof. Let $w \in V$ be a generator of the P-module V. Then the P-linear map $\tilde{\Theta} : P \longrightarrow V$ given by $1 \mapsto w$ is surjective. Let $I = \ker \tilde{\Theta}$ be its kernel and consider the induced isomorphism of P-modules $\Theta : P/I \to V$. The P-linearity of Θ shows $\Theta\big(X_i(g+I)\big) = \varphi_i\big(\Theta(g+I)\big)$ for $1 \le i \le n$ and $g + I \in P/I$. □

By [KR00], Proposition 3.7.1, zero-dimensional ideals $I \subseteq P$ are characterized by $\dim_K(P/I) < \infty$. Hence, if the vector space V in this proposition is finite dimensional, the ideal I is necessarily zero-dimensional. Now we want to answer the question, given $\varphi_1, \ldots, \varphi_n$, when is V a cyclic P-module via the structure defined in Remark 4.2.3.1? We note that if the P-module V is cyclic, then there exists an element $w \in V$ such that $\operatorname{Ann}_P(w) = \operatorname{Ann}_P(V)$.

Proposition 4.2.6 (Characterization of Cyclic P-Modules).
Let V be a K-vector space which carries the structure of a P-module.

1. *Given $w \in V$, we have $\operatorname{Ann}_P(V) \subseteq \operatorname{Ann}_P(w)$. In particular, there exists a P-linear map $\Psi_w :\ P/\operatorname{Ann}_P(V) \longrightarrow V$ defined by $f + \operatorname{Ann}_P(V) \mapsto f \cdot w$.*
2. *Let $w \in V$. The map Ψ_w is an isomorphism of P-modules if and only if w generates V as a P-module.*

Proof. The first claim follows from the definitions. To prove the second claim, we note that if Ψ_w is an isomorphism, then we have $V = P \cdot w$. Conversely, suppose that $V = P \cdot w$. Then the map Ψ_w is surjective. Let $f \in P$ be such that $f + \operatorname{Ann}_P(V) \in \ker(\Psi_w)$. Then $f(\varphi_1, \ldots, \varphi_n) \cdot w = 0$ implies $f(\varphi_1, \ldots, \varphi_n) = 0$ since w generates V. Hence we see that $f \in \operatorname{Ann}_P(V)$ and Ψ_w is injective. $\square$

4.2.2 Commuting matrices

In the remainder of this paper, we let V be a finite-dimensional K-vector space and μ its dimension. We fix a K-basis $\mathcal{V} = (v_1, \ldots, v_\mu)$ of V. Thus every endomorphism of V can be represented by a matrix of size $\mu \times \mu$ over K. In particular, when V is a P-module, then $\mathcal{M}_1, \ldots, \mathcal{M}_n$ denote the matrices corresponding to the multiplication endomorphisms $\varphi_1, \ldots, \varphi_n$.

Using the following variant of the Buchberger-Möller algorithm, we can calculate $\operatorname{Ann}_P(V)$ as the kernel of the composite map

$$\eta :\ P \longrightarrow \operatorname{End}_K(V) \cong \operatorname{Mat}_\mu(K)$$

where η is the map defined in Remark 4.2.3.2. Moreover, the algorithm provides a vector space basis of $P/\operatorname{Ann}_P(V)$. To facilitate the formulation of this algorithm, we use the following convention. Given a matrix $\mathcal{A} = (a_{ij}) \in \operatorname{Mat}_\mu(K)$, we order its entries by letting $a_{ij} \prec a_{k\ell}$ if $i < k$, or if $i = k$ and $j < \ell$. In this way we "flatten" the matrix to a vector in K^{μ^2}. Then we can reduce $\mathcal{A}$ against a list of matrices by using the usual Gaußian reduction procedure.

Theorem 4.2.7 (The Buchberger-Möller Algorithm for Matrices).
Let σ be a term ordering on $\mathbb{T}^n$, and let $\mathcal{M}_1, \ldots, \mathcal{M}_n \in \operatorname{Mat}_\mu(K)$ be pairwise commuting matrices. Consider the following sequence of instructions.

M1. Start with empty lists $G = [\,]$, $\mathcal{O} = [\,]$, $S = [\,]$, $N = [\,]$, and a list $L = [1]$.

M2. *If $L = [\,]$, return the pair $(G, \mathcal{O})$ and stop. Otherwise let $t = \min_\sigma(L)$ and delete it from L.*

M3. *Compute $t(\mathcal{M}_1, \ldots, \mathcal{M}_n)$ and reduce it against $N = (\mathbb{N}_1, \ldots, \mathbb{N}_k)$ to obtain*

$$\mathcal{R} = t(\mathcal{M}_1, \ldots, \mathcal{M}_n) - \sum_{i=1}^{k} c_i \mathbb{N}_i \qquad \textit{with} \quad c_i \in K$$

M4. *If $\mathcal{R} = 0$, then append the polynomial $t - \sum_i c_i s_i$ to the list G, where s_i denotes the i^{th} element of S. Remove from L all multiples of t. Continue with step M2.*

M5. *If $\mathcal{R} \neq 0$, then append $\mathcal{R}$ to the list N and $t - \sum_i c_i s_i$ to the list S. Append the term t to $\mathcal{O}$, and append to L those elements of $\{x_1 t, \ldots, x_n t\}$ which are neither multiples of a term in L nor in $\mathrm{LT}_\sigma(G)$. Continue with step M2.*

This is an algorithm which returns the reduced σ-Gröbner basis G of $\mathrm{Ann}_P(V)$ and a list of terms $\mathcal{O}$ whose residue classes form a K-vector space basis of $P/\mathrm{Ann}_P(V)$.

Proof. Let $I = \mathrm{Ann}_P(V)$, and let H be the reduced σ-Gröbner basis of I.

First we prove termination. In each iteration either step M4 or step M5 is performed. By its construction, the list N always contains linearly independent matrices. Hence step M5, which appends an element to N, can be performed only finitely many times. By Dickson's Lemma (see [KR00], Corollary 1.3.6), step M4 can be performed only finitely many times. Thus the algorithm terminates.

To show correctness, we prove that after a term t has been treated by the algorithm, the following holds: the list G contains all elements of H whose leading terms are less than or equal to t, and the list $\mathcal{O}$ contains all elements of $\mathbb{T}^n \setminus \mathrm{LT}_\sigma(I)$ which are less than or equal to t.

This is true after the first term $t = 1$ has been treated, i.e. appended to $\mathcal{O}$. Now suppose that the algorithm has finished an iteration. By the method used to append new terms to L in step M5, all elements of the set $(x_1\mathcal{O} \cup \cdots x_n\mathcal{O}) \setminus (\mathcal{O} \cup \mathrm{LT}_\sigma(I))$ are contained in L. From this it follows that the next term t chosen in step M2 is the smallest term in $\mathbb{T}^n \setminus (\mathcal{O} \cup \mathrm{LT}_\sigma(I))$. Furthermore, the polynomials appended to S in step M5 are supported in $\mathcal{O}$. Hence the polynomial $t - \sum_{i=1}^k c_i s_i$ resulting from step M3 of the next iteration has leading term t.

Now suppose that $\mathcal{R} = 0$ in step M4. By construction, the matrix of the endomorphism $\eta(s_i)$ is $\mathbb{N}_i$ for $i = 1, \ldots, k$. Therefore the polynomial $g = t - \sum_{i=1}^k c_i s_i$ is an element of $I = \mathrm{Ann}_P(V)$. Since the support of $\sum_{i=1}^k c_i s_i$ is contained in $\mathcal{O}$, the polynomial g is a new element of H.

On the other hand, if $\mathcal{R} \neq 0$ in step M5, then we claim that the term t is not contained in $\mathrm{LT}_\sigma(I)$. In view of the way we update L in step M5, the term t is not in $\mathrm{LT}_\sigma(G)$ for the current list G. By induction, the term t is not a proper multiple of a term in $\mathrm{LT}_\sigma(H)$. Furthermore, the term t is not the leading term of an element of H because such an element would be of the form $t - \sum_{i=1}^{k} c_i' s_i \in I$ with $c_i' \in K$ in contradiction to $\mathcal{R} \neq 0$. Altogether it follows that t is an element of $\mathbb{T}^n \setminus \mathrm{LT}_\sigma(I)$ and can be appended to $\mathcal{O}$.

In both cases we see that the claim continues to hold. Therefore, when the algorithm terminates, we have computed the desired lists G and $\mathcal{O}$. □

Let us illustrate the performance of this algorithm with an example.

Example 4.2.8. Let $V = \mathbb{Q}^3$, and let $\mathcal{V} = (e_1, e_2, e_3)$ be its canonical basis. Since the two matrices

$$\mathcal{M}_1 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 1 \\ 0 & 1 & 1 \end{pmatrix} \quad \text{and} \quad \mathcal{M}_2 = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

commute, they define a $\mathbb{Q}[x,y]$-module structure on V. Let us follow the iterations of the algorithm in computing the reduced σ-Gröbner basis of $\mathrm{Ann}_P(V)$, where $\sigma = \mathtt{DegLex}$.

1. $t = 1$, $L = [\,]$, $\mathcal{R} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \mathcal{I}_3$, $N = [\mathcal{I}_3]$, $S = [1]$, $\mathcal{O} = [1]$, $L = [x, y]$.
2. $t = y$,$L = [x]$, $\mathcal{R} = \begin{pmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix} = \mathcal{M}_2$, $M = [\mathcal{I}_3, \mathcal{M}_2]$, $S = [1, y]$, $\mathcal{O} = [1, y]$, $L = [x, y^2]$.
3. $t = x$, $L = [y^2]$, $\mathcal{R} = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \mathcal{M}_1 - \mathcal{M}_2$, $M = [\mathcal{I}_2, \mathcal{M}_2, \mathcal{M}_1 - \mathcal{M}_2]$, $S = [1, y, x - y]$, $\mathcal{O} = [1, x, y]$, $L = [x^2, xy, y^2]$.
4. $t = y^2$, $L = [x^2, xy]$, $\mathcal{R} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \mathcal{M}_2^2 - \mathcal{M}_2 - (\mathcal{M}_1 - \mathcal{M}_2)$, $G = [y^2 - x]$.
5. $t = xy$, $L = [x^2]$, $\mathcal{R} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \mathcal{M}_1\mathcal{M}_2 - 2\mathcal{M}_2 - (\mathcal{M}_1 - \mathcal{M}_2)$, $G = [y^2 - x, xy - x - y]$.
6. $t = x^2$, $L = [\,]$, $\mathcal{R} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = \mathcal{M}_1^2 - 3\mathcal{M}_2 - 2(\mathcal{M}_1 - \mathcal{M}_2)$, $G = [y^2 - x,\ xy - x - y,\ x^2 - 2x - y]$.

Thus we have $\mathrm{Ann}_P(V) = (y^2 - x,\ xy - x - y,\ x^2 - 2x - y)$, and $\mathcal{O} = \{1, x, y\}$ represents a K-basis of $P/\mathrm{Ann}_P(V)$.

Now we are ready for the main algorithm of this subsection: we can check effectively whether a P-module structure given by commuting matrices defines a cyclic module.

Theorem 4.2.9 (Cyclicity Test).
Let V be a finite dimensional K-vector space with basis $\mathcal{V} = (v_1, \dots, v_m)$, and let $\varphi_1, \dots, \varphi_n$ be pairwise commuting endomorphisms of V given by their respective matrices $\mathcal{M}_1, \dots, \mathcal{M}_n$. We equip V with the P-module structure defined by $\varphi_1, \dots, \varphi_n$. Consider the following sequence of instructions.

C1. Using Theorem 4.2.7, compute a tuple of terms $\mathcal{O} = (t_1, \dots, t_\mu)$ whose residue classes form a K-basis of $P/\operatorname{Ann}_P(V)$.
C2. If $\dim_K(V) \neq \mu$, then return `"V is not cyclic"` *and stop.*
C3. Let $z_1, \dots, z_\mu$ be further indeterminates and $\mathcal{A} \in \operatorname{Mat}_\mu(K[z_1, \dots, z_\mu])$ the matrix whose columns are $t_i(\mathcal{M}_1, \dots, \mathcal{M}_n) \cdot (z_1, \dots, z_\mu)^{\mathrm{tr}}$ for $i = 1, \dots, \mu$. Compute the determinant $d = \det(\mathcal{A}) \in K[z_1, \dots, z_\mu]$.
C4. Check if there exists a tuple $(c_1, \dots, c_\mu) \in K^\mu$ such that the polynomial value $d(c_1, \dots, c_\mu)$ is non-zero. In this case return `"V is cyclic"` *and $w = c_1 v_1 + \dots + c_\mu v_\mu$. Then stop.*
C5. Return `"V is not cyclic"` *and stop.*

This is an algorithm which checks whether V is a cyclic P-module via $\varphi_1, \dots, \varphi_n$ and, in the affirmative case, computes a generator.

Proof. This procedure is clearly finite. Hence we only have to prove correctness. By Proposition 4.2.6, we have to check whether $\Psi_w : P/\operatorname{Ann}_P(V) \longrightarrow V$ is an isomorphism for some $w \in V$. For this it is necessary that the dimensions of the two vector spaces agree. This condition is checked in step C2. Then we use the basis elements $\{\bar{t}_1, \dots, \bar{t}_\mu\}$ and examine their images for linear independence. Since we have $\Psi_w(\bar{t}_i) = t_i(\varphi_1, \dots, \varphi_n)(w)$ for $i = 1, \dots, \mu$, the map Ψ_w is an isomorphism for some $w \in V$ if and only if the vectors $\{t_i(\mathcal{M}_1, \dots, \mathcal{M}_n)(c_1, \dots, c_\mu)^{\mathrm{tr}} \mid 1 \le i \le \mu\}$ are K-linearly independent for some tuple $(c_1, \dots, c_\mu) \in K^\mu$. This is checked in step C4. $\square$

If the field K is infinite, the check in step C4 can be simplified to checking $d \neq 0$. For a finite field K, we can, in principle, check all tuples in K^μ. Let us apply this algorithm by applying it in the setting of Example 4.2.8.

Example 4.2.10. Let V and $\mathcal{M}_1, \mathcal{M}_2$ be defined as in Example 4.2.8. We follow the steps of the cyclicity test.

C1. The residue classes of $\mathcal{O} = \{1, x, y\}$ form a K-basis of $P/\operatorname{Ann}_P(V)$.
C2. We have $\mu = 3 = \dim_{\mathbb{Q}}(V)$.
C3. We compute $\mathcal{I}_3 \cdot (z_1, z_2, z_3)^{\mathrm{tr}} = (z_1, z_2, z_3)^{\mathrm{tr}}$ as well as $\mathcal{M}_1 \cdot (z_1, z_2, z_3)^{\mathrm{tr}} = (z_2 + z_3, 2z_2 + z_3, z_2 + z_3)^{\mathrm{tr}}$ and $\mathcal{M}_2 \cdot (z_1, z_2, z_3)^{\mathrm{tr}} = (z_2, z_2 + z_3, z_2)^{\mathrm{tr}}$. Thus we let $\mathcal{A} = \begin{pmatrix} z_1 & z_2 + z_3 & z_2 \\ z_2 & 2z_2 + z_3 & z_2 + z_3 \\ z_3 & z_2 + z_3 & z_2 \end{pmatrix}$ and calculate $d = \det(\mathcal{A}) = (z_1 - z_3)(z_2^2 - z_2 z_3 - z_3^2)$.
C4. Since K is infinite and $d \neq 0$, the algorithm returns `"V is cyclic"`. For instance, since $d(1, 1, 0) = 1$, the element $w = e_1 + e_2$ generates V as a P-module.

The following example shows that V can fail to be cyclic even when the dimensions of V and $P/\operatorname{Ann}_P(V)$ agree.

Example 4.2.11. Let $V = \mathbb{Q}^3$, and let $\mathcal{V} = (e_1, e_2, e_3)$ be its canonical basis. We equip V with the $\mathbb{Q}[x,y]$-module structure defined by the commuting matrices

$$\mathcal{M}_1 = \begin{pmatrix} 0&0&0\\ 1&0&0\\ 0&0&0 \end{pmatrix} \quad \text{and} \quad \mathcal{M}_2 = \begin{pmatrix} 0&0&0\\ 0&0&1\\ 0&0&0 \end{pmatrix}$$

Let us apply the cyclicity test step-by-step.

C1. The algorithm of Theorem 4.2.7 yields $\mathcal{O} = \{1, x, y\}$.
C2. We have $\mu = 3 = \dim_{\mathbb{Q}}(V)$.
C3. We calculate $\mathcal{A} = \begin{pmatrix} z_1 & 0 & 0\\ z_2 & z_1 & z_3\\ z_3 & 0 & 0 \end{pmatrix}$ and $d = \det(\mathcal{A}) = 0$.
C5. The algorithm returns `"V is not cyclic"`.

We end this section by considering the special case $n = 1$. In this univariate case some of the topics discussed in this section look very familiar.

Example 4.2.12. Suppose we are given a finitely generated K-vector space V and an endomorphism φ of V. We let $P = K[x]$ and observe that V becomes a P-module via the rule $(f, v) \mapsto f(\varphi)(v)$. When is it a cyclic P-module? Let us interpret the meaning of the steps of our cyclicity test in the univariate case. To start with, let $\mathcal{M}$ be a matrix representing φ.

C1. The algorithm of Theorem 4.2.7 applied to $\mathcal{M}$ yields a monic polynomial $f(x) = x^d + c_{d-1}x^{d-1} + \cdots + c_0$, which is the *minimal polynomial* of $\mathcal{M}$ (and of φ), and the tuple $\mathcal{O} = (1, x, x^2, \ldots, x^{d-1})$.
C2. The minimal polynomial of $\mathcal{M}$ is a divisor of the characteristic polynomial of $\mathcal{M}$, and the degree of the latter is $\dim_K(V)$. So the algorithm stops at step C2 only if the minimal polynomial and the characteristic polynomial differ.
C3. The matrix $\mathcal{A}$ can be interpreted as the matrix whose columns are the vectors $v, \varphi(v), \ldots, \varphi^{d-1}(v)$ for a generic v. If $\det(\mathcal{A}) = 0$, then the endomorphisms $1, \varphi, \ldots, \varphi^{d-1}$ are linearly dependent, a contradiction. Hence $\det(\mathcal{M})$ necessarily is non-zero and V is a cyclic P-module.

In conclusion, steps C3, C4, C5 are redundant in the univariate case. This corresponds to the well-known fact that V is a cyclic $K[x]$-module if and only if the minimal polynomial and the characteristic polynomial of φ coincide.

4.3 Border prebases

Given a zero-dimensional polynomial ideal I, we want to study the residue class ring P/I by choosing a K-basis and examining the multiplication matrices with respect to that basis. How can we find a basis having "nice" properties? One possibility is to take the residue classes of the terms in an order ideal, i.e. in a finite set of terms which is closed under forming divisors.

The choice of an order ideal $\mathcal{O}$ yields additional structure on the monoid of terms $\mathbb{T}^n$. For instance, there are terms forming the border of $\mathcal{O}$, i.e. terms t outside $\mathcal{O}$ such that there exist an indeterminate x_i and a term t' in $\mathcal{O}$ with $t = x_i t'$. Moreover, every term t has an $\mathcal{O}$-index which measures the distance from t to $\mathcal{O}$. The properties of order ideals, borders, and $\mathcal{O}$-indices are collected in the first subsection.

The second subsection deals with $\mathcal{O}$-border prebases. These are sets of polynomials each of which consists of one term in the border of $\mathcal{O}$ and a linear combination of terms in $\mathcal{O}$. Using $\mathcal{O}$-border prebases, we construct a division algorithm and define normal remainders.

4.3.1 Order ideals

Let $\mathbb{T}^n$ denote the monoid of terms in n indeterminates. Moreover, for every $d \geq 0$, we let $\mathbb{T}^n_d$ be the set of terms of degree d and $\mathbb{T}^n_{<d} = \bigcup_{i=0}^{d-1} \mathbb{T}^n_i$. The following kind of subset of $\mathbb{T}^n$ is central to this paper.

Definition 4.3.1. *A non-empty, finite set of terms $\mathcal{O} \subset \mathbb{T}^n$ is called an* **order ideal** *if it is closed under forming divisors, i.e. if $t \in \mathcal{O}$ and $t' \mid t$ imply $t' \in \mathcal{O}$.*

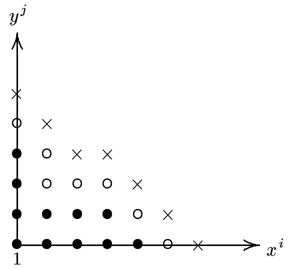
Order ideals have many other names in the literature. For instance, statisticians sometimes call them **complete sets of estimable terms** (see Section 4.5). In Chapter 3, the more general notion of "sets of polynomials connected to 1" is used.

Definition 4.3.2. *Let $\mathcal{O} \subset \mathbb{T}^n$ be an order ideal.*

1. *The* **border** *of $\mathcal{O}$ is the set*
$$\partial\mathcal{O} = \mathbb{T}^n_1 \cdot \mathcal{O} \setminus \mathcal{O} = (x_1\mathcal{O} \cup \cdots \cup x_n\mathcal{O}) \setminus \mathcal{O}$$
The **first border closure** *of $\mathcal{O}$ is the set $\overline{\partial\mathcal{O}} = \mathcal{O} \cup \partial\mathcal{O}$.*
2. *For every $k \geq 1$, we inductively define the $(k+1)^{\text{st}}$* **border** *of $\mathcal{O}$ by $\partial^{k+1}\mathcal{O} = \partial(\overline{\partial^k\mathcal{O}})$ and the $(k+1)^{\text{st}}$* **border closure** *of $\mathcal{O}$ by the rule $\overline{\partial^{k+1}\mathcal{O}} = \overline{\partial^k\mathcal{O}} \cup \partial^{k+1}\mathcal{O}$. For convenience, we let $\partial^0\mathcal{O} = \overline{\partial^0\mathcal{O}} = \mathcal{O}$.*

The k^{th} border closure of an order ideal $\mathcal{O}$ is an order ideal for every $k \geq 0$. In Chapter 3, the k^{th} border of $\mathcal{O}$ is denoted by $\mathcal{O}^{[k]}$.

Example 4.3.3. Let $\mathcal{O}$ be the order ideal $\{1, x, y, x^2, xy, y^2, x^3, x^2y, y^3, x^4, x^3y\}$ in $\mathbb{T}^2$. Then we visualize $\mathcal{O}$ and its first two borders as follows.



Let us collect some properties of order ideals, their borders and border closures.

Proposition 4.3.4 (Basic Properties of Borders).
Let $\mathcal{O} \subset \mathbb{T}^n$ be an order ideal.

1. *For every $k \geq 0$, we have a disjoint union $\overline{\partial^k \mathcal{O}} = \bigcup_{i=0}^{k} \partial^i \mathcal{O}$.*
2. *For every $k \geq 1$, we have $\partial^k \mathcal{O} = \mathbb{T}^n_k \cdot \mathcal{O} \setminus \mathbb{T}^n_{<k} \cdot \mathcal{O}$.*
3. *We have a disjoint union $\mathbb{T}^n = \bigcup_{i=0}^{\infty} \partial^i \mathcal{O}$.*
4. *A term $t \in \mathbb{T}^n$ is divisible by a term in $\partial \mathcal{O}$ if and only if $t \in \mathbb{T}^n \setminus \mathcal{O}$.*

Proof. The definition of the first border closure of $\mathcal{O}$ yields $\overline{\partial \mathcal{O}} = \mathcal{O} \cup \mathbb{T}^n_1 \cdot \mathcal{O}$. Inductively, it follows that $\overline{\partial^{k+1} \mathcal{O}} = \overline{\partial^k \mathcal{O}} \cup \mathbb{T}^n_1 \cdot \overline{\partial^k \mathcal{O}} \cup = \overline{\partial^k \mathcal{O}} \cup \mathbb{T}^n_{k+1} \mathcal{O}$. This proves the first claim. Then the second claim is a consequence of the equality $\partial^{k+1} \mathcal{O} = \overline{\partial^{k+1} \mathcal{O}} \setminus \overline{\partial^k \mathcal{O}}$. The third claim follows from the observation that every term is in $\overline{\partial^k \mathcal{O}}$ for some $k \geq 0$.

Finally, the fourth claim holds because the second claim implies the fact that $t \in \partial^k \mathcal{O}$ for some $k \geq 1$ is equivalent to the existence of a factorization $t = t't''$ where $\deg(t') = k - 1$ and $t'' \in \partial \mathcal{O}$. □

The above partition of $\mathbb{T}^n$ allows us to define a "distance" between a term and an order ideal.

Definition 4.3.5. *Let $\mathcal{O} \subset \mathbb{T}^n$ be an order ideal.*

1. *For every $t \in \mathbb{T}^n$, there exists a unique number $k \in \mathbb{N}$ such that $t \in \partial^k \mathcal{O}$. We call k the* **index** *of t with respect to $\mathcal{O}$ and write $\operatorname{ind}_{\mathcal{O}}(t) = k$.*
2. *For an arbitrary polynomial $f \in P \setminus \{0\}$, we define the* **index** *of f with respect to $\mathcal{O}$ by $\operatorname{ind}_{\mathcal{O}}(f) = \max\{\operatorname{ind}_{\mathcal{O}}(t) \mid t \in \operatorname{Supp}(f)\}$.*

By this definition, the k^{th} border of $\mathcal{O}$ consists precisely of the terms of index k. Notice that every polynomial $f \in P \setminus \{0\}$ has a representation $f = c_1 t_1 + \cdots + c_s t_s$ where $c_1, \ldots, c_s \in K \setminus \{0\}$ and such that $t_1, \ldots, t_s \in \mathbb{T}^n$ satisfy $\operatorname{ind}_{\mathcal{O}}(t_1) \geq \cdots \geq \operatorname{ind}_{\mathcal{O}}(t_s)$. However, this representation is in general not unique since several terms in the support of f may have the same index with respect to $\mathcal{O}$.

Let us point out some of the most useful properties of the index.

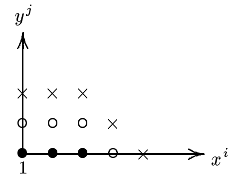
Proposition 4.3.6. *Let $\mathcal{O} \subset \mathbb{T}^n$ be an order ideal.*

1. *For a term $t \in \mathbb{T}^n$, the number $k = \mathrm{ind}_{\mathcal{O}}(t)$ is the smallest natural number such that $t = t't''$ with a term $t' \in \mathbb{T}^n$ of degree k and with $t'' \in \mathcal{O}$.*
2. *Given two terms $t, t' \in \mathbb{T}^n$, we have $\mathrm{ind}_{\mathcal{O}}(t\,t') \leq \deg(t) + \mathrm{ind}_{\mathcal{O}}(t')$.*
3. *For $f, g \in P \setminus \{0\}$ such that $f + g \neq 0$, we have*
$$\mathrm{ind}_{\mathcal{O}}(f+g) \leq \max\{\mathrm{ind}_{\mathcal{O}}(f), \mathrm{ind}_{\mathcal{O}}(g)\}$$
4. *For $f, g \in P \setminus \{0\}$, we have*
$$\mathrm{ind}_{\mathcal{O}}(f\,g) \leq \min\{\deg(f) + \mathrm{ind}_{\mathcal{O}}(g), \deg(g) + \mathrm{ind}_{\mathcal{O}}(f)\}$$

Proof. The first claim follows from the proof of Proposition 4.3.4.4. The second claim follows from the first. The third claim is a consequence of the inclusion $\mathrm{Supp}\,(f+g) \subseteq \mathrm{Supp}\,(f) \cup \mathrm{Supp}\,(g)$. The last claim follows from the observation that $\mathrm{Supp}\,(fg) \subseteq \{t't'' \mid t' \in \mathrm{Supp}\,(f),\ t'' \in \mathrm{Supp}\,(g)\}$ and from the second claim. □

Although the partial ordering on $\mathbb{T}^n$ defined by the index appears similar to a term ordering, it has a serious drawback: this ordering is incompatible with term multiplication, i.e. $\mathrm{ind}_{\mathcal{O}}(t) \geq \mathrm{ind}_{\mathcal{O}}(t')$ does not, in general, imply $\mathrm{ind}_{\mathcal{O}}(t\,t'') \geq \mathrm{ind}_{\mathcal{O}}(t'\,t'')$. Our next example is a case in point.

Example 4.3.7. Let $\mathcal{O} = \{1, x, x^2\} \subset \mathbb{T}(x,y)$. Then $\mathcal{O}$ is an order ideal with border $\partial\mathcal{O} = \{y, xy, x^2y, x^3\}$. The following sketch illustrates the situation.



Multiplying the terms on both sides of the inequality $\mathrm{ind}_{\mathcal{O}}(y) > \mathrm{ind}_{\mathcal{O}}(x^2)$ by x^2, we get $\mathrm{ind}_{\mathcal{O}}(x^2 \cdot y) < \mathrm{ind}_{\mathcal{O}}(x^2 \cdot x^2)$. Similarly, if we multiply the terms on both sides of the equality $\mathrm{ind}_{\mathcal{O}}(y) = \mathrm{ind}_{\mathcal{O}}(x^2 y)$ by x, we get the inequality $\mathrm{ind}_{\mathcal{O}}(x \cdot y) < \mathrm{ind}_{\mathcal{O}}(x \cdot x^2 y)$.

4.3.2 Border division

In this subsection we introduce an important tool for dealing with zero-dimensional ideals: an $\mathcal{O}$-border prebasis, i.e. a set of polynomials of which each is a linear combination of one term in $\partial\mathcal{O}$ and terms in $\mathcal{O}$. In this way we imitate the definition of a Gröbner basis where each polynomial is a linear combination of the leading term and smaller terms. Then we present a process for dividing arbitrary polynomials by those of an $\mathcal{O}$-border prebasis. However, the remainder of this division process is not uniquely determined. This indicates that $\mathcal{O}$-border prebases are a first step in the right direction and that we must take one more step in the next section.

Definition 4.3.8. *Let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal, and let $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$ be its border. A set of polynomials $G = \{g_1, \ldots, g_\nu\}$ is called an $\mathcal{O}$-**border prebasis** if the polynomials have the form $g_j = b_j - \sum_{i=1}^{\mu} \alpha_{ij} t_i$ such that $\alpha_{ij} \in K$ for $1 \le i \le \mu$ and $1 \le j \le \nu$.*

In particular, a border prebasis can be interpreted as a tuple of polynomials *marked* by the border terms $(b_1, \ldots, b_\nu)$ in the following sense.

Definition 4.3.9. *A pair (g, b) is said to be a **marked polynomial** if g is a non-zero polynomial and $b \in \mathrm{Supp}\,(g)$ with coefficient 1. A tuple of polynomials $(g_1, \ldots, g_\nu)$ is **marked** by a tuple of terms $(b_1, \ldots, b_\nu)$ if $(g_1, b_1), \ldots, (g_\nu, b_\nu)$ are marked polynomials.*

The definition of a border prebasis only fixes the shape of our generators. Note that this notion requires a bit more than that of marked polynomials – the unmarked terms in the polynomial's support have to be in the order ideal. Border prebases are already sufficient to perform polynomial division with remainder. The following algorithm provides a fundamental tool in working with border prebases. It is similar to the procedure called "B-reduction" in Chapter 3.

Proposition 4.3.10 (Border Division Algorithm).
Let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal, let $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$ be its border, and let $\{g_1, \ldots, g_\nu\}$ be an $\mathcal{O}$-border prebasis. Given a polynomial $f \in P$, consider the following instructions.

D1. Let $f_1 = \cdots = f_\nu = 0$, $c_1 = \cdots = c_\mu = 0$, and $h = f$.
D2. If $h = 0$, then return $(f_1, \ldots, f_\nu, c_1, \ldots, c_\mu)$ and stop.
D3. If $\mathrm{ind}_\mathcal{O}(h) = 0$, then find $c_1, \ldots, c_\mu \in K$ such that $c_1 t_1 + \cdots + c_\mu t_\mu = h$. Return $(f_1, \ldots, f_\nu, c_1, \ldots, c_\mu)$ and stop.
D4. If $\mathrm{ind}_\mathcal{O}(h) > 0$, then let $h = a_1 h_1 + \cdots + a_s h_s$ such that $a_1, \ldots, a_s \in K \setminus \{0\}$ and $h_1, \ldots, h_s \in \mathbb{T}^n$ satisfy $\mathrm{ind}_\mathcal{O}(h_1) = \mathrm{ind}_\mathcal{O}(h)$. Determine the smallest index $i \in \{1, \ldots, \nu\}$ such that h_1 factors as $h_1 = t'\, b_i$ and so that the term $t' \in \mathbb{T}^n$ has degree $\mathrm{ind}_\mathcal{O}(h) - 1$. Subtract $a_1 t' g_i$ from h, add $a_1 t'$ to f_i, and continue with step D2.

This is an algorithm which returns a tuple $(f_1, \ldots, f_\nu, c_1, \ldots, c_\mu) \in P^\nu \times K^\mu$ such that

$$f = f_1 g_1 + \cdots + f_\nu g_\nu + c_1 t_1 + \cdots + c_\mu t_\mu$$

and $\deg(f_i) \le \mathrm{ind}_\mathcal{O}(f) - 1$ for all $i \in \{1, \ldots, \nu\}$ with $f_i g_i \ne 0$. This representation does not depend on the choice of the term h_1 in Step D4.

For the reader's convenience we reproduce the proof from [KK03a].

Proof. First we show that Step D4 can be executed. Let $k = \mathrm{ind}_\mathcal{O}(h_1)$. By Proposition 4.3.4.2, there is a factorization $h_1 = \tilde{t}\, t_i$ for some term $\tilde{t}$ of degree k and some $t_i \in \mathcal{O}$, and there is no such factorization with a term $\tilde{t}$ of smaller degree. Since $k > 0$, we can write $\tilde{t} = t'\, x_j$ for some $t' \in \mathbb{T}^n$ and $j \in \{1,\ldots,n\}$. Then we have $\deg(t') = k-1$, and the fact that $\tilde{t}$ has the smallest possible degree implies $x_j\, t_i \in \partial\mathcal{O}$. Thus we have $h_1 = t'\,(x_j\, t_i) = t'\, b_k$ for some $b_k \in \partial\mathcal{O}$.

Next we prove termination. We show that Step D4 is performed only finitely many times. Let us investigate the subtraction $h - a_1 t' g_i$ in Step D4. Using the representation $g_i = b_i - \sum_{k=1}^{\mu} \alpha_{ki} t_k$ given in Definition 4.3.8, this subtraction becomes

$$h - a_1 t' g_i = a_1 h_1 + \cdots + a_s h_s - a_1 t' b_i + a_1 t' \sum_{k=1}^{\mu} \alpha_{ki} t_k$$

Now $a_1 h_1 = a_1 t' b_i$ shows that a term of index $\mathrm{ind}_{\mathcal{O}}(h)$ is removed from h and replaced by terms of the form $t'\, t_l \in \overline{\partial^{k-1}\mathcal{O}}$ which have strictly smaller index. The algorithm terminates after finitely many steps because, for a given term, there are only finitely many terms of smaller or equal index.

Finally, we prove correctness. To this end, we show that the equation

$$f = \ h \ + f_1 g_1 + \cdots + f_\nu g_\nu + c_1 t_1 + \cdots + c_\mu t_\mu$$

is an invariant of the algorithm. It is satisfied at the end of Step D1. A polynomial f_i is only changed in Step D4. There the subtraction $h - a_1 t' g_i$ is compensated by the addition $(f_i + a_1 t')g_i$. The constants $c_1,\ldots,c_\mu$ are only changed in Step D3 in which h is replaced by the expression $c_1 t_1 + \cdots + c_\mu t_\mu$. When the algorithm stops, we have $h = 0$. This proves the stated representation of f. The additional claim that this representation does not depend on the choice of h_1 in Step D4 follows from the observation that h_1 is replaced by terms of strictly smaller index. Thus the different executions of Step D4 corresponding to the reduction of several terms of a given $\mathcal{O}$-index in h do not interfere with one another, and the final result – after all those terms have been rewritten – is independent of the order in which they are taken care of. □

Notice that in Step D4 the algorithm uses a representation of h which is not necessarily unique. Moreover, to make the factorization of h_1 unique, we chose the index i minimally, but this choice had not been forced upon us. Finally, the result of the division depends on the numbering of the elements of $\partial\mathcal{O}$, as our next example shows.

Example 4.3.11. Let $n = 2$, and let $\mathcal{O} = \{t_1, t_2, t_3\}$ with $t_1 = 1$, $t_2 = x$, and $t_3 = y$. Then the border of $\mathcal{O}$ is $\partial\mathcal{O} = \{b_1, b_2, b_3\}$ with $b_1 = x^2$, $b_2 = xy$, and $b_3 = y^2$. The polynomials $g_1 = x^2 + x + 1$, $g_2 = xy + y$, and $g_3 = y^2 + x + 1$ constitute an $\mathcal{O}$-border prebasis. We want to divide the polynomial $f = x^3y^2 - xy^2 + x^2 + 2$ by this $\mathcal{O}$-border prebasis.

For easy reference, the next borders are $\partial^2\mathcal{O} = \{x^3, x^2y, xy^2, y^3\}$, $\partial^3\mathcal{O} = \{x^4, x^3y, x^2y^2, xy^3, y^4\}$, and $\partial^4\mathcal{O} = \{x^5, x^4y, x^3y^2, x^2y^3, xy^4, y^5\}$. We apply the Border Division Algorithm and follow its steps.

D1. Let $f_1 = f_2 = f_3 = 0$, $c_1 = c_2 = c_3 = 0$, and $h = x^3y^2 - xy^2 + x^2 + 2$. The $\mathcal{O}$-indices of the terms in h are 4,2,1 and 0 respectively, so h has index 4.
D4. We have $x^3y^2 = xy^2 \cdot b_1$ with $\deg xy^2 = \mathrm{ind}(h) - 1$. Thus we put $f_1 = xy^2$ and $h = x^3y^2 - xy^2 + x^2 + 2 - xy^2(x^2 + x + 1)$. The terms in the support of $h = -x^2y^2 - 2xy^2 + x^2 + 2$ have $\mathcal{O}$-indices 3,2,1 and 0 respectively.
D4. We have $x^2y^2 = y^2 \cdot b_1$ with $\deg y^2 = \mathrm{ind}(h) - 1$. Add $-y^2$ to f_1 to obtain $f_1 = xy^2 - y^2$ and put $h = -x^2y^2 - 2xy^2 + x^2 + 2 + y^2(x^2 + x + 1)$. The terms in the support of $h = -xy^2 + x^2 + y^2 + 2$ have $\mathcal{O}$-indices 2,1,1 and 0 respectively.
D4. We have $xy^2 = y \cdot b_2$ with $\deg y = \mathrm{ind}(h) - 1$. Put $f_2 = -y$ and put $h = -xy^2 + x^2 + y^2 + 2 + y(xy + y)$. The terms in the support of $h = x^2 + 2y^2 + 2$ have $\mathcal{O}$-indices 1,1 and 0 respectively.
D4. We have $x^2 = 1 \cdot b_1$ with $\deg 1 = \mathrm{ind}(h) - 1$. Add 1 to f_1 to obtain $f_1 = xy^2 - y^2 + 1$ and put $h = x^2 + 2y^2 + 2 - 1(x^2 + x + 1)$. The terms in the support of $h = 2y^2 - x + 1$ have $\mathcal{O}$-indices 1,0 and 0 respectively.
D4. We have $y^2 = 1 \cdot b_3$ with $\deg 1 = \mathrm{ind}(h) - 1$. Add 2 to f_3 to obtain $f_3 = 2$ and put $h = 2y^2 - x + 1 - 2(y^2 + x + 1)$. The terms in the support of $h = -3x - 1$ have $\mathcal{O}$-indices 0 and 0. Thus $\mathrm{ind}_{\mathcal{O}}(h) = 0$.
D3. We have $h = -1 \cdot t_1 - 3t_2 + 0t_3$. The algorithm returns the following tuple $(xy^2 - y^2 + 1, -y, 2, 1, -3, 0)$ and stops.

Therefore we have a representation

$$f = (xy^2 - y^2 + 1)g_1 - y\, g_2 + 2\, g_3 - 1\, t_1 - 3\, t_2 + 0\, t_3$$

Second we perform the algorithm with respect to the shuffled tuple $(g_1', g_2', g_3') = (g_3, g_2, g_1)$.

D1. Let $f_1 = f_2 = f_3 = 0$, $c_1 = c_2 = c_3 = 0$, and $h = x^3y^2 - xy^2 + x^2 + 2$. The $\mathcal{O}$-indices of the terms in in the support of h are 4,2,1 and 0 respectively, so h has index 4.
D4. We have $x^3y^2 = x^3 \cdot b_1'$ with $\deg x^3 = \mathrm{ind}(h) - 1$. Thus we put $f_1' = x^3$ and $h = x^3y^2 - xy^2 + x^2 + 2 - x^3(y^2 + x + 1)$. The terms in the support of $h = -x^4 - x^3 - xy^2 + x^2 + 2$ have $\mathcal{O}$-indices 3,2,2,1 and 0 respectively.
D4. We have $x^4 = x^2 \cdot b_3'$ with $\deg x^2 = \mathrm{ind}(h) - 1$. Add $-x^2$ to f_3' to obtain $f_3' = x^2$ and put $h = -x^4 - x^3 - xy^2 + x^2 + 2 + x^2(x^2 + x + 1)$. The terms in the support of $h = -xy^2 + 2x^2 + 2$ have $\mathcal{O}$-indices 2,1, and 0 respectively.
D4. We have $xy^2 = x \cdot b_1'$ with $\deg x = \mathrm{ind}(h) - 1$. Add x to f_1' to obtain $f_1' = x^3 + x$ and put $h = -xy^2 + 2x^2 + 2 + x(y^2 + y + 1)$. The terms in the support of $h = 2x^2 + xy + x + 2$ have $\mathcal{O}$-indices 1,1,0 and 0 respectively.
D4. We have $x^2 = 1 \cdot b_3'$ with $\deg 1 = \mathrm{ind}(h) - 1$. Add 2 to f_3' to obtain $f_3' = x^2 + 2$ and put $h = 2x^2 + xy + x + 2 - 2(x^2 + x + 1)$. The terms in the support of $h = xy - x$ have $\mathcal{O}$-indices 1 and 0 respectively.
D4. We have $xy = 1 \cdot b_2'$ with $\deg 1 = \mathrm{ind}(h) - 1$. Add 1 to f_2' to obtain $f_2' = 1$ and put $h = xy - x - 1(xy + y)$. The terms in the support of $h = x - y$ have $\mathcal{O}$-indices 0 and 0. Thus we have $\mathrm{ind}_{\mathcal{O}}(h) = 0$.

D3. We write $h = 0t_1 + 1t_2 - 1t_3$. The algorithm returns the following tuple $(x^3 + x,\ -1,\ x^3 + x, 0,\ 1,\ -1)$ and stops.

Therefore we have a representation

$$\begin{aligned} f &= (x^3 + x)g'_1 - 1\,g'_2 + (x^2 + 2)\,g'_3 + 1\,t_1 - 3\,t_2 - 1\,t_3 \\ &= (x^2 + 2)g_1 - 1\,g_2 + (x^3 + x)\,g_3 + 0\,t_1 + 1\,t_2 - 1\,t_3 \end{aligned}$$

These calculations show that the order of the polynomials does affect the outcome of the Border Division Algorithm.

If we fix the tuple $(g_1, \dots, g_\nu)$ then the result of the Border Division Algorithm is uniquely determined. The given polynomial f is represented in $P/(g_1, \dots, g_\nu)$ by the residue class of the linear combination $c_1t_1 + \cdots + c_\mu t_\mu$. We introduce a name for this linear combination.

Definition 4.3.12. *Let $\mathcal{O}=\{t_1, \dots, t_\mu\}$ be an order ideal, let $G = \{g_1, \dots, g_\nu\}$ be an $\mathcal{O}$-border prebasis, and let $\mathcal{G} = (g_1, \dots, g_\nu)$. The* **normal $\mathcal{O}$-remainder** *of a polynomial f with respect to $\mathcal{G}$ is*

$$\mathrm{NR}_{\mathcal{O},\mathcal{G}}(f) = c_1t_1 + \cdots + c_\mu t_\mu$$

where $f = f_1g_1 + \cdots + f_\nu g_\nu + c_1t_1 + \cdots + c_\mu t_\mu$ is the representation computed by the Border Division Algorithm.

Example 4.3.13. Let $\mathcal{G} = (g_1, g_2, g_3)$ and $\mathcal{G}' = (g'_1, g'_2, g'_3)$ be the tuples considered in Example 4.3.11. The above computations lead to

$$\mathrm{NR}_{\mathcal{O},\mathcal{G}}(f) = -3x - 1 \quad \text{and} \quad \mathrm{NR}_{\mathcal{O},\mathcal{G}'}(f) = x - y$$

So the normal $\mathcal{O}$-remainder depends on the ordering of the polynomials in $\mathcal{G}$. In the next section we shall encounter a special kind of border prebasis for which this unwanted dependence disappears.

An important consequence of the Border Division Algorithm is that the residue classes of the elements of $\mathcal{O}$ generate $P/(g_1, \dots, g_\nu)$ as a K-vector space. But, as the above examples show, this system of generators is not necessarily a basis.

Corollary 4.3.14. *Let $\mathcal{O}=\{t_1, \dots, t_\mu\}$ be an order ideal and $G = \{g_1, \dots, g_\nu\}$ an $\mathcal{O}$-border prebasis. Then the residue classes of the elements of $\mathcal{O}$ generate $P/(g_1, \dots, g_\nu)$ as a K-vector space. More precisely, the residue class of every polynomial $f \in P$ can be represented as a linear combination of the residue classes $\{\bar{t}_1, \dots, \bar{t}_\nu\}$ by computing the normal remainder $\mathrm{NR}_{\mathcal{O},\mathcal{G}}(f)$ for $\mathcal{G} = (g_1, \dots, g_\nu)$.*

4.4 Border bases

After all these preparations we are ready to introduce the fundamental notion of this article: border bases. They are special systems of generators of zero-dimensional ideals which do not depend on the choice of a term ordering, but the choice of an order ideal. We discuss their existence and uniqueness and compare them to Gröbner bases of the given ideal. Then we show how one can use border bases to define normal forms, and we characterize border bases by the property that the associated multiplication matrices are pairwise commuting.

4.4.1 Existence and uniqueness of border bases

As above, let $P = K[x_1, \ldots, x_n]$ be a polynomial ring over a field K. Moreover, let I be a zero-dimensional ideal in P.

Definition 4.4.1. *Let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal and $G = \{g_1, \ldots, g_\nu\}$ an $\mathcal{O}$-border prebasis consisting of polynomials in I. We say that the set G is an* $\mathcal{O}$-**border basis** *of I if the residue classes of $t_1, \ldots, t_\mu$ form a K-vector space basis of P/I.*

Next we see that this definition implies that an $\mathcal{O}$-border basis of I actually generates I.

Proposition 4.4.2. *Let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal, and let G be an $\mathcal{O}$-border basis of I. Then I is generated by G.*

Proof. By definition, we have $(g_1, \ldots, g_\nu) \subseteq I$. To prove the converse inclusion, let $f \in I$. Using the Border Division Algorithm 4.3.10, the polynomial f can be expanded as $f = f_1 g_1 + \cdots + f_\nu g_\nu + c_1 t_1 + \cdots + c_\mu t_\mu$, where $f_1, \ldots, f_\nu \in P$ and $c_1, \ldots, c_\mu \in K$. This implies the equality of residue classes $0 = \bar{f} = c_1 \bar{t}_1 + \cdots + c_\mu \bar{t}_\mu$ in P/I. By assumption, the residue classes $\bar{t}_1, \ldots, \bar{t}_\mu$ form a K-vector space basis. Hence $c_1 = \cdots = c_\mu = 0$, and the expansion of f turns out to be $f = f_1 g_1 + \cdots + f_\nu g_\nu$. This completes the proof. □

Remark 4.4.3. Let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal and G an $\mathcal{O}$-border prebasis which generates an ideal I. We let $\langle \mathcal{O} \rangle_K = Kt_1 + \cdots + Kt_\mu$ be the vector subspace of P generated by $\mathcal{O}$. Then Corollary 4.3.14 shows that the residue classes of the elements of $\mathcal{O}$ generate P/I. Since the border basis property requires that these residue classes are linearly independent, the following conditions are equivalent.

1. The set G is an $\mathcal{O}$-border basis of I.
2. We have $I \cap \langle \mathcal{O} \rangle_K = \{0\}$.
3. We have $P = I \oplus \langle \mathcal{O} \rangle_K$.

Having defined a new mathematical object, it is natural to look for its existence and possibly its uniqueness. In the following theorem, we mention the field of definition of an ideal. For a discussion on this concept, see [KR00], Section 2.4. Furthermore, given an ideal $I \subseteq P$ and a term ordering σ, we denote the order ideal $\mathbb{T}^n \setminus \mathrm{LT}_\sigma(I)$ by $\mathcal{O}_\sigma(I)$.

Theorem 4.4.4 (Existence and Uniqueness of Border Bases).
Let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal, let I be a zero-dimensional ideal in P, and assume that the residue classes of the elements in $\mathcal{O}$ form a K-vector space basis of P/I.

1. *There exists a unique $\mathcal{O}$-border basis G of I.*
2. *Let G' be an $\mathcal{O}$-border prebasis whose elements are in I. Then G' is the $\mathcal{O}$-border basis of I.*
3. *Let k be the field of definition of I. Then we have $G \subset k[x_1, \ldots, x_n]$.*

Proof. First we prove Claim 1. Let $\partial\mathcal{O} = \{b_1, \ldots, b_\nu\}$. For every $i \in \{1, \ldots, \nu\}$, the hypothesis implies that the residue class of b_i in P/I is linearly dependent on the residue classes of the elements of $\mathcal{O}$. Therefore I contains a polynomial of the form $b_i - \sum_{j=1}^{\mu} \alpha_{ij} t_j$ such that $\alpha_{ij} \in K$. Then $G = \{g_1, \ldots, g_\nu\}$ is an $\mathcal{O}$-border prebasis, and hence an $\mathcal{O}$-border basis of I by Definition 4.4.1. Let $G' = \{g'_1, \ldots, g'_\nu\}$ be another $\mathcal{O}$-border basis of I. If, for contradiction, there exists a term $b \in \partial\mathcal{O}$ such that the polynomials in G and G' marked by b differ, their difference is a non-zero polynomial in I whose support is contained in $\mathcal{O}$. This contradicts the hypothesis and Claim 1 is proved.

To prove the second claim, it suffices to observe that, by Definition 4.4.1, the set G' is an $\mathcal{O}$-border basis of I and to apply the first part. Finally, we prove Claim 3. Let k be the field of definition of I, let $P' = k[x_1, \ldots, x_n]$, and let $I' = I \cap P'$. Given a term ordering σ, the ideals I and I' have the same reduced σ-Gröbner basis (see [KR00], Lemma 2.4.16). Hence we have $\mathcal{O}_\sigma(I) = \mathcal{O}_\sigma(I')$, and therefore $\dim_k(P'/I') = \dim_K(P/I)$. The elements of $\mathcal{O}$ are in P' and they are linearly independent modulo I'. Hence their residue classes form a k-vector space basis of P'/I'. Let G' be the $\mathcal{O}$-border basis of I'. Then G' is an $\mathcal{O}$-border prebasis whose elements are contained in I. Thus the statement follows from Claim 2. $\square$

Given an order ideal $\mathcal{O}$ consisting of $\dim_K(P/I)$ many terms, does the $\mathcal{O}$-border basis of I always exist? The answer is negative, as our next example shows.

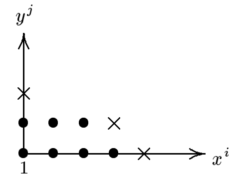
Example 4.4.5. Let $P = \mathbb{Q}[x, y]$, and let I be the vanishing ideal of the set of five points $X = \{(0,0), (0,-1), (1,0), (1,1), (-1,1)\}$ in the affine space $\mathbb{A}^2(\mathbb{Q})$, i.e. let $I = \{f \in P \mid f(p) = 0 \text{ for all } p \in X\}$. It is known that $\dim_K(P/I) = 5$. In $\mathbb{T}^2$, the following order ideals contain five elements:

$$\mathcal{O}_1 = \{1, x, x^2, x^3, x^4\},\ \mathcal{O}_2 = \{1, x, x^2, x^3, y\},\ \mathcal{O}_3 = \{1, x, x^2, y, y^2\}$$
$$\mathcal{O}_4 = \{1, x, x^2, y, xy\},\ \mathcal{O}_5 = \{1, x, y, y^2, y^3\},\ \mathcal{O}_6 = \{1, y, y^2, y^3, y^4\}$$
$$\mathcal{O}_7 = \{1, x, y, xy, y^2\}$$

Not all of these are suitable for border bases of I. For example, the residue classes of the elements of $\mathcal{O}_1$ cannot form a K-vector space basis of P/I since $x^3 - x \in I$. Similarly, the residue classes of the elements of $\mathcal{O}_6$ cannot form a K-vector space basis of P/I since $y^3 - y \in I$.

So, let us strive for less and ask another question. Does a given zero-dimensional ideal possess a border basis at all? Using Theorem 4.4.4, we can rephrase the question in the following way. Given a zero-dimensional ideal I, are there order ideals such that the residue classes of their elements form a K-vector space basis of P/I? This time the answer is yes, as we can show with the help of Gröbner bases.

Given an order ideal $\mathcal{O} \subset \mathbb{T}^n$, its complement $\mathbb{T}^n \setminus \mathcal{O}$ is the set of terms of a monomial ideal. Recall that every monomial ideal has a unique minimal set of generators (see [KR00], Proposition 1.3.11). The elements of the minimal set of generators of the monomial ideal corresponding to $\mathbb{T}^n \setminus \mathcal{O}$ are called the **corners** of $\mathcal{O}$. A picture illustrates the significance of this name.



Proposition 4.4.6. *Let σ be a term ordering on $\mathbb{T}^n$. Then there exists a unique $\mathcal{O}_\sigma(I)$-border basis G of I, and the reduced σ-Gröbner basis of I is the subset of G consisting of the polynomials marked by the corners of $\mathcal{O}_\sigma(I)$.*

Proof. By Macaulay's Basis Theorem (see [KR00], Theorem 1.5.7), the residue classes of the elements in $\mathcal{O}_\sigma(I)$ form a K-vector space basis of P/I. Thus Theorem 4.4.4.1 implies the existence and uniqueness of the $\mathcal{O}_\sigma(I)$-border basis G of I.

To prove the second claim, we let $b \in \mathbb{T}^n \setminus \mathcal{O}_\sigma(I)$ be a corner of $\mathcal{O}_\sigma(I)$. The element of the minimal σ-Gröbner basis of I with leading term b has the form $b - \mathrm{NF}_{\sigma,I}(b)$, where $\mathrm{NF}_{\sigma,I}(b)$ is contained in the span of $\mathcal{O}_\sigma(I)$. Since the $\mathcal{O}_\sigma(I)$-border basis of I is unique, this Gröbner basis element agrees with the border basis element marked by b. Thus the second claim follows and the proof is complete. $\square$

To summarize the discussion, the ideal I does not necessarily have an $\mathcal{O}$-border basis for every order ideal $\mathcal{O}$ consisting of $\dim_K(P/I)$ terms, but there always is an $\mathcal{O}$-border basis if $\mathcal{O}$ is of the form $\mathcal{O} = \mathcal{O}_\sigma(I)$ for some term ordering σ. This motivates our next question. Do all border bases belong to order ideals of the form $\mathcal{O}_\sigma(I)$? In other words, is there a bijection between the reduced Gröbner bases and the border bases of I? The answer is no, as our next example shows.

Example 4.4.7. Let $P = \mathbb{Q}[x,y]$, and let $X \subset \mathbb{A}^2(\mathbb{Q})$ be the set of points $X = \{p_1,p_2,p_3,p_4,p_5)\}$, where $p_1 = (0,0)$, $p_2 = (0,-1)$, $p_3 = (1,0)$, $p_4 = (1,1)$, and $p_5 = (-1,1)$. Furthermore, let $I \subset P$ be the vanishing ideal of X (see Example 4.4.5). The map eval : $P/I \longrightarrow \mathbb{Q}^5$ defined by $f + I \mapsto (f(p_1),\dots,f(p_5))$ is an isomorphism of K-vector spaces.

Consider the order ideal $\mathcal{O} = \{1,x,y,x^2,y^2\}$. The matrix of size 5×5 whose columns are $(\mathrm{eval}(1),\mathrm{eval}(x),\dots,\mathrm{eval}(y^2))$ is invertible. Therefore the residue classes of the terms in $\mathcal{O}$ form a $\mathbb{Q}$-vector space basis of P/I, and I has an $\mathcal{O}$-border basis by Theorem 4.4.4.1.

The border of $\mathcal{O}$ is $\partial\mathcal{O} = \{xy,x^3,y^3,xy^2,x^2y\}$. The $\mathcal{O}$-border basis of I is $G = \{g_1,\dots,g_5\}$ with $g_1 = x^3 - x$, $g_2 = x^2y - \frac{1}{2}y - \frac{1}{2}y^2$, $g_3 = xy - x - \frac{1}{2}y + x^2 - \frac{1}{2}y^2$, $g_4 = xy^2 - x - \frac{1}{2}y + x^2 - \frac{1}{2}y^2$, and $g_5 = y^3 - y$. To show that this border basis is not of the form $\mathcal{O}_\sigma(I)$, consider the polynomial g_3 in more detail. For any term ordering σ we have $x^2 >_\sigma x$ and $y^2 >_\sigma y$. Moreover, either $x^2 >_\sigma xy >_\sigma y^2$ or $y^2 >_\sigma xy >_\sigma x^2$. This leaves either x^2 or y^2 as the leading term of g_3. Since these terms are contained in $\mathcal{O}$, the order ideal $\mathcal{O}$ cannot be the complement of $\mathrm{LT}_\sigma(I)$ in $\mathbb{T}^2$ for any term ordering σ.

The upshot of this example is that the set of border bases of a given zero-dimensional ideal is strictly larger than the set of its reduced Gröbner bases. Therefore there is a better chance of finding a “nice” system of generators of I among border bases than among Gröbner bases. For instance, sometimes border bases are advertised by saying that they *keep symmetry*. While this is true in many cases, the claim has to be taken with a grain of salt. Just have a look at the following example.

Example 4.4.8. Let $P = \mathbb{Q}[x,y]$ and $I = (x^2 + y^2 - 1,\ xy - 1)$. The ideal I is symmetric with respect to the indeterminates x and y. Moreover, we have $\dim_K(P/I) = 4$. The only symmetric order ideal consisting of four terms is $\mathcal{O} = \{1,\ x,\ y,\ xy\}$. But I does not have an $\mathcal{O}$-border basis, since we have $xy - 1 \in I$. It may be interesting to observe that the residue classes of the elements 1, $x - y$, $x + y$, $x^2 - y^2$ form a K-vector space basis of P/I.

Let us investigate the relationship between Gröbner bases and border bases a little further. A list (or a set) of marked polynomials $((g_1,b_1),\dots,(g_\nu,b_\nu))$ is said to be **marked coherently** if there exists a term ordering σ such that $\mathrm{LT}_\sigma(g_i) = b_i$ for $i = 1,\dots,\nu$. Furthermore, recall that an $\mathcal{O}$-border (pre)basis can be viewed as a tuple of polynomials marked by terms in the border of $\mathcal{O}$.

Proposition 4.4.9. *Let $\mathcal{O}$ be an order ideal such that the residue classes of the elements of $\mathcal{O}$ form a K-vector space basis of P/I. Let G be the $\mathcal{O}$-border basis of I, and let G' be the subset of G consisting of the elements marked by the corners of $\mathcal{O}$. Then the following conditions are equivalent.*

1. *There exists a term ordering σ such that $\mathcal{O} = \mathcal{O}_\sigma(I)$.*
2. *The elements in G' are marked coherently.*

3. The elements in G are marked coherently.

Moreover, if these conditions are satisfied, then G' is the reduced σ-Gröbner basis of I.

Proof. Let us prove that 1) implies both 2) and the additional claim. The fact that G' is the reduced σ-Gröbner basis of I follows from Proposition 4.4.6. Hence G' is marked coherently. Now we show that 2) implies 3). For every polynomial $g \in G \setminus G'$, there exists a polynomial $g' \in G'$ such that the marked term of g is of the form $b = t\,\mathrm{LT}_\sigma(g')$. Then the support of the polynomial $g - t\,g'$ is contained in $\mathcal{O}$, and therefore $g = t\,g'$. Thus proves that also g is marked coherently with respect to σ.

Since 3) $\Rightarrow$ 2) is obvious, only 2) $\Rightarrow$ 1) remains to be shown. Let σ be a term ordering which marks G' coherently. Denote the monomial ideal generated by the leading terms of the elements in G' by $\mathrm{LT}_\sigma(G')$. Since $\mathrm{LT}_\sigma(I) \supseteq \mathrm{LT}_\sigma(G')$, we get $\mathcal{O}_\sigma(I) = \mathbb{T}^n \setminus \mathrm{LT}_\sigma(I) \subseteq \mathbb{T}^n \setminus \mathrm{LT}_\sigma(G') = \mathcal{O}$. Also the residue classes of the elements of $\mathcal{O}_\sigma(I)$ form a K-vector space basis of P/I, and hence the inclusion is indeed an equality. $\square$

The proposition applies for instance to the monomial ideal I generated by the corners of $\mathcal{O}$. Later we shall see that the equivalent conditions of this proposition apply for a particular type of zero-dimensional ideals, namely the vanishing ideals of distracted fractions (see Example 4.5.5). The following remark will be useful in the last section.

Remark 4.4.10. Assume that there exists a term ordering σ such that every corner of $\mathcal{O}$ is σ-greater than every element in $\mathcal{O}$. Then we have $\mathcal{O} = \mathcal{O}_\sigma(I)$ for all ideals I such that the residue classes of the terms in $\mathcal{O}$ form a K-vector space basis of P/I. We do not know whether the converse holds, but we believe it does.

4.4.2 Normal forms

In Gröbner basis theory one can define a unique representative of a residue class in P/I by using the normal form of a polynomial f. The normal form is obtained by computing the normal remainder of f under the division by a Gröbner basis. It does not depend on the Gröbner basis, but only on the given term ordering and the ideal I. Hence it can be used to make the ring operations in P/I effectively computable. In this subsection we imitate this approach and generalize the normal form to border basis theory.

Let $\mathcal{O} = \{t_1, \ldots, t_\mu\}$ be an order ideal, let $G = \{g_1, \ldots, g_\nu\}$ be the $\mathcal{O}$-border basis of a zero-dimensional ideal I, and let $\mathcal{G}$ be the tuple $(g_1, \ldots, g_\nu)$. In this situation the normal $\mathcal{O}$-remainder of a polynomial does not depend on the order of the elements in $\mathcal{G}$.

Proposition 4.4.11. *Let $\pi : \{1, \ldots, \nu\} \longrightarrow \{1, \ldots, \nu\}$ be a permutation, and let $\mathcal{G}' = (g_{\pi(1)}, \ldots, g_{\pi(\nu)})$ be the corresponding permutation of the tuple $\mathcal{G}$. Then we have $\mathrm{NR}_{\mathcal{O},\mathcal{G}}(f) = \mathrm{NR}_{\mathcal{O},\mathcal{G}'}(f)$ for every polynomial $f \in P$.*

Proof. The Border Division Algorithm applied to $\mathcal{G}$ and $\mathcal{G}'$, respectively, yields representations

$$f = f_1 g_1 + \cdots + f_\nu g_\nu + \mathrm{NR}_{\mathcal{O},\mathcal{G}}(f) = f_1' g_{\pi(1)} + \cdots + f_\nu' g_{\pi(\nu)} + \mathrm{NR}_{\mathcal{O},\mathcal{G}'}(f)$$

where $f_i, f_j' \in P$. Therefore we have $\mathrm{NR}_{\mathcal{O},\mathcal{G}}(f) - \mathrm{NR}_{\mathcal{O},\mathcal{G}'}(f) \in \langle \mathcal{O} \rangle_K \cap I$. The hypothesis that I has an $\mathcal{O}$-border basis implies $\langle \mathcal{O} \rangle_K \cap I = \{0\}$. Hence the claim follows. $\square$

This result allows us to introduce the following definition.

Definition 4.4.12. *Let $\mathcal{O}=\{t_1, \ldots, t_\mu\}$ be an order ideal and $G = \{g_1, \ldots, g_\nu\}$ an $\mathcal{O}$-border basis of I. The* **normal form** *of a polynomial $f \in P$ with respect to $\mathcal{O}$ is the polynomial $\mathrm{NF}_{\mathcal{O},I}(f) = \mathrm{NR}_{\mathcal{O},\mathcal{G}}(f)$.*

The normal form $\mathrm{NF}_{\mathcal{O},I}(f)$ of $f \in P$ can be calculated by dividing f by the $\mathcal{O}$-border basis of I. It is zero if and only if $f \in I$. Further basic properties of normal forms are collected in the following proposition.

Proposition 4.4.13 (Basic Properties of Normal Forms).
Let $\mathcal{O}$ be an order ideal, and suppose that I has an $\mathcal{O}$-border basis.

1. *If there exists a term ordering σ such that $\mathcal{O} = \mathcal{O}_\sigma(I)$, then we have $\mathrm{NF}_{\mathcal{O},I}(f) = \mathrm{NF}_{\sigma,I}(f)$ for all $f \in P$.*
2. *For $f_1, f_2 \in P$, we have $\mathrm{NF}_{\mathcal{O},I}(f_1 - f_2) = \mathrm{NF}_{\mathcal{O},I}(f_1) - \mathrm{NF}_{\mathcal{O},I}(f_2)$.*
3. *For $f \in P$, we have $\mathrm{NF}_{\mathcal{O},I}(\mathrm{NF}_{\mathcal{O},I}(f)) = \mathrm{NF}_{\mathcal{O},I}(f)$.*
4. *For $f_1, f_2 \in P$, we have $\mathrm{NF}_{\mathcal{O},I}(f_1\, f_2) = \mathrm{NF}_{\mathcal{O},I}\big(\mathrm{NF}_{\mathcal{O},I}(f_1)\ \mathrm{NF}_{\mathcal{O},I}(f_2)\big)$.*
5. *Let $\mathcal{M}_1, \ldots, \mathcal{M}_n \in \mathrm{Mat}_n(K)$ be the matrices of the multiplication endomorphisms of P/I with respect to the basis given by the residue classes of the terms in $\mathcal{O}$. Suppose that $t_1 = 1$, and let e_1 be the first standard basis vector of K^ν. Then we have*

   $$\mathrm{NF}_{\mathcal{O},I}(f) = (t_1, \ldots, t_\nu) \cdot f(\mathcal{M}_1, \ldots, \mathcal{M}_n) \cdot e_1$$

   for every $f \in P$.

Proof. Claim 1) follows because both $\mathrm{NF}_{\mathcal{O},I}(f)$ and $\mathrm{NF}_{\sigma,I}(f)$ are equal to the uniquely determined polynomial in $f + I$ whose support is contained in $\mathcal{O}$. Claims 2), 3), and 4) follow from the same uniqueness. To prove the last claim, we observe that e_1 is the coordinate tuple of $1 + I$ in the basis of P/I given by the residue classes of the terms in $\mathcal{O}$. Since $\mathcal{M}_i$ is the matrix of the multiplication by x_i, the tuple $f(\mathcal{M}_1, \ldots, \mathcal{M}_n) \cdot e_1$ is the coordinate tuple of $f + I$ in this basis. From this the claim follows immediately. $\square$

4.4.3 Border bases and commuting matrices

The purpose of this subsection is to provide the link between border bases and the theory of commuting endomorphisms discussed in the second section. More precisely, we shall characterize border bases by the property that their corresponding formal multiplication matrices commute.

Let $\mathcal{O} = \{t_1, \dots, t_\mu\}$ be an order ideal with border $\partial\mathcal{O} = \{b_1, \dots, b_\nu\}$, and let $G = \{g_1, \dots, g_\nu\}$ be an $\mathcal{O}$-border prebasis. For $j = 1, \dots, \nu$, we write $g_j = b_j - \sum_{i=1}^{\mu} \alpha_{ij} t_i$ with $\alpha_{1j}, \dots, \alpha_{\mu j} \in K$.

In Section 4.2 we saw that a K-vector space basis of P/I allows us to describe the multiplicative structure of this algebra via a tuple of commuting matrices. If G is a border bases, we can describe these matrices as follows.

Remark 4.4.14. In the above setting, assume that G is a border basis. Then $\{\bar{t}_1, \dots, \bar{t}_\mu\}$ is a K-vector space basis of P/I, and each multiplication endomorphism X_k of P/I corresponds to a matrix $\mathcal{X}_k = (\xi_{ij})$, i.e.,

$$\begin{aligned} X_k(\bar{t}_1) &= \xi_{11}\bar{t}_1 + \cdots + \xi_{\mu 1}\bar{t}_\mu \\ &\vdots \\ X_k(\bar{t}_\mu) &= \xi_{1\mu}\bar{t}_1 + \cdots + \xi_{\mu\mu}\bar{t}_\mu \end{aligned}$$

In these expansions only two cases occur. The product $x_k\, t_j$ either equals some term in the order ideal $t_r \in \mathcal{O}$ or some border term $b_s \in \partial\mathcal{O}$. In the former case we have

$$X_k(\bar{t}_j) = 0\,\bar{t}_1 + \cdots + 0\,\bar{t}_{r-1} + 1\,\bar{t}_r + 0\,\bar{t}_{r+1} + \cdots + 0\,\bar{t}_\mu$$

i.e., the j^{th} column of $\mathcal{X}_k$ is the r^{th} standard basis vector e_r. In the latter case we have $x_k t_j + I = b_s + I = \alpha_{1s}t_1 + \cdots + \alpha_{\mu s}t_\mu + I$, where the coefficients α_{is} are given by $g_s = b_s - \sum_i \alpha_{is}t_i$. Therefore we have

$$X_k(\bar{t}_j) = \alpha_{1s}\bar{t}_1 + \cdots + \alpha_{\mu s}\bar{t}_\mu$$

i.e., the j^{th} column of $\mathcal{X}_k$ is $(\alpha_{1s}, \dots, \alpha_{\mu s})^{\text{tr}}$. Observe that all matrix components ξ_{ij} are determined by the polynomials $g_1, \dots, g_\nu$.

In view of this remark, at least formally, multiplication matrices can be defined for any border prebasis.

Definition 4.4.15. *Let $\mathcal{O}=\{t_1, \dots, t_\mu\}$ be an order ideal and $G = \{g_1, \dots, g_\nu\}$ an $\mathcal{O}$-border prebasis. For $1 \le k \le n$, define the k^{th}* **formal multiplication matrix** *$\mathcal{X}_k$ columnwise by*

$$(\mathcal{X}_k)_{*j} = \begin{cases} e_r, & \text{if } x_k\, t_j = t_r \\ (\alpha_{1s}, \dots, \alpha_{\mu s})^{\text{tr}}, & \text{if } x_k\, t_j = b_s \end{cases}$$

To get some insight into the meaning of this definition, let us have a look at example 4.4.7 "from the outside."

Example 4.4.16. Let $P = \mathbb{Q}[x,y]$, and let $\mathcal{O} = \{t_1,t_2,t_3,t_4,t_5\}$ be the order ideal given by $t_1 = 1$, $t_2 = x$, $t_3 = y$, $t_4 = x^2$, and $t_5 = y^2$. The border of $\mathcal{O}$ is $\partial\mathcal{O} = \{b_1,b_2,b_3,b_4,b_5\}$ where $b_1 = xy$, $b_2 = x^3$, $b_3 = y^3$, $b_4 = x^2y$, and $b_5 = xy^2$. The polynomials $g_1 = xy - x - \frac{1}{2}y + x^2 - \frac{1}{2}y^2$, $g_2 = x^3 - x$, $g_3 = y^3 - y$, $g_4 = x^2y - \frac{1}{2}y - \frac{1}{2}y^2$, and $g_5 = xy^2 - x - \frac{1}{2}y + x^2 - \frac{1}{2}y^2$ define a border prebasis of $I = (g_1,\dots,g_5)$. Now we compute the formal multiplication matrices $\mathcal{X}$ and $\mathcal{Y}$.

On the one hand, we have $x\,t_1 = t_2$, $x\,t_2 = t_4$, $x\,t_3 = b_1$, $x\,t_4 = b_2$, and $x\,t_5 = b_5$. On the other hand, we have $y\,t_1 = t_3$, $y\,t_2 = b_1$, $y\,t_3 = t_5$, $y\,t_4 = b_4$, and $y\,t_5 = b_3$. Thus we obtain

$$\mathcal{X} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1/2 & 0 & 1/2 \\ 0 & 1 & -1 & 0 & -1 \\ 0 & 0 & 1/2 & 0 & 1/2 \end{pmatrix} \quad \text{and} \quad \mathcal{Y} = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 1 & 1/2 & 0 & 1/2 & 1 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 1/2 & 1 & 1/2 & 0 \end{pmatrix}$$

By Example 4.4.7, this border prebasis is even a border basis of I. Hence the formal multiplication matrices are the actual multiplication matrices. As such they commute.

The following theorem is the main result of this subsection. We characterize border bases by the property that their formal multiplication matrices commute. A more general theorem is contained in Chapter 3.

Theorem 4.4.17 (Border Bases and Commuting Matrices).
Let $\mathcal{O} = \{t_1,\dots,t_\mu\}$ be an order ideal. An $\mathcal{O}$-border prebasis $\{g_1,\dots,g_\nu\}$ is an $\mathcal{O}$-border basis of $I = (g_1,\dots,g_\nu)$ if and only if its formal multiplication matrices are pairwise commuting. In that case the formal multiplication matrices represent the multiplication endomorphisms of P/I with respect to the basis $\{\bar{t}_1,\dots,\bar{t}_\mu\}$.

Proof. Let $\mathcal{X}_1,\dots,\mathcal{X}_n$ be the formal multiplication matrices corresponding to the given $\mathcal{O}$-border prebasis $G = \{g_1,\dots,g_\nu\}$. If G is an $\mathcal{O}$-border basis, then Remark 4.4.14 shows that $\mathcal{X}_1,\dots,\mathcal{X}_n$ represent the multiplication endomorphisms of P/I. Hence they are pairwise commuting.

It remains to show sufficiency. Without loss of generality, let $t_1 = 1$. The matrices $\mathcal{X}_1,\dots,\mathcal{X}_n$ define a P-module structure on $\langle\mathcal{O}\rangle_K$ via

$$f \cdot (c_1t_1 + \dots c_\mu t_\mu) = (t_1,\dots,t_\mu) f(\tilde{\mathcal{X}}_1,\dots,\tilde{\mathcal{X}}_n)(c_1,\dots,c_\mu)^{\mathrm{tr}}$$

First we show that this P-module is cyclic with generator t_1. To do so, we use induction on the degree to show $t_i \cdot t_1 = t_i$ for $i = 1,\dots,\mu$. The induction starts with $t_1 = (t_1,\dots,t_\mu)\mathcal{I}_\mu \cdot e_1$. For the induction step, let $t_i = x_j\,t_k$. Then we have

$$\begin{aligned} t_i \cdot t_1 &= (t_1, \ldots, t_\mu) t_i(\mathcal{X}_1, \ldots, \mathcal{X}_n) e_1 = (t_1, \ldots, t_\mu) \mathcal{X}_j \, t_k(\mathcal{X}_1, \ldots, \mathcal{X}_n) e_1 \\ &= (t_1, \ldots, t_\mu) \mathcal{X}_j e_k = (t_1, \ldots, t_\mu) e_i = t_i \end{aligned}$$

Thus we obtain a surjective P-linear map $\tilde{\Theta} : P \to \langle \mathcal{O} \rangle_K$ such that $f \mapsto f \cdot t_1$ and an induced isomorphism of P-modules $\Theta \colon P/J \to \langle \mathcal{O} \rangle_K$ with $J = \ker \tilde{\Theta}$. In particular, the residue classes $t_1 + J, \ldots, t_\mu + J$ are K-linearly independent.

Next we show $I \subseteq J$. Let $b_j = x_k \, t_l$. Then we have

$$\begin{aligned} g_j(\mathcal{X}_1, \ldots, \mathcal{X}_n) e_1 &= b_j(\mathcal{X}_1, \ldots, \mathcal{X}_n) e_1 - \sum_{i=1}^{\mu} \alpha_{ij} t_i(\mathcal{X}_1, \ldots, \mathcal{X}_n) e_1 \\ &= \mathcal{X}_k \, t_l(\mathcal{X}_1, \ldots, \mathcal{X}_n) e_1 - \sum_{i=1}^{\mu} \alpha_{ij} e_i = \mathcal{X}_k \, e_l - \sum_{i=1}^{\mu} \alpha_{ij} e_i \\ &= \sum_{i=1}^{\mu} \alpha_{ij} e_i - \sum_{i=1}^{\mu} \alpha_{ij} e_i = 0 \end{aligned}$$

Therefore we have $g_j \in \ker \tilde{\Theta}$ for $j = 1, \ldots, \nu$ and $I \subseteq J$, as desired.

Hence there is a natural surjective ring homomorphism $\Psi \colon P/I \to P/J$. Since the set $\{t_1 + I, \ldots t_\mu + I\}$ generates the K-vector space P/I, and since the set $\{t_1 + J, \ldots, t_\mu + J\}$ is K-linearly independent, both sets must be bases and $I = J$. This shows that G is an $\mathcal{O}$-border basis of I. □

The following example shows that the formal multiplication matrices corresponding to an $\mathcal{O}$-border prebasis are not always commuting.

Example 4.4.18. Let $P = \mathbb{Q}[x, y]$ and $\mathcal{O} = \{t_1, t_2, t_3, t_4, t_5\}$ with $t_1 = 1$, $t_2 = x$, $t_3 = y$, $t_4 = x^2$, and $t_5 = y^2$. Then the border of $\mathcal{O}$ is $\partial\mathcal{O} = \{b_1, b_2, b_3, b_4, b_4\}$ with $b_1 = xy$, $b_2 = x^3$, $b_3 = y^3$, $b_4 = x^2 y$, and $b_5 = xy^2$. Consider the set of polynomials $G = \{g_1, g_2, g_3, g_4, g_5\}$ with $g_1 = xy - x^2 - y^2$, $g_2 = x^3 - x^2$, $g_3 = y^3 - y^2$, $g_4 = x^2 y - x^2$, and $g_5 = xy^2 - y^2$. It is an $\mathcal{O}$-border prebasis of the ideal $I = (g_1, \ldots, g_5)$. Its multiplication matrices

$$\mathcal{X} = \begin{pmatrix} 0&0&0&0&0 \\ 1&0&0&0&0 \\ 0&0&0&0&0 \\ 0&1&1&1&0 \\ 0&0&1&0&1 \end{pmatrix} \qquad \text{and} \qquad \mathcal{Y} = \begin{pmatrix} 0&0&0&0&0 \\ 0&0&0&0&0 \\ 1&0&0&0&0 \\ 0&1&0&1&0 \\ 0&1&1&0&1 \end{pmatrix}$$

do not commute:

$$\mathcal{X} \cdot \mathcal{Y} = \begin{pmatrix} 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 1&1&0&1&0 \\ 1&1&1&0&1 \end{pmatrix} \quad \neq \quad \mathcal{Y} \cdot \mathcal{X} = \begin{pmatrix} 0&0&0&0&0 \\ 0&0&0&0&0 \\ 0&0&0&0&0 \\ 1&1&1&1&0 \\ 1&0&1&0&1 \end{pmatrix}$$

By the theorem, the set G is not an $\mathcal{O}$-border basis of I.

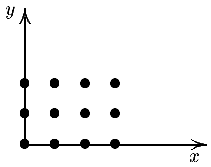
The condition that the formal multiplication matrices of a border basis have to commute can also be interpreted in terms of the syzygies of that basis (see [Ste04]). Based on the results of this section one can now imitate the development of Gröbner basis theory for border bases. For instance, the border basis analogues of the conditions A – D which characterize Gröbner bases in [KR00], Chapter 2, are examined by the first two authors in [KK03a].

4.5 Application to statistics

Fifty percent of the citizens of this country
have a below average understanding of statistics.
(Anonymous)

In this last section we see how to solve a problem in computational commutative algebra whose motivation comes from statistics. Does this sound strange to you? Well, come and see. Our problem comes up in the branch of statistics called *design of experiments.* If you want to get a more detailed understanding of this theory, we suggest that you start exploring it by reading [Rob98]. Or, if you prefer the statisticians' point of view, you can consult [GP00].

To get to the heart of the problem, let us introduce some fundamental concepts of design of experiments. A **full factorial design** is a finite set of points in affine space $\mathbb{A}^n(K) \cong K^n$ of the form $D = D_1 \times \cdots \times D_n$ where D_i is a finite subset of K. Associated to it we may consider the vanishing ideal $I_D = \{f \in P \mid f(p) = 0 \text{ for all } p \in D\}$. It is a complete intersection $I_D = (f_1, \ldots, f_n)$ such that $f_i \in K[x_i]$ is a product of linear forms for $i = 1, \ldots, n$. For instance, in $\mathbb{A}^2(\mathbb{Q})$ we have the full factorial design



whose vanishing ideal in $\mathbb{Q}[x,y]$ is $I_D = \big(x(x-1)(x-2)(x-3),\ y(y-1)(y-2)\big)$. The particular shape of the generators of I_D implies that they are the reduced σ-Gröbner basis of I_D with respect to any term ordering σ. Hence the order ideal $\mathcal{O}_D = \mathbb{T}^n \setminus \mathrm{LT}_\sigma(I_D)$ is canonically associated to D. In the example at hand we have for instance

$$\mathcal{O}_D = \{1,\, x,\, y,\, x^2,\, xy,\, y^2,\, x^3,\, x^2y,\, xy^2,\, x^3y,\, x^2y^2,\, x^3y^2\}$$

If a particular problem depends on n parameters and each parameter can assume finitely many values $D_i \subseteq K$, the full factorial design $D = D_1 \times \cdots \times D_n$ corresponds to the set of all possible experiments. The main task in the design of experiments is to identify an unknown function

$f : D \longrightarrow K$. This function is a mathematical **model** of a quantity which has to be computed or optimized. Since it is defined on a finite set, it can be determined by performing all experiments in D and measuring the value of f each time. Notice that a function f defined on a finite set is necessarily a polynomial function.

However, in most cases it is impossible to perform all experiments corresponding to the full factorial design. The obstacles can be, for instance, lack of time, lack of money, or lack of patience. Only a subset of those experiments can be performed. The question is how many and which? In statistical jargon a subset F of a full factorial design D is called a **fraction**. Our task is to choose a fraction $F \subseteq D$ that allows us to identify the model. In particular, we need to describe the order ideals whose residue classes form a K-basis of P/I_F. Statisticians express this property by saying that such order ideals (or complete sets of estimable terms, as they call them) are *identified* by F.

Even more important is the so-called *inverse problem.* Suppose we are given an order ideal $\mathcal{O}$. We would like to determine all fractions $F \subseteq D$ such that the residue classes of the elements of $\mathcal{O}$ form a K-basis of P/I_F. The main result of [CR97] was a partial solution of this inverse problem. More precisely, all fractions $F \subseteq D$ were found such that $\mathcal{O} = \mathcal{O}_\sigma(I_F)$ for some term ordering σ. However, we have already pointed out that some order ideals $\mathcal{O}$ do not fit into this scheme (see Example 4.4.7). Later, in the paper [CR01] the full solution was presented, and the main idea was to use border bases.

Before delving into the general solution of the inverse problem following the technique employed in [CR01], let us briefly explain an example of an actual statistical problem. This example is taken from [GBH78] and adapted to our setting and terminology.

Example 4.5.1. A number of similar chemical plants had been successfully operating for several years in different locations. In a newly constructed plant the filtration cycle took almost twice as long as in the older plants. Seven possible causes of the difficulty were considered by the experts.

1. The water for the new plant was somehow different in mineral content.
2. The raw material was not identical in all respects to that used in the older plants.
3. The temperature of filtration in the new plant was slightly lower than in the older plants.
4. A new recycle device was absent in the older plants.
5. The rate of addition of caustic soda was higher in the new plant.
6. A new type of filter cloth was being used in the new plant.
7. The holdup time was lower than in the older plants.

These causes lead to seven variables $x_1, \ldots, x_7$. Each of them can assume only two values, namely *old* and *new* which we denote by 0 and 1, respectively. Our full factorial design $D \subseteq \mathbb{A}^7(\mathbb{Q})$ is therefore the set $D = \{0,1\}^7$. Its vanishing ideal is $I_D = (x_1^2 - x_1,\ x_2^2 - x_2, \ldots,\ x_7^2 - x_7)$ in the polynomial ring $P = \mathbb{Q}[x_1, x_2, \ldots, x_7]$.

The model $f : D \longrightarrow \mathbb{Q}$ is the length of a filtration cycle. In order to identify it, we would have to perform 128 cycles. This is impracticable, since it would require too much time and money. On the other hand, suppose for a moment that we conduct all experiments and the output is $f = a + b\,x_1 + c\,x_2$ for some $a, b, c \in \mathbb{Q}$. At this point it becomes clear that we wasted many resources. Had we known in advance that the polynomial has only three unknown coefficients, we could have identified them by performing only *three* suitable experiments! Namely, if we determine three values of the polynomial $a + b\,x_1 + c\,x_2$, we can find a, b, c by solving a system of three linear equations in these three indeterminates. If the matrix of coefficients is invertible, this is an easy task.

However, a priori one does not know that the answer has that shape indicated above. In practice, one has to make some guesses, perform well-chosen experiments, and possibly modify the guesses until the process yields the desired answer. In the case of the chemical plant, it turned out that only x_1 and x_5 were relevant for identifying the model.

In this example there is one point which needs additional explanation. How can we choose the fraction F such that the matrix of coefficients is invertible? In other words, given a full factorial design D and an order ideal $\mathcal{O} \subseteq \mathcal{O}_D$, which fractions $F \subseteq D$ have the property that the residue classes of the elements of $\mathcal{O}$ are a K-basis of P/I_F? This is precisely the inverse problem stated above. In order to explain its solution, we introduce the following terminology.

Definition 4.5.2. *For $i = 1, \ldots, n$, let $\ell_i \geq 1$ and $D_i = \{a_{i1}, a_{i2}, \ldots, a_{i\ell_i}\} \subseteq K$. Then we say that the full factorial design $D = D_1 \times \cdots \times D_n \subseteq \mathbb{A}^n(K)$ has* **levels** $(\ell_1, \ldots \ell_n)$.

The polynomials $f_i = (x_i - a_{i1}) \cdots (x_i - a_{i\ell_i})$ with $i = 1, \ldots, n$ generate the vanishing ideal I_D of D. They are called the **canonical polynomials** *of D. Since $\{f_1, \ldots, f_n\}$ is a universal Gröbner basis of I_D (i.e. a Gröbner basis with respect to every term ordering), the order ideal*

$$\mathcal{O}_D = \{x_1^{\alpha_1} \cdots x_n^{\alpha_n} \mid 0 \leq \alpha_i < \ell_i \text{ for } i = 1, \ldots, n\}$$

represents a K-basis of P/I_D. We call it the **complete set of estimable terms of** D.

The following auxiliary result will be useful for proving the main theorem.

Lemma 4.5.3. *Let D be a full factorial design, let $\{f_1, \ldots, f_n\}$ be its canonical polynomials, let $\overline{K}$ be the algebraic closure of K, and let I be a proper ideal of $\overline{K}[x_1, \ldots, x_n]$ such that $I_D \subseteq I$.*

1. *The ideal I is a radical ideal. It is the vanishing ideal of a fraction of D.*
2. *The ideal I is generated by elements of P and $I \cap P$ a radical ideal.*

3. The polynomials of every border basis of I are elements of P.

Proof. First we prove Claim 1. Let $\mathbb{A}^n(\overline{K})$ be the affine space of dimension n over $\overline{K}$, and let $F \subset \mathbb{A}^n(\overline{K})$ be the set of zeros of I. Since $I_D \subseteq I$, we have $F \subseteq D$. By localizing the ring $A = \overline{K}[x_1, \dots, x_n]/I_D$ at the maximal ideals $\mathfrak{m}$ corresponding to the points of d, we see that either $IA_{\mathfrak{m}} = (1)$ or $IA_{\mathfrak{m}} = \mathfrak{m}A_{\mathfrak{m}}$. Therefore I is a radical ideal, and hence it is the defining ideal of F.

Since I is the defining ideal of a finite set of points with coordinates in K, it is the intersection of ideals generated by linear forms having coefficients in K. Consequently, the ideal I is defined over K which proves Claim 2. The third claim follows from Theorem 4.4.4. □

Now we are ready to state the main result of this section. Our goal is to solve the inverse problem. The idea is to proceed as follows. We are given a full factorial design D and an order ideal $\mathcal{O}$. By Theorem 4.4.4, ideals I such that $\mathcal{O}$ represents a K-basis of P/I are in 1-1 correspondence with border bases whose elements are marked by the terms in $\partial\mathcal{O}$. Except for the border basis elements which are canonical polynomials of D, we can write them down using indeterminate coefficients and require that the corresponding formal multiplication matrices are pairwise commuting. For I to be the vanishing ideal of a fraction contained in D, we have to make sure that I contains I_D. To this end, we require that the normal $\mathcal{O}$-remainders of the canonical polynomials of D are zero. By combining these requirements, we arrive at the following result.

Theorem 4.5.4 (Computing All Fractions).
Let D be a full factorial design with levels $(\ell_1, \dots, \ell_n)$, and let $\mathcal{O} = \{t_1, \dots, t_\mu\}$ be a complete set of estimable terms contained in $\mathcal{O}_D$ with $t_1 = 1$. Consider the following definitions.

1. *Let $C = \{f_1, \dots, f_n\}$ be the set of canonical polynomials of D, where f_i is marked by $x_i^{\ell_i}$ for $i = 1, \dots, n$.*
2. *Decompose $\partial\mathcal{O}$ into $\partial\mathcal{O}_1 = \{x_1^{\ell_1}, \dots, x_n^{\ell_n}\} \cap \partial\mathcal{O}$ and $\partial\mathcal{O}_2 = \partial\mathcal{O} \setminus \partial\mathcal{O}_1$.*
3. *Let C_1 be the subset of C marked by $\partial\mathcal{O}_1$, and let $C_2 = C \setminus C_1$.*
4. *Let $\eta = \#(\partial\mathcal{O}_2)$. For $i = 1, \dots, \eta$ and $j = 1, \dots, \mu$, introduce new indeterminates z_{ij}.*
5. *For every $b_k \in \partial\mathcal{O}_2$, let $g_k = b_k - \sum_{j=1}^{\mu} z_{kj} t_j \in K(z_{ij})[x_1, \dots, x_n]$.*
6. *Let $G = \{g_1, \dots, g_\eta\}$ and $H = G \cup C_1$. Let $\mathcal{M}_1, \dots, \mathcal{M}_n$ be the formal multiplication matrices associated to the $\mathcal{O}$-border prebasis H.*
7. *Let $\mathcal{I}(\mathcal{O})$ be the ideal in $K[z_{ij}]$ generated by the entries of the matrices $\mathcal{M}_i\mathcal{M}_j - \mathcal{M}_j\mathcal{M}_i$ for $1 \le i < j \le n$, and by the entries of the column matrices $f(\mathcal{M}_1, \dots, \mathcal{M}_n) \cdot e_1$ for all $f \in C_2$.*

Then $\mathcal{I}(\mathcal{O})$ is a zero-dimensional ideal in $K[z_{ij}]$ whose zeros are in 1-1 correspondence with the solutions of the inverse problem, i.e. with fractions $F \subseteq D$ such that $\mathcal{O}$ represents a K-basis of P/I_F.

Proof. Let $p = (\alpha_{11}, \dots, \alpha_{\mu\eta}) \in \overline{K}^{\mu\eta}$ be a zero of $\mathcal{I}(\mathcal{O})$. When we substitute the indeterminates z_{ij} by the coordinates of p in the matrices $\mathcal{M}_1, \dots, \mathcal{M}_n$, we obtain pairwise commuting matrices $\overline{\mathcal{M}}_1, \dots, \overline{\mathcal{M}}_n$ which feature the additional property that $f(\overline{\mathcal{M}}_1, \dots, \overline{\mathcal{M}}_n) \cdot e_1 = 0$ for every $f \in C_2$.

Now we substitute the coordinates of p in the polynomials of G and get polynomials $\bar{g}_k = b_k - \sum_{j=1}^{\mu} \alpha_{kj} t_j \in P$. Then we form the sets $\overline{G} = \{\bar{g}_1, \dots, \bar{g}_\eta\}$ and $\overline{H} = \overline{G} \cup C_1$, and we let $\overline{I}$ be the ideal generated by $\overline{H}$. Since the set H is an $\mathcal{O}$-border prebasis of the ideal generated by it, the set $\overline{H}$ is an $\mathcal{O}$-border prebasis of $\overline{I}$. Moreover, the fact that $\mathcal{M}_1, \dots, \mathcal{M}_n$ are the formal multiplication matrices of H implies that $\overline{\mathcal{M}_1}, \dots, \overline{\mathcal{M}}_n$ are the formal multiplication matrices of $\overline{H}$. Hence we can apply Theorem 4.4.17 and conclude that $\overline{H}$ is the $\mathcal{O}$-border basis of $\overline{I}$.

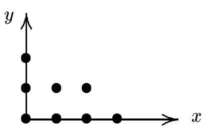
By definition, we have $C_1 \subseteq \overline{I}$. Using Proposition 4.4.13.5, we see that $f(\overline{\mathcal{M}}_1, \dots, \overline{\mathcal{M}}_n) \cdot e_1 = 0$ implies $\mathrm{NF}_{\mathcal{O},\overline{I}}(f) = 0$, and therefore $f \in \overline{I}$ for all $f \in C_2$. Altogether, we have $C = C_1 \cup C_2 \subseteq \overline{I}$, and thus $I_D \subseteq \overline{I}$. By Lemma 4.5.3.1, it follows that $\overline{I}$ is the vanishing ideal of a fraction of D.

Conversely, let F be a fraction of D such that $\mathcal{O}$ represents a K-basis of P/I_F. Consider the $\mathcal{O}$-border basis B of I_F and write $B = B_1 \cup B_2$ such that B_1 contains the polynomials marked by $\partial\mathcal{O}_1$ and B_2 contains the polynomials marked by $\partial\mathcal{O}_2$. Since $\partial\mathcal{O}_1 \subseteq \partial\mathcal{O}_D$, the polynomials in B_1 have the shape required for $\mathcal{O}_D$-border basis elements of I_D, i.e. they agree with the polynomials in C_1. The polynomials in B_2 are of the form $\bar{g}_k = b_k - \sum_{j=1}^{\mu} \alpha_{kj} t_j$ where $b_k \in \partial\mathcal{O}_2$ and $\alpha_{kj} \in K$. Let $p = (\alpha_{ij}) \in K^{\mu\eta}$. We claim that p is a zero of $\mathcal{I}(\mathcal{O})$.

The point p is a zero of the entries of the matrices $\mathcal{M}_i\mathcal{M}_j - \mathcal{M}_j\mathcal{M}_j$ for $1 \le i < j \le n$, since the matrices $\overline{\mathcal{M}}_1, \dots, \overline{\mathcal{M}}_n$ obtained by substituting p in $\mathcal{M}_1, \dots, \mathcal{M}_n$ are the formal multiplication matrices of B and thus commute by Theorem 4.4.17. The point p is a zero of the entries of $f(\mathcal{M}_1, \dots, \mathcal{M}_n) \cdot e_1$ for $f \in C_2$, since $f(\overline{\mathcal{M}}_1, \dots, \overline{\mathcal{M}}_n) \cdot e_1$ equals $\mathrm{NF}_{\mathcal{O},I_F}(f)$ by Proposition 4.4.13.5, and this normal form is zero because $f \in C_2 \subseteq I_D \subseteq I_F$. Altogether, we have shown that p is a zero of $\mathcal{I}(\mathcal{O})$, as claimed. □

Using *distracted fractions* (see [RR98]), one can show that there always exists at least one solution of the inverse problem. Let us look at an example to illustrate the method.

Example 4.5.5. Let D be the full factorial design $D = \{0, 1, 2, 3\} \times \{0, 1, 2\}$ contained in $\mathbb{A}^2(\mathbb{Q})$, and let $\mathcal{O} = \{1, x, y, x^2, xy, y^2, x^3, x^2y\} \subset \mathcal{O}_D$. The order ideal $\mathcal{O}$ can be visualized as follows.



We want to find a fraction $F \subseteq D$ such that $\mathcal{O}$ represents a K-basis of P/I_F. One solution is to use the distracted fraction whose points are exactly the points marked by bullets in the above sketch, i.e. the following set $F = \{(0,0),\, (0,1),\, (0,2),\, (1,0),\, (1,1),\, (2,0),\, (2,1),\, (3,0)\}$. An easy computation shows that the vanishing ideal of F is

$$I_F = \big(x(x-1)(x-2)(x-3),\, x(x-1)(x-2)y,\, xy(y-1,\, y(y-1)(y-2)\big)$$

Moreover, these three generators are a universal Gröbner basis of I_F and $\mathcal{O}_\sigma(I_F) = \mathcal{O}$ for every term ordering σ.

We end this section with two examples intended to explain how Theorem 4.5.4 solves the inverse problem.

Example 4.5.6. Let D be the full factorial design $D = \{-1,0,1\} \times \{-1,1\}$ with levels $(3,2)$ contained in $\mathbb{A}^2(\mathbb{Q})$. The complete set of estimable terms of D is $\mathcal{O}_D = \{1,\, x,\, y,\, x^2,\, xy,\, x^2y\}$. We want to solve the inverse problem for the order ideal $\mathcal{O} = \{1,\, x,\, y\}$ and follow the steps of Theorem 4.5.4.

1. The set of canonical polynomials of D is $C = \{f_1, f_2\}$, where $f_1 = x^3 - x$ and $f_2 = y^2 - 1$.
2. We decompose $\partial\mathcal{O} = \{x^2,\, xy,\, y^2\}$ into $\partial\mathcal{O}_1 = \{y^2\}$ and $\partial\mathcal{O}_2 = \{x^2,\, xy\}$.
3. Let $C_1 = \{f_2\}$ and $C_2 = \{f_1\}$.
4. Let $\eta = 2$. Choose six new indeterminates $z_{11},\, z_{12},\, z_{13},\, z_{21},\, z_{22},\, z_{23}$.
5. Define $g_1 = x^2 - (z_{11} + z_{12}x + z_{13}y)$ and $g_2 = xy - (z_{21} + z_{22}x + z_{23}y)$.
6. Let $G = \{g_1, g_2\}$ and $H = \{g_1, g_2, f_2\}$. The formal multiplication matrices associated to H are

$$\mathcal{M}_1 = \begin{pmatrix} 0 & z_{11} & z_{21} \\ 1 & z_{12} & z_{22} \\ 0 & z_{13} & z_{23} \end{pmatrix} \qquad \text{and} \qquad \mathcal{M}_2 = \begin{pmatrix} 0 & z_{21} & 1 \\ 0 & z_{22} & 0 \\ 1 & z_{23} & 0 \end{pmatrix}$$

7. Let $\mathcal{I}(\mathcal{O}) \subseteq \mathbb{Q}[z_{11}, \ldots, z_{23}]$ be the ideal generated by the entries of the matrices $\mathcal{M}_1\mathcal{M}_2 - \mathcal{M}_2\mathcal{M}_1$ and $f_1(\mathcal{M}_1, \mathcal{M}_2) \cdot e_1 = (\mathcal{M}_1^3 - \mathcal{M}_1) \cdot e_1$. We obtain $\mathcal{I}(\mathcal{O}) = (z_{12}z_{21} - z_{11}z_{22} - z_{21}z_{23} + z_{13},\; z_{21}z_{22} + z_{23},\; z_{22}z_{23} + z_{21},\; z_{22}^2 - 1,\; z_{13}z_{22} - z_{12}z_{23} + z_{23}^2 - z_{11},\; z_{22}z_{23} + z_{21},\; z_{11}z_{12} + z_{13}z_{21},\; z_{12}^2 + z_{13}z_{22} + z_{11} - 1,\; z_{12}z_{13} + z_{13}z_{23})$.

Using a computer algebra system, for instance CoCoA, we can check that $\mathcal{I}(O)$ is a zero-dimensional, radical ideal of multiplicity 18. This means that among the $20 = \binom{6}{3}$ triples of points of D, there are 18 triples which solve the inverse problem. The two missing fractions are $\{(0,0),\, (0,1),\, (0,2)\}$ and $\{(1,0),\, (1,1),\, (1,2)\}$.

When we apply the theorem to larger full factorial designs, the calculations involved in determining the zeros of $\mathcal{I}(\mathcal{O})$ quickly become voluminous.

Example 4.5.7. Let D be the full factorial design $D = \{-1,0,1\} \times \{-1,0,1\}$ with levels $(3,3)$ contained in $\mathbb{A}^2(\mathbb{Q})$. The complete set of estimable terms of D is $\mathcal{O}_D = \{1, x, y, x^2, xy, y^2, x^2y, xy^2, x^2y^2\}$. We want to solve the inverse problem for the order ideal $\mathcal{O} = \{1, x, y, x^2, y^2\}$ and follow the steps of Theorem 4.5.4.

1. The set of canonical polynomials of D is $C = \{f_1, f_2\}$, where $f_1 = x_1^3 - x_1$ and $f_2 = x_2^3 - x_2$.
2. We decompose $\partial\mathcal{O} = \{x^3, x^2y, xy, xy^2, y^3\}$ into $\partial\mathcal{O}_1 = \{x^3, y^3\}$ and $\partial\mathcal{O}_2 = \{x^2y, xy, xy^2\}$.
3. Let $C_1 = \{f_1, f_2\}$ and $C_2 = \emptyset$.
4. Let $\eta = 3$. Choose 15 new indeterminates $z_{11}, z_{12}, \dots, z_{35}$.
5. Define $g_1 = x^2y - (z_{11} + z_{12}x + z_{13}y + z_{14}x^2 + z_{15}y^2)$ and $g_2 = xy - (z_{21} + z_{22}x + z_{23}y + z_{24}x^2 + z_{25}y^2)$ and $g_3 = xy^2 - (z_{31} + z_{32}x + z_{33}y + z_{34}x^2 + z_{35}y^2)$.
6. Let $G = \{g_1, g_2, g_3\}$ and $H = \{g_1, g_2, g_3, f_1, f_2\}$. The formal multiplication matrices associated to H are

$$\mathcal{M}_1 = \begin{pmatrix} 0 & 0 & z_{21} & 0 & z_{31} \\ 1 & 0 & z_{22} & 1 & z_{32} \\ 0 & 0 & z_{23} & 0 & z_{33} \\ 0 & 1 & z_{24} & 0 & z_{34} \\ 0 & 0 & z_{25} & 0 & z_{35} \end{pmatrix} \qquad \mathcal{M}_2 = \begin{pmatrix} 0 & z_{21} & 0 & z_{11} & 0 \\ 0 & z_{22} & 0 & z_{12} & 0 \\ 1 & z_{23} & 0 & z_{13} & 1 \\ 0 & z_{24} & 0 & z_{14} & 0 \\ 0 & z_{25} & 1 & z_{15} & 0 \end{pmatrix}$$

7. Let $\mathcal{I}(\mathcal{O})$ be the ideal in $\mathbb{Q}[z_{11}, \dots, z_{35}]$ generated by the entries of the matrix $\mathcal{M}_1\mathcal{M}_2 - \mathcal{M}_2\mathcal{M}_1$. Thus $\mathcal{I}(\mathcal{O})$ is the ideal generated by the following 20 polynomials:

$$\begin{array}{cc}
z_{21}z_{23} + z_{25}z_{31} - z_{11} & z_{21}z_{22} + z_{11}z_{24} - z_{31} \\
z_{13}z_{21} + z_{15}z_{31} - z_{21} & z_{21}z_{32} + z_{11}z_{34} - z_{21} \\
z_{22}z_{23} + z_{25}z_{32} - z_{12} + z_{21} + z_{24} & z_{22}^2 + z_{12}z_{24} - z_{32} \\
z_{13}z_{22} + z_{15}z_{32} + z_{11} + z_{14} - z_{22} & z_{22}z_{32} + z_{12}z_{34} - z_{22} \\
z_{23}^2 + z_{25}z_{33} - z_{13} & z_{22}z_{23} + z_{13}z_{24} + z_{21} + z_{25} - z_{33} \\
z_{13}z_{23} + z_{15}z_{33} - z_{23} & z_{23}z_{32} + z_{13}z_{34} - z_{23} + z_{31} + z_{35} \\
z_{23}z_{24} + z_{25}z_{34} - z_{14} + z_{22} & z_{14}z_{24} + z_{22}z_{24} - z_{34} \\
z_{13}z_{24} + z_{15}z_{34} + z_{12} - z_{24} & z_{24}z_{32} + z_{14}z_{34} - z_{24} \\
z_{23}z_{25} + z_{25}z_{35} - z_{15} & z_{15}z_{24} + z_{22}z_{25} + z_{23} - z_{35} \\
z_{13}z_{25} + z_{15}z_{35} - z_{25} & z_{25}z_{32} + z_{15}z_{34} - z_{25} + z_{33}
\end{array}$$

Again we can use a computer algebra system and check that $\mathcal{I}(O)$ is a zero-dimensional, radical ideal of multiplicity 81. This means that among the $126 = \binom{9}{5}$ five-tuples of points in D there are 81 five-tuple which solve the inverse problem.

One of the zeros of $\mathcal{I}(\mathcal{O})$ is the point $p \in \mathbb{Q}^{15}$ whose coordinates are

$$\begin{array}{lllll}
z_{11} = 0 & z_{12} = 0 & z_{13} = -\frac{1}{2} & z_{14} = 0 & z_{15} = -\frac{1}{2} \\
z_{21} = 0 & z_{22} = -1 & z_{23} = -\frac{1}{2} & z_{24} = 1 & z_{25} = -\frac{1}{2} \\
z_{31} = 0 & z_{32} = -1 & z_{33} = -\frac{1}{2} & z_{34} = 1 & z_{35} = -\frac{1}{2}
\end{array}$$

The corresponding $\mathcal{O}$-border basis is $\{x^3 - x,\ x^2y - \frac{1}{2}y - \frac{1}{2}y^2,\ xy - x - \frac{1}{2}y + x^2 - \frac{1}{2}y^2,\ xy^2 - x - \frac{1}{2}y + x^2 - \frac{1}{2}y^2,\ y^3 - y\}$. The fraction defined by this basis is

$$F_0 = \{(0,0),\ (0,-1),\ (1,0),\ (1,1),\ (-1,1)\}$$

This is our old friend of Example 4.4.7!

In view of our discussion in Section 4.1, it is natural to ask how many of the 81 fractions F found above have the property that $\mathcal{O}$ is not of the form $\mathcal{O}_\sigma(I_F)$ for any term ordering σ. We have seen in Example 4.4.7 that at least the fraction F_0 is of that type. By combining Theorem 4.5.4 and some techniques discussed in [CR97], one can show that 36 of those 81 fractions are of that type. This is a surprisingly high number which shows that border bases provide sometimes a much more flexible environment for working with zero-dimensional ideals than Gröbner bases do.

There will never be a last tango
(Brad Hooper)