STANDARD BASES IN MIXED POWER SERIES AND POLYNOMIAL RINGS OVER RINGS

THOMAS MARKWIG, YUE REN, OLIVER WIENAND

Abstract. In this paper we study standard bases for submodules of a mixed power series and polynomial ring $R[\![t_1,\ldots,t_m]\!][x_1,\ldots,x_n]^s$ respectively of their localization with respect to a $\underline{t}$-local monomial ordering for a certain class of noetherian rings R. The main steps are to prove the existence of a division with remainder generalizing and combining the division theorems of Grauert–Hironaka and Mora and to generalize the Buchberger criterion. Everything else then translates naturally. Setting either $m = 0$ or $n = 0$ we get standard bases for polynomial rings respectively for power series rings over R as a special case.

The paper follows to a large part the lines of [Mar10], or alternatively [GrP02] and [DeS07], adapting to the situation that the coefficient domain R is no field. We generalize the Division Theorem of Grauert–Hironaka respectively Mora (the latter in the form stated and proved first by Greuel and Pfister, see [GGM+94], [GrP96]; see also [Mor82], [Grä94]). The paper should therefore be seen as a unified approach for the existence of standard bases in polynomial and power series rings for coefficient domains which are not fields. Standard bases of ideals in such rings come up naturally when computing Gröbner fans (see [MaR15a]) and tropical varieties (see [MaR15b]) over non-archimedian valued fields, even though we consider a wider class of base rings than actually needed for this.
An important point is that if the input data is polynomial in both $\underline{t}$ and $\underline{x}$ then we can actually compute the standard basis in finite time since a standard basis computed in $R[t_1,\ldots,t_m]_{\langle t_1,\ldots,t_m\rangle}[x_1,\ldots,x_n]$ will do.
Many authors contributed to the further development (see e.g. [Bec90] for a standard basis criterion in the power series ring) and to generalizations of the theory, e.g. to algebraic power series (see e.g. [Hir77], [AMR77], [ACH05]) or to differential operators (see e.g. [GaH05]). This list is by no means complete.

Date: March, 2015.
1991 *Mathematics Subject Classification.* Primary 13P10, 13F25, 16W60; Secondary 12J25, 16W60.
Key words and phrases. Standard basis, monomial ordering, division with remainder.
The author was supported by ...

1. Division with remainder

In this section, we construct a division with remainder following the first three chapters of [Mar08]. Please mind the assumptions on our ground ring in Convention 1.1 for that, which were taken from Definition 1.3.14 in [Wie11].
After a quick introduction of the basic terminology, we begin with a division algorithm over the ground ring in the form of Algorithm 1.11. We then continue with homogeneous division with remainder in Algorithm 1.13, and finally end with a weak division with remainder in Algorithm 1.22.

Convention 1.1 (The class of base rings)
For this chapter, let R be a noetherian ring in which *linear equations are solvable* as in Definition 1.3.14 of [Wie11]. The latter means that, given any finite tuple of arbitrary length $(c_1, \ldots, c_k)$ with $c_i \in R$, we must be able to do the following:

(1) decide for $b \in R$ whether $b \in \langle c_1, \ldots, c_k \rangle$, and, if yes, find $a_1, \ldots, a_k \in R$ such that
$$b = a_1 \cdot c_1 + \cdots + a_k \cdot c_k.$$
(2) find a finite generating set $S \subseteq R^k$ of its syzygies as module over R,
$$\mathrm{syz}_R(c_1, \ldots, c_k) = \{(a_1, \ldots, a_k) \in R^k \mid a_1 \cdot c_1 + \ldots + a_k \cdot c_k = 0\} = \langle S \rangle_R.$$

We will use the notion $R[\![t]\!][x] := R[\![t_1, \ldots, t_m]\!][x_1, \ldots, x_n]$ to denote a mixed power series and polynomial ring over R in several variables $t = (t_1, \ldots, t_m)$ and $x = (x_1, \ldots, x_n)$, and $R[\![t]\!][x]^s$ will denote the free module of rank s over $R[\![t]\!][x]$.
R being noetherian is most notably required for the conditional termination of Algorithm 1.22, while linear equations being solvable is required in the instructions of Algorithm 1.11 and Algorithm 2.16.

Example 1.2
Admissible ground rings satisfying Convention 1.1 include the following:

- Obviously any field, assuming we are able to compute inverse elements.
- The ring of integers $\mathbb{Z}$. The division with remainder in $\mathbb{Z}$ allows us to solve the ideal membership problem, while the least common multiple allows us to compute finite generating sets of syzygies, see Theorem 2.2.5 in [Wie11] for the latter.
- Also, $\mathbb{Z}/m\mathbb{Z}$ for an arbitrary $m \in \mathbb{Z}$. While it generally is neither Euclidean nor factorial like $\mathbb{Z}$, many problems can nonetheless be solved by tracing them back to the integers.
- Similarly, any Euclidean ring for which we are able to compute its division with remainder, or, more generally, any factorial ring for which we can compute the unique factorization. Classical examples hereof are the ring of Gaussian integers $\mathbb{Z}[i]$, the polynomial ring $\mathbb{Q}[y]$, the power series ring $\mathbb{Q}[\![s]\!]$ or multivariate polynomial rings.

- Moreover, thanks to the theory of Gröbner bases, any quotient ring of a polynomial ring, e.g. the ring of Laurent polynomials $K[y_1^{\pm 1},\dots,y_n^{\pm 1}] = K[y_0,\dots,y_n]/(1-y_0\cdots y_n)$.
- And, thanks to the theory of standard bases, any localization of a polynomial ring at a prime ideal, as it can be traced back to a quotient of a polynomial ring localized at a mixed ordering, see [Mor91].
- Also, Dedeking domains. A solution to the ideal membership problem and the computation of syzygies can be found in [HKY10].
- Finally, product rings like $\mathbb{Z}\times\mathbb{Z}$, because any ideal in it is the product of two ideals in $\mathbb{Z}$.

We now begin with introducing some very basic notions of standard basis theory to our ring resp. module, definitions such as monomials, monomial orderings and leading monomials.

Definition 1.3
The *set of monomials* of $R[\![t]\!][x]$ is defined to be

$$\mathrm{Mon}(t,x) := \{t^\beta x^\alpha \mid \beta\in\mathbb{N}^m, \alpha\in\mathbb{N}^n\} \subseteq R[\![t]\!][x],$$

and a *monomial ordering* on $\mathrm{Mon}(t,x)$ is an ordering $>$ that is compatible with its natural semigroup structure, i.e.

$$\forall a,b,q\in\mathrm{Mon}(t,x): \quad a>b \quad\Longrightarrow\quad q\cdot a > q\cdot b.$$

We call a monomial ordering $>$ *t-local*, if $1>t^\beta$ for all $\beta\in\mathbb{N}^m$.
Let $>$ be a t-local monomial ordering on $\mathrm{Mon}(t,x)$, and let $w\in\mathbb{R}^m_{<0}\times\mathbb{R}^n$ be a weight vector. Then the ordering $>_w$ is defined to be:

$$\begin{aligned} t^\beta x^\alpha >_w t^\delta x^\gamma\cdot \quad :\Longleftrightarrow \quad & w\cdot(\beta,\alpha) > w\cdot(\delta,\gamma) \text{ or}\\ & w\cdot(\beta,\alpha) = w\cdot(\delta,\gamma) \text{ and } t^\beta x^\alpha > t^\delta x^\gamma. \end{aligned}$$

We will refer to orderings of the form $>_w$ as a *weighted ordering* with weight vector w and tiebreaker $>$.

Definition 1.4
The *set of module monomials* of $R[\![t]\!][x]^s$ is defined to be

$$\mathrm{Mon}^s(t,x) := \{t^\beta x^\alpha\cdot e_i \mid \beta\in\mathbb{N}^m, \alpha\in\mathbb{N}^n, i=1,\dots,s\} \subseteq R[\![t]\!][x]^s.$$

A *monomial ordering* on $\mathrm{Mon}^s(t,x)$ is an ordering $>$ that is compatible with the natural $\mathrm{Mon}(t,x)$-action on it, i.e.

$$\forall a,b\in\mathrm{Mon}^s(t,x)\ \ \forall q\in\mathrm{Mon}(t,x): \quad a>b \quad\Longrightarrow\quad q\cdot a>q\cdot b,$$

and that restricts onto the same monomial ordering on $\mathrm{Mon}(t,x)$ in each component, i.e.

$$\forall a,b\in\mathrm{Mon}(t,x)\ \ \forall i,j\in\{1,\dots,s\}: \quad a\cdot e_i > b\cdot e_i \quad\Longleftrightarrow\quad a\cdot e_j > b\cdot e_j.$$

We call a monomial ordering $>$ *t-local*, if $1 \cdot e_i > t^\beta \cdot e_i$ for all $\beta \in \mathbb{N}^m$ and $i = 1, \ldots, s$. Let $>$ be a t-local monomial ordering on $\mathrm{Mon}^s(t,x)$, and let $w \in \mathbb{R}^m_{<0} \times \mathbb{R}^n \times \mathbb{R}^s$ be a weight vector. Then the ordering $>_w$ is defined to be:

$$\begin{aligned} &t^\beta x^\alpha \cdot e_i >_w t^\delta x^\gamma \cdot e_j \quad \Longleftrightarrow \\ &\quad w \cdot (\beta, \alpha, e_i) > w \cdot (\delta, \gamma, e_j) \text{ or} \\ &\quad w \cdot (\beta, \alpha, e_i) = w \cdot (\delta, \gamma, e_j) \text{ and } t^\beta x^\alpha \cdot e_i > t^\delta x^\gamma \cdot e_j. \end{aligned}$$

We will refer to orderings of the form $>_w$ as a *weighted ordering* with weight vector w and tiebreaker $>$.
From now on, we will simply refer to module monomials as monomials.

Definition 1.5
Given a t-local monomial ordering $>$ on $\mathrm{Mon}^s(t,x)$ and an element $f = \sum_{\alpha,\beta,i} c_{\alpha,\beta,i} \cdot t^\beta x^\alpha \cdot e_i \in R[\![t]\!][x]^s$, we define its *leading monomial*, *leading coefficient*, *leading term* and *tail* to be

$$\begin{aligned} \mathrm{LM}_>(f) &= \max\{t^\beta x^\alpha \cdot e_i \mid c_{\alpha,\beta,i} \neq 0\}, \\ \mathrm{LC}_>(f) &= c_{\alpha,\beta,i}, \text{ where } t^\beta x^\alpha \cdot e_i = \mathrm{LM}_>(f), \\ \mathrm{LT}_>(f) &= c_{\alpha,\beta,i} \cdot t^\beta x^\alpha \cdot e_i, \text{ where } t^\beta x^\alpha \cdot e_i = \mathrm{LM}_>(f), \\ \mathrm{tail}_>(f) &= f - \mathrm{LT}_>(f). \end{aligned}$$

For a submodule $M \leq R[\![t]\!][x]^s$, we set

$$\begin{aligned} \mathrm{LM}_>(M) &= \langle \mathrm{LM}_>(f) \mid f \in M \rangle_{R[t,x]} \leq R[t,x]^s, \\ \mathrm{LT}_>(M) &= \langle \mathrm{LT}_>(f) \mid f \in M \rangle_{R[t,x]} \leq R[t,x]^s. \end{aligned}$$

Note that we regard the two modules above as submodules of $R[t,x]^s$, while the original module lies in $R[\![t]\!][x]^s$. We refer to $\mathrm{LT}_>(M)$ as the *leading module* of M with respect to $>$.

Example 1.6
Observe that in general

$$\mathrm{LM}_>(M) \neq \mathrm{LT}_>(M).$$

Consider the ideal

$$I := \langle 1 + t^6 x + t^4 y + t^7 x^2 + t^5 xy + t^8 y^2, 2 - t \rangle \trianglelefteq \mathbb{Z}[\![t]\!][x],$$

and let $>_w$ be the weighted ordering with weight vector $w = (-1, 3, 3)$ and any arbitrary tiebreaker. Then by weighted degree alone we have

$$\mathrm{LT}_{>_w}(I) = \langle t^5 xy, 2 \rangle \neq \mathrm{LM}_{>_w}(I) = \langle 1 \rangle,$$

since $\mathrm{LM}_{>_w}(2-t) = 1$. In fact, the last equation holds true for any t-local monomial ordering, while the former varies depending on the ordering. This is why the role of leading monomials in the classical standard basis theory over fields is played by leading terms over rings.

Remark 1.7
Note that the t-locality of the monomial ordering $>$ is essential for leading monomials and other associated objects to exist, as elements of $R[\![t]\!][x]$ resp. $R[\![t]\!][x]^s$ may be unbounded in their degrees of t.
However, given a weight vector in $\mathbb{R}^m_{<0}\times\mathbb{R}^n$ resp. $\mathbb{R}^m_{<0}\times\mathbb{R}^n\times\mathbb{R}^s$, a weighted monomial ordering does not need a t-local tiebreaker for leading monomials to be well-defined. But for sake of simplicity, we nevertheless assume all occuring monomial orderings to be t-local.

$\mathrm{Mon}(t,x)$ comes equipped with a natural notion of divisibility and least common multiple. For module monomials, we define:

Definition 1.8
For two module monomials $t^\beta x^\alpha \cdot e_i$ and $t^\delta x^\gamma \cdot e_j \in \mathrm{Mon}(t,x)^s$, we say

$$t^\beta x^\alpha \cdot e_i \text{ divides } t^\delta x^\gamma \cdot e_j \quad :\Longleftrightarrow \quad e_i = e_j \text{ and } t^\beta x^\alpha \text{ divides } t^\delta x^\gamma,$$

and in this case we set

$$\frac{t^\beta x^\alpha \cdot e_i}{t^\delta x^\gamma \cdot e_j} := \frac{t^\beta x^\alpha}{t^\delta x^\gamma} = t^{\beta-\delta}x^{\alpha-\gamma} \in \mathrm{Mon}(t,x).$$

We define the *least common multiple* of two module monomials $t^\beta x^\alpha\cdot e_i$ and $t^\delta x^\gamma \cdot e_j \in \mathrm{Mon}(t,x)^s$ to be

$$\mathrm{lcm}(t^\beta x^\alpha \cdot e_i, t^\delta x^\gamma \cdot e_j) := \begin{cases} \mathrm{lcm}(t^\beta x^\alpha, t^\delta x^\gamma)\cdot e_j, & \text{if } i=j, \\ 0, & \text{otherwise.} \end{cases}$$

We now devote the remaining section to proving the existence of a division with remainder, starting with its definition.

Definition 1.9
Let $>$ be a t-local monomial ordering on $\mathrm{Mon}^s(t,x)$. Given $f \in R[\![t]\!][x]^s$ and $g_1,\ldots,g_k \in R[\![t]\!][x]^s$ we say that a representation

$$f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$$

with $q_1,\ldots,q_k \in R[\![t]\!][x]$ and $r = \sum_{j=1}^s r_j \cdot e_j \in R[\![t]\!][x]^s$ satisfies
(ID1): if $\mathrm{LM}_>(f) \geq \mathrm{LM}_>(q_i\cdot g_i)$ for all $i=1,\ldots,k$,
(ID2): if $\mathrm{LT}_>(r) \notin \langle \mathrm{LT}_>(g_1),\ldots,\mathrm{LT}_>(g_k)\rangle$, unless $r=0$,
(DD1): if no term of $q_i \cdot \mathrm{LT}_>(g_i)$ lies in $\langle \mathrm{LT}_>(g_j) \mid j<i\rangle$ for all $i=1,\ldots,k$,
(DD2): if no term of r lies in $\langle \mathrm{LT}_>(g_1),\ldots,\mathrm{LT}_>(g_k)\rangle$,
(SID2): if $\mathrm{LT}_>(r_j\cdot e_j) \notin \langle \mathrm{LT}_>(g_1),\ldots,\mathrm{LT}_>(g_k)\rangle$, unless $r_j=0$, for all $j=1,\ldots,s$.

A representation satisfying (ID1) and (ID2) is called an *(indeterminate) division with remainder*, and a representation satisfying (DD1) and (DD2) is called a *determinate division with remainder*. In each of these two cases we call r a *remainder* or *normal form* of f with respect to $(g_1, \dots, g_k)$. Moreover, if the remainder r is zero, we call the representation a *standard representation* of f with respect to $(g_1, \dots, g_k)$.
A division with remainder of $u \cdot f$ for some $u \in R[\![t]\!][x]$ with $\mathrm{LT}_>(u) = 1$ is also called a *weak division with remainder* of f. A remainder of $u \cdot f$ will be called a *weak normal form* of f with respect to $(g_1, \dots, g_k)$, and a standard representation of $u \cdot f$ will be called a *weak standard representation* of f.

Proposition 1.10
Consider a representation

$$f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r \quad \textit{or} \quad u \cdot f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$$

with $f, g_1, \dots, g_k, r \in R[\![t]\!][x]^s$, $q_1, \dots, q_k \in R[\![t]\!][x]$ *and* $\mathrm{LT}_>(u) = 1$. *Then:*
(1) if the representation satisfies (DD2)*, then it also satisfies* (SID2)*,*
(2) if the representation satisfies (SID2)*, then it also satisfies* (ID2)*,*
(3) if it satisfies both (DD1) *and* (ID2)*, then it also satisfies* (ID1)*.*
In particular, (DD1) *and* (DD2) *imply* (ID1) *and* (ID2)*.*

Proof. (1) and (2) are obvious, so suppose the representation satisfies both (DD1) and (DD2).
Take the maximal monomial $t^\beta x^\alpha$ occurring in any of the expressions $q_i \cdot g_i$ or r on the right hand side, and assume $t^\beta x^\alpha > \mathrm{LM}_>(f)$. Because of maximality, it has to be the leading monomial of each expression it occurs in. And because it does not occur on the left hand side, the leading terms have to cancel each other out. Let $q_{i_1} \cdot g_{i_1}, \dots, q_{i_l} \cdot g_{i_l}$ be the $q_i \cdot g_i$ containing $t^\beta x^\alpha$ with $i_1 < \ldots < i_l$.
If r contains $t^\beta x^\alpha$, then $\sum_{j=1}^{l} \mathrm{LT}_>(q_{i_j} \cdot g_{i_j}) + \mathrm{LT}_>(r) = 0$, and hence

$$\mathrm{LT}_>(r) = t^\beta x^\alpha \in \langle \mathrm{LT}_>(g_1), \dots, \mathrm{LT}_>(g_k) \rangle,$$

contradicting (ID2).
If r does not contain a, then we have $\sum_{j=1}^{l} \mathrm{LT}_>(q_{i_j} \cdot g_{i_j}) = 0$, thus

$$\mathrm{LT}_>(q_{i_l} \cdot g_{i_l}) \in \langle \mathrm{LT}_>(g_j) \mid j < i_l \rangle,$$

contradicting (DD1). □

Next, we pay a little attention to our ground ring. Convention 1.1 states that our ring already comes equipped with everything we need to compute representations of members in given ideals, but we still need to make sure that these representations satisfy our needs in Algorithm 1.13.

Algorithm 1.11 (Div_R, division in the ground ring)
Input: (b, C), where $C = (c_1, \dots, c_k) \in R^k$ and $b \in \langle C \rangle$.

Output: $(a_1, \ldots, a_k) \subseteq R^k$, such that

$$b = a_1 \cdot c_1 + \ldots + a_k \cdot c_k$$

with $a_i \cdot c_i \notin \langle c_j \mid j < i\rangle$ unless $a_i \cdot c_i = 0$, for any $i = 1, \ldots, k$.

Find $a_1, \ldots, a_k \in R$ with $b = a_1 \cdot c_1 + \ldots + a_k \cdot c_k$, which is possible by Convention 1.1.
for $i = k, \ldots, 1$ **do**
  if $a_i \cdot c_i \neq 0$ and $a_i \cdot c_i \in \langle c_j \mid j < i\rangle$ **then**
    Find $h_1, \ldots, h_{i-1} \in R$ such that $a_i \cdot c_i = h_1 \cdot c_1 + \ldots + h_{i-1} \cdot c_{i-1}$.
    Set $a_j := a_j + h_j$ for all $j < i$, and $a_i := 0$.
return $(a_1, \ldots, a_k)$

Proof. Termination and correctness are obvious. □

With this preparation we are able to formulate and prove determinate division with remainder for x-homogeneous ideals and modules.

Definition 1.12
For an element $f = \sum_{\beta,\alpha,i} c_{\alpha,\beta,i} \cdot t^\beta x^\alpha \cdot e_i \in R[\![t]\!][x]^s$ we define its *x-degree* to be

$$\deg_x(f) := \max\{|\alpha| \mid c_{\alpha,\beta,i} \neq 0\},$$

and we call it *x-homogeneous*, if all its terms are of the same x-degree.
Given a weight vector $w \in \mathbb{R}^m_{<0} \times \mathbb{R}^n \times \mathbb{R}^s$, we define its *weighted degree* with respect to w to be

$$\deg_w(f) := \max\{w \cdot (\beta, \alpha, e_i) \mid c_{\alpha,\beta,i} \neq 0\},$$

and we call it *weighted homogeneous* with respect to w, if all its terms are of the same weighted degree.

Algorithm 1.13 (HDDwR, homogeneous determinate division with remainder)
Input: $(f, G, >)$, where $f \in R[\![t]\!][x]^s$ x-homogeneous, $G = (g_1, \ldots, g_k)$ a k-tuple of x-homogeneous elements in $R[\![t]\!][x]^s$ and $>$ be a t-local monomial ordering on $\mathrm{Mon}^s(t, x)$.
Output: (Q, r), where $Q = (q_1, \ldots, q_k) \in R[\![t]\!][x]^k$ and $r \in R[\![t]\!][x]^s$ such that

$$f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$$

satisfies

(DD1): no term of $q_i \cdot \mathrm{LT}_>(g_i)$ lies in $\langle \mathrm{LT}_>(g_j) \mid j < i\rangle$ for all i,
(DD2): no term of r lies in $\langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_k)\rangle$,
(DDH): the $q_1, \ldots, q_k, r$ are either 0 or x-homogeneous of x-degree $\deg_x(f) - \deg_x(g_1), \ldots, \deg_x(f) - \deg_x(g_k), \deg_x(f)$ respectively.

Set $q_i := 0$ for $i = 1, \ldots, k$, $r := 0$, $\nu := 0$, $f_\nu := f$.
while $f_\nu \neq 0$ **do**
  if $\mathrm{LT}_>(f_\nu) \in \langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_k)\rangle$ **then**

Let $D_\nu := \{g_i \in G \mid \mathrm{LM}_>(g_i) \text{ divides } \mathrm{LM}_>(f_\nu)\}\{g_{i_1}, \dots, g_{i_l}\}$.
Compute $(a_{i_1}, \dots, a_{i_l}) = \mathrm{Div}_R(\mathrm{LC}_>(f_\nu), (\mathrm{LC}_>(g_{i_1}), \dots, \mathrm{LC}_>(g_{i_l})))$.
Set

$$q_{i,\nu} := \begin{cases} a_i \cdot \frac{\mathrm{LM}_>(f_\nu)}{\mathrm{LM}_>(g_i)} & \text{, if } g_i \in D_\nu, \\ 0 & \text{, otherwise,} \end{cases}$$

for $i = 1, \dots, k$, and $r_\nu := 0$.
else
Set $q_{i,\nu} := 0$, for $i = 1, \dots, k$, and $r_\nu := \mathrm{LT}_>(f_\nu)$.
Set $q_i := q_i + q_{i,\nu}$ for $i = 1, \dots, k$ and $r := r + r_\nu$.
Set $f_{\nu+1} := f_\nu - (q_{1,\nu} \cdot g_1 + \dots + q_{k,\nu} \cdot g_k + r_\nu)$ and $\nu := \nu + 1$.
return $((q_1, \dots, q_k), r)$

Proof. Note that we have a descending chain of terms to be eliminated

$$\mathrm{LM}_>(f_0) > \mathrm{LM}_>(f_1) > \mathrm{LM}_>(f_2) > \dots,$$

which implies that, except the terms that are zero, we have $k+1$ descending chains of factors and remainders

$$\begin{array}{ccccccc} \mathrm{LM}_>(q_{i,0}) & > & \mathrm{LM}_>(q_{i,1}) & > & \mathrm{LM}_>(q_{i,2}) & > & \dots \;, \\ \mathrm{LM}_>(r_0) & > & \mathrm{LM}_>(r_1) & > & \mathrm{LM}_>(r_2) & > & \dots \;. \end{array}$$

By construction, each $q_{i,\nu}$, $i = 1, \dots, k$, is x-homogeneous of x-degree $\deg_x(f) - \deg_x(g_i)$, and each r_ν is x-homogeneous of x-degree $\deg_x(f)$, unless they are zero. Because of Lemma 1.14 we may assume that the ordering $>$ is a t-local weighted monomial ordering. Thus, by Lemma 1.16, the $q_{i,\nu}$ and r_ν converge to zero in the $\langle t \rangle$-adic topology, so that

$$q_i := \sum_{\nu=0}^{\infty} q_{i,\nu} \in R[\![t]\!][x] \text{ and } r := \sum_{\nu=0}^{\infty} r_\nu \in R[\![t]\!][x]^s$$

exist and the following representation satisfies (DDH):

$$f = q_1 \cdot g_1 + \dots + q_k \cdot g_k + r. \tag{1}$$

Observe that, because all $q_{i,\nu}$ and r_ν are terms with distinct monomials, each non-zero term of $q_i \cdot \mathrm{LT}_>(g_i)$ or r equals $q_{i,\nu} \cdot \mathrm{LT}_>(g_i)$ or r_ν respectively, for some $\nu \in \mathbb{N}$. So first, let p be a non-zero term of $q_i \cdot \mathrm{LT}_>(g_i)$, say $p = q_{i,\nu} \cdot \mathrm{LT}_>(g_i)$ for some $\nu \in \mathbb{N}$. Then $\mathrm{LC}_>(q_{i,\nu}) \neq 0$ implies that $\mathrm{LC}_>(q_{i,\nu} \cdot g_i) \notin \langle \mathrm{LC}_>(g_j) \mid j < i \text{ with } g_j \in D_\nu \rangle_R$. In particular, we have $\mathrm{LT}_>(q_{i,\nu} \cdot g_i) = q_{i,\nu} \cdot \mathrm{LT}_>(g_i) \notin \langle \mathrm{LT}_>(g_j) \mid j < i \text{ with } g_j \in D_\nu \rangle$. Therefore we also get $q_{i,\nu} \cdot \mathrm{LT}_>(g_i) \notin \langle \mathrm{LT}_>(g_j) \mid j < i \rangle$, since the leading monomials of all $g_j \notin D_\nu$ do not divide $\mathrm{LM}_>(f_\nu) = \mathrm{LM}_>(q_{i,\nu} \cdot g_i)$. Thus (1) satisfies (DD1).
Lastly, let p be a non-zero term of r, i.e. $p = r_\nu$ for a suitable ν. But because $r_\nu \neq 0$, we have $r_\nu = \mathrm{LT}_>(f_\nu) \notin \langle \mathrm{LT}_>(g_1), \dots, \mathrm{LT}_>(g_k) \rangle$ by default. Therefore, our representation (1) also satisfies (DD2). □

In the proof we have used the following two Lemmata whose proof can be found in [Mar08]. The first Lemma allows us to restrict ourselves to weighted monomial orderings, while the second guarantees $\langle t\rangle$-adic convergence.

Lemma 1.14 ([Mar08] Lemma 2.5)
Let $>$ be a t-local monomial ordering on $\mathrm{Mon}^s(t,x)$, and let $g_1,\dots,g_k \in R[\![t]\!][x]^s$ be x-homogeneous. Then there exists a weight vector $w \in \mathbb{R}^m_{<0}\times\mathbb{R}^{n+s}$ such that any t-local weight ordering with weight vector w, say $>_w$, induces the same leading monomials as $>$ on $g_1,\dots,g_k$, i.e.

$$\mathrm{LM}_{>_w}(g_i) = \mathrm{LM}_{>}(g_i) \text{ for all } i = 1,\dots,k.$$

Example 1.15
A monomial ordering can always be expressed by an invertible matrix. For example, the lexicographical ordering $>$ on $\mathrm{Mon}(t,x)$ with $x_1 > x_2 > 1 > t$ is given by

$$t^\beta x^\alpha > t^\delta x^\gamma \quad\Longleftrightarrow\quad A\cdot(\beta,\alpha)^t > A\cdot(\delta,\gamma)^t, \text{ where } A = \begin{pmatrix} 0 & 1 & 0\\ 0 & 0 & 1\\ -1 & 0 & 0\end{pmatrix},$$

where the $>$ on the right hand side denotes the lexicographical ordering on $\mathbb{R}^3$. Consider the polynomial $g = t^5x_1 + t^2x_2$. In order to find a weight vector $w \in \mathbb{R}_{<0}\times\mathbb{R}^2$ such that $\mathrm{LM}_{>_w}(g) = \mathrm{LM}_{>}(g) = t^5x_1$, consider the first row vector of A, $a_1 = (0,1,0)\in\mathbb{R}^3$. Since $a_1 \notin \mathbb{R}_{<0}\times\mathbb{R}^2$ it represents no viable choice for w. But because $\deg_{a_1}(t^5x_1) > \deg_{a_1}(t^2x_2)$, adding a sufficiently small negative weight in t will not break the strict inequality. Hence we obtain $w = (-\frac{1}{5},1,0)\in\mathbb{R}_{<0}\times\mathbb{R}^2$:

$$\begin{array}{ccccccc}
\deg_{(0,1,0)}(t^5x_1) & = & 1 & > & 0 & = & \deg_{(0,1,0)}(t^2x_2)\\
\big\downarrow{\scriptstyle -(1/5,0,0)} & & & & & & \big\downarrow{\scriptstyle -(1/5,0,0)}\\
\deg_{(-1/5,1,0)}(t^5x_1) & = & 0 & > & -\frac{2}{5} & = & \deg_{(-1/5,1,0)}(t^2x_2).
\end{array}$$

In particular, a determinate division with remainder with respect to $>_w$ will also be a determinate division with remainder with respect to $>$, as (DD1) and (DD2) are only dependant on the leading terms.

Lemma 1.16 ([Mar08] Lemma 2.6)
Let $>_w$ be a t-local monomial ordering on $\mathrm{Mon}^s(t,x)$ with weight vector $w\in\mathbb{R}^m_{<0}\times\mathbb{R}^{n+s}$, and let $(f_k)_{k\in\mathbb{N}}$ be a sequence of x-homogeneous elements of fixed x-degree in $R[\![t]\!][x]^s$ such that $\mathrm{LM}_{>_w}(f_k) > \mathrm{LM}_{>_w}(f_{k+1})$ for all $k\in\mathbb{N}$. Then $(f_k)_{k\in\mathbb{N}}$ converges to zero in the $\langle t\rangle$-adic topology, i.e.

$$\forall\, N\in\mathbb{N}\ \exists\, M\in\mathbb{N}:\ \ f_k \in \langle t\rangle^N\cdot R[\![t]\!][x]^s\ \ \forall k\geq M.$$

In particular, the element $\sum_{k=0}^\infty f_k \in R[\![t]\!][x]^s$ exists.

Remark 1.17 (polynomial input)
In case $m=0$, i.e. $R[\![t]\!][x]^s = R[x]^s$, all $f,g_1,\dots,g_k\in R[x]^s$ are homogeneous and so

is any polynomial appearing in our algorithm. Moreover, all f_ν, unless $f_\nu = 0$, have the same x-degree as f. And since there are only finitely many monomials of a given degree, there cannot exist an infinite sequence of decreasing leading monomials

$$\mathrm{LM}_>(f_0) > \mathrm{LM}_>(f_1) > \mathrm{LM}_>(f_2) > \dots ,$$

and Algorithm 1.13 has to terminate.

Remark 1.18 (weighted homogeneous input)
Similar to how the output is x-homogeneous because the input is x-homogeneous, note that if the input is weighted homogeneous with respect to a certain weight vector $w \in \mathbb{R}^m_{<0} \times \mathbb{R}^n$, then so is the output. This will be essential when computing tropical varieties over the p-adic numbers.

Example 1.19
Over a ground field, as in the proof of Theorem 2.1 in [Mar08], all the terms of f_ν can be simultaneously checked for containment in $\langle \mathrm{LT}_>(g_1), \dots, \mathrm{LT}_>(g_k)\rangle$, eliminating the terms which lie in the ideal using $g_1, \dots, g_k$ and discarding the terms which are outside the ideal to the remainder. However, this is not possible if R is no field.
Let $f = 2x, g = 2x + 2tx + t^2x + 3t^3x \in \mathbb{Z}[\![t]\!][x]$ and consider a weighted ordering $> = >_w$ with weight vector $w = (-1, 1) \in \mathbb{R}_{<0} \times \mathbb{R}$. Then Figure 1 illustrates a division algorithm, which discards any term of f_ν not divisible by $\mathrm{LT}_>(g)$ directly to the remainder. The underlined term marks the respective leading term.

$$\begin{array}{rcl} f_0 & = & \underline{2x} \\ & {\scriptstyle -g}\big\downarrow & \\ f_1 & = & -\underline{2tx} - \overbrace{t^2x - 3t^3x}^{\text{to remainder}} \\ & {\scriptstyle +tg}\big\downarrow & \\ f_2 & = & \underline{2t^2x} + \overbrace{t^3x + 3t^4x}^{\text{to remainder}} \\ & {\scriptstyle -t^2g}\big\downarrow & \\ f_3 & = & -\underline{2t^3x} - \overbrace{t^4x - 3t^5x}^{\text{to remainder}} \\ & \vdots & \end{array} \qquad \begin{array}{c} r \\ \| \\ -t^2x \\ - \\ 3t^3x \\ + \\ t^3x \\ + \\ 3t^4x \\ - \\ t^4x \\ - \\ 3t^5x \\ \vdots \end{array}$$

FIGURE 1. division slice by slice

Not only would this process continue indefinitely, every term in our remainder but the first would actually be divisible by $\mathrm{LT}_>(g)$:

$$r = -t^2x - 3t^3x + t^3x + 3t^4x - t^4x - \dots = -xt^2 - 2xt^3 + 2xt^4 - 2xt^5 + \dots .$$

As we see, it is important to know when terms can be safely discarded to the remainder, and the only way to guarantee that is by proceeding term by term instead of slice by slice. And in order to guarantee that our result converges in the $\langle t\rangle$-adic topology, the order needs to be compatible with a weighted monomial order $>_w$ with $w \in \mathbb{R}^m_{<0} \times \mathbb{R}^{n+s}$. Figure 2 shows the same example in our algorithm.

$$
\begin{array}{rrcll}
 & f_0 & = & \underline{2x} & r \\
{\scriptstyle -g} & & \Big\downarrow & & \| \\
 & f_1 & = & -\underline{2tx} - \overbrace{t^2x - 3t^3x}^{\text{to be processed}} & \\
{\scriptstyle +tg} & & \Big\downarrow & & \\
 & f_2 & = & \underline{t^2x} - 2t^3x + 3t^4x & t^2x \\
\text{to remainder} & & \Big\downarrow & & \\
 & f_3 & = & -\underline{2t^3x} + 3t^4x & \\
{\scriptstyle +t^2g} & & \Big\downarrow & & + \\
 & f_4 & = & \underline{5t^4x} + t^5x + 3t^6x & 5t^4x \\
\text{to remainder} & & \Big\downarrow & & + \\
 & & \vdots & & t^5x \\
 & & & & + \\
\text{to remainder} & & \Big\downarrow & & 3t^6x \\
 & f_7 & = & 0 &
\end{array}
$$

FIGURE 2. division term by term

We obtain a representation satisfying (DD1), (DD2) and (DDH):

$$f = (\underbrace{1 - t - t^3}_{=q}) \cdot g + (\underbrace{xt^2 + 5xt^4 + xt^5 + 3xt^6}_{=r}).$$

Having constructed a homogeneous determinate division with remainder, we will now introduce homogenization, dehomogenization and the ecart to continue with a weak division with remainder.

Definition 1.20 (Homogenization and dehomogenization)
For an element $f = \sum_{\beta,\alpha,i} c_{\alpha,\beta,i} \cdot t^\beta x^\alpha \cdot e_i \in R[\![t]\!][x]^s$ we define its *homogenization* to be

$$f^h := \sum_{\alpha,\beta,i} c_{\alpha,\beta,i} \cdot t^\beta x_0^{\deg_x(f)-|\alpha|} x^\alpha \cdot e_i \in R[\![t]\!][x_h]^s$$

with $x_h = (x_0, x) = (x_0, x_1, \ldots, x_n)$. And for an element $F \in R[\![t]\!][x_h]^s$ we define its *dehomogenization* to be $F|_{x_0=1} \in R[\![t]\!][x]^s$.

Remark 1.21 (Homogenization and dehomogenization)
Any monomial ordering $>$ on $\mathrm{Mon}^s(t,x)$, can be naturally extended to an ordering $>_h$ on $\mathrm{Mon}^s(t,x_0,x)$ through

$$a >_h b \quad :\Longleftrightarrow \quad \begin{array}{l} \deg_{x_h}(a) > \deg_{x_h}(b) \text{ or} \\ \deg_{x_h}(a) = \deg_{x_h}(b) \text{ and } a|_{x_0=1} > b|_{x_0=1}. \end{array}$$

Defining the *ecart* of an element $f \in R[\![t]\!][x]^s$ with respect to $>$ to be

$$\mathrm{ecart}_>(f) := \deg_x(f) - \deg_x(\mathrm{LM}_>(f)) \in \mathbb{N},$$

one can show that for any elements $g, f \in R[\![t]\!][x]^s$ and any x_h-homogeneous $F \in R[\![t]\!][x_h]$:

(1) $f = (f^h)^d$,
(2) $F = x_0^{\deg_{x_h}(F) - \deg_x(F^d)} \cdot (F^d)^h$,
(3) $\mathrm{LT}_{>_h}(f^h) = x_0^{\mathrm{ecart}_>(f)} \cdot \mathrm{LT}_>(f)$,
(4) $\mathrm{LT}_{>_h}(F) = x_0^{\mathrm{ecart}_>(F^d) + \deg_{x_h}(F) - \deg_x(F^d)} \cdot \mathrm{LT}_>(F^d)$,
(5) $\mathrm{LM}_{>_h}(g^h) | \mathrm{LM}_{>_h}(f^h) \quad \Longleftrightarrow$
$\quad \mathrm{LM}_>(g) | \mathrm{LM}_>(f)$ and $\mathrm{ecart}_>(g) \leq \mathrm{ecart}_>(f)$,
(6) $\mathrm{LM}_{>_h}(g^h) \mid \mathrm{LM}_{>_h}(F) \quad \Longleftarrow$
$\quad \mathrm{LM}_>(g) | \mathrm{LM}_>(F^d)$ and $\mathrm{ecart}_>(g) \leq \mathrm{ecart}_>(F^d)$.

With this preparation we are now able to formulate and prove weak division with remainder.

Algorithm 1.22 (DwR, weak division with remainder)
Input: $(f, G, >)$, where $f \in R[\![t]\!][x]^s$ and $G = (g_1, \ldots, g_k)$ is a k-tuple in $R[\![t]\!][x]^s$ and $>$ a weighted t-local monomial ordering on $\mathrm{Mon}^s(t,x)$.
Output: (u, Q, r), where $u \in R[\![t]\!][x]$ with $\mathrm{LT}_>(u) = 1$, $Q = (q_1, \ldots, q_k) \subseteq R[\![t]\!][x]^k$ and $r \in R[\![t]\!][x]^s$ such that

$$u \cdot f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$$

satisfies

(ID1): $\mathrm{LM}_>(f) \geq \mathrm{LM}_>(q_i \cdot g_i)$ for $i = 1, \ldots, k$ and
(ID2): $\mathrm{LT}_>(r) \notin \langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_k) \rangle$, unless $r = 0$.

Moreover, the algorithm requires only a finite number of recursions.

if $f \neq 0$ and $\mathrm{LT}_>(f) \in \langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_k) \rangle$ **then**
  Set $D := \{g_i \in G \mid \mathrm{LM}_>(g_i) \text{ divides } \mathrm{LM}_>(f)\}$ and $D' := \emptyset$.
  while $\mathrm{LT}_>(f) \notin \langle \mathrm{LT}_>(g_i) \mid g_i \in D' \rangle$ **do**
    Pick $g \in D$ with minimal ecart.

Set $D' := D' \cup \{g\}$ and $D := D \setminus \{g\}$.
if $e := \max\{\mathrm{ecart}_>(g) \mid g \in D'\} - \mathrm{ecart}_>(f) > 0$ **then**
Compute
$$((Q'_1, \dots, Q'_k), R') := \mathrm{HDDwR}(x_0^e \cdot f^h, (\mathrm{LT}_>(g_1^h), \dots, \mathrm{LT}_>(g_k^h)), >_h).$$
Set $f' := (x_0^e \cdot f^h - \sum_{i=1}^k Q'_i \cdot g_i^h)^d$.
Run
$$(u'', (q''_1, \dots, q''_{k+1}), r) := \mathrm{DwR}(f', (g_1, \dots, g_k, f), >).$$
Set $q_i := q''_i + u'' \cdot Q_i'^d$, $i = 1, \dots, k$.
Set $u := u'' - q''_{k+1}$.
else
Compute
$$((Q'_1, \dots, Q'_k), R') := \mathrm{HDDwR}(f^h, (g_1^h, \dots, g_k^h), >_h).$$
Run
$$(u, (q''_1, \dots, q''_k), r) := \mathrm{DwR}((R')^d, (g_1, \dots, g_k), >).$$
Set $q_i := q''_i + u \cdot Q_i'^d$, $i = 1, \dots, k$.
else
Set $(u, (q_1, \dots, q_k), r) := (1, (0, \dots, 0), f)$.
return $(u, (q_1, \dots, q_k), r)$.

Proof. Finiteness of recursions: For sake of clarity, label all the objects appearing in the ν-th recursion step by a subscript ν. For example the ecart $e_\nu \in \mathbb{N}$, the element $f_\nu \in R[\![t]\!][x]^s$ and the subset $G_\nu \subseteq R[\![t]\!][x]^s$.
Since $G_1^h \subseteq G_2^h \subseteq G_3^h \subseteq \dots$, we have an ascending chain of leading ideals in $R[\![t]\!][x_h]^s$, which eventually stabilizes unless the algorithm terminates beforehand
$$\mathrm{LT}_{>_h}(G_1^h) \subseteq \mathrm{LT}_{>_h}(G_2^h) \subseteq \dots \subseteq \mathrm{LT}_{>_h}(G_N^h) = \mathrm{LT}_{>_h}(G_{N+1}^h) = \dots.$$
Assume $e_N > 0$. Then we'd have $f_N \in G_{N+1}$, and thus
$$\mathrm{LT}_{>_h}(f_N^h) \in \mathrm{LT}_{>_h}(G_{N+1}^h) = \mathrm{LT}_{>_h}(G_N^h).$$
To put it differently, we'd have
$$\mathrm{LT}_{>_h}(f_N^h) \in \langle \mathrm{LT}_{>_h}(g^h) \mid g^h \in G_N^h \text{ with } \mathrm{LM}_{>_h}(g^h) \text{ divides } \mathrm{LM}_{>_h}(f_N^h) \rangle,$$
which by Remark 1.21 (5) would imply that
$$\mathrm{LT}_>(f_N) \in \langle \mathrm{LT}_>(g) \mid g \in G_N \text{ with } \mathrm{LM}_>(g) \text{ divides } \mathrm{LM}_>(f_N), \text{ and } \mathrm{ecart}_>(g) \leq \mathrm{ecart}_>(f_N) \rangle.$$
Consequently, we'd get
$$D'_N \subseteq \{g \in G_N \mid \mathrm{LM}_>(g) \text{ divides } \mathrm{LM}_>(f_N) \text{ and } \mathrm{ecart}_>(g) \leq \mathrm{ecart}_>(f_N)\},$$

contradicting our assumption

$$e_N = \max\{\mathrm{ecart}_>(g) \mid g \in D'_N\} - \mathrm{ecart}_>(f_N) \overset{!}{>} 0. \quad ↯$$

Therefore we have $e_N \leq 0$. By induction we conclude that $e_\nu \leq 0$ for all $\nu \geq N$, i.e. that we will exclusively run through steps 14-16 of the "else" case from the N-th recursion step onwards.

By the properties of HDDwR we know that in particular

$$\mathrm{LT}_{>_h}(R'_N) \notin \mathrm{LT}_{>_h}(G^h_N).$$

Now assume that the recursions would not stop with the next recursion. That means there exists a $D'_{N+1} \subseteq D_{N+1}$ with

$$\mathrm{LT}_>((R'_N)^d) = \mathrm{LT}_>(f_{N+1}) \in \langle \mathrm{LT}_>(g) \mid g \in D'_{N+1} \rangle$$

such that $e_{N+1} = \max\{\mathrm{ecart}_>(g) \mid g \in D'_{N+1}\} - \mathrm{ecart}_>((R'_N)^d) \leq 0$. From Remark 1.21 (6), this immediately implies the following contradiction

$$\mathrm{LT}_{>_h}(R'_N) \in \mathrm{LT}_{>_h}(G^h_{N+1}) = \mathrm{LT}_{>_h}(G^h_N). \quad ↯$$

Hence the algorithm terminates after the $N+1$-th recursion step.

Correctness: We make an induction on the number of recursions, say $N \in \mathbb{N}$. If $N = 1$ then either $f = 0$ or $\mathrm{LT}_>(f) \notin \langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_k) \rangle$, and in both cases

$$1 \cdot f = 0 \cdot g_1 + \ldots + 0 \cdot g_k + f$$

satisfies (ID1) and (ID2).

So suppose $N > 1$ and consider the first recursion step. If $e \leq 0$, then by the properties of HDDwR the representation

$$f^h = Q'_1 \cdot g^h_1 + \ldots + Q'_k \cdot g^h_k + R'$$

satisfies (DD1), (DD2) and (DDH). (DD1) and (DD2) imply (ID1), which means that for each $i = 1, \ldots, k$ we have

$$x_0^{\mathrm{ecart}_>(f)} \cdot \mathrm{LM}_>(f) = \mathrm{LM}_{>_h}(f^h) \overset{\text{(ID1)}}{\geq_h} \mathrm{LM}_{>_h}(Q'_i) \cdot \mathrm{LM}_{>_h}(g^h_i) = \ldots$$
$$\ldots = x_0^{a_i + \mathrm{ecart}_>(g_i)} \cdot \mathrm{LM}_>(Q'^d_i) \cdot \mathrm{LM}_>(g_i)$$

for some $a_i \geq 0$. Since f^h and $Q'_i \cdot g^h_i$ are both x_h-homogeneous of the same x_h-degree by (DDH), the definition of the homogenized ordering $>_h$ implies

$$\mathrm{LM}_>(f) \geq \mathrm{LM}_>(Q'^d_i) \cdot \mathrm{LM}_>(g_i) \text{ for all } i = 1, \ldots, k. \tag{2}$$

Moreover, by induction the representation $u \cdot R'^d = q''_1 \cdot g_1 + \ldots + q''_k \cdot g_k + r$ satisfies (ID1), (ID2) and $\mathrm{LT}_>(u) = 1$, the first implying that

$$\mathrm{LM}_>(f) \overset{(17)}{\geq} \mathrm{LM}_> \underbrace{\left(f - \sum_{i=1}^{k} Q'^d_i \cdot g_i \right)}_{=R'^d} \overset{\text{(ID1)}}{\geq} \mathrm{LM}_>(q''_i \cdot g_i). \tag{3}$$

Therefore, the representation

$$u \cdot f = \sum_{i=1}^{k} (q_i'' + u \cdot Q_i'^d) \cdot g_i + r$$

satisfies (ID1) by (17), (18), $\mathrm{LT}_>(u) = 1$ and (ID2) by induction.
Similarly, if $e > 0$, then by the properties of HDDwR the representation

$$x_0^e \cdot f^h = Q_1' \cdot \mathrm{LT}_{>_h}(g_1^h) + \ldots + Q_k' \cdot \mathrm{LT}_{>_h}(g_k^h) + R'$$

satisfies (DD1), (DD2) and (DDH). (DD1) and (DD2) imply (ID1), which means that for each $i = 1, \ldots, k$ we have

$$x_0^{e+\mathrm{ecart}_>(f)} \cdot \mathrm{LM}_>(f) = \mathrm{LM}_{>_h}(x_0^e \cdot f^h) \geq \ldots$$

$$\ldots \geq \mathrm{LM}_{>_h}(Q_i') \cdot \mathrm{LM}_{>_h}(\mathrm{LT}_{>_h}(g_i^h)) = x_0^{a_i+\mathrm{ecart}_>(g_i)} \cdot \mathrm{LM}_>(Q_i'^d) \cdot \mathrm{LM}_>(g_i),$$

for some $a_i \geq 0$. Since $x_0^e \cdot f^h$ and $Q_i' \cdot \mathrm{LT}_{>_h}(g_i^h)$ are both x_h-homogeneous of the same x_h-degree by (DDH), the definition of the homogenized ordering $>_h$ implies

$$\mathrm{LM}_>(f) \geq \mathrm{LM}_>(Q_i'^d) \cdot \mathrm{LM}_>(g_i). \tag{4}$$

Moreover, by induction the representation $u'' \cdot f' = \sum_{i=1}^{k} q_i'' \cdot g_i + q_{k+1}'' \cdot f + r$ satisfies (ID1), (ID2) and $\mathrm{LT}_>(u'') = 1$ with the first implying that

$$\mathrm{LM}_>(f) \overset{(19)}{\geq} \underbrace{\mathrm{LM}_> \left(f - \sum_{i=1}^{k} Q_i'^d \cdot g_i \right)}_{=\mathrm{LM}_>(R'^d)} \overset{(\mathrm{ID1})}{\geq} \mathrm{LM}_>(q_i'' \cdot g_i). \tag{5}$$

Therefore, the representation

$$u \cdot f = \sum_{i=1}^{k} (q_i'' + u'' \cdot Q_i'^d) \cdot g_i + r, \text{ with } u = u'' - q_{k+1}''$$

satisfies (ID1) by (19), (20), $\mathrm{LT}_>(u'') = 1$ and (ID2) by induction.
To see that $\mathrm{LT}_>(u) = 1$, observe that

$$\mathrm{LT}_{>_h}(x_0^e \cdot f^h) \in \langle \mathrm{LT}_>(g_1^h), \ldots, \mathrm{LT}_>(g_k^h) \rangle,$$

which is why

$$\mathrm{LM}_>(f) = \mathrm{LM}_{>_h}(x_0^e \cdot f^h)^d > \mathrm{LM}_{>_h} \left(x_0^e \cdot f^h - \sum_{i=1}^{k} Q_i' \cdot g_i^h \right)^d = \mathrm{LM}_>(f').$$

Thus $\mathrm{LM}_>(f) > \mathrm{LM}_>(f') \geq \mathrm{LM}_>(q_{k+1}'') \cdot \mathrm{LM}_>(f)$, which necessarily implies $\mathrm{LM}(q_{k+1}'') < 1$. By induction we get $\mathrm{LT}_>(u) = \mathrm{LT}_>(u'') = 1$. $\square$

Remark 1.23 (polynomial input)
If the input is polynomial, $f, g_1, \ldots, g_k \in R[t,x]^s$, then we can regard them as elements of $R[\![t']\!][x'] = R[t,x]$ with $t' = ()$ and $x' = (t,x)$. In that case, our homogeneous determinate divisions with remainder terminates by Remark 1.17, and hence so does our weak division with remainder. In particular, the output $q_1, \ldots, q_k, r$ will be polynomial as well.

The next corollary will prove to be very useful in Theorem 2.14, though not for elements in $R[\![t]\!][x]^s$, but for elements in $R[\![t]\!][x]^k$ under the Schreyer ordering.

Corollary 1.24
Let $>$ be a t-local monomial ordering and $g_1, \ldots, g_k \in R[\![t]\!][x]^s$. Then any $f \in R[\![t]\!][x]^s$ has a weak division with remainder

$$u \cdot f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$$

with $r = \sum_{j=1}^s r_j e_j \in R[\![t]\!][x]^s$ satisfying
(SID2): $\mathrm{LT}_>(r_j \cdot e_j) \notin \langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_k) \rangle$, *unless $r_j = 0$, for $j = 1, \ldots, s$.*

Proof. We make an induction on s, in which the base case $s = 1$ follows from Algorithm 1.22, as condition (SID2) coincides with (ID2).
Suppose $s > 1$. By Algorithm 1.22 there exists a weak division with remainder

$$u \cdot f = q_i \cdot g_1 + \ldots + q_k \cdot g_k + r. \tag{6}$$

If $r = 0$, then the representation satisfies (SID2) and we're done. If $r \neq 0$, there is a unique $j \in \{1, \ldots, s\}$ such that $\mathrm{LT}_>(r) \in R[\![t]\!][x] \cdot e_j$. For sake of simplicity, suppose that $j = s$ and that $g_1, \ldots, g_k$ are ordered in such that

$$\underbrace{\mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_l)}_{\notin R[\![t]\!][x] \cdot e_s}, \quad \underbrace{\mathrm{LT}_>(g_{l+1}), \ldots, \mathrm{LT}_>(g_s)}_{\in R[\![t]\!][x] \cdot e_s} \quad \text{for some } 1 \leq l < s.$$

Consider the projection

$$\sigma : R[\![t]\!][x]^s \longrightarrow R[\![t]\!][x]^{s-1}, \quad (p_1, \ldots, p_s) \longmapsto (p_1, \ldots, p_{s-1}),$$

the inclusion

$$\iota : R[\![t]\!][x]^{s-1} \longrightarrow R[\![t]\!][x]^s, \quad (p_1, \ldots, p_{s-1}) \longmapsto (p_1, \ldots, p_{s-1}, 0),$$

and let $>_*$ denote the restriction of $>$ on $\mathrm{Mon}(t,x)^{s-1}$. Note that we have
(1) for $h \in R[\![t]\!][x]^{s-1}$: $\mathrm{LM}_>(\iota(h)) = \iota(\mathrm{LM}_{>_*}(h))$,
(2) for $i = 1, \ldots, l$: $\mathrm{LM}_>(g_i) = \mathrm{LM}_>(\iota(\sigma(g_i)))$.

By induction, there exists a weak division with remainder of $\sigma(r) \in R[\![t]\!][x]^{s-1}$ satisfying (SID2), say

$$u' \cdot \sigma(r) = q'_1 \cdot \sigma(g_1) + \ldots + q'_l \cdot \sigma(g_l) + r'. \tag{7}$$

Writing $r = \sum_{j=1}^{s} r_j \cdot e_j$ and $r' = \sum_{j=1}^{s-1} r'_j \cdot e_j$, we want to show that the following constructed representation

$$u \cdot u' \cdot f = \sum_{i=1}^{l} (u' \cdot q_i + q'_i) \cdot g_i + \sum_{i=l+1}^{k} u' \cdot q_i \cdot g_i + r'' \text{ with } r'' = \sum_{j=1}^{s-1} r'_j \cdot e_j + r_s \cdot e_s$$

is a weak division with remainder satisfying (SID2).

As (6) satisfies (ID2), (7) satisfies (ID1), and $\mathrm{LT}_>(r) \in R[\![t]\!][x]_> \cdot e_s$, we obtain for $i = 1, \ldots, l$

$$\mathrm{LM}_>(f) \geq \mathrm{LM}_>(r) > \mathrm{LM}_>(\iota(\sigma(r))) \geq \mathrm{LM}_>(\iota(q'_i \cdot \sigma(g_i))) = \ldots$$
$$\ldots = \mathrm{LM}_>(q'_i \cdot \iota(\sigma(g_i))) = \mathrm{LM}_>(q'_i \cdot g_i).$$

Now since (6) satisfies (ID1) and $\mathrm{LT}_>(u) = 1 = \mathrm{LT}_>(u')$, we have for $i \leq l$

$$\mathrm{LM}_>(u \cdot u' \cdot f) = \mathrm{LM}_>(f) \geq \mathrm{LM}_>((u' \cdot q_i + q'_i) \cdot g_i)$$

and for $i > l$

$$\mathrm{LM}_>(u \cdot u' \cdot f) = \mathrm{LM}_>(f) \geq \mathrm{LM}_>(q_i \cdot g_i) = \mathrm{LM}_>(u' \cdot q_i \cdot g_i),$$

proving that our constructed representation satisfies (ID1).
Moreover, (SID2) of (7) tells us that for $j = 1, \ldots, s-1$

$$\mathrm{LT}_{>_*}(r'_j \cdot e_j) \notin \langle \mathrm{LT}_{>_*}(\sigma(g_1)), \ldots, \mathrm{LT}_{>_*}(\sigma(g_l)) \rangle, \text{ unless } r'_j = 0,$$

And because $\mathrm{LT}_>(g_i) \in R[\![t]\!][x] \cdot e_s$ for $i > l$, we get for $j = 1, \ldots, s-1$

$$\mathrm{LT}_>(r'_j \cdot e_j) \notin \langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_s) \rangle, \text{ unless } r'_j = 0.$$

In addition, by (ID2) of (6), we have

$$\mathrm{LT}_>(r'_s \cdot e_s) = \mathrm{LM}_>(r) \notin \langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_s) \rangle,$$

which completes the proof that our constructed representation satisfies (SID2). By Proposition 1.10 this implies (ID2). □

We will now introduce localizations at monomial orderings. More than just a convenience to get rid of the u with $\mathrm{LM}_>(u) = 1$ in our weak division with remainder, localization at monomial orderings allows geometers to compute in localizations at ideals generated by variables. It is a technique that has been applied in the study of isolated singularities to great success.

Definition 1.25 (Localization at monomial orderings)
For a t-local monomial ordering $>$ on $\mathrm{Mon}(t, x)$, we define

$$S_> := \{u \in R[\![t]\!][x] \mid \mathrm{LT}_>(u) = 1\} \text{ and } R[\![t]\!][x]_> := S_>^{-1} R[\![t]\!][x].$$

We will refer to $R[\![t]\!][x]_>$ as $R[\![t]\!][x]$ *localized at the monomial ordering* $>$.

Let $>$ be a module monomial ordering on $\mathrm{Mon}^s(t,x)$. Recall that it restricts to the same monomial ordering on $\mathrm{Mon}(t,x)$ in each component by Definition 1.4, which we will denote by $>_{R[\![t]\!][x]}$. We then define for any $k \in \mathbb{N}$

$$R[\![t]\!][x]^s_> := S^{-1}_{>_{R[\![t]\!][x]}} \left(R[\![t]\!][x]^s \right).$$

We will refer to $R[\![t]\!][x]^s_>$ as $R[\![t]\!][x]^s$ *localized at the monomial ordering* $>$. For $s = 1$, it coincides with the first definition.

Our definitions on $R[\![t]\!][x]^s$ extend naturally to $R[\![t]\!][x]^s_>$, since for any element $f \in R[\![t]\!][x]^s_>$ there exists an element $u \in S_>$ such that $u \cdot f \in R[\![t]\!][x]^s$. We define the *leading monomial, leading coefficient* and *leading term* of f with respect to $>$ to be that of $u \cdot f \in R[\![t]\!][x]^s$. The *leading module* of a submodule $M \leq R[\![t]\!][x]^s_>$ is again the module generated by the leading terms of its elements.

And given $f, g_1, \ldots, g_k, r = \sum_{j=1}^s r_j \cdot e_j \in R[\![t]\!][x]^s_>$, we say a representation

$$f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$$

satisfies

(ID1): if $\mathrm{LM}_>(f) \geq \mathrm{LM}_>(q_i \cdot g_i)$ for all $i = 1, \ldots, k$,
(ID2): if $\mathrm{LT}_>(r) \notin \langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_k) \rangle_{R[\![t]\!][x]}$, unless $r = 0$,
(DD1): if no term of $q_i \cdot \mathrm{LT}_>(g_i)$ lies in $\langle \mathrm{LT}_>(g_j) \mid j < i \rangle_{R[\![t]\!][x]}$ for all $i = 1, \ldots, k$,
(DD2): if no term of r lies in $\langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_k) \rangle$,
(SID2): if $\mathrm{LT}_>(r_j \cdot e_j)$ does not lie in $\langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_k) \rangle_{R[\![t]\!][x]}$, unless $r_j = 0$, for $j = 1, \ldots, s$.

We will refer to a representation satisfying (ID1) and (ID2) as *(indeterminate) division with remainder*, and we will refer to a representation satisfying (DD1) and (DD2) as *determinate division with remainder*. In each of these two cases we call r a *remainder* or *normal form* of f with respect to $(g_1, \ldots, g_k)$. Moreover, if the remainder r is zero, we call the representation a *standard representation* of f with respect to $(g_1, \ldots, g_k)$.

With these notions, Corollary 1.24 then implies:

Corollary 1.26
Let $>$ be a monomial ordering and $g_1, \ldots, g_k \in R[\![t]\!][x]^s_>$. Then any $f \in R[\![t]\!][x]^s_>$ has a division with remainder with respect to $g_1, \ldots, g_k$ satisfying (SID2).

2. Standard bases and syzygies

In this section, we introduce standard bases for rings satisfying Convention 1.1. We also incorporate some remarks on possible optimizations for R being a principal ideal domain. Similar to the classical theory, it opens with introducing the Schreyer ordering and syzygies, and finishes with proving Buchberger's criterion.

Definition 2.1
Let $>$ be a t-local monomial ordering on $\mathrm{Mon}(t,x)^s$ and $M \leq R[\![t]\!][x]^s$ or $M \leq R[\![t]\!][x]^s_>$. A *standard basis* of M with respect to $>$ is a finite set $G \subseteq M$ with

$$\mathrm{LT}_>(G) = \mathrm{LT}_>(M)$$

where $\mathrm{LT}_>(G) := \langle \mathrm{LT}_>(g) \mid g \in G \rangle$. G is simply called a *standard basis* with respect to $>$, if G is a standard basis of $\langle G \rangle_{R[\![t]\!][x]_>}$ with respect to $>$.

With this definition we get the usual results for standard bases. We will formulate them, but we will only prove them if the proof has to be adjusted due to the fact that the base ring is not a field. For the existence of standard bases it is important to note, that our base ring is noetherian.

Proposition 2.2
For any monomial ordering $>$ all submodules of $R[\![t]\!][x]^s$ and $R[\![t]\!][x]^s_>$ have a standard basis.

Proof. Let $M \leq R[\![t]\!][x]^s$ resp. $M \leq R[\![t]\!][x]^s_>$ be a submodule. Since R is noetherian, so are $R[\![t]\!][x]^s$ and $R[\![t]\!][x]^s_>$, and $\mathrm{LT}_>(M) \leq R[\![t]\!][x]^s$ has a finite generating set $h_1, \ldots, h_k$. Because

$$\mathrm{LT}_>(M) = \langle \mathrm{LT}_>(g) \mid g \in M \rangle \stackrel{!}{=} \{\mathrm{LT}_>(g) \mid g \in M\},$$

there exist $g_1, \ldots, g_k$ with $\mathrm{LT}_>(g_i) = h_i$ forming a standard basis of M. □

Computing weak normal forms is essential in the standard bases algorithm. While it can be essentially done by computing a division with remainder and discarding everything but the remainder, as in the following algorithm, the fact that everything but the remainder is discarded may be used for some optimization in the division algorithm, which we leave out for sake of clarity.

Algorithm 2.3 (normal form)
Input: $(f, G, >)$, where $f \in R[\![t]\!][x]$, $G = (g_1, \ldots, g_k)$ a k-tuple in $R[\![t]\!][x]^s$ and $>$ a t-local monomial ordering.
Output: $r = \mathrm{NF}(f, G, >) \in R[\![t]\!][x]$, a normal form of f with respect to G and $>$.
1: Use Algorithm 1.22 to compute a division with remainder,

$$(u, (q_1, \ldots, q_k), r) = \mathrm{DwR}(f, G, >).$$

2: **return** r.

Remark 2.4 (polynomial input)
Should the input be polynomial, i.e. $f \in R[t,x]$ and $G \subseteq R[t,x]$, then by Remark 1.23 we automatically obtain a polynomial normal form $\mathrm{NF}(f, G, >) \in R[t,x]$.

Convention 2.5
For the remainder of the section, fix a t-local monomial ordering $>$ on $\mathrm{Mon}(t,x)^s$.

Proposition 2.6
Let $M \leq R[\![t]\!][x]^s$ be a module and let $G = \{g_1, \ldots, g_k\}$ be a standard basis of M. Then given an element $f \in R[\![t]\!][x]$ and a weak division with remainder

$$u \cdot f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r,$$

we have $f \in M$ if and only if $r = 0$. In particular, we see that $M = \langle G \rangle$

Proof. If $r = 0$, then obviously $f \in \langle G \rangle \subseteq J$. Conversely, if $f \in J$, then $r = u \cdot f - q_1 \cdot g_1 + \ldots + q_k \cdot g_k \in J$ and therefore $\mathrm{LT}_>(r) \in \mathrm{LT}_>(J) = \mathrm{LT}_>(G)$. Hence $r = 0$ by (ID2).
We obviously have $M \supseteq \langle G \rangle$. For the converse, note that $u \in R[\![t]\!][x]_>$ with $\mathrm{LT}_>(u) = 1$ is a unit, and hence the weak division with remainder implies $M \subseteq \langle G \rangle$. □

Proposition 2.7
Let M be a submodule of $R[\![t]\!][x]^s_>$ (resp. of $R[\![t]\!][x]^s$) and let $G = \{g_1, \ldots, g_k\} \subseteq M$. Then the following statements are equivalent:

(a) *G is a standard basis of M.*
(b) *Every (weak) normal form of any element in M with respect to G is zero.*
(c) *Every element in M has a (weak) standard representation with respect to G.*

Proof. By Proposition 2.6 (a) implies (b), and the implication (b) to (c) is true by Corollary 1.26. And if any $f \in J$ has a standard representation

$$f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k,$$

then, since $\mathrm{LM}_>(f) \geq \mathrm{LM}_>(q_i \cdot g_i)$ for $i = 1, \ldots, k$, there can be no total cancellation of the leading terms on the right hand side. Hence $\mathrm{LT}_>(f) \in \mathrm{LT}_>(G)$, and (c) implies (a). □

Also note that this in particular implies for x-homogeneous modules that being a standard basis only depends on the leading monomials.

Corollary 2.8
Let G be an x-homogeneous standard basis of an x-homogeneous module $M \leq R[\![t]\!][x]$ with respect to $>$. Let $>'$ be another t-local monomial ordering on $\mathrm{Mon}^s(t, x)$ such that $\mathrm{LM}_{>'}(g) = \mathrm{LM}_>(g)$ for all $g \in G$. Then G is also a standard basis of M with respect to $>'$.

Proof. By Algorithm 1.13, for any $f \in M = \langle G \rangle$ we can compute a determinate division with remainder 0 with respect to $>$,

$$f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + 0.$$

However, since the conditions (DD1) and (DD2) are only dependant on $\mathrm{LM}_>(g_i) = \mathrm{LM}_{>'}(g_i)$, this is also a valid determinate division with remainder under $>'$. By

Proposition 1.10, this is in particular a valid division with remainder, proving that G is also a standard basis with respect to $>'$. □

Definition 2.9 (Syzygies and Schreyer ordering)
Given a k-tuple $G = (g_1, \ldots, g_k)$ in $R[\![t]\!][x]_>^s$, we define the *Schreyer ordering* $>_S$ on $\mathrm{Mon}^k(t, x)$ associated to G and $>$ to be

$$\begin{aligned} t^\alpha \cdot x^\beta \cdot \varepsilon_i >_S t^{\alpha'} \cdot x^{\beta'} \cdot \varepsilon_j \quad :\Longleftrightarrow \\ t^\alpha \cdot x^\beta \cdot \mathrm{LM}_>(g_i) > t^{\alpha'} \cdot x^{\beta'} \cdot \mathrm{LM}_>(g_j) \text{ or} \\ t^\alpha \cdot x^\beta \cdot \mathrm{LM}_>(g_i) = t^{\alpha'} \cdot x^{\beta'} \cdot \mathrm{LM}_>(g_j) \text{ and } i > j. \end{aligned}$$

Note that we distinguish between the canonical basis elements e_j of the free module $R[\![t]\!][x]_>^s$ and the canonical basis elements ε_i of the free module $R[\![t]\!][x]_>^k$.
Moreover, observe that $>_S$ and $>$ restrict to the same monomial ordering on $\mathrm{Mon}(t, x)$, so that

$$R[\![t]\!][x]_{>_S}^k = S_{>_{S,R[\![t]\!][x]}}^{-1} R[\![t]\!][x]^k = S_{>_{R[\![t]\!][x]}}^{-1} R[\![t]\!][x]^k = R[\![t]\!][x]_>^k.$$

We may, therefore, stick with the notation $R[\![t]\!][x]_>^k$ also when replacing $>$ by the Schreyer ordering $>_S$.
Let φ denote the substitution homomorphism

$$\begin{aligned} \varphi : R[\![t]\!][x]_>^k = \bigoplus_{i=1}^k R[\![t]\!][x]_> \cdot \varepsilon_i \ &\longrightarrow \ R[\![t]\!][x]_>^s = \bigoplus_{j=1}^s R[\![t]\!][x]_> \cdot e_j, \\ \varepsilon_i \ &\longmapsto \ g_i. \end{aligned}$$

We call its kernel the *syzygy module* or simply the *syzygies* of G,

$$\mathrm{syz}(G) := \left\{ \sum_{i=1}^k q_i \cdot \varepsilon_i \in R[\![t]\!][x]_{>_S}^k \ \middle| \ \sum_{i=1}^k q_i \cdot g_i = 0 \right\}.$$

The concept of syzygies is one that can be applied to any ring, and one of the conditions on our ground ring R in Convention 1.1 states that we assume to be able to compute a finite system of generators for the syzygies of our leading coefficients,

$$\begin{aligned} &\mathrm{syz}_R(\mathrm{LC}_>(g_1), \ldots, \mathrm{LC}_>(g_k)) := \\ &\quad \{(c_1, \ldots, c_k) \in R^k \mid c_1 \cdot \mathrm{LC}_>(g_1) + \ldots + c_k \cdot \mathrm{LC}_>(g_k) = 0\}. \end{aligned}$$

In the case of a base field one constructs certain syzygies of a standard basis G with the aid of s-polynomials in order to show that G is a standard basis. In order to treat the class of base rings introduced in Convention 1.1 we have to replace this set by a more subtle set of syzygies which we will now introduce. We will then show in Remark 2.11 and Proposition 2.12 that in the case of a factorial base ring the new set of syzygies coincides with the classical one.

Definition 2.10
For a k-tuple $G=(g_1,\dots,g_k)$ in $R[\![t]\!][x]^s$ and a fixed index $1\leq l\leq k$, we will now introduce several objects which will be of importance in the upcoming theory.
Recall the notions of divisibility and least common multiple of module monomials in Definition 1.8. We denote the set of least common multiples of the leading monomials up to and including g_l with

$$C_l := \Big\{\operatorname{lcm}(\mathrm{LM}_>(g_i)\mid i\in J)\;\Big|\; J\subseteq\{1,...,k\} \text{ with } \max(J)=l\Big\}\setminus\{0\}.$$

Note that $C_l\subseteq R[\![t]\!][x]\cdot e_\lambda$ for the index $1\leq\lambda\leq s$ such that $\mathrm{LT}_>(g_l)\in R[\![t]\!][x]\cdot e_\lambda$. And for a least common multiple $a\in C_l$, we abbreviate the set of all indices j up to l such that $\mathrm{LM}_>(g_j)$ divides it with

$$J_{l,a} := \Big\{i\in\{1,\dots,l\}\;\Big|\;\mathrm{LM}_>(g_i) \text{ divides } a\Big\}.$$

Now given $J_{l,a}$, we can compute a finite generating set for the syzygies of the tuple $(\mathrm{LC}_>(g_i))_{i\in J_{l,a}}$, which we will temporarily denote with S_R. Let $\mathrm{syz}_{R,l,a}$ be the set of elements of S_R with non-trivial entry in l:

$$\begin{aligned}\langle\; S_R\;\rangle_R &= \Big\{(c_i)_{i\in J_{l,a}}\in R^{|J_{l,a}|}\;\Big|\;\textstyle\sum_{i\in J_{l,a}} c_i\cdot\mathrm{LC}_>(g_i)=0\Big\},\\ &\cup\!\mid\\ \mathrm{syz}_{R,l,a} &= \Big\{(c_i)_{i\in J_{l,a}}\in S_R\;\Big|\; c_l\neq 0\Big\}.\end{aligned}$$

With this, we can write down a finite set of syzygies of the leading terms of the g_i up to and including $\mathrm{LT}_>(g_l)$ with non-trivial entry in l,

$$\mathrm{syz}_l := \left\{\sum_{i\in J_{l,a}}\frac{c_i\cdot a}{\mathrm{LM}_>(g_i)}\cdot\varepsilon_i\in R[\![t]\!][x]^k\;\middle|\; a\in C_l \text{ and } c\in\mathrm{syz}_{R,l,a}\right\}.$$

For each $\xi'\in\mathrm{syz}_l$, we can then fix a single weak division with remainder of $\varphi(\xi')\in R[\![t]\!][x]^s$ with respect to $g_1,\dots,g_l$ to obtain

$$\mathfrak{S}_l := \left\{u\cdot\xi'-\sum_{i=1}^k q_i\cdot\varepsilon_i\;\middle|\;\begin{array}{c}\xi'\in\mathrm{syz}_l \text{ and } u\cdot\varphi(\xi')=q_1\cdot g_1+\ldots+q_l\cdot g_l+r\\ \text{the fixed weak division with remainder}\end{array}\right\}.$$

As $\mathfrak{S}_l$ obviously depends on G, we write $\mathfrak{S}_{G,l}$ instead whenever G is not clear from the context. Moreover, we abbreviate

$$\mathfrak{S}^{(G)} := \mathfrak{S}_{G,|G|}.$$

Also, there is a certain degree of ambiguity in the construction of $\mathfrak{S}_l$ since we are actively choosing generating sets and divisions with remainders. Hence whenever we use $\mathfrak{S}_l$, it will represent any possible outcome of our construction. For example, when we write $\mathfrak{S}\subseteq\mathfrak{S}_l$ for a set $\mathfrak{S}\subseteq R[\![t]\!][x]^k_{>_S}$, it means that the elements of $\mathfrak{S}$ are possible outcomes of our construction of $\mathfrak{S}_l$.

Remark 2.11 (factorial ground rings)
Should R be a factorial ring in which we have a natural notion of a least common multiple, then the construction above simplifies to extensions of classical techniques. Suppose $a \in C_l$ is a least common multiple of various leading monomials including $\mathrm{LM}_>(g_l)$. Let $J_{l,a}$ be the set of all indices i for which $\mathrm{LM}_>(g_i)$ divides a. Then the syzygy module of all leading coefficients of g_i with $i \in J_{l,a}$ is generated by syzygies of the form (see Proposition 2.12)

$$\frac{\mathrm{lcm}(\mathrm{LC}_>(g_i), \mathrm{LC}_>(g_j))}{\mathrm{LC}_>(g_i)} \cdot \varepsilon_i - \frac{\mathrm{lcm}(\mathrm{LC}_>(g_i), \mathrm{LC}_>(g_j))}{\mathrm{LC}_>(g_j)} \cdot \varepsilon_j, \text{ with } i, j \in J_{l,a}, i > j.$$

Abbreviating $\lambda_i := \mathrm{LC}_>(g_i)$, we consequently get

$$\mathrm{syz}_{R,l,a} = \left\{ \frac{\mathrm{lcm}(\lambda_l, \lambda_i)}{\lambda_l} \cdot \varepsilon_l - \frac{\mathrm{lcm}(\lambda_l, \lambda_i)}{\lambda_i} \cdot \varepsilon_i \;\middle|\; i \in J_{l,a} \right\}.$$

Hence,

$$\mathrm{syz}_l = \bigcup_{a \in C_l} \left\{ \frac{\mathrm{lcm}(\lambda_l, \lambda_i) \cdot a}{\mathrm{LT}_>(g_l)} \cdot \varepsilon_l - \frac{\mathrm{lcm}(\lambda_l, \lambda_i) \cdot a}{\mathrm{LT}_>(g_i)} \cdot \varepsilon_i \;\middle|\; i \in J_{l,a} \right\}.$$

The definition of the Schreyer ordering $>_S$ now states

$$\mathrm{LT}_{>_S} \left(\frac{\mathrm{lcm}(\lambda_l, \lambda_i) \cdot a}{\mathrm{LT}_>(g_l)} \cdot \varepsilon_l - \frac{\mathrm{lcm}(\lambda_l, \lambda_i) \cdot a}{\mathrm{LT}_>(g_i)} \cdot \varepsilon_i \right) = \frac{\mathrm{lcm}(\lambda_l, \lambda_i) \cdot a}{\mathrm{LT}_>(g_l)} \cdot \varepsilon_l.$$

Therefore, the module generated by the leading terms of syz_l is generated by the leading terms of its elements of the form

$$\frac{\mathrm{lcm}(\mathrm{LT}_>(g_l), \mathrm{LT}_>(g_i))}{\mathrm{LT}_>(g_l)} \cdot \varepsilon_l - \frac{\mathrm{lcm}(\mathrm{LT}_>(g_l), \mathrm{LT}_>(g_i))}{\mathrm{LT}_>(g_i)} \cdot \varepsilon_i \text{ with } l > i \in J_{l,a},$$

which we obtain by setting $a = \mathrm{lcm}(\mathrm{LM}_>(g_l), \mathrm{LM}_>(g_i))$. Note that for $i \notin J_{l,a}$ the expression would just be zero.
The images of these generators under φ are, in the classical case of polynomial rings, commonly known as *s-polynomials*, and the fixed divisions with remainder, which we considered for the definition of $\mathfrak{S}_l$, represent the normal form computations of these s-polynomials that are commonly done in the standard basis algorithm (and also Buchberger's Algorithm). We continue this train of thought in Remark 2.15.

Proposition 2.12
Let R be a factorial ring, and let $c_1, \ldots, c_k \in R$. Then

$$\mathrm{syz}(c_1, \ldots, c_k) = \left\langle \frac{\mathrm{lcm}(c_i, c_j)}{c_i} \cdot \varepsilon_i - \frac{\mathrm{lcm}(c_i, c_j)}{c_j} \cdot \varepsilon_j \;\middle|\; k \geq i > j \geq 1 \right\rangle.$$

Proof. We make an induction on k with $k = 1, 2$ being clear. Now let $k > 2$ and consider a syzygy $a := a_1 \cdot \varepsilon_1 + \ldots + a_k \cdot \varepsilon_k$. Then

$$a_k \cdot c_k \in \langle c_1, \ldots, c_{k-1} \rangle,$$

from which we can infer

$$\begin{aligned} a_k \in \langle c_1,\dots,c_{k-1}\rangle : \langle c_k\rangle &= \langle c_1\rangle : \langle c_k\rangle + \ldots + \langle c_{k-1}\rangle : \langle c_k\rangle \\ &= \left\langle \frac{\operatorname{lcm}(c_1,c_k)}{c_k} \right\rangle + \ldots + \left\langle \frac{\operatorname{lcm}(c_{k-1},c_k)}{c_k} \right\rangle \end{aligned}$$

Setting

$$s_{ij} := \frac{\operatorname{lcm}(c_i,c_j)}{c_i}\cdot \varepsilon_i - \frac{\operatorname{lcm}(c_i,c_j)}{c_j}\cdot \varepsilon_j \quad \text{and} \quad \mu_{ij} := \frac{\operatorname{lcm}(c_i,c_j)}{c_j},$$

we have shown that there are $b_1,\dots,b_{k-1}\in R$ such that

$$a_k = b_1\cdot \mu_{k1} + \ldots + b_{k-1}\cdot \mu_{kk-1},$$

so that, by induction,

$$\begin{aligned} a - b_1\cdot s_{k1} + \ldots + b_{k-1}\cdot s_{kk-1} &\in \operatorname{syz}(c_1,\dots,c_{k-1}) \\ &= \langle s_{ij} \mid k-1\geq i > j \geq 1\rangle. \end{aligned}$$

Hence,

$$a \in \langle s_{ij} \mid k-1 \geq i > j \geq 1\rangle + \langle s_{k1},\dots,s_{kk-1}\rangle. \qquad \square$$

We now come back to the general case that R is a noetherian ring in which linear equations are solvable. For the objects in Definition 2.10 the following holds:

Lemma 2.13
For any $a \in C_l$ and any $(c_i)_{i\in J_{l,a}} \in syz_{R,l,a}$ there exists a $\xi \in \mathfrak{S}_l$ such that

$$\operatorname{LT}_{>_S}(\xi) = \frac{c_l\cdot a}{\operatorname{LM}_>(g_l)}\cdot \varepsilon_l.$$

Proof. By construction in Definition 2.10, for any $a\in C_l$ and any $(c_i)_{i\in J_{l,a}} \in syz_{R,l,a}$, there exists a $\xi\in\mathfrak{S}_l$ of the form

$$\xi = u\cdot \xi' - \sum_{i=1}^{k} q_i\cdot \varepsilon_i = \sum\nolimits_{i\in J_{l,a}} \frac{c_i\cdot a}{\operatorname{LM}_>(g_i)}\cdot \varepsilon_i - \sum_{i=1}^{l} q_i\cdot\varepsilon_i.$$

First, recall that $J_{l,a}$ is the set of indices i up to l for which $\operatorname{LM}_>(g_i)$ divides a. Hence for all $i,j\in J_{l,a}$ we have

$$\operatorname{LM}_>\Big(\underbrace{\frac{c_i\cdot a}{\operatorname{LM}_>(g_i)}}_{\neq 0}\cdot g_i\Big) = a = \operatorname{LM}_>\Big(\underbrace{\frac{c_j\cdot a}{\operatorname{LM}_>(g_j)}}_{\neq 0}\cdot g_j\Big).$$

As an immediate consequence, we get

$$\operatorname{LT}_{>_S}\Big(\sum\nolimits_{i\in J_{l,a}} \frac{c_i\cdot a}{\operatorname{LM}_>(g_i)}\cdot\varepsilon_i\Big) = \frac{c_l\cdot a}{\operatorname{LM}_>(g_l)}\cdot\varepsilon_l, \tag{8}$$

because the Schreyer ordering prefers the highest component in case of a tie, and $l = \max J_{l,a}$, $c_l \neq 0$ by definition.

Next, recall that $(c_i)_{i\in J_{l,a}} \in \operatorname{syz}_R(\operatorname{LC}_>(g_i) \mid i \in J_{l,a})$, which means that

$$\sum_{i\in J_{l,a}} \frac{c_i \cdot a}{\operatorname{LM}_>(g_i)} \cdot \operatorname{LT}_>(g_i) = \sum_{i\in J_{l,a}} c_i \operatorname{LC}_>(g_i)\cdot a \overset{!}{=} 0.$$

Therefore, for all $j \in J_{l,a}$,

$$\operatorname{LM}_>\left(\frac{c_j\cdot a}{\operatorname{LM}_>(g_j)}\cdot g_j\right) > \operatorname{LM}_>\left(\sum_{i\in J_{l,a}} \frac{c_i\cdot a}{\operatorname{LM}_>(g_i)}\cdot g_i\right) = \operatorname{LM}_>(\varphi(\xi))$$

as all summands have the same leading monomial a and the leading terms in the sum cancel each other out.
Finally, recall that $\varphi(\xi) = q_1 \cdot g_1 + \ldots + q_l \cdot g_l + r$ was a division with remainder, whose (ID1) property implies for all $j \in J_{l,a}$ and $i = 1, \ldots, l$

$$\operatorname{LM}_>\left(\frac{c_j\cdot a}{\operatorname{LM}_>(g_j)}\cdot g_j\right) > \operatorname{LM}_>(\varphi(\xi)) \overset{\text{(ID1)}}{\geq} \operatorname{LM}_>(q_i\cdot g_i).$$

Thus we have for all $j \in J_{l,a}$ and $i = 1, \ldots, l$

$$\operatorname{LM}_{>_S}\left(\frac{c_j\cdot a}{\operatorname{LM}_>(g_j)}\cdot \varepsilon_j\right) >_S \operatorname{LM}_{>_S}(q_i\cdot \varepsilon_i). \tag{9}$$

Together, we obtain

$$\begin{aligned}\operatorname{LT}_{>_S}(\xi) &= \operatorname{LT}_{>_S}\left(u\cdot \sum_{j\in J_{l,a}} \frac{c_j\cdot a}{\operatorname{LM}_>(g_j)}\cdot\varepsilon_j - \sum_{i=1}^{l} q_i\cdot\varepsilon_i\right)\\ &\overset{(9)}{=} \operatorname{LT}_{>_S}\left(u\cdot \sum_{j\in J_{l,a}} \frac{c_j\cdot a}{\operatorname{LM}_>(g_j)}\cdot\varepsilon_j\right) \overset{(8)}{=} \frac{c_l\cdot a}{\operatorname{LM}_>(g_l)}\cdot\varepsilon_l.\end{aligned}$$ □

Theorem 2.14
Let $G = (g_1, \ldots, g_k)$ be a k-tuple of elements in $R[\![t]\!][x]^s$ and let $\mathfrak{S}_1, \ldots, \mathfrak{S}_k$ be constructed as in Definition 2.10. Suppose there exists an $\mathfrak{S} \subseteq \bigcup_{l=1}^k \mathfrak{S}_l$ such that $\operatorname{LT}_{>_S}(\mathfrak{S}) = \operatorname{LT}_{>_S}(\bigcup_{l=1}^k \mathfrak{S}_l)$ and $\varphi(\xi) = 0$ for all $\xi \in \mathfrak{S}$. Then G is a standard basis with respect to $>$ and $\mathfrak{S}$ is a standard basis of $\operatorname{syz}(G)$ *with respect to $>_S$.*

Proof. Let $q_1, \ldots, q_k \in R[\![t]\!][x]_> = R[\![t]\!][x]_{>_S}$ be chosen arbitrarily. We will proof both statements simultaneously via the standard representation criteria in Proposition 2.7 (c), by considering

$$\chi := \sum_{i=1}^k q_i\cdot\varepsilon_i \quad \text{and} \quad g := \varphi(\chi) = \sum_{i=1}^k q_i \cdot g_i.$$

Here g represents an arbitrary element of M, and, in case $g = 0$, χ represents an arbitrary element of $\operatorname{syz}(G)$.

First compute a division with remainder of χ with respect to $\mathfrak{G}$ and the Schreyer ordering,

$$\chi = \sum_{\xi\in\mathfrak{G}} a_\xi \cdot \xi + r.$$

Should r be zero, then the expression above is a standard representation of χ with respect to $>_S$. Moreover, as $\varphi(\xi) = 0$ for all $\xi \in \mathfrak{G}$ by assumption, $g = \varphi(\chi) = 0$ trivially possesses a standard representation. Hence, in case $r = 0$, both g and χ satisfy the standard representation criteria. So suppose $r \neq 0$ for the remainder of the proof.

By Corollary 1.26, we may assume that our division with remainder satisfies (SID2), i.e. say

$$r = r_1 \cdot \varepsilon_1 + \ldots + r_k \cdot \varepsilon_k \text{ with } \mathrm{LT}_>(r_i \cdot \varepsilon_i) \notin \mathrm{LT}_{>_S}(\mathfrak{G}) \text{ for all } i = 1, \ldots, k. \tag{10}$$

Since by assumption $\varphi(\xi) = 0$ for all $\xi \in \mathfrak{G}$, we have

$$g = \varphi(\chi) = \varphi(r) = r_1 \cdot g_1 + \ldots + r_k \cdot g_k. \tag{11}$$

To proof the statement for $G \subseteq M$, it suffices to show that the expression above is a standard representation of g. To proof the statement for $\mathfrak{G} \subseteq \mathrm{syz}(G)$, we will show that $r \neq 0$ contradicts $g = 0$. This leaves $r = 0$ as the only viable case, assuming $g = 0$, for which we have already established that χ satisfies the standard representation criteria.

Now assume that $\mathrm{LM}_>(g) < \mathrm{LM}_>(r_i \cdot g_i)$ for some $i = 1, \ldots, k$, and hence for $J := \{i \in \{1, \ldots, k\} \mid \mathrm{LM}_>(r_i \cdot g_i) \text{ maximal}\}$

$$\sum_{i\in J} \mathrm{LT}_>(r_i \cdot g_i) = 0.$$

Set $l := \max(J)$ and $a := \mathrm{lcm}(\mathrm{LM}_>(g_i) \mid i \in J)$, so that obviously $J \subseteq J_{l,a}$. We will now concentrate on $r_l \cdot \varepsilon_l$.

For the leading coefficient of $r_l \cdot \varepsilon_l$, note that the leading coefficients sum up to zero, i.e. $\sum_{i\in J} \mathrm{LC}_>(r_i) \cdot \varepsilon_i \in \mathrm{syz}(\mathrm{LC}_>(g_i) \mid i \in J_{l,a})$. Recall that $\mathrm{syz}_{R,l,a}$ are the elements of a generating system of $\mathrm{syz}(\mathrm{LC}_>(g_i) \mid i \in J_{l,a})$ with non-trivial entry in l. Hence there are suitable $d_{(c_i)} \in R$ such that

$$\mathrm{LC}_>(r_l) \cdot \varepsilon_l = \sum_{(c_i)\in \mathrm{syz}_{l,a}} d_{(c_i)} \cdot c_l \cdot \varepsilon_l. \tag{12}$$

For the leading monomial of $r_l \cdot \varepsilon_l$, note that $\mathrm{LM}_>(r_l \cdot g_l)$ is divisible by $\mathrm{LM}_>(g_i)$ for all $i \in J$. Hence it is divisible by $a = \mathrm{lcm}(\mathrm{LM}_>(g_i) \mid i \in J)$, i.e. there exists a $t^\delta x^\gamma$ such that $\mathrm{LM}_>(r_l \cdot g_l) = t^\delta x^\gamma \cdot a$, or equivalently

$$\mathrm{LM}_>(r_l) = t^\delta x^\gamma \cdot \frac{a}{\mathrm{LM}_>(g_l)}. \tag{13}$$

Now, by the previous Lemma 2.13 there exists a $\xi_{(c_i)} \in \mathfrak{S}_l$ for any $(c_i) \in \mathrm{syz}_{R,l,a}$ such that

$$\mathrm{LT}_{>_S}(\xi_{(c_i)}) = \frac{c_l \cdot a}{\mathrm{LM}_>(g_l)} \cdot \varepsilon_l. \tag{14}$$

Piecing everything together, we thus get

$$\begin{aligned} \mathrm{LT}_>(r_l) \cdot \varepsilon_l &\overset{(12)+(13)}{=} t^\delta x^\gamma \sum_{(c_i) \in \mathrm{syz}_{l,a}} d_{(c_i)} \cdot \frac{c_l \cdot a}{\mathrm{LM}_>(g_l)} \cdot \varepsilon_l \\ &\overset{(14)}{=} t^\delta x^\gamma \sum_{(c_i) \in \mathrm{syz}_{l,a}} d_{(c_i)} \cdot \mathrm{LT}_{>_S}(\xi_{(c_i)}) \in \mathrm{LT}_{>_S}(\mathfrak{S}_l). \end{aligned}$$

And since $\mathrm{LT}_{>_S}(\mathfrak{S}_l) \subseteq \mathrm{LT}_{>_S}(\mathfrak{S})$ by our first assumption, this contradicts the (SID2) condition in Equation (10). Therefore, Equation (11) has to be a standard representation, implying that G is a standard basis of M with respect to $>$.

Moreover, since $r \neq 0$, Equation (11) being standard representation yields an obvious contradiction if $g = 0$. Hence in the case $g = 0$, we have $r = 0$ and we have already seen how this implies that $\mathfrak{S}$ is a standard basis of $\mathrm{syz}(G)$ with respect to $>_S$. □

Remark 2.15 (factorial rings continued)
Suppose again that R is a factorial ring. We have seen in Remark 2.11, that the leading module of $\bigcup_{l=1}^k \mathfrak{S}_{G,l}$ is generated by the leading terms of elements of the form

$$\frac{\mathrm{lcm}(\mathrm{LT}_>(g_i), \mathrm{LT}_>(g_j))}{\mathrm{LT}_>(g_i)} \cdot \varepsilon_i - \frac{\mathrm{lcm}(\mathrm{LT}_>(g_i), \mathrm{LT}_>(g_j))}{\mathrm{LT}_>(g_j)} \cdot \varepsilon_j,\ i > j.$$

They are, thus, the only elements we need to keep track of for Theorem 2.14. These elements are obviously characterized by pairs of distinct elements (g_i, g_j) that is, by elements in a so-called *pair-set*, which commonly appear in the classical standard basis algorithm and in Buchberger's Algorithm.

Algorithm 2.16 (standard basis algorithm)

Input: $(G, >)$, where $G = (g_1, \ldots, g_k)$ be a k-tuple of elements in $R[\![t]\!][x]^s$ generating $M \leq R[\![t]\!][x]^s$ and $>$ a t-local monomial ordering on $\mathrm{Mon}^s(t, x)$.

Output: $G' \subseteq M$ a standard basis of M with respect to $>$.

1: Pick $\mathfrak{S} \subseteq \bigcup_{l=1}^k \mathfrak{S}_{G,l} \subseteq R[\![t]\!][x]^k$ such that

$$\mathrm{LT}_{>_S}(\mathfrak{S}) = \mathrm{LT}_{>_S}\Big(\bigcup_{l=1}^k \mathfrak{S}_{G,l}\Big),$$

where $>_S$ is the Schreyer ordering on $\mathrm{Mon}^k(t, x)$ associated to G and $>$.

2: **while** $\mathfrak{S} \neq \emptyset$ **do**

3: Set $k := |G|$, so that $G := \{g_1, \ldots, g_k\}$ and $\mathfrak{S} \subseteq R[\![t]\!][x]^k_>$.

4: Choose $q = \sum_{i=1}^k q_i \cdot \varepsilon_i \in \mathfrak{S}$.

5: Set $\mathfrak{S} := \mathfrak{S} \setminus \{q\}$.

6: Compute a weak normal form r of $q_1 \cdot g_1 + \ldots + q_k \cdot g_k$ with respect to G

$$r := \mathrm{NF}_>(q_1 \cdot g_1 + \ldots + q_k \cdot g_k, G, >).$$

7: **if** $r \neq 0$ **then**
8: Set $g_{k+1} := r$.
9: Set $G := G \cup \{g_{k+1}\}$.
10: Pick $\mathfrak{S}' \subseteq \mathfrak{S}^{(G)} \subseteq R[\![t]\!][x]^{k+1}$ such that

$$\mathrm{LT}_{>_S}(\mathfrak{S}') = \mathrm{LT}_{>_S}\left(\mathfrak{S}^{(G)}\right),$$

where $>_S$ is the Schreyer ordering on $\mathrm{Mon}^{k+1}(t,x)$ induced by the newly extended G and $>$.
11: Set $\mathfrak{S} := (\mathfrak{S} \times \{0\}) \cup \mathfrak{S}'$.
12: **return** G.

Proof. Label all objects in the ν-th iteration of the while loop with a subscript ν. That is, to be more precise,

- G_ν as it exists in Step 4,
- k_ν as it exists in Step 4,
- q_ν as chosen in Step 5
- r_ν as computed in Step 7,
- $\mathfrak{S}_\nu$ as $\mathfrak{S}$ exists in Step 4,
- $\mathfrak{S}'_{\nu+1}$ as $\mathfrak{S}'$ exists in Step 9 if $r_{\nu-1} \neq 0$, $\mathfrak{S}'_{\nu+1} = \emptyset$ otherwise, $\mathfrak{S}'_1 := \mathfrak{S}_1$,

so that

$$G_{\nu+1} = G_\nu \cup \{r_\nu\} \text{ and } \mathfrak{S}_{\nu+1} = (\mathfrak{S}_\nu \times \{0\}) \cup \mathfrak{S}'_{\nu+1}.$$

Termination. Note that we have a nested sequence of modules

$$\mathrm{LT}_>(G_1) \subseteq \mathrm{LT}_>(G_2) \subseteq \mathrm{LT}_>(G_3) \subseteq \ldots \subseteq \mathrm{LT}_>(G_\nu) \subseteq \mathrm{LT}_>(G_{\nu+1}) \subseteq \ldots,$$

which has to stabilize at some point. Because $r_\nu \neq 0$ implies $\mathrm{LT}_>(G_\nu) \subsetneq \mathrm{LT}_>(G_{\nu+1})$, it means that our sets $\mathfrak{S}_\nu$ have to be strictly decreasing in every step beyond the point of stabilization. And since all $\mathfrak{S}_\nu$ are finite, our algorithm terminates eventually.

Correctness. Let N be the total number of iterations, and let G be the return value, $k := |G|$. We will prove that G is a standard basis by constructing a set $\mathfrak{S} \subseteq R[\![t]\!][x]^k$ that satisfies the two conditions in Theorem 2.14. For that, consider all $\mathfrak{S}_\nu \subseteq R[\![t]\!][x]^{k_\nu}_>$ canonically embedded in $R[\![t]\!][x]^k_>$ due to $G_\nu \subseteq G$ and $k_\nu \leq k$. Let $\mathfrak{S}$ be the union of all $\mathfrak{S}'_\nu$,

$$\mathfrak{S} := \bigcup_{\nu=1}^{N+1} \mathfrak{S}'_\nu \subseteq R[\![t]\!][x]^k.$$

Note that $\mathfrak{S}'_\nu \subseteq \mathfrak{S}_{G,k_\nu}$, because the construction of $\mathfrak{S}_{G,k_\nu}$ only depends on the first k_ν elements of G, which are exactly the elements of G_ν. Moreover, Step 9 implies that $\mathrm{LT}_{>_S}(\mathfrak{S}_\nu) = \mathrm{LT}_{>_S}(\mathfrak{S}_{G,k_\nu})$, which shows that $\mathfrak{S}$ satisfies the first condition of our theorem,

$$\mathrm{LT}_{>_S}(\mathfrak{S}) = \mathrm{LT}_{>_S}\left(\bigcup_{l=1}^{k} \mathfrak{S}_{G,l}\right).$$

Now for each $\xi \in \mathfrak{S}$ there exists an iteration $1 \leq \nu \leq N$ in which it is chosen in Step 5, $\xi = \sum_{i=1}^{k_\nu} q_{i,\nu} \cdot \varepsilon_i$.
If $\varphi(\xi) = r_\nu = 0$, then ξ satisfies the second condition of our theorem. However if $\varphi(\xi) = r_\nu \neq 0$, then $g_{\nu+1} = r_\nu$ and ξ can be replaced with $\xi - \varepsilon_{\nu+1}$ so that $\varphi(\xi - \varepsilon_{\nu+1}) = 0$. Note that this does not change the leading term, since by construction the maximal leading terms of $q_1 \cdot g_1, \ldots, q_{l_\nu} \cdot g_{l_\nu}$ cancel each other out, which implies that $q_{i,\nu} \cdot \varepsilon_i >_S \varepsilon_{\nu+1}$ for any $1 \leq i \leq \nu$ with $q_{i,\nu} \neq 0$. Hence we obtain a set $\mathfrak{S}$ completely satisfying the second condition of our theorem. □

Remark 2.17 (polynomial input)
Should our input be polynomial, $g_1, \ldots, g_k \in R[t,x]^s$, then all normal form computations terminate and yield polynomial outputs as noted in 2.4. In particular, our standard basis algorithm will terminate and the output will be polynomial as well. Moreover, if our input is x-homogeneous, then so is the resulting standard basis.

Should R be a factorial ring, Algorithm 2.16 can be simplified to:

Algorithm 2.18 (standard basis algorithm for factorial rings)
Input: $(G, >)$, where $G = (g_1, \ldots, g_k)$ be a k-tuple of elements in $R[\![t]\!][x]^s$ generating $M \leq R[\![t]\!][x]^s$ with R factorial and $>$ a t-local monomial ordering on $\mathrm{Mon}^s(t,x)$.
Output: $G' \subseteq M$ a standard basis of M with respect to $>$.
1: Suppose $G := \{g_1, \ldots, g_k\}$.
2: Initialize a pair-set, $P := \{(g_i, g_j) \mid i < j\}$.
3: **while** $P \neq \emptyset$ **do**
4: Pick $(g_i, g_j) \in P$.
5: Set $P := P \setminus \{(g_i, g_j)\}$.
6: Compute a weak normal form

$$r := \mathrm{NF}_>(\mathrm{spoly}(g_i, g_j), G, >),$$

where

$$\begin{aligned} &\mathrm{spoly}(g_i, g_j) \\ &\quad = \frac{\mathrm{lcm}(\mathrm{LT}_>(g_i), \mathrm{LT}_>(g_j))}{\mathrm{LT}_>(g_i)} \cdot g_i - \frac{\mathrm{lcm}(\mathrm{LT}_>(g_i), \mathrm{LT}_>(g_j))}{\mathrm{LT}_>(g_j)} \cdot g_j \end{aligned}$$

and

$$\begin{aligned}&\operatorname{lcm}(\mathrm{LT}_>(g_i), \mathrm{LT}_>(g_j))\\ &\quad = \operatorname{lcm}(\mathrm{LC}_>(g_i), \mathrm{LC}_>(g_j)) \cdot \operatorname{lcm}(\mathrm{LM}_>(g_i), \mathrm{LM}_>(g_j)).\end{aligned}$$

if $r \neq 0$ **then**
 Extend the pair-set, $P := P \cup \{(g, r) \mid g \in G\}$.
 Set $G := G \cup \{r\}$.
return $G' := G$.

3. Standard basis algorithm for an application in tropical geometry

Remark 3.1 (simplification for ideals in tropical geometry)
The most important application of standard bases over rings that we have in mind is motivated by tropical geometry over the field of p-adic numbers $\mathbb{Q}_p$. Given a homogeneous ideal in $\mathbb{Q}_p[x]$ we have to decide if the initial ideal with respect to some weight vector $w \in \mathbb{R}^n$ is monomial free or not, where for the initial forms the valuation of the coefficients is taken into account. For this the ideal can be restricted to $\mathbb{Z}_p[x]$ and via the surjection

$$\pi : \mathbb{Z}[\![t]\!][x] \longrightarrow \mathbb{Z}_p[x] : t \mapsto p$$

we may pull the ideal back to the mixed power series ring $\mathbb{Z}[\![t]\!][x]$. It is not hard to see ([MaR15b]) that the initial ideal of $I = \langle f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Q}_p[x]$ with respect to w with $f_i \in \mathbb{Z}[x]$ is monomial free if and only if the initial ideal with respect to $(-1, w)$ of

$$J = \langle p - t, f_1, \ldots, f_k \rangle \trianglelefteq \mathbb{Z}[\![t]\!][x]$$

is monomial free. But this can be read of a certain standard basis of J. We are, thus, particularly interested in computing standard bases of x-homogeneous ideals in $\mathbb{Z}[\![t]\!][x]$ generated by polynomials and containing $p - t$ for some prime number p. In that situation our reduction algorithm can be simplified a lot. For any polynomial f occuring in the reduction process either the leading coefficient c is divisible by p and can thus be reduced by p, or it is coprime to p, in which case the Euclidean Algorithm provides integers $a, b \in \mathbb{Z}$ such that

$$1 = a \cdot c + b \cdot p,$$

and hence replacing f by $a \cdot f + b \cdot (p - t)$ we can pass to a polynomial with leading coefficient 1. If we preprocess all polynomials, except $p - t$, added to our standard basis in the standard basis algorithm that way, checking if a leading term can be reduced burns down to a simple divisibility check as in the case of standard bases over fields.

We will now describe the algorithms for the special case described in Remark 3.1 in detail, starting with the algorithm reducing a polynomial with respect to $p - t$.

Algorithm 3.2 (pRed — $(p-t)$-reduce)

Input: $(g,>)$, where $>$ a t-local monomial ordering and $g \in \mathbb{Z}[t,x]$.

Output: (a,q,r) with $a \in \{1,\dots,p-1\}$ and $q,r \in \mathbb{Z}[t,x]$, such that $a \cdot g = q \cdot (p-t) + r$, $\mathrm{LM}_>(g) \geq \mathrm{LM}_>(q)$ and either $r = 0$ or $\mathrm{LC}_>(r) = 1$.

1: Set $q := 0$
2: Set $r := g$.
3: **while** $p \mid \mathrm{LC}_>(r)$ **do**
4: Let $l := \max\{m \in \mathbb{N} \mid p^m \text{ divides } \mathrm{LC}_>(r)\} > 0$.
5: Set $r := r - \frac{\mathrm{LT}_>(r)}{p^l} \cdot (p^l - t^l)$.
6: Set $q := q + \frac{\mathrm{LT}_>(r)}{p^l} \cdot \frac{(p^l-t^l)}{p-t}$.
7: **if** $r \neq 0$ **then**
8: Compute with the Euclidean Algorithm $a \in \{1,\dots,p-1\}$ and $b \in \mathbb{Z}$ such that $1 = a \cdot \mathrm{LC}_>(r) + b \cdot p$.
9: Set $r := a \cdot r + b \cdot (p-t) \cdot \mathrm{LM}_>(r)$.
10: Set $q := a \cdot q - b \cdot \mathrm{LM}_>(r)$.
11: **return** (a,q,r)

Proof. Termination: We need to show that eventually p does not divide the leading coefficient of r anymore. Let us for a moment consider the polynomial

$$r = \sum_{i=1}^{k} r_i \cdot x^{\alpha_i}$$

as a polynomial in x with coefficients r_i in $\mathbb{Z}[t]$. Then the set of monomials in x occuring in r does not increase throughout the algorithm. Moreover, if the leading monomial of r is contained in $r_i \cdot x^{\alpha_i}$ with

$$r_i = c_{i_1} \cdot t^{i_1} + \ldots + c_{i_j} \cdot t^{i_j}, i_1 < \ldots < i_j,$$

then in Step 5 we substitute the term $c_{i_1} \cdot t^{i_1} x^{\alpha_i}$ by the term $c_{i_1}/p^l \cdot t^{i_1+l} x^{\alpha_i}$, increasing the minimal t-degree in r_i strictly.

Let $\nu_p(c) := \max\{m \in \mathbb{N} \mid p^m \text{ divides } c\}$ denote the p-adic valuation on $\mathbb{Z}$, so that $l = \nu_p(c_{i_1})$, and consider the valued degree of r_i defined by

$$m_i := \max\{\nu_p(c_{i_1}) + \deg(t^{i_1}), \dots, \nu_p(c_{i_j}) + \deg(t^{i_j})\}.$$

This is a natural upper bound on the t-degree of our substituted r_i, and hence

$$\max\{m_1, \dots, m_k\}$$

is an upper bound for the t-degree of all terms in our new r.

If the monomial of the substitute, $t^{i_1+l} x^{\alpha_i}$, does not occur in the original r, then this upper bound remains the same for out new r. If it does occur in the original r, then this valued degree might increase depending on the sum of the coefficients, however the number of terms in r strictly decreases.

Because r has only finitely many terms to begin with, this upper bound may therefore only increase a finite number of times. And since the minimal t-degree is strictly increasing, if p divides the leading coefficient of r, our algorithm terminates eventually.

Correctness: Once the while loop is done, we have found polynomials q and r such that $g = q\cdot(p-t)+r$ and $\mathrm{LM}_>(g) \geq \mathrm{LM}_>(q)$. Moreover, we may assume that $r \neq 0$. Since p does not divide the leading coefficient of r, these numbers are coprime and the Euclidean Algorithm computes integers $a, b \in \mathbb{Z}$ such that

$$1 = a \cdot \mathrm{LC}_>(r) + b \cdot p,$$

and we may assume $a \in \{1, \dots, p-1\}$. This leads to the equation

$$a \cdot g = (a \cdot q - b \cdot \mathrm{LM}_>(r)) \cdot (p-t) + (a \cdot r + b \cdot (p-t) \cdot \mathrm{LM}_>(r)),$$

and we are done by replacing q with $a\cdot q - b\cdot \mathrm{LM}_>(r)$ and r with $a\cdot r + b\cdot(p-t)\cdot\mathrm{LM}_>(r)$. It is clear by construction that then $\mathrm{LM}_>(g) \geq \mathrm{LM}_>(q)$ and $\mathrm{LC}_>(r) = 1$. □

Remark 3.3

Given $p-t$ and a polynomial g as in Algorithm 3.2, we are interested in the ideal generated by these in the ring $\mathbb{Z}[\![t]\!][x]$. If r is the output of Algorithm 3.2, then we have indeed

$$\langle p-t, g\rangle = \langle p-t, r\rangle \trianglelefteq \mathbb{Z}[\![t]\!][x].$$

To see this consider the equation

$$a \cdot g = s \cdot (p-t) + r$$

which implies the inclusion $\supseteq$. For the other inclusion it suffices to note that the integer $a \in \{1, \dots, p-1\}$ is a unit in the ring of p-adic numbers $\mathbb{Z}[\![t]\!]/\langle p-t\rangle \cong \mathbb{Z}_p$. Moreover, note that the polynomials q and r will be x-homogeneous, if the input g was x-homogeneous.

Next we adjust the homogeneous determinate division with remainder to the situation that all but the first element in G have leading coefficient one. This will be formulated for any base ring as in Convention 1.1.

Algorithm 3.4 (SHDDwR — special version)

Input: $(f, G, >)$, where $f \in R[\![t]\!][x]^s$ x-homogeneous, $G = (g_1, \dots, g_k)$ a k-tuple of x-homogeneous elements in $R[\![t]\!][x]^s$ with with $\mathrm{LC}_>(g_i) = 1$ for $i = 2, \dots, k$ and $>$ a t-local monomial ordering on $\mathrm{Mon}^s(t, x)$.

Output: (Q, r), where $Q = (q_1, \dots, q_k) \in R[\![t]\!][x]^k$ and $r \in R[\![t]\!][x]^s$ such that

$$f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r$$

satisfies

(DD1): no term of $q_i \cdot \mathrm{LT}_>(g_i)$ lies in $\langle \mathrm{LT}_>(g_j) \mid j < i\rangle$ for all i,

(DD2): no term of r lies in $\langle \mathrm{LT}_>(g_1), \dots, \mathrm{LT}_>(g_k)\rangle$, (DDH): the $q_1,\ldots,q_k,r$ are either 0 or x-homogeneous of x-degree $\deg_x(f)-\deg_x(g_1),\ldots,\deg_x(f)-\deg_x(g_k),\deg_x(f)$ respectively.

1: Set $q_i := 0$ for $i=1,\ldots,k$, $r:=0$, $\nu:=0$, $f_\nu := f$.
2: **while** $f_\nu \neq 0$ **do**
3:   **if** $\exists\, i\ :\ \mathrm{LT}_>(g_i)\ \mid\ \mathrm{LT}_>(f_\nu)$ **then**
4:     Choose $i\in\{1,\ldots,k\}$ minimal with $\mathrm{LT}_>(g_i)\ \mid\ \mathrm{LT}_>(f_\nu)$.
5:     **for** j=1,...,k **do**
6:       Set

$$q_{j,\nu} := \begin{cases} \frac{\mathrm{LM}_>(f_\nu)}{\mathrm{LM}_>(g_i)} & \text{, if } j=i,\\ 0 & \text{, otherwise,}\end{cases}$$

7:     Set $r_\nu := 0$.
8:   **else**
9:     Set $q_{i,\nu} := 0$, for $i=1,\ldots,k$, and $r_\nu := \mathrm{LT}_>(f_\nu)$.
10:   Set $q_i := q_i + q_{i,\nu}$ for $i=1,\ldots,k$ and $r := r + r_\nu$.
11:   Set $f_{\nu+1} := f_\nu - (q_{1,\nu}\cdot g_1 + \ldots + q_{k,\nu}\cdot g_k + r_\nu)$ and $\nu := \nu+1$.
12: **return** $((q_1,\ldots,q_k),r)$

Proof. We just have to note that the condition

$$\mathrm{LT}_>(f_\nu)\in\langle \mathrm{LT}_>(g_1),\ldots,\mathrm{LT}_>(g_k)\rangle$$

is equivalent to the condition

$$\exists\, i\ :\ \mathrm{LT}_>(g_i)\ \mid\ \mathrm{LT}_>(f_\nu).$$

For this observe, that as soon as some $\mathrm{LT}_>(g_i)$ for $i=2,\ldots,k$ occurs in a linear combination representing $\mathrm{LT}_>(f_\nu)$ then necessarily $\mathrm{LT}_>(g_i)$ divides $\mathrm{LT}_>(f_\nu)$.
Hence, the algorithm coincides with Algorithm 1.13, only the test in Step 3 has been simplified. □

In the specialized algorithm for weak division with remainder we restrict to the base ring $\mathbb{Z}$. Moreover, we assume that the input is polynomial, so that we are able to homogenize also with respect to the variable t. We, therefore, change our convention for this one algorithm and set $x=(t,x_1,\ldots,x_n)$.

Algorithm 3.5 (SDwR - special version of DwR)

Input: $(f,G,>)$, where $f\in\mathbb{Z}[x]=\mathbb{Z}[t,x_1,\ldots,x_n]$ and $G=(g_1,\ldots,g_k)$ is a k-tuple in $\mathbb{Z}[x]$ with $g_1=p-t$ and $\mathrm{LC}_>(g_i)=1$ for $i=2,\ldots,k$ and $>$ a t-local monomial ordering on $\mathrm{Mon}(x)=\mathrm{Mon}(t,x_1,\ldots,x_n)$.

Output: (u,Q,r), where $u\in\mathbb{Z}[x]$ with $p\nmid \mathrm{LC}_>(u)=\mathrm{LT}_>(u)$, $Q=(q_1,\ldots,q_k)\subseteq\mathbb{Z}[x]^k$ and $r\in\mathbb{Z}[x]$ such that

$$u\cdot f = q_1\cdot g_1+\ldots+q_k\cdot g_k + r$$

satisfies (ID1) and (ID2):

(ID1): $\mathrm{LM}_>(f)\geq \mathrm{LM}_>(q_i\cdot g_i)$ for $i=1,\ldots,k$ and

(ID2): $\mathrm{LT}_>(r) \notin \langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_k) \rangle$, unless $r = 0$.

Moreover, the algorithm requires only a finite number of recursions.

1: Compute

$$(a, q, f) := \mathrm{pRed}(f, >).$$

2: **if** $f \neq 0$ and $\exists\, i \,:\, \mathrm{LT}_>(g_i) \mid \mathrm{LT}_>(f)$ **then**
3: Set $D := \{g_i \in G \mid \mathrm{LT}_>(g_i) \text{ divides } \mathrm{LT}_>(f)\}$.
4: Pick $g_j \in D$ with minimal ecart.
5: **if** $e := \mathrm{ecart}_>(g_j) - \mathrm{ecart}_>(f) > 0$ **then**
6: Compute

$$((Q'_1, \ldots, Q'_k), R') := \mathrm{SHDDwR}(x_0^e \cdot f^h, (\mathrm{LT}_>(g_1^h), \ldots, \mathrm{LT}_>(g_k^h)), >_h).$$

7: Set $f' := (x_0^e \cdot f^h - \sum_{i=1}^k Q'_i \cdot g_i^h)^d$.
8: Compute

$$(u'', (q''_1, \ldots, q''_{k+1}), r) := \mathrm{SDwR}(f', (g_1, \ldots, g_k, f), >).$$

9: Set $q_i := q''_i + u'' \cdot Q_i'^d$, $i = 1, \ldots, k$.
10: Set $u := u'' - q''_{k+1}$.
11: **else**
12: Compute

$$((Q'_1, \ldots, Q'_k), R') := \mathrm{SHDDwR}(f^h, (g_1^h, \ldots, g_k^h), >_h).$$

13: Compute

$$(u, (q''_1, \ldots, q''_k), r) := \mathrm{SDwR}((R')^d, (g_1, \ldots, g_k), >).$$

14: Set $q_i := q''_i + u \cdot Q_i'^d$, $i = 1, \ldots, k$.
15: **else**
16: Set $(u, (q_1, \ldots, q_k), r) := (1, (0, \ldots, 0), f)$.
17: **return** $(a \cdot u, (q_1 + q, q_2, \ldots, q_k), r)$.

Proof. Note first, that after Step 1 the new polynomial f has leading coefficient 1, its leading monomial is less than or equal to that of the original f and the same holds for the leading monomial $\mathrm{LM}_>(q) = \mathrm{LM}_>(q \cdot g_1)$.
We then should keep in mind that, as in Algorithm 3.4, the condition

$$\mathrm{LT}_>(f) \in \langle \mathrm{LT}_>(g_1), \ldots, \mathrm{LT}_>(g_k) \rangle$$

is equivalent to

$$\exists\, i \,:\, \mathrm{LT}_>(g_i) \mid \mathrm{LT}_>(f).$$

Finiteness of recursions: For sake of clarity, label all the objects appearing in the ν-th recursion step by a subscript ν. For example the ecart $e_\nu \in \mathbb{N}$, the element $f_\nu \in \mathbb{Z}[x]$ and the subset $G_\nu \subseteq \mathbb{Z}[x]$.

Since $G_1^h \subseteq G_2^h \subseteq G_3^h \subseteq \ldots$, we have an ascending chain of leading ideals in $\mathbb{Z}[x_h]$, which eventually stabilizes unless the algorithm terminates beforehand

$$\mathrm{LT}_{>_h}(G_1^h) \subseteq \mathrm{LT}_{>_h}(G_2^h) \subseteq \ldots \subseteq \mathrm{LT}_{>_h}(G_N^h) = \mathrm{LT}_{>_h}(G_{N+1}^h) = \ldots.$$

Assume $e_N > 0$. Then we'd have $f_N \in G_{N+1}$, and thus

$$\mathrm{LM}_{>_h}(f_N^h) = \mathrm{LT}_{>_h}(f_N^h) \in \mathrm{LT}_{>_h}(G_{N+1}^h) = \mathrm{LT}_{>_h}(G_N^h).$$

To put it differently, we'd have a $g^h \in G_N^h$ such that

$$\mathrm{LT}_{>_h}(g^h) \mid \mathrm{LT}_{>_h}(f_N^h),$$

which by Remark 1.21 (5) would imply that

$$\mathrm{LT}_>(g) \mid \mathrm{LT}_>(f_N) \text{ and } \mathrm{ecart}_>(g) \leq \mathrm{ecart}_>(f_N).$$

This contradicts our assumption

$$e_N = \min\{\mathrm{ecart}_>(g) \mid g \in D_N\} - \mathrm{ecart}_>(f_N) \overset{!}{>} 0. \quad ↯$$

Therefore we have $e_N \leq 0$. By induction we conclude that $e_\nu \leq 0$ for all $\nu \geq N$, i.e. that we will exclusively run through steps 13-15 of the "else" case from the N-th recursion step onwards.
By the properties of HDDwR we know that in particular

$$\mathrm{LT}_{>_h}(R'_N) \notin \mathrm{LT}_>(G_N^h). \tag{15}$$

Now assume that the recursions would not stop with the next recursion. That means there exists a $g \in D_{N+1} \subseteq G_N = G_{N+1}$ such that

$$\mathrm{LT}_>(g) \mid \mathrm{LT}_>(f_{N+1}) = \mathrm{LT}_>((R'_N)^d),$$

and because of $e_{N+1} \leq 0$ also

$$\mathrm{ecart}(g) \leq \mathrm{ecart}(f_{N+1}) = \mathrm{ecart}((R'_N)^d).$$

It then follows from Remark 1.21 (6) that

$$\mathrm{LT}_{>_h}(g^h) \mid \mathrm{LT}_{>_h}(R'_N),$$

in contradiction to (15). Hence the algorithm terminates after the $N+1$-th recursion step.
Correctness: In what follows we will denote by f the original polynomial and by $\tilde{f}$ the polynomial f after Step 1. Moreover, we recall that

$$a \cdot f = q \cdot g_1 + \tilde{f} \tag{16}$$

with $\mathrm{LM}_>(f) \geq \mathrm{LM}_>(q) = \mathrm{LM}_>(q \cdot g_1)$.
We make an induction on the number of recursions, say $N \in \mathbb{N}$. If $N = 1$ then either $\tilde{f} = 0$ or $\mathrm{LT}_>(\tilde{f})$ is not divisible by any $\mathrm{LT}_>(g_i)$, and in both cases

$$1 \cdot \tilde{f} = 0 \cdot g_1 + \ldots + 0 \cdot g_k + \tilde{f}$$

satisfies (ID1) and (ID2), and thus by (16) so does

$$a \cdot f = q \cdot g_1 + 0 \cdot g_2 + \ldots 0 \cdot g_k + \tilde{f}.$$

So suppose $N > 1$ and consider the first recursion step. If $e \leq 0$, then by the properties of HDDwR the representation

$$\tilde{f}^h = Q'_1 \cdot g_1^h + \ldots + Q'_k \cdot g_k^h + R'$$

satisfies (DD1), (DD2) and (DDH). (DD1) and (DD2) imply (ID1), which means that for each $i = 1, \ldots, k$ we have

$$x_0^{\mathrm{ecart}_>(\tilde{f})} \cdot \mathrm{LM}_>(\tilde{f}) = \mathrm{LM}_{>_h}(\tilde{f}^h) \overset{\text{(ID1)}}{\geq_h} \mathrm{LM}_{>_h}(Q'_i) \cdot \mathrm{LM}_{>_h}(g_i^h) = \ldots$$
$$\ldots = x_0^{a_i + \mathrm{ecart}_>(g_i)} \cdot \mathrm{LM}_>(Q_i'^d) \cdot \mathrm{LM}_>(g_i)$$

for some $a_i \geq 0$. Since $\tilde{f}^h$ and $Q'_i \cdot g_i^h$ are both x_h-homogeneous of the same x_h-degree by (DDH), the definition of the homogenized ordering $>_h$ implies

$$\mathrm{LM}_>(\tilde{f}) \geq \mathrm{LM}_>(Q_i'^d) \cdot \mathrm{LM}_>(g_i) \text{ for all } i = 1, \ldots, k. \tag{17}$$

Moreover, by induction the representation $u \cdot R'^d = q''_1 \cdot g_1 + \ldots + q''_k \cdot g_k + r$ satisfies (ID1), (ID2) and $p \nmid \mathrm{LC}_>(u) = \mathrm{LT}_>(u)$, the first implying that

$$\mathrm{LM}_>(\tilde{f}) \overset{(17)}{\geq} \mathrm{LM}_> \underbrace{\left(\tilde{f} - \sum_{i=1}^{k} Q_i'^d \cdot g_i \right)}_{=R'^d} \overset{\text{(ID1)}}{\geq} \mathrm{LM}_>(q''_i \cdot g_i). \tag{18}$$

Therefore, the representation

$$u \cdot \tilde{f} = \sum_{i=1}^{k} (q''_i + u \cdot Q_i'^d) \cdot g_i + r$$

satisfies (ID1) by (17), (18), $p \nmid \mathrm{LC}_>(u) = \mathrm{LT}_>(u)$ and (ID2) by induction, and hence by (16) so does the representation

$$a \cdot u \cdot f = (q''_1 + u \cdot Q_i'^d + q) \cdot g_1 + \sum_{i=2}^{k} (q''_i + u \cdot Q_i'^d) \cdot g_i + r.$$

Similarly, if $e > 0$, then by the properties of HDDwR the representation

$$x_0^e \cdot \tilde{f}^h = Q'_1 \cdot \mathrm{LT}_{>_h}(g_1^h) + \ldots + Q'_k \cdot \mathrm{LT}_{>_h}(g_k^h) + R'$$

satisfies (DD1), (DD2) and (DDH). (DD1) and (DD2) imply (ID1), which means that for each $i = 1, \ldots, k$ we have

$$x_0^{e + \mathrm{ecart}_>(\tilde{f})} \cdot \mathrm{LM}_>(\tilde{f}) = \mathrm{LM}_{>_h}(x_0^e \cdot \tilde{f}^h) \geq \ldots$$
$$\ldots \geq \mathrm{LM}_{>_h}(Q'_i) \cdot \mathrm{LM}_{>_h}(\mathrm{LT}_{>_h}(g_i^h)) = x_0^{a_i + \mathrm{ecart}_>(g_i)} \cdot \mathrm{LM}_>(Q_i'^d) \cdot \mathrm{LM}_>(g_i),$$

for some $a_i \geq 0$. Since $x_0^e \cdot \tilde{f}^h$ and $Q_i' \cdot \mathrm{LT}_{>_h}(g_i^h)$ are both x_h-homogeneous of the same x_h-degree by (DDH), the definition of the homogenized ordering $>_h$ implies

$$\mathrm{LM}_>(\tilde{f}) \geq \mathrm{LM}_>(Q_i'^d) \cdot \mathrm{LM}_>(g_i). \tag{19}$$

Moreover, by induction the representation $u'' \cdot \tilde{f}' = \sum_{i=1}^k q_i'' \cdot g_i + q_{k+1}'' \cdot \tilde{f} + r$ satisfies (ID1), (ID2), $p \nmid \mathrm{LC}_>(u'') = \mathrm{LT}_>(u'')$ with the first implying that

$$\mathrm{LM}_>(\tilde{f}) \overset{(19)}{\geq} \underbrace{\mathrm{LM}_>\left(\tilde{f} - \sum_{i=1}^k Q_i'^d \cdot g_i\right)}_{=\mathrm{LM}_>(R'^d)} \overset{(\mathrm{ID1})}{\geq} \mathrm{LM}_>(q_i'' \cdot g_i). \tag{20}$$

Therefore, the representation

$$u \cdot \tilde{f} = \sum_{i=1}^k (q_i'' + u'' \cdot Q_i'^d) \cdot g_i + r, \text{ with } u = u'' - q_{k+1}''$$

satisfies (ID1) by (19), (20), $\mathrm{LM}_>(u'') = 1$ and (ID2) by induction.
To see that $\mathrm{LT}_>(u) = \mathrm{LT}_>(u'')$ and hence $p \nmid \mathrm{LC}_>(u) = \mathrm{LT}_>(u)$, observe that

$$\mathrm{LT}_{>_h}(x_0^e \cdot \tilde{f}^h) \in \langle \mathrm{LT}_>(g_1^h), \ldots, \mathrm{LT}_>(g_k^h) \rangle,$$

which is why

$$\mathrm{LM}_>(\tilde{f}) = \mathrm{LM}_{>_h}(x_0^e \cdot \tilde{f}^h)^d > \mathrm{LM}_{>_h}\left(x_0^e \cdot \tilde{f}^h - \sum_{i=1}^k Q_i' \cdot g_i^h\right)^d = \mathrm{LM}_>(\tilde{f}').$$

Thus $\mathrm{LM}_>(\tilde{f}) > \mathrm{LM}_>(\tilde{f}') \geq \mathrm{LM}_>(q_{k+1}'') \cdot \mathrm{LM}_>(\tilde{f})$, which necessarily implies $\mathrm{LM}(q_{k+1}'') < 1$ and thus $\mathrm{LT}_>(u) = \mathrm{LT}_>(u'')$. □

Remark 3.6
The representation

$$u \cdot f = q_1 \cdot g_1 + \ldots + q_k \cdot g_k + r \tag{21}$$

that we compute in Algorithm 3.5 is actually not a standard representation in the sense that we defined, even though it satisfies (ID1) and (ID2). The reason is, that we replaced the condition

$$\mathrm{LT}_>(u) = 1$$

by the weaker condition

$$p \nmid \mathrm{LC}_>(u) \text{ and } \mathrm{LM}_>(u) = 1.$$

However, if p does not divide the integer $\mathrm{LC}_>(u)$ then this number is invertible in the ring of p-adic numbers

$$\mathbb{Z}[\![t]\!]/\langle p - t \rangle \cong \mathbb{Z}_p,$$

which implies that there are power series $g, h \in \mathbb{Z}[\![t]\!]$ such that

$$g \cdot \mathrm{LC}_>(u) = 1 + h \cdot (p - t).$$

Replacing in the above representation u by $g \cdot u$, r by $g \cdot r$, q_1 by $g \cdot q_1 - h$ and q_i by $g \cdot q_i$ for $i = 2, \ldots, k$ we get a standard representation with coefficients in $\mathbb{Z}[\![t]\!][x]$. The representation is thus good enough for our purposes.

We, actually, could even easily turn (21) into a polynomial standard representation as follows. If $a, b \in \mathbb{Z}$ with

$$a \cdot \mathrm{LC}_>(u) + b \cdot p = 1$$

and if

$$b = \sum_{j=0}^{l} c_j \cdot p^j$$

is the p-adic expansion of b, then

$$a \cdot \mathrm{LC}_>(u) = 1 - \sum_{j=1}^{l+1} c_{j-1} \cdot p^j = 1 - \sum_{j=1}^{l+1} c_{j-1} \cdot t^j + h \cdot (p - t)$$

for some polynomial $h \in \mathbb{Z}[t]$. With

$$v = 1 - \sum_{j=1}^{l+1} c_{j-1} \cdot t^j + \mathrm{tail}(u)$$

and multiplying (21) by a we thus get

$$(v + h \cdot (p - t)) \cdot f = \sum_{i=1}^{k} a \cdot q_i + a \cdot r$$

or equivalently

$$v \cdot f = (a \cdot q_1 - h \cdot f) \cdot g_1 + \sum_{i=2}^{k} a \cdot q_i \cdot g_i + a \cdot r,$$

which is a standard representation with $\mathrm{LC}_>(v) = 1$ and $v, q_1, \ldots, q_k, r \in \mathbb{Z}[t, x]$. If needed, one can actually turn (21) into a standard representation

It remains to formulate the standard basis algorithm in this special case.

Algorithm 3.7 (standard basis algorithm — special case)

Input: $(G, >)$, where $G = (g_1, \ldots, g_k)$ be a k-tuple of elements in $\mathbb{Z}[\![t]\!][x]$ with $g_1 = p - t$ and $>$ a t-local monomial ordering on $\mathrm{Mon}(t, x)$.

Output: $G' = (g'_1, \ldots, g'_l)$ a standard basis of $\langle G \rangle \trianglelefteq \mathbb{Z}[\![t]\!][x]$ with respect to $>$ such that $g'_1 = p - t$ and $\mathrm{LC}_>(g'_i) = 1$ for $i = 2, \ldots, l$.

1: **for** $i = 2, \ldots, k$ **do**
2: Compute $(a, q, r) := \mathrm{pRed}(g_i, >)$.
3: Set $g_i := r$.
4: Initialize a pair-set, $P := \{(g_i, g_j) \mid i < j\}$.
5: **while** $P \neq \emptyset$ **do**
6: Pick $(g_i, g_j) \in P$.

Set $P := P \setminus \{(g_i, g_j)\}$.
Compute

$$(u, (q_1, \ldots, q_k), r) := \mathrm{SDwR}_>(\mathrm{spoly}(g_i, g_j), G, >),$$

where

$$\begin{aligned}&\mathrm{spoly}(g_i, g_j)\\ &\quad= \frac{\mathrm{lcm}(\mathrm{LT}_>(g_i), \mathrm{LT}_>(g_j))}{\mathrm{LT}_>(g_i)} \cdot g_i - \frac{\mathrm{lcm}(\mathrm{LT}_>(g_i), \mathrm{LT}_>(g_j))}{\mathrm{LT}_>(g_j)} \cdot g_j\end{aligned}$$

and

$$\begin{aligned}&\mathrm{lcm}(\mathrm{LT}_>(g_i), \mathrm{LT}_>(g_j))\\ &\quad= \mathrm{lcm}(\mathrm{LC}_>(g_i), \mathrm{LC}_>(g_j)) \cdot \mathrm{lcm}(\mathrm{LM}_>(g_i), \mathrm{LM}_>(g_j)).\end{aligned}$$

if $r \neq 0$ **then**
  Compute $(a, q, r) := \mathrm{pRed}(r, >)$.
  Extend the pair-set, $P := P \cup \{(g, r) \mid g \in G\}$.
  Set $G := G \cup \{r\}$.
return $G' := G$.

Remark 3.8
We should like to remark that the standard basis elements $g_2', \ldots, g_l'$ will be x-homogeneous if the input $g_2, \ldots, g_k$ was so.

4. Reduced standard bases

In this rather short section we recall the notion of a reduced standard basis and show what problems we run into when allowing base rings that are not fields and local orderings. Reduced standard bases play a very important role in the computation of Gröbner fans and tropical varieties. Since they turn not to be computationally feasible in our setting, we will replace them by a weaker notion that is good enough for the computation of Gröbner fans and tropical varieties.

Definition 4.1
Let $G, H \subseteq R[\![t]\!][x]^s$ be two finite subsets. Given a t-local monomial ordering $>$ on $\mathrm{Mon}^s(t, x)$, we call G *reduced* with respect to H, if, for all $g \in G$, no term of $\mathrm{tail}_>(g)$ lies in $\mathrm{LT}_>(H)$.
And we simply call G *reduced*, if it is reduced with respect to itself and minimal in the sense that no proper subset $G' \subsetneq G$ is sufficient to generate its leading module, i.e. $\mathrm{LT}_>(G') \subsetneq \mathrm{LT}_>(G)$.
Observe that we forego any kind of normalization of the leading coefficients that is normally done in polynomial rings over ground fields.

If our module is generated by x-homogeneous elements, it is not hard to show that reduced standard bases exist. Given an x-homogeneous standard basis, one can pursue a strategy similar to the classical reduction algorithm based on repeated tail reduction. Lemma 1.16 guarantees its convergence in the $\langle t\rangle$-adic topology.

Algorithm 4.2 (reduction algorithm)

Input: $(G,>)$, where $G=\{g_1,\ldots,g_k\}$ is a minimal x-homogeneous standard basis of $M\leq R[\![t]\!][x]^s$ with respect to the weighted ordering $>=>_w$ with $w\in\mathbb{R}^m_{<0}\times\mathbb{R}^{n+s}$.

Output: $G'=\{g_1',\ldots,g_k'\}$ an x-homogeneous reduced standard basis of M with respect to $>$ such that $\mathrm{LM}_>(g_i')=\mathrm{LM}_>(g_i)$.

for $i=1,\ldots,k$ **do**
  Set $g_i':=g_i$.
  Create a working list

$$L:=\{p\in R[\![t]\!][x]^s\mid p\text{ term of }g_i',\ \mathrm{LM}_>(g_i')>p\},$$

  while $L\neq\emptyset$ **do**
    Pick $p\in L$ with $\mathrm{LM}_>(p)$ maximal.
    Set $L:=L\setminus\{p\}$.
    if $p\in\mathrm{LT}_>(M)$ **then**
      Compute homogeneous division with remainder

$$((q_1,\ldots,q_k),r)=\mathrm{HDDwR}(p,(g_1,\ldots,g_k),>).$$

      Set $g_i':=g_i'-(q_1\cdot g_1+\ldots+q_k\cdot g_k)$.
      Update the working list

$$L:=\{p'\in R[\![t]\!][x]^s\mid p'\text{ term of }g_i,\ \mathrm{LM}_>(p)>\mathrm{LM}_>(p')\}.$$

return $\{g_1',\ldots,g_k'\}$

Proof. Pick an $i=1,\ldots,k$. Labelling all objects occurring in the ν-the recurring step by a subscript ν, we have a strictly decreasing sequence

$$\mathrm{LM}_>(p_1)>\mathrm{LM}_>(p_2)>\mathrm{LM}_>(p_3)>\ldots.$$

And since $\mathrm{LM}_>(p_\nu)\geq\mathrm{LM}_>(q_{j,\nu}\cdot g_j)$ for all $j=1,\ldots,k$, the sequence $(q_{j,\nu}\cdot g_j)_{\nu\in\mathbb{N}}$ must also converge in the $\langle t\rangle$-adic topology together with $(p_\nu)_{\nu\in\mathbb{N}}$. In particular, the element $g_i'=g_i-\sum_{\nu=0}^\infty\sum_{j=1}^k q_{j,\nu}\cdot g_j$ in our output exists.

Also, while setting $g_{i,\nu+1}'=g_{i,\nu}'-(q_{1,\nu}\cdot g_1+\ldots+q_{k,\nu}\cdot g_k)$ apart from the term p_ν cancelling, the terms changed are all strictly smaller than p. Hence for any term p of g_i', $p\neq\mathrm{LT}_>(g_i)$, there is a recursion step in which it is picked. Because p is not cancelled during the step, we have $p\notin\mathrm{LT}_>(M)$. Therefore no term of g_i' apart from its leading term lies in $\mathrm{LT}_>(M)$. □

One nice property of reduced standard bases, that is repeatedly used in the established theory of Gröbner fans of polynomial ideals over a ground field, is their uniqueness up to multiplication by units. In fact, this property does not change even if we add power series into the mix.

Lemma 4.3
Let R be a field and let $M \leq R[\![t]\!][x]^s$ or $M \leq R[\![t]\!][x]^s_>$ be a module generated by x-homogeneous elements. Then M has a unique monic, reduced standard basis.

Proof. Because R is a field, we have $\mathrm{LT}_>(M) = \mathrm{LM}_>(M)$ and since $\mathrm{LM}_>(M)$ has a unique minimal generating system consisting of monomials, let's call it A, so does $\mathrm{LT}_>(M)$.
Let $G = \{g_1, \dots, g_k\}$ be a monic, reduced standard bases of M. Observe that the leading terms of G form a standard basis of the leading module of M. That means each $a \in A \subseteq \mathrm{LT}_>(M)$ can be expressed with a standard representation of the leading terms of G,

$$a = q_1 \cdot \mathrm{LT}_>(g_1) + \ldots + q_k \cdot \mathrm{LT}_>(g_k).$$

Since there is no cancellation of higher terms in the standard representation, there must exist an $i = 1 \dots, k$ with $a = \mathrm{LM}_>(q_i \cdot g_i)$. This implies $\mathrm{LM}_>(g_i) = a$ because a wouldn't be a minimal generator of $\mathrm{LM}_>(M)$ otherwise. And because G is monic, $\mathrm{LT}_>(g_i) = a$.
Therefore, given a reduced standard basis G, we see that for any minimal generator $a \in A$ there exists an element $g \in G$ with $\mathrm{LM}_>(g) = a$. And since reduced standard bases are minimal themselves, it means that there is exactly one element $g \in G$ per minimal generator $a \in A$.
Now let G and H be two different reduced standard basis of M. Let $a \in A$ and let $g \in G$, $h \in H$ be the basis element with leading monomial a. If $g - h \neq 0$, then $g - h \in M$ must have a non-zero leading monomial which lies in $\mathrm{LM}_>(M)$. However, that monomial also has to occur in either g and h, and since R is a field the term with that monomial has to lie in $\mathrm{LT}_>(M) = \mathrm{LM}_>(M)$, contradicting that G and H were reduced. ☐

However, it can easily be seen that this does not hold over rings.

Example 4.4
Consider the ring $\mathbb{Z}[x, y]$ and the degree lexicographical ordering $>$, i.e.

$$\begin{aligned} x^{a_1}y^{a_2} > x^{b_1}y^{b_2} \quad &:\Longleftrightarrow \\ &a_1 + a_2 > b_1 + b_2 \text{ or} \\ &a_1 + a_2 = b_1 + b_2 \text{ and } (a_1, a_2) > (b_1, b_2) \text{ lexicographically in } \mathbb{R}^2. \end{aligned}$$

Consider the following ideal and its leading ideal:

$$I := \langle 2x^2y + 1, 3xy^2 + 1 \rangle \text{ and } \mathrm{LT}_>(I) = \langle 2x, 9y^3, xy^2 \rangle.$$

Two possible standard bases, both reduced, are

$$\begin{array}{rcccccl} G_1 = \{ & \underline{2x} - 3y, & \underline{9y^3} + 2, & \underline{xy^2} + 3y^3 + 1 & \}, \\ & \parallel & \parallel & \nparallel & \\ G_2 = \{ & \underline{2x} - 3y, & \underline{9y^3} + 2, & \underline{xy^2} - 6y^3 - 1 & \}. \end{array}$$

Hence, unlike their classical counterparts over ground fields, reduced standard bases over ground rings are not unique up to multiplication with units. The key problem is that leading modules are not necessarily saturated with respect to the ground ring. This allowed the third basis element to have terms with monomials in $\mathrm{LM}_>(M)$, to which we could add a constant multiple of the second basis element without changing it being reduced.

Note also, that even if the base ring is a field and the ideal is generated by a polynomial, the reduced standard basis might contain power series. This is a well known fact when dealing with local orderings.

Example 4.5
Consider the principal ideal generated by the element $g = x + y + tx \in \mathbb{Q}[\![t]\!][x, y]$ and the monomial ordering $>_w$ with weight vector $w = (-1, 1, 1)$ and $>$ the lexicographical ordering with $x > y > 1 > t$ as tiebreaker. Then $\{g\}$ is a standard basis and one can show that it converges to $g' = x + \sum_{i=0}^{\infty}(-1)^i \cdot t^i y$ in its reduction process.

$$\begin{array}{r} x + y + \underline{tx} \\ \Big\downarrow {\scriptstyle -t \cdot g} \\ x + y - ty - \underline{t^2 x} \\ \Big\downarrow {\scriptstyle +t^2 \cdot g} \\ x + y - ty + t^2 y + \underline{t^3 x} \\ \Big\downarrow \\ \vdots \end{array}$$

FIGURE 3. reduction of $tx + t^2 x + y$

Since the reduced standard basis is unique, this implies that I has no reduced standard basis consisting of polynomials, even though I is generated by a polynomial itself. Consequently, this means that the reduced standard bases which play a central role in the established Gröbner fan theory are useless in our case from a practical perspective.

In [MaR15a] we will weaken the notion of reducedness, and we will show that this weakened version can be computed and is strong enough to compute Gröbner fans (see [MaR15a]) and tropical varieties (see [MaR15b]).

References

[ACH05] Maria-Emilia Alonso, Francisco Castro, and Herwig Hauser, *Effective algebraic power series*, Preprint, 2005.

[AMR77] Maria-Emilia Alonso, Teo Mora, and Mario Raimondo, *A computational model for algebraic power series*, J. Pure Appl. Alg. **77** (1977), 1–38.

[Bec90] Thomas Becker, *Stability and Buchberger criterion for standard bases in power series rings*, J. Pure Appl. Algebra **66** (1990), 219–227.

[DeS07] Wolfram Decker and Frank-Olaf Schreyer, *Varieties, Gröbner bases and algebraic curves*, Saarbrücken, 2007.

[GaH05] Sebastian Gann and Herwig Hauser, *Perfect bases for differential equations*, J. Symbolic Computation **40** (2005), 979–997.

[GGM+94] Hubert Grassmann, Gert-Martin Greuel, Bernd Martin, Wolfgang Neumann, Gerhard Pfister, Wilfred Pohl, Hans Sch"onemann, and Thomas Siebert, *Standard bases, syzygies and their implementation in* SINGULAR, Beitr"age zur angewandten Analysis und Informatik, Shaker, Aachen, 1994, pp. 69–96.

[GrP96] Gert-Martin Greuel and Gerhard Pfister, *Advances and improvements in the theory of standard bases and syzygies*, Arch. Math. **66** (1996), 163–176.

[GrP02] Gert-Martin Greuel and Gerhard Pfister, *A* SINGULAR *introduction to commutative algebra*, Springer, 2002.

[Grä94] Hans-Gert Gräbe, *The tangent cone algorithm and homogenization*, J. Pure Appl. Algebra **97** (1994), no. 3, 303–312.

[Hir77] Heisuke Hironaka, *Idealistic exponents of singularity*, J. J. Sylvester Sympos.,Johns Hopkins Univ., Baltimore, Md., 1976, Johns Hopkins Univ. Press, 1977, pp. 52–125.

[HKY10] Amina Hadj Kacem and Ihsen Yengui, *Dynamical Gröbner bases over Dedekind rings*, J. Algebra **324** (2010), no. 1, 12–24.

[Mar08] Thomas Markwig, *Standard bases in* $K[[t_1,\ldots,t_m]][x_1,\ldots,x_n]^s$, J. Symbolic Comput. **43** (2008), no. 11, 765–786.

[Mar10] Thomas Markwig, *A field of generalised puiseux series for tropical geometry*, Rend. Semin. Mat. Torino **68** (2010), 79–92.

[MaR15a] Thomas Markwig and Yue Ren, *Gröbner fans of* $\underline{x}$*-homogeneous ideals in* $r[[t]][\underline{x}]$, Preprint, 2015.

[MaR15b] Thomas Markwig and Yue Ren, *Tropical varieties of* $\underline{x}$*-homogeneous ideals in* $r[[t]][\underline{x}]$ *and over the p-adic numbers*, Preprint, 2015.

[Mor82] Teo Mora, *An algorithm to compute the equations of tangent cones*, Proceedings EUROCAM 82, Lecture Notes in Comp. Sci., 1982.

[Mor91] Teo Mora, *La queste del Saint* $\mathrm{Gr}_a(AL)$*: a computational approach to local algebra*, Discrete Appl. Math. **33** (1991), no. 1-3, 161–190, Applied algebra, algebraic algorithms, and error-correcting codes (Toulouse, 1989).

[Wie11] Oliver Wienand, *Algorithms for symbolic computation and their applications*, Ph.D. thesis, Technische Universität Kaiserslautern, Germany, 2011.

Technische Universität Kaiserslautern, Fachbereich Mathematik, Erwin–Schrödinger–Strasse, D — 67663 Kaiserslautern
E-mail address: keilen@mathematik.uni-kl.de
URL: http://www.mathematik.uni-kl.de/~keilen