PART SEVEN

Beyond

And when he had opened the seventh seal, there was silence in heaven about the space of half an hour.

And I saw the seven angels which stood before God; and to them were given seven trumpets.

Revelation

The things depending from Moon: sweat, silver, pearl, *selenotrope*, cat, goose, frog.

E. C. Agrippa, *De occulta phylosophia*

It was time of vengeance, time of slauthering all sinners, time of the wrath of God and time of punishment

Jan z Př′brami, *Life of Taborite Priests*

46

Zacharias

In her 1978 Bachelor's thesis, Zacharias discussed how to extend Buchberger's theory and algorithm from the case of a polynomial ring over a field (as presented in the second volume) to that of polynomials over a Noetherian ring. In the introduction she wrote[1]:

> Since the structure of $R[X_1, \ldots, X_n]$ is totally determined by R, any problem in $R[X_1, \ldots, X_n]$ is in effect solved by translating it to some equivalent problem in R. In the recursive approach we take the problem and translate it into $R[X_1, \ldots, X_{n-1}]$, then $R[X_1, \ldots, X_{n-2}]$, and so on, until we get to R and finally start solving it. It is apparent that there are many opportunities for unnecessary work in this project. There is also an advantage in going straight from $R[X_1, \ldots, X_n]$ to R from a theoretical point view. For such a direct approach might make it easier to discern the relationship between the coefficient ring R and the structure it imposes on $R[X_1, \ldots, X_n]$.

Her approach is based on the remark that, if $R[X_1, \ldots, X_n]$ satisfies an ideal-theoretical property, the same property must also be satisfied by R and thus effectiveness of a such property necessarily must be assumed in R and thus can be used as a seed for a procedure that effects such a property in $R[X_1, \ldots, X_n]$. In particular, the aim of Buchberger's theory being membership testing and syzygies computations, such properties can be assumed in R as a tool for defining and computing Gröbner bases.

In her approach she continued the approach of Szekeres, who in 1952 studied the structure of ideal bases for univariate polynomials and the extension performed in 1974 by Richman, which

> generalized the construction to coefficient rings in which ideal membership and syzygies are solvable. He then used this construction to show that ideal membership and syzygies are solvable in the polynomial ring as well. Then by induction he extended his results to multivariate polynomial rings.

Her main contribution is removing the useless inductive approach, thus making her tools available in the more general setting of monoid rings.

Moreover, she applied her approach to properly characterize canonical forms over monoid rings, assuming that a notion of canonical form is already available in the coefficient ring R.

[1] Zacharias, G., *Generalized Gröbner bases in commutative polynomial rings*, Bachelor's thesis, M.I.T. (1978), pp. 6–7.

In the meantime, within the frame of rewriting-rule theory, Kandri-Rody and Kapur extended Buchberger theory from polynomials over fields to polynomials over $\mathbb{Z}$ and over Euclidean rings.

The next important contribution was that of Luquan Pan, who extended Buchberger theory and algorithm to polynomial rings over principal ideal domains and pointed out that each step of Buchberger reduction, which, over fields and over Euclidean domains applies a single element, in general can involve more than a single element. This led to the introduction of the notions of strong and weak Gröbner bases.

Pan's theory was then improved by Möller who, after refining the properties of Zacharias rings, applied his lifting theorem presentation of Buchberger's algorithm thus extending it to polynomial rings over principal ideal rings.

An older interesting approach to univariate polynomial rings that can be inductively extended to multivariate polynomials, and for which a Buchberger theory has been proposed, is the theory developed by Ore in the 1930s.

After constructing quotient fields of non-commutative rings, provided they satisfy a necessary condition of *regularity*, he studied how to define on the polynomial ring $R[X]$ over a field R a twisted multiplication that preserves the property of the degree of a product to be equal to the sum of the degree of the factors, and remarked that such multiplication can be characterized by assigning an endomorphism $\alpha : R \to R$ and an α-derivation $\delta : R \to R$, and defining

$$X \cdot r = \alpha(r)X + \delta(r) \text{ for each } r \in R.$$

He further discussed how to define and compute in such a setting greatest common right divisors and least common left multiple and, with that aim, he adapted and reformulated the Euclidean algorithm; his direct application of the Euclidean algorithm allowed him to compute both greatest common right divisors and *a* common left multiple but also required an involved argument in order to obtain the *least* common left multiple

Later P. M. Cohn provided a finer reformulation of the Euclidean algorithm that directly also provides the least common left multiple and characterized Bezout domains.

I begin with an introductory section on the Buchberger–Zacharias theory (Section 46.1) in the general setting of a monoid ring; after introducing the general setting, defining weak and strong Gröbner bases (Section 46.1.1) and normal forms (Section 46.1.3) and outlining Szekeres theory (Section 46.1.2), I cover Buchberger reduction (Section 46.1.4) and the notion of canonical forms and their computation, both over a field (Section 46.1.5) and over a Zacharias ring (Section 46.1.6), concluding with a reconsideration of the notion of strong reduction by requiring, in the mood of Zacharias, that a similar property is already satisfied by the coefficient rings R and label as *strong rings* those satisfying such a property (Section 46.1.7).

Next, after reporting the results of Kandri-Rody and Kapur (Section 46.2), Pan (Section 46.3) and the finer properties of Zacharias rings discussed by Möller and Logar (Section 46.4), I report the extension performed by Möller of his lifting theorem to polynomial rings over a Zacharias ring (Section 46.5) and, in particular, over principal ideal rings (Section 46.6), and discuss the application of

Gebauer–Möller criteria in this setting (Section 46.7) and Möller's completion procedure for extending a week Gröbner basis to a strong one (Section 46.8).

I conclude the argument by showing how Lazard's Structure Theorem, originally stated for $\mathbb{K}[X, Y]$ actually holds *verbatim* for univariate polynomial rings over a domain and present the extension to PIRs performed by Norton and Sălăgean (Section 46.9).

After discussing Ore's construction of quotient fields of a non-commutative ring and his related notion of *order of irregularity* (Section 46.10), I cover his theory (Section 46.11) discussing Ore extensions (Section 46.11.1), his Euclidean algorithm (Section 46.11.2), both his formulation of the least common left multiple and Cohn's reformulation of the Euclidean algorithm (Section 46.11.3), and I show how to adapt it when the coefficients are not in a field but in a domain satisfying Ore's regularity condition (Section 46.11.4); finally I report the results by Cohn on Bezout Domains (Section 46.11.5) and by Tamari on the order of irregularity.

Next (Section 46.13), I consider the rings that are obtained by properly adapting Ore's multiplication to *multivariate* polynomials[2]; I show how the Buchberger–Zacharias theory (Section 46.13.1), Möller lifting approach (Section 46.13.3), Szekeres theory (Section 46.13.4), Buchberger reduction (Section 46.13.5), Gröbner basis computation (Section 46.13.6), and Gebauer–Möller criteria (Section 46.13.7) can be adapted to them, stressing the rôle of Ore extensions with zero derivation as associated graded rings (Section 46.13.2)

Finally, I report recent results that properly describe the ideal, which, for a polynomial ring over $\mathbb{Z}_m$, vanishes in all points of the (finite) affine space (Section 46.14).

46.1 Buchberger–Zacharias Theory

Given an (associative but not necessarily commutative) ring R with identity and an (associative but not necessarily commutative nor cancellative) monoid S, we can consider the set $R[[\mathsf{S}]]$ whose elements are the infinite linear combinations $f := \sum_{t\in\mathsf{S}} c(f,t)t$ of terms $t \in \mathsf{S}$ with coefficients in R, and impose on it a ring structure by defining addition componentwise and multiplication via distributive laws, i.e. for each $f, g \in R[[\mathsf{S}]]$ and each $t \in \mathsf{S}$ we set[3]

$$c(f+g,t) = c(f,t) + c(g,t), \quad c(fg,t) = \sum_{\substack{u,v\in\mathsf{S}\\ uv=t}} c(f,u)c(g,v);$$

for each $f \in R[[\mathsf{S}]]$, its *support* is the set $\mathrm{supp}(f) := \{t : c(f,t) \neq 0\}$.

[2] I label here such rings as the *multivariate Ore extension*. They were introduced by F. Chyzak and B. Salvy under the name *Ore algebra* and further studied by M. Pesch as *iterative Ore extension with commuting variables*.

[3] In simpler terms, we implicitly assume that

$$tr = rt \text{ for each } r \in R \setminus \{0\}, t \in \mathsf{S}. \tag{46.1}$$

This assumption will be relaxed later; the *definitions* introduced in this chapter applies *verbatim* also in the generalized settings of the next chapters; the same, up to trivial adaptations, holds for the *procedures*. *Statements* and *proofs*, requiring of course a more careful adaptation, also apply within this chapter; the required modifications are sometimes reformulated, but at other times are left to the reader.

Let us denote by $\mathsf{R} := R[\mathsf{S}]$ the *monoid ring over* R *and* S

$$\mathsf{R} := R[\mathsf{S}] := \mathrm{Span}_R(\mathsf{S}) = \left\{ f \in R[[\mathsf{S}]] : \mathrm{supp}(f) \text{ is finite} \right\};$$

R being an associative but non-commutative ring, the notion of ideal must be further specified:

Definition 46.1.1. *An* R*-module* $\mathsf{I} \subset \mathsf{R}$ *is called*

a left ideal *if it is an* R*-left module, i.e. for each* $f \in \mathsf{I}$ *and each* $l \in \mathsf{R}$, $lf \in \mathsf{I}$,
a right ideal *if it is an* R*-right module, i.e. for each* $f \in \mathsf{I}$ *and each* $r \in \mathsf{R}$, $fr \in \mathsf{I}$,
a bilateral ideal *if it is a bilateral* R*-module, i.e. for each* $f \in \mathsf{I}$ *and each* $l, r \in \mathsf{R}$, $lfr \in \mathsf{I}$.

For each $m \in \mathbb{N}$, the free R-module R^m – the canonical basis of which will be denoted by $\{\mathbf{e}_1, \ldots, \mathbf{e}_m\}$ – is an (R, R)-bimodule with its basis the set of the *terms*

$$\mathsf{S}^{(m)} := \{t\mathbf{e}_i : t \in \mathsf{S}, 1 \leq i \leq m\}.$$

Definition 46.1.2. *For any set* $F \subset \mathsf{R}^m$,

the left R*-module*[4] *generated by* F *is the set of all the finite sums*

$$\mathbb{I}_L(F) := \left\{ \sum_{i=1}^{u} l_i g_i : l_i \in \mathsf{R}, g_i \in F \right\};$$

the right R*-module generated by* F *is the set of all the finite sums*

$$\mathbb{I}_R(F) := \left\{ \sum_{i=1}^{u} g_i r_i : r_i \in \mathsf{R}, g_i \in F \right\};$$

the bilateral R*-module generated by* F *is the set of all the finite sums*

$$\mathbb{I}_2(F) := \left\{ \sum_{i=1}^{u} l_i g_i r_i : l_i, r_i \in \mathsf{R}, g_i \in F \right\}.$$

□

Lemma 46.1.3. *For any set* $F \subset \mathsf{R}^m$ *a generating set (not necessarily an* R*-basis) of*

- $\mathbb{I}_L(F)$ *as a left* R*-module is* $\mathcal{B}_L := \mathcal{B}_L(F) := \{\lambda g : \lambda \in \mathsf{S}, g \in F\}$,
- $\mathbb{I}_R(F)$ *as a right* R*-module is* $\mathcal{B}_R := \mathcal{B}_R(F) := \{g\rho : \rho \in \mathsf{S}, g \in F\}$,
- $\mathbb{I}_2(F)$ *as an* (R, R)*-bimodule is* $\mathcal{B}_2 := \mathcal{B}_2(F) := \{\lambda g \rho : \lambda, \rho \in \mathsf{S}, g \in F\}$. □

Definition 46.1.4. *A set* $S \subset \mathsf{S}^{(m)}$ *is called*

a left semigroup module *if for each* $\lambda \in \mathsf{S}, \tau \in \mathsf{S}^{(m)}$, $\tau \in S \implies \lambda\tau \in S$;
a right semigroup module *if for each* $\rho \in \mathsf{S}, \tau \in \mathsf{S}^{(m)}$, $\tau \in S \implies \tau\rho \in S$;
a bilateral semigroup module *if for each* $\lambda, \rho \in \mathsf{S}, \tau \in \mathsf{S}^{(m)}$, $\tau \in S \implies \lambda\tau\rho \in S$;
a left order module *if for each* $\lambda \in \mathsf{S}, \tau \in \mathsf{S}^{(m)}$, $\lambda\tau \in S \implies \tau \in S$;

[4] While the notation also applies to *modules* and is thus given for them, we are thinking of *ideals* and mainly applying it to them; this justifies the choice of the notation.

a right order module *if for each* $\rho \in \mathsf{S}, \tau \in \mathsf{S}^{(m)}$, $\tau\rho \in S \implies \tau \in S$;
a bilateral order module *if for each* $\lambda, \rho \in \mathsf{S}, \tau \in \mathsf{S}^{(m)}$, $\lambda\tau\rho \in S \implies \tau \in S$.

We will speak of left/right/bilateral semigroup/order ideals *when* $m = 1$. ▯

If we impose on $\mathsf{S}^{(m)}$ a total ordering $<$, then each $f \in \mathsf{R}^m$ has a unique representation as an ordered linear combination of terms $t \in \mathsf{S}^{(m)}$ with coefficients in R:

$$f = \sum_{i=1}^{s} c(f, t_i)t_i : c(f, t_i) \in R \setminus \{0\}, t_i \in \mathsf{S}^{(m)}, t_1 > \cdots > t_s.$$

With respect to $<$ we denote $\mathbf{T}(f) := t_1$ the *maximal term* of f, $\mathrm{lc}(f) := c(f, t_1)$ its *leading coefficient* and $\mathbf{M}(f) := c(f, t_1)t_1$ its *maximal monomial*.

Remark 46.1.5 *(Reinert).* If we denote

$$\mathsf{M}(\mathsf{R}) := \{c\tau : \tau \in \mathsf{S}, c \in R \setminus \{0\}\},$$

then each $f \in \mathsf{R} \setminus \{0\}$ has a unique finite representation

$$f = \sum_{\tau \in \mathrm{supp}(f)} m_\tau : m_\tau = c(f, \tau)\tau$$

as a sum of elements of the *monomial set* $\mathsf{M}(\mathsf{R})$.

Similarly, each $f \in \mathsf{R}^m \setminus \{0\}$ has a unique finite representation

$$f = \sum_{\tau \in \mathrm{supp}(f)} m_\tau : m_\tau = c(f, \tau)\tau, \tau = t\mathbf{e}_i$$

as a sum of elements of the *monomial set* $\mathsf{M}(\mathsf{R}^m) = \{ct\mathbf{e}_i : c \in R \setminus \{0\}, t \in \mathsf{S}, 1 \leq i \leq m\}$. ▯

Definition 46.1.6. *A (total) ordering* $<$ *on* $\mathsf{S}^{(m)}$ *will be called*

a semigroup ordering *if* $t_1 < t_2 \implies \lambda t_1\rho < \lambda t_2\rho$, *for each* $t_1, t_2 \in \mathsf{S}^{(m)}, \lambda, \rho \in \mathsf{S}$;
a term ordering *if it is a well-ordering and a semigroup ordering;*
a monotone ordering *if* $t_1 \leq t_2 \implies \lambda t_1\rho \leq \lambda t_2\rho$, *for each* $t_1, t_2 \in \mathsf{S}^{(m)}, \lambda, \rho \in \mathsf{S}$;
an admissible ordering *if it is a well-ordering and a monotone ordering;*
a $\prec$-extension of *(or:* $\prec$*-compatible with) a term-ordering* $\prec$ *on* S *if*

$$\omega_1 \prec \omega_2 \implies \omega_1 t < \omega_2 t, t\omega_1 < t\omega_2 \text{ for each } t \in \mathsf{S}^{(m)}, \omega_1, \omega_2 \in \mathsf{S}.$$

▯

While the following lemma is trivial, we need to stress it, since in Section 47.9.1 we will relax the assumption that $<$ is a semigroup ordering.

Lemma 46.1.7. *Let* $<$ *be an ordering on* $\mathsf{S}^{(m)}$. *Then the following conditions are equivalent:*

- $<$ *is a semigroup ordering;*
- *for each* $f \in \mathsf{R}^m$ *and each* $\lambda, \rho \in \mathsf{S}$, $\mathbf{T}(\lambda f\rho) = \lambda\mathbf{T}(f)\rho$.

▯

Corollary 46.1.8. *If $\prec$ is a term-ordering on S and $<$ is a $\prec$-compatible term-ordering on $\mathsf{S}^{(m)}$, then, for each $l, r \in \mathsf{R}$ and $f \in \mathsf{R}^{(m)}$,*

(1) $\mathbf{M}(lf) = \mathbf{M}(l)\mathbf{M}(f)$ *provided* $\mathrm{lc}(l)\,\mathrm{lc}(f) \neq 0$;
(2) $\mathbf{M}(fr) = \mathbf{M}(f)\mathbf{M}(r)$ *provided* $\mathrm{lc}(f)\,\mathrm{lc}(r) \neq 0$;
(3) $\mathbf{M}(lfr) = \mathbf{M}(l)\mathbf{M}(f)\mathbf{M}(r)$ *provided* $\mathrm{lc}(l)\,\mathrm{lc}(f)\,\mathrm{lc}(r) \neq 0$.
(4) $\mathbf{T}(lf) \leq \mathbf{T}(l)\mathbf{T}(f)$ *equality holding provided that* $\mathrm{lc}(l)\,\mathrm{lc}(f) \neq 0$;
(5) $\mathbf{T}(fr) \leq \mathbf{T}(f)\mathbf{T}(r)$ *equality holding provided that* $\mathrm{lc}(f)\,\mathrm{lc}(r) \neq 0$;
(6) $\mathbf{T}(lfr) \leq \mathbf{T}(l)\mathbf{T}(f)\mathbf{T}(r)$ *equality holding provided that* $\mathrm{lc}(l)\,\mathrm{lc}(f)\,\mathrm{lc}(r) \neq 0$.

If, moreover, R is a domain, then

(7) $\mathbf{T}(lf) = \mathbf{T}(l)\mathbf{T}(f)$;
(8) $\mathbf{T}(fr) = \mathbf{T}(f)\mathbf{T}(r)$;
(9) $\mathbf{T}(lfr) = \mathbf{T}(l)\mathbf{T}(f)\mathbf{T}(r)$.

Remark 46.1.9. Let $<$ be a total well-ordering on a monoid S; if $<$ is a term-ordering then S is cancellative[5]; group rings prove that the converse does not hold (Remark 46.1.13).

If $<$ is just a monotone but not a semigroup ordering, we can have $\lambda, t_1, t_2, \rho \in \mathsf{S}$ for which $t_1 < t_2$ and either $\lambda t_1 = \lambda t_2$, $t_1\rho = t_2\rho$ or $\lambda t_1\rho = \lambda t_2\rho$.

Also, if S is not cancellative, R can have zero-divisors, namely $t_1 - t_2$ and, respectively, $\lambda(t_1 - t_2) = 0$, $(t_1 - t_2)\rho = 0$, $\lambda(t_1 - t_2)\rho = 0$ (see Example 46.1.11).

Lemma 46.1.10. *The following conditions are equivalent:*

(1) R *is a domain,*
(2) *it holds both that*
   (a) *R is a domain and*
   (b) *each monotone ordering $<$ on S is a semigroup ordering.*

Proof.

(1) $\Longrightarrow$ (2) (a) is trivial; ad (b): if $<$ is a monotone ordering, which is not a term ordering, as mentioned in Remark 46.1.9, there were $\lambda, t_1, t_2, \rho \in \mathsf{S}$ for which $t_1 < t_2$ and either $\lambda t_1 = \lambda t_2$, $t_1\rho = t_2\rho$ or $\lambda t_1\rho = \lambda t_2\rho$, so that $t_1 - t_2$ is a zero-divisor.

(2) $\Longrightarrow$ (1) Let $f, g \in \mathsf{R} \setminus \{0\}$; then $at =: \mathbf{M}(f) \neq 0 \neq \mathbf{M}(g) := b\tau$ and by Corollary 46.1.8(1)

$$\mathbf{M}(fg) = \mathbf{M}(f)\mathbf{M}(g) = abt\tau$$

provided $ab \neq 0$; however, since by (a) $ab \neq 0$, then $\mathbf{M}(fg) \neq 0$ whence $fg \neq 0$.

□

Example 46.1.11. Let S be the non-cancellative commutative monoid generated by $\{X, Y, Z\}$ under the relations $\{YX \equiv XY, ZX \equiv XZ, ZY \equiv YZ, XZ \equiv YZ\}$.

Then, in $\mathbb{Z}_2[\mathsf{S}]$ $(X - Y)Z = 0$. □

[5] In fact assume $\lambda t_1\rho = \lambda t_2\rho$ and $t_1 \neq t_2$; since $<$ is total either $t_1 < t_2$, which is impossible since it implies $\lambda t_1\rho < \lambda t_2\rho$, or $t_1 > t_2$, which gives the contradiction $\lambda t_1\rho > \lambda t_2\rho$.

Example 46.1.12. A group S containing a cyclic group of finite order, while being obviously cancellative, does not possess any semigroup ordering.

In fact, for each element x, $1 \neq x \in \mathsf{S}$, $1 < x \iff x^{-1} < 1$; under this assumption, we can therefore fix an element x of finite order m and such that $1 < x$; for such an element we then have $1 < x < x^2 < \ldots x^{m-1} < x^m = 1$. ◻

Remark 46.1.13 *(Madlener–Reinert).* The situation is, in fact, more involved: let S be any group possessing a semigroup ordering $<$. Then the example above immediately implies that S cannot contain an element $x \neq 1$ of finite order. Moreover $<$ is not a well-ordering.

In fact for some $x \neq 1$ let us wlog assume $x > 1$; this implies

$$x > 1 > x^{-1} > x^{-2} > \cdots > x^{-n} > \cdots$$

since any equality $x^{-n} = x^{-m}$, $n < m$ would imply an equality $x^{m-n} = 1$. ◻

Example 46.1.14. In this general setting, we must keep in mind that the semigroup S does not in general satisfy Dickson's Lemma (Corollary 20.8.4).

The easiest example is the semigroup S of the words over $\{a, b\}$.

It is sufficient to set $t_i := ab^i a$, $i \in \mathbb{N}$, in order to obtain an infinite set for which $t_i \nmid t_j$ for each $i \neq j$. ◻

46.1.1 Gröbner Bases

In the function of a term ordering $<$ on $\mathsf{S}^{(m)}$ which is compatible with a term ordering on S which, with a slight abuse of notation, we still denote $<$, we denote, for any set $F \subset \mathsf{R}^m$,

- $\mathbf{T}\{F\} := \{\mathbf{T}(f) : f \in F\} \subset \mathsf{S}^{(m)}$;
- $\mathbf{M}\{F\} := \{\mathbf{M}(f) : f \in F\} \subset \mathsf{M}(\mathsf{R}^m)$.

In the rest of this chapter we will fix a term ordering $<$ on S; in a function of such ordering, we denote, for any set $F \subset \mathsf{R}$,

- $\mathbf{T}_L(F) := \mathbb{I}_L(\mathbf{T}\{F\}) = \{\mathbf{T}(\lambda f) : \lambda \in \mathsf{S}, f \in F\} = \{\lambda\mathbf{T}(f) : \lambda \in \mathsf{S}, f \in F\} \subset \mathsf{S}^{(m)}$;
- $\mathbf{M}_L(F) := \{\mathbf{M}(a\lambda f) : a \in R \setminus \{0\}, \lambda \in \mathsf{S}, f \in F\} = \{m\mathbf{M}(f) : m \in \mathsf{M}(\mathsf{R}), f \in F\} \subset \mathsf{M}(\mathsf{R}^m)$;
- $\mathbf{T}_R(F) := \mathbb{I}_R(\mathbf{T}\{F\}) = \{\mathbf{T}(f\rho) : \rho \in \mathsf{S}, f \in F\} = \{\mathbf{T}(f)\rho : \rho \in \mathsf{S}, f \in F\} \subset \mathsf{S}^{(m)}$;
- $\mathbf{M}_R(F) := \{\mathbf{M}(fb\rho) : b \in R \setminus \{0\}, \rho \in \mathsf{S}, f \in F\} = \{\mathbf{M}(f)n : n \in \mathsf{M}(\mathsf{R}), f \in F\} \subset \mathsf{M}(\mathsf{R}^m)$;
- $\mathbf{T}_2(F) := \mathbb{I}_2(\mathbf{T}\{F\}) = \{\mathbf{T}(\lambda f\rho) : \lambda, \rho \in \mathsf{S}, f \in F\} = \{\lambda\mathbf{T}(f)\rho : \lambda, \rho \in \mathsf{S}, f \in F\} \subset \mathsf{S}^{(m)}$;
- $\mathbf{M}_2(F) := \{\mathbf{M}(a\lambda fb\rho) : a, b \in R \setminus \{0\}, \lambda, \rho \in \mathsf{S}, f \in F\} = \{m\mathbf{M}(f)n : m, n \in \mathsf{M}(\mathsf{R}), f \in F\} \subset \mathsf{M}(\mathsf{R}^m)$.

Remark 46.1.15. If R is a skew field for each set $F \subset \mathsf{R}^m$ we have[6]

$$\begin{aligned} \mathbf{M}_L(F) = \mathbf{M}\{\mathbb{I}_L(\mathbf{M}\{F\})\} &= \mathbb{I}_L(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m), \\ \mathbf{M}_R(F) = \mathbf{M}\{\mathbb{I}_R(\mathbf{M}\{F\})\} &= \mathbb{I}_R(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m), \\ \mathbf{M}_2(F) = \mathbf{M}\{\mathbb{I}_2(\mathbf{M}\{F\})\} &= \mathbb{I}_2(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m) \end{aligned} \tag{46.2}$$

and the following conditions are equivalent and can be naturally chosen as definitions of Gröbner bases[7]

(1) $\mathbf{M}(\mathbb{I}(F)) = \mathbf{M}\{\mathbb{I}(F)\} = \mathbf{M}\{\mathbb{I}(\mathbf{M}\{F\})\} = \mathbb{I}(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m)$,
(2) for each $f \in \mathbb{I}(F)$ there is $g \in F$ such that $\mathbf{M}(g) \mid \mathbf{M}(f)$.

But, in general, between these statements there is just the implication (2) $\Longrightarrow$ (1).

In fact, unless R is a skew field, equalities (46.2) do not necessarily hold (cf. Example 46.1.16 below) but we have only the weaker inclusion

$$\mathbf{M}(F) \subseteq \mathbf{M}\{\mathbb{I}(\mathbf{M}\{F\})\} = \mathbb{I}(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m);$$

as a consequence there are two alternative natural definitions for the concept of Gröbner bases:

- a stronger one, which satisfies the following equivalent conditions:
  (i) for each $f \in \mathbb{I}(F)$ there is $g \in F$ such that $\mathbf{M}(g) \mid \mathbf{M}(f)$,
  (ii) for each $f \in \mathbb{I}(F)$ there are $g \in F$, $a, b \in R \setminus \{0\}$, $\lambda, \rho \in \mathsf{S}$ such that $\mathbf{M}(f) = \mathbf{M}(a\lambda\mathbf{M}(g)b\rho) = \mathbf{M}(a\lambda g b\rho)$,
  (iii) $\mathbf{M}(\mathbb{I}(F)) = \mathbf{M}\{\mathbb{I}(F)\} = \mathbf{M}(F)$;
- and a weaker one, which satisfies the following equivalent conditions:
  (iv) for each $f \in \mathbb{I}(F)$ there are $g_i \in F$, $a_i, b_i \in R \setminus \{0\}$, $\lambda_i, \rho_i \in \mathsf{S}$ for which, one has
  – $\mathbf{T}(f) = \lambda_i \mathbf{T}(g_i)\rho_i$ for each i, and $\mathrm{lc}(f) = \sum_i a_i \,\mathrm{lc}(g_i) b_i$
  and, equivalently,
  – $\mathbf{M}(f) = \sum_i \mathbf{M}(a_i\lambda_i\mathbf{M}(g_i)b_i\rho_i) = \sum_i \mathbf{M}(a_i\lambda_i g_i b_i \rho_i)$;

[6] From now on, in order to avoid cumbersome notation and boring repetition, we will drop the subscripts when it is clear which kind of module (left, right, bilateral) we are discussing. As a consequence, these three statements will be summarized as

$$\mathbf{M}(F) = \mathbf{M}\{\mathbb{I}(\mathbf{M}\{F\})\} = \mathbb{I}(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m).$$

For instance, the statement below must be read as

- The following conditions are equivalent
  (1) $\mathbf{M}_L(\mathbb{I}_L(F)) = \mathbf{M}\{\mathbb{I}_L(F)\} = \mathbf{M}\{\mathbb{I}_L(\mathbf{M}\{F\})\} = \mathbb{I}_L(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m)$,
  (2) for each $f \in \mathbb{I}_L(F)$ there are $g \in F$, $a \in R \setminus \{0\}$, $\lambda \in \mathsf{S}$ such that $a\lambda\mathbf{M}(g) = \mathbf{M}(f)$.
- The following conditions are equivalent
  (1) $\mathbf{M}_R(\mathbb{I}_R(F)) = \mathbf{M}\{\mathbb{I}_R(F)\} = \mathbf{M}\{\mathbb{I}_R(\mathbf{M}\{F\})\} = \mathbb{I}_R(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m)$,
  (2) for each $f \in \mathbb{I}_R(F)$ there are $g \in F$, $a \in R \setminus \{0\}$, $\rho \in \mathsf{S}$ such that $\mathbf{M}(g)a\rho = \mathbf{M}(f)$.
- The following conditions are equivalent
  (1) $\mathbf{M}_2(\mathbb{I}_2)(F)) = \mathbf{M}\{\mathbb{I}_2(F)\} = \mathbf{M}\{\mathbb{I}_2(\mathbf{M}\{F\})\} = \mathbb{I}_2(\mathbf{M}\{F\}) \cap \mathsf{M}(\mathsf{R}^m)$,
  (2) for each $f \in \mathbb{I}_2(F)$ there are $g \in F$, $a_l, a_r \in R \setminus \{0\}$, $\lambda, \rho \in \mathsf{S}$ such that $a_l\lambda\mathbf{M}(g)a_r\rho = \mathbf{M}(f)$.

[7] In the polynomial case they are respectively conditions **G1** and **G2** of Lemma 22.2.2.