Orderings and Algorithms in Commutative Algebra

Gerhard Schiffels

Introduction

For polynomial rings R in n indeterminates $X_1, \ldots, X_n$ over a field K, *B. Buchberger* introduced in 1965 a far reaching generalisation of both the euclidean algorithm ($n = 1$) and the Gauß elimination algorithm (linear systems). Given a set $A = (a_1, \ldots, a_m)$ of elements $a_i \in R$, *Buchberger's algorithm* calculates a *Gröbner basis* $B = (b_1, \ldots, b_p)$ of the ideal generated by A (cf. §4 or [Bu], 6.3 or [BW], 5.3 or [DST], 3.1). Gröbner bases are very useful for many important calculations, e.g. to decide if a given $f \in R$ lies in the ideal generated by A (cf. [Bu], 6.5 or [BW], Th. 5.58) or to solve the system of algebraic equations given by A (cf. [Bu], 6.6 or [BW], Chap. 7 and 8). We give here a *generalised version* of the Buchberger-Gröbner theory by taking for K a (noetherian) domain and for R the *K-algebra* of a (finitely generated, torsionfree) *monoid* Γ and by introducing *some more partial orderings* on K and R. We combine this with an extensive use of the theory of *well-partial orderings* (cf. [Kr] or [Mi] or [Ro], Chap. 10, §3).
In §1 - §3 and in §6 – §8 we take the point of view of classical mathematics, using freely also non-constructive methods such as the axiom of choice, Zorn's lemma and proofs by contradiction. The calculation methods are in §4 and §5. In §6 – §8 generalisations of §2 – §5 are indicated to equivariant ideals (§6), to modules (§7) and to lexicographical orderings (§8). These three last paragraphs do not depend on each other.
Related work is by Zacharias [Za], Möller [Mö], Shtokhamer [Sh], Adams-Boyle-Loustaunau [ABL], Ribenboim [Ri] and others. Articles especially related to §6 – §8 are by Cohen [Co] (§6), Möller-Mora [MM] and Rutman [Ru] (§7) and by Conrad-Harvey-Holland [CHH] (§8).
I am grateful to Andreas Dress for suggesting the following particular approach (cf. [DS]).

§ 1. Some orderings on certain monoids Γ

A relation $\alpha \leq \beta$ on a set Γ is a *partial ordering,* if it is transitive ($\alpha \leq \gamma$, if $\alpha \leq \beta$ and $\beta \leq \gamma$) and irreflexive ($\alpha = \beta$, if $\alpha \leq \beta$ and $\beta \leq \alpha$). We write $\alpha < \beta$, if $\alpha \leq \beta$ and $\alpha \neq \beta$. A partial ordering is called *well-founded,* if there are no infinite strictly descending chains $\alpha_0 > \alpha_1 > \alpha_2 > \ldots$. The elements α and β are *incomparable* (denoted $\alpha \| \beta$), if neither $\alpha \leq \beta$ nor $\beta \leq \alpha$. An *antichain* is a set of pairwise incomparable elements. The partially ordered (p.o.) set $(\Gamma, \leq)$ is called *narrow,* if there are no infinite antichains. If $(\Gamma, \leq)$ is well-founded and narrow, it is called *well partially ordered* (wpo). A *linear* ordering (always $\alpha \leq \beta$ or $\beta \leq \alpha$) surely is narrow; if it is well-founded, it is usually called a *well-ordering.* A partial ordering $\leq'$ *extends* $\leq$, if $\alpha \leq \beta$ implies $\alpha \leq' \beta$. We use $\mathbb{N}$ for $\{0, 1, 2, \ldots\}$. If a set S contains a zero 0, we put $S^\bullet = S\backslash\{0\}$. So we have $\mathbb{N}^\bullet = \{1, 2, \ldots\}$. For $n \in \mathbb{N}^\bullet$ we put $\underline{n} = \{1, \ldots, n\}$.

(1.1) **Theorem** ([Kr], [Mi]): For a p.o. set $(\Gamma, \leq)$, the following are equivalent:

(1) $(\Gamma, \leq)$ is well-founded and narrow (i.e. wpo).

(2) For every non-void subset M of Γ, the set
$\mathrm{Min}(M, \leq) := \{\alpha \in M \mid \text{there is no } \beta \in M \text{ s.t. } \beta < \alpha\}$
of its minimal elements is non-void and finite.

(3) For every sequence $(\alpha_i)_{i\in\mathbb{N}}$ of elements $\alpha_i \in \Gamma$ there are indices $j < k$ s.t. $\alpha_j \leq \alpha_k$.

(4) Every sequence $(\alpha_i)_{i\in\mathbb{N}}$ of elements $\alpha_i \in \Gamma$ contains an ascending subsequence $(\alpha_{i_j})_{j\in\mathbb{N}}$, i.e. $i_j < i_k$ and $\alpha_{i_j} \leq \alpha_{i_k}$ for all $j < k$.

(5) All linear extensions $\leq'$ of $\leq$ are well-orderings.

Sketch of proof: (1) $\Longleftrightarrow$ (2): The antichains of $(\Gamma, \leq)$ are just the subsets of the form $\mathrm{Min}(M, \leq), M \subseteq \Gamma$. If a non-void M has no minimal elements, we get an infinite strictly descending chain of elements of M by using the axiom of choice. Conversely, if $(\alpha_i)_{i\in\mathbb{N}}$ $(\alpha_i \in \Gamma)$ is strictly descending, the set $\{\alpha_i \mid i \in \mathbb{N}\}$ has no minimal elements.
(1) $\Longrightarrow$ (4): Given a sequence $(\alpha_i)_{i\in\mathbb{N}}$ in Γ, for each $j < k$ we have *either* $\alpha_j > \alpha_k$ *or* $\alpha_j \| \alpha_k$ *or* $\alpha_j \leq \alpha_k$. Consequently, by the infinite Ramsey theorem (see [Ro], 7.4 and 10.16) there is an infinite subset R of $\mathbb{N}$ with $\alpha_j > \alpha_k$ for all $(j, k) \in R \times R$ satisfying $j < k$ *or* there is an infinite subset S of $\mathbb{N}$ with $\alpha_j \| \alpha_k$ for all $(j, k) \in S \times S$ satisfying $j \neq k$ *or* there is an infinite subset T of $\mathbb{N}$ with $\alpha_j \leq \alpha_k$ for all $(j, k) \in T \times T$ satisfying $j < k$. But by (1), the first two possibilities are excluded.
(4) $\Longrightarrow$ (3) $\Longrightarrow$ (1) is trivial. If (5) is false, so is (3).
(5) $\Longrightarrow$ (1): If $\alpha \| \beta$ in $(\Gamma, \leq)$, following [Sz] we may define an extension $\leq_1$ of $\leq$ satisfying $\alpha >_1 \beta$ by putting $\xi \geq_1 \eta$ iff $\xi \geq \eta$ or both $\xi \geq \alpha$ and $\beta \geq \eta$. If there is an infinite antichain $(\alpha_i)_{i\in\mathbb{N}}$ in $(\Gamma, \leq)$, we may apply this extension process infinitely often, and we get an extension $\leq_\infty$ of $\leq$, in which our antichain becomes a strictly descending sequence. On the other hand, the set E of all extensions of $\leq$ is inductive when seen as a set of subsets of $\Gamma \times \Gamma$, ordered by inclusion. By Zorn's lemma, E contains maximal elements, which extend a given element $\leq_\infty$ of E. All maximal elements of E are linear orderings, for otherwise we could strictly extend one of them by the above process from [Sz]. So if $(\Gamma, \leq)$ is not narrow, there are linear extensions of $\leq$, which are not well-ordered. If $(\Gamma, \leq)$ is not well-founded, no linear extension of $\leq$ is well-ordered. $\square$

In the following, a *monoid* $\Gamma = (\Gamma, +, 0)$ will always be *commutative* $(\alpha + \beta = \beta + \alpha)$, *cancellative* $(\alpha + \gamma = \beta + \gamma \Rightarrow \alpha = \beta)$ and *inverse-free* $(\alpha + \beta = 0 \Rightarrow \alpha = \beta = 0)$. Consequently, the relation on Γ

$$\alpha \leq_+ \beta :\Longleftrightarrow \exists\, \gamma \in \Gamma : \alpha + \gamma = \beta \tag{1.2}$$

is a partial ordering, called the *addition ordering.* It is *compatible* with the monoid structure of Γ in the sense that $\alpha <_+ \beta$ implies $\alpha + \gamma <_+ \beta + \gamma$ and that furthermore $0 <_+ \alpha$ for all $\alpha \neq 0$. Every compatible partial ordering on the monoid Γ is an extension of $\leq_+$.

(1.3) **Proposition:** $(\Gamma, \leq_+)$ is wpo iff the monoid $(\Gamma, +, 0)$ is finitely generated.

Proof: 1. If $(\Gamma, \leq_+)$ is wpo, then by (1.1.2) the set $A = \mathrm{Min}(\Gamma\backslash\{0\}, \leq)$ is finite. If then the subset $\overline{A}$ generated by A in the monoid Γ is different from Γ, take a minimal element β of $\Gamma\backslash\overline{A}$. There is an $\alpha \in A$ with $\alpha \leq_+ \beta$, so we have a $\gamma \in \Gamma$ with $\alpha + \gamma = \beta$. Consequently $\gamma <_+ \beta, \gamma \in \overline{A}$ and so $\beta = \gamma + \alpha \in \overline{A}$, a contradiction.
2. If the monoid Γ is generated by $A = (\gamma_1, \ldots, \gamma_n)$, there is a surjective monoid-homomorphism $f : \mathbb{N}^n \to \Gamma$ with $f(\delta_i) = \gamma_i$ for all $i \in \underline{n}$. Here $\mathbb{N}^n$ is the n-fold cartesian product of $\mathbb{N}$ with componentwise addition, and δ_i is $(\delta_{i1}, \ldots, \delta_{in})$ with $\delta_{ii} = 1$ and $\delta_{ij} = 0$ for $i \neq j$. It turns out, that the addition ordering on the monoid $\mathbb{N}^n$ is just the usual product-partial-ordering of the natural well-orderings of the factors $\mathbb{N}$. Consequently by (1.1.4) we see easily, that $(\mathbb{N}^n, \leq_+)$ is wpo ("Dickson's Lemma", 1913). Now, if $(\alpha_i)_{i\in\mathbb{N}}$ is a sequence in Γ, for every $i \in \mathbb{N}$ take an $a^{(i)} \in \mathbb{N}^n$ with $f(a^{(i)}) = \alpha_i$. Then by (1.1.3) there are $j < k$ and $c \in \mathbb{N}^n$ s.t. $a^{(j)} + c = a^{(k)}$. Consequently we have $\alpha_j + f(c) = \alpha_k$ and $\alpha_j \leq_+ \alpha_k$. So $(\Gamma, \leq_+)$ is wpo too. $\square$

(1.4) **Proposition:** The monoid Γ admits a compatible linear ordering iff it is torsion-free, i.e.

(1) $$k \in \mathbb{N}^\bullet,\ k \circ \alpha = k \circ \beta \quad \Rightarrow \quad \alpha = \beta,$$

where $k \circ \gamma$ means the sum of k elements $\gamma \in \Gamma$.

Proof. 1. If $\leq$ is a compatible linear ordering on Γ and if $\alpha \neq \beta$, we have $\alpha < \beta$ or $\alpha > \beta$. So for every $k \in \mathbb{N}^\bullet$ we get $k \circ \alpha < k \circ \beta$ or $k \circ \alpha > k \circ \beta$.
2. Let Γ be torsionfree and let Δ be the difference group of Γ. We have
$\Delta = \{\alpha - \beta \,|\, \alpha, \beta \in \Gamma\}$, where $\alpha - \beta := \{(\gamma, \delta) \in \Gamma \times \Gamma \,|\, \alpha + \delta = \beta + \gamma\}$. Since Γ is cancellative, it is embedded into Δ by $\alpha \longmapsto \alpha - 0$. By (1), Δ is torsionfree in the group-theoretic sense, i.e. $k \in \mathbb{N}^\bullet$ and $k \circ (\alpha - \beta) = 0$ imply $\alpha - \beta = 0$. The addition ordering $\leq_+$ of Γ may be continued to Δ by putting $\alpha - \beta \leq'_+ \gamma - \delta$ iff $\alpha + \delta \leq_+ \gamma + \beta$. We have $\Gamma = \{a \in \Delta \,|\, 0 \leq'_+ a\}$, and $\leq'_+$ is compatible in the group-theoretic sense, i.e. for $a, b, c \in \Delta$ the relation $a \leq'_+ b$ implies $a + c \leq'_+ b + c$. In [FE], the method of (1.1), (5) $\Rightarrow$ (1) is carried over to abelian groups, supplying group-compatible linear extensions $\leq'$ of $\leq'_+$. The restriction to Γ of such a $\leq'$ is a monoid-compatible linear ordering on Γ. $\square$
Remark: If Γ is torsionfree and generated by n elements, it is well-known that $\Delta \cong \mathbb{Z}^r$ for some $r \leq n$.

§ 2. The algebra R of Γ over a domain K

Let Γ be a monoid, and let K be a *domain,* i.e. a commutative ring with identity 1, having no zero-divisors. We denote by R or $K^{(\Gamma)}$ the K-module of all maps $f : \Gamma \to K, \alpha \longmapsto f_\alpha$ with finite support $\mathrm{supp}(f) := \{\alpha \in \Gamma \,|\, f_\alpha \neq 0\}$. Let X be a bijection $\alpha \longmapsto X^\alpha$ of Γ onto some set $P_\Gamma(X)$. By the definition

(2.1) $$X^\alpha \cdot X^\beta = X^{\alpha+\beta} \qquad (\alpha, \beta \in \Gamma),$$

$P_\Gamma(X)$ becomes a multiplicative monoid and X becomes an isomorphism. Writing

$$(2.2) \qquad f = \sum_{\alpha\in\Gamma} f_\alpha X^\alpha \qquad \text{for} \quad f \in K^{(\Gamma)}$$

and applying the multiplication table (2.1), we see that $K^{(\Gamma)}$ becomes the *monoid-algebra* of $P_\Gamma(X) \cong \Gamma$ over K. We denote $R = K^{(\Gamma)}$ also by $K[X]$. – It will be important (§ 3) to choose a monoid-compatible *linear* ordering $\leq$ on Γ. Depending on $\leq$, for each $f \in R^\bullet$ we define the *leading exponent* by

$$(2.3) \qquad le(f) := \max(\mathrm{supp}(f), \leq)$$

and the *leading coefficient* by

$$(2.4) \qquad lc(f) = f_{(le(f))}.$$

Note that for $f, g \in R^\bullet$ we have

$$(2.5) \qquad le(f+g) \leq \max(le(f), le(g)) \qquad (\text{if } f+g \neq 0)$$

and, as K has no zero-divisors,

$$(2.6) \qquad le(f\cdot g) = le(f) + le(g),\ lc(f\cdot g) = lc(f)\cdot lc(g).$$

We have the "sparse" representation

$$(2.7) \qquad f = \sum_{i=1}^{k} f_{\alpha_i} X^{\alpha_i}, \qquad f_{\alpha_i} \in K^\bullet, \alpha_i \in \Gamma, \alpha_1 > \alpha_2 > \cdots > \alpha_k.$$

Consider the special case $\Gamma = \mathbb{N}^n, n \in \mathbb{N}^\bullet$. If $\delta_i = (\delta_{i1}, \dots, \delta_{in})$, we put $X_i = X^{\delta_i}$. Then for $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ we have $X^\alpha = X_1^{\alpha_1} \cdot \ldots \cdot X_n^{\alpha_n}$, where $X_i^{\alpha_i}$ is the α_i-th power of X_i in the ring $R = K^{(\Gamma)}$. So R is the usual polynomial ring $K[X_1, \dots, X_n]$ in the indeterminates $X_1, \dots, X_n$ over K. Frequent choices of a linear ordering $\leq$ on $\mathbb{N}^n$ (see e.g. the Gröbner Basis Package of MAPLE V, [MA]) are the *purely lexicographical ordering*

$$(2.8) \qquad \alpha < \beta : \iff \exists k \in \underline{n} : \alpha_k < \beta_k \text{ and } \alpha_i = \beta_i \text{ for } i < k.$$

and the *total degree ordering* with *ties broken* by the *inverse lexicographical ordering,* i.e. writing $|\alpha| = \alpha_1 + \cdots + \alpha_n$ we have

$$(2.9)\ \alpha < \beta :\Leftrightarrow (|\alpha| < |\beta| \text{or both } |\alpha| = |\beta| \text{and } \exists k \in \underline{n} : \alpha_k < \beta_k \text{ and } \alpha_i = \beta_i \text{ for } i > k).$$

§ 3. Top-reductions and Gröbner Bases

From now on we suppose always that the monoid $(\Gamma, +, 0)$ is *finitely generated* and *torsionfree. We suppose also* that a *monoid-compatible linear ordering* $\leq$ on Γ (cf. (1.4)) has been chosen (and will be kept fixed). Both the basic notions (like (2.3), (2.4), (3.3), (3.9)) and the practical performance of Gröbner methods depend heavily on this choice. By (1.3) and (1.1.5), $\leq$ is a well-ordering.

We consider the algebra $R = K^{(\Gamma)}$, where K is a domain. Let A be any subset of $R^\bullet$ and denote by $\mathfrak{A}$ the R-ideal generated by A. Here the void set is supposed to generate the ideal $\{0\}$. If A is non-void, every $a \in \mathfrak{A}^\bullet$ has a representation

$$a = \sum_{i=1}^{m} f_i a_i, \quad m \in \mathbb{N}^\bullet, f_i \in R^\bullet, a_i \in A \ (i \in \underline{m}). \tag{3.1}$$

We call (3.1) a *standard representation* (w.r.t. $\leq$) of a by A, if

$$le(f_i a_i) \leq le(a) \ \text{ for all } \ i \in \underline{m}. \tag{3.2}$$

(3.3) **Definition:** For $f \in R^\bullet$ and $g \in R$ we write $f \underset{A}{\longrightarrow} g$ iff there are $m \in \mathbb{N}^\bullet, u_i \in K^\bullet, \gamma_i \in \Gamma, a_i \in A$ ($i \in \underline{m}$) such that

(1) $g = f - \sum_{i=1}^{m} u_i X^{\gamma_i} a_i$,

(2) $\gamma_i + le(a_i) = le(f)$ for all $i \in \underline{m}$,

(3) $lc(f) = \sum_{i=1}^{m} u_i \cdot lc(a_i)$.

We write $f \overset{*}{\underset{A}{\longrightarrow}} g$, if $g = f$ or g is a member of a chain

(4) $f \underset{A}{\longrightarrow} f_1 \underset{A}{\longrightarrow} f_2 \underset{A}{\longrightarrow} \ldots$

beginning with f. The relations $\underset{A}{\longrightarrow}$ and $\overset{*}{\underset{A}{\longrightarrow}}$ are called *top-reductions.*

Clearly $f \underset{A}{\longrightarrow} g$ implies $g \in f + \mathfrak{A}$, and using (2.5) and (2.6) we see that $le(g) < le(f)$. Consequently, $\leq$ being well-ordered, all chains (3.3.4) are finite.

(3.4) **Definition:** For each $\gamma \in \Gamma$ let A_γ (resp. A'_γ) be the K-ideal generated by all elements $lc(a)$, where $a \in A$ and $le(a) \leq_+ \gamma$ (resp. $le(a) <_+ \gamma$). In case $A = \mathfrak{A}^\bullet$ we write simply $\mathfrak{A}_\gamma$ (resp. $\mathfrak{A}'_\gamma$).

By (1.2) and (2.6) we see that

$$\beta <_+ \gamma \implies A_\beta \subseteq A'_\gamma \subseteq A_\gamma. \tag{3.5}$$

We have also

$$A \subseteq B \subseteq R^\bullet \implies A_\gamma \subseteq B_\gamma \ \text{ and } \ A'_\gamma \subseteq B'_\gamma. \tag{3.6}$$

Finally, we define the *critical index set* of $\mathfrak{A}$ by

$$C(\mathfrak{A}) = \{\gamma \in \Gamma \,|\, \mathfrak{A}'_\gamma \neq \mathfrak{A}_\gamma\}. \tag{3.7}$$

(3.8) **Proposition:** For $A \subseteq R^\bullet$ and the R-ideal $\mathfrak{A}$ generated by A the following are equivalent:

(1) Every $a \in \mathfrak{A}^\bullet$ is $(\underset{A}{\longrightarrow})$-*reducible,* i.e. $a \underset{A}{\longrightarrow} a'$ for some $a' \in \mathfrak{A}$.

(2) $a \overset{*}{\underset{A}{\longrightarrow}} 0$ for all $a \in \mathfrak{A}$.

(3) Every $a \in \mathfrak{A}^\bullet$ has a standard representation by A.

(4) $A_\gamma = \mathfrak{A}_\gamma$ for all $\gamma \in \Gamma$.

(5) $A_\gamma = \mathfrak{A}_\gamma$ for all $\gamma \in C(\mathfrak{A})$.

Proof: (1) $\Longrightarrow$ (2) holds because the $(\underset{A}{\longrightarrow})$-chains are finite. (2) $\Longrightarrow$ (3) follows by collecting the subtrahends (3.3.1) of the reductions $a \underset{A}{\longrightarrow} a'_1 \underset{A}{\longrightarrow} a'_2 \underset{A}{\longrightarrow} \cdots \underset{A}{\longrightarrow} a'_n = 0$. (3) $\Longrightarrow$ (1): If (3.1) and (3.2) hold and M is the set of all $i \in \underline{m}$ satisfying $le(f_i a_i) = le(a)$, we get the reduction $a \underset{A}{\longrightarrow} a'$ with $a' = a - \sum_{i \in M} u_i X^{\gamma_i} a_i,\ \gamma_i = le(f_i),\ u_i = lc(f_i)$.
(3) $\Longrightarrow$ (4) $\Longrightarrow$ (1) is easy and (4) $\Longrightarrow$ (5) is trivial. Now suppose that (5) is true and (4) is false. Then take a $(\leq_+)$-minimal $\gamma \in \Gamma$ with $A_\gamma \neq \mathfrak{A}_\gamma$. By (5) we have $\gamma \notin C(\mathfrak{A})$, consequently

$$\mathfrak{A}_\gamma = \mathfrak{A}'_\gamma = \sum_{\alpha <_+ \gamma} \mathfrak{A}_\alpha = \sum_{\alpha <_+ \gamma} A_\alpha = A'_\gamma \subseteq A_\gamma$$

and so we get the contradiction $A_\gamma = \mathfrak{A}_\gamma$. □

(3.9) **Definition.** $A \subseteq R^\bullet$ is a *Gröbner basis* (w.r.t. $\leq$) of the ideal $\mathfrak{A}$ generated by A, if A is finite and the conditions (1) – (5) of (3.8) hold.

As is well known, every ideal of K has a finite system of generators (finite "basis" as it is called by Hilbert) iff in K there are no infinite strictly ascending chains $\mathfrak{a}_0 \subset \mathfrak{a}_1 \subset \mathfrak{a}_2 \subset \cdots$ of ideals. If both conditions are satisfied, the domain K is called *noetherian.* We now get a "Gröbner version" of the well known Hilbert Basis Theorem:

(3.10) **Theorem:** Suppose K to be noetherian. Then in $R = K^{(\Gamma)}$ every ideal has a Gröbner basis.

Proof: If $\mathfrak{A}$ is any R-ideal, its critical set $C(\mathfrak{A})$ is finite, since otherwise by (1.1.4) the set $C(\mathfrak{A})$ would contain a sequence $(\gamma_i)_{i \in \mathbb{N}}$ satisfying $\gamma_i <_+ \gamma_{i+1}$ for all $i \in \mathbb{N}$. Consequently there would be the strictly ascending chain $(\mathfrak{A}_{\gamma_i})_{i \in \mathbb{N}}$ of K-ideals (see (3.5) and (3.7)), a contradiction to K being noetherian. Now, for every $\gamma \in C(\mathfrak{A})$ we may select finitely many elements $a_i^\gamma \in \mathfrak{A}$ $(i = 1, \dots n_\gamma)$ such that $le(a_i^\gamma) = \gamma$ for all i and

$$\mathfrak{A}_\gamma = \mathfrak{A}'_\gamma + \sum_{i=1}^{n_\gamma} K \cdot lc(a_i^\gamma). \tag{3.11}$$

Remarking that $\mathfrak{A}'_\gamma = \{0\}$ for $\gamma \in \mathrm{Min}(C(\mathfrak{A}), \leq_+)$ and using induction in $(C(\mathfrak{A}), \leq_+)$, we see by (3.11) that (3.8.5) holds for the finite set

$$A = \{a_i^\gamma \mid \gamma \in C(\mathfrak{A}), i = 1, \dots, n_\gamma\}, \tag{3.12}$$

and so A is a Gröbner basis for $\mathfrak{A}$.

§ 4. Buchberger's algorithmic method

From now on *we suppose also* that the domain K is *noetherian.*

The classical Hilbert Basis Theorem of 1888 asserts, that *every* ideal of the polynomial ring $R = K[X_1, \dots, X_n]$ over a field K has a finite system of generators. As is well known by the historical discussion (see e.g. [Be], App. 1) this result is essentially nonconstructive, and consequently so is (3.10). But *given* a *finite* list

$$A = (a_1, \dots, a_m) \in (R^\bullet)^m \tag{4.1}$$

the Buchberger algorithm calculates a Gröbner basis $B = (b_1, \dots, b_p)$ of the ideal $\mathfrak{A}$ generated by A. In our generalised version, the Buchberger method reads as follows:

First *suppose,* that the monoid Γ and the domain K are *computable* (see [BW], 4.6), which essentially means that there are algorithms for the algebraic operations $(\alpha, \beta) \longmapsto \alpha + \beta, (u, v) \longmapsto u + v$ etc. (including $u \longmapsto u^{-1}$ in case of a field K). *Suppose* also that the orderings $\leq_+$ and $\leq$ are *decidable* ([BW], 4.6). So given α and β, there are algorithms which decide $\alpha \leq_+ \beta$ and $\alpha \leq \beta$. We shall need three further conditions of computability, which we introduce more conveniently below. All these conditions are fullfilled e.g. if Γ is $\mathbb{N}^n$, if $\leq$ is given by (2.8) or (2.9) and if K is $\mathbb{Z}, \mathbb{Q}$, an algebraic number field or a finite field. – We shall use finiteness properties of chains for proving that our algorithms will terminate after some finite numbers of steps. We do not enter into questions on upper bounds for these numbers of steps. (But see e.g. [Bu], 6.10 or [DST], 3.1.4 or [Bu2].)

Then given (4.1), put

(4.2) $$\alpha_i = le(a_i),\ \ v_i = lc(a_i) \ \text{ for all } \ i \in \underline{m}.$$

For any $F = (f_1, \dots, f_m) \in R^m$ with some $f_i \neq 0$, put

(4.3) $$F \cdot A = f_1 a_1 + \dots + f_m\, a_m$$

and call

(4.4) $$le(F, A) := \max\Big(\{le(f_i) + \alpha_i \,|\, i \in \underline{m},\ f_i \neq 0\}, \leq\Big)$$

the *formal degree* of $F \cdot A$ (w.r.t. to the representation given by F and A). Put also

(4.5) $$M(F, A) = \{i \in \underline{m} \,|\, f_i \neq 0, le(f_i) + \alpha_i = le(F, A)\}.$$

Then we have

(4.6) $$le(F, A) > le(F \cdot A) \quad \text{iff} \quad \sum_{i \in M(F,A)} lc(f_i) \cdot v_i = 0 \quad (\text{ and } \ |M(F, A)| \geq 2).$$

Vice versa, for each $M \subseteq \underline{m}$ with $|M| \geq 2$ consider the K-module (of *"syzygies"*)

(4.7) $$\mathfrak{S}_M = \Big\{u = (u_i)_{i \in \underline{m}} \in K^m \mid u_i = 0 \text{ for } i \notin M,\ \sum_{i=1}^{m} u_i v_i = 0\Big\}$$

Clearly we have $\mathfrak{S}_N \subseteq \mathfrak{S}_M$ for $N \subseteq M$. *We suppose now,* that given a finite set of elements of $\mathfrak{S}_M$, we may decide if it generates $\mathfrak{S}_M$, and in the negative case we may calculate a further independent element of $\mathfrak{S}_M$. Considering at first the case $|M| = 2$, we then may calculate successively elements

(4.8) $$u_M^{(k)} = (u_{M,i}^{(k)})_{i \in \underline{m}} \in \mathfrak{S}_M\ , \quad k = 1, 2 \dots$$

such that $u_M^{(k)}$ is not in the K-module generated by the $u_M^{(i)}$ with $i < k$. Since $\mathfrak{S}_M$

is well-known to be noetherian (no infinite strictly ascending chains of submodules), this process terminates after some natural number t_M of steps, supplying a system of generators of $\mathfrak{S}_M$. If $|M| > 2$ and the elements $u_N^{(k)}$ $(k = 1, \ldots, t_N)$ are already found for all $N \subset M$ satisfying $2 \leq |N| < |M|$, we calculate in the same manner as before elements (4.8) such that

$$\mathfrak{S}_M = \left(\sum_{N \subset M} \sum_{k=1}^{t_N} K u_N^{(k)} \right) + \sum_{k=1}^{t_M} K u_M^{(k)}. \tag{4.9}$$

(If K is a field resp. a principal ideal domain, by [Bu] resp. [Mö] we have $t_M = 0$ for $|M| > 2$.)

Note that we get $\alpha_i \leq_+ \gamma$ for all $i \in M \subseteq \underline{m}$, if γ is e.g. the sum of the α_i. Consequently since $(\Gamma, \leq_+)$ is wpo, for each $M \subseteq \underline{m}$ the set

$$\Gamma_M = \mathrm{Min}\Big(\{ \gamma \in \Gamma \,|\, \alpha_i \leq_+ \gamma \ \text{ for all } \ i \in M \}, \leq_+ \Big) \tag{4.10}$$

is non-void and finite. For $\Gamma = \mathbb{N}^n$ the set Γ_M contains only the element $\sup(\{\alpha_i | i \in M\}, \leq_+)$. In the general case (see also [Re]), *we suppose now* that we have a monoid Γ, in which each Γ_M is computable from the α_i $(i \in M)$. Consequently we may compute the finitely many *"S-polynoms"* (w.r.t. A)

$$S_{M,\varepsilon}^{(k)} := \sum_{i \in M} u_{M,i}^{(k)} X^{\varepsilon - \alpha_i} a_i \quad (M \subseteq \underline{m}, \varepsilon \in \Gamma_M, k = 1, \ldots, t_M) \tag{4.11}$$

Surely, all S-polynoms of A are elements of $\mathfrak{A}$. *Our final condition of computability* concerns inhomogeneous linear equations with coefficients in K (like (3.3.3), where $u_1, \ldots, u_m$ are the unknowns). We suppose that K is such that we can decide about solvability, and that in the positive case we may compute a solution. Consequently we are able to decide if a given $f \in R^\bullet$ is $(\underset{A}{\longrightarrow})$-*reduced* (no $g \in R$ satisfying $f \underset{A}{\longrightarrow} g$), and in the negative case we may compute a reduction $f \underset{A}{\longrightarrow} f_1$. So we may also compute a reduced f_n satisfying $f \overset{*}{\underset{A}{\longrightarrow}} f_n$.

(4.12) **Theorem:** (Buchberger's algorithmic criterium for Gröbner Bases).
Let A be a finite basis of $\mathfrak{A}$. Then A is a Gröbner basis, if

(1) $$S_{M,\varepsilon}^{(k)} \overset{*}{\underset{A}{\longrightarrow}} 0 \qquad \text{for all } S\text{-polynoms (4.11) of } A.$$

Conversely A is not a Gröbner basis, if for some S-polynom of A we get a relation $S_{M,\varepsilon}^{(k)} \overset{*}{\underset{A}{\longrightarrow}} a$ with an $(\underset{A}{\longrightarrow})$-reduced $a \neq 0$.

Proof: In view of (3.9) the converse part follows from (3.8.1). Now suppose that (1) holds. Then every $S_{M,\varepsilon}^{(k)}$ has a standard representation $F \cdot A$, by the proof (2) $\Longrightarrow$ (3) of (3.8). Since the elements (4.8) used in definition (4.11) lie in the module $\mathfrak{S}_M$ of syzygies, we have $le(F, A) = le(S_{M,\varepsilon}^{(k)}) < \varepsilon$. If A was not a Gröbner basis, consider an $a \in \mathfrak{A}$ without standard representation by A and then take a non-standard representation $G \cdot A$ $(G = (g_1, \ldots, g_m))$ of a with $(\leq)$-smallest formal degree $le(G, A)$. By the definition of the set (4.11), in view of (4.5) – (4.10) we easily see that we may replace $\sum_{i \in M(G,A)} g_i a_i$ by a sum $\sum_{i=1}^{m} h_i a_i$ of smaller formal degree, using standard representations of the S-polynoms. The result will be a representation of the element a having smaller formal degree than $le(G, A)$, contradiction. $\square$

Now we easily get the *Buchberger algorithm* for transforming a finite basis (4.1) of $\mathfrak{A}$ into a Gröbner basis B of $\mathfrak{A}$. We start with $A^{(0)} = A$. If (4.12.1) turns out to be satisfied, take $B = A^{(0)}$. Otherwise we meet some (M, ε, k) and some $(\underset{A^{(0)}}{\longrightarrow})$-reduced $a_{m+1} \neq 0$ satisfying $S^{(k)}_{M,\varepsilon} \overset{*}{\longrightarrow} a_{m+1}$. Surely $a_{m+1} \in \mathfrak{A}$, and by the definitions (3.3) and (3.4) we have $lc(a_{m+1}) \notin A^{(0)}_{\gamma_1}$ for $\gamma_1 = le(a_{m+1})$. Now take for $A^{(1)}$ the vector $(a_1, \ldots, a_m, a_{m+1})$ or some vector obtained from this one by reducing some elements $a_i, i < m+1$ w.r.t. the set formed by a_{m+1} and the a_j with $j \neq i$. In any case we have $A^{(1)}_\gamma \supseteq A^{(0)}_\gamma$ for all $\gamma \in \Gamma$, with strict inclusion for $\gamma = \gamma_1$. Now form the S-polynoms of $A^{(1)}$ and restart. If $A^{(1)}$ is not yet a Gröbner basis, we get elements a_{m+2}, γ_2 just as before a_{m+1}, γ_1. The algorithm terminates at some $t \in \mathbb{N}$ with a Gröbner basis $A^{(t)}$, since otherwise we would get an infinite sequence of elements γ_i $(i \in \mathbb{N}^\bullet)$, such that $A^{(i)}_\gamma \subseteq A^{(i+1)}_\gamma$ for all $\gamma \in \Gamma$, with strict inclusion for $\gamma = \gamma_{i+1}$. Consequently if $i < j$, we have $A^{(i)}_\gamma \subseteq A^{(j)}_\gamma$ for all $\gamma \in \Gamma$, with strict inclusion for $\gamma = \gamma_j$. Since $(\Gamma, \leq_+)$ is wpo, passing to a subsequence of $(\gamma_i)_i$ we may also suppose that $\gamma_i \leq_+ \gamma_j$ for $i < j$ (cf. (1.1.4)). But then by (3.5) we get $A^{(i)}_{\gamma_i} \subseteq A^{(i)}_{\gamma_j} \subset A^{(j)}_{\gamma_j}$ for all $i < j$. So we would get an infinite strictly ascending chain of K-ideals, a contradiction to K being noetherian.

§ 5. General reductions and normal forms

Maintaining the assumptions of § 3 and § 4 on $K, \Gamma, \leq_+$ and $\leq$, *we now suppose* that for each $\alpha \in \Gamma$ we are given a well-founded partial ordering $\preceq_\alpha$ of K satisfying $0 \in \operatorname{Min}(K, \preceq_\alpha)$. Then we introduce on $R = K^{(\Gamma)}$ the *inverse lexicographical partial ordering* $\sqsubseteq = \operatorname{invlex}(\leq, (\preceq_\alpha)_{\alpha \in \Gamma})$ defined by

(5.1) $\qquad f \sqsubset g$ iff there is $\gamma \in \Gamma$ satisfying $f_\gamma \prec_\gamma g_\gamma$ and $f_\alpha = g_\alpha$ for all $\alpha > \gamma$.

We have

(5.2) **Proposition:** The partial ordering $\sqsubseteq$ is well-founded.

Proof: By the proof (1) $\iff$ (2) of (1.1) we see that a partially ordered set is well-founded iff every non-void subset has minimal elements. By our definitions, the zero-element of R is $(\sqsubseteq)$-minimal in R. So we need only to show that every non-void set $\mathfrak{M} \subseteq R^\bullet$ has $(\sqsubseteq)$-minimal elements. Consider $\mu = \min(\{le(f) \mid f \in \mathfrak{M}\}, \leq)$, $\mathfrak{M}_\mu = \{f \in \mathfrak{M} \mid le(f) = \mu\}$ and $M = \operatorname{Min}(\{lc(f) \mid f \in \mathfrak{M}_\mu\}, \preceq_\mu)$. Since $(K, \preceq_\mu)$ is well-founded, the set M is non-void. Every $f \in \mathfrak{M}_\mu$ satisfying $lc(f) \in M$ is a $(\sqsubseteq)$-minimal element of $\mathfrak{M}$. $\square$

(5.3) **Definition:** In $R = K^{(\Gamma)}$ let A be a Gröbner basis of $\mathfrak{A}$. For any $f \in R^\bullet$ and $g \in R$ we say that a ("general") *reduction* relation $f \xrightarrow[A]{} g$ holds, iff there are $m \in \mathbb{N}^\bullet$, $u_i \in K^\bullet, \gamma_i \in \Gamma, a_i \in A$ $(i \in \underline{m})$ and $\gamma \in$ supp(f) such that

(1) $g = f - \sum_{i=1}^{m} u_i X^{\gamma_i} a_i,$

(2) $\gamma_i + le(a_i) = \gamma$ for all $i \in \underline{m}$,

(3) $g_\gamma \prec_\gamma f_\gamma$.

If $\gamma = le(f), lc(f) \in A_\gamma$ and $g_\gamma = 0$, we get as a special case a top-reduction (3.3). In (5.3) we have $g_\gamma \in f_\gamma + A_\gamma$. By the definition of the ordering $\sqsubseteq$ we have also

(5.4)
$$f \xrightarrow[A]{} g \quad \text{implies} \quad f \sqsupset g.$$

Consequently by (5.2) we get

(5.5) **Proposition:** All chains $f \xrightarrow[A]{} f_1 \xrightarrow[A]{} f_2 \xrightarrow[A]{} \cdots$ of general reductions are finite.

Now *suppose* that for every $\alpha \in \Gamma$ we are given also a family $\mathfrak{F}_\alpha$ of K-ideals satisfying

(5.6) For every $u \in K$ and $\mathfrak{a}_\alpha \in \mathfrak{F}_\alpha$ the residue class $u + \mathfrak{a}_\alpha$ contains an element $m(u, \mathfrak{a}_\alpha)$ satisfying $m(u, \mathfrak{a}_\alpha) \prec_\alpha u + a$ for all $a \in \mathfrak{a}_\alpha^\bullet$.

So $m(u, \mathfrak{a}_\alpha)$ is the *least* element $\min(u + \mathfrak{a}_\alpha, \preceq_\alpha)$ of $(u + \mathfrak{a}_\alpha, \preceq_\alpha)$ or equivalently the *unique* element of $\mathrm{Min}(u + \mathfrak{a}_\alpha, \preceq_\alpha)$. We may think of $m(u, \mathfrak{a}_\alpha)$ as the *normal form* of u modulo $\mathfrak{a}_\alpha$. Since $0 \in \mathrm{Min}(K, \preceq_\alpha)$ we have $m(u, \mathfrak{a}_\alpha) = 0$ for $u \in \mathfrak{a}_\alpha$. We may also think that for each $\mathfrak{a}_\alpha$ we are furthermore given a set of (computable) reductions $u \xrightarrow[\mathfrak{a}_\alpha]{} v$ with the two properties that $u \xrightarrow[\mathfrak{a}_\alpha]{} v$ implies $v \in u + \mathfrak{a}_\alpha$ and $v \prec_\alpha u$ and that $m(u, \mathfrak{a}_\alpha)$ is the only $(\xrightarrow[\mathfrak{a}_\alpha]{})$-reduced element of $u + \mathfrak{a}_\alpha$. In this case we have always $u \xrightarrow[\mathfrak{a}_\alpha]{*} m(u, \mathfrak{a}_\alpha)$.

(5.7) **Theorem:** In $R = K^{(\Gamma)}$ let A be a Gröbner basis of an ideal $\mathfrak{A}$, which satisfies $\mathfrak{A}_\alpha \in \mathfrak{F}_\alpha$ for all $\alpha \in \Gamma$. If $f \xrightarrow[A]{*} h$ with an $(\xrightarrow[A]{})$-reduced h, we have $h_\alpha = m(h_\alpha, \mathfrak{A}_\alpha)$ for all $\alpha \in \Gamma$, and furthermore, in the residue class $f + \mathfrak{A}$ the element h is the $(\sqsubseteq)$-least element and also the only $(\xrightarrow[A]{})$-reduced element.

Proof: 1. Consider any $g \in R$. If there is a $\gamma \in \Gamma$ satisfying $g_\gamma \neq m := m(g_\gamma, \mathfrak{A}_\gamma)$, we get $m = g_\gamma + a_\gamma$ with $a_\gamma \in \mathfrak{A}_\gamma^\bullet$ and $m \prec_\gamma g_\gamma$. Consequently by (5.3) we find an element $g' \in R$ satisfying $g \xrightarrow[A]{} g'$.
2. Let h be as stated in the theorem. By part 1, we have $h_\alpha = m(h_\alpha, \mathfrak{A}_\alpha)$ for all $\alpha \in \Gamma$. Consider an element $g \in f + \mathfrak{A}$ with $g \neq h$. The element $a = h - g$ is in $\mathfrak{A}^\bullet$. If $\gamma = le(a)$, we have $h_\alpha = g_\alpha$ for all $\alpha > \gamma$ and $h_\gamma \prec_\gamma g_\gamma$. Consequently $h \sqsubset g$ and furthermore we find an element $g' \in R$ satisfying $g \xrightarrow[A]{} g'$. $\square$

By (5.7) we may think of $h = \min(f + \mathfrak{A}, \sqsubseteq)$ as the *normal form* of f modulo $\mathfrak{A}$. Note also that h does not depend on the choice of the Gröbner basis A of $\mathfrak{A}$.

(5.8) **Examples:** In the following examples (1) – (5) all $\mathfrak{F}_\alpha$ will be identical with the set $\mathfrak{K}$ of all K-ideals, and $\preceq_\alpha = \preceq$ will not depend on α. Condition (5.6) will be satisfied, i.e. for every $u \in K$ and $\mathfrak{a} \in \mathfrak{K}$ the residue class $u + \mathfrak{a}$ has a least element $m(u, \mathfrak{a}) = \min(u + \mathfrak{a}, \preceq)$. In (5.7), we have $\mathfrak{A}_\alpha \in \mathfrak{F}_\alpha = \mathfrak{K}$ trivially. Consequently (5.7) will hold for every R-ideal $\mathfrak{A}$ and every Gröbner basis A of $\mathfrak{A}$.

(1) K is any noetherian domain and $\preceq$ is any well-ordering on K with least element 0.

(2) K is any field and we have $0 \prec u$ for all $u \in K^\bullet$, but no further relation $v \prec u$.

(3) K is a discrete valuation ring with prime element p and the canonical homomorphism $\pi : K \to \overline{K}$, where $\overline{K} = K/Kp$. If $\sigma : \overline{K} \to K$ is a section of π satisfying $\sigma(0) = 0$, we may consider $C := \sigma(\overline{K}) \subset K$ as a system of normal forms modulo Kp. Using the unique representation

$$\sum_{i=0}^{k} c_i\, p^i \quad (c_i \in C,\ 0 \le k \le \infty \ \text{ and } \ c_k \neq 0 \ \text{ for } \ k < \infty)$$

of the elements of $K^\bullet$, put

$$0 \preceq \sum_{i=0}^{k} c_i\, p^i \preceq \sum_{i=0}^{l} c_i p^i \quad \text{if } \ 0 \le k \le l \le \infty \ \text{ and all } \ c_i \ \text{ are in } \ C$$

but do not allow any further relation $u \preceq v$.

(4) K is $\mathbb{Z}$ and $u \prec v$ holds iff in the natural ordering of $\mathbb{Z}$ we have $0 \le u < v$ or $v < 0 \le u$. The normal form of the residue class $v + Ku$ ($u > 0$) is the $r \in \mathbb{Z}$ satisfying $0 \le r < u$ and $v = qu + r$ with some $q \in \mathbb{Z}$. Alternatively we may define $u \prec v$ to hold iff $|u| < |v|$ or ($u > 0$ and $v = -u$). Then the normal form of $v + Ku$ ($u > 0$) is the $r_1 \in \mathbb{Z}$ satisfying $-\frac{u}{2} < r_1 \le \frac{u}{2}$ and $v = q_1 u + r_1$ with some $q_1 \in \mathbb{Z}$.

(5) Call some $(K, \preceq)$ of examples (1) – (4) now $(K_0, \preceq_0)$. Let Γ_0 be a finitely generated torsionfree monoid with a compatible well-ordering $\le_0$. Then let $(K, \preceq)$ be $(K_0^{(\Gamma_0)}, \sqsubseteq_0)$ with $\sqsubseteq_0 = \mathrm{invlex}(\le_0, \preceq_0)$.

(5.9) **Example:** ("Lifting of normal forms", see also [Sh]).
If K and Γ satisfy the conditions of § 3 and § 4, let $\mathfrak{A}$ be an ideal of $R = K^{(\Gamma)}$. For every $\alpha \in \Gamma$, consider the canonical homomorphism $\pi_\alpha : K \to K_\alpha$, where $K_\alpha = K/\mathfrak{A}_\alpha$. If $\sigma_\alpha : K_\alpha \to K$ is a section of π_α satisfying $\sigma_\alpha(0) = 0$, we may consider $C_\alpha := \sigma_\alpha(K_\alpha) \subset K$ as a system of normal forms modulo $\mathfrak{A}_\alpha$. Now put $\mathfrak{F}_\alpha = \{\mathfrak{A}_\alpha\}$ and introduce the relations

$$c_\alpha \prec_\alpha c_\alpha + a_\alpha \quad \text{for} \quad c_\alpha \in C_\alpha, a \in \mathfrak{A}_\alpha^\bullet$$

but do not allow any further relation $u \prec_\alpha v$. Clearly $\preceq_\alpha$ is well-founded and the condition $0 \in \mathrm{Min}(K, \preceq_\alpha)$ holds. Condition (5.6) holds also with $c_\alpha = \min(c_\alpha + \mathfrak{a}_\alpha, \preceq_\alpha)$. Consequently, (5.7) is true and supplies the lifted normal forms $\min(f + \mathfrak{A}, \sqsubseteq)$.

§ 6. An equivariant Gröbner Theory

Let $\Lambda = (\Lambda, +, 0) = \{\lambda, \mu, \ldots\} \neq \{0\}$ be a monoid, which is commutative, cancellative, inversefree (§1), finitely generated and torsionfree (§3). So Λ is wpo in its addition ordering $\preceq_+$, by (1.3). Let $I = \{\iota, \kappa, \ldots\}$ be a set with a well-ordering $\leq_I$, i.e. an ordinal number. We consider the monoid $\Gamma := \Lambda^{(I)}$ of all maps $\gamma : I \to \Lambda, \iota \longmapsto \gamma_\iota$ with finite support $\mathrm{supp}(\gamma) := \{\iota \in I \,|\, \gamma_\iota \neq 0\}$. The addition ordering $\alpha \leq_+ \beta$ of Γ turns out to be the usual product partial ordering, given by $\alpha_\iota \preceq_+ \beta_\iota$ for all $\iota \in I$. Generalising the case $\Lambda = \mathbb{N}, I = \underline{n}$ of §2, we introduce the elements

(6.1) $$\delta^{\iota,\lambda} \in \Gamma \qquad (\iota \in I, \lambda \in \Lambda)$$
by
(6.1.1) $$\delta^{\iota,\lambda}_\iota = \lambda \quad \text{and} \quad \delta^{\iota,\lambda}_\kappa = 0 \ \text{ for } \ \kappa \neq \iota.$$

For fixed $\lambda \neq 0$, the elements (6.1) form an antichain in $(\Gamma, \leq_+)$. So we see that the addition ordering $\leq_+$ is *not* wpo for infinite I. For finite I, using (1.1.4) we easily see that $\Gamma = \Lambda^I$ is wpo in $\leq_+$. *Now suppose* as in §3, that we have chosen a monoid-compatible well-ordering $\preceq$ on Λ. Then the well-ordering $\leq := \mathrm{invlex}(\leq_I, \preceq)$ on Γ is an extension of $\leq_+$. Since there are no infinite strictly descending chains in $(\Gamma, \leq)$, so is what more than ever in $(\Gamma, \leq_+)$. Consequently $(\Gamma, \leq_+)$ is still well-founded even for infinite I.

Now consider the set Σ of all maps
(6.2) $$\sigma : I \longrightarrow I, \quad \iota \longmapsto \sigma\iota$$
which satisfy the condition that
(6.2.1) $$\iota <_I \kappa \quad \text{implies} \quad \sigma\iota <_I \sigma\kappa.$$

Clearly we have $\Sigma = \{id_I\}$ iff I is finite. On $\Gamma = \Lambda^{(I)}$ the relation

(6.3) $$\alpha \leq_e \beta \quad :\Longleftrightarrow \quad \exists\, \sigma \in \Sigma : \alpha \leq_+ \beta \circ \sigma \ \ (\text{i.e. } \alpha_\iota \preceq_+ \beta_{\sigma\iota} \text{ for all } \iota \in I)$$

is a partial ordering, called the *embedding ordering* (or Higman ordering) of $\Lambda = \Gamma^{(I)}$ with respect to Σ (cf. [Mi] or [Ro], Chap. 10, §4). Since $id_I \in \Sigma$, the ordering $\leq_e$ extends $\leq_+$, with equality iff I is finite. We have to use now the notion of a *better-partial-ordering* (bpo), which is weaker than well-ordering and stronger than wpo (loc. cit.). But $(\Lambda, \preceq_+)$ turns out to be even bpo, since by the proof of (1.3) it is an epimorphic image of some $(\mathbb{N}^l, \leq_+)$ and the latter set is even bpo. Consequently (loc. cit.), $(\Gamma, \leq_e)$ is bpo and thus more than ever wpo.

Now consider a domain K and the ring $R = K^{(\Gamma)} = K[X]$ of §2. Then we may take over (2.3) – (2.7), recalling that we have chosen here $\leq$ to be $\mathrm{invlex}(\leq_I, \preceq)$. Using (6.1) we put

(6.4) $$X^\lambda_\iota := X^{\delta^{\iota,\lambda}} \qquad (\iota \in I, \lambda \in \Lambda).$$

So we have $X_\iota^0 = X^0 = 1$ and $X_\iota^\lambda \cdot X_\iota^\mu = X_\iota^{\lambda+\mu}$. For any $\gamma \in \Gamma$, we get a representation of X^γ as "power product"

(6.5) $$X^\gamma = \prod_{\iota\in I} X_\iota^{\gamma_\iota} \qquad , \ \gamma = (\gamma_\iota)_{\iota\in I}.$$

So if $\Lambda = \mathbb{N}$, the ring R is the polynomial ring $K[(X_\iota)_{\iota\in I}]$ in the indeterminates $X_\iota (\iota \in I)$.

Now we introduce an operation

(6.6) $$\Sigma \times R \longrightarrow R, \ (\sigma, f) \longmapsto \sigma f$$

by

(6.6.1) $$\sigma\left(\prod_{\iota\in I} X_\iota^{\gamma_\iota}\right) = \prod_{\iota\in I} X_{\sigma\iota}^{\gamma_\iota}$$

and K-linearity. For fixed σ we get a monomorphism $f \longmapsto \sigma f$ of the K-algebra R into itself. Writing

$$X^\beta = \prod_{\iota\in I} X_{\sigma\iota}^{\beta_{\sigma\iota}} \cdot \prod_{\iota\notin\sigma(I)} X_\iota^{\beta_\iota}$$

we see that (6.3) means

(6.7) $$\alpha \le_e \beta \quad \Longleftrightarrow \quad \exists\, \sigma \in \Sigma : \sigma(X^\alpha) \,|\, X^\beta.$$

It is convenient to define also the operation

(6.8) $$\Sigma \times \Gamma \longrightarrow \Gamma, \ (\sigma, \gamma) \longmapsto \sigma\gamma \qquad , \text{by } X^{\sigma\gamma} := \sigma(X^\gamma).$$

Then we have

(6.9) $$\alpha \le_+ \beta \circ \sigma \quad \Longleftrightarrow \quad \sigma\alpha \le_+ \beta.$$

We also see that

(6.10) $$\alpha \le_+ \beta \Longrightarrow \sigma\alpha \le_+ \sigma\beta \quad \text{and} \quad \alpha \le \beta \Longrightarrow \sigma\alpha \le \sigma\beta.$$

We have

(6.11) $$\sigma\left(\sum_{\gamma\in\Gamma} f_\gamma X^\gamma\right) = \sum_{\gamma\in\Gamma} f_\gamma X^{\sigma\gamma}$$

and so we see that for $f \neq 0$

(6.12) $$le(\sigma f) = \sigma(le f),$$

(6.13) $$lc(\sigma f) = lc(f)\ .$$

Consequently we have for $f, g \in R^\bullet$

(6.14) $$le(f \cdot \sigma g) = le(f) + \sigma(le(g)).$$

An R-ideal $\mathfrak{A}$ is called *equivariant (ev)*, if $\sigma a \in \mathfrak{A}$ for all $a \in \mathfrak{A}$ and all $\sigma \in \Sigma$. So for any given $A \subseteq R^\bullet$ we may define the *ev ideal* $\mathfrak{A}$ *generated by* A to be the set of all elements of the form

$$a = \sum_{i=1}^{m} \sum_{j=1}^{n_i} f_{ij} \cdot \sigma_{ij} a_i \qquad (f_{ij} \in R, \sigma_{ij} \in \Sigma, a_i \in A). \tag{6.15}$$

We call A also an *ev basis* of $\mathfrak{A}$. Again let $\{0\}$ be the ev ideal generated by the void set. If $\nu = \min(I, \leq_I)$, the element X_ν generates the ev ideal

$$\mathfrak{M} = \sum_{\iota \in I} R \cdot X_\iota. \tag{6.16}$$

If I is infinite, $\mathfrak{M}$ has no finite basis as an R-ideal, so R is not noetherian. For $a \neq 0$, we call (6.15) a *standard representation of a by A*, if

$$f_{ij} \neq 0 \quad \text{and} \quad le(f_{ij}\sigma_{ij}a_i) \leq le(a) \qquad \text{for all } i, j. \tag{6.17}$$

We proceed now to carry over the results of §3 – §5 (without the considerations about computability) to equivariant ideals. Because of (6.13) we may translate (3.3) to the definition of an ev top-reduction simply by replacing the a_i by $\sigma_i a_i (i \in \underline{m})$. So for each $i \in \underline{m}$ we take just one $\sigma_i \in \Sigma$. In (3.4) and (3.5) we just replace $\leq_+$ and $<_+$ by $\leq_e$ and $<_e$. Then in view of (6.7) and (6.13), implication (3.6) and proposition (3.8) continue to hold. Here (3.7) is not changed, and in the proof of (3.8) we have to replace $\leq_+$ by $\leq_e$, which is wpo. Further, (3.9) may be carried over without change to the definition of an ev Gröbner basis, and then (3.10) holds for all ev ideals of R. In the proof of (3.10) we replace again $\leq_+$ by $\leq_e$.

To translate §4 and §5, *we suppose now K to be noetherian*. Given (4.1), we leave (4.2) unchanged, but for $F = (f_1, \ldots, f_m) \in R^m$ with some $f_i \neq 0$ and for a vector $\vec{\sigma} = (\sigma_1, \ldots, \sigma_m) \in \Sigma^m$, we replace (4.3) – (4.5) respectively by

$$F \cdot \vec{\sigma} \cdot A = f_1\sigma_1 a_1 + \cdots + f_m \sigma_m a_m \,,$$

$$le(F, \vec{\sigma}, A) = \max\left(\{le(f_i) + \sigma_i\alpha_i \,|\, i \in \underline{m}, f_i \neq 0\}, \leq\right) \,,$$

$$M(F, \vec{\sigma}, A) = \{i \in \underline{m} \,|\, f_i \neq 0, le(f_i) + \sigma_i\alpha_i = le(F, \vec{\sigma}, A)\} \,.$$

With these replacements we get (4.6). After that, (4.7) – (4.9) remain unchanged, and in (4.10) replace $\leq_+$ by $\leq_e$. If $\varepsilon \in \Gamma_M$, for each $i \in M$ we get elements $\beta_{M,i,\varepsilon} \in \Gamma$ and $\sigma_{M,i,\varepsilon} \in \Sigma$ satisfying $\beta_{M,i,\varepsilon} + \sigma_{M,i,\varepsilon}\alpha_i = \varepsilon$. Then in (4.11) we have to replace the part $X^{\varepsilon - \alpha_i} a_i$ by $X^{\beta_{M,i,\varepsilon}} \cdot \sigma_{M,i,\varepsilon} a_i$. After that, (4.12) and the Buchberger algorithm carry over with the obvious changes. We may also translate §5, forgetting that we had used the sign $\preceq$ also for orderings of the building part Λ of $\Gamma = \Lambda^{(I)}$.

For another form of an equivariant Gröbner theory see [Co].

§ 7. A Gröbner Theory for Modules

Let $\Lambda = (\Lambda, +, 0) = \{\lambda, \mu, \ldots\}$ be a monoid, which is commutative, cancellative, inverse-free (§1), finitely generated and torsionfree (§3). So Λ is wpo in its addition ordering $\leq_+$, by (1.3). Then consider a Λ-*set* $\Gamma = \{\alpha, \beta, \gamma, \ldots\}$, i.e. a non-void set Γ together with a map

(7.1) $$\Lambda \times \Gamma \longrightarrow \Gamma, \quad (\lambda, \gamma) \longmapsto \lambda + \gamma$$

satisfying $0 + \gamma = \gamma$ and $\lambda + (\mu + \gamma) = (\lambda + \mu) + \gamma$ for all $\lambda, \mu \in \Lambda$ and $\gamma \in \Gamma$. *We suppose also*, that both cancellation laws

(7.2.1) $$\lambda + \gamma = \lambda' + \gamma \quad \Longrightarrow \quad \lambda = \lambda'$$

and

(7.2.2) $$\lambda + \gamma = \lambda + \gamma' \quad \Longrightarrow \quad \gamma = \gamma'$$

are satisfied. So the maps

(7.3.1) $$\Lambda \longrightarrow \Gamma, \quad \lambda \longmapsto \lambda + \gamma \qquad (\gamma \in \Gamma)$$

and

(7.3.2) $$\Gamma \longrightarrow \Gamma, \quad \gamma \longmapsto \lambda + \gamma \qquad (\lambda \in \Lambda)$$

are injective, and if $\lambda + \alpha = \beta$ we may write $\lambda = \beta - \alpha$ and $\alpha = \beta - \lambda$. The relation on Γ

(7.4) $$\alpha \leq_+ \beta \quad :\Longleftrightarrow \quad \exists\, \lambda \in \Lambda : \lambda + \alpha = \beta$$

turns out to be a partial ordering and satisfies the relations

(7.5.1) $$\lambda \leq_+ \mu \quad \Longleftrightarrow \quad \lambda + \gamma \leq_+ \mu + \gamma$$

(7.5.2) $$\alpha \leq_+ \beta \quad \Longleftrightarrow \quad \lambda + \alpha \leq_+ \lambda + \beta.$$

Now let K be a *noetherian domain* and consider the ring $Q = K^{(\Lambda)} = \{q, p, \ldots\}$. We introduce X as a bijection $\lambda \mapsto X^\lambda$ of Λ onto some set (cf. §2), and so we may write

(7.7) $$q = \sum_{\lambda \in \Lambda} q_\lambda X^\lambda \qquad \text{for } q = (q_\lambda)_{\lambda \in \Lambda} \in K^{(\Lambda)}$$

and $Q = K[X]$. By (3.10) the ring Q is *noetherian*. Now let $R = \{f, g, \ldots\}$ be a *finitely generated unitary Q-module*; so we are given an operation

(7.8) $$Q \times R \longrightarrow R, \quad (q, f) \longmapsto q \cdot f$$

with the usual distributive and associative laws and $1 \cdot f = f$. As is well known, the Q-module R is noetherian too. Using the Λ-set Γ, we suppose that we are given a decomposition

(7.9) $$R = \sum_{\gamma \in \Gamma} R_\gamma$$

into a direct sum of K-modules such that the condition

$$X^\lambda \cdot R_\gamma \subseteq R_{\lambda+\gamma} \qquad \text{for all } \lambda \in \Lambda \text{ and } \gamma \in \Gamma \tag{7.10}$$

is satisfied. In particular every $f \in R$ has a unique representation $f = \sum_{\gamma\in\Gamma} f_\gamma$ with $f_\gamma \in R_\gamma$ and finite support $\mathrm{supp}(f) = \{\gamma \in \Gamma \mid f_\gamma \neq 0\}$. Here f_γ is called the *homogeneous component of degree γ of f*. An element of R is *homogeneous*, if it lies in some R_γ.

We proceed now to carry over the results of §3 and §4 (without the considerations about computability) to modules. Therefore suppose $R \neq \{0\}$ and let

$$\{r_1, \ldots, r_n\} \qquad (r_i \in R^\bullet) \tag{7.11}$$

be a finite system of generators of the Q-module R. Surely we may suppose that every r_i is homogeneous, say of degree γ_i. The K-module R_γ is generated by the elements $X^{\lambda_i} r_i$ with $i \in \underline{n}$ and $\lambda_i + \gamma_i = \gamma$. In particular we have $R_\gamma = \{0\}$, if γ is not in some $\Lambda + \gamma_i$. So we may suppose that Γ is the union of its Λ-subsets $\Lambda + \gamma_i$ $(i \in \underline{n})$.

Let i, j, k be three different numbers of $\underline{n}$ such that $\lambda_i + \gamma_i = \lambda_j + \gamma_j$ for some $\lambda_i, \lambda_j \in \Lambda$ and that $\mu_j + \gamma_j = \mu_k + \gamma_k$ for some $\mu_j, \mu_k \in \Lambda$. Then we get

$$(\mu_j + \lambda_i) + \gamma_i = (\mu_j + \lambda_j) + \gamma_j = (\lambda_j + \mu_k) + \gamma_k\,.$$

So we see that there is a partition $(N_c)_{c\in\underline{d}}$ of $\underline{n}$ with the two properties that at first the Λ-subsets

$$\Gamma_c := \bigcup\{\Lambda + \gamma_i \mid i \in N_c\} \qquad (c \in \underline{d}) \tag{7.12}$$

form a partition

$$\Gamma = \Gamma_1 \cup \ldots \cup \Gamma_d \tag{7.13}$$

of Γ and that secondly for every $c \in \underline{d}$ there are elements $\beta_c \in \Gamma$ and $\lambda_i \in \Lambda$ $(i \in N_c)$ satisfying

$$\beta_c = \lambda_i + \gamma_i \quad \text{for all } i \in N_c. \tag{7.14}$$

So corresponding to (7.13) the Q-module R decomposes into a direct sum of Q-modules

$$R = \sum_{c\in\underline{d}} R^{(c)} \quad , \quad R^{(c)} = \sum_{\gamma\in\Gamma_c} R_\gamma. \tag{7.15}$$

Furthermore for $\mu_c := \sum_{i\in N_c} \lambda_i$ we get from (7.12) and (7.14) the inclusion

$$\mu_c + \Gamma_c \subseteq \Lambda + \beta_c. \tag{7.16}$$

Consequently for fixed c every $\gamma \in \Gamma_c$ is associated to a unique $\lambda \in \Lambda$ satisfying $\mu_c + \gamma = \lambda + \beta_c$. So we get monomorphisms of Λ-sets

$$(7.17) \qquad \varphi_c : \Gamma_c \longrightarrow \Lambda, \quad \gamma \longmapsto (\mu_c + \gamma) - \beta_c \qquad (c \in \underline{d}).$$

Now suppose (cf. §3), that we have chosen a monoid-compatible well-ordering $\le$ on Λ, which will be kept fixed further on. Then we get well-orderings $\le_c$ on the Λ-sets Γ_c by $\alpha \le_c \beta :\Leftrightarrow \varphi_c(\alpha) \le \varphi_c(\beta)$. The orderings $\le_c$ are $(\Lambda, \le)$-compatible in the sense that $\lambda \le \mu$ implies $\lambda + \gamma \le_c \mu + \gamma$ for all $\gamma \in \Gamma_c$ and that $\alpha \le_c \beta$ implies $\lambda + \alpha \le_c \lambda + \beta$ for all $\lambda \in \Lambda$.
There are two simple ways to continue these $\le_c$ to a $(\Lambda, \le)$-compatible well-ordering $\le$ of Γ: For $\alpha \in \Gamma_a$ and $\beta \in \Gamma_b$ $(a, b \in \underline{d})$ we may define $\alpha \le \beta$ by

$$(7.18.1) \qquad a < b \quad \text{or} \quad (a = b \text{ and } \alpha \le_a \beta)$$

or by

$$(7.18.2) \qquad \varphi_a(\alpha) < \varphi_b(\beta) \quad \text{or} \quad (\varphi_a(\alpha) = \varphi_b(\beta) \text{ and } a \le b).$$

In the following let $\le$ be any $(\Lambda, \le)$-compatible well-ordering of Γ, which will be kept fixed. Surely the addition ordering $\le_+$ of Γ is $(\Lambda, \le_+)$-compatible. Note that elements of different subsets Γ_c and Γ_b are incomparable in $(\Gamma, \le_+)$.

For special cases of our data $(\Lambda, \le), (\Gamma, \le), Q, R$ see [MM] and [R].

Now for (7.9) and $(\Gamma, \le)$ we first take over (2.3) and we get (2.5). Instead of (2.4), we introduce the *leading term*

$$(7.19) \qquad lt(f) := f_{(le(f))} \in R_{le(f)} \quad (f \in R^\bullet)$$

For convenience we define also for Q the notion of a leading term by

$$(7.20) \qquad lt(q) = lc(q) \cdot X^{le(q)} \quad (q \in Q^\bullet).$$

We do not suppose the Q-module R to be torsionfree, so $q \cdot f = 0$ may happen for some $q \in Q^\bullet$ and $f \in R^\bullet$. If $q \cdot f \neq 0$ we may have $lt(q) \cdot lt(f) = 0$, and so instead of (2.6) we get only

$$(7.21) \qquad le(q \cdot f) \le le(q) + le(f).$$

In the following we will use at several places the fact that the Q-module R is noetherian. So we skip translating (3.10) and we suppose that we are given a list (4.1), whose elements $a_1, \ldots, a_m$ generate a Q-submodule $\mathfrak{A}$ of R. Surely the a_i may be inhomogeneous.

Every $a \in \mathfrak{A}^\bullet$ has a representation

$$(7.22) \qquad a = \sum_{i \in M} q_i a_i \quad (M \subseteq \underline{m}, q_i \in Q^\bullet),$$

which is called *standard*, if

$$(7.23) \qquad le(q_i) + le(a_i) \leq le(a) \quad \text{for all } i \in M.$$

We introduce now the abbreviations

$$(7.24) \qquad \alpha_i := le(a_i) \in \Gamma \text{ (as in (4.2))} \quad \text{and} \quad v_i := lt(a_i) \in R_{\alpha_i} \quad (i \in \underline{m}).$$

Recalling (7.13) and (7.15), we put

$$(7.25) \qquad \underline{m}_c = \{i \in \underline{m} \mid \alpha_i \in \Gamma_c\} \quad (c \in \underline{d})$$

and

$$(7.26) \qquad \mathfrak{M} = \{M \subseteq \underline{m} \mid M \neq \emptyset \text{ and } M \subseteq \underline{m}_c \text{ for some } c \in \underline{d}\}.$$

Then we change definition (3.3) by writing

(7.27) $f \underset{A}{\longrightarrow} g$ iff there are $M \in \mathfrak{M}, u_i \in K^\bullet, \lambda_i \in \Lambda$ $(i \in M)$ such that

(1) $g = f - \sum_{i \in M} u_i X^{\lambda_i} a_i$

(2) $u_i X^{\lambda_i} a_i \neq 0$ and $\lambda_i + \alpha_i = le(f)$ for all $i \in M$

(3) $lt(f) = \sum_{i \in M} u_i X^{\lambda_i} v_i$.

Clearly $f \underset{A}{\longrightarrow} g$ implies $g \in f + \mathfrak{A}$ and $le(g) < le(f)$, and so all $(\underset{A}{\longrightarrow})$-chains are finite. As a substitute of (3.4) we define $\tilde{A}$ (resp. $\tilde{\mathfrak{A}}$) to be the Q-module generated in R by all $lt(a)$ with $a \in A$ (resp. $a \in \mathfrak{A}^\bullet$). Since $\tilde{A}$ and $\tilde{\mathfrak{A}}$ are generated by homogeneous elements, we have

$$(7.28.1) \qquad \tilde{A} = \sum_{\gamma \in \Gamma} A_\gamma \quad \text{with} \quad A_\gamma := \tilde{A} \cap R_\gamma$$

and

$$(7.28.2) \qquad \tilde{\mathfrak{A}} = \sum_{\gamma \in \Gamma} \mathfrak{A}_\gamma \quad \text{with} \quad \mathfrak{A}_\gamma := \tilde{\mathfrak{A}} \cap R_\gamma.$$

Then proposition (3.8) carries over with (5) deleted. If (1) – (4) are fulfilled, A is called a *Gröbner basis* of $\mathfrak{A}$. Now (4.3) – (4.5) carry over with $F = (f_1, \ldots, f_m)$ replaced by $\vec{q} = (q_1, \ldots, q_m) \in Q^m$ with some $q_i \neq 0$. Instead of (4.6) we get

$$(7.29) \qquad le(\vec{q}, A) > le(\vec{q} \cdot A) \quad \text{iff} \quad \sum_{i \in M(\vec{q}, A)} lt(q_i) \cdot v_i = 0 \text{ (and } |M(\vec{q}, A)| \geq 1)$$

In order to translate (4.7) – (4.9), for every $M \in \mathfrak{M}$ we define $\mathfrak{H}_M$ to be the *set* of all vectors

$$(7.30) \qquad u := (u_i X^{\lambda_i})_{i \in \underline{m}} \quad (u_i \in K, \lambda_i \in \Lambda, \quad u_i = 0 \text{ iff } i \notin M),$$

which are "homogeneous" in the sense that

$$\lambda_i + \alpha_i = \beta_u \quad \text{for some } \beta_u \in \Gamma \text{ and all } i \in M, \tag{7.31}$$

and which satisfy

$$\sum_{i \in M} u_i X^{\lambda_i} v_i = 0. \tag{7.32}$$

Since the Q-module Q^m is noetherian, for the $N \in \mathfrak{M}$ with $N \subseteq M$ we get (by induction) still numbers $t_N \in \mathbb{N}$ and vectors

$$u_N^{(k)} := (u_{N,i} X^{\lambda_{N,i}^{(k)}})_{i \in \underline{m}} \in \mathfrak{H}_N \quad (k = 1, \ldots, t_N) \tag{7.33}$$

such that the Q-submodule of Q^m generated by $\bigcup\{\mathfrak{H}_N \,|\, N \subseteq M\}$ is already generated by the elements $u_N^{(k)}$ ($N \subseteq M, k = 1, \ldots, t_N$). We denote this submodule by $\mathfrak{S}_M$. After that, if $t_M > 0$ we replace (4.10) by

$$\Gamma_M := \mathrm{Min}\Big(\{\gamma \in \Gamma \,|\, \lambda_{M,i}^{(k)} + \alpha_i \leq_+ \gamma \text{ for } k = 1, \ldots, t_M \text{ and all } i \in M\}, \leq_+\Big) \tag{7.34}$$

Then we may define the "*S-polynomials for A*" by formula (4.11), replacing only $M \subseteq \underline{m}$ by $M \in \mathfrak{M}$. Note that $\varepsilon - \alpha_i \in \Lambda$ and $(\varepsilon - \alpha_i) + \alpha_i = \varepsilon$. But now, theorem (4.12) is easily translated including its proof. After that, we may translate also the *Buchberger algorithm* from the end of §4: Suppose that we meet some (M, ε, k) and some $(\underset{A^{(0)}}{\longrightarrow})$-reduced $a_{m+1} \neq 0$. Then for $A^{(1)} := (a_1, \ldots, a_m, a_{m+1})$ we get the strict inclusion $\tilde{A}^{(0)} \subset \tilde{A}^{(1)}$ of Q-submodules of the Q-module R. Since R is noetherian, the Buchberger algorithm terminates.

Remark: By the proof of (1.3), for some $l \in \mathbb{N}$ there is an epimorphism $\varphi : \mathbb{N}^l \to \Lambda$. So if $P = K[T]$ is the polynomial ring in l indeterminates $T_1, \ldots, T_l$ over K, there is a unique K-algebra-epimorphism

$$\Phi : P \to Q = K[X] \quad \text{with} \quad \Phi(T^\nu) = X^{\varphi(\nu)} \text{ for all } \nu \in \mathbb{N}^l. \tag{7.35}$$

Since the Q-module R was not supposed to be torsionfree, in the Gröbner theory of R we may now replace Q by the graded polynomial ring

$$P = \sum_{\lambda \in \Lambda} \left(\sum_{\varphi(\nu) = \lambda} K \cdot T^\nu \right). \tag{7.36}$$

In the other direction we may allow for K any epimorphic image of a noetherian domain L by using the extended epimorphism from $L[X]$ onto $Q = K[X]$.

§ 8. A lexicographical ordering with a partially ordered index set

As in §1 let $(\Gamma, \leq)$ now be a *partially ordered set.* Let $(K, \preceq)$ be a partially ordered set with a least element $0 = \min(K, \preceq)$. As in §2 we define $R = K^{(\Gamma)}$ to be the set of all maps $f : \Gamma \to K,\ \alpha \mapsto f_\alpha$ with finite support $\mathrm{supp}(f) := \{\alpha \in \Gamma \mid f_\alpha \neq 0\}$. For f and g in R we put $\Delta(f, g) = \{\alpha \in \Gamma \mid f_\alpha \neq g_\alpha\}$. This set is void iff $f = g$. Note also that $\Delta(f, 0) = \mathrm{supp}(f)$. Following [CHH], we generalise (5.1) by defining

$$(8.1) \qquad f \sqsubset g \quad \text{iff} \quad f \neq g \text{ and } f_\gamma \prec g_\gamma \text{ for all } \gamma \in \mathrm{Max}(\Delta(f, g), \leq).$$

(8.2) **Proposition:** The relation $f \sqsubseteq g$ is a partial ordering on R.

Proof. Suppose $f \sqsubset g$ and $g \sqsubset h$, and put $A = \Delta(f, g)$ $B = \Delta(g, h)$, $C = \Delta(f, h)$. If $f_\alpha \neq h_\alpha$, we have $f_\alpha \neq g_\alpha$ or $g_\alpha \neq h_\alpha$, so we get $C \subseteq A \cup B$. Consider an element $\gamma \in \mathrm{Max}C$. Then choose an element $\lambda \in \mathrm{Max}(A \cup B)$ satisfying $\lambda \geq \gamma$. Suppose first that $\lambda \in A$. In this case we have even $\lambda \in \mathrm{Max}A$ and consequently $f_\lambda \prec_\lambda g_\lambda$. Furthermore we have $\lambda \in \mathrm{Max}B$ or $\lambda \notin B$ and consequently $g_\lambda \preceq h_\lambda$. So we have $f_\lambda \prec g_\lambda$ and thus $\lambda \in C$ and thus finally $\lambda = \gamma$. So we have $f_\gamma \prec h_\gamma$. This relation can be derived in the same manner also in the second case $\gamma \in B$. So we get $f \sqsubset h$. We cannot have both $f \sqsubset g$ and $g \sqsubset f$, because this would imply $f \sqsubset f$, a contradiction to our definition (8.1). $\square$

We write $\sqsubseteq = \mathrm{invlex}(\leq, \preceq)$ and call it the *inverse lexicographical ordering belonging to the partial orderings $\leq$ and $\preceq$.*

(8.3) **Proposition:** If $\leq$ and $\preceq$ are well-founded, so is $\sqsubseteq$.

Proof. By [PR] a partial ordering is well-founded, iff it has a well-ordered extension. So let $\leq^*$ (resp. $\preceq^*$) be a well-ordered extension of $\leq$ (resp. $\preceq$). Then $\sqsubseteq^* = \mathrm{invlex}(\leq, \preceq^*)$ is a well-ordered extension of $\sqsubseteq$, and so $\sqsubseteq$ is well-founded. $\square$

(8.4) **Theorem:** If $\leq$ and $\preceq$ are wpo, so is $\sqsubseteq$.

Proof. Suppose $\leq$ and $\preceq$ wpo, but $\sqsubseteq$ not wpo. So there are sequences $f_i = (f_{i\alpha})_{\alpha \in \Gamma}$ $(i \in \mathbb{N})$ in R, which are *bad,* i.e. for no $j < k$ we have $f_j \sqsubseteq f_k$ (cf. (1.1.3)). On the set $\mathbb{N}^{\mathbb{N}}$ of all maps from $\mathbb{N}$ to $\mathbb{N}$, the lexicographical ordering $\sqsubseteq'$ belonging to the natural well-ordering of $\mathbb{N}$ is also a well-ordering. Writing $F_i = \mathrm{supp}(f_i)$ and denoting by $|F_i|$ the number of elements of $F_i \subset \Gamma$, we may associate to $(f_i)_{i \in \mathbb{N}}$ the element $(|F_i|)_{i \in \mathbb{N}}$ of $\mathbb{N}^{\mathbb{N}}$. Now from the set $\mathfrak{S}$ of bad sequences in R, take a sequence $(g_i)_{i \in \mathbb{N}}$ with $(\sqsubseteq')$-minimal $(|G_i|)_{i \in \mathbb{N}}$. Since $g_i \not\sqsubseteq g_{i+1}$, we have $G_i \neq \emptyset$. So for every $i \in \mathbb{N}$, we may choose an element $\gamma_i \in \mathrm{Max}(G_i, \leq)$. Since $(\Gamma, \leq)$ is wpo, by (1.1.4) there exists an infinite set $A \subseteq \mathbb{N}$ such that $\gamma_j \leq \gamma_k$ for all $j < k$ in A. Since $(K, \preceq)$ is wpo, there exists an infinite subset $B \subseteq A$ such that $g_{j\gamma_j} \preceq g_{k\gamma_k}$ for all $j < k$ in B. Now put $m = \min B$ and let φ be the monotone bijection from $\mathbb{N}$ onto $\{0, \ldots, m-1\} \cup B$. So we have $\varphi(i) = i$ for

$i \leq m$. Then define a sequence $h_i \in R$ ($i \in \mathbb{N}$) by

$$(1) \quad \begin{cases} h_i = g_{\varphi(i)} \text{ for } i \neq m\,, \\ h_{m\alpha} = g_{m\alpha} \text{ for } \alpha \neq \gamma_m\,, \qquad h_{m\gamma_m} = 0\,. \end{cases}$$

So we have $|H_i| = |G_i|$ for $i < m$ and $|H_m| = |G_m| - 1$. We shall prove that $(h_i)_{i\in\mathbb{N}}$ is bad, and so we get a contradiction to $(|G_i|)_{i\in\mathbb{N}}$ being $(\sqsubseteq')$-minimal. First consider a number $j < m$. Since $h_j \not\sqsubseteq g_m$ there is an element $\delta \in \mathrm{Max}(\Delta(h_j, g_m))$ such that $h_{j\delta} \not\preceq g_{m\delta}$ and therefore $h_{j\delta} \neq 0$. If $\delta = \gamma_m$, we get $h_{j\delta} \not\preceq 0 = h_{m\delta}$. If $\delta \neq \gamma_m$, we get $h_{j\delta} \not\preceq g_{m\delta} = h_{m\delta}$. So in both cases we have $h_j \not\sqsubseteq h_m$. Now consider a number $j > m$. Since $g_m \not\sqsubseteq g_{\varphi(j)} = h_j$, there is an element $\delta \in \mathrm{Max}(\Delta(g_m, h_j))$ such that $g_{m\delta} \not\preceq h_{j\delta}$. Suppose first that $\gamma_m < \gamma_{\varphi(j)}$. Then $\gamma_m \notin \mathrm{Max}(\Delta(g_m, h_j))$, so we have $\delta \neq \gamma_m$ and therefore $h_{m\delta} = g_{m\delta}$ and $h_m \not\sqsubseteq h_j$. Suppose now $\gamma_m = \gamma_{\varphi(j)}$. Then we get again an element $\delta \in \mathrm{Max}(\Delta(g_m, h_j))$ with $g_{m\delta} \not\preceq h_{j\delta}$, but now we have always $\delta \neq \gamma_m$ since $g_{m\gamma_m} \preceq h_{j\gamma_m} = g_{\varphi(j)\gamma_{\varphi(j)}}$. So in this second case, we have also $h_m \not\sqsubseteq h_j$. So $(h_i)_{i\in\mathbb{N}}$ is bad, as required. $\square$

Now let $(K^\bullet_\alpha)_{\alpha\in\Gamma}$ be a partition of $K^\bullet = K\backslash\{0\}$, with Γ as indexing set. Put $K_\alpha = K^\bullet_\alpha \cup \{0\}$ and

$$(8.5) \qquad \sum_{\alpha\in\Gamma} K_\alpha := \{f = (f_\alpha)_{\alpha\in\Gamma} \in K^{(\Gamma)} \mid f_\alpha \in K_\alpha \text{ for all } \alpha \in \Gamma\}.$$

Call $\preceq_\alpha$ the restriction of $\preceq$ to K_α. Then define $\mathrm{invlex}(\leq, (\preceq_\alpha)_{\alpha\in\Gamma})$ to be the restriction of $\sqsubseteq = \mathrm{invlex}(\leq, \preceq)$ to $\sum_{\alpha\in\Gamma} K_\alpha$. Clearly this restriction is also wpo. In $\sum_{\alpha\in\Gamma} K_\alpha$ the disjointness of the $K^\bullet_\alpha$ does not matter. So from (8.4) we get

(8.6) **Theorem:** Let $(\Gamma, \leq)$ be a wpo set. For each $\alpha \in \Gamma$ let $(K_\alpha, \preceq_\alpha)$ be a wpo set with a least element $0_\alpha = \min(K_\alpha, \preceq_\alpha)$. Then the set

$$\sum_{\alpha\in\Gamma} K_\alpha := \{f = (f_\alpha)_{\alpha\in\Gamma} \mid f_\alpha \in K_\alpha\,, \mathrm{supp}(f) \text{ finite}\}$$

is wpo in its inverse lexicographical ordering $\sqsubseteq = \mathrm{invlex}(\leq, (\preceq_\alpha)_{\alpha\in\Gamma})$.

References

[ABL] W.W. Adams, A. Boyle, P. Loustaunau: Transitivity for Weak and Strong Gröbner Bases. J. Symb. Comp. **15** (1993), 49–65.

[Be] M. Beeson: Foundations of Constructive Mathematics. Springer 1985.

[Bu] B. Buchberger: Gröbner Bases: An Algorithmic Method in Polynomial Ideal Theory. In N.K. Bose (ed.) Multidimensional Systems Theory, 184–232. Reidel 1985.

[Bu2] B. Buchberger: A note on the Complexity of Constructing Gröbner Bases. In H. van Hulzen (ed.) Proc. Eurocal '83, Lecture Notes in Computer Science **162**, 137–145. Springer 1983.

[BW] Th. Becker, V. Weispfenning: Gröbner Bases, a Computational Approach to Commutative Algebra. Springer 1993.

[Co] D.E. Cohen: Closure Relations, Buchberger's Algorithm, and Polynomials in infinitely many Variables. In E. Boerger (ed.): Computation Theory and Logic, Lecture Notes in Computer Science **270**, 78–87. Springer 1987.

[CHH] P. Conrad, J. Harvey, C. Holland: The Hahn Embedding Theorem for Abelian Lattice-ordered Groups. Trans. Am. Math. Soc. **108** (1963), 143–169.

[DS] A.W.M. Dress, G. Schiffels: Noetherian Quasi Orders and Canonical Ideal Bases. Preprint, Bielefeld 1987.

[DST] J. Davenport, Y. Siret, E. Tournier: Calcul formel, systèmes et algorithmes de manipulations algébriques. Masson 1987. (English: Computer Algebra, . . . Acad. Press 1988).

[FE] L. Fuchs: On the extension of the partial order of groups. Amer. J. Math. **72** (1950), 191–194, addendum by C.J. Everett, p. 216.

[Kr] J.B. Kruskal: The Theory of Well-Quasi-Ordering: A Frequently Discovered Concept. J. Comb. Th. (A), **13** (1972), 297–305.

[MA] B.W. Char et al.: Maple V Library Reference Manual. Springer 1991.

[Mi] E.C. Milner: Basic WQO- and BQO-Theory. In I. Rival (ed.) Graphs and Orders. Reidel 1985.

[Mö] H.M. Möller: On the Constructing of Gröbner Bases Using Syzygies. J. Symb. Comp. **6** (1988), 345–359.

[MM] H.M. Möller, T. Mora: New Constructive Methods in Classical Ideal Theory. J. Algebra **100** (1986), 138–178.

[PR] M. Pouzet, I. Rival: Which Ordered Sets have a Complete Linear Extension? Can. J. Math. **33** (1981), 1245–1254.

[Re] L. Rédei: The Theory of Finitely Generated Commutative Semigroups. Pergamon Press 1965.

[Ri] P. Ribenboim: Extension of Hironaka's standard basis theorem for generalised power series. Arch. Math. **60** (1993), 436–439.

[Ro] J.G. Rosenstein: Linear Orderings. Acad. Press (1982).

[Ru] E.W. Rutman: Gröbner Bases and Primary Decomposition of Modules. J. Symb. Comp. **14** (1992), 483–503.

[Sh] R. Shtokhamer: Lifting canonical algorithms from a ring R to the ring $R[X]$. J. Sym. Comp. **6** (1988), 169–179.

[Sz] E. Szpilrajn: Sur l'extension de l'ordre partiel. Fund. Math. **16** (1930), 386–389.

[Za] G. Zacharias: Generalized Gröbner Bases in Commutative Polynomial Rings, Ba. Thesis at M.I.T., Dep. Comp. Sci., 1978.