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
$\operatorname{Min}(M, \leq) := \{\alpha \in M \mid \text{there is no } \beta \in M \text{ s.t. } \beta < \alpha\}$
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 $\operatorname{Min}(M, \leq), M \subseteq \Gamma$. 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 $\leq_+$.