# On the structure of order domains

Olav Geil and Ruud Pellikaan *

Appered in:
*Finite Fields and their Applications,* vol. 8, pp. 369-396, 2002.

**Abstract**

The notion of an order domain is generalized. The behaviour of an order domain by taking a sub algebra, the extension of scalars and the tensor product is studied. The relation of an order domain with valuation theory, Gröbner algebras and graded structures is given. The theory of Gröbner bases for order domains is developed and used to show that the factor ring theorem and its converse, the presentation theorem hold. The dimension of an order domain is related to the rank of its value semigroup.

*Keywords:* Order domain, order function, order structure, well-ordered semigroup, valuation theory, Gröbner bases, Hilbert functions, construction and decoding of algebraic geometry codes, algorithm of Berlekamp-Massey-Sakata.

*AMS classification:* 06F05, 11T71, 13A18, 13D40, 94B27

## 1 Introduction

The notion of an order domain came as a result of the aim to put the theory of algebraic geometry codes on a more elementary foundation. With this

*The first author is from the Department of Mathematics of Aalborg University, Frederik Bajersvej 7G, DK-9220 Aalborg Ø, Denmark, the second author is from the Department of Mathematics and Computing Science, Technical University of Eindhoven , P.O. Box 513, 5600 MB Eindhoven, The Netherlands.

notion it was possible to derive the parameters of these codes [12, 13, 14, 17] and to give an efficient decoding algorithm with the help of the algorithm of Berlekamp-Massey-Sakata [3, 16, 20, 35] due to [26]. Furthermore order domains are rings that are suitable for the theory of Gröbner bases [2, 7, 9], are closely related to Gröbner algebras [2] and the graded structures of [32] as shown by [27]. The construction of new order domains with the help of the factor ring theorem was found independently in the rank one case by [22, 23, 24, 25] and [28]. The presentation of order domains was found in the rank one case by [22, 23, 24, 25] and preluded by [34], and shown for arbitrary rank in [27]. Associated with an order domain we have a well-ordered semigroup [17, 27]. The relation between order domains and valuation theory [5, 11] was given in [27]. The dimension of an order domain with a finitely generated semigroup is equal to the rank of the value semigroup. This was shown in [27] under the extra assumption of the existence of a monomial basis. Furthermore a surprising example of an order function on $\mathbb{F}[X, Y]$ was given with a sub semigroup of the rational numbers as value semigroup. The notion of an order domain was generalized in [13] and the parameters of the codes were determined.

The content of this paper is as follows. In Section 2 the notion of an order function and an order domain is generalized. An order structure is a triple $(R, \rho, \Gamma)$ consisting of an order domain $R$, a well-order $\Gamma$ and an order function $\rho : R \to \Gamma \cup \{-\infty\}$. A direct consequence is that a sub algebra of an order domain is again an order domain. In Section 3 we introduce the useful notion of a well-behaving basis [12, 18] and show a result on the extension of scalars [27]. The value semigroup of an order structure and a weight function of rank $r$ are defined in Section 4. It is shown that every finitely generated inverse-free semigroup appears as the value semigroup of an order structure. The filtration, the associated graded algebra of an order structure are defined and its relation with the graded structures of [32] are given. In Section 5 it is proved that every order domain over $\mathbb{F}$ with a finitely generated value semigroup is finitely generated as an algebra over $\mathbb{F}$ and has a weight function. This will play a crucial role in the sequel in particular in Sections 6, 8, 10 and 11. In Section 6 it is shown that the order function on an order domain gives a valuation on the field of fractions. This result is used to prove that a finitely generated order structure has a normalized basis, and that the associated graded algebra is isomorphic with the semigroup algebra of the value semigroup. In Section 7 we show that the tensor product of order domains is again an order domain. We consider a generalization of the theory of Gröbner bases on order domains due to [27] in Section 8, which turns out to be vital for the following two sections. The factor ring theorem is given in Section 9 in its full generality. This theorem is very useful for the construction of new order structures. The result of [27] on the order function on $\mathbb{F}[X, Y]$ with a sub semigroup of the rational numbers as value semigroup is derived in an alternative way, as a consequence of the factor ring theorem. The presentation theorem is the converse of the factor ring construction, as shown in [22] for numerical semigroups. This result is generalized in a straightforward way in Section 10. Special attention is devoted to monomial algebra's. In Section 11 we will show using the theory of Hilbert functions that the dimension of an order domain with a finitely generated semigroup is equal to the rank of its value semigroup, without the assumption in [27] on the existence of a monomial basis. As a corollary it is proved that an order domain with a finitely generated semigroup has a monomial basis.

**Notation and terminology.** For the theory of monoids and semigroups we refer to [4, 30, 32]. Let $+$ be a binary operation on $\Gamma$. Let $0 \in \Gamma$. Then $(\Gamma, +, 0)$ is called a *commutative monoid* if $+$ is associative, commutative and has 0 as the neutral element. A commutative monoid $(\Gamma, +, 0)$ is called a *semigroup* if it is cancellative. A *numerical semigroup* is a sub semigroup of $(\mathbb{N}_0, +, 0)$. Let $(\Gamma, +, 0)$ be a commutative monoid. A partial order $\prec$ on $\Gamma$ is called *admissible* if $0 \preceq \alpha$ for all $\alpha \in \Gamma$; and if $\alpha \prec \beta$, then $\alpha + \gamma \prec \beta + \gamma$ for all $\alpha, \beta, \gamma \in \Gamma$. A commutative monoid with an admissible total order is cancellative and hence a semigroup. Now $(\Gamma, +, 0, <)$ is called a *(well)-ordered semigroup*, if $(\Gamma, +, 0)$ is a semigroup and $<$ is an admissible (well)-order on $\Gamma$. A well-ordered semigroup is inverse-free, and hence torsion free. A subset $\Sigma$ of $\Gamma$ is called an *ideal* if $\alpha + \beta \in \Sigma$ for all $\alpha \in \Sigma$ and $\beta \in \Gamma$.
Let $(\Gamma, +, 0)$ be an inverse-free semigroup. Define $\leq_p$ by $\alpha \leq_p \beta$ if and only if $\beta = \alpha + \gamma$ for a unique $\gamma \in \Gamma$, and this $\gamma$ is denoted by $\gamma = \beta - \alpha$. Then the relation $\leq_p$ is an admissible partial order on $\Gamma$.
The *group of differences* of a semigroup $\Gamma$ gives a group and is denoted by $D(\Gamma)$. An admissible (total) order on $\Gamma$ induces an admissible (total) order on $D(\Gamma)$, by defining $\alpha - \beta < \gamma - \delta$ if and only if $\alpha + \delta < \beta + \gamma$.
If $(\Gamma, +, 0)$ is a finitely generated inverse-free semigroup, then the set of minimal elements with respect to $\leq_p$ of a nonempty subset of $\Gamma$ is finite and nonempty, by Dickson's Lemma. See [1, Exercise 1.4.12] or [36, Proposition 1.3]. As a consequence, every admissible total order on a finitely generated

semigroup is a well-order.
If $\Gamma$ is a sub semigroup of $\mathbb{N}_0^r$ such that $D(\Gamma) = \mathbb{Z}^r = D(\mathbb{N}_0^r)$ and if moreover $\Gamma$ is well-ordered, then this order has a unique extension to a total order on $D(\Gamma) = \mathbb{Z}^r$, This total order can be restricted to an admissible total order on $\mathbb{N}_0^r$. The total $\leq$ order on $\mathbb{N}_0^r$ is in fact a well-order.
A map $w : \Gamma \rightarrow \Lambda$ between semigroups is called a *morphism of semigroups* if $w(0) = 0$ and $w(\alpha + \beta) = w(\alpha) + w(\beta)$ for all $\alpha, \beta \in \Gamma$. If moreover $\Gamma$ and $\Lambda$ are ordered semigroups, then $w$ is called a morphism of ordered semigroups if it is a morphism of semigroups and $w(\alpha) \leq w(\beta)$ for all $\alpha, \beta \in \Gamma$ such that $\alpha \leq \beta$.
For the theory of commutative algebra we refer to [6, 10]. A ring will always be a commutative ring with a unit. If $\mathbb{F}$ is a field, then an $\mathbb{F}$-*algebra* is a ring that contains $\mathbb{F}$ as a unitary subring. An *affine ring* over a field $\mathbb{F}$ is by definition a ring isomorphic with $\mathbb{F}[X_1, \ldots, X_m]/I$ for some ideal $I$ in $\mathbb{F}[X_1, \ldots, X_m]$. Let $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m$. Then a monomial $X_1^{\alpha_1} \cdots X_m^{\alpha_m}$ will be denoted by $X^\alpha$.
For the theory of valuations we refer to [5, VI] and [11]. For the theory of Gröbner basis we refer to [1, 9, 10].

# 2 A generalization of an order function

In this paper the minimal element of a well-order $(\Gamma, <)$ is denoted by 0, unless it is mentioned otherwise. If $(\Gamma, <)$ is an order, then $\Gamma_{-\infty} = \Gamma \cup \{-\infty\}$ is the order with $-\infty$ as minimal element, and $\Gamma_\infty = \Gamma \cup \{\infty\}$ is the order with $\infty$ as maximal element.
Consider the following definitions from [17, 28, 27].

**Definition 2.1** Let $(\Gamma, <)$ be a well-order. An *order function* on an $\mathbb{F}$-algebra $R$ is a surjective function

$$\rho : R \longrightarrow \Gamma_{-\infty},$$

such that the following conditions hold

$(O.0)$ $\rho(f) = -\infty$ if and only if $f = 0$
$(O.1)$ $\rho(af) = \rho(f)$ for all nonzero $a \in \mathbb{F}$
$(O.2)$ $\rho(f + g) \leq \max\{\rho(f), \rho(g)\}$
$(O.3)$ If $\rho(f) < \rho(g)$ and $h \neq 0$, then $\rho(fh) < \rho(gh)$
$(O.4)$ If $f$ and $g$ are nonzero and $\rho(f) = \rho(g)$, then there exists a nonzero $a \in \mathbb{F}$ such that $\rho(f - ag) < \rho(g)$.

for all $f, g, h \in R$.

**Remark 2.2** let $\rho$ be an order function on $R$. Suppose for instance that $\rho(f) < \rho(g)$ and $\rho(f+g) < \max\{\rho(f), \rho(g)\}$. Then $\rho(f) = \rho(-f)$ and $\rho(g) = \rho((-f) + (f+g)) \leq \max\{\rho(f), \rho(f+g)\} < \rho(g)$, which is a contradiction. Therefore $\rho(f+g) = \max\{\rho(f), \rho(g)\}$ if $\rho(f) \neq \rho(g)$ for $f, g \in R$.

**Remark 2.3** This definition is more general than the one given in [17, 27] in the sense that we have a map $\rho$ from $R$ to $\Gamma_{-\infty}$, where $(\Gamma, <)$ is an arbitrary well-order, instead of the nonnegative integers $(\mathbb{N}_0, <)$. In [27] it is assumed that the map $\rho$ is surjective. In [17] the surjectivity is not assumed, and the trivial case $R = \mathbb{F}$ is allowed. For an arbitrary well-order the surjectivity is not a restriction, since we can take the well-order on the image of $\rho$.
The definition of a *Gröbner algebra* [2] is close to the definition of an order domain, it is more general in the sense that the semigroup is not necessarily commutative and that the total order on the semigroup is not necessarily a well-order, and it is more restricted in the sense that the semigroup satisfies some finiteness conditions such as the Noetherian property. Gröbner algebras and finitely generated order domains are suited to develop the theory of Gröbner basis as noted in [2].
Notice that the definition of an order function in this paper and [17, 27] is distinct from the one given in [5, III 2.2].

We mention some facts that remain valid in this general setting.

A direct consequence of the definition is the following proposition on subalgebras.

**Proposition 2.4** *Let $R$ be an $\mathbb{F}$-algebra with order function $\rho : R \rightarrow \Gamma_{-\infty}$. Let $S$ be a sub $\mathbb{F}$-algebra of $R$. Let $\Lambda = \{\rho(f) | f \in S, f \neq 0\}$. Let $\sigma(f) = \rho(f)$ for all $f \in S$. Then $\sigma : S \rightarrow \Lambda_{-\infty}$ is an order function on $S$.*

**Proof.** One can generalize the proof in [27, Lemma 2.4]. $\diamond$

**Proposition 2.5** *Let $\rho$ be an order function on $R$. Then we have:*
*(1) If $\rho(f) = \rho(g)$, then $\rho(fh) = \rho(gh)$ for all $h \in R$.*
*(2) If $f \in R$ and $f \neq 0$, then $\rho(1) \leq \rho(f)$.*
*(3) $\mathbb{F} = \{ f \in R \mid \rho(f) \leq \rho(1) \}$.*
*(4) If $f$ and $g$ are nonzero and $\rho(f) = \rho(g)$, then there exists a unique nonzero $a \in \mathbb{F}$ such that $\rho(f - ag) < \rho(g)$.*

**Proof.** One can generalize the proof in [17, Lemma 3.9]. ◇

**Proposition 2.6** *If there exists an order function on $R$, then $R$ is an integral domain.*

**Proof.** One can generalize the proof in [17, Proposition 3.10]. ◇

**Definition 2.7** Let $\mathbb{F}$ be a field. Let $R$ be an $\mathbb{F}$-algebra, $\Gamma$ a well-order and $\rho : R \rightarrow \Gamma_{-\infty}$ an order function. Then $(R, \rho, \Gamma)$ is called an *order structure* and $R$ an *order domain* over $\mathbb{F}$.

# 3 Well-behaving basis

In this section we introduce the useful notion of a well-behaving basis [12, 17, 18] and show a result on the extension of scalars.

**Definition 3.1** Let $(\Gamma, <)$ be a well-order. Let $R$ be an $\mathbb{F}$-algebra. Let $(f_\alpha \mid \alpha \in \Gamma)$ be a basis of $R$ over $\mathbb{F}$. Let $R_\gamma$ be the subspace of $R$ generated by $(f_\alpha \mid \alpha \leq \gamma)$. Define

$$l(\alpha, \beta) = \min\{ \ \gamma \in \Gamma \mid f_\alpha f_\beta \in R_\gamma \ \}.$$

The basis is called *well-behaving*, if $l(\alpha, \gamma) < l(\beta, \gamma)$ for all $\alpha, \beta, \gamma \in \Gamma$ such that $\alpha < \beta$.

**Proposition 3.2** *Let $(R, \rho, \Gamma)$ be an order structure over $\mathbb{F}$. Let $(f_\alpha \mid \alpha \in \Gamma\ )$ be a sequence of elements in $R$ such that $\rho(f_\alpha) = \alpha$ for all $\alpha \in \Gamma$. Then this is a well-behaving basis. So there exists a well-behaving basis.*

**Proof.** The induction argument with respect to an arbitrary well-order is similar to the one given for $\mathbb{N}_0$ in [17, Proposition 3.12]. ◇

**Proposition 3.3** *Let $(\Gamma, <)$ be a well-order. Let $(f_\alpha \mid \alpha \in \Gamma)$ be a well-behaving basis of the $\mathbb{F}$-algebra $R$. Define $\rho(f) = -\infty$, if $f = 0$. If $f$ is not zero define $\rho(f) = \gamma$, where $\gamma$ is the minimal element of $\Gamma$ such that $f \in R_\gamma$. Then $(R, \rho, \Gamma)$ is an order structure.*

**Proof.** The induction argument with respect to an arbitrary well-order is similar to the one given for $\mathbb{N}_0$ in [17, Proposition 3.14]. $\diamond$

A consequence of the propositions on well-behaving bases is the following result on the *extension of scalars*.

**Proposition 3.4** *Let* $\mathbb{F}$ *be a subfield of* $\mathbb{G}$. *Let* $(R, \rho, \Gamma)$ *be an order structure over* $\mathbb{F}$. *Then* $(R \otimes_{\mathbb{F}} \mathbb{G}, \rho, \Gamma)$ *is an order structure over* $\mathbb{G}$.

**Proof.** See [27, Proposition 1.18]. The $\mathbb{F}$-algebra $R$ has a well-behaving basis $(f_\alpha \mid \alpha \in \Gamma)$ over $\mathbb{F}$ by Proposition 3.2. So $(f_\alpha \mid \alpha \in \Gamma)$ is a well-behaving basis over $\mathbb{G}$ for $R \otimes_{\mathbb{F}} \mathbb{G}$. Hence $R \otimes_{\mathbb{F}} \mathbb{G}$ is an order domain over $\mathbb{G}$ by Proposition 3.3. $\diamond$

# 4 The value semigroup

The value semigroup of an order structure and a weight function of rank $r$ are defined. It is shown that every finitely generated inverse-free semigroup appears as the value semigroup of an order structure. The filtration, the associated graded algebra of an order structure are defined and its relation with the graded structures in [32] is given.

**Remark 4.1** Let $(R, \rho, \Gamma)$ be an order structure. We have seen in Proposition 3.2 that $R$ has a well-behaving basis, and with the help of this basis the function $l(\alpha, \beta)$ was defined. But in fact this function does not depend on the chosen well-behaving basis, since $R_\gamma = \{ f \in R \mid \rho(f) \leq \gamma \}$ and $l(\alpha, \beta) = \min\{ \gamma \mid R_\alpha R_\beta \subseteq R_\gamma \}$.

**Definition 4.2** Let $(R, \rho, \Gamma)$ be an order structure. Consider the following definitions as in [17, 7.1] and [27, Definition 1.9]. The binary operation $+$ on $\Gamma$ is defined by $\alpha + \beta = l(\alpha, \beta)$. The minimum element of $\Gamma$ is denoted by 0. Then $(\Gamma, +, 0)$ is called the *value semigroup* of the order structure.

**Proposition 4.3** *Let* $(R, \rho, \Gamma)$ *be an order structure. Then* $(\Gamma, +, 0, <)$ *is a well-ordered semigroup.*

**Proof.** See also [27, Proposition 1.10]. That 0 is the neutral element follows from Proposition 2.5 and Condition $(O.0)$ of Definition 2.1.

The associativity and commutativity of + follow from the fact that multiplication in $R$ is associative and commutative and properties of the order function.
The well-order $<$ is admissible, since $l(\alpha, \gamma) < l(\beta, \gamma)$ if $\alpha < \beta$. $\diamond$

**Remark 4.4** From now on the well-order $(\Gamma, <)$ of an order structure $(R, \rho, \Gamma)$ is a well-ordered semigroup. It follows directly from the definitions that

$$(O.5) \quad \rho(fg) = \rho(f) + \rho(g)$$

for all $f, g \in R$. Here $-\infty + \alpha = -\infty$ for all $\alpha \in \Gamma_{-\infty}$. It is clear that condition $(O.3)$ is a consequence of $(O.5)$.

We generalize the definition of a "weight function" [17, Definition 3.5] as follows.

**Definition 4.5** Let $<$ be an admissible well-order on $(\mathbb{N}_0^r, +)$. Let $R$ be an $\mathbb{F}$-algebra. A *weight function* on $R$ is a function

$$\rho : R \longrightarrow \mathbb{N}_0^r \cup \{-\infty\},$$

such that it satisfies the conditions $(O.0)$, $(O.1)$, $(O.2)$, $(O.4)$ and $(O.5)$. Then $\Gamma = \{ \rho(f) \mid 0 \neq f \in R \}$ is called the value semigroup of the weight function.

**Remark 4.6** Notice that we do not require that the weight function be surjective.
Let $\rho$ be a weight function. Then the order and the addition on $\mathbb{N}_0^r$ induce a well-ordered semigroup on $\Gamma$, and $(R, \rho, \Gamma)$ is an order structure.
We will see in Corollary 5.7 that every order structure with a finitely generated value semigroup is induced by a weight function.
Remark that our use of the notion "weight function" is distinct from [10, §15.2, p. 327].

A second consequence of the proposition on well-behaving bases is the existence of order structures over $\mathbb{F}$-algebras with a given well-ordered value semigroup. This uses the well-known construction of semigroup algebras.

**Definition 4.7** Let $(\Gamma, +, 0, <)$ be a well-ordered semigroup. By definition the *semigroup algebra* $\mathbb{F}[\Gamma]$ has as basis $( X^\alpha \mid \alpha \in \Gamma )$ over $\mathbb{F}$. The multiplication is defined on the basis elements by

$$X^\alpha X^\beta = X^{\alpha+\beta}$$

and extended linearly.

**Proposition 4.8** *Let* $(\Gamma, +, 0, <)$ *be a well-ordered semigroup. Let* $\mathbb{F}$ *be a field. Then there exists an order structure over* $\mathbb{F}$ *with* $(\Gamma, +, 0, <)$ *as well-ordered value semigroup.*

**Proof.** Consider the semigroup algebra $R = \mathbb{F}[\Gamma]$ with basis $( X^\alpha \mid \alpha \in \Gamma )$. Then $l(\alpha, \beta)$, the minimal element $\gamma$ in $\Gamma$ such that $X^\alpha X^\beta \in \mathbb{F}[\Gamma]_\gamma$, is equal to $\alpha + \beta$. Hence $l(\alpha, \gamma) < l(\beta, \gamma)$ if $\alpha < \beta$, since $<$ is admissible. Therefore $( X^\alpha \mid \alpha \in \Gamma )$ is a well-behaving basis by Proposition 3.3, and $\mathbb{F}[\Gamma]$ is an order domain with $(\Gamma, +, 0, <)$ as well-ordered value semigroup. $\diamond$

**Remark 4.9** Every well-ordered semigroup is inverse-free, and therefore torsion free. A torsion free semigroup has an admissible linear order by [36, Proposition 1.3]. An admissible linear order on a finitely generated inverse free semigroup is a well-order. Hence every finitely generated inverse free semigroup appears as the value semigroup of an order structure.

**Remark 4.10** The orders on $\mathbb{N}_0^r$ and $\mathbb{Z}^r$ are classified in [31, Theorem 5] and [32, Theorem 2.5]. That is to say we can find $\mathbf{a}_1, \ldots, \mathbf{a}_r$ in $\mathbb{R}^r$ such that for $\mathbf{a}, \mathbf{b} \in \mathbb{N}_0^r$: $\mathbf{a} < \mathbf{b}$ if and only if there exists a $t$ such that $\mathbf{a}.\mathbf{a}_i = \mathbf{b}.\mathbf{a}_i$ for all $i < t$ and $\mathbf{a}.\mathbf{a}_t < \mathbf{b}.\mathbf{a}_t$. Here $\mathbf{a}.\mathbf{b}$ means the standard innerproduct.

**Definition 4.11** Let $(R, \rho, \Gamma)$ be an order structure. Let $R_\gamma = \{ f \in R \mid \rho(f) \leq \gamma \}$. Define $R_{<\gamma} = \{ f \in R \mid \rho(f) < \gamma \}$. Then $( R_\gamma \mid \gamma \in \Gamma )$ defines a *filtration* of $R$ , that means that [5, III.§2]

$$R_\alpha R_\beta \subseteq R_{\alpha+\beta}$$

for all $\alpha, \beta \in \Gamma$. Define the *associated* $\Gamma$- *graded algebra* by

$$Gr(R) = \bigoplus_{\gamma \in \Gamma} R_\gamma / R_{<\gamma}$$

**Remark 4.12** Let $\Gamma$ be a well-ordered semigroup. Let $R = \mathbb{F}[\Gamma]$. Then clearly the graded ring $Gr(R)$ of the order structure $(R, \rho, \Gamma)$ is isomorphic with $R$. We will see in Proposition 6.5 that for every order domain $R$ with a finitely generated semigroup $\Gamma$ we have that $Gr(R)$ is isomorphic with $\mathbb{F}[\Gamma]$.

**Remark 4.13** Let $(R, \rho, \Gamma)$ be an order structure. Let $(f_\alpha \mid \alpha \in \Gamma)$ be a well-behaving basis. Let $g_\alpha$ be the coset of $f_\alpha$ modulo $R_{<\alpha}$. Define the map $F : R \rightarrow Gr(R)$ by $F(0) = 0$ and $F(f) = a_{\rho(f)} g_{\rho(f)}$ for every nonzero $f \in R$ such that $f = \sum_{\alpha \leq \rho(f)} a_\alpha f_\alpha$. Let $D(\Gamma)$ be the totally ordered group of differences of $\Gamma$. Then $(R, D(\Gamma), \rho, Gr(R), F)$ is a *graded $\mathbb{F}$-structure* in the sense of [32].

# 5 Finitely generated order structures

It is shown that every order structure over $\mathbb{F}$ with a finitely generated value semigroup is finitely generated as an algebra over $\mathbb{F}$ and has a weight function.

**Definition 5.1** An order structure $(R, \rho, \Gamma)$ over a field $\mathbb{F}$ is called *finitely generated* or *Noetherian* if $(\Gamma, +)$ is a finitely generated semigroup.

**Proposition 5.2** *Let $(R, \rho, \Gamma)$ be a finitely generated order structure over a field $\mathbb{F}$. Then $R$ is a finitely generated algebra over $\mathbb{F}$.*

**Proof.** The semigroup is finitely generated, so there exist $\gamma_1, \ldots, \gamma_m \in \Gamma$ such that for all $\gamma \in \Gamma$ there exist $\alpha_1, \ldots, \alpha_m \in \mathbb{N}_0$ such that $\gamma = \alpha_1\gamma_1 + \cdots + \alpha_m\gamma_m$. The order function $\rho$ is surjective, so there exist $x_1, \ldots, x_m \in R$ such that $\rho(x_i) = \gamma_i$ for all $i = 1, \ldots, m$. We claim that $\mathbb{F}[x_1, \ldots, x_m] = R$. The proof is by induction on $\rho(f)$. The minimal element of $\Gamma_{-\infty}$ is $-\infty$ and $0 \in \mathbb{F}[x_1, \ldots, x_m]$ is the only element of $R$ that maps to $-\infty$. Let $\gamma \in \Gamma$. Suppose that $g \in \mathbb{F}[x_1, \ldots, x_m]$ for all $g \in R$ such that $\rho(g) < \gamma$. Let $f \in R$ such that $\rho(f) = \gamma$. Then there exist $\alpha_1, \ldots, \alpha_m \in \mathbb{N}_0$ such that $\gamma = \alpha_1\gamma_1 + \cdots + \alpha_m\gamma_m$. Hence $\rho(f) = \rho(x_1^{\alpha_1} \cdots x_m^{\alpha_m})$. So there exists a nonzero $a \in \mathbb{F}$ such that $g = f - a x_1^{\alpha_1} \cdots x_m^{\alpha_m}$ and $\rho(g) < \gamma$. Therefore $g \in \mathbb{F}[x_1, \ldots, x_m]$ by the induction assumption, so $f \in \mathbb{F}[x_1, \ldots, x_m]$. Hence $R = \mathbb{F}[x_1, \ldots, x_m]$ is finitely generated as an algebra over $\mathbb{F}$.
The proof of Proposition 5.2 in case $\Gamma$ is a sub semigroup of $\mathbb{N}_0$ is given in [29, Theorem 1]. ◇

**Definition 5.3** Let $(\Gamma, +, 0)$ be a semigroup. The *rank* of $\Gamma$ is defined by

$$\dim_{\mathbb{Q}} D(\Gamma) \otimes_{\mathbb{Z}} \mathbb{Q},$$

where $D(\Gamma)$ is the *group of differences* of $\Gamma$.

**Remark 5.4** Let $(\Gamma, +, 0)$ be a finitely generated semigroup. Then $D(\Gamma)$ is a finitely generated abelian group. Hence $D(\Gamma)$ is isomorphic with the direct sum of a finite group and $\mathbb{Z}^r$ for some nonnegative integer $r$, by the structure theorem of finitely generated abelian groups [19, §10]. So $D(\Gamma) \otimes_{\mathbb{Z}} \mathbb{Q} \cong \mathbb{Q}^r$, where $r$ is the rank of $\Gamma$.

**Remark 5.5** If an order domain over a field $\mathbb{F}$ is finitely generated as an algebra over $\mathbb{F}$, then it is not necessarily so that the semigroup $\Gamma$ is finitely generated. In Example 9.6 from [27, Example 5.2] an order function is given on $\mathbb{F}[X, Y]$ which has a semigroup in $\{a/2^n | a \in \mathbb{Z}, n \in \mathbb{N}_0\}$ of rank one that is not finitely generated.

**Theorem 5.6** *Let* $(\Gamma, +, 0)$ *be an inverse-free semigroup. Suppose that* $\Gamma$ *is finitely generated and of rank* $r$. *Then there exists an embedding* $\varphi : \Gamma \to \mathbb{N}_0^r$ *of semigroups. Furthermore the rank* $r$ *of* $\Gamma$ *is the smallest integer such that there exist an embedding of* $\Gamma$ *in* $\mathbb{N}_0^r$.

**Proof.** The semigroup is finitely generated and inverse-free, and therefore torsion free. So $\Gamma$ is embedded in $D(\Gamma)$ which is isomorphic with $\mathbb{Z}^r$, where $r$ is the rank of $\Gamma$, by Remark 5.4. Identify the embedding and the isomorphism as a subset and an equality, respectively, as follows

$$\Gamma \subseteq D(\Gamma) = \mathbb{Z}^r \subseteq \mathbb{R}^r.$$

Let $\mathbf{g}_1, \ldots, \mathbf{g}_m$ be generators of $\Gamma$. Let $C(\Gamma)$ be the *cone* of $\Gamma$ defined by

$$C(\Gamma) = \{ \mathbf{x} \in \mathbb{R}^r \mid \mathbf{x} = \sum a_i \mathbf{g}_i,\ a_i \in \mathbb{R},\ a_i \geq 0 \text{ for all } i = 1, \ldots, m \}.$$

Then $C(\Gamma)$ is convex, and an inverse-free sub semigroup of $\mathbb{R}^r$.
The cone $C(\Gamma)$ is the intersection of finitely many halfspaces $H_1, \ldots, H_m$, by [41, Theorem 1.3], where $H_i = \{ \mathbf{x} \in \mathbb{R}^r \mid \mathbf{h}_i \cdot \mathbf{x} \geq 0 \}$. We may assume that the $\mathbf{h}_i$ have integer coefficients, since the generators $\mathbf{g}_1, \ldots, \mathbf{g}_m$ have integer coefficients.
Moreover the $\mathbf{h}_i$ generate $\mathbb{R}^r$ as a vector space over $\mathbb{R}$, since $C(\Gamma)$ is inverse

free.
Therefore we may assume that $\mathbf{h}_1, \ldots, \mathbf{h}_r$ generate $\mathbb{R}^r$. The intersection of $H_1, \ldots, H_{i-1}, H_{i+1}, \ldots, H_r$ is a halfline. Let $\mathbf{b}_i$ be a vector with integer coefficients in this halfline. Then $\mathbf{b}_1, \ldots, \mathbf{b}_r$ are independent. Let $\Lambda$ be the sub semigroup generated by $\mathbf{b}_1, \ldots, \mathbf{b}_r$. Then the cone $C(\Lambda)$ is equal to the intersection of the halfspaces $H_1, \ldots, H_r$, which contains $C(\Gamma)$. Hence the $\mathbf{g}_i$ are a linear combination of the $\mathbf{b}_j$

$$\mathbf{g}_i = \sum_{j=1}^{r} \alpha_{ij} \mathbf{b}_j$$

with $\alpha_{ij}$ nonnegative real numbers. The $\alpha_{ij}$ are in fact rational numbers, since the coefficients of the $\mathbf{g}_i$ and the $\mathbf{b}_j$ are integers. Divide the $\mathbf{b}_j$ by the least common multiple of the denominators of the $\alpha_{ij}$. Then we may assume that the $\alpha_{ij}$ are nonnegative integers. Let $\mathbf{a}_i = (\alpha_{i1}, \ldots, \alpha_{ir})$. Then the map $\varphi(\sum \alpha_i \mathbf{g}_i) = \sum \alpha_i \mathbf{a}_i$ is well-defined and is an embedding of semigroups of $\Gamma$ in $\mathbb{N}_0^r$.
If $\Gamma$ is embedded in $\mathbb{N}_0^s$ as semigroups, then $D(\Gamma) \cong \mathbb{Z}^r$ is embedded in $\mathbb{Z}^s$ as groups. Hence $r \leq s$, and the rank of $\Gamma$ is smallest number $s$ such that $\Gamma$ has an embedding in $\mathbb{N}_0^s$.
Notice that in [6, Proposition 6.1.5] it is shown that $\Gamma$ has an embedding in $\mathbb{N}_0^m$, where $m$ is the number of halfspaces that have the cone $C(\Gamma)$ as common intersection. ◇

**Corollary 5.7** *Let $(R, \rho, \Gamma)$ be a finitely generated order structure of rank $r$. Then there exists an admissible well-order on $\mathbb{N}_0^r$ and an embedding of $\Gamma$ in $\mathbb{N}_0^r$ of well-ordered semigroups such that $\rho : R \rightarrow \mathbb{N}_0^r \cup \{-\infty\}$ is a weight function and $r$ is the rank of the value semigroup.*

**Proof.** The value semigroup $\Gamma$ is a finitely generated semigroup, and $\Gamma$ can be viewed as a sub semigroup of $\mathbb{N}_0^r$, where $r$ is the rank of $\Gamma$, by Theorem 5.6. Now $\Gamma$ is a well-ordered semigroup so this well-order has an extension to an admissible well-order on $D(\Gamma)$. Now $D(\Gamma)$ is embedded in $D(\mathbb{N}_0^r) = \mathbb{Z}^r$ and is also free of rank $r$. Hence $D(\Gamma) \otimes_{\mathbb{Z}} \mathbb{R} = \mathbb{R}^r$. The orders $\mathbb{Z}^r$ are classified by Remark 4.10. That is to say we can find $\mathbf{a}_1, \ldots, \mathbf{a}_r$ in $\mathbb{R}^r$ such that for $\mathbf{a}, \mathbf{b} \in D(\Gamma)$: $\mathbf{a} < \mathbf{b}$ if and only if there exists a $t$ such that $\mathbf{a}.\mathbf{a}_i = \mathbf{b}.\mathbf{a}_i$ for all $i < t$ and $\mathbf{a}.\mathbf{a}_t < \mathbf{b}.\mathbf{a}_t$. This defines an order on $\mathbb{R}^r$ and therefore an well-order on $\mathbb{N}_0^r$ that extends the order on $\Gamma$. Hence $\rho : R \rightarrow \mathbb{N}_0^r \cup \{-\infty\}$ is a weight function and $r$ is the rank of the value semigroup. ◇

**Remark 5.8** The value semigroup of a weight function of rank 1 is finitely generated. Order domains with a weight function of rank 1 are classified in [21, Theorem 1]. They are the affine coordinate rings of absolutely irreducible (possibly singular) affine curves over $\mathbb{F}$ that have exactly one place $P$ at infinity, this place is rational over $\mathbb{F}$ and $\rho(f) = -v_P(f)$, where $v_P$ is the valuation at $P$.
The value semigroup of a weight function of rank larger than 1 is not necessarily finitely generated. Take for instance the sub semigroup $\Gamma$ in $\mathbb{N}_0^2$ generated by the elements $(1, j)$ for all $j \in \mathbb{N}_0$. Then we have a weight function of rank 2 on the order domain $\mathbb{F}[\Gamma]$.

We will see in Theorem 11.9 that the rank of a finitely generated order structure is equal to the dimension of the order domain as a ring.

# 6 The Krull valuation of an order structure

In this section it is shown that the order function on an order domain gives a valuation on the field of fractions. This result is used to prove that a finitely generated order structure has a normalized basis, and that the associated graded algebra is isomorphic with the semigroup algebra of the value semigroup. For the theory of valuations we refer to [5, VI] and [11].

**Proposition 6.1** *Let $(R, \rho, \Gamma)$ be an order structure. Let $D(\Gamma)$ be the totally ordered group of differences of $\Gamma$. Let $K$ be the field of fractions of $R$. Then there is a unique way to extend the order function $\rho : R \to \Gamma_{-\infty}$ to a map $\tilde{\rho} : K \to D(\Gamma)_{-\infty}$ that satisfies the conditions $(O.0)$, $(O.1)$, $(O.2)$, $(O.3)$, $(O.4)$ and $(O.5)$.*

**Proof.** See also [27, Theorem 3.1]. Define $\tilde{\rho}(0) = -\infty$ and $\tilde{\rho}(f/g) = \rho(f) - \rho(g)$ for $f, g \in R$ and $f \neq 0$. Then $\tilde{\rho}$ is well-defined.
We will show condition $(O.4)$. Let $\tilde{\rho}(f/g) = \tilde{\rho}(h/k)$. Then $\rho(f) + \rho(k) = \rho(h) + \rho(g)$. So $\rho(fk) = \rho(gh)$. Hence there exists a nonzero $a \in \mathbb{F}$ such that $\rho(fk - agh) < \rho(fk)$. Therefore

$$\tilde{\rho}(f/g - ah/k) = \rho(fk - agh) - \rho(gk) < \rho(fk) - \rho(gk) = \tilde{\rho}(f/g).$$

The other conditions are straightforward to check and are left to the reader. Condition (($O.5$) gives that the extension $\tilde{\rho}$ is unique. $\diamond$

**Remark 6.2** The map $v = -\rho : K \to D(\Gamma)_\infty$ is a *Krull valuation*, with $R_v = \{ f \in K \mid v(f) \geq 0 \}$ as *valuation ring* , $\mathcal{M}_v = \{ f \in K \mid v(f) > 0 \}$ as the maximal ideal and with residue field $\mathbb{F}$. This is shown in [27, Theorem 3.1].
The ring $R_v$ is in a sense the opposite ring of the order domain $R$ in the field of fractions $K$ that is to say $R_v = \{ f \in K \mid \rho(f) \leq 0 \}$ and $R \subset \{ f \in K \mid \rho(f) \geq 0 \} \cup \{0\}$.
The Krull dimension of $R_v$ is equal to the *height* of $D(\Gamma)$, that is the number of *isolated subgroups* minus one. See [5, VI.4.3]. We will show in Section 11 a similar characterization of the Krull dimension of $R$ as the rank of $\Gamma$.
In [27, Proposition 4.2] it is shown that three of the four cases in Zariski's [40] classification of valuations on function fields of algebraic surfaces give rise to order domains and one does not. See also Remark 11.10.
Condition $(O.4)$ is not part of the definition of a Krull valuation.
Similarly as for $\rho$ one sees that also for $\tilde{\rho}$ the constant $a$ in Condition $(O.4)$ is unique.

**Definition 6.3** Let $(R, \rho, \Gamma)$ be an order structure. A well-behaving basis $(f_\alpha \mid \alpha \in \Gamma)$ is called *normalized* if

$$\rho(f_\alpha f_\beta - f_{\alpha+\beta}) < \rho(f_{\alpha+\beta})$$

for all $\alpha, \beta \in \Gamma$.

**Proposition 6.4** *A finitely generated order structure has a normalized basis.*

**Proof.** Let $(R, \rho, \Gamma)$ be a finitely generated order structure. Then $D(\Gamma) = \mathbb{Z}^r$, where $r$ is the rank of $\Gamma$, by Theorem 5.6. Let $K$ be the field of fractions of $R$. Consider $\tilde{\rho} : K \to \mathbb{Z}^r_{-\infty}$. Choose $t_i \in K$ such that $\tilde{\rho}(t_i) = \mathbf{e}_i$, the $i$-th standard basis element of $\mathbb{Z}^r$. Let $t^\alpha = t_1^{\alpha_1} \cdots t_r^{\alpha_r}$. Let $(f_\alpha \mid \alpha \in \Gamma)$ be a well-behaving basis. For every $\alpha \in \Gamma$ there is a unique nonzero $a_\alpha \in \mathbb{F}$ such that

$$\tilde{\rho}(t^\alpha - a_\alpha f_\alpha) < \tilde{\rho}(t^\alpha),$$

by Proposition 6.1 and Remark 6.2. Then $a_\alpha a_\beta = a_{\alpha+\beta}$ for all $\alpha, \beta \in \Gamma$, since the $a_\alpha$ are unique. Define $\tilde{f}_\alpha = a_\alpha f_\alpha$. Then $(\tilde{f}_\alpha \mid \alpha \in \Gamma)$ is a normalized basis. ◇

The following proposition gives an application of the existence of a normalized basis.

**Proposition 6.5** *Let* $(R, \rho, \Gamma)$ *be a finitely generated order structure. Then the graded algebra* $Gr(R)$ *is isomorphic with the semigroup algebra* $\mathbb{F}[\Gamma]$.

**Proof.** The order structure has a normalized basis $( f_\alpha \mid \alpha \in \Gamma )$ by Proposition 6.4. Then $f_\alpha \in R_\alpha \setminus R_{<\alpha}$. Let $g_\alpha$ be the coset of $f_\alpha$ in $R_\alpha / R_{<\alpha}$. Then $( g_\alpha \mid \alpha \in \Gamma )$ is a normalized basis of $Gr(R)$, we even have that $g_\alpha g_\beta = g_{\alpha+\beta}$ for all $\alpha, \beta \in \Gamma$. Hence the map $g_\alpha \mapsto X^\alpha$ maps a basis of $Gr(R)$ to a basis of $\mathbb{F}[\Gamma]$ which gives an isomorphism of vector spaces from $Gr(R)$ to $\mathbb{F}[\Gamma]$, which is an isomorphism of $\mathbb{F}$-algebras. ◇

# 7 Tensor product

A third consequence of the proposition on well-behaving bases is on the tensor product of order domains. Before giving this result, we give the algebraic geometric meaning of the tensor product and a preparation on the direct sum of well-ordered semigroups.

**Example 7.1** Let $R$ and $S$ be affine $\mathbb{F}$-algebras, so $R = \mathbb{F}[X_1, \ldots, X_m]/I$ and $S = \mathbb{F}[Y_1, \ldots, Y_n]/J$ are the coordinate rings of the varieties $\mathcal{X}$ and $\mathcal{Y}$. Then the tensor product $R \otimes_{\mathbb{F}} S$ is given by

$$R \otimes_{\mathbb{F}} S = \mathbb{F}[X_1, \ldots, X_m, Y_1, \ldots, Y_n]/(I + J).$$

It is the coordinate ring of $\mathcal{X} \times \mathcal{Y}$. See [10, 39].

**Definition 7.2** Let $(\Gamma, +_\Gamma, 0, <_\Gamma)$ and $(\Lambda, +_\Lambda, 0, <_\Lambda)$ be well-ordered semigroups. Let $<$ be an admissible well-order on the direct sum $\Gamma \oplus \Lambda$. Then $<$ is *compatible* with the well-orders on $\Gamma$ and $\Lambda$ if $(\alpha, \delta) < (\gamma, \delta)$ for all $\alpha, \gamma \in \Gamma$ and $\delta \in \Lambda$ such that $\alpha <_\Gamma \gamma$; and $(\alpha, \beta) < (\alpha, \delta)$ for all $\alpha \in \Gamma$ and $\beta, \delta \in \Lambda$ such that $\beta <_\Lambda \delta$.

**Example 7.3** Let $(\Gamma, +_\Gamma, 0, <_\Gamma)$ and $(\Lambda, +_\Lambda, 0, <_\Lambda)$ be well-ordered semigroups. Define the *lexicographic order* $<_{lex}$ on $\Gamma \oplus \Lambda$ by $(\alpha, \beta) <_{lex} (\gamma, \delta)$ if and only if $\alpha <_\Gamma \gamma$, or $\alpha = \gamma$ and $\beta <_\Lambda \delta$. Then $<_{lex}$ is an admissible well-order on the direct sum that is compatible.

**Example 7.4** Let $(\Gamma, +_\Gamma, 0, <_\Gamma)$ and $(\Lambda, +_\Lambda, 0, <_\Lambda)$ be well-ordered semigroups, that are embedded in $(\mathbb{N}_0^r, +_\Gamma, 0, <_\Gamma)$ and $(\mathbb{N}_0^s, +_\Lambda, 0, <_\Lambda)$, respectively, as well-ordered semigroups. The degree of $\alpha \in \mathbb{N}_0^r$ is defined by

$\deg(\alpha) = \sum \alpha_i$. Define the *total degree lexicographic order* $<_{dlex}$ on $\Gamma \oplus \Lambda$ by $(\alpha, \beta) <_{dlex} (\gamma, \delta)$ if and only if $\deg(\alpha, \beta) < \deg(\gamma, \delta)$, or $\deg(\alpha, \beta) = \deg(\gamma, \delta)$ and $(\alpha, \beta) <_{lex} (\gamma, \delta)$. Then $<_{dlex}$ is an admissible well-order on the direct sum that is compatible. Furthermore, if $<_\Gamma$ and $<_\Lambda$ are well-orders that are isomorphic with the well-order on $\mathbb{N}_0$, then $<_{dlex}$ is also an well-order that is isomorphic with the well-order on $\mathbb{N}_0$,

From now on we will omit the subscripts $\Gamma$ and $\Lambda$ in $+_\Gamma$, $<_\Gamma$, $+_\Lambda$ and $<_\Lambda$.

Let $(R, \rho, \Gamma)$ and $(S, \sigma, \Lambda)$ be order structures. The $\mathbb{F}$-algebra $R$ has a well-behaving basis $(f_\alpha \mid \alpha \in \Gamma)$ over $\mathbb{F}$, and $S$ has a well-behaving basis $(g_\beta \mid \beta \in \Lambda)$, by Proposition 3.2. Then the elements $f_\alpha \otimes g_\beta$, $\alpha \in \Gamma$, $\beta \in \Lambda$ form a basis of $R \otimes_\mathbb{F} S$ by [39, Theorem 33].

Let $<$ be an admissible well-order on $\Gamma \oplus \Lambda$ that is compatible. Define the map

$$\rho \otimes \sigma : R \otimes_\mathbb{F} S \to (\Gamma \oplus \Lambda)_{-\infty},$$

by

$$\rho \otimes \sigma \left( \sum \lambda_{\alpha\beta} f_\alpha \otimes g_\beta \right) = \max\{ \ (\alpha, \beta) \mid \lambda_{\alpha\beta} \neq 0 \ \},$$

where the maximum is taken with respect to the well-order $<$ on $\Gamma \oplus \Lambda$.

**Proposition 7.5** *Let $(R, \rho, \Gamma)$ and $(S, \sigma, \Lambda)$ be order structures over $\mathbb{F}$. Then $(R \otimes_\mathbb{F} S, \rho \otimes \sigma, \Gamma \oplus \Lambda)$ is an order structure over $\mathbb{F}$.*

**Proof.** We have that $\alpha_1 + \alpha_2 = \min\{ \ \gamma \in \Gamma \mid f_{\alpha_1} f_{\alpha_2} \in R_\gamma \ \}$ for $\alpha_1, \alpha_2 \in \Gamma$, and $\beta_1 + \beta_2 = \min\{ \ \delta \in \Lambda \mid g_{\beta_1} g_{\beta_2} \in S_\delta \ \}$ for $\beta_1, \beta_2 \in \Lambda$,which are strictly increasing in both arguments. Define the function $l$ by

$$l((\alpha_1, \beta_1), (\alpha_2, \beta_2)) = \min\{ \ (\gamma, \delta) \in \Gamma \oplus \Lambda \mid (f_{\alpha_1} \otimes g_{\beta_1})(f_{\alpha_2} \otimes g_{\beta_2}) \in (R \otimes_\mathbb{F} S)_{(\gamma, \delta)} \ \}.$$

There exist $a_{\alpha_1 \alpha_2 \gamma} \in \mathbb{F}$ such that

$$f_{\alpha_1} f_{\alpha_2} = \sum_{\gamma \leq \alpha_1 + \alpha_2} a_{\alpha_1 \alpha_2 \gamma} f_\gamma,$$

and for every $\alpha_1, \alpha_2 \in \Gamma$: $a_{\alpha_1 \alpha_2 \alpha_1 + \alpha_2} \neq 0$. Similarly, there exist $b_{\beta_1 \beta_2 \delta} \in \mathbb{F}$ such that

$$g_{\beta_1} g_{\beta_2} = \sum_{\delta \leq \beta_1 + \beta_2} b_{\beta_1 \beta_2 \delta} g_\delta,$$

and for every $\beta_1, \beta_2 \in \Lambda$: $b_{\beta_1\beta_2\beta_1+\beta_2} \neq 0$.
Now

$$(f_{\alpha_1} \otimes g_{\beta_1})(f_{\alpha_2} \otimes g_{\beta_2}) = (f_{\alpha_1} f_{\alpha_2}) \otimes (g_{\beta_1} g_{\beta_2}) = \sum_{\gamma \leq \alpha_1+\alpha_2} \sum_{\delta \leq \beta_1+\beta_2} a_{\alpha_1\alpha_2\gamma} b_{\beta_1\beta_2\delta} f_\gamma g_\delta,$$

and $a_{\alpha_1\alpha_2\alpha_1+\alpha_2} b_{\beta_1\beta_2\beta_1+\beta_2} \neq 0$.
Furthermore, $(\gamma, \delta) \leq (\alpha_1 + \alpha_2, \beta_1 + \beta_2)$ if $\gamma \leq \alpha_1 + \alpha_2$ and $\delta \leq \beta_1 + \beta_2$ and the first inequality is strict if $\gamma < \alpha_1 + \alpha_2$ or $\delta < \beta_1 + \beta_2$, since $<$ is compatible with the well-orders on $\Gamma$ and $\Lambda$.
Hence $l((\alpha_1, \beta_1), (\alpha_2, \beta_2)) = (\alpha_1 + \alpha_2, \beta_1 + \beta_2)$. Therefore $l$ is strictly increasing in both arguments, since $<$ is admissible. So $(f_\alpha \otimes g_\beta \mid \alpha \in \Gamma,\ \beta \in \Lambda)$ is a well-behaving basis of $R \otimes_{\mathbb{F}} S$. By Proposition 3.3 we have that $\rho \otimes \sigma$ is an order function. $\diamond$

**Remark 7.6** Similarly one shows that if $\rho : R \to \mathbb{N}_0^r \cup \{-\infty\}$ is a weight function of rank $r$ and $\sigma : S \to \mathbb{N}_0^s \cup \{-\infty\}$ is a weight function of rank $s$, then $\rho \otimes \sigma : R \otimes_{\mathbb{F}} S \to \mathbb{N}_0^{r+s} \cup \{-\infty\}$ is a weight function of rank $r + s$.

**Remark 7.7** If the well-orders on $\Gamma$ and $\Lambda$ of the order domains $R$ and $S$ are finitely generated and both are isomorphic with $(\mathbb{N}_0, <)$, then $<_{dlex}$ is an admissible well-order on $\Gamma \oplus \Lambda$ that is isomorphic with $(\mathbb{N}_0, <)$, by Example 7.4. Hence Proposition 7.5 is also true in the old sense of order domains [17, 27] in case they are finitely generated.

# 8 The theory of Gröbner bases for order domains

We consider the following generalization of the *theory of Gröbner bases* [1, 7, 9, 36] on order domains due to [27], which is closely related to the work of [2].

**Definition 8.1** Let $(\Gamma, +, 0, <)$ be a well-ordered semigroup. Let $\leq_p$ be the partial order defined by $\alpha \leq_p \beta$ if and only if $\beta = \alpha + \gamma$ for some $\gamma \in \Gamma$. Let $\Sigma$ be a subset of $\Gamma$. Define

$$\min \Sigma = \{ \ \alpha \in \Sigma \mid \ \text{if } \beta \in \Sigma, \beta \leq_p \alpha, \ \text{then } \beta = \alpha \ \},$$

the set of *minimal elements* of $\Sigma$.

For every $\beta \in \Sigma$ there exists an $\alpha \in \min \Sigma$ such that $\alpha \leq_p \beta$, see [27, Lemma 1.12].

**Definition 8.2** Let $(R, \rho, \Gamma)$ be an order structure. Let $I$ be an ideal in $R$. Define

$$\Sigma(I) = \{\ \rho(f) \mid f \in I,\ f \neq 0\ \}.$$

$$\sigma(I) = \min \Sigma(I).$$

The *footprint* or *delta set* of $I$ is by definition

$$\Delta(I) = \Gamma \setminus \Sigma(I).$$

A subset $\mathcal{G}$ of $I$ is called a *Gröbner basis* of I if $\sigma(I) \subseteq \{\ \rho(g) \mid g \in \mathcal{G}\ \}$. A Gröbner basis $\mathcal{G}$ of $I$ is called *minimal* if for every $\gamma \in \sigma(I)$ there is exactly one $g \in \mathcal{G}$ such that $\gamma = \rho(g)$.

**Theorem 8.3** *Let $(R, \rho, \Gamma)$ be an order structure over $\mathbb{F}$. Let $I$ be an ideal in $R$ and $\mathcal{G}$ a Gröbner basis of $I$. Then $\Sigma(I)$ is an ideal in $\Gamma$ and $\mathcal{G}$ generates $I$ in $R$. Let $(\ f_\alpha \mid \alpha \in \Gamma\ )$ be a well-behaving basis. Then every $f \in R$ is equivalent modulo $I$ to*

$$\sum_{\alpha \in \Delta(I)} a_\alpha f_\alpha$$

*with $a_\alpha \in \mathbb{F}$ for all $\alpha$, and this expression is unique. In particular, the dimension of $R/I$ over $\mathbb{F}$ is equal to the number of elements of $\Delta(I)$. If $\Gamma$ is finitely generated, then $\sigma(I)$ is finite.*

**Proof.** Generalize the proof of [27, Proposition 1.13]. See also [2]. $\diamond$

**Definition 8.4** A minimal Gröbner basis $\mathcal{G}$ of $I$ is called *reduced* with respect to a given well-behaving basis $(f_\alpha \mid \alpha \in \Gamma)$ if for every $\gamma \in \sigma(I)$ the unique $g \in \mathcal{G}$ such that $\gamma = \rho(g)$ can be written as $g = f_\gamma - \sum_{\alpha \in \Delta(I)} a_\alpha f_\alpha$ with $a_\alpha \in \mathbb{F}$ for all $\alpha$.

**Proposition 8.5** *Let $(R, \rho, \Gamma)$ be an order structure over $\mathbb{F}$. Let $I$ be an ideal in $R$. Then there exists a unique reduced Gröbner basis of $I$ with respect to a given well-behaving basis. If moreover the order structure is finitely generated, then for a given ideal $I$ one can choose a normalized basis $(f_\alpha \mid \alpha \in \Gamma)$ in such a way that $f_\alpha \in I$ for all $\alpha \in \Sigma(I)$ and the reduced Gröbner basis of $I$ is equal to $(f_\alpha \mid \alpha \in \sigma(I))$.*

**Proof.** Generalize the proof of [27, Proposition 1.15] for the first part. For the second part. Choose elements $f_\alpha \in R$ for all $\alpha \in \Gamma$ such that $f_\alpha \in I$ for all $\alpha \in \Sigma(I)$. Then $(f_\alpha \mid \alpha \in \Gamma)$ is a well-behaving basis by Proposition 3.2. We may assume that the basis is normalized by multiplying all the basis elements with a suitable constant, as shown in Proposition 6.4. We still have that $f_\alpha \in I$ for all $\alpha \in \Sigma(I)$. The reduced Gröbner basis of $I$ are now elements of this well-behaving basis, by the first part of the proposition. $\diamond$

**Remark 8.6** We refer to [2, Theorem 12] for the generalization of the algorithm of Buchberger to obtain a Gröbner basis. The *algorithm of Berlekamp-Massey-Sakata* [3, 20, 35] can be generalized for order domains [17, 16, 26, 27]. For both algorithms one has a generalization of the notion of S polynomials: the set of S-elements $S(f, g)$. To be of practical use one has to assume that the value semigroup is finitely generated. Then the set of S-elements and $\min \Sigma(I)$ are finite.

# 9 The factor ring construction

The *factor ring theorem* will be given. It turns out to be very useful for the construction of new order structures.

**Theorem 9.1** *Let $(\Gamma, +, 0, <)$ and $(\Lambda, +, 0, <)$ be well-ordered semigroups. Let $w : \Gamma \to \Lambda$ be a surjective morphism of well-ordered semigroups. Let $(R, \rho, \Gamma)$ be an order structure. Let $(\ f_\alpha \mid \alpha \in \Gamma\ )$ be a well-behaving basis. Let $I$ be an ideal in $R$ with Gröbner bases $\mathcal{G}$. Suppose that the restriction $w : \Delta(I) \to \Lambda$ of $w$ to the footprint of $I$ is injective. Suppose that every element $g$ of $\mathcal{G}$ has exactly two terms of the same maximal $w$-value, that is to say $g$ is of the form*

$$g = af_\alpha + bf_\beta + \sum_{w(\gamma)<\delta} c_\gamma f_\gamma,$$

*where $a, b \in \mathbb{F}^*$, $\alpha \neq \beta$ and $\delta := w(\alpha) = w(\beta)$. Let $S = R/I$. Let $g_\alpha$ be the coset of $f_\alpha$ modulo $I$ in $S$. Then $(\ g_\alpha \mid \alpha \in \Delta(I)\ )$ is a well-behaving basis of $S$. Let $\sigma : S \to \Lambda_{-\infty}$ be the the associated order function. Then $(S, \sigma, \Lambda)$ is an order structure and $\sigma$ has the property that $\sigma(g_\alpha) = w(f_\alpha)$ for all $\alpha \in \Gamma$.*

**Proof.** This theorem is the fourth consequence of well-behaving bases. It is a generalization of [13, Theorem I.7.1] for weight functions of arbitrary rank, and of [28, Theorem 5.11] [23, Theorem 1], [24, Theorem 5.17], [25, p.1411] and [22, Theorem 3.11] for weight functions of rank 1. In all these cases $R = \mathbb{F}[X_1, \ldots, X_m]$ and $\Gamma = \mathbb{N}_0^m$. The above proofs can be generalized in a straightforward manner using the Gröbner basis theory of Theorem 8.3.
From the above references it might not be clear that the assumptions imply that the map $\sigma : S \rightarrow \Lambda_{-\infty}$ is surjective. But is assumed that the map $w : \Gamma \rightarrow \Lambda$ is surjective. Hence for every $\alpha \in \Lambda$ there is a $\beta \in \Gamma$ such that $w(\beta) = \alpha$. Now using the appropriate generalization of [28, Lemma 5.10] one shows that

$$f_\beta \equiv a f_\delta + \sum_{\delta \neq \gamma \in \Delta(I)} a_\gamma f_\gamma \quad (\bmod I),$$

for some $\delta \in \Delta(I)$ and $a_\gamma \in \mathbb{F}$ and $a \in \mathbb{F}^*$ such that $w(\beta) = w(\delta) > w(\gamma)$ for all $\gamma$ with $\delta \neq \gamma \in \Delta(I)$. Hence $\sigma(f_\delta + I) = w(\delta) = \alpha$. Therefore $\sigma : S \rightarrow \Lambda_{-\infty}$ is surjective. $\diamond$

**Definition 9.2** Let

$$w : \mathbb{N}_0^m \rightarrow \mathbb{N}_0^r$$

be a morphism of semigroups. Let $<$ be an admissible order on $\mathbb{N}_0^r$. Let $\prec$ be an admissible order on $\mathbb{N}_0^m$. Define $\prec_w$ by $\alpha \prec_w \beta$ if and only $w(\alpha) < w(\beta)$, or $w(\alpha) = w(\beta)$ and $\alpha \prec \beta$. Then $\prec_w$ is an admissible well-order on $\mathbb{N}_0^m$ and $w$ is a morphism of ordered semigroups. This map induces a map on the monomials by $w(X^\alpha) = w(\alpha)$ and on the nonzero polynomials, by $w(\sum a_\alpha X^\alpha) = \max\{w(\alpha) \mid a_\alpha \neq 0\}$, where the maximum is taken with respect to $<$.

**Example 9.3** Let $a_1, \ldots, a_{m-1}$ and $b_1, \ldots, b_{m-1}$ be positive integers such that $\gcd(a_i, b_j) = 1$ for all $1 \leq i \leq j < m$. Let $w : \mathbb{N}_0^m \rightarrow \mathbb{N}_0$ be the morphism of semigroups defined by $w(\alpha) = \sum_{i=1}^m \alpha_i a_1 \cdots a_{i-1} b_i \cdots b_{m-1}$. Let $I$ be the ideal in $\mathbb{F}[X_1, \ldots, X_m]$ generated by

$$F_i = X_i^{a_i} - X_{i+1}^{b_i} + G_i \text{ for } i = 1, \ldots, m-1,$$

where $G_i \in \mathbb{F}[X_1, \ldots, X_{i+1}]$ and $w(G_i) < a_1 \cdots a_i b_i \cdots b_{m-1}$. Then the ring $S = \mathbb{F}[X_1, \ldots, X_m]/I$ has a weight function $\sigma$, such that $\sigma(x_i) = a_1 \cdots a_{i-1} b_i \cdots b_{m-1}$ for all $i$. See [17, Example 3.22] and [28].

**Example 9.4** Let $R(m,n) = \mathbb{F}[X_{ij} | 1 \leq i \leq m, 1 \leq j \leq n]$ be the polynomial ring in the variables $X_{ij}$, the entries of an $m \times n$ matrix. Let $I(m,n,r)$ be the ideal in $R(m,n)$ generated by the $r \times r$ minors of this matrix. The ring $R(m,n,r) = R(m,n)/I(m,n,r)$ is called a *generic determinantal ring*. In [13, Example I.6.6] and [13, Example I.7.9] it is shown that $R(2,n,2)$ and $R(m,m,m)$ are order domains as a consequence of Theorem 9.1. We leave it as an open question which generic determinantal rings are order domains.

**Example 9.5** The admissible well-orders on $\mathbb{N}_0^m$ are classified in [32]. In this way we get a family of order functions on $\mathbb{F}[X_1, \ldots, X_m] \cong \mathbb{F}[\mathbb{N}_0^m]$. But not all order functions on $\mathbb{F}[X_1, \ldots, X_m]$ are of this type. Consider the morphism of semigroups $w : \mathbb{N}_0^3 \to \mathbb{N}_0^2$ defined by $w(\alpha_1, \alpha_2, \alpha_3) = \alpha_1(3,0) + \alpha_2(4,0) + \alpha_3(0,1)$. Let $\Lambda$ be the numerical semigroup generated by $(3,0)$, $(4,0)$ and $(0,1)$. Let $G = X_1^4 - X_2^3 + X_3$. Let $I$ be the ideal generated by $G$. Then the conditions of Theorem 9.1 are fullfilled. Hence we have an order structure $(S, \sigma, \Lambda)$, where $S = \mathbb{F}[X_1, X_2, X_3]/I \cong \mathbb{F}[X_1, X_2]$ and a value semigroup that is not isomorphic with $\mathbb{N}_0^2$. See [13, Example I.7.8]. We leave it as an open question to classify all the order functions on polynomial rings.

**Example 9.6** Here we derive an alternative way of the surprising result in [27, Example 5.2] by using the factor ring construction. In [27] the theory of [40] on valuations of the field of rational function on algebraic surfaces and an infinite sequence of blowing ups is used.
Define by recursion the following sequence of rational numbers:

$$\lambda_1 = 1, \quad \text{and} \quad \lambda_{i+1} = 2\lambda_i - 2^{-i} \quad \text{for all } i \in \mathbb{N}.$$

Then

$$\lambda_i = \tfrac{1}{3}\left(2^i + 2^{-i+1}\right) \quad \text{for all} \quad i \in \mathbb{N}.$$

Let $\Lambda$ be the semigroup generated by all the $\lambda_j$, $j \in \mathbb{N}$. Let $\Lambda_i$ be the semigroup generated by all the $\lambda_j$, $j \leq i+1$. We have the following relations between the generators

$$2\lambda_{i+1} = 3\lambda_i + \sum_{j=0}^{i-1} \lambda_j.$$

The semigroup $2^{i-1}\Lambda_i$ is a sub semigroup of $\mathbb{N}_0$ and is telescopic, see [17, 18], as we can see from the above relations. Hence the semigroup is a complete

intersection, by [15], that is to say the above relations generate all the relations.
Let $R = \mathbb{F}[X_1, X_2, \ldots, X_n, \ldots]$, the polynomial ring with infinitely many variables. Take the lexicographic order on the monomials with

$$1 < X_1 < X_2 < \cdots < X_n < \cdots$$

By definition $\mathbb{N}_0^{(\infty)}$ is the set of all sequences of nonnegative integers such that at most finitely many of them are nonzero. So $R = \mathbb{F}[\mathbb{N}_0^{(\infty)}]$. Let $w$ be the morphism of semigroups from $\mathbb{N}_0^{(\infty)}$ to $\Lambda$ defined by $w(\alpha) = \sum_i \alpha_i \lambda_i$. Let $\prec_w$ be the monomial order on $\mathbb{N}_0^{(\infty)}$ associated to $w$ and the lexicographic order on $\mathbb{N}_0^{(\infty)}$. Then the image of this map is $\Lambda$. Let $\rho$ be the order function on $R$ associated with $\prec_w$. Let

$$G_i = X_{i+1}^2 - X_i^3 \prod_{j \leq i-1} X_j + X_{i+2}$$

for $i \in \mathbb{N}$. Then

$$w(X_{i+1}^2) = 2\lambda_{i+1} = 3\lambda_i + \sum_{j=0}^{i-1} \lambda_j = w\left( X_i^3 \prod_{j \leq i-1} X_j \right) > w(X_{i+2}).$$

Let $\mathcal{G} = \{G_i \mid i \in \mathbb{N}\}$. Then $\mathcal{G}$ is a Gröbner basis. This is a consequence of the fact that the semigroups $\Lambda_i$ are complete intersection, but it also follows from the fact that the $S$-polynomials reduce to zero under $\mathcal{G}$.
Let $I$ be the ideal in $R$ generated by $\mathcal{G}$. Then

$$\Delta(I) = \{ \ \alpha \in \mathbb{N}_0^{(\infty)} \mid \alpha_i \leq 1 \text{ for all } i \geq 2 \ \}.$$

Notice that $\lambda_i = n_i 2^{-i+1}$, where $n_i$ is a positive odd integer. Define $l(\alpha) = \max\{i \mid \alpha_i \neq 0\}$ for $\alpha \in \mathbb{N}_0^{(\infty)}$. Then $w(\alpha) = n(\alpha) 2^{-l(\alpha)+1}$ for all $\alpha \in \Delta(I)$, where $n(\alpha)$ is a positive odd integer. Hence the restriction of $w$ to $\Delta(I)$ is injective.
In this way we get by Theorem 9.1 an order structure $(S, \sigma, \Lambda)$, where $S = R/I$. Now $S$ is isomorphic with $\mathbb{F}[X_1, X_2]$ and $\Lambda$ is a sub semigroup of $\mathbb{Q}_2$, the localization of $\mathbb{Z}$ at the prime 2, that is to say the rational numbers with only powers of 2 in the denominator. Therefore $S$ is an example of an order domain of dimension 2 with a value semigroup of rank 1.

# 10 The presentation of order domains

The factor ring construction has a converse as shown in [22] for numerical semigroups. This result can be generalized in a straightforward way. That is to say every order domain of a finitely generated order structure can be constructed as a factor ring of the order structure $(\mathbb{F}[X_1,\ldots,X_m],\rho,\mathbb{N}_0^m)$, where $\rho(X^\alpha)=\alpha$ and $\prec_w$ is an appropriate order on $\mathbb{N}_0^m$. Special attention is devoted to monomial order domains.

Let $(R,\rho,\Gamma)$ be a finitely generated order structure. We may assume that $\Gamma$ is embedded in $\mathbb{N}_0^r$ as well-ordered semigroup by Theorem 5.6 where $r$ is the rank of $\Gamma$. Let $\gamma_1,\ldots,\gamma_m$ be generators of $\Gamma$ as a semigroup. Choose $x_1,\ldots,x_m\in R$ from a normalized basis, see Proposition 6.4, such that $\rho(x_i)=\gamma_i$ for all $i$. Then $R=\mathbb{F}[x_1,\ldots,x_m]$ by Proposition 5.2. Let $\varphi:\mathbb{F}[X_1,\ldots,X_m]\rightarrow R$ be defined by $\varphi(X_i)=x_i$. Then the map is a morphism of rings. Let $I$ be the kernel of $\varphi$. Then $\varphi$ induces an isomorphism , since $\varphi$ is surjective. From now on we identify $R$ with $\mathbb{F}[X_1,\ldots,X_m]/I$.

Let $\mathcal{A}=\{\gamma_1,\ldots,\gamma_m\}$. Define the map $w:\mathbb{N}_0^m\rightarrow\mathbb{N}_0^r$ by $w(\alpha)=\sum\alpha_i\gamma_i$. Let $<$ be the order on $\mathbb{N}_0^r$. Let $\prec$ be an admissible order on $\mathbb{N}_0^m$. Let $\prec_w$ be the admissible order on $\mathbb{N}_0^m$ as in Definition 9.2.

**Definition 10.1** Let

$$\Delta(\mathcal{A})=\{\alpha\in\mathbb{N}_0^m \mid \text{ if } w(\alpha)\leq w(\beta), \text{ then } \alpha\preceq_w\beta\ \}$$

as in [22, 23, 24, 25]. Let $\sigma(\mathcal{A})$ be the set of minimal elements with respect to the partial order $\leq_p$ of the set $\Sigma(\mathcal{A})=\mathbb{N}_0^m\setminus\Delta(\mathcal{A})$.

**Lemma 10.2** *The set* $\{\ x^\alpha \mid \alpha\in\Delta(\mathcal{A})\ \}$ *is a basis of* $R$ *over* $\mathbb{F}$.

**Proof.** See [23, Lemma 10], [24, Lemma 5.13], [25, p. 1410]. Generalize the proof in [22, Proposition 3.4]. ◇

**Lemma 10.3** *We have that* $\Delta(I)=\Delta(\mathcal{A})$.

**Proof.** See [24, Section 5.4], [25, p. 1417]. Generalize the proof in [22, Lemma 3.7]. ◇

**Theorem 10.4** *With the above notation we have that $\sigma(\mathcal{A})$ is finite and for each $\alpha \in \sigma(\mathcal{A})$ there is a unique $\alpha' \in \Delta(\mathcal{A})$ such that $w(\alpha') = w(\alpha)$ and we can write $x^\alpha$ in a unique way as*

$$x^{\alpha'} + \sum_{\gamma \in \Delta(\mathcal{A}),\ w(\gamma) < w(\alpha)} c_{\alpha\gamma} x^\gamma,$$

*where $c_{\alpha\gamma} \in \mathbb{F}$ for all $\gamma$. Given this representation, define the polynomial*

$$G_\alpha = X^\alpha - X^{\alpha'} - \sum_{\gamma \in \Delta(\mathcal{A}),\ w(\gamma) < w(\alpha)} c_{\alpha\gamma} X^\gamma.$$

*Then $\sigma(I) = \sigma(\mathcal{A})$ and $\{G_\alpha \mid \alpha \in \sigma(\mathcal{A})\ \}$ is a reduced Gröbner basis of $I$.*

**Proof.** See [34, Propositions 13 and 14], [23, Lemma 14], [24, Lemma 5.16], [25, p. 1410-1411] and [27, Proposition 1.15]. The proof in [22, Theorem 3.10] in the rank one case can be generalized to arbitrary well-ordered finitely generated semigroups in a straightforward way. That the coefficient of $x^{\alpha'}$ can be chosen to be 1 is new and is a consequence of Proposition 6.4 on the existence of a normalized basis. $\diamond$

**Remark 10.5** In Proposition 4.8 we have seen that every well-ordered semigroup appears as the value semigroup of an order structure. In particular $\mathbb{F}[\mathbb{N}_0^r]$ which is isomorphic with $\mathbb{F}[T_1, \ldots, T_r]$, is an order domain. Let $\Gamma$ be a finitely generated sub semigroup of $\mathbb{N}_0^r$, with generators $\gamma_1, \ldots, \gamma_m$. Then $\mathbb{F}[\Gamma]$ is an order domain by Remark 4.9, but also by Proposition 2.4, since it is a sub $\mathbb{F}$-algebra of $\mathbb{F}[\mathbb{N}_0^r]$.
The algebra $\mathbb{F}[\Gamma]$ is called a *monomial* algebra. We prefer this terminology above *toric* algebra, since the exponents $\alpha$ have nonnegative integers as coordinates, and the ring $\mathbb{F}[\Gamma]$ is not necessarily normal, see [38, Chap. 13]. Let $w : \mathbb{N}_0^m \rightarrow \mathbb{N}_0^r$ be the morphism of semigroups defined by $w(\alpha) = \sum_{i=1}^m \alpha_i \gamma_i$ as before. Define the ideal $I(\Gamma)$ in $\mathbb{F}[X_1, \ldots, X_m]$ by

$$I(\Gamma) = \{\ X^\alpha - X^\beta \mid w(\alpha) = w(\beta) \text{ for } \alpha, \beta \in \mathbb{N}_0^m\ \}.$$

Then $I(\Gamma)$ is called the *binomial ideal* or *toric ideal* of the monomial algebra. The following proposition states that $\mathbb{F}[X_1, \ldots, X_m]/I(\Gamma)$ is an order domain isomorphic with $\mathbb{F}[\Gamma] \cong \mathbb{F}[T^{\gamma_1}, \ldots, T^{\gamma_r}]$ and with Theorem 10.4 we conclude that $I(\Gamma)$ has $\{\ X^\alpha - X^{\alpha'} \mid \alpha \in \sigma(I)\ \}$ as a reduced Gröbner basis, but this theorem does not give an algorithm to compute $\sigma(I)$. This will be the content of the following proposition. Let $<_{lex}$ be the order on $\mathbb{N}_0^r \oplus \mathbb{N}_0^m$ defined in Example 7.3 such that the order on $\mathbb{N}_0^r$ is the lexicographic order and $\prec_w$ is the order on $\mathbb{N}_0^m$.

**Proposition 10.6** *With the above notation we have that* $\mathbb{F}[X_1, \dots, X_m]/I(\Gamma)$ *is an order domain isomorphic with* $\mathbb{F}[\Gamma] \cong \mathbb{F}[T^{\gamma_1}, \dots, T^{\gamma_r}]$ *with a weight function* $\sigma$ *such that* $\sigma(x_i) = w(X_i)$ *for all* $i$*, and value semigroup equal to* $\Gamma$*. Apply Buchberger's algorithm to produce a Gröbner basis* $\mathcal{G}$ *of the ideal generated by*

$$T^{\gamma_1} - X_1, \dots, T^{\gamma_m} - X_m$$

*with respect to* $<_{lex}$*. Let* $\mathcal{G}_X = \mathcal{G} \cap \mathbb{F}[X_1, \dots, X_m]$*. Then* $\mathcal{G}_X$ *is a Gröbner basis of* $I(\Gamma)$ *with respect to* $\prec_w$*.*

**Proof.** See [13, Proposition I.6.2], and Lemma 4.1 and Algorithm 4.5 of [38]. It is used that $<_{lex}$ is a so called *elimination order* , see [9, Chap. 3 §3] and [10, 15.10.4]. That $\mathbb{F}[\Gamma]$ has a finite presentation is also shown in [15]. ⋄

**Remark 10.7** Since we have a found in Theorem 10.4 a Gröbner basis for the defining ideal of a finitely generated order domain, we can apply Schreyer's procedure, see [37] and [10, Theorem 15.5], to get the *syzygies* of the order domain. See [8] for the syzygies of monomial algebras.

# 11 The dimension of order domains

The dimension of a ring can be given in many different ways, such as the Krull dimension, by means of the transcendence degree or with the help of Hilbert functions. For affine domains over a field these definitions all agree. See [10, Chap. 8].

In this section we will show that the dimension of an order with a finitely generated semigroup is equal to the rank of the value semigroup. Although this theorem looks rather obvious at first sight, there are several pitfalls one must circumvent.

**Definition 11.1** Let $R$ be a ring. Then the *Krull dimension* of $R$ is the length $d$ of the longest chain

$$\mathcal{P}_0 \subset \mathcal{P}_1 \subset \cdots \subset \mathcal{P}_d$$

of $d + 1$ mutually distinct prime ideals in $R$, and is denoted by $\dim R$.

Let $R$ be a ring, then

$$\dim R = \sup\{ \dim R_{\mathcal{P}} \mid \mathcal{P} \text{ a prime ideal in } R \},$$

where $R_{\mathcal{P}}$ is the localization of $R$ at $\mathcal{P}$. See [10, Ch. 8].

**Definition 11.2** The *transcendence degree* $\text{tr.deg.}_{\mathbb{F}} R$ of an affine domain $R$ over a field $\mathbb{F}$ is the transcendence degree of $\mathbb{Q}(R)$ over $\mathbb{F}$, where $\mathbb{Q}(R)$ is the field of fractions of $R$. See [10, Appendix A.1] and [9, Ch. 9, §5 Definition 8].

If $R$ is an affine domain over a field $\mathbb{F}$, then $\dim R = \text{tr.deg.}_{\mathbb{F}}$. See [10, Theorem A, page 286]

**Proposition 11.3** *The dimension of an order domain is at least the rank of the value semigroup.*

**Proof.** Let $r$ be the rank of the value semigroup $\Gamma$ of the order domain $R$. Then we can find elements $\gamma_1, \dots, \gamma_r \in \Gamma$ that are independent in $\mathbb{Q}(D(\Gamma))$ over $\mathbb{Q}$. So $\mathbb{N}_0\langle \gamma_1, \dots, \gamma_r \rangle$ is isomorphic to $\mathbb{N}_0^r$. Choose $x_1, \dots, x_r \in R$ such that $\rho(x_i) = \gamma_i$ for all $i$. Let $S = \mathbb{F}[x_1, \dots, x_r]$. Then $S$ is a subring of $R$ and is isomorphic to the polynomial ring $\mathbb{F}[X_1, \dots, X_r]$. Hence

$$r = \text{tr.deg.}_{\mathbb{F}} S \leq \text{tr.deg.}_{\mathbb{F}} R.$$

◇

The following proposition holds in greater generality as we will see in Theorem 11.9. We have included this formulation since its proof is elementary. The general proof needs the theory of *Hilbert functions.*

**Proposition 11.4** *Let $(R, \rho, \Gamma)$ be a finitely generated order structure such that the well-order on $\Gamma$ is isomorphic with the natural numbers. Then the dimension of $R$ is equal to the rank of $\Gamma$.*

**Proof.** We may assume by Theorem 5.6 that $\Gamma$ is a sub semigroup of $\mathbb{N}_0^r$, where $r$ is the rank of $\Gamma$, since $\Gamma$ is finitely generated. The well-order $<$ on the value semigroup is induced by a well-order on $\mathbb{N}_0^r$ and these are all classified in [31, 32] and mentioned in Remark 4.10. That is to say we can

find $\mathbf{a}_1, \ldots, \mathbf{a}_r$ in $\mathbb{R}^r$ such that for $\mathbf{a}, \mathbf{b} \in \mathbb{N}_0^r$: $\mathbf{a} < \mathbf{b}$ if and only if there exists a $t$ such that $\mathbf{a}.\mathbf{a}_i = \mathbf{b}.\mathbf{a}_i$ for all $i < t$ and $\mathbf{a}.\mathbf{a}_t < \mathbf{b}.\mathbf{a}_t$. Here $\mathbf{a}.\mathbf{b}$ means the standard innerproduct.
Now the order $<$ is isomorphic to the natural numbers if and only if the coordinates of $\mathbf{a}_1$ are all positive. See [27, Example 1.3].
Define

$$R(n) = \{f \in R \mid \rho(f).\mathbf{a}_1 \leq n\}.$$

Then $R(n)$ is a vector space over $\mathbb{F}$ and its dimension is at most equal to the number of integral points $\mathbf{b} \in \mathbb{N}_0^r$ such that $\mathbf{b}.\mathbf{a}_1 \leq n$.
Suppose that $\text{tr.deg.}_{\mathbb{F}} R = s$, then there exists a transcendence basis $x_1, \ldots, x_s$ of $R$. Let

$$b = \max\{\ \rho(x_i).\mathbf{a}_1 \mid \text{ for all } i = 1, \ldots, s\ \}.$$

Then $R(b)$ contains $x_1, \ldots, x_s$ and $R(bn)$ contains all monomials in $x_1, \ldots, x_s$ of degree at most $n$. These are independent and the number of these is

$$\binom{n+s}{s} = \frac{n^s}{s!} + \text{ lower order terms in } n$$

which is a polynomial in $n$ of degree $s$. Hence the dimension of $R(bn)$ is bounded from below by a polynomial in $n$ of degree $s$.
Now $\mathbf{a}_1$ is a vector with positive coordinates. Let $c$ be the minimum of all the coordinates of $\mathbf{a}_1$. Then $c > 0$.
The set of all $\mathbf{b} \in \mathbb{N}_0^r$ such that $\mathbf{b}.\mathbf{a}_1 \leq bn$ is included in the multi-cube of all all $\mathbf{b} \in \mathbb{N}_0^r$ such that $b_i \leq bn/c$ for all $i$. The dimension of $R(bn)$ is at most the number of integral points in this multi-cube which is at most $(1+bn/c)^r$. Hence the dimension of $R(bn)$ is bounded from above by a polynomial in $n$ of degree $r$. Therefore $s \leq r$. Proposition 11.3 gives $s \geq r$. $\diamond$

**Definition 11.5** See [27, Definition 2.3]. Let $R$ be an order domain with order function $\rho$. A *monomial basis* is a set of elements $x_1, \ldots, x_r$ in $R$ such that $x_1, \ldots, x_r$ is a transcendence basis of $R$ and the order of the monomials in $x_1, \ldots, x_r$ are mutually distinct, that is to say $\rho$ is injective on the set $\{\ x^\alpha \mid \alpha \in \mathbb{N}_0^r\ \}$.

**Remark 11.6** We want to show Theorem 11.9 that the dimension of an order domain is equal to the rank of the value semigroup. In case $R$ is a semigroup algebra, this is well-known and not difficult to show. In general

we have to assume that the semigroup is finitely generated as Example 9.6 from [27, Example 5.2], of an order function on $\mathbb{F}[X,Y]$ with a semigroup in $\mathbb{Q}$ of rank 1 shows us.
One might think that any transcendence basis of an affine order domain is monomial. But Example 9.5 shows us that this is not the case. If $\Gamma$ has rank $r$, then there exist elements $\gamma_1, \ldots, \gamma_r$ that are independent. Take $x_1, \ldots, x_r$ such that $\rho(x_i) = \gamma_i$. Then the order of the monomials in $x_1, \ldots, x_r$ are mutually distinct, by definition. Hence the sub ring $\mathbb{F}[x_1, \ldots, x_r]$ is isomorphic to the polynomial ring in $r$ variables, as we have seen in Proposition 11.3. But it is not clear whether $x_1, \ldots, x_r$ is a transcendence basis. If we could choose $x_1, \ldots, x_r$ in such a way that $R$ is finitely generated as a module over the sub ring $\mathbb{F}[x_1, \ldots, x_r]$, then $\mathbb{Q}(R)$ is a finite field extension of the field of rational functions $\mathbb{F}(x_1, \ldots, x_r)$, by [10, Corollary 4.5], thus we would have shown the theorem. But it is not clear whether this is always possible.

We will show the theorem by means of the theory of Hilbert functions. In our set up the existence of a monomial basis will be Corollary 11.11.

**Definition 11.7** Let $(A, \mathcal{M}, \mathbb{F})$ be a *local ring*, that is to say $\mathcal{M}$ is the unique maximal ideal of the ring $A$ and $A/\mathcal{M} = \mathbb{F}$ is the *residue field*. The *Hilbert functions* $H$ and $h$ of $(A, \mathcal{M}, \mathbb{F})$ are defined by

$$H(n) = \dim_{\mathbb{F}} A/\mathcal{M}^{n+1},$$

$$h(n) = \dim_{\mathbb{F}} \mathcal{M}^n/\mathcal{M}^{n+1}.$$

**Remark 11.8** Let $(A, \mathcal{M}, \mathbb{F})$ be a local ring with Hilbert functions $H$ and $h$, then $H(n) = \sum_{m \leq n} h(m)$ and then there exist (unique) polynomials $P(T), p(T) \in \mathbb{Z}[T]$ such that $H(n) = P(n)$ and $h(n) = p(n)$ for all large $n \in \mathbb{N}$. So the degree of $H$ and $h$ is well defined. We have that

$$\dim A = \deg P = 1 + \deg p$$

whenever $(A, \mathcal{M}, \mathbb{F})$ is a Noetherian local ring. See [10, Theorem 12.1].

**Theorem 11.9** *Let $(R, \rho, \Gamma)$ be a finitely generated order structure over a field $\mathbb{F}$. Then the dimension of $R$ is equal to the rank of $\Gamma$.*

**Proof.** Let $(R, \rho, \Gamma)$ be a finitely generated order structure. Then we may assume that $\Gamma$ is embedded in $\mathbb{N}_0^r$ as an ordered semigroup, where $r$ is the rank of $\Gamma$ by Theorem 5.6.
We may assume without loss of generality that $\mathbb{F}$ is algebraically closed by Proposition 3.4 on the extension of scalars.
Let $\mathcal{M}$ be a maximal ideal of $R$. Then $R/\mathcal{M} = \mathbb{F}$ by Hilbert's Nullstellensatz [10, Theorem 4.19].
Theorem 8.3 on Gröbner bases gives that the size of the delta set of $\mathcal{M}$ is the dimension of $R/\mathcal{M}$ which is 1. Furthermore $\rho(f) \neq 0$ for all $f \in \mathcal{M}$, otherwise $\mathcal{M}$ contains a unit. Hence the delta set of $\mathcal{M}$ is equal to $\{0\}$ and $\Sigma(\mathcal{M}) = \{\rho(f) \mid 0 \neq f \in \mathcal{M}\ \} = \Gamma \setminus \{0\}$.
Let $\mathbf{a}_1, \dots \mathbf{a}_m$ be a set of generators of $\Gamma$. We can choose $x_1, \dots, x_m \in \mathcal{M}$ such that $\rho(x_i) = \mathbf{a}_i$ for all $i$. We proceed as in Theorem 10.4 on the presentation of $R$. We identify $R$ with $\mathbb{F}[X_1, \dots, X_m]/I$ where $I$ has Gröbner basis $\{\ G_\alpha \mid \alpha \in \sigma(\mathcal{A})\ \}$ and $\Delta(\mathcal{A})$ is the delta set of $I$. Now the $x_1, \dots, x_m$ generate the ideal $\mathcal{M}$. Hence the monomials $x^\alpha$ with $\deg(\alpha) = n$ generate the ideal $\mathcal{M}^n$. So the monomials $x^\alpha$ with $\deg(\alpha) \leq n$ generate $R/\mathcal{M}^{n+1}$ as a vector space over $\mathbb{F}$. Now the monomials $x^\alpha$ such that $\alpha \in \Delta(\mathcal{A})$ form a basis for $R$ over $\mathbb{F}$. Therefore the monomials $x^\alpha$ such that $\alpha \in \Delta(\mathcal{A})$ and $\deg(\alpha) \leq n$ generate $R/\mathcal{M}^{n+1}$ as a vector space over $\mathbb{F}$. The restriction of the weight function $w$ to $\Delta(\mathcal{A})$ is injective by definition of $\Delta(\mathcal{A})$. So the dimension of $R/\mathcal{M}^{n+1}$ is at most equal to the number of elements in the set

$$\Delta(\mathcal{A}, n) = \{\ w(\alpha) \mid \alpha \in \Delta(\mathcal{A}),\ \deg(\alpha) \leq n\ \}.$$

Let $N = \max\{\ a_{ij} \mid i = 1, \dots, r,\ j = 1, \dots, m\ \}$. Then $\Delta(\mathcal{A}, n)$ is contained in the multi-cube $\{\mathbf{b} \in \mathbb{N}_0^r \mid b_i \leq N \text{ for all } i\ \}$ which has $(N(n+1))^r$ elements. The dimension of $R_{\mathcal{M}}/(\mathcal{M}R_{\mathcal{M}})^{n+1}$ is at most the dimension of $R/\mathcal{M}^{n+1}$. Hence $H(n) \leq (N(n+1))^r$. So the degree of $H$ is at most $r$, since $N$ is independent of $n$. Therefore the dimension of $(R_{\mathcal{M}}, \mathcal{M}R_{\mathcal{M}}, \mathbb{F})$ is at most $r$ for every maximal ideal of $R$. So the dimension of $R$ is at most $r$, by [10, Theorem 12.1]. We have already seen in Proposition 11.3 that the dimension of $R$ is at least $r$. ◇

**Remark 11.10** The special case of Theorem11.9 where the transcendence degree of $R$ is at least 2 and $\Gamma$ is a numerical semigroup is excluded by [27, Proposition 4.2], [21, Theorem 1], and [13, Theorem I.9.1].

**Corollary 11.11** *A finitely generated order structure has a monomial basis.*

**Proof.** We have seen in Proposition 11.3 that we can find $x_1, \ldots, x_r \in R$ such that $\rho(x_1), \ldots, \rho(x_r)$ are independent and $\mathbb{F}[x_1, \ldots, x_r]$ is isomorphic to the polynomial ring in $r$ variables, where $r$ is the rank of $\Gamma$. Hence they are transcendent over $\mathbb{F}$. Theorem 11.9 gives that the transcendence degree of $R$ is $r$. Hence $x_1, \ldots, x_r$ is a transcendence basis of $R$. The map $\rho$ is injective on the monomials in $x_1, \ldots, x_r$, since $\rho(x_1), \ldots, \rho(x_r)$ are independent. Therefore they form a monomial basis. $\diamond$

**Remark 11.12** Let $\rho$ be a weight function of rank $r$ on an order domain $R$. So the value semigroup $\Gamma$ is a sub semigroup of $\mathbb{N}_0^r$, but it is not necessarily finitely generated. We leave it as an open question whether also in this case the rank of $\Gamma$ is equal to the dimension of $R$.

# References


[1] W.W. Adams and P. Loustaunau, *An introduction to Gröbner bases,* Grad. Studies in Math., vol. 3, Amer. Math. Soc., 1994.

[2] P. Beckmann and J. Stückrad, "The concept of Gröbner algebras," *J. Symbolic Computation,* vol. 10, pp. 465-479, 1990.

[3] E.R. Berlekamp, *Algebraic coding theory*, McGraw-Hill, New York, 1968.

[4] N. Bourbaki, *Elements of mathematics. Algebra,* Hermann, Paris, Addison-Wesley, Massachusetts, 1972.

[5] N. Bourbaki, *Elements of mathematics. Commutaive algebra,* Hermann, Paris, Addison-Wesley, Massachusetts, 1972.

[6] W. Bruns and J. Herzog, *Cohen-Macaulay rings,* Cambridge Stud. in Advanced Math. vol. 39, Cambridge Univ. Press 1993.

[7] B. Buchberger, *Ein Algorithmus zum Auffinden der Basiselemente des Restklassenringes nach einem nulldimensionalen Polynomideal*, Ph.D. thesis, Univ. of Innsbruck, Austria, 1965.

[8] A. Campillo and P. Gimenez, "Syzygies of affine toric varieties," *Journ. Algebra,* vol. 225, pp. 142-161, 2000.

[9] D. Cox, J. Little and D. O'Shea, *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry*, Springer-Verlag, New York 1992.

[10] D. Eisenbud, *Commutative algebra with a view towards algebraic geoemtry,* Grad. Texts in Math. vol. 150, Springer-Verlag, New York 1995.

[11] O. Endler, *Valuation theory,* Universitext, Springer-Verlag, Berlin 1972.

[12] G.-L. Feng and T.R.N. Rao, "A simple approach for construction of algebraic-geometric codes from affine plane curves," *IEEE Trans. Inform. Theory*, vol. 40, pp. 1003-1012, July 1994.

[13] O. Geil, *Codes based on an* $\mathbb{F}_q$*-algebra,* Ph.D. Thesis, Aalborg Univ., Denmark, December 1999.

[14] O. Geil, "On the construction of codes from order domains," submitted to *IEEE Trans. Inform. Theory.*

[15] J. Herzog, "Generators and relations of abelian semigroups and semigroup rings," *Manuscripta Math.,* vol. 3, pp. 175-193, 1970.

[16] T. Høholdt and R. Pellikaan, "On decoding algebraic-geometric codes," *IEEE Trans. Inform. Theory,* vol. 41, pp. 1589-1614, 1995.

[17] T. Høholdt, J.H. van Lint and R. Pellikaan, "Algebraic geometry codes," in *Handbook of Coding Theory*, (V.S. Pless and W.C. Huffman Eds.), vol 1, pp. 871-961, Elsevier, Amsterdam 1998.

[18] C. Kirfel and R. Pellikaan, "The minimum distance of codes in an array coming from telescopic semigroups," *IEEE Trans. Inform. Theory,* vol. 41, pp. 1720-1732, 1995.

[19] S. Lang, *Algebra,* Addison-Wesley Publ. Co., Reading Massachusetts, 1965.

[20] J.L. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inform. Theory*, vol. 15, pp. 122-127, Jan. 1969.

[21] R. Matsumoto, "Miura's generalization of one-point AG codes is equivalent to Høholdt, van Lint and Pellikaan's generalization," *IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences,* vol. E82-A, no.10, pp. 2007-2010, October 1999.

[22] R. Matsumoto and S. Miura, "On construction and generalization of algebraic geometry codes," *Proc. Algebraic Geometry, Number Theory, Coding Theory and Cryptography.* (T. Katsura, T. Okamoto, S. Miura, and H. Hiramatsu, Eds) Jan. 19-20, 2000, Univ. of Tokyo, pp. 3-15.

[23] S. Miura, "Constructive theory of algebraic curves," *Proc. 17 th Symp. Inform. Theory and its Applications* (Hiroshima, Japan), December 1994, pp. 461-464 (Japanese).

[24] S. Miura, Ph.D. Thesis, Univ. Tokyo, May 1997 (Japanese).

[25] S. Miura, "Linear codes on affine algebraic curves," *Trans. IEICE,* vol. J81-A, no. 10, pp.1398-1421, 1998 (Japanese).

[26] M.E. O'Sullivan, "Decoding of codes defined by a single point on a curve," *IEEE Trans. Inform. Theory*, vol. 41, pp. 1709-1719, Nov. 1995.

[27] M.E. O'Sullivan, "New codes for the Berlekamp-Massey-Sakata algorithm," *Finite Fields and their Applications,* vol. 7, pp. 293-317, 2001.

[28] R. Pellikaan, "On the existence of order functions," in Proc. 2nd Shanghai Conference on Designs, Codes and Finite Geometries, May 1996, as a special issue of *Journal of Statistical Planning and Inference,* vol. 94, pp. 287-301, 2001.

[29] S.C. Porter, B.-Z. Shen and R. Pellikaan, "Decoding geometric Goppa codes using an extra place," *IEEE Trans. Inform. Theory,* vol. 38, pp. 1663-1676, 1992.

[30] L. Rédei, *The theory of finitely generated commutative semigroups,* Pergamon Press, 1965.

[31] L. Robbiano, "Term orderings on the polynomial ring," in Eurocal 1985 (B. Buchberger, C. Caviness eds.) *Lect. Notes Comp. Sc.,* vol. 204, pp.513-517, 1985.

[32] L. Robbiano, "On the theory of graded structures," *J. Symbolic Computation,* vol. 2, pp. 139-170, 1986.

[33] J.G. Rosenstein, *Linear orderings,* Acad. Press, 1982.

[34] K. Saints and C. Heegard, "Algebraic-geometric codes and multidimensional cyclic codes," *IEEE Trans. Inform. Theory,* vol. 41, pp. 1733-1751, 1995.

[35] S. Sakata, "Extension of the Berlekamp-Massey algorithm to N dimensions," *Information and Computation*, vol. 84, pp. 207-239, 1990.

[36] G. Schiffels, "Orderings and algorithms in commutative algebra," *Afrika Mathematika,* Series 3, vol. 2, pp. 79-101, 1993.

[37] F.-O. Schreyer, *Die Berechnung von Syzygien mit dem veralgemeinerten Weierstrass'chen Divisionssatz,* Diplom Thesis, Univ. Hamburg, 1980.

[38] B. Sturmfels, *Gröbner bases and convex polytopes,* Univ. Lect. Series vol. 8, Amer. math. Soc., Providence, Rhode Island, 1996.

[39] O. Zariski and P.Samuel, *Commutative algebra,* vol I, Van Nostrand, London 1958.

[40] O. Zariski, "The reduction of singularities of an algebraic surface," *Ann. of Math.* vol. 40, pp. 639-689, 1939.

[41] G. Ziegler, *Lectures on polytopes,* Grad. Texts in Math. vol. 152, Springer, New York 1995.