Ioana Cristina Serban

One-dimensional local rings and canonical ideals

Dottorato in Matematica, Roma «La Sapienza» (2006).

<http://www.bdim.eu/item?id=tesi_2006_SerbanIoanaCristina_1>

ONE-DIMENSIONAL LOCAL RINGS AND CANONICAL IDEALS

Ioana Cristina Şerban

PhD thesis in Pure Mathematics
supervisor: Valentina Barucci

Università di Roma “La Sapienza”, Dip. di Matematica, 2006.

PREFACE

This PhD thesis in Pure Mathematics contains both a general overview and some original research results about one-dimensional local analytically irreducible rings. The questions investigated in this work concern with *canonical ideals*, *Apèry Basis* and the growth of the *Hilbert function*.

An interesting problem is to find (suitable) characterizations of canonical ideals. Under various assumptions on the ring, this has been succesfully achieved. One of the assumptions which is often imposed is *residual rationality*, i.e. that the residue class field of the ring coincides with that of its integral closure. Untill now, the case of residually non (necessarily) rational rings was somewhat less studied.

One of the main results of this thesis is a generalization of a characterization which (previously) regarded the residually rational case, only. This result is achieved by considering a new construction.

Many questions regarding residually rational rings are answered by considering their *value semigroup*, which is a numerical semigroup associated to the ring. However, this semigroup turns out to reveal much less, when the assumption of residual rationality is dropped. In order to treat the general case, instead of a numerical semigroup, we shall associate to the ring a so-called *generalized semigroup ring*.

Apart from results concerning canonical ideals, this newly introduced associated object can help to generalize other results, too. For example, a generalization will be given of a construction (originally given in the residually rational case) of a so-called Apéry Basis.

The last chapter regards a conjecture of Sally about the growth of the Hilbert function of a one dimensional local CM ring of small embeddding dimension. In this thesis only the case of a semigroup ring is investigated. In particular, it will be shown that the conjecture is true for semigroup rings of embedding dimension three.

The case of embedding dimension three has been already proved in a somewhat more general context. However, the proof presented in this thesis is different from the previously known one, and it was found independently. Moreover, it is also much more "elementary" (but of course it covers only a less general case).

The result regarding the characterization of canonical ideals forms the base of a single-author work submitted for publication to the journal "Communications in Algebra".

Contents

Chapter 1

One dimensional CM rings and canonical ideals

1.1 Canonical ideals

§1. In this thesis the word "**ring**" stands for a *commutative* algebraic structure with *identity* satisfying the usual requirements. We shall be mainly occupied with canonical ideals of one-dimensional Cohen-Macaulay (CM) rings. A good introduction to one-dimensional (local) CM rings can be found in the book [M] of Matlis. However, the reference which will appear here most often is the book [HK] of Kunz and Herzog, which was published some two years after the other mentioned book. (Both of them are from the beginning of the 70's).

The ring R is said to be **local** if it has a unique maximal ideal $\mathfrak{m} \subset R$, and **one-dimensional** if the maximal length of a chain of prime ideals of R is one. In this case the **CM property** simply means that $\mathfrak{m}$ contains a nonzero divisor. We shall denote by $k = R/\mathfrak{m}$ the residue class field and by $Q(R)$ the total ring of fractions of R.

For two fractional ideals $F_1, F_2 \subset Q(R)$ of R, the **quotient** is defined by the formula

$$(F_1 : F_2) := \{x \in Q(R) | \;\; xF_2 \subseteq F_1\}. \tag{1.1}$$

Note that the quotient $(F_1 : F_2)$ is not necessarily a fractional ideal; e.g. $F : 0 = Q(R)$. Nevertheless, it is easy to see, that if F_2 contains a nonzero divisor , then $(F_1 : F_2)$ is again a fractional ideal. (We call **nonzero divisor** an element from F such that its product with every nonzero element of R is again non zero.) Note also that a fractional ideal F of R contains a nonzero divisor if and only if $FQ(R) = Q(R)$. We shall call **regular** the fractional ideals of R which contain a nonzero divisor.

From the definition of the quotient operation it follows, that with F and H (with and without indices) being fractional ideals of R, we have:

1. if $F_1 \subseteq F_2$ then $(F_1 : H) \subseteq (F_2 : H)$ while if $H_1 \subseteq H_2$ then we have the "inverted" relation $(F : H_1) \supseteq (F : H_2)$,
2. $(F : R) = F$,
3. $((F : H_1) : H_2) = (F : H_1 H_2)$ where $H_1 H_2$ is the product of the two fractional ideals i.e. all possible finite sums of elements of the form $h_1 h_2$ where $h_1 \in H_1$ and $h_2 \in H_2$,
4. $H \subseteq (F : (F : H))$.

With respect to the last listed property, it is important to mention that easy examples show, that in general the relation between H and $F : (F : H)$ is really just an inclusion (and not equality). In connection of sums and intersections, the quotient of fractional ideals has the following properties:

$$\begin{aligned} F : \sum_{i\in I}(F_i) &= \cap_{i\in I}(F : F_i); \\ F : \cap_{i\in I} F_i &\supseteq \sum_{i\in I}(F : F_i) \end{aligned} \tag{1.2}$$

where F and F_i are fractional ideals of R and the index set $I \subset \mathbb{N}$ is finite.

Certain quotients are of particular interest. For a fractional ideal F of R, the quotient $0 : F$ is called the **annulator** of F, and it is denoted by $Ann(F)$. The fractional ideal $R : F$ is called the **inverse** of F, and it is denoted by F^{-1}.

For shortening formulae, sometimes we shall use the following notation:

$$(F_1 : F_2)_M \equiv (F_1 : F_2) \cap M, \tag{1.3}$$

where M is a set with or without an algebraic structure. Note that if $(F_1 : F_2)$ is a fractional ideal of R, then $(F_1 : F_2)_R$ is actually an *ideal* (i.e. not only fractional ideal) of R.

One-dimensional local CM rings are especially "good" in the sense that we can define for them not only a canonical module but also a *canonical ideal* which is a more simple object being a fractional ideal. So following [HK], we shall introduce the notion of canonical ideal — rather than a special case of canonical modules — in its own. (See a short explanation how this definition can be obtained from the general one at paragraph 3 of this section.)

Let R be a one-dimensional (local) CM ring.

Definition 1.1.1. *A regular fractional ideal $\omega \subset Q(R)$ is called a* **canonical ideal** *of R if it plays the role of an "identity" in the sense that it satisfies the equality*

$$\omega : (\omega : F) = F \tag{1.4}$$

for every regular fractional ideal $F \subset Q(R)$.

From the definition, it follows easily that if ω is a canonical ideal of R, then

1. $\omega : \omega = R$,

2. For two regular fractional ideals F_1 and F_2 , $F_1 = F_2$ if and only if $\omega : F_1 = \omega : F_2$,

3. With $\ell_R(\cdot)$ denoting the length (over R) of an R-module,
$$\ell_R(F_1/F_2) = \ell_R(\omega : F_2/\omega : F_1), \tag{1.5}$$
for every two regular fractional ideals F_1 and F_2 such that $F_2 \subset F_1$.

There are some further interesting properties of canonical ideals that follow somewhat less directly from definition. Recall that a fractional ideal $F \subset Q(R)$ is called **irreducible** if $F = H_1 \cap H_2$ (where H_1 and H_2 are fractional ideals) implies that either $F = H_1$ or $F = H_2$. In [HK] there exists the following proposition:

Proposition 1.1.2 (Herzog). *Every canonical ideal of a local ring is irreducible.*

Proof. Let ω be a canonical ideal of the local ring R, and suppose that
$$\omega = F_1 \cap F_2, \tag{1.6}$$
where F_1 and F_2 are two fractional ideals of R. Note that by the definition of canonical ideals, from the above equation it follows that both F_1 and F_2 must contain a nonzero divisor i.e. are regular fractional ideals.

Using the mentioned properties of canonical ideals and the property expressed by equation (1.2) regarding quotients, we have that
$$\omega : ((\omega : F_1) + (\omega : F_2)) = (\omega : (\omega : F_1)) \cap (\omega : (\omega : F_2)) = F_1 \cap F_2 = \omega. \tag{1.7}$$
However, $\omega : \omega = R$, and thus
$$(\omega : F_1) + (\omega : F_2) = R. \tag{1.8}$$
But as R is local, either $\omega : F_1$ or $\omega : F_2$ must be equal to R, which in turn is equal to $\omega : \omega$. This means that either $\omega = F_1$ or $\omega = F_2$. $\square$

A little observation is that in fact it is possible to show using the same argument as in the proof of Proposition 1.1.2 that a canonical ideal ω of the ring R is *completely irreducible* i.e. if $\omega = \cap_{i \in I} F_i$, where $\{F_i\}_{i \in I}$ is any family of fractional ideals, then $\omega = F_j$ for some $j \in I$.

§2. In this paragraph the context is more general. Consider a d-dimensional local Noetherian ring $(R, \mathfrak{m})$ and a finitely generated non zero R-module, M. An **M-sequence** is a sequence of elements $x_1, \dots, x_s$ of R, such that
1. $(x_1, \dots, x_s)M \neq M$, and
2. x_{i+1} is a nonzero divisor on the quotient module $M/(x_1, \dots, x_i)M$ for $0 \leq i \leq s-1$.
For $M = R$ an R-sequence is called a *regular sequence*. For an R-module M we can define an important invariant, namely the **depth** of M,

$$\mathrm{depth} M := \text{length of a maximal } M \text{ sequence in } \mathfrak{m} \tag{1.9}$$

A good introduction into the fundamental notions of commutative algebra is the first Chapter of the book of Bruns and Herzog, [BH]. Depth of an R-module M can be computed using the next theorem from [BH], which is in fact a corollary to a theorem of Rees.

Theorem 1.1.3. *With the previous notations*

$$\mathrm{depth} M = \min\{i | \ \mathrm{Ext}^i_R(k, M) \neq 0\}. \tag{1.10}$$

Using this theorem we can define another important invariant of an R-module M which is the **type** of M. The type of M refines the information given by the depth.

Definition 1.1.4. *Let M be a non zero finitely generated module of depth t. The* **type** *of M is*

$$\mathrm{type}(M) := \dim_k \mathrm{Ext}^t_R(k, M). \tag{1.11}$$

One can prove that

$$\mathrm{type}(M) = \dim_k \mathrm{Soc}(M/\underline{x}M), \tag{1.12}$$

where $\underline{x} = \{x_1, x_2, \dots, x_t\}$ is a maximal M-sequence in $\mathfrak{m}$ and the socle of an R-module M is defined:

$$\mathrm{Soc}(M) := (0 : \mathfrak{m})_M = \{x \in M | \ x\mathfrak{m} = 0\} \simeq \mathrm{Hom}_R(k, M). \tag{1.13}$$

Add the hypothesis that the ring R is CM. (Here CM-ness means that $\dim R = \mathrm{depth} R$.) One can define also **CM modules**. An R-module M is called CM if $\dim M = \mathrm{depth} M$, where the dimension of the R-module M is the dimension of the ring $R/\mathrm{Ann}_R(M)$, $\mathrm{Ann}_R(M) = (0 : M)_R$. A **maximal CM R-module** is a CM R-module with the property that $\dim M = \dim R$.

The CM rings of type 1 have interesting properties. We shall call these rings **Gorenstein**. These rings play an important role in our study.

For the ring R a canonical module is defined in the following manner (see [BH]):

Definition 1.1.5. *A maximal CM module Ω of type 1 and of finite injective dimension is called a canonical module of R*

One can find many details about this topic in [BH]. What interests us is only the relation between a canonical module and a canonical ideal in the case of a one-dimensional local CM ring. For investigate this we shall use the following characterization of a canonical module taken from [BH].

Proposition 1.1.6. *Let Ω be an R-module. Then Ω is a canonical module of R if and only if for all maximal CM R-modules M the natural homomorphism*

$$M \to \mathrm{Hom}_R(\mathrm{Hom(M,\Omega)},\Omega) \tag{1.14}$$

is an isomorphism.

The next theorem whose proof can be find in [HK] gives a sufficient and necessary condition for which a canonical module is a fractional ideal.

Theorem 1.1.7. *For the ring R with the property that it has a canonical module, Ω, the following conditions are equivalent:*

1. *For every minimal prime ideal $\mathfrak{p}$ of R, $R_{\mathfrak{p}}$ is a Gorenstein ring;*

2. *Ω is a fractional ideal of R;*

3. *Ω is a fractional ideal of R which contains a nonzero divisor of R.*

§3. Return to the one-dimensional local CM ring R. In this case a regular fractional ideal of R is a maximal CM R-module. And we can show that between the quotient of regular fractional ideals $(F_1 : F_2)$ defined by equation 1.1 and $\mathrm{Hom}_R(F_2, F_1)$, there exists an isomorphism. Let Φ the R-homomorphism

$$\Phi : (F_1 : F_2) \to \mathrm{Hom}_R(F_2, F_1), \tag{1.15}$$

which sends every $x \in (F_1 : F_2)$ in the multiplication with x in $\mathrm{Hom}_R(F_2, F_1)$.

Lemma 1.1.8. Φ *is an isomorphism of R-modules.*

Proof. We shall construct an inverse of Φ. Let $\psi \in \mathrm{Hom}_R(F_2, F_1)$. Because of the fact that $F_2 Q(R) = Q(R)$ we can extend ψ to all $Q(R)$, for $x \in F_2$ and a nonzero divisor $r \in R$:

$$\overline{\psi}(\frac{x}{r}) = \frac{1}{r}\psi(x) \tag{1.16}$$

Consider $\beta = \overline{\psi}(1)$. For every $x \in F_2$ we have $\psi(x) = \overline{\psi}(x) = x\overline{\psi}(1) = x\beta$. (This fact that $\overline{\psi}$ is taking out the elements from F_2 is evident from the definition of $\overline{\psi}$.) Define

$$\Phi' : \mathrm{Hom}_R(F_2, F_1) \to (F_1 : F_2), \tag{1.17}$$

by

$$\Phi'(\psi) = \overline{\psi}(1). \tag{1.18}$$

It is easy to see that Φ' is the inverse of Φ. □

With the same notations as in Lemma 1.1.8 we have the next corollary.

Corollary 1.1.9. *The map*

$$\Psi : (F_1 : (F_1 : F_2)) \to \mathrm{Hom}_R(\mathrm{Hom}_R(F_2, F_1), F_1), \tag{1.19}$$

defined as the composition of the two R morphisms:

$$F_1 : (F_1 : F_2) \to \mathrm{Hom}_R(F_1 : F_2, F_1) \to \mathrm{Hom}_R(\mathrm{Hom}_R(F_2, F_1), F_1), \tag{1.20}$$

is an isomorphism.

Thus we can conclude that if a one-dimensional (local) CM ring R has a canonical module which is a fractional ideal (for example if the ring R satisfies the condition 1 of Theorem 1.1.7) then the canonical module is a canonical ideal.

§4. We shall see from another point of view why is convenient to work with one-dimensional local CM rings. Assume that R is such a ring with the property that has a canonical ideal. We shall give an easy, but useful formula for computing the type of the ring R and also we shall show a correlation between the type of R and a canonical ideal ω of R. First we denote by $\mu(\omega)$ the number of elements in a minimal set of generators of ω. As a consequence of Nakayama's Lemma we have that:

$$\mu(\omega) = \ell_R(\omega/\mathfrak{m}\omega) \tag{1.21}$$

The next proposition is from [HK].

Proposition 1.1.10.

$$\mathrm{type}(R) = \mu(\omega) = \ell_R(\mathfrak{m}^{-1}/R). \tag{1.22}$$

Proof. We shall prove that $\mu(\omega) = \ell_R(\mathfrak{m}^{-1}/R)$. Using the properties of a canonical ideal ω of R and those of the quotient of two ideals we have that:

$$\begin{aligned}\mu(\omega) &= \ell_R(\omega/\mathfrak{m}\omega) = \ell_R((\omega : \mathfrak{m}\omega)/(\omega : \omega)) = \\ &= \ell_R((\omega : \omega) : \mathfrak{m}/(\omega : \omega)) = \ell_R(R : \mathfrak{m}/R).\end{aligned}$$

We know that in general $\mathrm{type}(R) = \dim_k \mathrm{Soc}(R/\underline{x}R)$, where $\underline{x} = (x_1, \ldots, x_t)$ is a regular sequence in $\mathfrak{m}$. Our ring R is one-dimensional and CM then $t = 1$. Therefore $\mathrm{type}(R) = \dim_R \mathrm{Soc}(R/xR)$ where x is a non zero divisor of R in $\mathfrak{m}$. It is easy to see that

$$\mathrm{Soc}(R/xR) = (0 : \mathfrak{m})_{R/xR} \simeq (xR : \mathfrak{m})_R/xR. \tag{1.23}$$

We shall prove that

$$(xR : \mathfrak{m})_R/xR \simeq \mathfrak{m}^{-1}/R. \tag{1.24}$$

Consider

$$\mu_{x^{-1}} : (xR : \mathfrak{m})_R \to \mathfrak{m}^{-1}, \;\; \mu_{x^{-1}}(r) = x^{-1}r. \tag{1.25}$$

$\mu_{x^{-1}}$ is a well defined morphism of R-modules. Let see that it is also surjective. For this, take $y \in \mathfrak{m}^{-1}$, then $xy = r \in R$ and $r\mathfrak{m} = xy\mathfrak{m} \subseteq (x)$. Thus $\mu_{x^{-1}}(r) = y$. Therefore we can define $\widetilde{\mu_{x^{-1}}} : (xR : \mathfrak{m})_R \to \mathfrak{m}^{-1}/R$ which is surjective and $\mathrm{Ker}(\widetilde{\mu_{x^{-1}}}) = xR$. Thus we have the isomorphism (1.24). And this means that

$$\mathrm{type}(R) = \dim_k \mathrm{Soc}(R/xR) = \ell_R(\mathfrak{m}^{-1}/R). \tag{1.26}$$

□

§5. We shall see in this paragraph a characterization of one-dimensional Gorenstein rings. For showing this we need the next theorem which gives some properties of a non necessarily one-dimensional. Gorenstein ring. This theorem and also that about one-dimensional local rings could be find in [HK].

Theorem 1.1.11. *Let R be a CM ring. The following conditions are equivalent:*

i) R is a Gorenstein ring.

ii) For every system of parameters $\underline{x}$ of R we have that

$$\dim_k \mathrm{Soc}(R/(\underline{x})) = 1. \tag{1.27}$$

Theorem 1.1.12. *Let $(R, \mathfrak{m})$ be a one-dimensional local CM ring. Then the following conditions are equivalent:*

1. *R is a Gorenstein ring;*

2. *For every nonzero divisor $x \in \mathfrak{m}$, $\ell_R((xR : \mathfrak{m})_R/xR) = 1$;*

3. *$\ell_R(\mathfrak{m}^{-1}/R) = 1$.*

Proof. $1 \iff 2$
As we have already seen in the proof of Proposition 1.1.10 there exists an isomorphism of R-modules:

$$(xR : \mathfrak{m})_R/(x) \simeq (0 : \mathfrak{m})_{R/xR} \simeq \mathrm{Hom}_{R/xR}(R/\mathfrak{m}, R/xR) \simeq \mathrm{Soc}(R/xR). \tag{1.28}$$

Our ring R is one-dimensional and $x \in \mathfrak{m}$ is a nonzero divisor, thus x is a system of parameters of R. And we conclude the proof of the equivalence using the previous theorem.

$2 \iff 3$
Using again the proof of Proposition 1.1.10 we have that

$$(xR : \mathfrak{m})_R/xR \simeq \mathfrak{m}^{-1}/R. \tag{1.29}$$

And the proof for the equivalence is finished as the previous isomorphism implies that $\ell_R(((x) : \mathfrak{m})/(x)) = \ell_R(\mathfrak{m}^{-1}/R)$. □

§6. So far we have said nothing about the existence of canonical ideals. The natural questions to ask are: does every one-dimensional local ring R has a canonical ideal? "How many" canonical ideals R may have? Is a canonical ideal — at least in some weaker sense — unique?

To answer, let us mention that there are examples of one-dimensional local rings (in fact, even domains!) possessing no canonical ideal, see the remark at the end of [HK, Sect. 2.3]. However, in most cases of interest the existence of a canonical ideal can be established. Before citing the relevant propositions and theorems, recall that the **nilradical** of a ring R is the ideal of R defined by:

$$\mathcal{N} := \{x \in R | \ \exists \ n \in \mathbb{N} \ \ s.t. \ \ x^n = 0\}, \tag{1.30}$$

i.e. it is the union of all **nilpotent** elements. Let us now return to the question of existence.

Theorem 1.1.13. *Let R be a one-dimensional local CM ring which is* reduced *(i.e. $\mathcal{N} = 0$). If there exists a Dedekind ring $P \subseteq R$ such that R becomes a finitely generated P-module, then there exists a canonical ideal of R.*

Proposition 1.1.14. *If a canonical ideal exists for the $\mathfrak{m}$-adic completion $\widehat{R}$ of R, then there exists a canonical ideal of R.*

For proofs of the above statements, see e.g. [HK, Sect. 2.3].

Definition 1.1.15. *R is called* **analytically unramified** *if the $\mathfrak{m}$-adic completion, $\widehat{R}$, of R is a reduced ring.*

Proposition 1.1.16. *If the one-dimensional local CM ring R is analytically unramified, then there exists a canonical ideal of R.*

The proof of the previous proposition relies on an important result of commutative algebra, namely on the theorem of I.S. Cohen regarding the structure of complete local rings. His article ([C]) from 1946 "provides a very thorough insight into the structure of a local ring" (citation from the review of O.Todd-Taussky), and it is a beatiful and essential work for everyone who wants to study local rings. Nevertheless, for some further details on the theorem of Cohen, one may look at the second volume of the book of Zariski and Samuel ([ZS]), and the book of Matsumura ([Ma]).

Theorem 1.1.17 (Cohen). *Every complete local ring is a homomorphic image of a certain type of complete local rings, namely the ring of all power series in a given number of variables with coefficient from a field or from a valuation ring.*

Proof. (of Proposition 1.1.16; addopted from the book [HK].) We know that $\dim\widehat{R} = \dim R = 1$. This implies that also $\widehat{R}$ is a one-dimensional local CM ring which is also reduced. Thus using Proposition 1.1.14 we may reduce the statement to complete local rings. The Cohen Theorem applied to one-dimensional complete reduced local rings implies that there exists a DVR contained in the ring for which the ring is a finitely generated module. Thus the conclusion follows from Theorem 1.1.13. $\square$

A particular type of analytically unramified rings are the *analytically irreducible* rings.

Definition 1.1.18. *The ring R is called* **analytically irreducible** *if the $\mathfrak{m}$-adic completion $\widehat{R}$ of R is an integral domain.*

As an easy consequence of the previous definition we have that an analytically irreducible ring is itself an integral domain. The new results presented in this thesis about canonical ideals are concerned with this type of ring. It is therefore worth to spend some more time on them, which we shall do in Sect. 1.3.

Let us now turn to the question of uniqueness. First, let us comment, that if R is Dedekind, then every fractional ideal of R is canonical. This example immediately shows, that in general, canonical ideals are not unique. Nevertheless, they are all isomorphic (as modules), and any two of them are related in a certain, very close way. Let us see now more in particular, what is known. Assume that the ring R is ane-dimensional local CM.

Proposition 1.1.19. *1. If ω is a canonical ideal of R and a is an invertible element in $Q(R)$ then $a\omega$ is again a canonical ideal of R.*

2. If ω and ω' are two canonical ideals of the ring R then there exists an invertible element $a \in Q(R)$ such that $\omega' = a\omega$.

Proof. 1. For a fractional ideal F of R

$$a\omega : (a\omega : F) = a(\omega : a(\omega : F)) = aa^{-1}(\omega : (\omega : F)) = F. \tag{1.31}$$

Thus by Definition 1.1.1 $a\omega$ is again a canonical ideal.

2. ω' is a canonical ideal then:

$$\omega = \omega' : (\omega' : \omega) \tag{1.32}$$

$\omega' : \omega$ is a fractional ideal of R then there exist invertible elements in $Q(R)$ $\{a_i\}_i \in I$ (I is a finite set) such that $\omega' : \omega = \sum_i a_i R$. Then equation 1.32 becomes:

$$\omega = \omega' : \sum_i a_i R = \bigcap_i (\omega' : a_i R). \tag{1.33}$$

By Proposition 1.1.2 ω is irreducible and so

$$\omega = \omega' : a_i R, \tag{1.34}$$

for some i.
Thus

$$a_i\omega = a_i(\omega' : a_i R) = \omega' : R = \omega'. \tag{1.35}$$

□

§7. How we have already mentioned an interesting problem is to find characterizations of a a canonical ideal with the purpose of finding those ideals which are canonical. A characterization of a canonical ideal which will be used many times in Chapter 2 is presented in [HK, Satz 3.3]. In fact in the first volume of the book of Zariski and Samuel a similar result is proved (see [ZS, Theorem 34]) not for canonical ideals but for irreducible ones. We have seen in 1.1.2 that every canonical ideal is irreducible, now we shall prove the converse of this fact. The ring R is assumed to be local one-dimensional and CM.

Proposition 1.1.20. *Assume that the ring R has a canonical ideal and let I be a regular fractional ideal of R. If the ideal I is irreducible then I is a canonical ideal of R.*

Proof. Let ω be a canonical ideal of R. Then

$$I = \omega : (\omega : I) = \bigcap_{x \in \omega : I} (\omega : x). \tag{1.36}$$

Since I is an irreducible ideal, the above equation implies that there exists $x \in Q(R)$, x invertible such that

$$I = \omega : x = x(\omega : R) = x\omega. \tag{1.37}$$

Thus from Proposition 1.1.19 the conclusion follows. □

Let formulate the result characterizing a canonical ideal from [HK]

Theorem 1.1.21. *Assume that the ring R has a canonical ideal. Let ω be a regular fractional ideal of R. Then the following conditions are equivalent:*

i) ω *is a canonical ideal of R;*

ii) ω *is an irreducible ideal;*

iii) $\ell_R(\omega : \mathfrak{m}/\omega) = 1$.

We have already proved the equivalence $i) \iff ii)$ in Proposition 1.1.2 and in Proposition 1.1.20. For proving the other one we shall use the ideas from [ZS]. To begin with: we can suppose that our irreducible fractional ideal ω is a proper ideal of R. The ring $(R, \mathfrak{m})$ is one-dimensional and local then the ideal $\omega \subset R$ is $\mathfrak{m}$-primary, this means that there exists $s \geq 1$ such that $\mathfrak{m}^s \subseteq \omega$. We reduced our problem to prove the next theorem.

Theorem 1.1.22. *Let $(R, \mathfrak{m})$ be a local Noetherian ring (non necessarily one-dimensional), and $\mathfrak{q}$ an $\mathfrak{m}$-primary ideal of R. Then the following conditions are equivalent:*

i) The ideal $\mathfrak{q}$ *is irreducible;*

ii) The vector space $(\mathfrak{q} : \mathfrak{m})/q$ *is one dimensional.*

Proof. $i) \Longrightarrow ii)$: From the fact that $\mathfrak{q}$ is $\mathfrak{m}$-primary we have that $\mathfrak{q} \subset \mathfrak{q} : \mathfrak{m}$ with strict inclusion. $(\mathfrak{q} : \mathfrak{m})/\mathfrak{q}$ is an R-module and $\mathfrak{m}(\mathfrak{q} : \mathfrak{m}) \subset \mathfrak{q}$ then $(\mathfrak{q} : \mathfrak{m})/\mathfrak{q}$ is an $R/\mathfrak{m}$ module, but $k = R/\mathfrak{m}$ is a field then $(\mathfrak{q} : \mathfrak{m})/\mathfrak{q}$ is a vector space over k. Suppose that

$$\dim_k(\mathfrak{q} : \mathfrak{m})/\mathfrak{q} > 1. \tag{1.38}$$

We know that in this case there exist two non trivial vector subspaces with intersection the zero space. Note that the subspaces of the vector space $(\mathfrak{q} : \mathfrak{m})/\mathfrak{q}$ correspond to the ideals of R which are between $\mathfrak{q}$ and $\mathfrak{q} : \mathfrak{m}$. The existence of the two non trivial subspaces with zero intersection means at the level of the ring R that $\mathfrak{q}$ is reducible which is a contradiction.
$ii) \Longrightarrow i)$ First we shall show that condition ii) of Theorem 1.1.22 implies that the set of all ideals of R properly containing $\mathfrak{q}$ admits a smallest element which in this case is $\mathfrak{q} : \mathfrak{m}$. Let I be an ideal of R properly containing $\mathfrak{q}$. Note that

$$\mathfrak{q} \subsetneqq (\mathfrak{q} : \mathfrak{m}) \cap I, \tag{1.39}$$

because, as $\mathfrak{q}$ is $\mathfrak{m}$-primary there exists $s \geq 1$ such that $\mathfrak{m}^s \subseteq \mathfrak{q}$, thus $I\mathfrak{m}^s \subseteq \mathfrak{q}$ and $I\mathfrak{m}^{s-1} \nsubseteq \mathfrak{q}$, but $I\mathfrak{m}^{s-1} \subseteq \mathfrak{q} : \mathfrak{m}$. Since $(\mathfrak{q} : \mathfrak{m})/\mathfrak{q}$ is a one-dimensional vector space there are no ideals between $\mathfrak{q}$ and $\mathfrak{q} : \mathfrak{m}$. From what we have shown before we have that:

$$\mathfrak{q} \subsetneqq (\mathfrak{q} : \mathfrak{m}) \cap I \subseteq \mathfrak{q} : \mathfrak{m}. \tag{1.40}$$

Therefore $(\mathfrak{q} : \mathfrak{m}) \cap I = \mathfrak{q} : \mathfrak{m}$, this means that $\mathfrak{q} : \mathfrak{m} \subseteq I$. Then $\mathfrak{q} : \mathfrak{m}$ is the smallest element in the set of all ideals of R properly containing $\mathfrak{q}$. We shall see that the proof is finished using the fact proved before. Consider $\mathfrak{q} = I_1 \cap I_2$, where I_1, I_2 are two ideals of R. Suppose that $\mathfrak{q} \subsetneqq I_1$ and $\mathfrak{q} \subsetneqq I_2$. Then applying what we have already proved for I_1 and I_2 we have that $\mathfrak{q} : \mathfrak{m} \subseteq I_1$ and $\mathfrak{q} : \mathfrak{m} \subseteq I_2$. Thus

$$\mathfrak{q} : \mathfrak{m} \subseteq I_1 \cap I_2 = \mathfrak{q}. \tag{1.41}$$

This means that $\mathfrak{q} : \mathfrak{m} = \mathfrak{q}$, which is a contradiction. Then either $\mathfrak{q} = I_1$ or $\mathfrak{q} = I_2$. $\square$

§8. We shall see now another characterization of a one-dimensional Gorenstein ring which shows that for a Gorenstein ring its canonical ideal is trivial.

Theorem 1.1.23. *Let R be a one-dimensional local CM ring. The following conditions are equivalent:*

1. *R is a Gorenstein ring;*
2. *R is a canonical ideal of R;*
3. *For every fractional ideal F of R which contains a nonzero divisor of R, we have that $(F^{-1})^{-1} = F$.*
4. *For every ideal $I \subseteq R$ which contains a nonzero divisor of R, we have that $\ell_R(R/I) = \ell_R(I^{-1}/R)$.*

Proof. $1 \Longrightarrow 2$ We have already seen in Theorem 1.1.12 that R is Gorestein implies that $\ell_R(\mathfrak{m}^{-1}/R) = 1$ and this means that R is a canonical ideal of R as we can apply Theorem 1.1.21.

$2 \Longrightarrow 1$ We know that $\mu(\omega) = \text{type}(R)$ (Proposition 1.1.10). As R is a canonical ideal of R we have that $\text{type}(R) = 1$, which means that R is Gorenstein.

$2 \Longrightarrow 3$ Evident, it is exactly the definition of a canonical ideal.

$3 \Longrightarrow 4$ Also this is trivial. From condition 3 we have that R is a canonical ideal of R and we use a simple property of a canonical ideal (see equation 1.5).

$4 \Longrightarrow 1$ We apply the lengths equality which appears in 4 for the maximal ideal $\mathfrak{m}$. Thus $\ell_R(R/\mathfrak{m}) = \ell_R(\mathfrak{m}^{-1}/R)$, but $\ell_R(R/\mathfrak{m}) = \dim_k(k) = 1$. We obtain that $\ell_R(\mathfrak{m}^{-1}/R) = 1$, thus R is Gorenstein. □

As a consequence of the previous theorem is the next corrolary.

Corollary 1.1.24. *Let R be a local one-dimensional Gorenstein ring and $R : \overline{R}$ the conductor of the integral closure $\overline{R}$ in R. Then*

$$2\ell_R(R/R : \overline{R}) = \ell_R(\overline{R}/R : \overline{R}) \tag{1.42}$$

Proof. From condition 4 of Theorem 1.1.23 we have that $\ell_R(R/R : \overline{R}) = \ell_R(\overline{R}/R)$. And $\ell_R(\overline{R}/R) = \ell_R(\overline{R}/R : \overline{R}) - \ell_R(R/R : \overline{R})$ which finishes the proof. □

§9. In [BF1] the authors introduce the *almost Gorenstein* rings a notion which generalizes Gorenstein rings. Assume that the ring R is like usually one dimensional local CM. Moreover R has a canonical ideal ω such that $R \subseteq \omega \subseteq \overline{R}$.

Definition 1.1.25. *R is called* **almost Gorenstein** *if*

$$\ell_R(\overline{R}/R) = \ell_R(R/(R:\overline{R})) + \mathrm{type}(R) - 1. \tag{1.43}$$

A particular case of almost Gorestein rings is that one of *Kunz* rings which was introduced in [BDoFo]. A ring R is called Kunz if $\ell_R(\overline{R}/R) = \ell_R(R/\underline{c})+1$. It is easy to see that Kunz rings are in fact almost Gorenstein rings of type 2.

We shall see some equivalent definitions of these two notions. For this we need some relations between lengths of some particular modules over R. These results are from [BF1].

Lemma 1.1.26. *1.* $\ell_R(\overline{R}/R) = \ell(R/(R:\overline{R})) + \ell_R(\omega/R)$.

2. $\ell_R(\overline{R}/R) \geq \ell_R(R/(R:\overline{R})) + \mathrm{type}(R) - 1$.

3. $\mathrm{type}(R) - 1 \leq \ell_R(\omega/R)$.

Then we can formulate:

Proposition 1.1.27. *The following conditions are equivalent:*

1. The ring R is almost Gorenstein.

2. $\mathrm{type}(R) = \ell_R(\omega/R) + 1$.

Proposition 1.1.28. *The following conditions are equivalent:*

1. The ring R is Kunz.

2. $\ell_R(\omega/R) = 1$.

1.2 Free modules over a DVR

§1. Consider R a one-dimensional local CM ring (not necessarily a domain), with maximal ideal $\mathfrak{m}$.

Northcott in a series of articles from the 50's. introduced the **first neighborhood ring**. In the more recent papers it is called the **blowing-up ring of the maximal ideal**. It is a ring which we shall denote it by $\mathcal{B}(\mathfrak{m})$ and it is defined with the following formula:

$$B(\mathfrak{m}) = \bigcup_{i\in\mathbb{N}} (\mathfrak{m}^i : \mathfrak{m}^i). \tag{1.44}$$

One can define the blowing-up ring not only for the maximal ideal, but for an arbitrary ideal of R, see the article of Lipman [L]. In [BF1] the authors considered this ring also for an arbitrary fractional ideal, in special for a canonical ideal ω of R with the property that $R \subseteq \omega \subseteq \overline{R}$.

Let I be a *regular* ideal of R or after Lipman's terminology an *open* ideal (equivalently, I contains a nonzero divisor or, equivalently $\mathfrak{m}^n \subseteq I$ for some $n > 0$). Define the blowing-up of I to be the ring:

$$\mathcal{B}(I) = \bigcup_{n>0} I^n : I^n. \tag{1.45}$$

(With the Lipman's notation $\mathcal{B}(I) = R^I$.) A characterization of this special ring is the next proposition from [L].

Proposition 1.2.1. *Let I be a regular ideal of R and $\mathcal{B}(I)$ its blowing-up. Then:*

1. *$\mathcal{B}(I)$ is a finitely generated R-module and*
$$\mathcal{B}(I) = I^n : I^n \tag{1.46}$$
for all sufficiently large n.
2. *$I\mathcal{B}(I) = x\mathcal{B}(I)$ for some nonzero divisor in $\mathcal{B}(I)$.*
3. *If S is any ring between R and $\overline{R}$ such that IS is principal ideal in S, then $\mathcal{B}(I) \subseteq S$.*

In the same article the next definition is given:

Definition 1.2.2. *An element of the regular ideal I of R is* ***I-transversal*** *if*

$$xI^n = I^{n+1} \tag{1.47}$$

for some integer $n > 0$.

Lipman in the same article proved that an element x is I-transversal if and only if $x\mathcal{B}(I) = I\mathcal{B}(I)$.

Another important element for the study of one-dimensional local CM rings is the **superficial** element of I. We shall use especially the superficial elements in $\mathfrak{m}$, and we shall renunce to write $\mathfrak{m}$.

Definition 1.2.3. *An element $x \in \mathfrak{m}^s$ is called a* **superficial of degree** *s if*

$$\mathfrak{m}^{n+s} : x = \mathfrak{m}^n \tag{1.48}$$

for large n.

Note that $x \in \mathfrak{m}$ is $\mathfrak{m}$-transversal if and only if it is superficial of degree 1 and

$$\sqrt{xR} = \sqrt{\mathfrak{m}}. \tag{1.49}$$

Equation 1.49 is true for every nonzero divisor $x \in \mathfrak{m}$. Then we can conclude with the fact that $x \in \mathfrak{m}^s$ is a superficial element of degree s if and only if

$$x\mathcal{B}(\mathfrak{m}) = \mathcal{B}(\mathfrak{m})\mathfrak{m}^s. \tag{1.50}$$

Another interesting property of the blowing-up ring of the maximal ideal which we shall use it in the next paragraph is:

$$\ell_R(\mathcal{B}(\mathfrak{m})/\mathfrak{m}\mathcal{B}(\mathfrak{m})) = e(R), \tag{1.51}$$

where $e(R) = e$ is the multiplicity of the ring R. (cf [N1] or [N2])

§2. We need the next proposition which can be find in [M]

Proposition 1.2.4. *Let I and J be two fractional ideals of R, both containing at least one nonzero divisor of the ring. Further, let $a \in R$ be a nonzero divisor element of R. Then*

1. *I/aI and J/aJ have finite length and*

$$\ell_R(I/aI) = \ell_R(J/aJ). \tag{1.52}$$

2. *If a is a superficial element of degree 1 the length from equation 1.52 is equal to the multiplicity $e(R)$ of the ring R. In this case, in particular we have that $\ell_R(R/aR) = e$.*

Proof. First suppose that I is a integral ideal of R. As I is a $\mathfrak{m}$-primary ideal of R, there exists $n \in \mathbb{N}$, $n \neq 0$ such that $\mathfrak{m}^n \subseteq I$. Thus

$$\ell_R(R/I) \leq \ell_R(R/\mathfrak{m}^n) < \infty. \tag{1.53}$$

The same argument shows that $\ell_R(R/aI) < \infty$. Therefore also $\ell_R(I/aI) < \infty$. We have the exact sequences:

$$0 \to I/aI \to R/aI \to R/I \to 0 \tag{1.54}$$

and

$$0 \to aR/aI \to R/aI \to R/aR \to 0. \tag{1.55}$$

The exact sequence (1.54) implies that

$$\ell_R(R/aI) = \ell_R(I/aI) + \ell_R(R/I) \tag{1.56}$$

while the sequence 1.55 implies that

$$\ell_R(R/aI) = \ell_R(R/aR) + \ell_R(aR/aI). \tag{1.57}$$

As a is a nonzero divisor, $R/I \simeq aR/aI$, thus

$$\ell_R(I/aI) = \ell_R(R/aR). \tag{1.58}$$

Similarly

$$\ell_R(J/aJ) = \ell_R(R/aR). \tag{1.59}$$

From the two equations we have that

$$\ell_A(I/aI) = \ell_A(J/aJ). \tag{1.60}$$

If I is a fractional ideal the rI is an integral ideal for some nonzero divisor element $r \in R$. Thus

$$\ell_R(I/aI) = \ell_R(rI/arI). \tag{1.61}$$

For the second part of the theorem we may assume that $I = B(\mathfrak{m})$ using the first part which we have already proved and choose as a a superficial element of degree 1. Since a is a superficial element of degree 1, by equation 1.50 we have that

$$a\mathcal{B}(\mathfrak{m}) = \mathfrak{m}\mathcal{B}(\mathfrak{m}). \tag{1.62}$$

Then we can conclude using (1.51)

$$\ell_R(\mathcal{B}(\mathfrak{m})/a\mathcal{B}(\mathfrak{m})) = \ell_R(\mathcal{B}(\mathfrak{m})/\mathfrak{m}\mathcal{B}(\mathfrak{m})) = e. \tag{1.63}$$

□

§3. Assume that the ring R is analytically irreducible and consider an element of R of smallest nonzero value in $v(R)$ and denote it by x. As usualy k is the residue field of the ring R. Then there exists a DVR W which is included in R, has the maximal ideal generated by x and residue field k. If we assume that the ring R is complete in the $\mathfrak{m}$-adic topology, then we can take W to be the formal power series ring $k[[x]]$. Our aim is to prove that every fractional ideal of R (then also the ring itself) is a free module over W.

The following is a well-known theorem about the finitely generated modules over PID (see [AuB], [Jac]):

Theorem 1.2.5. *A finitely generated torsion free module over a PID is free.*

Note that the ring W defined before is a DVR and so in particular a PID. The next theorem was proved in [E3].

Proposition 1.2.6. *R is a finitely generated, torsion free W-module.*

Proof. Evidently R is a torsion free W-module. If I and J are ideals of R, $I \subset J$, with the property that $\mathfrak{m}J \subset I$, then

$$\ell_R(J/I) = \ell_W(J/I) \tag{1.64}$$

because R and W have the same residue field k and J/I is a k-vector space.

From the definition of x this is a superficial element of degree 1. Therefore

$$x\mathfrak{m}^{n-1} = \mathfrak{m}^n \tag{1.65}$$

for some big $n \in \mathbb{N}$. We have that:

$$\begin{aligned} \ell_R(R/\mathfrak{m}^n) &= \ell_R(R/\mathfrak{m}) + \ell_R(\mathfrak{m}/\mathfrak{m}^2) + ... + \ell_R(\mathfrak{m}^{n-1}/\mathfrak{m}^n) \\ &= \ell_W(R/\mathfrak{m}) + \ell_W(\mathfrak{m}/\mathfrak{m}^2) + ... + \ell_W(\mathfrak{m}^{n-1}/\mathfrak{m}^n) \\ &= \ell_W(R/\mathfrak{m}^n). \end{aligned} \tag{1.66}$$

We know that $\ell_R(R/\mathfrak{m}^n) < \infty$, thus also $\ell_W(R/\mathfrak{m}^n) < \infty$. This means that $R/\mathfrak{m}^n$ is a W-module of finite length, thus it is a finitely generated W-module. Putting all these facts together we have that R is a finitely generated W-module, and so by Theorem 1.2.5, a free W-module. □

By the above proposition one can draw the following corollary.

Corollary 1.2.7. *All fractional ideals of R, including the ring itself, are free W-modules.*

The natural question is: what is the rank of a fractional ideal or of the ring R) as a free W-module? To answer this question we shall use Proposition 1.2.4.

Corollary 1.2.8. *The rank of a fractional ideal I of R as a free module over W is equal to $e(R)$. In particular the rank of R over W is equal to $e(R)$*

Proof. $rank_W(I) = \ell_R(I/xI)$ and by the definition of x, this is a superficial element of degree 1. Then we can conclude using Proposition 1.2.4. □

1.3 Numerical semigroups

§1. We have already gave a definition for analytical irreducibility. We shall now discuss a different, but equivalent way of describing the same concept.

It is known (see e.g. [M, Theorem 10.2]) that R is analytically unramified if and only if $\overline{R}$ is finitely generated as an R-module. In the work [Ka] published in 1986, Katz proved, that the integral closure of an analytically unramified ring is local if and only if the ring is analytically irreducible. Thus we may conclude the following.

Theorem 1.3.1. *A ring R is analytically irreducible if and only if its integral closure, $\overline{R}$ is a DVR and a finitely generated R-module.*

This means that we view analytical irreducibility as a condition on the integral closure. This is of crucial importance for us; in fact, this is how we shall always use analytical irreducibility.

The above theorem implies that there exists a valutation

$$v : Q(R) \to \mathbb{Z} \tag{1.67}$$

for which

$$\overline{R} = \{x \in \mathbb{Q}(R) |\ v(x) \geq 0\}. \tag{1.68}$$

As $R \subseteq \overline{R}$, we can define the **value set** of R as the subset of natural numbers.

$$v(R) \equiv \{v(x) \in \mathbb{Z} |\ x \in R \setminus \{0\}\}. \tag{1.69}$$

The difference set $\mathbb{N} \setminus v(R)$ is *finite*, it contains the number 0 and it is closed under addition. Thus $v(R)$ is a so called **numerical semigroup** [BF1, BDoFo]. Some authors (see e.g. the book of Rèdei) considere numerical semigroups only those subsemigroups of $\mathbb{N}$ which contains 0. In the next paragraphs we shall give more details about the notion of numerical semigroups in general.

§2. For a reference on commutative semigroups see e.g. the book of Rèdei ([Re]) or the book of Gilmer treating the semigroup rings ([G]). In Rédei monography the argument is treated in a very general context. There are many other newer references on this subject, see e.g. [RG].

Definition 1.3.2. *S is a* **numerical semigroup** *if $S \subseteq \mathbb{N}$, and S is a subsemigroup of $(\mathbb{N}, +)$ with $0 \in S$.*

Following the terminology from [Re] we shall call a numerical semigroup *prime* if its elements are relatively prime i.e. if their greatest common divisor is 1. The greatest common divisor of an infinitly many elements is defined in the natural way: set $\mathrm{Div}(s)$, the set of all divisors of an element $s \in S$. Of course, it is a finite set, then also $\cap_{s \in S}\mathrm{Div}(s)$ is a finite set, thus it has a maximum. This maximum is a greatest common divisor of all elements from S.

It is clear that all numerical semigroups different from 0 are of the form $S = dS'$ where d is a natural number and S' is a prime numerical semigroup. In fact d is the greatest common divisor of the elements of S. Therefore it is natural to investigate the properties of prime numerical semigroups. We shall see some of these properties in the following theorem from [Re].

Theorem 1.3.3. *1. For every prime numerical semigroup S the difference set $\mathbb{N} \setminus S$ is finite;*

2. Every numerical semigroup S is finitely generated in the sense that there exists $l \geq 1$ elements $a_1, a_2, \ldots, a_l$ such that

$$S =< a_1, a_2, \ldots, a_l >:= \left\{ \sum_{i=1}^{l} n_i a_i | \; n_i \in \mathbb{N} \right\}. \tag{1.70}$$

Moreover every numerical semigroup ($\neq 0$) has a single minimal generating system. The natural numbers $a_1 < \cdots < a_l$ form the minimal generating system of S if and only if no a_i ($i \geq 2$) is representable as

$$a_i = a_1 x_1 + \cdots + a_{i-1} x_{i-1} \tag{1.71}$$

with $x_1, \ldots, x_{i-1} \in \mathbb{N}$.

Proof. 1. First we shall prove that in the prime numerical semigroup S there exist two relatively prime elements. An easy consequence of the definition of a prime numerical semigroup is that there must exist finitely many relatively prime elements $b_1, \ldots, b_k$ ($k \geq 2$) in S. Then the Diophantine equation

$$b_1 x_1 + \cdots + b_{k-1} x_{k-1} = 1 + b_k x_k \tag{1.72}$$

has a solution $x_1, \ldots, x_k$. From this we have that $1 + b_k x_k \in S$ and of course $b_k \in S$. Thus these two elements are realtively prime in S.

Let a, b denote two relatively primes in S. Then for every $i \in \mathbb{N}$ the equation

$$ax + by = ab + i \tag{1.73}$$

has a solution x, y, non negative integers. This means that $ab + \mathbb{N} \subseteq S$.
2. It suffices to prove this for a prime numerical semigroup S. From 1. we have that

$$c + \mathbb{N} \subseteq S \tag{1.74}$$

for an integer $c > 0$. It is evident that $c, c+1, \ldots, 2c-1$ and the elements of the (finite) difference set $S \setminus (c + \mathbb{N})$ are generators of S. The last assertion of the theorem concerning the existence of a minimal generating system is evident. □

§3. For each numerical semigroup $S \subseteq \mathbb{N}$, the set of formal power series with coefficients in an arbitrary field k:

$$\{\sum_{i \in S} a_i t^i | \;\; a_i \in k\} \tag{1.75}$$

is in fact an analytically irreducible ring called the **semigroup ring** associated to S. It will be denoted by $k[[S]]$. This allows us to define the concepts as *ideal, canonical ideal, type, irreducibility* and many others for a numerical semigroup, too. We shall see more details in what follows

For references on the development of the theory of numerical semigroups see articles of Rosales and others or [FGH] and [D'Anna3]. In [BF1], [BDoFo], [Mat], [D'Anna1] etc. the authors are applying results from this theory in the study of analytically irreducible rings.

From now on we shall use the word semigroup for numerical semigroup and we shall furthermore always assume that semigroups have finite complement in $\mathbb{N}$.

For a semigroup S we define the **Frobenius number**

$$g := max(\mathbb{N} \setminus S). \tag{1.76}$$

In fact $g = c - 1$, where c is the same number which appears in the proof of Theorem 1.3.3. c is the smallest element of S with the property that $c+\mathbb{N} \subseteq S$ and we shall call it the **conductor** of S (as in [J]) or the **multiplicity** of S as in [BDoFo]. Others integers associated to S are:

1. The number of elements of a minimal set of generators of S (from Theorem 1.3.3 this set is unique) which is denoted by $e(S)$ and it is called the *embeding dimension* of S,

2. $r = n(S) := |S \cap \{0, 1, \ldots, g\}|$, if $S \neq \mathbb{N}$. By convention we put $n(\mathbb{N}) = 0$. (by $|U|$ we denote the cardinality of the set U)

Following the terminology of Jäger (see [J]) we shall call the following sets:

$$H := \{s \in \mathbb{Z}| \ \ s \notin S \text{ and } g - s \in S\} \tag{1.77}$$

and

$$L := \{s \in \mathbb{Z}| \ \ s \notin S \text{ and } g - s \notin S\}, \tag{1.78}$$

the **set of first type halls** and the **set of second type halls**, respectively.

How it was explained in the beginning of this paragraph there exists a relation between the sets of the semigroup S and those of the semigroup ring $k[[S]]$. Let U be a set included in the semigroup ring $k[[S]]$. Consider the set containing all the orders of nonzero elements of U. As the order is a valuation of k[[t]], we can denote this set by $v(U)$. It is evident that this set is included in S.

If F is a fractional ideal of $k[[S]]$, then v(F) satisfies the equality:

$$v(F) + S \subset v(F). \tag{1.79}$$

Vice versa if E is a subset of $\mathbb{Z}$ which is bounded below, and satisfies the equality $S + E \subset F$ then

$$k[[E]] := \{\sum_{i \in U} a_i t^i | \ a_i \in k\} \tag{1.80}$$

is a fractional ideal of $k[[s]]$.

After this explanation seems more then opportune to define an **ideal** of the semigroup S a subset I of S which satisfies

$$i + s \in I \tag{1.81}$$

for every $i \in I$ and $s \in S$. A **relative ideal** of S is a subset F of $\mathbb{Z}$ whith the property that

$$z + F := \{z + j | \ j \in F\} \tag{1.82}$$

is an ideal of the semigroup for some $z \in S$. This it is equivalent to $F+S \subseteq F$ and $F+z \subseteq S$ for some $z \in S$. The terminology presented here is from [BF1]. In [J] a relative ideal is called an S-ideal, and in this thesis is prefered the use of this terminology.

If F and F' are two S-ideals we can define

$$F - F' := \{x \in \mathbb{Z} | \ x + F' \subseteq F\} \tag{1.83}$$

which is an S-ideal. For every S-ideal F, $S' := F - F$ is a semigroup, and it is the largest semigroup such that F is an S'-ideal.

Following our way to explain how one can think to all these concepts regarding semigroups we shall observe that using the previous notations we have that

$$k[[F]] : k[[F']] = k[[F - F']], \tag{1.84}$$

where on the right-hand side of the equality the operation is the quotient of two fractional ideals defined in the beginning of Section 1.1. Then, as in that section the next definition is that of a special relative ideal of the semigroup namely a *canonical ideal*.

Definition 1.3.4. *An S-ideal Ω is called a* **canonical ideal** *of the semigroup S if*

$$\Omega - (\Omega - F) = F, \tag{1.85}$$

for every S-ideal F.

The next proposition from [J] gives an example of such an ideal which is called the **standard canonical ideal** of the semigroup.

Proposition 1.3.5 (Jäger). *$\Omega = S \cup L$ is a canonical ideal of the semigroup S, where L is the set of 2.nd type halls defined before.*

Proof. First we shall show that $\Omega = S \cup L$ is an S-ideal, in fact we shall prove that $L + S \subseteq \Omega$. For this take $z \in L$ and $s \in S$. From the definition of the set L, $g - z = c - 1 - z \notin S$. Thus $c - 1 - (z + s) \notin S$. We have two possibilities either $z + s \in S \subseteq \Omega$ or $z + s \notin S$ then $z + s \in L \subset \Omega$. For showing that Ω is a canonical ideal of S we will prove that:

$$\Omega - F = \{c - 1 - z| \ z \notin F\} \tag{1.86}$$

for any S-ideal F. Take $x \in \Omega - F$ and $z = c - 1 - x$. If $z \in F$ then $c - 1 = x + z \in \Omega$ which is a contradiction. Thus $z \notin F$. Now consider $x \notin \Omega - F$. Then there exists $a \in F$ with $x + a \notin \Omega$. This means that $x + a$ is a 1.st type hall for some $a \in F$. Thus $c - 1 - (x + a) \in S$ which means that $c - 1 - x \in a + S \subseteq F$. We have proved the equality from equation 1.86. And it is clear that from this it can be easily obtained that $\Omega - (\Omega - F) = F$ which is equivalent with the fact that Ω is a canonical ideal of the semigroup. □

In fact the standard canonical ideal from the previous proposition is obtained by the formula:

$$\Omega = S \cup L = \{z \in \mathbb{Z}| \ c - 1 - z \notin S\}. \tag{1.87}$$

Following again the notations from [BF1] we denote M the set $\{x \in S| \ x > 0\}$ which is an ideal of S called the **maximal ideal** of S. Let

$$T := (M - M) \setminus S \tag{1.88}$$

which is a finite set. We define the **type** of S

$$\text{type}(S) := |T|. \tag{1.89}$$

It is evident that $T \subseteq \{c - 1\} \cup L$.

A semigroup S is called **symmetric** if for any $z \in \mathbb{Z}$ we have, $z \notin S$ if and only if $c - 1 - z \in S$ and **pseudo-symmetric** if $z \notin S$ if and only if $c - 1 - z \in S$ or $z = \frac{c-1}{2}$. With the above notations it is evident that S is symmetric if and only if $L = \emptyset$ and pseudo-symmetric if and only if $L = \{\frac{c-1}{2}\}$. Then the symmetric semigroups are the semigroups of type 1 and the pseudo-symmetric ones are particular cases of semigroups of type 2. In [BF1] it is introduced the notion of *almost symmetric*. A semigroup is called **almost symmetric** if $L \subseteq T$. An easy implication of this definition is that S is almost symmetric if and only if $T = L \cup \{c - 1\}$. We shall see in Section 1.4 that every different type of semigroups has a corrispondent type of rings.

§4. Another important invariant of the semigroup S is the **type sequence** of S introduced in [BDoFo] see also [D'Anna2] and [D'Anna3]. If S is a semigroup, $S \neq \mathbb{N}$, then $S = \{0 = s_0, s_1, \dots, s_{r-1}, s_r = c, \rightarrow\}$, where $s_i < s_{i+1}$ $(0 \leq i \leq r = n(S))$ and the arrow means that every integer greater that c belongs to S. For every $i \geq 0$ we can consider the ideal:

$$S_i := \{s \in S | s \geq s_i\} \tag{1.90}$$

and the S-ideal

$$S(i) := S - S_i \tag{1.91}$$

In fact for every i, $S(i) = S_i - S_i$. Thus $S(i)$ is a semigroup. Moreover $S(0) = S$, $S(1) = M - M$ and $S(n) = \mathbb{N}$. We observe that if $i > n$ then $S_i - S_i = \mathbb{N} \subset S(i)$, thus $S(i)$ is not anymore a semigroup. We obtain the following chain:

$$S_n \subset S_{n-1} \subset \cdots \subset S_1 \subset S \subset S(1) \subset \cdots \subset S(n-1) \subset S(n) = \mathbb{N}. \tag{1.92}$$

Let $t_i(S) = |S(i) \backslash S(i-1)|$ for $1 \leq i \leq n$. (As $S(i) \backslash S(i-1)$ is a finite set $t_i(S)$ is equal to the number of elements of this set.) Observe that $t_1(S) = \text{type}(S)$ is the type of the semigroup S defined above. In this way, it is possible to associate to every semigroup S a numerical sequence $\{t_1, t_2, \dots, t_n\}$ which is called the **type sequence** of S. Since $\mathbb{N} \setminus S$ is the disjoint union of the sets $S(i) \setminus S(i-1)$ we have that:

$$c - n = \sum_{i=1}^{n} t_i(S). \tag{1.93}$$

This integer is called the **degree of singularity** of S and it is denoted by $\delta(S)$. Let now see a property of the elements t_i which define the type sequence of the semigroup S, this result can be find in [BDoFo] or in [D'Anna3].

Proposition 1.3.6. *Let S be a semigroup, $S \neq \mathbb{N}$. Then for every $i \in \{1, \dots, n\}$*

$$1 \leq t_i(S) \leq t_1(S). \tag{1.94}$$

Proof. If $s \in S_i$ then $g - s_{i-1} + s \geq g - s_{i-1} + s_i \geq c$, so $g - s_{i-1} \in S - S_i = S(i)$. But $g - s_{i-1} \notin S(i-1)$ and therefore $g - s_{i-1} \in S(i) \backslash S(i-1)$. Thus $t_i(S \geq 1)$.

For proving the other inequality consider the map $S(i) \setminus S(i-1) \rightarrow S(1) \setminus S(0)$ given by $x \rightarrow x + s_{i-1}$. We want to prove that this map is well defined and it is injective. Consider $x \in S(i)$. Then $x + s_{i-1} + s \in S$ for every $s \in S$. This means that $x + s_{i-1} \in S(1)$. The fact that it is injective is obvious. Thus $t_i(S) \leq t_1(S)$. $\square$

§5. With beginning of '90's it was built up a theory of Apéry sets for numerical semigroups in general (cf. the articles of J.C. Rosales and others, see [R1], [R2], [RB]). We give the definition of the Apéry set that appears in [R2].

Definition 1.3.7. *Let S be a numerical semigroup and $n \in S \setminus \{0\}$. The* **Apéry set** *with respect to n of S is the set $\mathrm{Ap}_n(S) = \{s \in S | s - n \notin S\}$.*

It can be easily proved that there are no two elements of $\mathrm{Ap}_n(S)$ belonging to the same congruence class modulo n. So it is clear, that $|\mathrm{Ap}_n(S)| = n$. A rather straightforward but nevertheless important consequence of the definition is the following

Lemma 1.3.8. *Let S be a numerical semigroup, $n \in S$, and $\mathrm{Ap}_n(S)$ be the Apéry set of S with respect to n. Then the Frobenius number g of S is*

$$g = max(\mathrm{Ap}_n(S)) - n.$$

We will always consider the Apéry set with respect to the element $e \in S$, where e is the smallest nonzero element in S. This set is called the Apéry set of the numerical semigroup.

We shall determine the Apery set of the standard canonical ideal of the semigroup, $\Omega = S \cup L$.

Proposition 1.3.9. *Let S be a numerical semigroup and let e be the smallest nonzero element of S. If the Apéry set of S is*

$$Ap_e(S) = \{p_0, p_1, ..., p_{e-1}\}, \tag{1.95}$$

$p_0 = 0 < p_1 < ... < p_{e-1}$, then the Apèry set of Ω is

$$Ap_e(\Omega) = \{p_{e-1} - p_{e-1}, ..., p_{e-1} - p_1, p_{e-1} - p_o\}. \tag{1.96}$$

Proof. By Lemma 1.3.8 $p_{e-1} = g + e$. First we shall show that

$$p_{e-1} - p_i \in \Omega \;\; \forall \;\; 0 \leq i \leq e - 1. \tag{1.97}$$

This is true because $g - (p_{e-1} - p_i) = p_i - e \notin S$.

Let us fix i. We want to prove that $p_{e-1} - p_i$ is the smallest element of Ω in its congruence class modulo e. Let

$$p_r \equiv p_{e-1} - p_i \text{ (mod } e). \tag{1.98}$$

This means that

$$p_{e-1} \equiv p_r + p_i \text{ (mod } e). \tag{1.99}$$

Since p_{e-1} is the smallest in its congrunce class mod e,

$$p_{e-1} \leq p_r + p_i \Leftrightarrow p_{e-1} - p_i \leq p_r. \tag{1.100}$$

Is it possible that an element $l \in L$ is such that $l \equiv p_{e-1} - p_i \pmod{e}$ and $l < p_{e-1} - p_i$? The answer is no because if $p_{e-1} - p_i - l = me$ for some $m \in \mathbb{N}$ $m > 0$ then $g - l = (m-1)e + p_i \in S$ which is in contradiction with the definition of L. □

1.4 Analytically irreducible and residually rational rings

§1. So far we have discussed properties of the numerical semigroups. Now we shall see how the theory of numerical semigroups can be applied to the theory of rings. Throughout this paragraph R will stand for a local, one-dimensional, analytically irreducible ring. Let $\mathfrak{m}$ be its unique maximal ideal, and $\overline{R}$, its integral closure. Under our hypothesis $\overline{R}$ is a DVR and a finitely generated R-module. Denote the unique maximal ideal of $\overline{R}$ by $\mathfrak{n}$. Thus there exists the field extension $k := R/m \subseteq \overline{R}/\mathfrak{n} =: K$. Due to the fact that $\overline{R}$ is a finitely generated R-module, we have that this field extension is finite, i.e. if we denote the degrre of this field extension $n := \dim_k K$ then $n < \infty$. How we have already seen in the beginning of Section 1.3 there exists a valuation $v : \mathbb{Q}(R) \to \mathbb{Z}$ and to such a ring R we can associate its value semigroup

$$S := v(R) = \{v(x) | \ x \in R \setminus \{0\}\}. \tag{1.101}$$

Moreover, here we consider only the rings which are also **residually rational** which means that the residue field of R, k is the same with the residue field of $\overline{R}$, K. In terms of the degree this is equivalent to the fact that $n = 1$.

Up to our knowledge one of the first results is that one of Apèry ([A]) from 1946. In this note it is announced the fact that the local ring of a plane curve singularity has a symmetric associated semigroup. In 1971 Kunz (see [K]) generalized the result of Apery. He proves:

Theorem 1.4.1 (Kunz). *The ring R is Gorenstein if and only if its value semigroup $v(R)$ is symmetric.*

Jäger gives a characterization of a canonical ideal of the ring R in terms of the valuation. His result from 1977 (see [J]) is important for us. In fact one of the new results which we shall present in this thesis is a characterization of a fractional ideal in order to be canonical for a non residually rational ring (see Section 2.5) which can be seen as a generalization of the Jäger's result.

We can define the value set not only for the ring but also for fractional ideals of the ring. (In fact Oneto and Zatini define the value set also for R-modules, see [OZ1].) Let $F \subseteq Q(R)$ be a fractional ideal. The **value set** of F is

$$v(F) := \{v(x) | \ x \in F \setminus \{0\}\}. \tag{1.102}$$

Let Ω be the standard ideal of the value semigroup $S := v(R)$, in fact $\Omega = S \cup L$ (see Section 1.3).

Theorem 1.4.2 (Jäger). *Let ω be a fractional ideal of R such that $R \subseteq \omega \subseteq \overline{R}$. Then ω is a canonical ideal of R if and only if $v(\omega) = \Omega$.*

Observe that the above theorem does not give a "universal" way to construct such an ω. However a simple consequence follows. For formulate this we need a simple observation. Since $\overline{R}$ is a DVR we have that the maximal ideal $\mathfrak{n}$ of $\overline{R}$ is generated by a single element, denote it by t. We can normalize our valuation and we can assume that $v(t) = 1$. Then the consequense of the Theorem of Jäger is that: ω ($R \subseteq \omega \subseteq \overline{R}$) is a canonical ideal of R if and only if the Frobenius number $g \notin v(\omega)$ and

$$\omega = R + \sum_{l \in L} e_l t^l R, \tag{1.103}$$

where e_l are some particular invertible elements in $\overline{R}$. In his article Jäger emphasizes the fact that usually e_l are different from the identity 1 of $\overline{R}$.

In [OZ1] Oneto and Zatini give a slight generalization of Theorem 1.4.2. Denote by c (as usually) the conductor of the value semigroup $S := v(R)$.

Theorem 1.4.3 (Oneto, Zatini). *Let N be a fnitely generated torsion free R-module of rank 1 containing $t^c\overline{R}$. If $v(N) \subset \{z \in \mathbb{Z} | \ c - 1 - z \notin S\}$ then there exists an unit u in $\overline{R}$ such that $uN \subset \omega$.*

§2. In an article from 1971 (see [Mat]) Matsuoka introduces another invariant of a one-dimensional, local, analytically irreducible and residually rational ring R, namely the **type sequence**. The type sequence is one of the subjects in many article, see [BDoFo], [D'Anna1], [OOZ]. Oneto and Zatini generalize it for modules (in [OZ2]). In [BDoFo] the authors analyze the relation between the type sequence of the ring R and that one of the value semgroup $S := v(R)$. Since $S := v(R)$ is a semigroup, $S \neq \mathbb{N}$, $S = \{0 = s_0, s_1, \ldots, s_{r-1}, s_r \rightarrow\}$ ($r = n(S)$), where $0 < s_1 < \cdots < s_{r-1} < s_r$ and s_r is the conductor of the semigroup, with the above notation $s_r = c = g + 1$. Consider the ideals of R:

$$\mathfrak{a}_i := \{x \in R | \ v(x) \geq s_i\}, \tag{1.104}$$

for every $0 \leq i \leq r$. We have that $\mathfrak{a}_0 = R$, $\mathfrak{a}_1 = \mathfrak{m}$, the maximal ideal of the ring, and $\mathfrak{a}_r = \mathfrak{f} := R : \overline{R}$, the conductor of $\overline{R}$ in R.

We may consider the following chain of fractional ideals of the ring R:

$$\mathfrak{f} = \mathfrak{a}_r \subset \mathfrak{a}_{r-1} \subset \cdots \subset \mathfrak{a}_1 \subset R \subset \mathfrak{a}_1^{-1} \subset \cdots \subset \mathfrak{a}_{r-1}^{-1} \subset \mathfrak{a}_r^{-1}. \tag{1.105}$$

Matsuoka in the obove cited article proves that in fact one has

$$\mathfrak{a}_r^{-1} = \overline{R}. \tag{1.106}$$

One can observe the analogy between the chain of $\mathfrak{a}_i$ and the chain of S_i considered for a semigroup in Section 1.3. If $1 \leq i \leq r$ define

$$t_i(R) = \ell_R(\mathfrak{a}_i^{-1}/\mathfrak{a}_{i-1}^{-1}). \tag{1.107}$$

Definition 1.4.4. *We call $(t_i(R),\ 1 \leq i \leq r)$ the* **type sequence** *of R.*

Note that $t_1(R) = \ell_R(\mathfrak{m}^{-1}/R)$ which is the type of the ring R as we have already proved in Section 1.1. Because the chain of $\mathfrak{a}_i^{-1}$ increases from R to $\overline{R}$, we have that:

$$\ell_R(\overline{R}/R) = \sum_{i=1}^{r} t_i(R). \tag{1.108}$$

We call $\ell_R(\overline{R}/R)$ the **degree of singularity** of R and also denote it by $\delta(R)$. A result from [Mat] is the next proposition about the bounds of the t_i:

Proposition 1.4.5 (Matsuoka). $1 \leq t_i(R) \leq t_1(R) = \mathrm{type}(R)$, *for* $1 \leq i \leq r$.

In the same article ([Mat]) Matsuoka gives a way to compute the length of the quotient module of two fractional ideals.

Theorem 1.4.6 (Matsuoka). *Let F_1, F_2 be two fractional ideals of R such that $F_2 \subseteq F_1$. Then:*

$$\ell_R(F_1/F_2) = |v(F_1) \setminus v(F_2)|. \tag{1.109}$$

§3. We shall present here some results from [BDoFo] and [BF1] caracterizing different types of analytically irreducible and residually rational rings in terms of the value semigroup of the ring.

Proposition 1.4.7 (Barucci, Dobbs, Fontana). *The ring R is Kunz if and only if its value semigroup is pseudo-symmetric.*

Proposition 1.4.8 (Barucci, Fröberg). *The ring R is almost Gorenstein if and only if its value semigroup $v(R)$ is almost symmetric and* $\mathrm{type}(R) = \mathrm{type}(v(R))$.

In [BF1] the authors emphasize the fact that the condition on the types of the ring R and of $v(R)$ is necessary, showing an example of a ring R which is almost Goresntein but its value semigroup is not almost symmetric. In this example R and $v(R)$ have different types.

§4. We have seen in Section 1.2 that every fractional ideal of a local one-dimensional CM ring is a free W-module of rank equal to the multiplicity of the ring, where W is a particular DVR included in the ring.

Recall that we have denoted by x the element of R of smallest nonzero value in $v(R)$. Denote this value by m. Then the DVR W is defined by the fact that it has the maximal ideal generated by x. With the assumption that the ring R is complete in the $\mathfrak{m}$-adic topology we can set $W = k[[x]]$.

We would like to know a basis of R (or of an arbitrary fractional ideal of R) as a free module over the DVR W.

In [BDF] the authors construct a basis for the ring

$$\mathcal{O} = \mathbb{C}[[X,Y]]/(F) = \mathbb{C}[[x,y]], \tag{1.110}$$

where $F(X,Y) \in \mathbb{C}[[X,Y]]$ is an irreducible formal power series, as a free $\mathbb{C}[[x]]$- module. The elements of the basis

$$\{y_0, y_1, \ldots, y_{e-1}\}, \tag{1.111}$$

where $e = v(x)$ is the multiplicity of the ring $\mathcal{O}$, are such that

$$\{v(y_0), \ldots, v(y_{e-1})\} \tag{1.112}$$

is the Apéry set of $v(\mathcal{O})$ with respect to e. This basis is called an **Apéry basis** of $\mathcal{O}$ with respect to x.

This can be done also in general for analyticaly irreducible and residually rational rings. In fact in a recent article of Barucci and Fröberg ([BF2]) the proof of this fact appears.

We know that in this case of residual rationality the multiplicity of the ring R is $e = e(R) = v(x) = m$

Theorem 1.4.9 (Barucci, Fröberg). *Let $\{f_0, f_1, ..., f_{e-1}\} \subset R$ be such that $\{v(f_0), v(f_1), ..., v(f_{e-1})\}$ is the Apéry set of the value semigroup $v(R)$ of R with respect to e. Then*

$$\{f_o, f_1, ..., f_{e-1}\} \tag{1.113}$$

is a free basis of R over W.

Proof. It is evidently true that the elements f_i are linearly independent. Let us denote $v(f_i) = r_i$, $r_i \in v(R)$. To prove that the elements f_i form a system of generators we consider an arbitrary element $a \in R$. Suppose

$$v(a) \equiv r_i \text{ (modulo } e). \tag{1.114}$$

Then there exists $a_0 \in W$ such that

$$v(a - a_0 f_i) > v(a). \tag{1.115}$$

Consider now $a - a_0 f_i$, there exists j such that

$$v(a - a_0 f_i) \equiv r_j \text{ (modulo } e). \tag{1.116}$$

Then there exists $a_1 \in W$ such that

$$v(a - a_0 f_i - a_1 f_j) > v(a - a_0 f_i). \tag{1.117}$$

And so on. Then using that R is complete we can conclude that

$$a = a_0 f_i + a_1 f_j + \dots. \tag{1.118}$$

Thus a is generated over W by elements f_i. □

Such a basis $\{f_0, f_1, ..., f_{e-1}\}$ is called an **Apéry basis** of the ring R. Note that in the same way we can construct Apéry Bases for all fractional ideals of the ring R.

Chapter 2

New results on the non residually rational case

2.1 What is a GSR

§1. Throughout this chapter R will stand for a local, one-dimensional analytically irreducible ring and $\mathfrak{m}$ its (unique) maximal ideal. As it was explained in Section 1.4, by our conditions, the integral closure of the ring, $\overline{R}$ is a DVR (so we have a valuation on the field of fractions $v : Q(\overline{R}) = Q(R) \to \mathbb{Z}$) and it is a finitely generated R-module. We shall denote by $\mathfrak{n}$ the (unique) maximal ideal of $\overline{R}$. Thus we have two fields: $k := R/\mathfrak{m}$ (the residue field of R) and $K := \overline{R}/\mathfrak{n}$ (the residue field of $\overline{R}$) and a natural extension between them, $k \subseteq K$. We shall set n for the degree of this extension; that is, $n = \dim_k(K)$. As $\overline{R}$ is finitely generated R-module, n must be finite and R is in fact a Noetherian ring.

In Section 1.4 some known results were discussed regarding canonical ideals of R. They all concerned the residually rational case, i.e. when $n = 1$. Our aim now is to extend and / or generalize these results so that they would also cover the non residually rational case, i.e. when $n \geq 1$.

Untill now, in many respects — and in particular with respect to canonical ideals — the case of analytically irreducible one-dimensional local rings *without* assuming residual rationality, was somewhat less studied. In [CDK] the authors characterized the Gorenstein property in the slightly more general setting of analytically unramified rings. From the results presented in [BHLP] we can imedialtely obtain a constructive criterion for a canonical ideal of rings of the form $R = k_0 + t^l k_1[[t]]$, where $l \neq 0$ is an arbitrary natural number and k_0, k_1 are fields such that $k_0 \subset k_1$, k_1 is a finite extension of k_0 and t is trascendental over k_1. These rings are in fact generalized semigroup rings (on short GSR) which are defined and studied in [BF]. One of the results obtained here is a criterion of Gorensteiness for GSR. The notion of GSR is the subject of this section.

Before defining what is a GSR we shall explain with more details the construction of a canonical ideal for rings studied in [BHLP], $R = k_0 + t^l k_1[[t]]$. Note that the ring R is Noetherian, the integral closure of R is $\overline{R} = k_1[[t]]$ and the maximal ideal $\mathfrak{m}$ of the ring R is a power of the maximal ideal of the integral closure $\overline{R}$. We shall construct in the next proposition a canonical ideal of R and we shall give a simple proof different from that given in [BHLP].

Proposition 2.1.1. *Let k_0, k_1 be two fields such that $k_0 \subseteq k_1$ is a finite extension and t is transcedental over k_1 and let R be the ring defined by*

$$R = k_0 + t^l k_1[[t]]. \tag{2.1}$$

Then the fractional ideal ω defined by

$$\omega = Ra_1 + Ra_2 + Ra_3 + ... + Ra_{m-1}, \tag{2.2}$$

where $\{a_1 = 1, a_2, a_3, ..., a_m\}$ is a particular finite system of generators of $\overline{R}$ over R, is a canonical ideal of R.

Proof. Let $\{1, b_2, ...b_s\}$ be a basis of k_1 over k_0. Using this basis we can determine a system of generators of $\overline{R}$ over R, namely

$$\begin{aligned}\overline{R} = R + b_2R + ... + b_sR + tR + b_2tRt + ... + b_stR + \\ +t^2R + b_2t^2R + ... + b_st^2R + ... + t^{l-1}R + ... + b_st^{l-1}R.\end{aligned} \tag{2.3}$$

Note that $m = sl$. Consider

$$\begin{aligned}\omega = R + b_2R + ... + b_sR + tR + b_2tR + ... + b_stR + \\ +t^2R + b_2t^2R + ... + b_st^2R + ... + t^{n-1}R + ... + b_{s-1}t^{n-1}R.\end{aligned} \tag{2.4}$$

We have that $R \subset \omega \subset \overline{R}$ and $\omega : \mathfrak{m} = k_1[[t]] = \overline{R}$. Then $\ell_R(\omega : \mathfrak{m}/\omega) = 1$ which is equivalent to ω being canonical (see [HK, Satz 3.3] or Theorem 1.1.21). □

For the proof of all results in the residually rational case one may use use the value semigroup of the ring. Looking only at the value semigroup surely cannot suffice when R is not necessarily residually rational. For example it is easy to construct two local one-dimensional analytically irreducible rings R_1

and R_2 such that their value semigroups will coincide, and yet one of them is Gorenstein while the other is not. Let

$$R_1 := \mathbb{R}[[it^3, t^5, it^{10}]], \tag{2.5}$$

and

$$R_2 := \mathbb{R}[[it^3, t^5, it^{10}, it^{17}]], \tag{2.6}$$

where $i \equiv \sqrt{-1} \in \mathbb{C}$.

The value semigroups of R_1 and R_2 are the same, denote this semigroup by S. In fact $S = \{0, 3, 5, 6, 8 \rightarrow\}$ is a symmetric semigroup. Using the criterion of Gorensteiness from [CDK] it is easy to see that R_1 is Gorenstein while R_2 is not. Observe that R_1 and R_2 are not residually rational. Thus the result of Kunz (see [K] or Theorem 1.4.1) does not remain true when we assume that the ring R is not residually rational.

Also the Jäger's characterization of a canonical ideal (see [J] or Theorem 1.4.2) does not remain true in this case. Consider

$$R = \mathbb{Q} + t^4\mathbb{Q}(\sqrt{2})[[t]], \tag{2.7}$$

a ring as in Proposition 2.1.1. Using this proposition a canonical ideal of R is

$$\omega = \mathbb{Q}(\sqrt{2}) + t\mathbb{Q}(\sqrt{2}) + t^2\mathbb{Q}(\sqrt{2}) + t^3\mathbb{Q} + t^4\mathbb{Q}(\sqrt{2})[[t]] \tag{2.8}$$

The value semigroup of the ring is $S = \{0, 4, \rightarrow\}$. Using the theory of the semigroups we have that $\Omega = \{0, 1, 2, 4, \rightarrow\}$ is a canonical ideal of the semigroup S. Note that $v(\omega) = \mathbb{N} \neq \Omega$.

The other implication in the Jäger's result is evidently not true. Considere

$$F = \mathbb{Q}(\sqrt{2}) + t\mathbb{Q}(\sqrt{2}) + t^2\mathbb{Q}(\sqrt{2}) + t^4\mathbb{Q}(\sqrt{2})[[t]]. \tag{2.9}$$

We have that F is a fractional ideal of the ring R, $R \subset F \subset \overline{R}$ and $v(F) = \Omega$, but F is not a canonical ideal of the ring R. This we can easily see from the fact that $\ell_R(F : \mathfrak{m}/F) \neq 1$, in fact is equal to 2.

Now we can proceede with presenting the generalized semigroup rings. The simplest type of a one-dimensional local analytically irreducible ring is the *semigroup ring* $k[[S]]$ associated to a numerical semigroup $S \subseteq \mathbb{N}$. If

$$S = \{s_0 = 0, s_1, \ldots, s_r \rightarrow\} \quad (n(S) = r), \tag{2.10}$$

then

$$R = k[[S]] = k + kt^{s_1} + \cdots + t^{s_r}k[[t]]. \tag{2.11}$$

Observe that such a ring is always residually rational. However, in [BF] the following generalization was given allowing non residually rational rings, too.

Definition 2.1.2. *Let $k \subseteq K$ be a finite extension of fields with the degree of the extension denoted by $n := dim_k(K) < \infty$. A ring R of the form*

$$R = k + V_1 t + ... + V_{N-1} t^{N-1} + t^N K[[t]] \tag{2.12}$$

where V_i ($i \in \{1, .., N-1\}$) are k-vector subspaces of K (we allow $V_i = \{0\}$) and $V_{N-1} \neq K$, is called a **generalized semigroup ring** *(or in short: a GSR). The integer N is said to be the* **conductor** *of R.*

Frequently we shall use a notation for which we must clarify the meaning of the symbol $\sum$. In this chapter, $\sum_{r=0}^{\infty} V_r t^r$ where $V_r \subseteq K$ ($r \in \mathbb{N}$) shall not mean the simple (algebraic) sum, but as usual, it will stand for the closure of $\oplus_{r \in \mathbb{N}} V_r t^r$ in $K[[t]]$. So, for example by our conventions $\sum_{r \in \mathbb{N}} k t^r$ stands for $k[[t]]$ and not for $k[t]$, and the above defined ring R may be written as

$$R = \sum_{i \in \mathbb{N}} V_i t^i \tag{2.13}$$

where here and all through the rest of this chapter, we have set $V_0 := k$ and $V_i := K$ for all $i \geq N$. Let us note now the following simple facts regarding the above definition of GSR rings.

1. R is a ring means that $V_i V_j \subseteq V_{i+j}$ for all $0 \leq i, j < N$.

2. A ring defined in this manner, due to the requirement $n < \infty$, is always Noetherian.

3. The integral closure of R is $K[[t]]$.

4. R is local and its (unique) maximal ideal is $\mathfrak{m} = \sum_{r=1}^{N-1} V_r t^r + t^N K[[t]]$.

5. R is analytically irreducible and furthermore, if $k \neq K$, then it is not residually rational, as the residue field of R is exactly k.

6.The conductor ideal of $\overline{R}$ in R is $R : \overline{R} = t^N K[[t]]$. This is the motivation of calling N the conductor of R. Observe that if the Frobenius number g of the value semigroup $v(R)$ of R equals to $N-1$ then $N = c$ is also the conductor of the value semigroup.

We saw before simple examples of GSR: the rings of the form $k_0 + t^l k_1[[t]]$. We can generalize this form of rings considering

$$R = \sum_{i=0}^{\infty} k_i t^i, \tag{2.14}$$

where k_i are subfields of a field L such that for every i and j, $k_i k_j \subseteq k_{i+j}$. Let $K = \cup_i k_i$. These rings were considered in [BF] where the authors proved that R is Noetherian if and only if $\dim_{k_0} K \leq \infty$. It is immediate that the integral closure of R, $\overline{R}$ is $K[[t]]$ and the value semigroup of R, $v(R) = \{i | \ k_i \neq 0\}$.

2.2 A canonical ideal of a GSR

§1. Let R be a GSR, defined by (2.12),

$$R = k + V_1 t + \dots + V_{N-1} t^{N-1} + t^N K[[t]] \tag{2.15}$$

where V_i ($i \in \{1, .., N-1\}$) are k-vector subspaces of K, $V_{N-1} \neq K$.

To deal with such rings we shall first study the structure of k-vector subspaces of K.

Definition 2.2.1. *For two k-vector subspaces V, W of K where $k \subseteq K$ is an extension of fields we shall set*

$$(V : W) := \{x \in K \mid \; xW \subseteq V\}. \tag{2.16}$$

Note that $(V : W)$ is again a k-vector subspace of K and that unlike with the division of numbers, the definition remains meaningful for $W = \{0\}$; in fact $(V : \{0\}) = K$. Some further observations are:

1. If $V_1 \subseteq V_2$ then $(V_1 : W) \subseteq (V_2 : W)$ while if $W_1 \subseteq W_2$ then we have the "inverted" relation $(V : W_1) \supseteq (V : W_2)$,
2. $(V : \langle W_1 W_2 \rangle) = ((V : W_1) : W_2)$ where $\langle W_1 W_2 \rangle \equiv \mathrm{Span}(W_1 W_2)$,
3. $W \subseteq (V : (V : W))$.

The third listed property may be a strict inclusion. This is related to another thing which is worth to comment; namely that in general the dimension of $(V : W)$ is not determined by the dimensions of the subspaces V, W and $V \cap W$. Indeed, consider the field extension

$$k := \mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}) =: K, \tag{2.17}$$

and set $V := (\sqrt{2} + \sqrt{3})^2 \mathbb{Q} + (2 + \sqrt{3})\sqrt{6}\mathbb{Q}$, $W_1 := \mathbb{Q}(\sqrt{2})$ and finally let $W_2 := (\sqrt{2} + \sqrt{3})\mathbb{Q} + \sqrt{6}\mathbb{Q}$. Then by direct calculation both

$$\dim_k(W_1) = \dim_k(W_2) = 2 \quad \text{and} \quad \dim_k(V \cap W_1) = \dim_k(V \cap W_2) = 0, \tag{2.18}$$

but $0 = \dim_k(V : W_1) \neq \dim_k(V : W_2) = 1$.

Nevertheless, at least in the special case when the codimension of V in K is one, it is possible to determine the dimension of $(V : W)$. This is due to the existence of a certain (nondegenerate) bilinear form that can be associated to such a subspace V. The following lemma and its proof is an adopted version of that of [CDK, Proposition 3.5].

Lemma 2.2.2. *Let $k \subseteq K$ be an extension of fields with $n = \dim_k K < \infty$ and $V \subset K$ is an $(n-1)$-dimensional k-vector subspace of K. Then for every k-vector subspace $W \subseteq K$ we have* $\dim(V : W) + \dim(W) = n$.

Proof. As $V \subset K$ is of dimension $n-1$, we have that there exists a linear surjection $\Phi : K \to k$ such that $\mathrm{Ker}\Phi = V$. Then define $B : K \times K \to k$ by the formula $B(a, b) \equiv \Phi(ab)$. It is clear that B is a nondegenerate bilinear form and hence

$$\dim(W) + \dim(W^{\perp_B}) = \dim(K) = n \tag{2.19}$$

where the B-orthogonal $W^{\perp_B} = \{x \in K|\ B(x, y) = 0, \forall y \in W\}$. The proof is then finished as a trivial check shows that, by its definition, the B-orthogonal of W is nothing else than the subspace $(V : W)$. □

As we have already remarked, W is always included in $(V : (V : W))$. Thus by the above lemma, using dimensional arguments, we can draw the following conclusion.

Corollary 2.2.3. *Let $k \subseteq K$ be an extension of fields with $n := \dim_k K < \infty$ and $V \subset K$ is an $n-1$-dimensional k-vector subspace of K. Then for every k-vector subspace $W \subseteq K$ we have $(V : (V : W)) = W$.*

§2. The above results show that among the k-subspaces of K, the $(n-1)$-dimensional ones play a similar role to that of the canonical ideals among fractional ideals. It is therefore natural to look for possible ways of exhibiting a canonical ideal of R starting from an $(n-1)$-dimensional subspace of K.

Theorem 2.2.4. *Let R be a GSR, $R = \sum_{r \in \mathbb{N}} V_r t^r$ where $V_0 = k$, $V_{N-1} \neq K$, and $V_r = K$ for every $r \geq N$. Moreover for a k-subspace $U \subseteq K$ setting*

$$\omega_U := \sum_{r=0}^{\infty} (U : V_{N-1-r}) t^r \subseteq K[[t]],$$

where we have set $V_j = \{0\}$ for all $j < 0$. If $\dim_k(U) = \dim_k(K) - 1$, then ω_U is a canonical ideal of R.

Proof. As

$$\langle V_{N-(s+r)-1} V_r \rangle \equiv \mathrm{Span}(V_{N-(s+r)-1} V_r) \subseteq V_{N-s-1} \tag{2.20}$$

for every r, $s \in \mathbb{N}$, we have that

$$(U : V_{N-s-1}) \subseteq (U : \langle V_{N-(s+r)-1} V_r \rangle) = ((U : V_{N-(s+r)-1}) : V_r). \tag{2.21}$$

But $(A : B) = C$ implies that $BC \subseteq A$, so "multiplying" both sides of the above containment by V_r we get that for every $r,\ s \in \mathbb{N}$:

$$V_r(U : V_{N-s-1}) \subseteq (U : V_{N-(s+r)-1}) \tag{2.22}$$

This shows that $R\omega_U \subseteq \omega_U$; i.e. that ω_U is a fractional ideal (as it is clearly closed under addition). What remains to show is that ω_U is canonical which is equivalent to prove that $\ell_R((\omega_U : \mathfrak{m})/\omega_U) = 1$; see [HK, Satz 3.3] or Theorem 1.1.21.

As $k \subset R$, we may view the inclusion $\omega_U \subseteq (\omega_U : \mathfrak{m})$ as an inclusion of k-vector spaces. In fact also in a more general case when the residue field of R is not a subset of the ring we have already seen at the proof of Theorem 1.1.21 that $\omega : \mathfrak{m}/\omega$ is a k-vector space.

We shall now calculate the codimension of the inclusion of the k-vector spaces $\omega_U \subseteq \omega_U : \mathfrak{m}$. (By *codimension* of an inclusion $U_1 \subseteq U_2$ of vector spaces over a field k we mean the dimension of the quotient vector space U_2/U_1.)

Let now

$$U_r := (U : V_{N-1-r}). \tag{2.23}$$

So in particular we have $U_{N-1} = U$. Recall that $\mathfrak{m}$ stands for the maximal ideal of R; that is, in this case $\mathfrak{m} = \sum_{r=1}^{\infty} V_r t^r$. We shall write $\omega_U : \mathfrak{m}$ in the form

$$\omega_U : \mathfrak{m} = \sum_{j \in \mathbb{Z}} W_j t^j, \tag{2.24}$$

where W_j are k-vector subspaces of K. (Not every fractional ideal of R can be written in this form, but it is an easy exercise to show that if I and J are two fractional ideals of R of this form then also $I : J$ is of this form.)

By the definition of quotient of ideals, as

$$\sum_{j \in \mathbb{Z}} W_j t^j = \sum_{r=0}^{\infty} U_r t^r : \sum_{r=1}^{\infty} V_r t^r \tag{2.25}$$

we find that

$$W_j = \bigcap_{r>0} (U_{r+j} : V_r). \tag{2.26}$$

We shall now consider the case when $j < N-1$. Then setting $r := N-1-j$ we have that $r > 0$ and $r + j = N-1$ resulting

$$W_j \subseteq (U_{r+j} : V_r) = (U : V_{N-1-j}) = U_j. \tag{2.27}$$

But ω_U is a fractional ideal so $(\omega_U : \mathfrak{m}) \supseteq (\omega_U : R) = \omega_U$ and hence $W_j \supseteq U_j$ for every $j \in \mathbb{Z}$. Thus by the above equation W_j actually coincides with U_j for every $j < N-1$.

Let us now consider the remaining case of $j \geq N-1$. In this case $r+j \geq N$ since $r > 0$ and so $U_{r+j} = K$ resulting that

$$W_j = \bigcap_{r>0}(U_{r+j} : V_r) = \bigcap_{r>0}(K : V_r) = \bigcap_{r>0} K = K. \tag{2.28}$$

To summarize: $W_j = U_j$ for every $j \in \mathbb{Z}$ except for $j = N-1$ in which case $U_j = U_{N-1} = U \subset K$ is a subspace of codimension 1, whereas $W_j = W_{N-1} = K$. It follows that the inclusion $\omega_U \subseteq (\omega_U : \mathfrak{m})$, as an inclusion of k vector subspaces, is of codimension 1. But as $k \subset R$, this shows that $(\omega_U : \mathfrak{m})/\omega_U$ has no proper R-submodules. Since $\omega_U : \mathfrak{m}$ is really bigger than ω_U, this in turn implies that the length $\ell_R((\omega_U : \mathfrak{m})/\omega_U) = 1$, which concludes the proof. $\square$

Let us now see same examples of computing a canonical ideal for a GSR.

Example 2.2.5. Let

$$R := \mathbb{Q}+\mathbb{Q}t^5+\mathbb{Q}(\sqrt{2})t^{10}+\mathbb{Q}(\sqrt{2})t^{11}+t^{14}\mathbb{Q}(\sqrt{2})[[t]]. \tag{2.29}$$

With the notations of Theorem 2.2.4 $k = \mathbb{Q}$, $K = \mathbb{Q}(\sqrt{2})$, $N = 14$. Note that $N = c$, where c is the conductor of $S := v(R)$. Consider $U = \mathbb{Q}$ which is a one-dimensional vector space of $\mathbb{Q}(\sqrt{2})$. Then

$$\begin{aligned} \omega_{\mathbb{Q}} \ = \ & \mathbb{Q}(\sqrt{2})+\mathbb{Q}(\sqrt{2})t+\mathbb{Q}(\sqrt{2})t^4+\mathbb{Q}(\sqrt{2})t^5+\mathbb{Q}(\sqrt{2})t^6 \\ & +\mathbb{Q}(\sqrt{2})t^7+\mathbb{Q}t^8+\mathbb{Q}(\sqrt{2})t^9+\mathbb{Q}(\sqrt{2})t^{10}+\mathbb{Q}(\sqrt{2})t^{11} \\ & +\mathbb{Q}(\sqrt{2})t^{12}+\mathbb{Q}t^{13}+t^{14}\mathbb{Q}(\sqrt{2})[[t]] \end{aligned} \tag{2.30}$$

is a canonical ideal of R.

Example 2.2.6. Let

$$R := \mathbb{R}+i\mathbb{R}t^4+i\mathbb{R}t^5+i\mathbb{R}t^6+\mathbb{C}t^7+\mathbb{C}t^8+\mathbb{R}t^9+\mathbb{R}t^{10}+t^{11}\mathbb{C}[[t]]. \tag{2.31}$$

For this ring $k = \mathbb{R}, K = \mathbb{C}$ and $N = 11$ (and already with such N it seems rather difficult to find a canonical ideal by some direct method). However, we now know that it is enough to find a real subspace of $\mathbb{C}$ of codimension 1, which is much more simpler; e.g. $\mathbb{R}$ is such a subspace. Then by direct calculation

$$\omega_{\mathbb{R}} = \sum_j(\mathbb{R} : V_{10-j})t^j = \mathbb{R} + \mathbb{R}t + i\mathbb{R}t^4 + i\mathbb{R}t^5 + i\mathbb{R}t^6 + t^7\mathbb{C}[[t]] \tag{2.32}$$

and by the above theorem this is a canonical ideal.

We have denoted the canonical ideal constructed in Theorem 2.2.4 by ω_U, emphasizing the fact that it depends on the subspace U.

Lemma 2.2.7. *With the notations of Theorem 2.2.4, $R \subseteq \omega_U$ if and only if $V_{N-1} \subseteq U$.*

Proof. If $V_{N-1} \subseteq U$ then $V_j V_{N-1-j} \subseteq V_{N-1} \subseteq U$ and so $V_j \subseteq (U : V_{N-1-j}) = U_j$. This shows the "if" part; the "only if" part is trivial. $\square$

§3. The natural question is: can every canonical ideal of R be written in the form ω_U? The answer in general is no. However, it is known that if ω_1, ω_2 are two canonical ideals of R then there exists a nonzero element $a \in \mathbb{Q}(R)$ such that $\omega_2 = a\omega_1$; see [HK] or Proposition 1.1.19.

All notations and assumptions regarding R are those appearing in Theorem 2.2.4, so, R is a GSR,

$$R = \sum_{r \in \mathbb{N}} V_r t^r, \tag{2.33}$$

where $V_0 = k$, $V_{N-1} \neq K$ and $V_r = K$ for all $r \geq N$. Moreover for a k-subspace U of K we consider ω_U constructed in Theorem 2.2.4.

Lemma 2.2.8. *Suppose that $U \subset K$ is of codimension 1 and $x \in K[[t]]$ is such that $(1 + tx)\omega_U$ is of the form $\sum_{r \in \mathbb{N}} W_r t^r$ where W_r ($r \in \mathbb{N}$) are k-subspaces of K. Then $(1 + tx) \in R$ and so $(1 + tx)\omega_U = \omega_U$.*

Proof. Let $r \in \mathbb{N}$ and $b \in (U : V_{N-1-r})$. Then $(1 + tx)bt^r \in (1 + tx)\omega_U$ as $bt^r \in \omega_U$. However, as $(1 + tx)\omega_U$ is of the form $\sum_{r \in \mathbb{N}} W_r t^r$, if an element belongs to it, then its lowest order term is also contained in it. It follows that $bt^r \in (1 + tx)\omega_U$ and thus by the arbitrariness of $r \in \mathbb{N}$ and $b \in (U : V_{N-1-r})$ we have that $\omega_U \subseteq (1 + tx)\omega_U$ and hence

$$R = (\omega_U : \omega_U) \supseteq (\omega_U : (1 + tx)\omega_U) = (1 + tx)^{-1}(\omega_U : \omega_U) = (1 + tx)^{-1}R \tag{2.34}$$

where we have used the well-known fact already mentioned after Definition 1.1.1, namely that for a canonical ideal ω one has $\omega : \omega = R$. As $1 \in R$, by the above containment from equation 2.34, $(1 + tx)^{-1} \in R$ and so actually $(1 + tx) \in R$. (Indeed, R is a local ring and $(1 + tx)^{-1}$ is of order 0 and so it is not in $\mathfrak{m}$. This implies that $(1 + tx)^{-1}$ is invertible *in* R.) $\square$

Proposition 2.2.9. *Suppose that*

$$\omega = \sum_{r \in \mathbb{N}} W_r t^r \subseteq K[[t]]$$

is a canonical ideal of R and $W_0 \neq 0$. Then $\omega = \omega_U$ where $U = W_{N-1}$.

Proof. Let $U' \subset K$ be a $(\dim_k(K)-1)$-dimensional k-subspace of K. As $\omega_{U'}$ is a canonical ideal, there exists an $a \in Q(R) \equiv K((t))$, $a \neq 0$ such that $\omega = a\omega_{U'}$ (see [HK] or Proposition 1.1.19). Since the minimal order of elements in ω as well as in $\omega_{U'}$ is zero, a must be of order zero. (As $V_{N-1} \neq K$, by the definition of $\omega_{U'}$, using Lemma 2.2.2, we have that $U'_0 = (U' : V_{N-1}) \neq \{0\}$ and thus $\omega_{U'}$ indeed contains elements of order 0.) So

$$a = \alpha(1 + tx) \tag{2.35}$$

for some $\alpha \in K$, $\alpha \neq 0$ and $x \in K[[t]]$. It is clear that

$$\alpha\omega_{U'} = \omega_{\alpha U'}, \tag{2.36}$$

and so by the previous lemma

$$\omega = a\omega_{U'} = (1 + tx)\omega_{\alpha U'} = \omega_{\alpha U'}. \tag{2.37}$$

□

Corollary 2.2.10. *Let $\omega = \sum_{r\in\mathbb{N}} W_r t^r \subseteq K[[t]] \equiv \overline{R}$ be a fractional ideal of R and assume that $W_0 \neq \{0\}$. Then ω is a canonical ideal of R if and only if*

$$\forall r \in \mathbb{N} : \quad \dim_k(W_r) + \dim_k(V_{N-1-r}) = \dim_k(K) \equiv n. \tag{2.38}$$

Proof. First we shall prove the "only if" part. From Proposition 2.2.9 we have that $\omega = \omega_U$, where $U = W_{N-1}$. Theorem 2.2.4 implies that $W_i = U : V_{N-1-i}$, for every $i \in \mathbb{N}$ and thus equation 2.38 follows from Lemma 2.2.2. For the "if" part, let us observe that by (2.38) we have that $\dim_k(W_{N-1}) = n - 1$. Moreover, as ω is at least a fractional ideal, we have that $V_{N-r-1}W_r \subseteq W_{N-1}$ and so $W_r \subseteq (W_{N-1} : V_{N-r-1})$. However, by reasons of dimension, using Lemma 2.2.2 and equation (2.38) we obtain that this inclusion is in fact an equality and hence $\omega = \omega_{W_{N-1}}$ and thus by Theorem 2.2.4 it is indeed canonical. □

Applying Proposition 2.2.9 to the residually rational case we obtain that if R is the semigroup ring, $R = k[[S]]$, then between R and $\overline{R}$ there exists a unique canonical ideal of the form

$$\sum_{i\in\Omega} kt^i, \tag{2.39}$$

where Ω is the standard canonical ideal of the semigroup S. It was already known that, even between R and $\overline{R}$, there are many canonical ideals of $k[[S]]$, but not of the previous form. An easy example is the follwing one (appearing in [D'Anna1]):

$$R = k[[t^3, t^5, t^7]]. \tag{2.40}$$

In this case, appart from the "standard" canonical ideal

$$\omega_{\text{st}} = k + kt^2 + kt^3 + t^5 k[[t]], \tag{2.41}$$

one has that for each $a \in k$ the fractional ideal

$$\omega_a = k + k(t^2 + at^4) + kt^3 + t^5 k[[t]] \tag{2.42}$$

is a canonical ideal of R. Note that $\omega_{\text{st}} = \omega_0$.

In the non residually rational case the canonical ideals of the GSR $R = \sum_{i\in\mathbb{N}} V_i t^i$, which are of the form $\sum_{i\in\mathbb{N}} U_i t^i$ are infinitly many. In fact if we consider one canonical ideal of this form, then it is equal to ω_U constructed in Theorem 2.2.4, for an $(n-1)-$dimensional $k-$vector subspace of K. Then all others canonical ideals of this particular form are in fact $\omega_{\alpha U} = \alpha\omega_U$ for an arbitrary $\alpha \in K$ as resulting from the proof of Proposition 2.2.9. Note that we obtain also the fact that if we have a field extension $k \subseteq K$ of finite degree n and U is a $(n-1)$-dimensional $k-$vector subspace of K then all $(n-1)$-dimensional $k-$vector subspaces in K are of the form αU for some $\alpha \in K$. To show this consider two $(n-1)$-dimensional k-vector subspaces of K, U_1 and U_2. Then by Lemma 2.2.2, $\dim_k(U_1 : U_2) = 1$. Take $a \in U_1 : U_2$, $a \neq 0$. Thus $aU_2 \subseteq U_1$. But $aU_2 \simeq U_2$ as k-vector spaces. Therefore $aU_2 = U_1$.

Let us see these facts on a concrete example. Consider the field extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{2})$ of degree 3. Let R be the ring

$$R = \mathbb{Q} + \mathbb{Q}(\sqrt[3]{2})t^3 + \alpha\mathbb{Q}t^5 + t^6\mathbb{Q}(\sqrt[3]{2}), \tag{2.43}$$

where α is an arbitrary element of $\mathbb{Q}(\sqrt[3]{2})$. Take U a 2-dimensional $\mathbb{Q}$-vector subspace of $\mathbb{Q}(\sqrt[3]{2})$. Then by Theorem 2.2.4 a canonical ideal of R is

$$\omega_U = \alpha^{-1}U + \mathbb{Q}(\sqrt[3]{2})t + \mathbb{Q}(\sqrt[3]{2})t^3 + \mathbb{Q}(\sqrt[3]{2})t^4 + Ut^5 + t^6\mathbb{Q}(\sqrt[3]{2})[[t]]. \tag{2.44}$$

All the others canonical ideals of the special form $\sum_i U_i t^i$ are

$$\omega_{U'} = \alpha^{-1}\beta U + \mathbb{Q}(\sqrt[3]{2})t + \mathbb{Q}(\sqrt[3]{2})t^3 + \mathbb{Q}(\sqrt[3]{2})t^4 + \beta Ut^5 + t^6\mathbb{Q}(\sqrt[3]{2})[[t]], \tag{2.45}$$

where $U' = \beta U$ for some $\beta \in \mathbb{Q}(\sqrt[3]{2})$.

Note that from Corollary 2.2.10 we obtain that the value set of all canonical ideal of the GSR R with the properties as in Corollary 2.2.10, is the same. In fact for the residually rational case we have the Jäger's Theorem (see [J] or Theorem 1.4.2).

2.3 Apéry Basis of a GSR

Let R be a GSR,

$$R = \sum_{i \in \mathbb{N}} V_i t^i, \tag{2.46}$$

where $V_i \subseteq K$, k-vector subspaces such that $V_0 = k$, $V_{N-1} \neq K$ and $V_r = K$ for every $r \geq N$. Recall that n is the degree of the field extension $k \subseteq K$. For this section we shall assume $n \geq 2$. As $R \subseteq K[[t]]$, we have that R is complete in the $\mathfrak{m}$-adic topology.

As we have already seen in Section 1.2 there exists a DVR $W \subseteq R$ for every R analytically irreducible. In our case i.e. R is a GSR this DVR is in fact

$$W = k[[\alpha t^m]], \tag{2.47}$$

where $\alpha \in K$ and $m \in v(R)$ is the smallest non zero value of elements of R. With the notation of Section 1.2 $x = \alpha t^m$. We know that every fractional ideal of R (then also the ring R itself) is a free W-module of rank equal to the multiplicity of the ring R, $e(R)$ (see [Ma] or Corrolaries 1.2.7 and 1.2.8). Our aim is to compute a free basis of the ring R as W-module, construction which can be done also for an arbitrary fractional ideal of R

We consider the elements of R of values congruent to i modulo m, where i is a natural number $0 \leq i \leq m-1$. Consider an element of R of smallest value among all these and denote it by $y_0^{(i)}$. There exist $\beta_0^{(i)} \in K$ and $s_0^{(i)} \in \mathbb{N}$ such that

$$y_0^{(i)} = \beta_0^{(i)} t^{s_0^{(i)} m + i}. \tag{2.48}$$

We know that there exists $N \in \mathbb{N}$ such that $t^N K[[t]] \subset R$ and also $n \geq 2$, then we can find an element

$$y_1^{(i)} = \beta_1^{(i)} t^{s_1^{(i)} m + i}, \tag{2.49}$$

$\beta_1^{(i)} \in K$, $s_1^{(i)} \in \mathbb{N}$, such that $\beta_0^{(i)}/\alpha^{s_0^{(i)}}$ and $\beta_1^{(i)}/\alpha^{s_1^{(i)}}$ are elements of K which are linearly independent over k and $y_1^{(i)}$ is of smallest value with this property. We can do this till the n-th step, then we constructed n elements of R of the value congruent to i modulo m,

$$\{y_0^{(i)}, y_1^{(i)}, ..., y_{n-1}^{(i)}\} \tag{2.50}$$

with

$$y_j^{(i)} = \beta_j^{(i)} t^{s_j^{(i)} m + i} \tag{2.51}$$

such that

$$\{\beta_0^{(i)}/\alpha^{s_0^{(i)}}, \beta_1^{(i)}/\alpha^{s_1^{(i)}}, ..., \beta_{n-1}^{(i)}/\alpha^{s_{n-1}^{(i)}}\} \tag{2.52}$$

is a basis of the k-vector space K. We can do this for every $i \in \mathbb{N}$, $0 \leq i \leq m-1$.

Theorem 2.3.1. *The elements*

$$\{y_j^{(i)}|\ \ i \in \{0, ...m-1\}, j \in \{0, ...n-1\}\} \tag{2.53}$$

form a free basis of R over W.

Proof. Denote $I = \{0, ...m-1\}$ and $J = \{0, ...n-1\}$. For prooving that (2.53) is a linearly independent system of elements we consider a linear combination:

$$\sum_{(i,j)\in I\times J} w_j^{(i)} y_j^{(i)} = 0, \tag{2.54}$$

where $w_j^{(i)} \in W$ for every $i \in I$ and $j \in J$,and

$$w_j^{(i)} = a_j^{(i)} (\alpha t^m)^{r_j^{(i)}}, \tag{2.55}$$

$a_j^{(i)} \in k$ and some $r_j^{(i)} \in \mathbb{N}$.

Assume that there exists a non trivial solution of 2.54, namely elements $w_j^{(i)} \in W$ satisfying equation 2.54 with

$$F = \{(i,j) \in I \times J|\ \ w_j^{(i)} \neq 0\} \neq \emptyset. \tag{2.56}$$

Then equation 2.54 becomes

$$\sum_{(i,j)\in F} w_j^{(i)} y_j^{(i)} = 0. \tag{2.57}$$

Consider

$$h = min\{v(w_j^{(i)} y_j^{(i)}) \neq 0|\ \ (i,j) \in F\}, \tag{2.58}$$

and let P be the set

$$P = \{(i,j) \in F|\ \ v(w_j^{(i)} y_j^{(i)}) = h\}. \tag{2.59}$$

Note that from our assumption $P \neq \emptyset$. If $(i,j) \in P$ then $v(w_j^{(i)} y_j^{(i)}) = h$ and $v(w_j^{(i)} y_j^{(i)}) \equiv i$ (modulo m). This means that there exists a unique $i \in \{0, ..., m-1\}$ such that P is of the form $P = \{i\} \times P_1$. Take $P_1 = \{j_0, ..., j_s\}$, and $h = mr + i$ for some $r \in \mathbb{N}$ and $r_j^{(i)} = r - s_j^{(i)}$. Then the sum which is a part of equation 2.57 becomes:

$$\sum_{j\in\{j_0,\ldots,j_s\}} w_j^{(i)} y_j^{(i)} = (a_{j_0}^{(i)} \alpha^v \frac{\beta_{j_0}^{(i)}}{\alpha^{s_{j_0}^{(i)}}} + ... + a_{j_s}^{(i)} \alpha^r \frac{\beta_{j_s}^{(i)}}{\alpha^{s_{j_s}^{(i)}}}) t^{mr+i}. \tag{2.60}$$

By equation 2.57 we have that

$$v(\sum_{j\in P_1} w_j^{(i)} y_j^{(i)}) > h. \tag{2.61}$$

Thus

$$a_{j_0}^{(i)}\alpha^v \frac{\beta_{j_0}^{(i)}}{\alpha^{s_{j_0}^{(i)}}} + ... + a_{j_s}^{(i)}\alpha^r \frac{\beta_{j_s}^{(i)}}{\alpha^{s_{j_s}^{(i)}}} = 0, \tag{2.62}$$

and by the fact that $\beta_{j_l}^{(i)}/\alpha^{s_{j_l}^{(i)}}$ with $l \in \{0, ..., s\}$ are linearly independent over k we have that $a_{j_l}^{(i)} = 0$ for every l, then $w_{j_l}^{(i)} = 0$ which is in contradiction with our assumption.

Now we shall prove that the elements $y_j^{(i)}$ form a system of generators for R as W-module. Take an arbitrary element $y \in R$ and suppose that its value is congruent to i modulo m. There exist $\gamma \in K$ and $r \in \mathbb{N}$ such that

$$y = \gamma t^{mr+i}. \tag{2.63}$$

By the construction of the elements $y_j^{(i)}$ we have that $s_0^{(i)} \leq r$. If $s_j^{(i)} \leq r$ for $j = 1, 2...l$ and $s_{l+1}^{(i)} > r$ then by the construction of the elements $y_j^{(i)}$ we have that all $\beta_j^{(i)}/\alpha^{s_j^{(i)}}$ with $j = 0, ..., l.$ and γ/α^r are linearly dependent. Suppose that

$$\gamma = \alpha^r \sum_{j=0}^{l} a_j \frac{\beta_j^{(i)}}{\alpha^{h-s_j^{(i)}}}, \tag{2.64}$$

where $a_j \in k$ for every $j = 0, ..., l$. We can consider the element $x_0 \in R$,

$$x_0 = \sum_{j=0}^{l} a_j x^{r-s_j^{(i)}} y_j^{(i)} = \alpha^r \sum_{j=0}^{l} a_j \frac{\beta_j^{(i)}}{\alpha^{s_j^{(i)}}} t^{mr+i} = \gamma t^{mr+i}. \tag{2.65}$$

We have that $v(y - x_0) > v(y)$ and x_0 is generated over W by some elements from the system $y_j^{(i)}$. We can do the same for the element $y - x_0$ and so on, then we obtain y as a series generated by the elements $y_j^{(i)}$, using the fact that the ring R is complete in the $\mathfrak{m}$-adic topology. □

Definition 2.3.2. *We call a basis* $\{y_j^{(i)} | i \in \{0, ..., m\}, j \in \{0, ..., n\}\}$ *constructed as in the described way a* **generalized Apéry basis** *of the GSR* R.

Example 2.3.3. Let

$$R = \mathbb{R}[[it^3, t^7, t^{11}, it^{12}]]. \tag{2.66}$$

For this ring $k=\mathbb{R}$, $K=\mathbb{C}$. Then the extension field has degree 2. The DVR included in the ring R is $W=\mathbb{R}[[it^3]]$. An Apéry bases of R over W constructed in the way presented before is:

$$R=W+it^{12}W+t^7W+it^{19}W+t^{11}W+t^{14}W. \tag{2.67}$$

2.4 Associated GSR

§1. We shall now leave the realm of generalized semigroup rings. We return to our ring R local one-dimensional analytically irreducible. Recall that we denoted by n the degree of the field extension $k\subseteq K$ where $k:=R/\mathfrak{m}$, the residue field of R and $K:=\overline{R}/\mathfrak{n}$, the residue field of the integral closure, $\overline{R}$. By definition $n:=\dim_k(K)$. We shall not assume residual rationality, that is, we shall not assume n to be 1.

Every ideal of $\overline{R}$ is principal and is a power of the maximal ideal. Thus we may fix a $t\in\overline{R}$ such that $\mathfrak{n}=t\overline{R}$ and we can normalize our valuation so that $v(t)=1$.

Let F be any fractional ideal of R. Then

$$F(i):=\{x\in F|v(x)\geq i\} \tag{2.68}$$

is a fractional ideal of R for every $i\in\mathbb{Z}$ and we have $F(i)\subseteq F(j)$ for every $i\geq j$. The R-modules $F(i)/F(i+1)$ are also vector spaces over k; we shall denote these by $V_F(i)$. For the special case of $F=R$, these vector spaces were already considered in the work [CDK] of Campillo, Delgado and Kiyek.

Passing from the ring to its value semigroup is in fact the passage from the ring of value semigroup S to the semigroup ring $k[[S]]$. We shall show that when the ring is not residually rational we can associate to it a GSR which encodes the information about the ring itself. This GSR may be viewed like a generalization of the value semigroup in non residually rational case.

For every fractional ideal F of R we can define a linear application

$$\eta_i^F:V_F(i)\to K,\ \eta_i^F([z])=zt^{-i}(mod\ \underline{n}), \tag{2.69}$$

where by $[\cdot]$ we denote the classes modulo $F(i+1)$. The application η_i^F is well defined and injective. The image $\eta_i^F(V_F(i))$ is a k vector subspace of K, which we shall denote by $\widetilde{V_F(i)}$. Of course $\dim_K(\widetilde{V_F(i)})=\dim_K(V_F(i))$.

If F is a fractional ideal then $F(i)R(j)\subseteq F(i+j)$ and for every $z\in F(i)$ and $w\in R(j)$ we have the equality:

$$\eta_i^F([z])\eta_j^R([w])=\eta_{i+j}^F([zw]) \tag{2.70}$$

by which it is not too hard to see that

$$\widetilde{R} := \sum_{i \in \mathbb{N}} \widetilde{V_R(i)} t^i \tag{2.71}$$

is a GSR; we shall say that $\widetilde{\mathbf{R}}$ is the **GSR associated** to R. The **conductor** of R is simply defined to be equal with that of the associated GSR and throughout the rest of this chapter it will be denoted by N. This is in agreement with the fact that $R : \overline{R}$ (or as it is called: the conductor ideal of $\overline{R}$ in R) equals to $t^N\overline{R}$. Note also that in the residually rational case $\widetilde{R}$ is exactly the semigroup ring $k[[v(R)]]$. Thus in this case, the passage from the ring to its associated GSR is essentially nothing else than the usual reduction to numerical semigroups.

In the same way, to every fractional ideal F of R we can associate a fractional ideal of the GSR $\widetilde{R}$ by

$$\widetilde{F} := \sum_{i \in \mathbb{Z}} \widetilde{V_F(i)} t^i. \tag{2.72}$$

Example 2.4.1. Consider $R := \mathbb{R}[[it^3 + t^4, t^5, it^{10} + t^{11}]]$. It is easy to show that $\widetilde{R}$ is exactly the ring $R_2 = \mathbb{R}[[it^3, t^5, it^{10}, it^{17}]]$. Since

$$(it^3+t^4)^5 - (it^{10}+t^{11})t^5 + 4((it^3+t^4)t^5)^2 = -6it^{17} + \text{higher order terms}, \tag{2.73}$$

it^{17} indeed appears in $\widetilde{R}$. Note that the image of the given set that generates R (as an $\mathbb{R}$-algebra), namely the set

$$\{\eta_3^R(it^3 + t^4)t^3,\ \eta_5^R(t^5)t^5,\ \eta_{10}^R(it^{10} + t^{11})t^{10} = \{it^3, t^5, it^{10}\} \tag{2.74}$$

does not generate $\widetilde{R}$ (as an $\mathbb{R}$-algebra); $\widetilde{R} \neq \overline{R}[[it^3, t^5, it^{10}]] = R_1$. For example, $it^{17} \in \widetilde{R}$ whereas it does not belong to R_1.

§2. We have seen in Section 1.4 how to compute lengths in a ring which is also residually rational, see Theorem 1.4.6 or [Mat]. Let us see now how we can compute lengths in R which is not residually rational, using the k vector spaces $V_F(i)$ defined above for a fractional ideal F of R by (2.68).

Proposition 2.4.2. *Let E, F be two fractional ideals of R such that $E \subseteq F$. Then there exist s_0, and $s_1 \in \mathbb{N}$ such that*

$$\ell_R(F/E) = \sum_{r=s_0}^{s_1-1} [\dim_k(V_F(r)) - \dim_k(V_E(r))]. \tag{2.75}$$

Proof. We know that there exist n_1 and $n_2 \in \mathbb{Z}$ such that $E : \overline{R} = t^{n_1}\overline{R} = E(n_1)$ and $F : \overline{R} = t^{n_2}\overline{R} = F(n_2)$. Take $s_1 := max(n_1, n_2)$. We also know that there exist the integers $m_1, m_2 \leq 0$, $m_1 \in v(E)$, the smallest element, and respectively, $m_2 \in v(F)$ with the same property. Consider $s_0 := \min(m_1, m_2)$.

It is easy to see that:

$$\ell_R(F/F(s_1)) = \sum_{r=s_0}^{s_1-1}(\ell_R(F(r)/F(r+1))) = \sum_{r=s_0}^{s_1-1}(\dim_k(V_F(r))). \tag{2.76}$$

Similarly we have $\ell_R(E/E(s_1)) = \sum_{r=s_0}^{s_1-1}\dim_k(V_E(s))$. But as $E(s_1) = t^{s_1}\overline{R} = F(s_1)$, from the chain of inclusions $F(s_1) = E(s_1) \subseteq E \subseteq F$ we obtain $\ell_R(F/E) = \ell_R(F/F(s_1)) - \ell_R(E/E(s_1))$ concluding our proof. $\square$

Corollary 2.4.3. *Let E and F be two fractional ideals of the ring R such that $E \subseteq F \subseteq \overline{R}$. If $\dim_k(V_E(i)) = \dim_k(V_F(i))$ for every $i \in \mathbb{N}$, then $E = F$.*

Many properties of fractional ideals of R can be reduced to properties of fractional ideals of the associated GSR. For example, by Proposition 2.4.2 if E and F are two fractional ideals with $E \subseteq F$, then

$$\ell_R(E/F) = \ell_{\widetilde{R}}(\widetilde{E}/\widetilde{F}). \tag{2.77}$$

§3. It is rather obvious that the passage to the GSR preserves, for example, the inclusion of fractional ideals (i.e. if $F_1 \subseteq F_2$ then $\widetilde{F_1} \subseteq \widetilde{F_2}$). It is somewhat less obvious whether this passage also "commutes" with the quotient of ideals.

Lemma 2.4.4. *Let F_1, F_2 be two fractional ideals of R. Then*

$$\widetilde{F_1 : F_2} \subseteq \widetilde{F_1} : \widetilde{F_2}. \tag{2.78}$$

Proof. Both $\widetilde{F_1}, \widetilde{F_2}$ and $\widetilde{F_1 : F_2}$ are of the form $\sum_{r\in\mathbb{Z}} W_r t^r$ where W_r $(r \in \mathbb{Z})$ are k subspaces of K. To be able to distinguish, we shall give an upper index and introduce W_r^1, W_r^2 and W_r^3, corresponding to $\widetilde{F_1}, \widetilde{F_2}$ and $\widetilde{F_1 : F_2}$, respectively.

We have to show that $\widetilde{F_2}(\widetilde{F_1 : F_2}) \subseteq \widetilde{F_1}$ or equivalently, that $W_r^2 W_k^3 \subseteq W_{r+k}^1$ for all $r, k \in \mathbb{Z}$. So let $\alpha \in W_r^2$ and $\beta \in W_k^3$; by definition this means that $\exists a, b \in K[[t]]$ such that

$$\alpha t^r + a t^{r+1} \in F_2 \quad \text{and} \quad \beta t^k + b t^{k+1} \in F_1 : F_2. \tag{2.79}$$

Since $F_2(F_1 : F_2) \subseteq F_1$, we have that $(\alpha t^r + a t^{r+1})(\beta t^k + b t^{k+1}) = (\alpha\beta t^{r+k}+$ higher order terms) is an element of F_1 and hence that $\alpha\beta \in W_{r+k}^1$. $\square$

Note that inclusion (2.78) may be strict. For example, with k being a field with $\mathrm{char}(k) \neq 2$, let $R := k[[t^4, t^6 + t^7, t^{13}]]$. Then the maximal ideal $\mathfrak{m}$, as a k-algebra, is generated by the set of elements $\{t^4, t^6 + t^7, t^{13}\}$ and

$$F := kt + kt^5 + k(t^7 + t^8) + kt^9 + k(t^{11} + t^{12}) + t^{13}k[[t]] \qquad (2.80)$$

is a fractional ideal of R for which $\widetilde{F : \mathfrak{m}} \neq \widetilde{F} : \widetilde{\mathfrak{m}}$. Indeed, by direct calculations, $t^3 \in \widetilde{F} : \widetilde{\mathfrak{m}}$, but it is not an element of $\widetilde{F : \mathfrak{m}}$.

§4. Let us now describe the process of associating a GSR to a ring in a slightly different way. Let the local ring R of maximal ideal $\mathfrak{m}$ and residue field k be a subring of the ring of formal series in one variable, $K[[t]]$, where $k \subset K$ is a finite extension of fields. Then the integral closure of R can be identified with $K[[t]]$, and the total ring of fractions with $K((t))$. Define the function

$$\Phi : K((t)) \to K((t)), \qquad (2.81)$$

by the formula

$$\Phi(\gamma t^i + \text{higher degree terms}) = \gamma t^i. \qquad (2.82)$$

In simple words, Φ "cuts" a formal power series, leaving only the first term of it, and as a function, it takes values in $\cup_{i\in\mathbb{Z}} Kt^i$, the set of all monomials in $K((t))$. It is evident that for every f, $g \in K((t))$

$$\Phi(fg) = \Phi(f)\Phi(g) \qquad (2.83)$$

but in general

$$\Phi(f + g) \neq \Phi(f) + \Phi(g) \qquad (2.84)$$

unless $\mathrm{order}(f) = \mathrm{order}(g)$. Thus Φ is not a homomorphism, and in general the image of a ring or an ideal is not any more a ring or an ideal.

Since $k \subset R \subset K[[t]] \subset K((t))$, we can think of all these rings as $k-$vector spaces, too. The map Φ fails to be a linear map, but we can consider the linear space generated by the image of a set in $K((t))$. More precisely, we shall set

Definition 2.4.5. *For every subset $F \subset K((t))$, let*

$$\widetilde{F} := \mathrm{Span}_k(\Phi(F)) = \{\sum_{i\in I} \alpha_i \Phi(x_i)| \ \alpha_i \in k, x_i \in F, \ |I| < \infty\}. \qquad (2.85)$$

Some trivial facts are the following:

1. As R is a ring, $\widetilde{R}$ is also ring; in fact it is exactly the (previously defined) associated GSR.
2. For any fractonal ideal F of R, the set $\widetilde{F}$ is fractional ideal of $\widetilde{R}$.
3. If $F \subseteq H$, then $\widetilde{F} \subseteq \widetilde{H}$.

These observations in fact were already mentioned before this (second) definition of associated objects. The point is, that thinking in this new way makes certain — already discussed — things much more clear. For example, as Φ respects the multiplication, we have that

$$\widetilde{FH} = \mathrm{Span}\{\widetilde{F}\widetilde{H}\} \tag{2.86}$$

and so it follows easily that if F, H are two fractional ideals, then — since $(F : H)H \subseteq F$ —

$$\widetilde{(F : H)}\widetilde{H} \subseteq \widetilde{(F : H)H} \subseteq \widetilde{F} \tag{2.87}$$

and hence that

$$\widetilde{(F : H)} \subseteq (\widetilde{F} : \widetilde{H}), \tag{2.88}$$

which is exactly what was stated at Lemma 2.4.4.

2.5 General case

§1. We shall use the facts proved about GSR till now to deal with the general case of an analytically irreducible ring not necessarily residually rational.

For this we shall need the following simple consequence of Lemma 2.2.2 concerning k subspaces of K.

Lemma 2.5.1. *Let $k \subseteq K$ be an n-dimensional extension of fields and $U, V \subseteq K$ two k-vector subspaces. If $\langle UV \rangle \equiv \mathrm{Span}(UV) \neq K$ then* $\dim_k U + \dim_k V \leq n$.

Proof. Denote the space $\langle UV \rangle$ by W. As $\dim_k W \neq n$, there exists a vector space $T \subset K$ of dimension $n - 1$, such that $W \subseteq T$. By Lemma 2.2.2, $\dim_k(T : V) = n - \dim_k V$. But $U \subseteq T : V$, and hence we obtain that $\dim_k V \leq n - \dim_K V$. ☐

Corollary 2.5.2. *Let $F \subseteq \overline{R}$ be a fractional ideal of R with the property that $F : \overline{R} = F(N)$. Then for every $r \in \mathbb{N}$:*

$$\dim_k(V_F(r)) + \dim_k(V_R(N - r - 1)) \leq n. \tag{2.89}$$

Proof. Clearly, the statement can be reduced to a similar one concerning the associated fractional ideal $\widetilde{F}$ of the GSR $\widetilde{R}$, and this is an easy application of the previous lema. □

Now we are ready to prove the main theorem of this chapter.

Theorem 2.5.3. *Let ω be a fractional ideal of R with $R \subseteq \omega \subseteq \overline{R}$. Then the following conditions are equivalent:*

i) ω is a canonical ideal of R.

ii) $\widetilde{\omega}$ is a canonical ideal of $\widetilde{R}$.

iii) $\forall j \in \mathbb{N}:\ \ \dim_k(V_\omega(j)) + \dim_k(V_R(N-1-j)) = n$.

Proof. The equivalence *iii)* $\Leftrightarrow$ *ii)* was already proved in Corollary 2.2.10. So let us try to prove the implication *ii)* $\Rightarrow$ *i)* and *i)* $\Leftrightarrow$ *ii)*.

ii) $\Leftrightarrow$ *i)*

Of course $\widetilde{\omega}$ is of the form $\sum_{j\in\mathbb{N}} \widetilde{V_\omega(j)} t^j$ where $\widetilde{V_\omega(0)} \supseteq k$ (as $\omega \supseteq R$) and hence $\widetilde{V_\omega(0)} \neq \{0\}$. Since $\widetilde{\omega}$ is a canonical ideal of $\widetilde{R}$, then by Proposition 2.2.9, $\widetilde{V_\omega(N-1)}$ is an $(n-1)$-dimensional k subspace of K and $\widetilde{V_\omega(j)} = K$ for $j \geq N$. It follows that $V_\omega(N-1) \neq K$ and $V_\omega(j) = K$ for $j \geq N$ and hence that there exists $\alpha \in K$ such that $\alpha t^{N-1} \notin \omega$ but $Kt^{N-1}\mathfrak{m} \subseteq \omega$. Thus

$$\omega : \mathfrak{m} \neq \omega. \tag{2.90}$$

In fact ω being a fractional ideal of R, it is a $\mathfrak{m}$-primary ideal of R, and the previous equation is known for these type of ideals.

On the other hand, as ω is a fractional ideal we have also that $\omega = \omega : R \subseteq \omega : \mathfrak{m}$ and thus, using Lemma 2.4.4, we have that

$$\widetilde{\omega} \subseteq \widetilde{\omega : \mathfrak{m}} \subseteq \widetilde{\omega} : \widetilde{\mathfrak{m}}. \tag{2.91}$$

Then, as by assumption $\widetilde{\omega}$ is a canonical ideal of $\widetilde{R}$,

$$1 = \ell_{\widetilde{R}}(\widetilde{\omega} : \widetilde{\mathfrak{m}}/\widetilde{\omega}) = \ell_{\widetilde{R}}(\widetilde{\omega} : \widetilde{\mathfrak{m}}/\widetilde{\omega : \mathfrak{m}}) + \ell_{\widetilde{R}}(\widetilde{\omega : \mathfrak{m}}/\widetilde{\omega}). \tag{2.92}$$

Therefore we have two possibilities:

$$\ell_{\widetilde{R}}(\widetilde{\omega} : \widetilde{\mathfrak{m}}/\widetilde{\omega : \mathfrak{m}}) = 1 \quad \text{and} \quad \ell_{\widetilde{R}}(\widetilde{\omega : \mathfrak{m}}/\widetilde{\omega}) = 0 \tag{2.93}$$

or

$$\ell_{\widetilde{R}}(\widetilde{\omega} : \widetilde{\mathfrak{m}}/\widetilde{\omega : \mathfrak{m}}) = 0 \quad \text{and} \quad \ell_{\widetilde{R}}(\widetilde{\omega : \mathfrak{m}}/\widetilde{\omega}) = 1. \tag{2.94}$$

However, (2.93) is not possible. Indeed, this would imply that $\widetilde{\omega : \mathfrak{m}} = \widetilde{\omega}$, and so that $\dim_k(V_{\omega:\mathfrak{m}}(j)) = \dim_k(V_\omega(j))$ for every j. But as $\omega \subseteq \omega : \mathfrak{m}$, by Corollary 2.4.3 this would further imply that $\omega : \mathfrak{m} = \omega$ in contradiction with (2.90).

This leaves us the possibility of (2.94), implying that $\widetilde{\omega : \mathfrak{m}} = \widetilde{\omega} : \widetilde{\mathfrak{m}}$ and so that $1 = \ell_{\widetilde{R}}(\widetilde{\omega} : \widetilde{\mathfrak{m}}/\widetilde{\omega}) = \ell_{\widetilde{R}}(\widetilde{\omega : \mathfrak{m}}/\widetilde{\omega}) = \ell_R(\omega : \mathfrak{m}/\omega)$ where in the last equality we have used Proposition 2.4.2 (see the remark before Lemma 2.5.1). This shows — using again [HK, Satz 3.3] or Theorem 1.1.21 — affirmation $i)$; that is, that ω is a canonical ideal.

i) ⇒ iii)

If ω is a canonical ideal of R such that $R \subseteq \omega \subseteq \overline{R}$, then we have (see [BF1, Lemma 19 (c)] or Lemma 1.1.26(1)):

$$\ell_R(\overline{R}/R) = \ell_R(R/\mathfrak{f}) + \ell_R(\omega/R), \tag{2.95}$$

where $\mathfrak{f} = R : \overline{R} = R(N)$ is the conductor ideal of $\overline{R}$ in R. By the inclusion $\mathfrak{f} \subseteq R \subseteq \overline{R}$ we have $\ell_R(R/\mathfrak{f}) + \ell_R(\overline{R}/R) = \ell_R(\overline{R}/\mathfrak{f})$. Thus the previous equation may be rewritten as:

$$\ell_R(\omega/R) + 2\ell_R(R/\mathfrak{f}) = \ell_R(\overline{R}/\mathfrak{f}). \tag{2.96}$$

Observe, that if ω is a canonical ideal of the ring R for which $R : \overline{R} = R(N) = t^N\overline{R}$, then also $\omega : \overline{R} = \omega(N) = t^N\overline{R}$. Indeed, $R : \overline{R} = (\omega : \omega) : \overline{R} = \omega : \omega\overline{R}$, and $\omega\overline{R} = \overline{R}$. This fact assures that we can apply Corollary 2.5.2 to ω.

As for the rest, we shall follow the idea of the proof of [CDK, Theorem 3.6]. Let us compute the left-hand side of equation (2.96):

$$\begin{aligned}\ell_R(\omega/R) + 2\ell_R(R/\mathfrak{f}) &= \sum_{i=0}^{N-1}(\dim_k(V_\omega(i)) - \dim_k(V_R(i))) + \\ &\quad + \sum_{i=0}^{N-1}\dim_k(V_R(i)) + \sum_{i=0}^{N-1}\dim_k(V_R(N-i-1)) \\ &= \sum_{i=0}^{N-1}(\dim_k(V_\omega(i)) + \dim_k(V_R(N-i-1))). \end{aligned}\tag{2.97}$$

Corollary 2.5.2 applied to ω, implies that

$$\dim_k V_\omega(i) + \dim_k V_R(N-i-1) \leq n \quad (i = 0, 1, .., N-1). \tag{2.98}$$

Thus, taking in account equation (2.96), we have that

$$\begin{aligned}\ell_R(\overline{R}/\mathfrak{f}) &= \ell_R(\omega/R)+2\ell_R(R/\mathfrak{f}) \\ &= \sum_{i=0}^{N-1}(\dim_k(V_\omega(i))+\dim_k(V_R(N-i-1))) \leq \sum_{i=0}^{N-1} n \\ &= Nn=\ell_R(\overline{R}/\mathfrak{f}),\end{aligned} \tag{2.99}$$

implying that the terms on the two side of the smaller or equal sign (in the second line) are in fact equal. Moreover, by equation (2.98), each of the summand in the above equation (appearing in the first sum of the second line) must take its possible maximum value. In other words,

$$\dim_k(V_\omega(i))+\dim_k(V_R(N-i-1))=n \tag{2.100}$$

for all $i \in \{0,1,..,N-1\}$. □

§2. One may expect to have many interesting properties of R to "survive" the transport to its GSR. In particular, by showing that *i)* is equivalent to *ii)* in the Theorem 2.5.3, we have just obtained that R is Gorenstein if and only if $\widetilde{R}$ is so. In this paragraph we shall see what happens when the ring is almost Gorenstein.

Proposition 2.5.4. *The ring R is almost Gorenstein if and only the associated GSR $\widetilde{R}$ is almost Gorenstein and* $\mathrm{type}(R)=\mathrm{type}(\widetilde{R})$.

Proof. Recall that R almost Gorenstein means that

$$\ell_R(\overline{R}/R)=\ell_R(R/R:\overline{R})+\mathrm{type}(R)-1, \tag{2.101}$$

(see Definition 1.1.25).

As usually let ω be a canonical ideal of R such that $R\subseteq\omega\subseteq\overline{R}$. The definition of almost Gorensteiness is equivalent to:

$$\mathrm{type}(R)=\ell_R(\omega/R)+1, \tag{2.102}$$

see [BF, Definition-Proposition 20] or Proposition 1.1.27. Thus

$$\mathrm{type}(\widetilde{R})=\mathrm{type}(R)=\ell_R(\omega/R)+1=\ell_{\widetilde{R}}(\widetilde{\omega}/\widetilde{R})+1. \tag{2.103}$$

Using Theorem 2.5.3 we have that $\widetilde{\omega}$ is a canonical ideal of $\widetilde{R}$. Then the previous equation is equivalent to the fact that $\widetilde{R}$ is almost Gorenstein. □

As a Kunz ring is an almost Gorenstein ring of type 2 we obtain the next corrolary:

Corollary 2.5.5. *The ring R is Kunz if and only if $\widetilde{R}$ is Kunz.*

§3. We have constructed in Section 2.3 a generalized Apéry basis for a GSR. We shall see in this paragraph that a generalized Apéry basis there exists also for an analytically irreducible ring R which is complete in the $\mathfrak{m}$-adic topology. As ujually k is the residue field of R, K is the residue field of $\overline{R}$ and $n := \dim_k K$.

Since R is complete in the $\mathfrak{m}$-adic topology, we can assume that $\overline{R} = K[[t]]$, the ring of formal power series in one variable. Set m the smallest nonzero element of $v(R)$. Let $x = \alpha t^m$+terms of higher degrees $\in R$ an element such that $v(x) = m$, where $\alpha \in K$. Denote W the DVR included in R which has its maximal ideal generated by x, in fact

$$W = k[[\alpha t^m + \text{terms of higher degrees}]]. \tag{2.104}$$

We know (see Section 1.2) that R is a free W-module of rank equal to the multiplicity of the ring $e(R)$.

Recall that we can associate to the ring R a GSR $\widetilde{R}$. In the last paragraph of Section 2.4 we showed how we can give $\widetilde{R}$ using the function Φ defined in that paragraph. Using again the function Φ we have that

$$\widetilde{W} = \mathrm{Span}_k(\Phi(W)) = k[[\alpha t^m]], \tag{2.105}$$

and it is the DVR included in $\widetilde{R}$, $\widetilde{R}$ being a free $\widetilde{W}$-module of rank equal to the multiplicity of $\widetilde{R}$, $e(\widetilde{R})$.

Note that if $\tilde{r} \in \widetilde{R}$ then $\Phi^{-1}(\tilde{r}) = \{r \in R | \ \ \Phi(r) = \tilde{r}\}$ is a subset of R which can have more than one element.

We want to show that if $\{\widetilde{y^i_j} | \quad 0 \leq i \leq m-1, \quad 0 \leq j \leq n-1\}$ is a generalized Apéry basis of $\widetilde{R}$ (as a free $\widetilde{W}$-module) then taking some representants in $\Phi^{-1}(\widetilde{y^i_j})$, these form a basis of R (as a free W-module). It would imply that $e(R) = e(\widetilde{R}) = mn$. This fact is known, see [ZS, Corollary 1 to Theorem 24].

Let us now give an example to ilustrate these facts.

Example 2.5.6. Let R be the ring

$$R := \mathbb{R}[[it^3 + t^4, t^5, it^{10} + t^{11}]]. \tag{2.106}$$

Then the associated GSR of R is

$$\widetilde{R} = \mathbb{R}[[it^3, t^5, it^{10}, it^{17}]], \tag{2.107}$$

see Example 2.4.1.

An Apéry basis of $\widetilde{R}$ over $\widetilde{W} = k[[it^3]]$ is: $\{0, t^{15}, t^{10}, it^{10}, t^5, it^{17}\}$. An Apéry basis for R is $\{0, t^{15}, t^{10}, it^{10} + t^{11}, t^5, f\}$, where f is an element of R of value 17 for which $\Phi(f) = it^{17}$.

Proposition 2.5.7. *Let R be an analytically irreducible non residually rational ring. If $\{\widetilde{y_j^i}|\ 0 \leq i \leq m-1,\ 0 \leq j \leq n-1\}$ is a generalized Apéry basis of the associated GSR $\widetilde{R}$ then fixing for every i, j, one element in $\Phi^{-1}(\widetilde{y_j^i})$, denoted by y_j^i, then $\{y_j^i|\ 0 \leq i \leq m-1,\ 0 \leq j \leq n-1\}$ is a basis of R over the DVR W.*

This basis is called *generalized Apéry basis* of R.

2.6 The type sequence

§1. We have already seen in Section 1.4 that for an analytically irreducible ring which is also residually rational one can define the *type sequence* of the ring. In this section we shall show that, with some care, this can be defined also for rings not necessarily residually rational. We keep the notation of the previous sections of this Chapter.

For our ring R consider the value semigroup

$$v(R) = \{s_0 = 0, s_1, \ldots, s_{r-1}, s_r = c, \rightarrow\}, \tag{2.108}$$

which does not give enough information about the ring. We defined in Section 2.4 another invariant of the ring, namely its *conductor* N, the element of $v(R)$ such that the ideal conductor of R is $R : \overline{R} = t^N\overline{R}$. Note that $N \geq c$, thus we can set $N = s_{r+l} = s_r + l = c + l$ for some $l \in \mathbb{N}$.

Consider the ideals of R:

$$\mathfrak{a}_i = \{x \in R|\ v(x) \geq s_i\},\ i \in \{0, \ldots, r+l\}. \tag{2.109}$$

It is evident that $\mathfrak{a}_0 = R$, $\mathfrak{a}_1 = \mathfrak{m}$, $\mathfrak{a}_{r+l} = R : \overline{R}$.

Consider for every $i \in \{0, \ldots, r+l\}$ the fractional ideal of R

$$\mathfrak{a}_i^{-1} := R : \mathfrak{a}_i. \tag{2.110}$$

Then we have;

$$\mathfrak{a}_{r+m} \subset \cdots \subset \mathfrak{a}_0 = R \subseteq \mathfrak{a}_1^{-1} \cdots \subseteq \mathfrak{a}_{r+l}^{-1}. \tag{2.111}$$

In fact also $\mathfrak{a}_i^{-1} \subsetneqq \mathfrak{a}_{i+1}^{-1}$, for every $i \in \{0, \ldots, r+l-1\}$. This we shall see in the next proposition.

Proposition 2.6.1. *With the above notations we have that:*

1. $\mathfrak{a}_{r+l}^{-1} = \overline{R}$;

2. *For every* $i \in \{0, \dots, r+l\}$ $\mathfrak{a}_i$ *is a divisorial ideal in the sense that* $R : (R : \mathfrak{a}_i) = \mathfrak{a}_i$*;*

3. $\ell_R(\mathfrak{a}_i^{-1}/\mathfrak{a}_{i-1}^{-1}) \geq 1$ *for every* $i \in \{1, \dots, r+l\}$*.*

Proof. 1. $\mathfrak{a}_{r+l} = t^n\overline{R}$. Then

$$\begin{aligned} \mathfrak{a}_{r+l}^{-1} &= R : t^N\overline{R} = t^{-N}(R : \overline{R}) \\ &= t^{-N}t^N\overline{R} = \overline{R} \end{aligned} \tag{2.112}$$

2. As $\overline{R} = R : \mathfrak{a}_{r+l}^{-1}$ then $\overline{R}$ is divisorial as fractional ideal of R (because every fractional ideal which can be written as $R : I$ for some other fractional ideal I of R is divisorail). Thus we have $t^h\overline{R}$ is divisorial for every $h \in \mathbb{N}$. We know that the intersection of fractional divisorial ideals is again a fractional divisorial ideal. Evidently, we can write

$$\mathfrak{a}_i = R \cap t^{s_i}\overline{R}. \tag{2.113}$$

Thus $\mathfrak{a}_i$ is divisorial.

3. From the fact that $\mathfrak{a}_i$, for every i, is divisorial we have that:

$$R : \mathfrak{a}_{i-1} \subsetneqq R : \mathfrak{a}_i, \tag{2.114}$$

because, if $R : \mathfrak{a}_{i-1} = R : \mathfrak{a}_i$ then $\mathfrak{a}_{i-1} = R : (R : \mathfrak{a}_{i-1}) = R : (R : \mathfrak{a}_i) = \mathfrak{a}_i$ which is impossible. And this also shows that $\ell_R(\mathfrak{a}_i^{-1}/\mathfrak{a}_{i-1}^{-1}) \geq 1$ □

Definition 2.6.2. *Set*

$$t_i(R) := \ell_R(\mathfrak{a}_i^{-1}/\mathfrak{a}_{i-1}^{-1}), \text{ for every } i \in \{1, 2, \dots, r+l\}. \tag{2.115}$$

We call the sequence of numbers $(t_1, t_2, \dots, t_{r+l})$ *the* **type sequence** *of* R*, we denote it by* $t.s.(R)$*.*

As in the case of R residually rational we have that $t_1(R) = \ell_R(\mathfrak{m}^{-1}/R) =:$ type(R). Note that the k-vector space $\mathfrak{a}_{i-1}/\mathfrak{a}_i$ was already considered in Section 2.4, with the previous notation this vector space is $V_R(s_{i-1})$. It is evident that $V_R(s_{i-1}) \neq 0$, denote $\dim_k V_R(s_{i-1}) := n_{i-1} > 0$. We shall see in the next proposition that there exists an upper bound for $t_i(R)$. The proof uses the same argument as that one used by Matsuoka in [Mat].

Proposition 2.6.3. *With the above notations*

$$1 \leq t_i(R) \leq \text{type}(R)\, n_{i-1}, \text{ for every } i \in \{1, \dots, r+l\}. \tag{2.116}$$

Proof. Fix an $i \in \{1, \ldots, r+l\}$. We have the short exact sequence of R-modules:

$$0 \to \mathfrak{a}_{i-1}/\mathfrak{a}_i \to R/\mathfrak{a}_i \to R/\mathfrak{a}_{i-1} \to 0. \tag{2.117}$$

This sequence gives rice to the long exact sequence:

$$\begin{aligned} \cdots \to \mathrm{Hom}_R(k^{n_{i-1}}, R) \to \mathrm{Ext}^1_R(R/\mathfrak{a}_{i-1}, R) \to \\ \mathrm{Ext}^1_R(R/\mathfrak{a}_i, R) \to \mathrm{Ext}^1_R(k^{n_{i-1}}, R) \to \ldots. \end{aligned} \tag{2.118}$$

It is evident that $\mathrm{Hom}_R(R/\mathfrak{a}_j, R) = 0$ for every j. Using Rees Theorem (see [R]) we have that for a nonzero divisor $a \in R$ and for every $j \in \{1, \ldots, r+l\}$:

$$\mathrm{Ext}^1_R(R/\mathfrak{a}_j, R) \simeq \mathrm{Hom}_R(R/\mathfrak{a}_j, R/aR) \simeq (aR : \mathfrak{a}_j)/aR. \tag{2.119}$$

And it is evident that

$$(aR : \mathfrak{a}_j)/aR \simeq a\mathfrak{a}_j^{-1}/aR \simeq a_j^{-1}/R. \tag{2.120}$$

It is clear that

$$\mathrm{Hom}_R(\oplus_{m=1}^{n_{i-1}} k, R) \simeq \oplus_{m=1}^{n_{i-1}} \mathrm{Hom}_R(k, R) = 0, \tag{2.121}$$

and also that

$$\mathrm{Ext}^1_R(\oplus_{m=1}^{n_{i-1}} k, R) \simeq \oplus_{m=1}^{n_{i-1}} \mathrm{Ext}^1_R(k, R) \simeq \oplus_{m=1}^{n_{i-1}} \mathfrak{m}^{-1}/R. \tag{2.122}$$

Thus the long exact sequence from equation (2.118) becomes:

$$0 \to \mathfrak{a}_{i-1}^{-1}/R \to \mathfrak{a}_i^{-1}/R \to \oplus_{m=1}^{n_{i-1}} \mathfrak{m}^{-1}/R \to \ldots, \tag{2.123}$$

and $\mathfrak{a}_i^{-1}/\mathfrak{a}_{i-1}^{-1}$ is a submodule of $\oplus_{m=1}^{n_{i-1}} \mathfrak{m}^{-1}/R$. Then

$$t_i(R) := \ell_R(\mathfrak{a}_i^{-1}/\mathfrak{a}_{i-1}^{-1}) \leq \ell_R(\oplus_{m=1}^{n_{i-1}} \mathfrak{m}^{-1}/R) = \sum_{m=1}^{n_{i-1}} \mathrm{type}(R) = \mathrm{type}(R)\ \ n_{i-1}. \tag{2.124}$$

□

Chapter 3

On the Hilbert function of a semigroup ring

3.1 The Hilbert functions

We shall briefly present the theory of Hilbert Functions and Hilbert Polynomials for general Noetherian graded rings, and only later we shall see how we can define a Hilbert Function for a one-dimenional CM ring. Every monography on commutative algebra (and not only) has a chapter dedicated to graded rings and Hilbert Function. The Hilbert function is important in the dimension theory of local (semilocal) rings. One of the possible way to define the dimension is using a particular graded ring associated to the ring and its Hilbert Function.

Let R be a Noetherian graded ring,

$$R = \bigoplus_{n \geq 0} R_n. \tag{3.1}$$

Then R_0 is Noetherian and R is finitely generated as an R_0-algebra. So we can set:

$$R = R_0[x_1, \dots x_s], \tag{3.2}$$

with x_i homogeneous of degree d_i. Moreover, assume that R_0 is an Artinian ring.

Let M be a finitely generated graded R-module,

$$M = \bigoplus_{n \geq 0} M_n. \tag{3.3}$$

One can easily show that M_n is a finitely generated R_0-module. From the fact that R_0 is an Artinian ring we have that $\ell_{R_0}(M_n) < \infty$. The **Hilbert**

function of M is defined by:

$$H(M, n) = \ell_{R_0}(M_n). \tag{3.4}$$

Define the **Hilbert series** of M to be the formal power series

$$P(M, t) = \sum_{n=0}^{\infty} \ell_{R_0}(M_n) t^n \in \mathbb{Z}[[t]]. \tag{3.5}$$

Theorem 3.1.1 (Hilbert, Serre). *$P(M, t)$ is a rational function of t of the form*

$$P(M, t) = \frac{f(t)}{\prod_{i=1}^{s}(1 - t^{d_i})}, \tag{3.6}$$

where $f(t)$ is a polynomial of $\mathbb{Z}[t]$.

We shall denote by $d(M)$ the order of the pole of $P(M, t)$ at $t = 1$. Especially simple is the case $d_1 = \cdots = d_s = 1$.

Corollary 3.1.2. *Id $d_i = 1$ for every $1 \leq i \leq s$, then for all sufficiently large n, $H(M, n) = \ell_{R_0}(M_n)$ is a polynomial in n with rational coefficients of degree $d - 1$, where $d = d(M)$.*

The polynomial appearing in 3.1.2 is called the **Hilbert polynomial** of the graded R-module M.

Let now R be a local Noetherian ring with $\mathfrak{m}$ its (unique) maximal ideal and I an $\mathfrak{m}$-primary ideal of R (equivalently I contains a power of $\mathfrak{m}$). We can consider the graded ring:

$$gr_I(R) = \bigoplus_{n \geq 0} I^n / I^{n+1}. \tag{3.7}$$

An important role in the study of the multiplicity of the ring R and not only for this is the previous graded ring for $I = \mathfrak{m}$, namely

$$\mathrm{gr}_{\mathfrak{m}}(R) = \bigoplus_{n \geq 0} \mathfrak{m}^n / \mathfrak{m}^{n+1}. \tag{3.8}$$

Set as usually $k = R/\mathfrak{m}$, the residue field of R. If $\mathfrak{m}$ is generated by r elements then

$$\mathrm{gr}_{\mathfrak{m}}(R) = k[X_1, \dots X_r]/J, \tag{3.9}$$

where J is a homogeneous ideal and $k[X_1, \dots X_r]$ is the polynomial ring in r indeterminates. Note that we can apply the Hilbert-Serre Theorem to this graded ring, because $R/\mathfrak{m}$ is a field. Then

$$H(\mathrm{gr}_{\mathfrak{m}}(R), n) = \ell_{R/\mathfrak{m}}(\mathfrak{m}^n / \mathfrak{m}^{n+1}) \leq \infty. \tag{3.10}$$

In fact using Nakayama‘s Lemma

$$H(\mathrm{gr}_{\mathfrak{m}}(R), n) = \mu(\mathfrak{m}^n), \tag{3.11}$$

where we denote by $\mu(I)$ the minimal number of generators of an ideal I of R. $H(\mathrm{gr}_{\mathfrak{m}}(R), n)$ is a polynomial for large enough n. We obtain that

$$\ell_R(R/\mathfrak{m}^n) = \sum_{j=0}^{n-1} \ell_R(\mathfrak{m}^n/\mathfrak{m}^{n+1}) \leq \infty \tag{3.12}$$

Moreover it is a polynomial in n of degree equal to $\dim(R)$ (the Krull dimension of R). The coefficient of the leading term of this polynomial is called the **multiplicity** of R, denoted by $e(R)$.

A lot of interesting problem appears in the study of Hilbert Function of $\mathrm{gr}_{\mathfrak{m}}(R)$. Sally in [Sa] put some questions:
1. "When is $H(\mathrm{gr}_{\mathfrak{m}}(R), n)$ a non decreasing function?"
2. "When does $H(\mathrm{gr}_{\mathfrak{m}}(R), n)$ become a polynomial?"
A connected problem with the first question is
3. "Under what necessary and sufficient conditions $\mathrm{gr}_{\mathfrak{m}}(R)$ is a CM graded algebra?"
Here we shall investigate the first problem in the case of the ring R being one-dimensional.

Assume that $\dim(R) = 1$ and also that $\mathfrak{m}$ contains a nonzero divisor, which is equivalent with R being CM. These rings were studied in many articles at the middle of the last century by Northcott, Kirby and later by Matlis. Using the general theory, we know that for all large value of n, $\ell_R(R/\mathfrak{m}^n)$ is a polynomial in n of degree 1 called the *Hilbert polynomial* of R (see [M1]). Thus

$$H_R(n) = \ell_R(R/\mathfrak{m}^n) = en - \rho \tag{3.13}$$

for large n. The pozitive integer e is called the *multiplicity* of R and ρ was called by Northcott the *reduction number* of R (see [N3], [N4]). Denote the Hilbert function of $\mathrm{gr}_{\mathfrak{m}}(R)$, in this case, by $H_R^0(n)$ and we shall call it shortly the *Hilbert function* of R. Thus

$$H_R^0(n) = \ell_R(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \mu(\mathfrak{m}^n). \tag{3.14}$$

Recall that the embedding dimension of a local ring is the minimal number of generators of the maximal ideal $\mathfrak{m}$, $\mu(\mathfrak{m})$ which is equal to $\dim_k(\mathfrak{m}/\mathfrak{m}^2)$. Sally in [Sa] stated the next conjecture about the growth of the Hilbert function of R:

Conjecture. If R is a one dimensional CM ring with small enough (say at most three?) embedding dimension, then

$$H_R^0(n) = \ell_R(\mathfrak{m}^n/\mathfrak{m}^{n+1}) \tag{3.15}$$

is non-decreasing.

Matlis in [M1] proved that for embedding dimension 2, H_R^0 is not decreasing.

Theorem 3.1.3 (Matlis). *Let R be a one-dimensional CM local ring. assume that the maximal ideal $\mathfrak{m}$ is generated by two eleements. Then*

$$\ell_R(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \begin{cases} n+1 & \text{if } n \le e-1 \\ e & \text{if } n \ge e-1. \end{cases}$$

Two years later than the article of Matlis in 1975 a first example of a ring R with decreasing Hilbert function was given by Herzog and Waldi ([HW]). In that example R was a semigroup ring with embedding dimension 10:

$$R = k[[t^{30}, t^{35}, t^{42}, t^{47}, t^{148}, t^{153}, t^{157}, t^{169}, t^{181}, t^{193}]], \tag{3.16}$$

for which $H_R^0(1) = 10$ and $H_R^0(2) = 9$. Orecchia proved that for all $b \ge 5$ there exists a reduced one-dimensional local ring of emebedding dimension b with decreasing Hilbert function, see [Or]. Then, only the cases of embedding dimension 3 and 4 remained open till the beginning of 90's when Elias ([E2]) solved the case of embedding dimension 3 showing that the Sally's conjecture is true assuming also that the one-dimensional CM ring is equicharacteristic. The case of embedding dimension 4 remains open.

3.2 Semigroup rings generated by 3 elements

§1. Consider the semigroup ring

$$k[[S]] = k + kt^{s_1} + kt^{s_2} + \cdots + t^{s_n}k[[t]] \subseteq k[[t]], \tag{3.17}$$

where

$$S = \{s_0 = 0, s_1, s_2, \ldots, s_n \rightarrow\} \subset \mathbb{N} \tag{3.18}$$

is a numerical semigroup with the conductor $c = s_n$. The semigroup ring $k[[S]]$ is an analytically irreducible and residually rational ring. We would like to investigate its Hilbert function

$$H^0_{k[[S]]}(n) = \ell_R(\mathfrak{m}^n/\mathfrak{m}^{n+1}) = \mu(\mathfrak{m}^n). \tag{3.19}$$

It is evident that there exist $g_0 < g_1 < \dots g_{r-1}$ elements of S such that $\mathfrak{m}$ is generated as a ideal of R by $\{t^{g_0}, t^{g_1}, \dots t^{g_{r-1}}\}$. In fact the semigroup is generated by $\{g_0, g_1, \dots, g_{r-1}\}$. To study the Hilbert function of a ring is exactly to see the number of generators of the powers of the maximal ideal of the ring. Thus we can reduce the problem of investigating the Hilbert function of the semigroup ring $k[[S]]$ to the study of the associated semigroup S. We shall treat the case $r = 3$, giving for this case a simple proof of the fact that the Hilbert function is not decreasing.

§2. Let now $S \subseteq \mathbb{N}$ be a numerical semigroup. As in Section 1.3, we shall set

$$M := S \setminus \{0\}, \tag{3.20}$$

for the maximal ideal of S, and

$$e := \min(M) \tag{3.21}$$

the smallest nonzero element of S. We have the decreasing chain of ideals of S:

$$S \supset M =: M^{(1)} \supset M^{(2)} \supset \cdots \supset M^{(k)} \supset \dots, \tag{3.22}$$

where $M^{(k)}$ is defined by the recursive formula

$$M^{(1)} := M, \quad M^{(n+1)} := M^{(n)} + M \ \ (n = 1, 2, ..). \tag{3.23}$$

To put it in another way, $M^{(k)}$ is the set of elements in S that can be written as a sum of k nonzero elements of S. A more or less trivial, but important observation is the following.

Lemma 3.2.1. *S, as a semigroup, has a unique minimal set of generators; namely the set*

$$M^{(1)} \setminus M^{(2)}. \tag{3.24}$$

Moreover, this set contains e, and it is finite; in fact

$$|M^{(1)} \setminus M^{(2)}| \leq e. \tag{3.25}$$

We say that an ideal N of a numerical semigroup S is generated (over S) by the set $H \subseteq N$, if $N = H + S$. Another easy observation, similar to the previous one, but regarding $M^{(k)}$, is the following one.

Lemma 3.2.2. *There exists a unique minimal set of generators of $M^{(k)}$ over S; namely the set*

$$M^{(k)} \setminus M^{(k+1)}. \tag{3.26}$$

Moreover, this set is finite; in fact

$$|M^{(k)} \setminus M^{(k+1)}| \leq e. \tag{3.27}$$

Definition 3.2.3. *Let us define the function*

$$\phi : S \to \mathbb{N} \tag{3.28}$$

by the formula

$$\forall\ \ s \in S, \ \ \phi(s) = \min\{k \in \mathbb{N} |\ \ x \notin M^{(k+1)}\}. \tag{3.29}$$

Note the following simple facts about the function ϕ:

1. ϕ is well defined, because $\cap_{k\in\mathbb{N}} M^{(k)} = \emptyset$.
2. $\phi(s) = k \Leftrightarrow s \in M^{(k)} \setminus M^{(k+1)}$.
3. For an $s \in S$, $s \neq 0$, $\phi(s)$ is the maximum number n such that s is a sum of n nonzero elements of S.
4. $\phi(s + u) \geq \phi(s) + \phi(u)$.

Some further properties of the function ϕ is collected into the next statement.

Lemma 3.2.4. *Let $s \in S$, $n := \phi(s)$ and suppose that $s = s_1 + \dots s_n$. Then*

1. *Each element appearing in the decomposition of s belongs to the set of minimal generators: $s_j \in M^{(1)} \setminus M^{(2)}$ $(j \in \{1, \dots, n\})$.*
2. *$s \leq \phi(s) \max(M^{(1)} \setminus M^{(2)})$.*

Proof. 1. By Lemma 3.2.1, if $s_j \notin M^{(1)} \setminus M^{(2)}$ then we can write s_j as a sum of (at least two, but possibly more) elements from $M^{(1)} \setminus M^{(2)}$. In turn, it would imply that also s could be expanded and written as a sum of more then $n = \phi(s)$ nonzero elements, which is in contradiction with the definition of $\phi(s)$.

2. By the previous point, each element appearing in the decomposition $s = s_1 + \dots s_n$, belongs to $M^{(1)} \setminus M^{(2)}$. Thus

$$s \leq n \max\{s_j : j = 1, \dots, n\} \leq n \max(M^{(1)} \setminus M^{(2)}). \tag{3.30}$$

□

From now on we shall assume that S is generated by 3 elements. Thus we may write that

$$M^{(1)} \setminus M^{(2)} = \{e, g_2, g_3\} \tag{3.31}$$

where the indexing is such that

$$e < g_2 < g_3. \tag{3.32}$$

We would like to see that the minimal number of generators of $M^{(k+1)}$ is bigger or equal to the minimal number of generators of $M^{(k)}$. If $e+g$ is a generator of $M^{(k+1)}$ for every g generator of $M^{(k)}$ the problem is solved. But how we can see from the next example this does not happen always.

Example 3.2.5. Let $S = \langle 6, 7, 15 \rangle$. In this case $e = 6$, $g_2 = 7$, $g_3 = 15$. A minimal set of generators of $M^{(2)} = M + M$ is: $\{12 = 6+6, 13 = 6+7, 14 = 7+7, 22 = 15+7\}$. Note that $21 = 6 + 15$ is not in this set because $21 = 7 + 7 + 7 \in M^{(3)}$.

Thus the natural way to continue is to see what happens when an element of the form $e + g$ with g generator of $M^{(k)}$ is not a generator of $M^{(k+1)}$. The answer is contained in the next proposition.

Proposition 3.2.6. *Let $k \in \mathbb{N}$, $s \in M^{(k)} \setminus M^{(k+1)}$, and assume that $e + s \notin M^{(k+1)} \setminus M^{(k+2)}$, i.e. that $\phi(e+s) > k+1$. Then there exist a unique pair $n_s, m_s \in \mathbb{N}$ such that*

$$e + s = n_s g_2 + m_s g_3, \quad \text{and} \quad n_s + m_s = \phi(e+s). \tag{3.33}$$

Moreover, if a, $b \in \mathbb{N}$, $a \leq n_s$, $b \leq m_s$, then

$$\phi(a g_2 + b g_3) = a + b. \tag{3.34}$$

Proof. By what was so far explained, we know that we can write $e + s$ as a sum $\phi(e+s)$ elements (with repetitions); that is, there exist three coefficients $r_s, n_s, m_s \in \mathbb{N}$ such that

$$e + s = r_s e + n_s g_2 + m_s g_3, \quad \text{and} \quad r_s + n_s + m_s = \phi(e+s). \tag{3.35}$$

At this point there could be more than one way of writting s in the above way. However, we shall show, that in such a decomposition e cannot appear. Indeed, assume that this happens; i.e. that in the above decomposition we have $r_s > 0$. Then $(r_s - 1) \geq 0$ and so from

$$s = (r_s - 1)e + n_s g_2 + m_s g_3 \tag{3.36}$$

it would follow that

$$\phi(s) \geq (r_s - 1) + n_s + m_s = \phi(e+s) - 1 > k \tag{3.37}$$

and so that $\phi(s) > k$, in the contradiction with the condition of the proposition. So in fact $r_s = 0$, and $s = n_s g_2 + m_s g_3$, $n_s + m_s = \phi(e) = k$. As for the unicity, assume that $\tilde{n}_s, \tilde{m_s} \in \mathbb{N}$, $n_s + m_s = k$ and $s = n_s g_2 + m_s g_3$. Then $\tilde{n}_s - n_s = m_s - \tilde{m_s}$ and

$$0 = s - s = (n_s g_2 + m_s g_3) - (\tilde{n}_s g_2 + \tilde{m_s} g_3) = (m_s - \tilde{m_s})(g_3 - g_2) \quad (3.38)$$

and hence $m_s - \tilde{m_s} = 0$; that is, $\tilde{m_s} = m_s$ and $\tilde{n}_s = n_s$.

As for the second part of the proposition, consider a subsum of the sum $n_s g_2 + m_s g_3$, namely $ag_2 + bg_3$, with $a \leq n_s$ and $b \leq m_s$. We have to prove that this is the maximal way in which we can write $u := ag_2 + bg_3$. If we can write u as a sum of more elements, then we can do the same with $n_s g_2 + m_s g_3$, and this is impossible. □

From Proposition 3.2.6 since $e + s \leq e + kg_3$ we have that

$$m_s < k + 1. \quad (3.39)$$

As $\phi(e + s) = n_s + m_s > k + 1$,

$$n_s > k + 1 - m_s. \quad (3.40)$$

We can define

$$q(s) := ((k + 1) - m_s)g_2 + m_s g_3. \quad (3.41)$$

Evidently $q(s) \in S$, and by Proposition 3.2.6, $\phi(q(s)) = k + 1$, so $q(s) \in M^{(k+1)} \setminus M^{(k+2)}$.

The aim is to find another element in a minimal set of generators of $M^{(k+1)}$ for each $u = e + s \notin M^{(k+1)} \setminus M^{(k+2)}$, where $s \in M^{(k)} \setminus M^{(k+1)}$, element which will be different from the others generators from the minimal set. We shall prove in the next theorem that the element which we look for is $q(s)$ defined before.

Proposition 3.2.7. *Let s, $u \in M^{(k)} \setminus M^{(k+1)}$ and assume that $e + s \notin M^{(k+1)} \setminus M^{(k+2)}$ while $e + u \in M^{(k+1)} \setminus M^{(k+2)}$. Then*

$$q(s) \neq e + u. \quad (3.42)$$

Proof. Assume that $q(s) = e + u$. By definition of $q(s)$

$$e + s = q(s) + (n_s - (k + 1) + m_s)g_2, \quad (3.43)$$

and

$$n_s - (k + 1) + m_s > 0. \quad (3.44)$$

Then

$$e + s = e + u + (n_s - (k + 1) + m_s)g_2 \Leftrightarrow s = u + (n_s - (k + 1) + m_s)g_2. \quad (3.45)$$

This means that

$$\phi(s) \geq \phi(u) + (n_s - (k+1) + m_s) > k, \tag{3.46}$$

and this is a contradiction. □

Proposition 3.2.8. *Let s, $u \in M^{(k)} \setminus M^{(k+1)}$ and assume that $e+s$, $e+u \notin M^{(k+1)} \setminus M^{(k+2)}$. Then*

$$q(s) = q(u) \Leftrightarrow s = u. \tag{3.47}$$

Proof. From the definition of $q(s)$:

$$q(s) = q(u) \Leftrightarrow ((k+1)-m_s)g_2+m_s g_3 = ((k+1)-m_u)g_2+m_u g_3 \Leftrightarrow m_s = m_u. \tag{3.48}$$

Assume that $n_s \neq n_u$, consider $n_s \geq n_u$. We know that

$$q(s) = q(u) = e + u - (n_u - (k+1) + m_u)g_2 \tag{3.49}$$

Then

$$\begin{aligned} e+s &= q(s) + (n_s - (k+1) + m_s)g_2 = \\ &= e + u - (n_u - (k+1) + m_s)g_2 + (n_s - (k+1) + m_s)g_2 = \\ &= e + u + (n_s - n_u)g_2 \end{aligned} \tag{3.50}$$

And this is equivalent to:

$$s = u + (n_s - n_u)g_2, \tag{3.51}$$

with $n_s - n_u > 0$. Therefore

$$\phi(s) \geq \phi(u) + (n_s - n_u) > k, \tag{3.52}$$

which is a contradiction with the fact that $s \in M^{(k)} \setminus M^{(k+1)}$. We obtain that $n_s = n_u$, this togheter with $m_s = m_u$ means that $e + s = e + u$, then $s = u$.
The viceversa is evident. □

Thus we can conclude:

Corollary 3.2.9. *The function*

$$\psi : M^{(k)} \setminus M^{(k+1)} \to M^{(k+1)} \setminus M^{(k+2)},$$

defined by

$$\psi(s) = \begin{cases} e+s & \text{if } e+s \in M^{(k+1)} \setminus M^{(k+2)} \\ q(s) & \text{otherwise} \end{cases}$$

is an injection.

Therefore we obtain that that

$$|M^{(k)} \setminus M^{(k+1)}| \leq |M^{(k+1)} \setminus M^{(k+2)}|. \tag{3.53}$$

This in terms of the semigroup ring means that

$$\mu(\mathfrak{m}^k) \leq \mu(\mathfrak{m}^{k+1}), \tag{3.54}$$

i.e. the Hilbert function $H^0_{k[[S]]}$ is not decreasing.

Bibliography

[An] G. Angermüler: Die Wertehalbgruppe einer ebenen irreduziblen algebroiden Kurve. *Math. Z.* **153** (1977), 267-282.

[A] R. Apèry: Sur les branches superlinéaires des courbes algébriques. *C. R. Acad. Sci. Paris* **222** (1946), 1198-2000.

[AuB] A.Auslander D.Buchsbaum: *Groups, Rings, Modules.* Harper and Row Publisher, 1974.

[BDF] V.Barucci, M. D'Anna, R. Fröberg: On plane algebroid curves. *Lectures Notes in Pure and Applied Math. Deker, New-York* **231** 2002, 37-50.

[BDoFo] V. Barucci, D.E. Dobbs, M. Fontana: *Maximality properties in numerical semigroups and applications to one-dimensional analytically irreducible local domains.* Mem. Amer. Math. Soc. **125** (1997).

[BF] V.Barucci and Fröberg: Maximality Properties for One-Dimensional Analytically Irreducible Local Gorenstein and Kunz Rings. *Math Scand.* **81** (1997), 149-160.

[BF1] V. Barucci and Ralf Fröberg: One-Dimensional Almost Gorestein Rings. *Journal of Algebra* **188** (1997), 418-442.

[BF2] V. Barucci and Ralf Fröberg: Associated graded rings of one-dimensional analytically ireducible rings. *Journal of Algebra* **304** (2006), 349-358.

[BHLP] V.Barucci, E.Houston, T.G.Lucas and I.Papick: m-Canonical Ideals in Integral Domains II. "Ideal Theoretic Methods in Commutative Algebra" (Columbia, MO, 1999), 9-108, Lecture Notes in Pure and Appl. Math., 220 Dekker, New-York, 2001.

[BH] W. Bruns, J. Herzog: *Cohen-Macaulay Rings. Cambridge University Press, 1993.*

[C] I.S. Cohen: On the structure and ideal theory of complete local rings. Trans. Amer. Math. Soc. **59** *(1946), 54-106.*

[CDK] A.Campillo, F.Delgado, K.Kiyek: Gorenstein Property and Symmetry for One-Dimensional Local Cohen-Macaulay Rings. Manuscripta Math. **83** *(1994), 405-423.*

[D'Anna1] M. D'Anna: Canonical module and one-dimensional analytically irreducible Arf domains. "Commutative ring theory" Fès, 1995, Lecture Notes in Pure and Appl. Math. **185**, *Dekker, New-York, 1997, 215-225.*

[D'Anna2] M. D'Anna: Modulo canonico di anelli ridotti di dimensione uno e semigruppi loro associati. t-successioni, tesi di dottorato. Centro Stampa del Dipartimento di Matematica dell'Università di Roma "La Sapienza", 1997.

[D'Anna3] M. D'Anna: Type sequences of numerical semigroups. Semigroup Forum **56** *(1998) no. 1, 1-31.*

[E1] J. Elias: *Characterization of the Hilbert-Samuel polynomials of curve singularities. CompositioMath.* **74** *(1990), 135-155.*

[E2] J. Elias: *The Conjecture of Sally on the Hilbert function for curve singularities. Journal of Algebra* **160** *(1993), 42-49.*

[E3] J. Elias: *On the deep structure of the blowing-up of curve singularities. Math. Proc. Camb. Phil. Soc.* **131** *(2001), 227-240.*

[FGH] R. Fröberg, C. Gottlieb, R. Häggkvist: *On numerical semigroups. Semigroup Forum* **35** *(1987) no. 1 63-83.*

[G] R.W. Gilmer: *Commutative Semigroup Rings. Chicago University Press, 1984.*

[HK] J.Herzog, E.Kunz: *Der kanonische Modul eines Cohen-Macaulay Rings. Lecture Notes in Math. 238, Springer-Verlag 1971.*

[HW] J.Herzog, R.Waldi: *A note on the Hilbert function of a one-dimensional Cohen-Macaulay ring. Manuscripta Math.* **16** *(1975), 251-260.*

[Jac] N.Jacobson: *Basic Algebra II, New-York: Freeman & Co.,1989*

[J] J. Jäger: *Längenberechnung und kanonische Ideale in eindimensionalen Ringen. Arch. Math.* **29** *(1977).*

[Ka] D. Katz: *On the number of minimal prime ideals in the completion of a local domain. Rocky Montain J. Math.* **16***, no. 3, (1986), 575-578.*

[K] E. Kunz: *The value semigroup of a one dimensional Gorestein ring. Proc. Amer.Math. Soc.* **25** *(1970), 748-751.*

[L] J. Lipman: *Stable ideals and Arf rings. Amer. J. Math.* **93** *(1971), 649-785.*

[M] E. Matlis: *One Dimemsional Local Cohen-Macaulay Rings, Lecture Notes in Mathematics, Vol. 327, Springer-Verlag, 1973.*

[M1] E. Matlis: *The multiplicity and reduction number of a one-dimensional local ring, Proc. of London Math. Soc.* **26** *(3), (1973), 273-288.*

[Ma] H. Matsumura: *Commutative Ring Theory, translated by M.Reid, Cambridge, C.U.P., 1986.*

[Mat] T. Matsuoka, *On the degree of singularity of one-dimensional analytically irreducible Noetherian local rings, J. Math. Kyoto Univ. (1971),485-494.*

[N1] D.G. Northcott: *On the Notion of a First Neighbourhood Ring. Proc. Cambridge Philos. Soc.* **53** *(1957), 43-56.*

[N2] D.G. Northcott: *The Theory of One-Dimensional Local Rings. Proc. London Math. Soc.* **8** *(1958) 388-415.*

[N3] D.G. Northcott: *The reduction number of one dimensional local ring. Mathematika* **6** *(1959), 87-90.*

[N4] D.G. Northcott: *A note on the abstract Hilbert function. Journal London Math. Soc.* **35** *(1960), 209-214.*

[Or] O.Orecchia: *One-dimensional local rings with reduced associated graded ring and their Hilbert function. Manuscripta Math.* **32** *(1980), 391-405.*

[OOZ] F. Odetti, A. Oneto, E. Zatini: *Dedekind different and type sequence. Matematiche (Catania)* **55** *(2000), no. 2, 499-516.*

[OZ1] *A. Oneto, E. Zatini: On the value set of modules. Comm. Alg.* **26** *(1998), no. 11, 3853-3870.*

[OZ2] *A. Oneto, E. Zatini: Type sequence of modules. J. Pure Appl. Algebra* **160** *(2001), no. 1, 105-122.*

[Re] *L. Rédei: The theory of finitely generated commutative semigroups. Translation edited by N. Reilly, Pergamon Press, 1965.*

[R] *D. Rees: A Theorem of Homological Algebra. Camb. Phil. Soc.* **52** *(1956), 605-610.*

[R1] *J.C. Rosales: On numerical semigroups. Semigroup Forum* **52** *(1996), 441-455.*

[R2] *J.C. Rosales: Numerical Semigroups with Apéry sets of unique expression. J. of Alg.* **226** *(2000), 479-487.*

[RB] *J.c. Rosales and M.B. Branco: Irreducible numerical semigroup with arbitrary multiplicity and embedding dimension. J. of Alg.* **264** *(2003), 305-315.*

[RG] *J.C. Rosales, P.A. García-Sánchez: Finitely generated commutative monoids, Nova Science Publishers, Inc., Commack, NY, 1999.*

[Sa] *J.D. Sally: Numbers of generators of ideals in local rings Lecture Notes in pure and applied math. 35, Marcel Dekker Inc., 1978.*

[ZS] *O. Zariski and P. Samuel: Commutative Algebra Vol. II, Springer Verlag, 1975.*