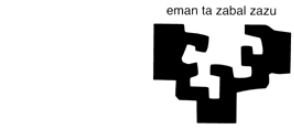



ZTF-FCT
Zientzia eta Teknologia Fakultatea
Facultad de Ciencia y Tecnología

# The Cohen structure theorem

Final Degree Dissertation
Degree in Mathematics

Andoni Zozaya Ursuegui

Supervisor:
Gustavo A. Fernández Alcober

Leioa, June 2017

# Contents

# Introduction

*"And the end of all our exploring*
*Will be to arrive where we started*
*And know the place for the first time"*
T. S. Eliot. Little Gidding.

The present dissertation aims to be an interesting summary about one fundamental branch of the theory of commutative rings with identity. More precisely, throughout this memory we are going to introduce the power series rings by means of their properties. Moreover, some of the aforementioned properties verified by the power series rings will turn out to be enough in order to characterize the power series ring.

The starting point will be the analysis of the general properties. Indeed, it is easy to see that the majority, but not all, of those properties are inherited from the properties of the ring of coefficients. Furthermore, if a ring verifies certain properties, it will be automatically isomorphic to the power series ring. But which ones are those properties? As we are about to see in our main theorem, they are four: being Noetherian, local, complete and regular. Moreover, if one removes the regularity condition, a weaker result will be obtained: although the ring may not be isomorphic to the power series ring, it will be reasonably close to the structure of a power series ring. This is briefly what is stated in the Cohen structure theorem.

This masterpiece, which in synthesis describes and sometimes classifies Noetherian, local and complete rings, was first developed by the young American algebraist Irvin Sol Cohen (1917-1955), who was the Ph. D. student of the famous mathematician Oscar Zariski (1899-1986), in 1946. It was published in the article *On the structure and ideal theory of complete local rings* in the Journal of the American Mathematical Society, and since then the result has been widely known as Cohen's structure theorem.

Another of the issues which are going to be developed in these notes is the problem of the essentially unique factorization in a ring. For decades, many algebraists struggled in order to figure out the minimal conditions for a ring

to be a unique factorization domain. A result related with the mentioned problem, which here is going to be presented as an immediate consequence of the main theorem, was solved in an alternative way by Masayoshi Nagata (1927-2006) in 1958 and by Maurice Auslander (1926-1994) and David Alvin Buchsbaum (1929-) in 1959. Indeed, they proved that any Noetherian regular local ring is a unique factorization domain.

In Chapter 1 three of our four main algebraic properties are analysed. Two of them have been studied in the degree (namely: locality and being Noetherian), reason why they are not going to be highlighted. Furthermore, we are going to focus on completeness. In order to speak about Cauchy sequences a metric space (or at least uniformity) is required. Therefore, the main goal of the chapter will be to define a metric over a ring and to describe its main features.

Chapter 2 will be a simple description of the algebraic properties of power series rings. As we have mentioned beforehand, the majority of those properties are inherited from the ring where the coefficients are taken. However, we are going to outline the power series whose coefficients lie in a field, since they are the objects of study of Cohen's structure theorem. Finally, we will study the essentially unique factorization in power series rings. Unfortunately, such study is not simple, but the reader is expected to become acquainted with useful results and techniques.

In Chapter 3 we are going to return to one of those essential properties of Cohen's structure theorem: regularity. In particular, it is related to the dimension of a local ring and both of them are concepts which have never been covered during the degree. Hence, both notions will be introduced in this chapter. They are strongly related to the set of prime ideals of a local ring. We are going to introduce a number of properties of the dimension, as well as to analyse its behaviour with respect to the number of generators, the quotients etc. Furthermore, regular rings shall be introduced, which, as their name implies, are rings with some "good" property involving the dimension. Such property will be helpful in order to define a set, called the system of parameters, which will describe the unique maximal ideal of a local ring and will perform a determinant role in our last theorem.

Finally, Chapter 4 presents the fundamental result, the one giving its name to the dissertation: the Cohen structure theorem. Unfortunately, even though the general result will be stated, we are going to study an easier case by making an additional assumption. Due to this extra condition, the coefficients of the series will turn out to lie in a field.

In short, the theorem has three parts. When regularity is left aside, the

initial ring will not be isomorphic to a power series ring. However, we shall obtain a partial result that asserts that the initial ring will be close to be a power series ring, either by being a quotient of such a power series ring (in the most general case); or by admitting a subring which is isomorphic to a power series ring (whenever the ring is an integral domain). Furthermore, if one additionally requires the regularity condition, we will obtain the expected theorem: the ring is isomorphic to a power series ring. Moreover, in all cases the number of variables of the power series ring will be related to the dimension of the ring.

The author of these notes hopes that the reader will get a global vision of the power series rings, as well as to provide a strong and powerful result of Commutative Algebra. And, of course I also hope that, above all, the reader will enjoy what is written through these pages.

# List of symbols

| | |
|---|---|
| $\operatorname{char} R$ | Characteristic of the ring $R$ |
| $\overline{B}(x, \varepsilon)$ | Closed ball of center $x$ and radious $\varepsilon$ |
| $\deg f$ | Degree of the polynomial $f$ |
| $(S)$ | Ideal generated by the set $S$ |
| $R_{\mathfrak{p}}$ | Localization of $R$ to the ideal $\mathfrak{p}$ |
| $B(x, \varepsilon)$ | Open ball of center $x$ and radious $\varepsilon$ |
| $\mathcal{U}(R)$ | Set of units of the ring $R$ |
| $\mathfrak{m}[X]$ | Set of polynomials with coefficients in the ideal $\mathfrak{m}$ |
| ED | Euclidean domain |
| ID | Integral domain |
| PID | Principal ideal domain |
| UFD | Unique factorization domain |

# Chapter 1

# Topological rings

Before starting it is important to remark that during these notes all the rings are considered to be commutative and with identity.

Throughout this dissertation, four basic ring properties will be analyzed: locality, Noetherian condition, completeness and regularity. Nevertheless, locality is a well-known property. This chapter deals with two of the remaining properties. Firstly, we will revise the concept of Noetherian ring. Secondly, we will define the completeness in one ring. In order to achieve that goal we are using algebraic structures such as the Jacobson radical and essential results as Krull's intersection theorem.

## 1.1 Noetherian and Artinian rings

One of the four fundamental ring properties that appear in Cohen's structure theorem is that a ring $R$ is Noetherian. In this section, we will define what a Noetherian ring is, and we will give some alternative characterizations. Their name was taken in honor of the mathematician Emmy Noether.

**Definition 1.1.1.** Let $R$ be a ring. Then $R$ is said to be *Noetherian* when it satisfies the following equivalent conditions:

(i) $R$ satisfies the ascending chain condition (acc). That is, whenever

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_n \subseteq \ldots$$

is a chain of ideals of $R$, then there exists $n_0 \in \mathbb{N}$ such that $\mathfrak{a}_n = \mathfrak{a}_{n_0}$ for all $n \geq n_0$;

(ii) every non-empty set of ideals of $R$ has a maximal member with respect to inclusion; and

(iii) every ideal $\mathfrak{a}$ of $R$ is finitely generated.

We ought to refresh one result concerning Noetherian rings.

**Proposition 1.1.2** (Hilbert)**.** *Let $R$ be a Noetherian ring, then the polynomial ring $R[X_1, \ldots, X_n]$ is a Noetherian ring.*

Since a similar result will be proved for power series in Chapter 2, we can skip this proof. Furthermore, in a similar way we can define what an Artinian ring is. Those rings were named after Emil Artin.

**Definition 1.1.3.** Let $R$ be a ring. Then $R$ is said to be *Artinian* when it satisfies the following equivalent conditions:

(i) $R$ satisfies the descending chain condition (dcc). That is, whenever

$$\mathfrak{a}_0 \supseteq \mathfrak{a}_1 \supseteq \cdots \supseteq \mathfrak{a}_n \supseteq \ldots$$

is a chain of ideals of $R$, then there exists $n_0 \in \mathbb{N}$ such that $\mathfrak{a}_n = \mathfrak{a}_{n_0}$ for all $n \geq n_0$ and

(ii) every non-empty set of ideals of $R$ has a minimal member with respect to inclusion.

## 1.2 Krull's intersection theorem

In order to speak about completeness, so of Cauchy sequences, we need a metric in the ring $R$ (or at least uniformity). This section presents Krull's intersection theorem, a necessary result in order to define the desired metric. First of all, let us recall the definition of local ring.

**Definition 1.2.1.** Let $R$ be a non-trivial ring, then $R$ is a *local* ring if it has a unique maximal ideal $\mathfrak{m}$.

Hereafter, we are writing $(R, \mathfrak{m})$ to denote a local ring $R$ and its unique maximal ideal $\mathfrak{m}$. Now we will introduce an ideal of an arbitrary ring named after Nathan Jacobson.

**Definition 1.2.2.** Let $R$ be a ring. The *Jacobson radical* of $R$, denoted by $\operatorname{Jac} R$, is the intersection of all the maximal ideals of $R$.

**Remark 1.2.3.** If $(R, \mathfrak{m})$ is a local ring, then $R$ has a unique maximal ideal, and thus $\operatorname{Jac} R = \mathfrak{m}$.

When $R$ is the trivial ring, the convention concerning the intersection of an empty family of ideals means that $\operatorname{Jac} R = R$. Moreover, notice that Zorn's lemma ensures the existence of maximal ideals in any non-trivial ring, so it is possible to intersect them. Thus, the Jacobson radical is well-defined.

Moreover, since the intersection of ideals is again an ideal, it is straightforward that $\operatorname{Jac} R$ is an ideal of $R$ and in particular it is not the empty set. The following proposition characterizes the Jacobson radical of $R$.

**Proposition 1.2.4.** *Let $R$ be a ring and let $r \in R$. Then $r \in \operatorname{Jac} R$ if and only if, for any $a \in R$, $1 - ar$ is a unit of $R$.*

*Proof.* $\Rightarrow$) Take $r \in \operatorname{Jac} R$ and suppose by contradiction that there exists $a \in R$ such that $1 - ar$ is not a unit of $R$. Then there exists a maximal ideal $\mathfrak{m}$ containing $1 - ar$. However, by the definition of $\operatorname{Jac} R$, $r \in \operatorname{Jac} R \subseteq \mathfrak{m}$ and so

$$1 = (1 - ar) + ar \in \mathfrak{m},$$

which is a contradiction.

$\Leftarrow$) Suppose that for any $a \in R$, we have that $1 - ar$ is a unit in $R$. Let $\mathfrak{m}$ be any maximal ideal, we shall see that $r \in \mathfrak{m}$. Suppose by contradiction that $r \notin \mathfrak{m}$ for a particular $\mathfrak{m}$, in this case we would have that

$$\mathfrak{m} \subsetneq (\mathfrak{m}, r) \subseteq R,$$

and by the maximality of $\mathfrak{m}$, $(\mathfrak{m}, r) = R$. Hence, there exist $b \in \mathfrak{m}$ and $a \in R$ such that $b + ar = 1$, and so $b = 1 - ar$ is a unit of $R$, which is a contradiction. Indeed, a unit $1 - ar$ cannot be contained in the maximal ideal $\mathfrak{m}$, because otherwise $\mathfrak{m} = R$. This shows that $r \in \mathfrak{m}$ for each maximal ideal and so $r \in \operatorname{Jac} R$. □

Let us now introduce two important results related to the Jacobson radical of a ring.

**Lemma 1.2.5** (Nakayama)**.** *Let $R$ be a ring, let $M$ be a finitely generated $R$-module and let $\mathfrak{a}$ be an ideal of $R$ such that $\mathfrak{a} \subseteq \operatorname{Jac} R$. If $M = \mathfrak{a}M$, then $M = \{0\}$.*

*Proof.* Suppose that $M \neq \{0\}$ and look for a contradiction. Consider a minimal generating set $L = \{g_1, \ldots, g_n\}$ of $M$. This means that $M$ is generated by $L$ but not by any proper subset of $L$. Since $M \neq \{0\}$ then $L$ is not the empty set.

On the one hand, $g_1 \in \mathfrak{a}M$ and so there exist some $a_1, a_2, \ldots, a_n \in \mathfrak{a} \subseteq R$ such that $g_1 = \sum_{i=1}^{n} a_i g_i$. Therefore,

$$(1 - a_1)g_1 = \sum_{i=2}^{n} a_i g_i.$$

Finally, since $a_1 \in \mathfrak{a} \subseteq \operatorname{Jac} R$ and $1 \in R$, according to Proposition 1.2.4, then $1 - a_1$ is a unit in $R$, with inverse $u$ say. Then

$$g_1 = u(1 - a_1)g_1 = \sum_{i=2}^{n} u a_i g_i.$$

Thus $M$ is generated by $\{g_2, \ldots, g_n\}$, a proper subset of $L$, which is a contradiction. Therefore, $M = \{0\}$. □

Notice that in a Noetherian ring $R$, any ideal is finitely generated as an $R$-module. Thus, the above lemma can be applied in Noetherian rings.

**Theorem 1.2.6** (Krull's intersection theorem)**.** *Let $R$ be a Noetherian ring and let $\mathfrak{a}$ be an ideal. Then*

$$\bigcap_{n=1}^{\infty} \mathfrak{a}^n = \{0\}$$

*under either of the following hypotheses:*

- *$R$ is an integral domain and $\mathfrak{a}$ is a proper ideal.*
- *$\mathfrak{a}$ is contained in the Jacobson radical of $R$.*

*Proof.* Since $R$ is a Noetherian ring $\mathfrak{a}$ is finitely generated so assume $\mathfrak{a} = (a_1, \ldots, a_k)$ and consider any $a \in \bigcap_{n=1}^{\infty} \mathfrak{a}^n$. For each $n$ there exists a homogeneous polynomial of degree $n$, say $P_n$, such that $a = P_n(a_1, \ldots, a_k)$. Indeed, since $a \in \mathfrak{a}^n$, then

$$a = \sum_{i=1}^{l} x_{i_1} \ldots x_{i_n} = \sum_{i=1}^{l} \tilde{P}_i(a_1, \ldots, a_k) = P_n(a_1, \ldots, a_k),$$

where each $x_{i_j} \in \{a_1, \ldots, a_k\}$ and each $\tilde{P}_i$ is a monomial of total degree $n$, so $P_n = \sum_{i=1}^{l} \tilde{P}_i$ is a homogeneous polynomial of total degree $n$.

In the Noetherian ring $R[X_1, \ldots, X_k]$ we consider the ascending chain of ideals defined by $\mathfrak{P}_j = (P_1, \ldots, P_j)$ for each $j \in \mathbb{N}$. Since this chain is eventually stationary we know that $\mathfrak{P}_m = \mathfrak{P}_{m+1}$ for some $m$. We claim that we can write

$$P_{m+1} = Q_m P_1 + \cdots + Q_1 P_m,$$

where every $Q_i$ is a homogeneous polynomial of degree $i$. Indeed, we know that there exist some polynomials $R_i$ such that

$$P_{m+1} = R_m P_1 + \cdots + R_1 P_m.$$

But $P_{m+1}$ is a homogeneous polynomial of degree $m+1$, so for each $R_i$ we can discard the monomials of degree different to $i$ and obtain a linear combination of homogeneous polynomials.

In fact, for each $i$ we can write $R_i = Q_i + F_i$ where $Q_i$ is the homogeneous polynomial part of degree $i$ and $F_i = R_i - Q_i$. Then

$$\begin{aligned} P_{m+1} &= R_m P_1 + \cdots + R_1 P_m \\ &= (Q_m + F_m) P_1 + \cdots + (Q_1 + F_1) P_m \\ &= Q_m P_1 + \cdots + Q_1 P_m + F_m P_1 + \cdots + F_1 P_m. \end{aligned}$$

Now $P_{m+1}$ and all the products $Q_m P_1, \ldots, Q_1 P_m$ are homogeneous polynomials of degree $m+1$ and it is clear that $F_i P_{m-i+1}$ has no monomial component of degree $m+1$. Thus, clearly $F_m P_1 + \cdots + F_1 P_m = 0$ and the assertion follows.

Evaluating the polynomial $P_{m+1}$ in $(a_1, \ldots, a_k)$ we get:

$$\begin{aligned} P_{m+1}(a_1, \ldots, a_k) &= \sum_{i=1}^{m} Q_i(a_1, \ldots, a_k) P_{m+1-i}(a_1, \ldots, a_k) \\ &= a \sum_{i=1}^{m} Q_i(a_1, \ldots, a_k). \end{aligned}$$

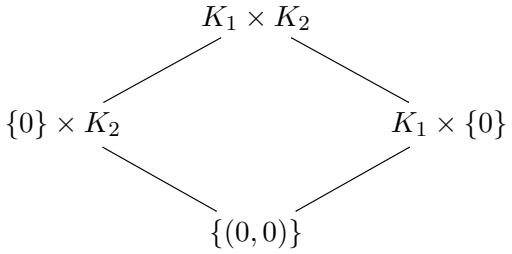
Say $r = \sum_{i=1}^{m} Q_i(a_1, \ldots, a_k) \in \mathfrak{a}$, then

$$a = a \cdot r \iff (1-r) \cdot a = 0.$$

In the case when $\mathfrak{a} \subseteq \operatorname{Jac} R$, according to Proposition 1.2.4, then $1-r$ is a unit, so $a = 0$. And when $\mathfrak{a}$ is a proper ideal of an integral domain, firstly $r \neq 1$, because $r \in \mathfrak{a} \subsetneq R$. Secondly $a \cdot (1-r) = 0$ and $r \neq 1$ implies $a = 0$. In both cases $a = 0$ and so $\cap_{n=1}^{\infty} \mathfrak{a}^n = \{0\}$. □

After presenting this result the reader ought to ask himself if all the conditions are really necessary. The following example will clarify that doubt.

**Remark 1.2.7.** Let $K_1$ and $K_2$ be two fields, and consider the ring $R = K_1 \times K_2$. Since $(1,0) \cdot (0,1) = (0,0)$, $R$ is not an integral domain. On the other hand, $\operatorname{Jac} R = \{0\} \times \{0\}$. Indeed, it is well-known that the ideals of a product ring are products of ideals of each factor ring. Hence, $R$ has four ideals: the total one, the trivial one and the two maximal ideals $K_1 \times \{0\}$ and $\{0\} \times K_2$.




Finally consider the ideal $\mathfrak{a} = K_1 \times \{0\}$, which does not satisfy either of the two possible hypotheses and observe that

$$\bigcap_{n=1}^{\infty} (K_1 \times \{0\})^n = K_1 \times \{0\}.$$

Hence, if $R$ is not an integral domain and $\mathfrak{a}$ is not contained in $\operatorname{Jac} R$, the result does not follow.

In the particular case when $R$ is a local ring and $\mathfrak{m}$ is its unique maximal ideal we have the following corollary.

**Corollary 1.2.8.** *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then*

$$\bigcap_{n=1}^{\infty} \mathfrak{m}^n = \{0\}.$$

*Proof.* It is straightforward from Theorem 1.2.6, once we notice that when $R$ is a local ring then $\operatorname{Jac} R = \mathfrak{m}$. □

## 1.3 The $\mathfrak{a}$-adic topology

Now we are ready to define a metric in a Noetherian ring. Moreover, the structure we are defining is more than a usual metric, it is an ultrametric.

**Definition 1.3.1.** Let $X$ be a set and let $d\colon X \times X \to [0, \infty)$ be a map with the following properties:
(i) Identity of indiscernibles:

$$d(x, y) = 0 \text{ if and only if } x = y.$$

(ii) Symmetry:

$$d(x, y) = d(y, x), \quad \forall x, y \in X.$$

(iii) Ultrametric triangle inequality:

$$d(x, z) \leq \max\{d(x, y), d(y, z)\}, \quad \forall x, y, z \in X.$$

Then $(X, d)$ is said to be an *ultrametric space*.

It is clear that the third condition implies the usual triangle inequality. Indeed, for any $x, y, z \in X$, it follows that

$$d(x, z) \leq \max\{d(x, y), d(y, z)\} \leq d(x, y) + d(y, z).$$

Thus any ultrametric space is a metric space. However, the converse implication in general is not true. For example, $\mathbb{R}$ with the usual metric is a metric space, but it is not an ultrametric space.

**Theorem 1.3.2.** *Let $R$ be a Noetherian ring and $\mathfrak{a} \subseteq R$ an ideal satisfying Krull's intersection theorem, thas is, $\cap_{n=1}^{\infty} \mathfrak{a}^n = \{0\}$. Define*

$$d\colon R \times R \to [0, \infty)$$

*as follows: $d(x, x) = 0$ and when $x \neq y$ set $d(x, y) = 2^{-t}$ where $t \in \mathbb{N} \cup \{0\}$ is the greatest integer such that $x - y \in \mathfrak{a}^t$ (by convention assume that $\mathfrak{a}^0 = R$). Then $d$ is an ultrametric on $R$.*

*Proof.* Firstly, we shall see that $d$ is well defined when $x \neq y$. It is a straightforward consequence of Krull's intersection theorem. Since

$$\mathfrak{a} \supseteq \mathfrak{a}^2 \supseteq \cdots \supseteq \mathfrak{a}^i \supseteq \ldots$$

is a descending chain $t$ must be finite. Otherwise it would mean that $x - y \in \cap_{n=1}^{\infty} \mathfrak{a}^n = \{0\}$, and so $x = y$ which is a contradiction.

Secondly, we shall check that the three conditions which define an ultrametric are satisfied.

(i) $d(x, y) = 0$ if and only if $x = y$.

The *if and only if* is clear by definition. Indeed, when $x \neq y$, then there exists an integer $t \in \mathbb{N} \cup \{0\}$ such that $d(x, y) = 2^{-t} > 0$.

(ii) $d(x, y) = d(y, x)\ \forall x, y \in R$.

Notice that $x - y \in \mathfrak{a}^t$ if and only if $y - x \in \mathfrak{a}^t$. So clearly $d(x, y) = d(y, x)$.

(iii) $d(x, z) \leq \max\{d(x, y), d(y, z)\},\ \forall\ x, y, z \in R$.

If there is some equality between $x, y$ or $z$ it is clear. Thus, consider that $d(x, y) = 2^{-t_1}$ and $d(y, z) = 2^{-t_2}$ and suppose without loss of generality that $t_2 \geq t_1$. Then since $\mathfrak{a}^{t_1} \supseteq \mathfrak{a}^{t_2}$ we have that $y - z,\ x - y \in \mathfrak{a}^{t_1}$. Hence,

$$x - z = (x - y) + (y - z) \in \mathfrak{a}^{t_1},$$

and so

$$d(x, z) \leq 2^{-t_1} = \max\{2^{-t_1}, 2^{-t_2}\} = \max\{d(x, y),\ d(y, z)\}.$$

□

Once we have defined a distance on $R$, we can consider $R$ as a topological space with the topology induced by the metric $d$. This topology is known as $\mathfrak{a}$-*adic topology.*

**Remark 1.3.3.** Note that the number 2 has been chosen rather arbitrarily, any other number strictly bigger than 1 will define an equivalent distance.*.

*Two distances $d_1$ and $d_2$ over a set $X$ are equivalent when there exist two positive constants $\alpha$ and $\beta$ such that

$$\alpha d_1(x, y) \leq d_2(x, y) \leq \beta d_1(x, y)\ \forall x, y \in X.$$

**Corollary 1.3.4.** *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Define*

$$d\colon R \times R \to [0, \infty)$$

*as follows: $d(x, x) = 0$ and when $x \neq y$ set $d(x, y) = 2^{-t}$ where $t \in \mathbb{N} \cup \{0\}$ is the greatest integer such that $x - y \in \mathfrak{m}^t$ (by convention assume that $\mathfrak{m}^0 = R$). Then $d$ is an ultrametric on $R$.*

In particular, the above topology on $R$ is called the $\mathfrak{m}$-adic topology. More precisely, once we have a distance, the $\mathfrak{a}$-adic topology is defined by considering the following collection of open sets:

$$\tau_R = \{U \subseteq R \mid \forall x \in U \ \ \exists \varepsilon > 0 \text{ such that } B(x, \varepsilon) \subseteq U\}.$$

Let us now look for some of the properties of the $\mathfrak{a}$-adic topology.

**Proposition 1.3.5.** *Let $R$ be a Noetherian ring and let $\mathfrak{a} \subseteq R$ be an ideal of $R$ satisfying Krull's intersection theorem. Then $R$ with the $\mathfrak{a}$-adic topology is Hausdorff.*

*Proof.* Any metric space is Hausdorff. □

Furthermore, open and closed balls can be easily characterized using ideals.

**Lemma 1.3.6.** *Let $R$ be a Noetherian ring with the $\mathfrak{a}$-adic topology, for some suitable ideal $\mathfrak{a} \subseteq R$. Then for every natural number $n \in \mathbb{N}$ and $x \in R$, we have*

$$\overline{B}(x, 2^{-n}) = x + \mathfrak{a}^n.$$

*Proof.* $\subseteq$) Set $y \in \overline{B}(x, 2^{-n})$, then $d(y, x) \leq 2^{-n}$ and so $y - x \in \mathfrak{a}^n$. Thus, $y \in x + \mathfrak{a}^n$.
$\supseteq$) Set $y \in x + \mathfrak{a}^n$. Then $y - x \in \mathfrak{a}^n$ and so $d(y, x) \leq 2^{-n}$. Hence, $y \in \overline{B}(x, 2^{-n})$. □

**Lemma 1.3.7.** *Let $R$ be a Noetherian ring with the $\mathfrak{a}$-adic topology, for some suitable ideal $\mathfrak{a} \subseteq R$. Then for every natural number $n \in \mathbb{N}$ and $x \in R$, we have*

$$B(x, 2^{-n}) = x + \mathfrak{a}^{n+1}.$$

*Proof.* $\subseteq$) Set $y \in B(x, 2^{-n})$, then $d(y, x) < 2^{-n}$ and so $y - x \in \mathfrak{a}^{n+1}$. Thus, $y \in x + \mathfrak{a}^{n+1}$.
$\supseteq$) Set $y \in x + \mathfrak{a}^{n+1}$. Then $y - x \in \mathfrak{a}^{n+1}$ and so $d(y, x) < 2^{-n}$. Hence, $y \in B(x, 2^{-n})$. □

**Lemma 1.3.8.** *Let $R$ be a Noetherian ring with the $\mathfrak{a}$-adic topology, for some suitable ideal $\mathfrak{a} \subseteq R$. Then $U \subseteq R$ is open if and only if for each $x \in U$ there exists a natural number $n \in \mathbb{N}$ such that $x + \mathfrak{a}^n \subseteq U$.*

*Proof.* Firstly notice that for any $\varepsilon > 0$, there exists $n \in \mathbb{N}$ such that $2^{-(n-1)} \leq \varepsilon$. Then we shall prove both implications.

$\Rightarrow$) By definition $U \subseteq R$ is open if and only if there exists an $\varepsilon > 0$ such that $B(x, \varepsilon) \subseteq U$. Hence, by the above remark and Lemma 1.3.7 there exists $n \in \mathbb{N}$ such that

$$x + \mathfrak{a}^n = B(x, 2^{-n+1}) \subseteq B(x, \varepsilon) \subseteq U.$$

$\Leftarrow$) According to Lemma 1.3.7 and the initial hypothesis, $B(x, 2^{-n+1}) = x + \mathfrak{a}^n \subseteq U$. Hence, it is enough to take $\varepsilon = 2^{-(n-1)} > 0$. □

Therefore using the notation of ideals, the $\mathfrak{a}$-adic topology can also be defined as:

$$\tau_R = \{U \subseteq R \mid \forall x \in U \ \ \exists n \in \mathbb{N} \text{ such that } x + \mathfrak{a}^n \subseteq U\}.$$

Naturally, all these properties stated and proved for the $\mathfrak{a}$-adic topology, hold for the $\mathfrak{m}$-adic topology over a Noetherian local ring $(R, \mathfrak{m})$.

## 1.4 Completeness

Finally, in this section the notion of completeness in a ring will be analyzed once we have the $\mathfrak{a}$-adic topology defined over the ring. General topology results (applicable in any metric space), as well as particular properties of the ultrametrics will be explained in order to apply them to the $\mathfrak{a}$-adic topology. We should begin refreshing some concepts.

**Definition 1.4.1.** Let $(X, d)$ be a metric space and let $(a_n)_{n\in\mathbb{N}} \subseteq X$ be a sequence. Then we say that $(a_n)_{n\in\mathbb{N}}$ is *convergent* to the point $a \in X$ if

$$\forall \varepsilon > 0 \ \ \exists n_0 \in \mathbb{N} \text{ such that } \forall n \geq n_0 \ a_n \in B(a, \varepsilon) \text{ (i.e. } d(a_n, a) < \varepsilon).$$

We denote it as $\lim_{n\to\infty} a_n = a$.

Clearly the above condition, the one which defines a convergent sequence, is equivalent to say that

$$\forall k \in \mathbb{N} \ \ \exists n_0 \in \mathbb{N} \text{ such that } \forall n \geq n_0 \ d(a_n, a) < 2^{-k}.$$

Moreover, when the set $X$ has ring structure with an addition and a multiplication, then those operations are completely compatible with the limit.

**Proposition 1.4.2.** *Let $R$ be a ring with the $\mathfrak{a}$-adic metric, for a suitable ideal $\mathfrak{a}$, and let $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ be two convergent sequences. Then*

(i) $\lim_{n\to\infty}(a_n + b_n) = \lim_{n\to\infty} a_n + \lim_{n\to\infty} b_n$.

(ii) $\lim_{n\to\infty}(a_n - b_n) = \lim_{n\to\infty} a_n - \lim_{n\to\infty} b_n$.

(iii) $\lim_{n\to\infty}(a_n \cdot b_n) = \lim_{n\to\infty} a_n \cdot \lim_{n\to\infty} b_n$.

*Proof.* Since the three cases are alike, here only case (ii) will be done as an example. Let $\lim_{n\to\infty} a_n = a$ and $\lim_{n\to\infty} b_n = b$. Then choose $k \in \mathbb{N}$

$$\exists\ n_1 \in \mathbb{N} \text{ such that } \forall n \geq n_1 \text{ then } d(a_n, a) < 2^{-k+1} \iff a_n - a \in \mathfrak{a}^k \text{ and}$$

$$\exists\ n_2 \in \mathbb{N} \text{ such that } \forall n \geq n_2 \text{ then } d(b_n, b) < 2^{-k+1} \iff b_n - b \in \mathfrak{a}^k.$$

Thus, when $n \geq \max\{n_1, n_2\}$, then

$$(a_n - b_n) - (a - b) = (a_n - a) - (b_n - b) \in \mathfrak{a}^k \iff d(a_n - b_n, a - b) < 2^{-k+1}.$$

Hence, $\lim_{n\to\infty}(a_n - b_n) = a - b$. □

**Definition 1.4.3.** Let $(X, d)$ be a metric space and let $(a_n)_{n\in\mathbb{N}} \subseteq X$ be a sequence. Then $(a_n)_{n\in\mathbb{N}}$ is said to be a *Cauchy sequence* when

$$\forall \varepsilon > 0 \text{ there exists } n_0 \in \mathbb{N} \text{ such that } \forall n, m \geq n_0 \ \ d(a_n, a_m) < \varepsilon.$$

Clearly the above condition is equivalent to

$$\forall k \in \mathbb{N} \text{ there exists } n_0 \in \mathbb{N} \text{ such that } \forall n, m \geq n_0 \ \ d(a_n, a_m) < 2^{-k}.$$

**Proposition 1.4.4.** *Let $(X, d)$ be a metric space and let $(a_n)_{n\in\mathbb{N}} \subseteq X$ be a convergent sequence. Then $(a_n)_{n\in\mathbb{N}}$ is a Cauchy sequence.*

*Proof.* Let $(a_n)_{n\in\mathbb{N}}$ be a convergent sequence such that $\lim_{n\to\infty} a_n = a$. Then for any $\varepsilon > 0$ there exists $n_0 \in \mathbb{N}$ such that for all $l \geq n_0$, $d(a, a_l) < \varepsilon/2$. Thus, when $n, m \geq n_0$,

$$d(a_n, a_m) \leq d(a_n, a) + d(a, a_m) < \varepsilon.$$

Therefore, $(a_n)_{n\in\mathbb{N}}$ is a Cauchy sequence. □

The converse of this theorem is not true. Consider the sequence $(1/n)_{n\in\mathbb{N}}$ with the usual metric. This sequence is convergent in $\mathbb{R}$, and so it is a Cauchy sequence. However, in the metric space $(0, 1]$ it is a Cauchy sequence (because the distance between the terms is the same) but it is not convergent.

**Definition 1.4.5.** Let $(X, d)$ be a metric space. Then $(X, d)$ is said to be a *complete* metric space when any Cauchy sequence is convergent.

**Examples 1.4.6.** (i) It is well-known that $\mathbb{R}^n$ is complete with the usual metric.
(ii) The power series ring in $n$ indeterminates over a field $K$, $K[[X_1, \ldots, X_n]]$, is complete with respect the $(X_1, \ldots, X_n)$-adic topology. (See Proposition 2.3.4.)
(iii) The field of rational numbers, $\mathbb{Q}$, is not complete with the usual metric. For example, $\left(\left(1 + \frac{1}{n}\right)^n\right)_{n\in\mathbb{N}}$ has not a rational limit.
(iv) On the other hand, $(0, 1)$ with the usual metric is not complete. Indeed, the sequence $\left(\frac{1}{n+1}\right)_{n\in\mathbb{N}}$ is a Cauchy sequence, but it is not convergent.

We have given the definition of a Cauchy sequence in any metric space. However, there is an alternative definition in an ultrametric space.

**Proposition 1.4.7.** *Let $(X, d)$ be an ultrametric space and let $(a_n)_{n\in\mathbb{N}} \subseteq X$ be a sequence. Assume that*

$$\forall \varepsilon > 0 \text{ there exists } n_0 \in \mathbb{N} \text{ such that } \forall n \geq n_0 \;\; d(a_n, a_{n+1}) < \varepsilon.$$

*Then $(a_n)_{n\in\mathbb{N}}$ is a Cauchy sequence.*

*Proof.* By hypothesis:

$$\forall \varepsilon > 0 \;\; \exists n_0 \in \mathbb{N} \text{ such that } \forall n \geq n_0 \;\; d(a_n, a_{n+1}) < \varepsilon.$$

Take any $m, n \geq n_0$ $(m > n)$. Since $d$ is an ultrametric distance, then

$$d(a_m, a_n) \leq \max\{d(a_m, a_{m-1}), \ldots, d(a_{n+1}, a_n)\} = d(a_{n_1+1}, a_{n_1}),$$

for some $n_1 \geq n_0$. Hence, $d(a_{n_1+1}, a_{n_1}) < \varepsilon$. And so,

$$\forall \varepsilon > 0 \;\; \exists n_0 \in \mathbb{N} \text{ such that } \forall m, n \geq n_0 \;\; d(a_m, a_n) \leq d(a_{n_1+1}, a_{n_1}) < \varepsilon.$$

Therefore, $(a_n)_{n\in\mathbb{N}}$ is a Cauchy sequence. □

Obviously, the converse of this result is true in any metric space. Hence, the above proposition gives another characterization for Cauchy sequences in ultrametric spaces.

However, the result is false in general metric spaces. Consider $\mathbb{R}$ with the usual distance (which is not an ultrametric distance). Then $\sum_{n=1}^{\infty} \frac{1}{n}$ is divergent, so the sequence of partial sums, $S_n$, is not convergent and since $(\mathbb{R}, d_u)$ is complete neither it is Cauchy. This sequence is given by

$$S_n = \sum_{k=1}^{n} \frac{1}{k}.$$

Nevertheless, the weaker property holds:

$$\lim_{n\to\infty} d_u(S_{n+1}, S_n) = \lim_{n\to\infty} \frac{1}{n+1} = 0.$$

With the following result the reader can appreciate how useful it is working with ultrametric distances in a complete ring. In fact, a necessary condition for series convergence will be a sufficient condition.

**Proposition 1.4.8.** *Let $R$ be a complete ring with respect to the $\mathfrak{a}$-adic topology, for some suitable ideal $\mathfrak{a} \subseteq R$. Then the series $\sum_{n=1}^{\infty} a_n$ is convergent if and only if the general term tends to zero.*

*Proof.* $\Rightarrow$) As $\sum_{n=1}^{\infty} a_n$ is convergent then the sequence of partial sums, $S_n$, is also convergent. Let $\lim_{n\to\infty} S_n = S$. For all $n \geq 2$, then $a_n = S_n - S_{n-1}$, so

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} (S_n - S_{n-1}) = \lim_{n\to\infty} S_n - \lim_{n\to\infty} S_{n-1} = S - S = 0.$$

$\Leftarrow$) On the one hand,

$$\lim_{n\to\infty} (S_n - S_{n-1}) = \lim_{n\to\infty} a_n = 0.$$

That is,

$$\forall k \in \mathbb{N}\ \exists n_0 \in \mathbb{N} \text{ such that } \forall n \geq n_0 \text{ then } S_n - S_{n-1} = a_n \in \mathfrak{a}^k.$$

Hence,

$$\forall k \in \mathbb{N}\ \exists n_0 \in \mathbb{N} \text{ such that } \forall n \geq n_0 \text{ then } d(S_n, S_{n-1}) \leq 2^{-k}.$$

Thus,

$$\lim_{n\to\infty} d(S_n, S_{n-1}) = 0.$$

According to Proposition 1.4.7 the sequence $(S_n)_{n\in\mathbb{N}}$ is Cauchy. Finally, as the space is complete $(S_n)_{n\in\mathbb{N}}$, which is Cauchy, is also convergent, so the series is convergent. □

We know that not all metric spaces are complete. However, one way of avoiding this problem is to construct a bigger metric space *containing* the initial one and which actually is complete.

**Definition 1.4.9.** Let $(X, d)$ be a metric space. A *completion* of $(X, d)$ is a metric space $(\hat{X}, \hat{d})$ such that

(i) $(\hat{X}, \hat{d})$ is a complete metric space.

(ii) There exists a map $\varphi\colon X \to \hat{X}$ such that

$$d(x, y) = \hat{d}(\varphi(x), \varphi(y)) \quad \forall x, y \in X.$$

(iii) $\varphi(X)$ is dense in $\hat{X}$.

Notice that (ii) means that the initial metric space $X$ is isometric to $\varphi(X)$, which is a dense subset of $\hat{X}$.

**Remark 1.4.10.** In several examples, $(\hat{X}, \hat{d})$ will be a metric space such that $X \subseteq \hat{X}$ and $\hat{d}|_X = d$. That is, the application $\varphi$ is actually the inclusion $\iota\colon X \to \hat{X}$ and $X$ is dense in $\hat{X}$.

As we shall see now, given an abstract metric space we will always be able to embed it in a unique (up to isometry) complete metric space which contains it. Morever, the new space will not be very *big* compared with the initial one. The proof is technical and long, and we will also need a technical lemma in order to prove it.

**Lemma 1.4.11.** *Let $(X, d)$ be a metric space and $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ two convergent sequences in $X$. Then*

$$d\left(\lim_{n\to\infty} a_n, \lim_{n\to\infty} b_n\right) = \lim_{n\to\infty} d(a_n, b_n)$$

*Proof.* It is a consequence of the triangle inequality. On the one hand, we have

$$\begin{aligned}\lim_{n\to\infty} d(a_n, b_n) &\leq \lim_{n\to\infty} \left[d\left(a_n, \lim_{n\to\infty} a_n\right) + d\left(\lim_{n\to\infty} a_n, \lim_{n\to\infty} b_n\right) + d\left(b_n, \lim_{n\to\infty} b_n\right)\right] \\ &= d\left(\lim_{n\to\infty} a_n, \lim_{n\to\infty} b_n\right).\end{aligned}$$

In a similar way,

$$\begin{aligned}d\left(\lim_{n\to\infty} a_n, \lim_{n\to\infty} b_n\right) &= \lim_{n\to\infty} d\left(\lim_{n\to\infty} a_n, \lim_{n\to\infty} b_n\right) \\ &\leq \lim_{n\to\infty} \left[d\left(a_n, \lim_{n\to\infty} a_n\right) + d(a_n, b_n) + d\left(b_n, \lim_{n\to\infty} b_n\right)\right] \\ &= \lim_{n\to\infty} d(a_n, b_n).\end{aligned}$$

Hence, we obtain the other inequality and the lemma is proved. □

**Theorem 1.4.12** (Completion theorem for metric spaces)**.** *Let $(X, d)$ be a metric (ultrametric) space. Then there exists a metric (ultrametric) space $(\hat{X}, \hat{d})$ that is the completion of $(X, d)$. Moreover, the space $(\hat{X}, \hat{d})$ is unique up to isometry.*

*Proof.* We will divide the proof into several steps.

*Step 1* (Construction of $(\hat{X}, \hat{d})$). In the set of all Cauchy sequences formed by elements of $X$, we define the following relation,

$$(a_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}} \iff \lim_{n\to\infty} d(a_n, b_n) = 0.$$

It can be easily checked that $\sim$ is an equivalence relation. Hence, we can define the quotient set

$$\hat{X} = \{[(a_n)_{n\in\mathbb{N}}] \mid (a_n)_{n\in\mathbb{N}} \text{ is Cauchy}\}.$$

Now we may define a new metric on the set $\hat{X}$. Let $A = [(a_n)_{n\in\mathbb{N}}]$ and $B = [(b_n)_{n\in\mathbb{N}}]$ be two elements in $\hat{X}$. We define

$$\hat{d}(A, B) = \lim_{n\to\infty} d(a_n, b_n).$$

We will show that $\hat{d}$ is a metric defined on $\hat{X}$. Firstly, we have to check that it is well-defined, that is, $\hat{d}(A, B) < +\infty$ and that it does not depend on the representatives chosen. First we see that $\lim_{n\to\infty} d(a_n, b_n) < +\infty$, i.e., that the sequence of distances $d(a_n, b_n)$ is convergent in $\mathbb{R}$. Since $\mathbb{R}$ is complete, it suffices to check that it is Cauchy. Being Cauchy is clear using the triangle inequality and taking into account that $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ are Cauchy :

$$\begin{aligned} d(a_n, b_n) - d(a_m, b_m) &\leq d(a_n, a_m) + d(a_m, b_m) + d(a_m, b_n) - d(a_m, b_m) \\ &= d(a_n, a_m) + d(b_m, b_n). \end{aligned}$$

We also have to prove that $\hat{d}$ does not depend on the sequences $(a_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}}$ chosen as representatives of $A$ and $B$, respectively. Assume that $A = [(a_n)_{n\in\mathbb{N}}] = [(a'_n)]_{n\in\mathbb{N}}$ and $B = [(b_n)_{n\in\mathbb{N}}] = [(b'_n)]_{n\in\mathbb{N}}$. Our aim is to show that $\lim_{n\to\infty} d(a_n, b_n) = \lim_{n\to\infty} d(a'_n, b'_n)$. Using the triangle inequality we get

$$\lim_{n\to\infty} d(a_n, b_n) \leq \lim_{n\to\infty} [d(a_n, a'_n) + d(a'_n, b'_n) + d(b'_n, b_n)] = \lim_{n\to\infty} d(a'_n, b'_n).$$

Notice that in the last equality $\lim_{n\to\infty} d(a_n, a'_n) = \lim_{n\to\infty} d(b_n, b'_n) = 0$ because $(a_n)_{n\in\mathbb{N}} \sim (a'_n)_{n\in\mathbb{N}}$ and $(b_n)_{n\in\mathbb{N}} \sim (b'_n)_{n\in\mathbb{N}}$. Now, by symmetry we obtain the opposite inequality and hence the desired equality.

It is straightforward to prove that $\hat{d}$ satisfies the axioms of a metric:

1) Since $d(a_n, b_n) \geq 0$ it is clear that $\hat{d}(A, B) \geq 0$.

2) We have the following chain of equivalences:

$$\begin{aligned} \hat{d}(A, B) = 0 &\iff \lim_{n\to\infty} d(a_n, b_n) = 0 \\ &\iff (a_n)_{n\in\mathbb{N}} \sim (b_n)_{n\in\mathbb{N}} \iff A = B. \end{aligned}$$

3) It is clear that $\hat{d}(A, B) = \hat{d}(B, A)$ because $d$ also satisfies the symmetric condition.

4) Let $A = [(a_n)_{n\in\mathbb{N}}]$, $B = [(b_n)_{n\in\mathbb{N}}]$ and $C = [(c_n)_{n\in\mathbb{N}}]$ be three elements in $\hat{X}$. By the triangle inequality for $d$, for each $n \in \mathbb{N}$ we have $d(a_n, b_n) \leq d(a_n, c_n) + d(c_n, b_n)$. Taking limits, we get

$$\hat{d}(A, B) \leq \hat{d}(A, C) + \hat{d}(C, B).$$

(When $d$ is an ultrametric the ultrametric triangle inequality for $\hat{d}$ is satisfied by the ultrametric triangle inequality for $d$.)

Thus $(\hat{X}, \hat{d})$ is a metric space. Moreover, when $d$ is an ultrametric $(\hat{X}, \hat{d})$ is an ultrametric space. The following steps are devoted to proving that the new metric space satisfies the required properties.

*Step 2.* ($X$ is isometric to a subspace of $\hat{X}$). Define the map

$$\begin{aligned} \varphi\colon X &\to \hat{X} \\ x &\mapsto \varphi(x) = [(x)_{n\in\mathbb{N}}] \end{aligned}$$

It is well-defined, that is $\varphi(x) \in \hat{X}$, because a constant sequence is always Cauchy. Now we prove that $\varphi$ is injective:

$$\begin{aligned} \varphi(x) = \varphi(y) &\implies [(x)_{n\in\mathbb{N}}] = [(y)_{n\in\mathbb{N}}] \implies (x)_{n\in\mathbb{N}} \sim (y)_{n\in\mathbb{N}} \\ &\implies \lim_{n\to\infty} d(x, y) = 0 \implies d(x, y) = 0 \implies x = y. \end{aligned}$$

Hence, $\varphi$ restricted to its image is a bijection. Let $X_1 = \varphi(X) \subseteq \hat{X}$. Notice that $X_1$ is the set of equivalence classes which admit a constant sequence as a representative.

We will prove that $\varphi\colon X \to X_1$ is an isometry. We only have to prove that distances are preserved:

$$\hat{d}(\varphi(x), \varphi(y)) = \hat{d}\,([(x)_{n\in\mathbb{N}}], [(y)_{n\in\mathbb{N}}]) = \lim_{n\to\infty} d(x, y) = d(x, y).$$

Hence $\varphi\colon X \to X_1$ is an isometry and $X$ is isometric to a subset of $\hat{X}$.

*Step 3.* ($X_1$ is dense in $\hat{X}$). We have to prove that $\hat{X} = \overline{X_1}$. Of course, it suffices to prove that $\hat{X} \subseteq \overline{X_1}$. Let $A = [(a_n)_{n\in\mathbb{N}}] \in \hat{X}$. We shall see that $A \in \overline{X_1}$ by constructing a sequence of elements in $X_1$ that converges to $A$.

For each $k \in \mathbb{N}$ take the constant sequence $(a_k)_{n\in\mathbb{N}}$ and the equivalence class $A_k = [(a_k)_{n\in\mathbb{N}}] \in X_1$. Our goal is to prove that $(A_k)_{k\in\mathbb{N}} \to A$, that is:

$$\forall \varepsilon > 0 \;\; \exists k_0 \in \mathbb{N} \text{ such that } \forall k \geq k_0, \;\; \hat{d}(A_k, A) = \lim_{n\to\infty} d(a_k, a_n) \leq \varepsilon$$

Set $\varepsilon > 0$. Since $(a_n)_{n\in\mathbb{N}}$ is Cauchy, there exists $k_0 \in \mathbb{N}$ such that for all $k, n \geq k_0$, $d(a_k, a_n) < \varepsilon$. Now, taking limits in the last inequality as $n$ goes

to infinity, it follows that $(A_k)_{k\in\mathbb{N}} \to A$, as we were required.

*Step 4.* ($\hat{X}$ is complete). Let $(A_n)_{n\in\mathbb{N}} \subseteq \hat{X}$ be a Cauchy sequence. Our goal is to show that it converges in $\hat{X}$. Now, for each $k \in \mathbb{N}$, since $A_k \in \hat{X} = \overline{X_1}$, we have that $B\left(A_k, \frac{1}{k}\right) \cap X_1 \neq \varnothing$. Pick $B_k \in B\left(A_k, \frac{1}{k}\right) \cap X_1$. Since $B_k \in X_1$, choose a constant representative:

$$B_k = [(b_k)_{n\in\mathbb{N}}].$$

Now we define a new element,

$$B = [(b_n)_{n\in\mathbb{N}}].$$

We will show that our initial sequence $(A_n)_{n\in\mathbb{N}}$ converges to $B$. We have to prove that the element $B \in \hat{X}$ is well-defined, i.e. that the sequence $(b_n)_{n\in\mathbb{N}}$ is Cauchy. Using the triangular inequality,

$$\begin{aligned} d(b_p, b_q) = \lim_{n\to\infty} d(b_p, b_q) = \hat{d}(B_p, B_q) &\leq \hat{d}(B_p, A_p) + \hat{d}(A_p, A_q) + \hat{d}(A_q, B_q) \\ &< \frac{1}{p} + \frac{1}{q} + \hat{d}(A_p, A_q). \end{aligned}$$

Now, since the sequence $(A_n)_{n\in\mathbb{N}}$ is Cauchy, it is clear that the expression above is arbitrarily small when $p$ and $q$ are big enough; thus the sequence $(b_n)_{n\in\mathbb{N}}$ is Cauchy.

Finally, we see that $(A_n)_{n\in\mathbb{N}} \to B$. Indeed, we have

$$\hat{d}(A_n, B) \leq \hat{d}(A_n, B_n) + \hat{d}(B_n, B) < \frac{1}{n} + \lim_{k\to\infty} d(b_n, b_k).$$

And since $(b_n)_{n\in\mathbb{N}}$ is Cauchy, it is clear that $\hat{d}(A_n, B)$ is arbitrarily small for $n$ big enough, that is, $(A_n)_{n\in\mathbb{N}} \to B$ and $(\hat{X}, \hat{d})$ is complete, as we wanted to prove.

*Step 5.* (Uniqueness). Assume that $(X', d')$ is another completion of $(X, d)$. Then there exists a subset of $X'$, say $X_2$, such that $X_2$ is isometric to $X$. Since being isometric is a equivalence relation, we conclude that $X_1$ and $X_2$ are isometric. Call $\psi$ the isometry between $X_1$ and $X_2$.

Now we may define an isometry between $\hat{X}$ and $X'$. To do so, let $A \in \hat{X}$. Since $X_1$ is dense, there exists a sequence $(A_k)_{k\in\mathbb{N}} \subseteq X_1$ such that $(A_k)_{k\in\mathbb{N}} \to A$. Now, since $(A_k)_{k\in\mathbb{N}}$ is convergent, it is Cauchy, and so the sequence of images $(\psi(A_k))_{k\in\mathbb{N}}$ is also Cauchy in $X_2$ (because $\psi$ is an isometry).

By completeness, $(\psi(A_k))_{k\in\mathbb{N}} \subseteq X'$ is also convergent. Let $A' \in X'$ be its limit. Then let

$$\begin{aligned}\Phi\colon \hat{X} &\to X'\\ A &\mapsto \Phi(A) = A'\end{aligned}$$

We claim that $\Phi$ is an isometry. We have to check that $\Phi$ is well-defined, in the sense of $A'$ being independent of the sequence $(A_k)_{k\in\mathbb{N}}$. Assume that we have two sequences $(A_k)_{k\in\mathbb{N}}$ and $(\tilde{A}_k)_{k\in\mathbb{N}}$ converging to $A$. Let $A' = \lim_{k\to\infty} \psi(A_k)$. Our goal is to see that $A' = \lim_{k\to\infty} \psi(\tilde{A}_k)$, and this follows from the triangle inequality:

$$\begin{aligned}\lim_{k\to\infty} d'(\psi(\tilde{A}_k), A') &\leq \lim_{k\to\infty} [d'(\psi(\tilde{A}_k), \psi(A_k)) + d'(\psi(A_k), A')]\\ &= \lim_{k\to\infty} d'(\psi(\tilde{A}_k), \psi(A_k)) = \lim_{k\to\infty} \hat{d}(A_k, \tilde{A}_k)\\ &\leq \lim_{k\to\infty} [\hat{d}(A_k, A) + \hat{d}(A, \tilde{A}_k)] = 0.\end{aligned}$$

To show that $\Phi$ is bijective, it suffices if we build an inverse. Of course, in the process of defining $\Phi$ we could have started from $(X', d')$ instead of $(\hat{X}, \hat{d})$, obtaining $\Psi$, which is $\Phi^{-1}$. Hence $\Phi$ is bijective.

Using Lemma 1.4.11, it is clear that distances are preserved:

$$\begin{aligned}d'(\Phi(A), \Phi(B)) = d'(A', B') &= d'\left(\lim_{k\to\infty} \psi(A_k), \lim_{k\to\infty} \psi(B_k)\right)\\ &= \lim_{k\to\infty} d'\left(\psi(A_k), \psi(B_k)\right) = \lim_{k\to\infty} \hat{d}(A_k, B_k)\\ &= \hat{d}\left(\lim_{k\to\infty} A_k, \lim_{k\to\infty} B_k\right) = \hat{d}(A, B).\end{aligned}$$

This shows that $\Phi$ is an isometry and hence the uniqueness is proved. □

**Examples 1.4.13.** (i) The field of rational numbers, $\mathbb{Q}$, is not complete with the usual metric. However, its completion is the field of real numbers $\mathbb{R}$.

(ii) Since $K[X]$ is an integral domain, we can define the $(X)$-adic metric on it. One of the motivations in order to define the power series ring $R[[X]]$ is that this ring is the completion of $R[X]$ with respect to the $(X)$-adic metric. However, this fact is going to be studied at length in Chapter 2.

# Chapter 2

# Power series rings

We all have the intuitive idea of what a power series in several variables with coefficients in a ring is. Let $X_1, \ldots, X_n$ be $n$ indeterminates and let $R$ be a ring. Then we denote by $R[[X_1, \ldots, X_n]]$ the power series ring over $R$, whose elements are described as formal sums of the form

$$a(X_1, \ldots, X_n) = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_1^{i_1} \ldots X_n^{i_n},$$

where each $i_1, \ldots, i_n$ is in $\mathbb{N} \cup \{0\}$ and $a_{i_1, \ldots, i_n}$ is in $R$.

The purpose of this chapter is to formalize this idea and present the main properties of that set which, as we will see, has got ring structure. In addition, we will also focus on the particular case when the ring $R$ is a field.

## 2.1 Power series ring

We start by giving the formal definition of the power series ring and seeing that it really has ring structure.

**Definition 2.1.1.** Let $X_1, \ldots, X_n$ be indeterminates. Then a *monomial* is a product of indeterminates of the type $X_1^{i_1} \ldots X_n^{i_n}$ where each $i_j \in \mathbb{N} \cup \{0\}$.

Notice that there is a bijection between the set of monomials and the set $(\mathbb{N} \cup \{0\})^n$, and so monomials can be interpreted as tuples of non-negative integers.

**Remark 2.1.2.** Naturally we assume that $X_i^0 = 1 \in R$, for any $i = 1 \ldots, n$.

**Definition 2.1.3.** Let $X_1, \ldots, X_n$ be $n$ indeterminates and let $R$ be a ring. Then a *power series* is a formal sum:

$$a(X_1, \ldots, X_n) = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_1^{i_1} \ldots X_n^{i_n},$$

where each $i_1, \ldots, i_n$ is in $\mathbb{N} \cup \{0\}$ and $a_{i_1, \ldots, i_n}$ is in $R$.

**Definition 2.1.4.** Let $a(X_1, \ldots, X_n)$ be a power series. Then the term $a_{0,\ldots,0}$ is the *constant term* of $a(X_1, \ldots, X_n)$.

**Remark 2.1.5.** Let $R$ be a ring. By definition two power series in $n$ indeterminates and over $R$ are the same element if and only if they have the same coefficients. That is,

$$\sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n} = \sum_{i_1,\ldots,i_n \geq 0} b_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}$$

if and only if

$$a_{i_1,\ldots,i_n} = b_{i_1,\ldots,i_n} \ \forall i_1, \ldots, i_n \in \mathbb{N} \cup \{0\}.$$

In particular, a power series $a = a(X_1, \ldots, X_n)$ is zero if and only if each coefficient of $a$ is zero. That is,

$$a = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n} = 0 \iff a_{i_1,\ldots,i_n} = 0 \ \forall i_j.$$

Moreover, $R[[X_1, \ldots, X_n]]$ is the collection of all power series in $n$ indeterminates and with coefficients in $R$ and it is called the *power series ring* over $R$ in the indeterminates $X_1, \ldots, X_n$. We have called it "ring", but has $R[[X_1, \ldots, X_n]]$ got ring structure? Of course it has.

Let $a = a(X_1, \ldots, X_n)$ and $b = b(X_1, \ldots, X_n)$ be two power series, it is easy to define the sum $a + b$ and the product $a \cdot b$ as follows.

- To add two power series we just add their coefficients;

$$(a + b)(X_1, \ldots, X_n) = \sum_{i_1,\ldots,i_n \geq 0} (a_{i_1,\ldots,i_n} + b_{i_1,\ldots,i_n}) X_1^{i_1} \ldots X_n^{i_n}.$$

- To multiply two power series we proceed as follows;

$$(a \cdot b)(X_1, \ldots, X_n) = \sum_{i_1,\ldots,i_n \geq 0} c_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n},$$

  where

$$c_{i_1,\ldots,i_n} = \sum_{\substack{j_1 + k_1 = i_1 \\ \ldots \\ j_n + k_n = i_n}} a_{j_1,\ldots,j_n} b_{k_1,\ldots,k_n}.$$

Once we have defined those two operations in $R[[X_1, \ldots, X_n]]$, we should prove that $(R[[X_1, \ldots, X_n]], +, \cdot)$ is a ring.

**Proposition 2.1.6.** *A power series ring $R[[X_1, \ldots, X_n]]$ in $n$ variables over $R$ is a ring with the two operations described as preceding.*

*Proof.* The proof is straightforward using that $R$ is a ring. Furthermore, since $R$ is a commutative ring, then $R[[X_1, \ldots, X_n]]$ is also commutative.

Finally the identity 1 is a power series. Indeed, 1 is a monomial with $i_1 = \cdots = i_n = 0$. Hence, $R[[X_1, \ldots, X_n]]$ is a commutative ring with identity. □

Since $R$ is a general ring we might not have a metric defined on it and so we can not speak about convergence of power series. However, the definition above is just a formal definition. Furthermore, notice that the power series are just infinite "linear combinations" of monomials with coefficients in $R$.

Moreover, evaluating a monomial in a tuple $(a_1, \ldots, a_n) \in R^n$ is just an map which maps $X_1^{i_1} \ldots X_n^{i_n} \cong (i_1, \ldots, i_n)$ into $a_1^{i_1} \ldots a_n^{i_n} \in R$.

Furthermore, what is evaluating a power series? That question may not have sense because firstly in order to speak about evaluations, i.e., convergence of infinite sums we should define a metric. Moreover, once we have a metric, to evaluate a power series at the tuple $(a_1, \ldots, a_n) \in R^n$ is making an infinite sum with the evaluated monomials. However, the preceding sum may not converge with respect to our metric, so in this case we can not talk about evaluating power series. When we have got a metric and the infinite sum of evaluated monomials converges with respect to that metric, we can speak about evaluating some power series.

Let $a(X_1, \ldots, X_n) \in R[[X_1, \ldots, X_n]]$ be a power series, then its *domain of convergence* is the subset of $R^n$ where the power series $a(X_1, \ldots, X_n)$ can be evaluated. Anyway, this is not the main objective of this dissertation.

Let us provide some examples of power series.

**Examples 2.1.7.** (i) Any polynomial in $R[X_1, \ldots, X_n]$ can be seen as a power series in $R[[X_1, \ldots, X_n]]$. Indeed, for a polynomial of total degree $d$ consider that $a_{i_1,\ldots,i_n} = 0$ when $i_1 + \cdots + i_n > d$. Hence, $R[X_1, \ldots, X_n]$ will be a subring of $R[[X_1, \ldots, X_n]]$.
(ii) The elements of $\mathbb{R}[[X]]$ and $\mathbb{C}[[X]]$ are power series in one indeterminate, which have been seen in real and complex analysis respectively.

## 2.2 Main properties of the power series ring

Let us see what the main properties of the ring of power series are or how the properties of the initial ring $R$ are inherited by the power series ring. In many of the proofs in this section we will proceed in the same way. First we will prove the property for a single indeterminate, and later we will

generalize it to the case of $n$ indeterminates. We start by describing the units of the power series ring.

**Lemma 2.2.1.** *Let $R$ be a ring and let $R[[X]]$ be a power series ring in one indeterminate. Then the units of $R[[X]]$ are exactly the power series whose constant term is a unit in $R$. That is,*

$$a(X) = \sum_{i=0}^{\infty} a_i X^i \in \mathcal{U}(R[[X]]) \iff a_0 \in \mathcal{U}(R).$$

*Proof.* $\Rightarrow$) Suppose that $a(X) \in R[[X]]$ is a unit, then there exists another power series $b(X) \in R[[X]]$ such that $a(X) \cdot b(X) = 1$. By comparing constant terms, we get $a_0 b_0 = 1$ and so $a_0$ is a unit in $R$.

$\Leftarrow$) Set $a = a(X_1, \ldots, X_n) = \sum_{i=0}^{\infty} a_i X^i \in R[[X]]$ such that $a_0 \in \mathcal{U}(R)$. We shall construct the inverse of $a$, say $b = \sum_{i=0}^{\infty} b_i X^i \in R[[X]]$.

Since $a_0$ is a unit in $R$ set $b_0 = a_0^{-1}$. Thus, if $a \cdot b = \sum_{i=0}^{\infty} c_i X^i$, then

$$c_0 = a_0 b_0 = a_0 a_0^{-1} = 1.$$

Moreover, define inductively

$$b_n = -a_0^{-1} \sum_{k=1}^{n} a_k b_{n-k} \quad \forall n \geq 1.$$

Then

$$\begin{aligned} c_n &= a_0 b_n + a_1 b_{n-1} + \cdots + a_n b_0 \\ &= -a_0 a_0^{-1}(a_1 b_{n-1} + \cdots + a_n b_0) + a_1 b_{n-1} + \cdots + a_n b_0 \\ &= -(a_1 b_{n-1} + \cdots + a_n b_0) + a_1 b_{n-1} + \cdots + a_n b_0 = 0 \quad \forall n \geq 1. \end{aligned}$$

Therefore, $a \cdot b = 1 + \sum_{i=1}^{\infty} 0 \cdot X^i = 1$ and so $b$ is the inverse of $a$. □

**Corollary 2.2.2.** *Let $R$ be a ring and let $R[[X_1, \ldots, X_n]]$ be a power series ring in $n$ indeterminates. Then the units of $R[[X_1, \ldots, X_n]]$ are the power series whose constant term is a unit in $R$.*

*Proof.* We proceed by induction on $n$. The case when $n = 1$ is proved in Lemma 2.2.1. Suppose that the statement is true for $n - 1$. Denote $R_{n-1} = R[[X_1, \ldots, X_{n-1}]]$ and consider

$$a = a(X_1, \ldots, X_n) \in R[[X_1, \ldots X_n]] \cong R[[X_1, \ldots, X_{n-1}]][[X_n]] = R_{n-1}[[X_n]].$$

Then

$$a = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_1^{i_1} \ldots X_n^{i_n} = \sum_{i=0}^{\infty} a_i(X_1, \ldots, X_{n-1}) X_n^i,$$

where $a_i(X_1, \ldots, X_{n-1}) \in R_{n-1}$ for all $i \geq 0$. Since the statement is true for the case $n = 1$, then

$$a \in \mathcal{U}(R_{n-1}[[X_n]]) \iff a_0(X_1, \ldots, X_{n-1}) \in \mathcal{U}(R_{n-1}).$$

Therefore, by induction hypothesis $a_0(X_1, \ldots, X_{n-1}) \in \mathcal{U}(R_{n-1})$ if and only if $a_{0,\ldots,0} \in \mathcal{U}(R)$. Thus, $a$ is a unit in $R[[X_1, \ldots, X_n]]$ if and only if $a_{0,\ldots,0}$ is a unit in $R$. □

We can continue with the property of being an integral domain

**Lemma 2.2.3.** *Let $R$ be a ring and let $R[[X]]$ be a power series ring in one indeterminate. Then $R[[X]]$ is an integral domain if and only if $R$ is an integral domain.*

*Proof.* $\Rightarrow$) Suppose that $R[[X]]$ is an integral domain. Thus $R \subseteq R[[X]]$ is a subring of an integral domain, so $R$ is an integral domain.
$\Leftarrow$) Suppose that $R$ is an integral domain and consider two power series $a(X)$, $b(X)$ which are not 0. Then call $a_i$ and $b_j$ to the smallest non-zero terms of $a(X)$ and $b(X)$ respectively. Then

$$a(X) \cdot b(X) = a_i b_j X^{i+j} + \sum_{k=i+j+1}^{\infty} c_k X^k.$$

Since $R$ is an integral domain then $a_i b_j \neq 0$. Hence, $a(X) \cdot b(X) \neq 0$. □

**Corollary 2.2.4.** *Let $R$ be a ring. Then $R[[X_1, \ldots, X_n]]$ is an integral domain if and only if $R$ is an integral domain.*

*Proof.* The *only if* implication is clear. For the *if* implication we proceed by induction on $n$. Lemma 2.2.3 proves the result for the case $n = 1$. Supposing that it holds for $n-1$, then $R_{n-1} = R[[X_1, \ldots, X_{n-1}]]$ is an integral domain. Therefore,

$$R[[X_1, \cdots, X_n]] \cong R[[X_1, \ldots, X_{n-1}]][[X_n]] = R_{n-1}[[X_n]]$$

is an integral domain, applying again Lemma 2.2.3. □

Being Noetherian is also inherited in a similar way.

**Definition 2.2.5.** Let $R$ be a ring and let $R[[X]]$ be a power series ring in one variable. Let

$$a(X) = \sum_{i=0}^{\infty} a_i X^i \in R[[X]]$$

be a non-zero power series. Then the *order* of $a$ is the lowest integer $i \in \mathbb{N}$ such that $a_i \neq 0$. Moreover, $a_i$ is called the *starting term* of $a(X)$.

Clearly all the non-zero power series in one variable have an order and it is unique. Clearly, for a power series of order $i$ then $a_j = 0$ for any $j < i$.

**Proposition 2.2.6.** *Let $R$ be a Noetherian ring. Then a power series ring $R[[X]]$ in one variable is also a Noetherian ring.*

*Proof.* This proof repeats the main ideas of the proof done by Hilbert for polynomials. We shall prove that any ideal of $R[[X]]$ can be generated by a finite number of elements. Let $\mathfrak{A}$ be an ideal of $R[[X]]$ and define the following sets

$$\mathfrak{a}_i = \{a_i \in R \mid a_i \text{ is the coefficient of } X^i \text{ for some } a \in \mathfrak{A} \text{ s.t. } a_j = 0 \ \forall j < i\}.$$

It is easy to verify that $\mathfrak{a}_i$ is an ideal of $R$ and $\mathfrak{a}_i \subseteq \mathfrak{a}_{i+1}$. Indeed, if $a \in \mathfrak{a}_i$, then there exists a power series

$$a(X) = aX^i + \sum_{j=i+1}^{\infty} a_j X^j \in \mathfrak{A}.$$

Thus, since $\mathfrak{A}$ is an ideal

$$Xa(X) = aX^{i+1} + \sum_{j=i+2}^{\infty} a_j X^j \in \mathfrak{A},$$

and by definition $a \in \mathfrak{a}_{i+1}$.

Since $R$ is Noetherian the following ascending chain of ideals of $R$ stops for some $n_0 \in \mathbb{N}$,

$$\mathfrak{a}_0 \subseteq \mathfrak{a}_1 \subseteq \cdots \subseteq \mathfrak{a}_{n_0-1} \subseteq \mathfrak{a}_{n_0} = \mathfrak{a}_{n_0+1} = \ldots$$

Furthermore, for each ideal $\mathfrak{a}_i$ there exists a finite generating set $G_i$ such that $\mathfrak{a}_i = (G_i)$. Then for each element $a_{ij}$ in $G_i$ we take one series, $g_{ij}$, whose minimum coefficient is $a_{ij}$. Then we consider the collection of those power series, call it $F_i$. Since $|F_i| = |G_i|$ both sets are finite. Now we define $F = \bigcup_{i=0}^{n_0} F_i$ which is still finite. We shall prove that $F$ generates $\mathfrak{A}$. For notation simplicity say $|F| = l$ and $F = \{g_1 \ldots, g_l\}$.

Given any non-zero series $f = f(X) \in \mathfrak{A}$ of order $d \leq n_0$ and starting term $a_d$, then $a_d \in \mathfrak{a}_d = (G_d)$ and so $a_d = c_1 s_1 + \cdots + c_m s_m$ for some $c_i \in R$ and for some $s_i \in G_d$. For each $i = 1, \ldots, m$ choose a $g_i \in F_d \subseteq F$ such that the starting term of $g_i$ is $s_i$. Then the order of

$$f - c_1 g_1 - \cdots - c_m g_m$$

is at least $d + 1$. That is, there exist some $c_i^{(d)} \in R$ such that the order of

$$f - c_1^{(d)} g_1 - \cdots - c_l^{(d)} g_l$$

is at least $d+1$. Then proceeding inductively for each $n = d+1, \ldots, n_0$ we can consider the combination

$$f - \sum_{j=d}^{n} c_1^{(j)} g_1 - \cdots - \sum_{j=d}^{n} c_l^{(j)} g_l,$$

which is zero or has order greater than $n+1$. Hence we can assume that $d > n_0$. Then $a_d \in \mathfrak{a}_d = \mathfrak{a}_{n_0} = (G_{n_0})$. Thus as before there exists a series $c_1^{(d)} g_1 + \cdots + c_l^{(d)} g_l$ of order $n_0$ and starting term $a_d$. Therefore, the order of

$$f - X^{d-n_0}(c_1^{(d)} g_1 + \cdots + c_l^{(d)} g_l)$$

is greater than $d+1$. Furthermore, let $f$ be a non-zero power series of order $d$. Then, for each $i = 1, \ldots, l$, using the preceding coefficients and proceeding by induction we define the power series

$$h_i(X) = \sum_{j=d}^{n_0} c_i^{(j)} + \sum_{j=n_0+1}^{\infty} c_i^{(j)} X^{j-n_0}. \tag{2.1}$$

Then using 2.1 $f$ can be expressed as combination of $g_1, \ldots, g_l$ as

$$f = h_1 g_1 + \cdots + h_l g_l.$$

Hence $\mathfrak{A}$ is finitely generated and $R[[X]]$ is Noetherian. □

**Corollary 2.2.7.** *Let $R$ be a Noetherian ring. Then a power series ring $R[[X_1, \ldots, X_n]]$ in $n$ indeterminates is also a Noetherian ring.*

*Proof.* Proposition 2.2.6 gives the result for $n = 1$. Then suppose inductively that the statement holds for $n-1$, so $R_{n-1} = R[[X_1, \ldots, X_{n-1}]]$ is a Noetherian ring. Thus, according to 2.2.6 $R[[X_1, \ldots, X_n]] \cong R_{n-1}[[X_n]]$ is also a Noetherian ring. □

When $R$ is Noetherian any ideal of the power series ring can be generated by a finite number of elements. However, stronger properties such as being a principal ideal domain or being a Euclidean domain are not inherited in the same way. Use the power series ring $\mathbb{Z}[[X]]$ as a counterexample. Although $\mathbb{Z}$ is a Euclidean domain (and therefore a PID) $\mathbb{Z}[[X]]$ is not a PID (and neither a ED). Indeed, the ideal $(2, X)$ can not be generated with less than two generators.

Suppose by contradiction that $(2, X)$ can be generated with a unique power series $c(X) \in \mathbb{Z}[[X]]$. Then there exist $a(X), b(X) \in \mathbb{Z}[[X]]$ such that $2 = a(X)c(X)$ and $X = b(X)c(X)$. Then considering the constant term of the first product:

$$a_0 c_0 = 2 \implies c_0 \neq 0,$$

and considering the two first coefficients of the power series $X$:

$$b_0c_0 = 0 \implies b_0 = 0,$$

$$b_0c_1 + b_1c_0 = b_1c_0 = 1 \implies c_0 \in \mathcal{U}(\mathbb{Z}) = \{\pm 1\}.$$

Furthermore, since $c_0 \in \mathcal{U}(\mathbb{Z})$ according to Lemma 2.2.1 the power series $c(X)$ is a unit in $\mathbb{Z}[[X]]$ and so $(2, X) = (c(X)) = \mathbb{Z}[[X]]$. Therefore, $1 \in (2, X)$. Then there exist two power series $d(X), e(X) \in \mathbb{Z}[[X]]$ such that

$$1 = 2d(X) + Xe(X) \implies 1 = 2d_0 + 0e_0 = 2d_0 \implies d_0 = 1/2.$$

However this is a contradiction, because $d_0$ must be an integer.

## 2.3 Power series over a field

Within power series rings, those defined over a field $K$ are particularly relevant. Although some of its properties do not differ in excess of those seen with whole generality, they do present interesting properties in terms of locality and completeness with respect to the $\mathfrak{a}$-adic topology, for a suitable ideal $\mathfrak{a}$. Let us first state the properties that do not vary.

**Lemma 2.3.1.** *Let $K$ be a field. Then the units of the power series ring $K[[X_1, \ldots, X_n]]$ are the power series with non-zero constant term.*

*Proof.* In any field $\mathcal{U}(K) = K \setminus \{0\}$. Then the result is immediate from Corollary 2.2.2. □

**Proposition 2.3.2.** *Let $K$ be a field. Then*

*(i) $K[[X_1, \ldots, X_n]]$ is an integral domain and*

*(ii) $K[[X_1, \ldots, X_n]]$ is a Noetherian ring.*

*Proof.* (i) Since any field is an integral domain, it is a straightforward consequence of Corollary 2.2.4.

(ii) Since any field is Noetherian, it is a straightforward consequence of Corollary 2.2.7.

□

Let us look at two interesting properties: locality and completeness.

**Proposition 2.3.3.** *Let $K$ be a field. Then $K[[X_1, \ldots, X_n]]$ is a local ring and its unique maximal ideal is $(X_1, \ldots, X_n)$.*

*Proof.* We have divided the proof into two steps. Say $R_n = K[[X_1, \ldots, X_n]]$ and $\mathfrak{m} = (X_1, \ldots, X_n)$.

First of all, we shall prove that $\mathfrak{m}$ is a maximal ideal of $R_n$. However, naturally the quotient $R_n/\mathfrak{m}$ is isomorphic to $K$, which is a field (See Exercise 2). Thus, $\mathfrak{m}$ is a maximal ideal.

Finally we shall see that $R_n \setminus \mathfrak{m} = \mathcal{U}(R)$, and hence $\mathfrak{m}$ is the unique maximal ideal of $R_n$. Since

$$(X_1, \ldots, X_n) = \{a \in R_n \mid a_{0,\ldots,0} \neq 0\}$$

the assertion follows. Indeed, any element of $R_n$ outside $\mathfrak{m}$ has non-zero constant term and so it is a unit according to Lemma 2.3.1. □

Notice that in the ring of polynomials this property is not true. That is, even when $K$ is field, $K[X]$ is not a local ring. Indeed, all the ideals of the form $(X - a)$ where $a \in K$ are maximal ideals.

Let us examine the completeness of the power series ring.

**Proposition 2.3.4.** *A power series ring $K[[X_1, \ldots, X_n]]$ in $n$ indeterminates and over a field $K$ is complete with the $(X_1, \ldots, X_n)$-adic topology.*

*Proof.* For notation simplicity denote $R_n = K[[X_1, \ldots, X_n]]$ and denote $\mathfrak{m} = (X_1, \ldots, X_n)$ its unique maximal ideal. Let $(a_k)_{k\in\mathbb{N}} \subseteq R_n$ be a Cauchy sequence, we shall prove that the sequence is convergent. We have divided the proof into two steps.

*Step 1* We will construct the possible limit $a \in R_n$. Since $(a_k)_{k\in\mathbb{N}}$ is a Cauchy sequence for each $k \in \mathbb{N}$ there exists an $N(k) \in \mathbb{N}$ such that, when $m \geq N(k)$ then

$$a_m - a_{N(k)} \in \mathfrak{m}^k, \tag{2.2}$$

which is equivalent to

$$d(a_m, a_{N(k)}) < 2^{-k+1}.$$

We can choose the numbers $N(k)$ so that

$$N(1) \leq N(2) \leq \cdots \leq N(k) \leq \ldots$$

Now for each $b \in R_n$ let $P_k(b)$ be the homegeneous polynomial part of $b$ with total degree $k$, that is, the sum of the monomials of $b$ such that their total degree is exactly $k$. Then we set

$$a = P_1(a_{N(1)}) + P_2(a_{N(2)}) + \cdots + P_k(a_{N(k)}) + \cdots \in R_n.$$

*Step 2.* We shall see that the sequence $(a_k)_{k\in\mathbb{N}}$ converges to $a$ in $R_n$. First of all notice that for any $m > 0$, $P_r(a_m - a) = P_r(a_m - a_{N(r)})$. Indeed,

$$P_r(a_m - a) = P_r(a_m) - P_r(a) = P_r(a_m) - P_r(a_{N(r)}) = P_r(a_m - a_{N(r)}).$$

Then for any $k \in \mathbb{N}$, there exists $k_0 = N(k) \in \mathbb{N}$ such that when $m \geq k_0$ then

$$P_r(a_m - a) = P_r(a_m - a_{N(r)}) = 0 \ \ \forall 1 \leq r < k,$$

by using 2.2. Therefore, $a_m - a \in \mathfrak{m}^k$ and so $d(a_m, a) < 2^{-k+1}$. Thus, $(a_k)_{k\in\mathbb{N}}$ converges to $a$ in $R_n$.

Therefore any Cauchy sequence is convergent in $R_n$, so $R_n$ is a complete space with the $\mathfrak{m}$-adic metric. □

**Lemma 2.3.5.** *Let $K$ be a field, let $d$ be the distance defined in a power series ring $K[[X_1, \ldots, X_n]]$ with respect to the $(X_1, \ldots, X_n)$-adic topology and let $\overline{d}$ be the distance defined in $K[X_1, \ldots, X_n]$ with respect to the $(X_1, \ldots, X_n)$-adic topology. Then for any $p, q \in K[X_1, \ldots, X_n]$ it follows $d(p, q) = \overline{d}(p, q)$.*

*Proof.* For notation simplicity from now on we denote: $T_n = K[X_1, \ldots, X_n]$, $R_n = K[[X_1, \ldots, X_n]]$, $\overline{\mathfrak{m}} = (X_1, \ldots, X_n)_{T_n}$ and $\mathfrak{m} = (X_1, \ldots, X_n)_{R_n}$.

On the one hand, since $\overline{\mathfrak{m}} \subseteq \mathfrak{m}$, then $\overline{\mathfrak{m}}^k \subseteq \mathfrak{m}^k$. Thus, if $\overline{d}(p, q) = 2^{-k}$, then $p - q \in \overline{\mathfrak{m}}^k \subseteq \mathfrak{m}^k$ and so $d(p, q) \leq 2^{-k} = \overline{d}(p, q)$.

On the other hand, suppose by contradiction that $d(p, q) < 2^{-k}$, then there exists a natural number $l \in \mathbb{N}$ such that $k < l$ and $p - q \in \mathfrak{m}^l$. That is,

$$p - q = \sum_i a_i m_i,$$

where $a_i \in R_n$ and each $m_i$ is a monomial of degree $l$ in the indeterminates $X_1, \ldots, X_n$. That is, $P_r(m_i) = 0$ for any $r \neq l$ and $m_i \in \overline{\mathfrak{m}}^l$ for any $i = 1, \ldots, n$. Since $p - q \in K[X_1, \ldots, X_n]$ is a polynomial of total degree say $m$, then $P_r(p - q) = 0$ for any $r > m$. Hence

$$\begin{aligned} p - q &= \sum_{r=0}^{m} \sum_i P_r(a_i m_i) + \sum_{r>m} \sum_i P_r(a_i m_i) \\ &= \sum_{r=0}^{m} \sum_i P_r(a_i m_i) = \sum_{r=0}^{m-l} \sum_i P_r(a_i) m_i. \end{aligned}$$

Since $P_r(a_i) \in K[X_1, \ldots, X_n]$ and $m_i \in \overline{\mathfrak{m}}^l$, then $p - q \in \overline{\mathfrak{m}}^l$. Therefore, $\overline{d}(p, q) \leq 2^{-l} < 2^{-k}$, which is a contradiction with the initial assumption. Hence, $d(p, q) = 2^{-k} = \overline{d}(p, q)$. □

**Proposition 2.3.6.** *Let $K$ be a field. The completion of $K[X_1, \ldots, X_n]$ with respect to the $(X_1, \ldots, X_n)$-adic topology is $K[[X_1, \ldots, X_n]]$.*

*Proof.* For notation simplicity we denote as before: $T_n = K[X_1, \ldots, X_n]$, $R_n = K[[X_1, \ldots, X_n]]$, $\overline{\mathfrak{m}} = (X_1, \ldots, X_n)_{T_n}$ and $\mathfrak{m} = (X_1, \ldots, X_n)_{R_n}$. The proof is completed by showing the properties which characterize the completion:

1) The ring $K[[X_1, \ldots, X_n]]$ is complete with respect to the $\mathfrak{m}$-adic topology, as we have seen in Proposition 2.3.4.

2) There exists the inclusion map $\iota\colon K[X_1, \ldots, X_n] \to K[[X_1, \ldots, X_n]]$ where according to Lemma 2.3.5 $\overline{d}(p, q) = d(p, q)$ for any $p, q \in T_n$, ($\overline{d}$ is the distance associated to the $\overline{\mathfrak{m}}$-adic topology and $d$ is the distance associated to the $\mathfrak{m}$-adic topology).

3) The ring $\iota(K[X_1, \ldots, X_n]) = K[X_1, \ldots, X_n]$ is dense in the power series ring $K[[X_1, \ldots, X_n]]$. Let $a \in R_n$, then for any $k \in \mathbb{N}$ there exists a $p \in K[X_1, \ldots X_n]$ such that $d(a, p) < 2^{-k}$. Indeed, for a fixed $k \in \mathbb{N}$ consider the polynomial

$$p = P_1(a) + \cdots + P_k(a) \in K[X_1, \ldots, X_n].$$

Then $P_r(a - p) = P_r(a) - P_r(p) = 0 \ \ \forall 1 \leq r \leq k$, and so $a - p \in \mathfrak{m}^{k+1}$. Thus, $d(a, p) \leq 2^{-(k+1)} < 2^{-k}$. Therefore $T_n$ is dense in $R_n$. □

An essential property of power series rings over a field is how easy it is to define homomorphisms between the power series ring and any $K$-algebra, just by giving the image of each indeterminate. We start by proving a technical lemma.

**Lemma 2.3.7.** *Let $A$ and $B$ be two $K$-algebras, let $\varphi\colon A \to B$ be a continuous $K$-algebra homomorphism and let $\sum_{k=0}^{\infty} a_k$ be a convergent series. Suppose that $\sum_{k=0}^{\infty} \varphi(a_k)$ is a convergent series. Then*

$$\varphi\left(\sum_{k=0}^{\infty} a_k\right) = \sum_{k=0}^{\infty} \varphi(a_k).$$

**Remark 2.3.8.** In the above lemma the series convergence and the continuity of $\varphi$ are considered with respect to the $\mathfrak{a}$-adic topology in $A$ and with respect to the $\mathfrak{b}$-adic topology in $B$, for two ideals $\mathfrak{a}$ of $A$ and $\mathfrak{b}$ of $B$ which satisfy Krull's intersection theorem.

*Proof.* Let $S_n$ be the $n$th partial sum of the series $\sum_{k=0}^{\infty} a_k$. Since $\varphi$ is linear, then

$$\varphi(S_n) = \varphi\left(\sum_{k=0}^{n} a_k\right) = \sum_{k=0}^{n} \varphi(a_k).$$

Moroever, since the second series is convergent in the space $(B, d)$ then

$$\forall \varepsilon > 0 \ \exists n_0 \in \mathbb{N} \text{ s.t. when } n \geq n_0 \text{ then } d\left(\sum_{k=0}^{n} \varphi(a_k), \sum_{k=0}^{\infty} \varphi(a_k)\right) < \varepsilon.$$

Hence, for any $n \geq n_0$ by the triangle inequality

$$\begin{aligned} d\left(\varphi(S_n), \sum_{k=0}^{\infty} \varphi(a_k)\right) &\leq d\left(\varphi(S_n), \sum_{k=0}^{n} \varphi(a_k)\right) + d\left(\sum_{k=0}^{n} \varphi(a_k), \sum_{k=0}^{\infty} \varphi(a_k)\right) \\ &\leq 0 + d\left(\sum_{k=0}^{n} \varphi(a_k), \sum_{k=0}^{\infty} \varphi(a_k\right) < \varepsilon. \end{aligned}$$

Therefore, $\lim_{n\to\infty} \varphi(S_n) = \sum_{k=0}^{\infty} \varphi(a_k)$. Finally since $\varphi$ is continuous we have that

$$\sum_{k=0}^{\infty} \varphi(a_k) = \lim_{n\to\infty} \varphi(S_n) = \varphi\left(\lim_{n\to\infty} S_n\right) = \varphi\left(\sum_{k=0}^{\infty} a_k\right).$$

□

**Proposition 2.3.9.** *Let $K$ be field. Then $K[[X_1, \ldots, X_n]]$ is a $K$-algebra.*

*Proof.* It is straightforward from the definition of $K$-algebra. □

**Proposition 2.3.10** (Universal property of power series algebras)**.** *Let $K$ be a field and let $B$ be a $K$-algebra, which is complete with the $\mathfrak{b}$-adic topology, for some ideal $\mathfrak{b}$ of $B$ that satisfies the Krull's intersection theorem. Then if we choose $b_1, \ldots, b_n \in \mathfrak{b}$, there exists a unique continuous $K$-algebra homomorphism $\varphi\colon K[[X_1, \ldots, X_n]] \to B$, such that $\varphi(X_i) = b_i$ for any $i = 1, \ldots, n$.*

*In particular, this is the image of a general power series by the homomorphism $\varphi$:*

$$\sum_{i_1,\ldots,i_n \geq 0} \lambda_{i_0,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n} \mapsto^{\varphi} \sum_{i_1,\ldots,i_n \geq 0} \lambda_{i_0,\ldots,i_n} b_1^{i_1} \ldots b_n^{i_n},$$

*that is, in order to obtain the image it is enough to substitute $b_i$ for each indeterminate $X_i$. We say that the map $\varphi$ is an* evaluation homomorphism*.*

*Proof.* First of all we shall see that $\varphi$ is well-defined. On the one hand, since the representation of one series $a = a(X_1, \ldots, X_n)$ in $K[[X_1, \ldots, X_n]]$ is unique, there is no doubt what the image of $a$ by $\varphi$ is. On the other hand, since $B$ is complete with the $\mathfrak{b}$-adic topology, then the image of one series is convergent in $B$ with respect to the $\mathfrak{b}$-adic topology.

Indeed, when $i_1 + \cdots + i_n = m$, then $\lambda_{i_0,\ldots,i_n} b_1^{i_i} \ldots b_n^{i_n} \in \mathfrak{b}^m$. Thus, using Krull's intersection theorem

$$\lim_{n\to\infty} \lambda_{i_0,\ldots,i_n} b_1^{i_i} \ldots b_n^{i_n} = 0.$$

Finally according Lemma 1.4.8, since the $\mathfrak{b}$-adic topology is complete, then the series is convergent.

Secondly, it is easy to verify that $\varphi$ is a $K$-algebra homomorphism and that $\varphi(X_i) = b_i$ for each $i = 1, \ldots, n$.

In order to prove the uniqueness, consider another continuous homomorphism $\psi\colon K[[X_1, \ldots, X_n]] \to B$ such that $\psi(X_i) = b_i$ for any $i = 1, \ldots, n$. Thus, since $\psi$ is a $K$-algebra homomorphism map and and a continuous map, then by Lemma 2.3.7

$$\begin{aligned}
\psi\left(\sum_{i_1,\ldots,i_n\geq 0} \lambda_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}\right) &= \sum_{i_1,\ldots,i_n\geq 0} \psi(\lambda_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}) \\
&= \sum_{i_1,\ldots,i_n\geq 0} \lambda_{i_1,\ldots,i_n} \psi(X_1)^{i_1} \ldots \psi(X_n)^{i_n} \\
&= \sum_{i_1,\ldots,i_n\geq 0} \lambda_{i_1,\ldots,i_n} b_1^{i_1} \ldots b_n^{i_n} \\
&= \varphi\left(\sum_{i_1,\ldots,i_n\geq 0} \lambda_{i_1,\ldots,i_n} X_1^{i_1} \ldots X_n^{i_n}\right).
\end{aligned}$$

Therefore, it follows that $\varphi = \psi$. □

## 2.4 Factorization in power series rings

The goal of this section is to show that the power series ring $K[[X_1, \ldots, X_n]]$ in $n$ variables and over a field $K$ is a unique factorization domain. The polynomial case is derived from the more general theorem that if $R$ is a UFD then so is the polynomial ring in one variable $R[X]$. Unfortunately, the analogous statement for power series is false (i.e. there are UFD's $R$ such that $R[[X]]$ is not a UFD). However to prove even the simplest example requires hard work. Let $R$ be the localization of $K[X, Y, Z]/(X^2 + Y^3 + Z^7)$ with respect to the ideal $(\overline{X}, \overline{Y}, \overline{Z})$. This ring $R$ is a UFD, but $R[[X]]$ is not a UFD.*

By simplicity during this section we will denote $R_n = K[[X_1, \ldots, X_n]]$. We will proceed by induction over $n$. Assuming that $R_{n-1}$ is a UFD, the

*It can be read in [2].

polynomial ring $R_{n-1}[X_n]$ is a UFD and our strategy will consist on relating the structure of $R_{n-1}[X_n]$ with the structure of $R_{n-1}[[X_n]]$, and derive that $R_n$ is a UFD. But we should prove two preliminary theorems in order to achieve our goal.

**Theorem 2.4.1** (Weierstrass division theorem)**.** *Let $K$ be a field, let $R_n$ be a power series ring and let $\mathfrak{m} = (X_1, \ldots, X_{n-1})$ be the unique maximal ideal of $R_{n-1}$. Suppose that $f \in R_n$ is of the form $f = uX_n^s - w$ where $s \geq 0$ is an integer, $u$ is a unit in $R_n$ and $w \in \mathfrak{m}[X_n]$ is a polynomial in $X_n$ such that $\deg w < s$. Then for any $g \in R_n$ there exist a unique $h \in R_n$ and a unique $r \in R_{n-1}[X_n]$ such that $r$ is a polynomial in $X_n$ of degree strictly less than $s$ and $g = hf + r$.*

*Proof.* Note that for any $g \in R_n$, it can be written in a unique way as $g = \alpha(g)X_n^s + \beta(g)$, where $\beta(g) \in R_{n-1}[X_n]$ is a polynomial in $X_n$ of degree strictly less than $s$. Both $\alpha$ and $\beta$ are $K$-linear functions and thus we define the operator

$$T\colon R_n \to R_n \text{ such that } T(g) = \alpha(g)u^{-1}f + \beta(g).$$

Clearly, since it is a linear combination of $K$-linear maps, then $T$ is also a $K$-linear map. We shall see that it is an isomorphism by finding its inverse. The idea is to give sense to the usual formal identity

$$T^{-1} = (I - (I - T))^{-1} = \sum_{i=0}^{\infty}(I - T)^i.$$

Firstly, we define the $K$-linear map $S$ such that

$$\begin{aligned} S(g) = g - T(g) &= \alpha(g)X_n^s + \beta(g) - \alpha(g)u^{-1}f - \beta(g) \\ &= \alpha(g)(X_n^s - u^{-1}f) = \alpha(g)u^{-1}w. \end{aligned}$$

Thus, for any $g \in R_n$ and for any $j \in \mathbb{N}$, then $S^j(g) \subseteq \mathfrak{m}^j[[X_n]]$. Indeed, it can be proved by induction over $j$. The case $j = 1$ is clear, since $w \in \mathfrak{m}[[X_n]]$ and $\mathfrak{m}$ is an ideal, then $S(g) = \alpha(g)u^{-1}w \in \mathfrak{m}[[X_n]]$. Furthermore, if $g \in \mathfrak{m}^k[[X_n]]$, then clearly $\alpha(g) \in \mathfrak{m}^k[[X_n]]$, so $S(g) = \alpha(g)u^{-1}w \in \mathfrak{m}^{k+1}[[X_n]]$ (because $\mathfrak{m}$ is an ideal and $w \in \mathfrak{m}[[X_n]]$). Then suppose that the statement holds for $j-1$, i.e., $S^{j-1}(g) \in \mathfrak{m}^{j-1}[[X_n]]$, then by the above argument

$$S^j(g) = S(S^{j-1}(g)) \in \mathfrak{m}^{j-1+1}[[X_n]] = \mathfrak{m}^j[[X_n]].$$

On the other hand, let $h_i \in R_n$ be a sequence such that $h_i \in \mathfrak{m}^i[[X_n]]$, then the power series $\sum_{i=0}^{\infty} h_i$ is a well defined element of $R_n$. Indeed, since only monomials of degree more or equal than $i$ can appear in each $h_i$, then each monomial in the $X_1, \ldots, X_n$ can appear only a finite number of times

in the previous sum. Thus, for any $g \in R_n$ the series $\sum_{j=0}^{\infty} S^j(g)$ is well defined and it is now straightforward to verify that $T^{-1} = \sum_{j=0}^{\infty} S^j$. Indeed,

$$(I - S) \circ (I + S + S^2 + \dots) = I + S - S + S^2 - S^2 + \cdots = I.$$

In a similar way $(I + S + \dots) \circ (I - S) = I$, so $(I - S)^{-1} = \sum_{i=0}^{\infty} S^i$. Thus,

$$T^{-1} = (I - (I - T))^{-1} = (I - S)^{-1} = \sum_{i=0}^{\infty} S^i$$

Hence, by finding the inverse of $T$ we have proved that $T$ is an isomorphism.

Finally, since $T$ is an isomorphism in particular it is surjective. Thus, there exists $l \in R_n$ such that $g = T(l) = \alpha(l)u^{-1}f + \beta(l)$. Now, we can define $h = \alpha(l)u^{-1} \in R_n$ and $r = \beta(l) \in R_{n-1}[X_n]$, such that $g = hf + r$ and $r = \beta(l)$ has degree in $X_n$ strictly lower than $s$. Moreover, the uniqueness of $h$ and $r$ follows from the fact that $T$ is an isomorphism and so $l$ is unique. □

**Definition 2.4.2.** Let $K$ be a field and let $f \in R_n$ be a power series. Then if $f$ satisfies the assumptions of the preceding theorem, $f$ is said to be a *regular power series* of order $s$ at $X_n$. That is, $f$ can be written as $f = uX_n^s - w$, where $u \in \mathcal{U}(R_n)$ and $w \in \mathfrak{m}[X_n]$ such that $r$ has degree strictly smaller than $s$.

The assumption of $f$ is regular at $X_n$ is not very restrictive. If $K$ is a field then any $f$ becomes regular after a suitable change of variables (See Exercise 3). That is, there exists an automorphism of $R_n$ such that the image of $f$ is regular. But be careful, we can assume that one power series $f$ is regular, not that any power series $f$ in $R_n$ is regular.

Another equivalent condition says that $f$ is regular of order $s$ at $X_n$ if and only if $f(0, \dots, 0, X_n)$ is a non-zero power series in $X_n$ and $X_n^s$ is the lowest power of $X_n$ which appears in $f(0, \dots, 0, X_n)$ with non-zero coefficient. From this characterization it follows that when $f = gh$ is regular, then both $g$ and $h$ are regular at $X_n$ as well, but with smaller order. Indeed, after the evaluation both of them are non-zero power series in $X_n$, because otherwise their product would be zero.

Before formulating our next auxiliary result, we need one more definition.

**Definition 2.4.3.** A polynomial in $R_{n-1}[X_n]$ is called a *Weierstrass polynomial* of degree $s$ if it is a monic polynomial of degree $s$ and all its coefficientes (except the leading one) are in $(X_1, \dots, X_{n-1})$.

**Lemma 2.4.4.** *Let $f \in R_{n-1}[X_n]$ be a Weierstrass polynomial. Then $f$ is a unit in $R_n$ if and only if it has degree* 0.

*Proof.* $\Rightarrow$) Suppose that $f$ is a Weierstrass polynomial of degree $s > 0$. Then $f(0,\dots,0) = 0^s = 0$ and so its constant term is zero. Hence $f$ is not a unit. $\Leftarrow$) Suppose that $f$ has degree zero. Then $f(0,\dots,0,X_n) = X_n^0 = 1$. In particular, the constant term of $f$ is 1, and so $f$ is a unit in $R_n$. □

Notice that the product of two Weierstrass polynomials is a Weierstrass polynomial as well.

**Theorem 2.4.5** (Weierstrass preparation theorem)**.** *Let $f \in R_n$ be regular of order $s$ at $X_n$. Then there exists a unique Weierstrass polynomial of degree $s$, say $p$, such that $f = vp$ for some unit $v \in R_{n-1}$.*

*Proof.* This result is a direct consequence of Weierstrass division theorem. According to that theorem there exist a unique $h \in R_n$ and a unique $r \in R_{n-1}[X_n]$ of degree strictly less than $s$, such that $X_n^s = hf + r$. We shall prove that $h$ is a unit and that $r \in \mathfrak{m}[X_n]$. Since $f$ is regular of order $s$, $f = uX_n^s - w$ where $w \in \mathfrak{m}[X_n]$, and so $w(0,\dots,0,X_n) = 0$. Therefore, evaluating the series at $(0,\dots,0,X_n)$,

$$\begin{aligned} X_n^s &= h(0,\dots,0,X_n)f(0,\dots,0,X_n) + r(0,\dots,0,X_n) \\ &= h(0,\dots,X_n)u(0,\dots,X_n)X_n^s - h(0,\dots,X_n)w(0,\dots,X_n) + r(0,\dots,X_n) \\ &= h(0,\dots,0,X_n)u(0,\dots,0,X_n)X_n^s + r(0,\dots,0,X_n). \end{aligned}$$

Therefore, $r(0,\dots,0,X_n) = 0$ and so all the coefficients of $r$ are in $\mathfrak{m}$. Moreover, $h(0,\dots,0,X_n)u(0,\dots,0,X_n) = 1$, then $h(0,\dots,0,X_n)$ is a unit. Thus, by Lemma 2.3.1 the constant term of $h(0,\dots,0,X_n) \in K[[X_n]]$ is not zero, so the constant term of $h$ (which is the same as before) is not zero and so $h$ is a unit.

Now define $p = X_n^s - r$, which clearly is a Weierstrass polynomial and $v = h^{-1}$ which is a unit. Then

$$X_n^s = hf + r \implies f = h^{-1}(X_n^s - r) = vp,$$

and the uniqueness of $v$ and $p$ follows from the uniqueness of $h$ and $r$. □

Now note that any Weierstrass polynomial of degree $s$ is regular at $X_n$ of order $s$. Indeed, that polynomial is of the form $1 \cdot X_n^s - w$ for some $w \in \mathfrak{m}[X_n]$ with degree stricly less than $s$.

**Corollary 2.4.6.** *Let $f, g \in R_n$ be Weierstrass polynomials. Suppose that $f = gh$ for some $h \in R_n$. Then $h$ is a Weierstrass polynomial.*

*Proof.* Since $f$ is regular at $X_n$ so it is $h$. Thus, by the Weierstrass preparation theorem $h = uq$ for some Weierstrass polynomial $q$ and a unit $u$. Since the product of Weierstrass polynomials is another Weierstrass polynomial

$gq$ is a Weierstrass polynomial of degree $m$. We shall see that $m = s$, where $s = \deg f$. Firstly, $f = ugq$ and evaluating it in the tuple $(0, \ldots, 0, X_n)$

$$f(0, \ldots, 0, X_n) = u(0, \ldots, 0, X_n)(gq)(0, \ldots, 0, X_n),$$

i.e.,

$$X_n^s = (a_0 + \sum_{i=1}^{\infty} a_i X_n^i) X_n^m = \sum_{i=0}^{\infty} a_i X_n^{i+m},$$

where $a_0 \neq 0$. By the uniqueness of the coefficients of a power series it follows that $a_i \neq 0$ if and only if $i + m = s$. In particular, $a_0 \neq 0$ and so $m = s$.

Then we have $1f = f = u(gq)$ (i.e. two decompositions of $f$ as a product of a unit and a Weierstrass polynomial with its same degree). The uniqueness of the Weierstrass preparation theorem implies that $u = 1$, and so $h = q$ is a Weierstrass polynomial. □

**Corollary 2.4.7.** *Let $f$ be a Weierstrass polynomial of degree $s$. Suppose that $f = gh$ for some $g, h \in R_{n-1}[X_n]$. Then there is an invertible element $u \in R_n$ such that both $ug$ and $u^{-1}h$ are Weierstrass polynomials.*

*Proof.* Since $f$ is a Weierstrass polynomial it is a regular power series at $X_n$. Then both $g$ and $f$ are regular at $X_n$. Thus, by Theorem 2.4.5 there exist a unit $u$ and a Weierstras polynomial $p$, such that $h = up$. Hence, $u^{-1}h = p$ is a Weierstrass polynomial. Furthermore, since $f = (ug)(u^{-1}h) = gh$ and $u^{-1}h$ are both Weierstrass polynomials, according to Corollary 2.4.6 $ug$ is a Weierstrass polynomial. □

**Lemma 2.4.8.** *A Weierstrass polynomial $f$ of degree $s > 0$ is irreducible in $R_n$ if and only if it is irreducible in $R_{n-1}[X_n]$. Furthermore, every Weierstrass polynomial degree $s > 0$ is a product of irreducible Weierstrass polynomials.*

*Proof.* Since $\deg f > 0$, then $f \neq 0$. Moreover, $f$ is not a unit in $R_{n-1}[X_n]$ and neither in $R_n$.

$\Leftarrow$) Suppose by contradiction that $f$ is reducible over $R_n$. Consequently, $f = gh$ in $R_n$ being both $g$ and $h$ non-units. Then by Corollary 2.4.7 there exists a unit $u \in R_n$ such that $f = (ug)(u^{-1}h)$ being both $ug$ and $u^{-1}h$ Weierstrass polynomials, whose degree is the order of $g$ and $h$ respectively. Since $g$ and $h$ are not units, then the degree of $p$ and $q$ is strictly greater than zero, so they are not units is $R_{n-1}[X_n]$. Thus, $f$ is reducible over $R_{n-1}[X_n]$, which is a contradiction.

$\Rightarrow$) Suppose by contradiction that $f = gh$ is reducible over $R_{n-1}[X_n]$. Since $f$ is monic the leading coefficients of $g$ and $h$ are invertible, so we can

assume that those polynomials are monic polynomials of degree $i$ and $s-i$ respectively. Since $f$ is a monic polynomials of degree $s$, then

$$X_n^s = f(0,\dots,0,X_n) = g(0,\dots,0,X_n)h(0,\dots,0,X_n).$$

Since $g$ and $h$ are monic polynomials of degree $i$ and $s-i$, then we have that $g(0,\dots,0,X_n) = X^i$ and $h(0,\dots,0,X_n) = X^{s-i}$. Then both $g$ and $h$ are monic polynomials, such that all their coefficients (except the leading one) are in $\mathfrak{m}$, so by definition both are Weierstrass polynomials. Moreover, neither of them is a unit in $R_n$. Indeed, neither of them is a unit in $R_{n-1}[X_n]$, so they are not Weierstrass polynomials of degree 0. Thus, $f$ is reducible in $R_n$, which is a contradiction.

This implication shows also the fact that any Weierstrass polynomial, which is not a unit in $R_n$, can be factorized into irreducible Weierstrass polynomials. Suppose by contradiction that there exists a Weierstrass polynomial $f$ which is not factorized as product of irreducible Weierstrass polynomials, moreover suppose without loss of generality that $f$ is the Weierstrass polynomial of lowest degree with that property. In particular, $f$ is not irreducible over $R_n$, because otherwise it would be a product of irreducible Weierstrass polynomials with one factor.

Thus, $f$ is reducible over $R_{n-1}[X_n]$, and so there exist two Weierstrass polynomials of lower degree, which are not units, such that $f = gh$. Since $g$ and $h$ have lower degree than $f$ they can be written as product of irreducible Weierstrass polynomials as follows: $g = \prod_{i=1}^{t} g_i$ and $h = \prod_{i=1}^{s} h_i$. Hence, $f$ is also a product of irreducible Weierstrass polynomials

$$f = gh = \prod_{i=1}^{t} g_i \prod_{i=1}^{s} h_i,$$

which is a contradiction. □

Now we can state and prove our main goal. As we have said before being a regular power series is not a hard condition. Indeed, fixed a series $f$, there exists (See Exercise 3) an isomorphism $\varphi\colon R_n \to R_n$ such that $\varphi(f)$ is regular of some order at $X_n$. Since the decomposition as product of irreducibles, being prime and being irreducible remain invariant by isomorphism, during the following proof we can suppose without loss of generality the regularity of certain power series.

**Theorem 2.4.9.** *Let $K$ be field. Then the power series ring in $n$ indeterminates $R_n = K[[X_1,\dots,X_n]]$ is a unique factorization domain.*

*Proof.* We proceed by induction over $n$. When $n = 0$, then $K$ is a field, so it is a UFD. Suppose inductively that $R_{n-1}$ is a UFD. Then so it is the polynomial ring $R_{n-1}[X_n]$. In order to show that $R_n$ is a UFD, we shall prove

that any non-zero and non-unit element factors as product of irreducible elements; and that each irreducible element is prime.

On the one hand, if $f$ is an arbitrary series, we may assume that $f$ is regular. Since $f$ is not zero or a unit, then it is regular at some order $s > 0$. By the Weierstrass preparation theorem $f = up$ where $u$ is a unit and $p$ is a Weierstrass polynomial of order $s > 0$. According to Lemma 2.4.8 $p$ factors as a product of irreducible Weierstrass polynomials. Moreover, each of those polynomials is irreducible in $R_n$, so we get a factorization of $f$ into irreducible elements.

On the other hand, let $f$ be an irreducible power series and suppose that $f|gh$. First, we can assume that $f$ is regular, so both $g$ and $h$ are regular power series. Then by the Weierstrass preparation theorem there exist some units $u, v, w \in R_n$ and some Weierstrass polynomials $p, q, r \in R_{n-1}[X_n]$ such that $f = up$, $g = vq$ and $h = wr$. Since $f$ is irreducible in $R_n$, $p$ is irreducible in $R_n$ and so it is irreducible in $R_{n-1}[X_n]$ (by Lemma 2.4.8). Moreover, since $f|gh$ and the divisibility does not depend on units, then $p|qr$. Now, since $p$ is irreducible in $R_{n-1}[X_n]$, which is a UFD, then $p$ is prime. Thus, there are two options $p|q$ and so $f|g$ or in the other case $p|r$ and so $f|h$. In any case, $f$ is prime. Hence, any irreducible element is a prime element. □

# Chapter 3

# Regular rings

The last property that remains to be analyzed, and which plays a fundamental role in this theory, is regularity. The aim of this chapter is to define regularity and present the results and basic features that have to do with it.

However, before explaining this concept, talking about the dimension of a ring is needed. This idea is strictly linked to the set of prime ideals of a ring and to the number of inclusions that can be done with them.

## 3.1 Dimension theory

### 3.1.1 Main definitions

**Definition 3.1.1.** Let $\mathfrak{a}$ be a proper ideal of the ring $R$. A *minimal prime ideal of* $\mathfrak{a}$ is an ideal $\mathfrak{p}$ which is minimal among the ideals containing $\mathfrak{a}$. That is, for any prime ideal $\mathfrak{q}$ of $R$,

$$\mathfrak{a} \subseteq \mathfrak{q} \subseteq \mathfrak{p} \implies \mathfrak{q} = \mathfrak{p}.$$

It can be seen, as a consequence of the uniqueness of the primary decomposition of ideals, that any proper ideal has only finitely many minimal prime ideals. Although this fact is not proved here, it can read in [8].

**Definition 3.1.2.** Let $\mathfrak{a}$ be a proper ideal of the ring $R$. Then, $\mathfrak{a}$ is a *minimal prime ideal* if it is a minimal prime ideal of the ideal $\{0\}$.

**Definition 3.1.3.** Let $R$ be a non-trivial ring, a *chain of prime ideals* of $R$ is chain of ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n,$$

in which $\mathfrak{p}_0, \mathfrak{p}_1, \ldots, \mathfrak{p}_n$ are prime ideals of $R$.

Consider a chain of prime ideals, the *length* of the chain is the number of inclusions in it, that is, one less than the number of prime ideals present.

We say that the chain is *saturated* when we can not introduce any prime ideals between the given ideals, that is, we can not find a chain of prime ideals with longer length but containing all the initial ideals.

**Definition 3.1.4.** Let $R$ be a non-trivial ring. The *dimension* of $R$, $\dim R$, is the number

$$\sup\{n \mid \text{ there exists a chain of prime ideals of } R \text{ of length } n\}.$$

**Examples 3.1.5.**

(i) If $R$ is an integral domain $\{0\}$ will be a prime ideal, so it is contained in any saturated chain of prime ideals. Therefore, if $\dim R = 0$ then $\{0\}$ is the unique prime ideal of $R$, so $\{0\}$ is a maximal ideal and so $R$ is a field. Conversely, if $R$ is a field its unique prime ideal is $\{0\}$ and so $\dim R = 0$. Hence we have a characterization for fields: an integral domain $R$ is a field if and only if $\dim R = 0$.

(ii) If $K$ is a field $K[[X_1, \ldots, X_n]]$ has dimension $n$. (See Exercise 5.)

(iii) Let us compute the dimension of $\mathbb{Z}$. On the one hand, $\{0\} \subsetneq (2)$ is a saturated chain of prime ideals. Thus, $\dim \mathbb{Z} \geq 1$.
On the other hand, in $\mathbb{Z}$ any non-zero prime ideal is maximal. Thus, there is not any chain of prime ideals of length 2, because the middle term of such a chain (which can not be the zero ideal) would be prime but not maximal, which is impossible. Hence, $\dim \mathbb{Z} = 1$.

(iv) In the same way as above, if $R$ is a PID which is not a field, then $\dim R = 1$.

(v) If $S \subseteq R$ is an integral ring extension, then $\dim S = \dim R$ (see Exercise 6). In particular, for any square-free integer $d$ the extension $\mathbb{Z} \subseteq \mathbb{Z}[\sqrt{d}]$ is integral, so the rings $\mathbb{Z}[\sqrt{d}]$ have dimension one.

By definition the dimension of a ring is related to its prime ideals. Moreover, the following concept will be useful in order to measure the size of a prime ideal.

**Definition 3.1.6.** Let $R$ be a non-trivial ring and let $\mathfrak{p}$ be a prime ideal. The *height of* $\mathfrak{p}$, denoted by $\operatorname{ht} \mathfrak{p}$ or $\operatorname{ht}_R \mathfrak{p}$ if we want to emphasize the ring $R$, is defined to be the maximum of the lengths of the saturated chains of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n,$$

such that $\mathfrak{p}_n = \mathfrak{p}$ if that maximum exists and infinity otherwise.

For example any minimal prime ideal has height 0, because it is impossible to find a prime ideal which is strictly contained in a minimal prime ideal.

In local rings the dimension and the height are closely related.

**Proposition 3.1.7.** *Let $(R, \mathfrak{m})$ be a local ring. Then the dimension of $R$ is the height of $\mathfrak{m}$. That is,*

$$\dim R = \operatorname{ht} \mathfrak{m}.$$

*Proof.* Firstly, notice that any maximal ideal is a prime ideal. Thus, $\operatorname{ht} \mathfrak{m}$ is well defined. Let the following be a longest possible saturated chain of prime ideals of $R$:

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n.$$

Then $\mathfrak{p}_n$ cannot be contained in a bigger prime ideal, so $\mathfrak{p}_n$ is a maximal ideal. Moreover $R$ has a unique maximal ideal, so $\mathfrak{p}_n = \mathfrak{m}$. Hence by definition $\operatorname{ht} \mathfrak{m} \geq \dim R$. On the other hand, let

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m = \mathfrak{m}$$

be one of the longest possible chains of prime ideals finishing with $\mathfrak{m}$. Since it is a chain of prime ideals of $R$ then $\dim R \geq m = \operatorname{ht} \mathfrak{m}$. Finally, since we have both inequalities $\operatorname{ht} \mathfrak{m} = \dim R$. □

### 3.1.2 Krull's ideal theorems

It would be interesting to relate the generators of a prime ideal, or at least the minimum amount of elements that are necessary to generate such an ideal to its height and, subsequently, to the dimension of a ring. That is exactly what is achieved from Krull's ideal theorems, first for principal ideals, and then for ideals generated by a finite number of elements. We should present two new concepts before

**Definition 3.1.8.** Let $R$ be a ring and let $\mathfrak{a}$ be an ideal of $R$. Then the *radical* of $\mathfrak{a}$, denoted by $\operatorname{Rad} \mathfrak{a}$, is the set

$$\operatorname{Rad} \mathfrak{a} = \{r \in R \mid \exists n \in \mathbb{N} \text{ such that } r^n \in \mathfrak{a}\}.$$

This set, which has got ideal structure, has been studied during the degree. However, its main properties are shown in Exercise 4.

**Definition 3.1.9.** Let $R$ be a ring and let $\mathfrak{a}$ be a proper ideal of $R$ such that whenever $ab \in \mathfrak{a}$ and $a \notin \mathfrak{a}$ then there exists an $n \in \mathbb{N}$ such that $b^n \in \mathfrak{a}$, (i.e. $b \in \operatorname{Rad} \mathfrak{a}$). Then $\mathfrak{a}$ is said to be a $\mathfrak{p}$-*primary ideal* where $\mathfrak{p} = \operatorname{Rad} \mathfrak{a}$.

It is clear that any prime ideal $\mathfrak{p}$ is a $\mathfrak{p}$-primary ideal. Moreover, for a maximal ideal $\mathfrak{m}$ and for any $n \in \mathbb{N}$ then $\mathfrak{m}^n$ is an $\mathfrak{m}$-primary ideal. (See Exercise 4.)

We also need an auxiliary result relating Noetherian and Artinian rings.

**Lemma 3.1.10.** *Let $R$ be a Noetherian ring with a unique prime ideal, then $R$ is an Artinian ring.*

**Theorem 3.1.11** (Krull's principal ideal theorem)**.** *Let $R$ be a non-trivial Noetherian ring and let $a$ be a non-unit (that is $(a) \neq R$). If $\mathfrak{p}$ is a minimal prime ideal of $(a)$, then* $\operatorname{ht}\mathfrak{p} \leq 1$.

*Proof.* First of all we will see that certain assumptions do not interfere in the proof, but they will simplify our work. Consider the minimal prime ideal $(a) \subseteq \mathfrak{p}$. After a localization consider the local ring $R_{\mathfrak{p}}$ and its unique maximal ideal $\mathfrak{p}R_{\mathfrak{p}}$, all the relevant data are preserved. Hence, we can assume without loss of generality that $(R, \mathfrak{m})$ is a local Noetherian ring and $\mathfrak{m}$ is a minimal prime ideal of $(a)$.

Consider the chain of prime ideals $\mathfrak{q}_1 \subseteq \mathfrak{q}_2 \subsetneq \mathfrak{m}$. Now we proceed to work in the quotient ring $R/\mathfrak{q}_1$ which is a domain, because $\mathfrak{q}_1$ is a prime ideal. Then $R/\mathfrak{q}_1$ is a local Noetherian domain such that $\{0\} \subseteq \mathfrak{q}_2/\mathfrak{q}_1 \subsetneq \mathfrak{m}/\mathfrak{q}_1$ and $(\overline{a}) \subseteq \mathfrak{m}/\mathfrak{q}_1$. Hence, we can also suppose without loss of generality that $(R, \mathfrak{m})$ is a local Noetherian domain, $\{0\} \subseteq \mathfrak{q} \subsetneq \mathfrak{m}$ is a chain of prime ideals and $\mathfrak{m}$ is a minimal prime ideal of $(a)$. Under those assumptions, if we prove that $\mathfrak{q} = \{0\}$ we are done.

Since $\mathfrak{m}$ is the unique minimal prime ideal of $(a)$ then $\mathfrak{m}/(a)$ is the unique prime ideal of $R/(a)$. Since $R/(a)$ is Noetherian then by Lemma 3.1.10 $R/(a)$ is an Artinian ring. Now let consider the ideals $\mathfrak{p}_i = (\mathfrak{q}^{(i)}, a)/(a)$, where $\mathfrak{q}^{(i)} = \mathfrak{q}^i R_{\mathfrak{q}} \cap R$. In Exercise 4 it is seen that $\mathfrak{q}^{(i)}$ is a $\mathfrak{q}$-primary ideal. Then

$$(\mathfrak{q}^{(1)}, a)/(a) \supseteq (\mathfrak{q}^{(2)}, a)/(a) \supseteq \cdots \supseteq (\mathfrak{q}^{(i)}, a)/(a) \supseteq \ldots$$

is a descending chain of ideals. Since $R/(a)$ is Artinian there exists some $n_0 \in \mathbb{N}$ such that $\mathfrak{p}_{i+1} = \mathfrak{p}_i$ for all $i \geq n_0$. Then by the correspondence theorem $(\mathfrak{q}^{(i)}, a) = (\mathfrak{q}^{(i+1)}, a)$ for all $i \geq n_0$. Hence, for any $v \in \mathfrak{q}^{(i)}$, there exist $r \in R$ and $w \in \mathfrak{q}^{(i+1)}$ such that $v = w + ar$ and so $ar = v - w \in \mathfrak{q}^{(i)}$. However, since $\mathfrak{m}$ is the minimal prime ideal of $(a)$ and $\mathfrak{q} \subsetneq \mathfrak{m}$ then $a \notin \mathfrak{q}$. Since $\operatorname{Rad}\mathfrak{q}^{(i)} = \mathfrak{q}$ and $a \notin \mathfrak{q}$ by the definition of a $\mathfrak{q}$-primary ideal, then $r \in \mathfrak{q}^{(i)}$. Therefore, $\mathfrak{q}^{(i)} \subseteq \mathfrak{q}^{(i+1)} + a\mathfrak{q}^{(i)}$. The reverse inclusion is clear so

$$\frac{\mathfrak{q}^{(i)}}{\mathfrak{q}^{(i+1)}} = a\frac{\mathfrak{q}^{(i)}}{\mathfrak{q}^{(i+1)}}.$$

Now $(R, \mathfrak{m})$ is a local Noetherian ring and $a \in \mathfrak{m} = \operatorname{Jac} R$, so applying Nakayama's lemma $\mathfrak{q}^{(i)}/\mathfrak{q}^{(i+1)} = \{0\}$. Thus, $\mathfrak{q}^{(i)} = \mathfrak{q}^{(i+1)} = \mathfrak{q}^{(n_0)}$ for all $i \geq n_0$. Moreover, $R_{\mathfrak{q}}$ is a local ring and $\mathfrak{q}R_{\mathfrak{q}} = \operatorname{Jac} R_{\mathfrak{q}}$. By the Krull's intersection theorem

$$\mathfrak{q}^{n_0} \subseteq \mathfrak{q}^{(n_0)} = \bigcap_{i=0}^{\infty} \mathfrak{q}^{(i)} \subseteq \bigcap_{i=0}^{\infty} \mathfrak{q}^i R_{\mathfrak{q}} = \bigcap_{i=0}^{\infty} (\mathfrak{q}R_{\mathfrak{q}})^i = \{0\}.$$

Therefore, $\mathfrak{q} = \{0\}$. Indeed, suppose that there exists a non-zero element $a \in \mathfrak{q}$, then $a^{n_0} \in \mathfrak{q}^{n_0} = \{0\}$. Hence $a \neq 0$ is a zero divisor, but it is a contradiction because $R$ is an integral domain. □

**Lemma 3.1.12.** *Let $(R, \mathfrak{m})$ be a local Noetherian ring and $\mathfrak{a}$ an ideal of $R$. Then the following statements are equivalent:*

*i)* $\operatorname{Rad} \mathfrak{a} = \mathfrak{m}$.

*ii)* $\mathfrak{a}$ *is* $\mathfrak{m}$*-primary.*

*iii)* $\mathfrak{m}$ *is the minimal prime ideal of* $\mathfrak{a}$.

*Proof.* See Exercise 4. □

**Theorem 3.1.13** (Krull's generalized ideal theorem)**.** *Let $R$ be a non-trivial Noetherian ring and let $\mathfrak{a}$ be a proper ideal which can be generated by $n$ elements. Then* $\operatorname{ht} \mathfrak{p} \leq n$ *for any minimal prime ideal $\mathfrak{p}$ of $\mathfrak{a}$.*

*Proof.* We proceed by induction on $n$. When $n = 0$, then $\mathfrak{a} = (\varnothing) = \{0\}$ and $\mathfrak{p}$ is a minimal prime ideal, so $\operatorname{ht} \mathfrak{p} = 0 \leq 0$. When $n = 1$ the statement holds by Theorem 3.1.11.

Now suppose that the result is true for smaller values than $n$ and consider the proper ideal $\mathfrak{a} = (x_1, \ldots, x_n)$ and its minimal prime ideal $\mathfrak{p}$. We can assume that $R$ is a local ring with $\mathfrak{p}$ as maximal ideal (otherwise it is enough to localize it at $\mathfrak{p}$). Hence by Lemma 3.1.12 then $\operatorname{Rad} \mathfrak{a} = \mathfrak{p}$ . Let

$$\mathfrak{p}_0 \subsetneq \cdots \subsetneq \mathfrak{p}_{m-1} \subsetneq \mathfrak{p}$$

be one of the longest saturated chains of prime ideals which finish in $\mathfrak{p}$. Choose the prime ideal $\mathfrak{q} = \mathfrak{p}_{m-1}$. Then $\mathfrak{q} \subsetneq \mathfrak{p}$ is saturated and $\operatorname{ht} \mathfrak{p} = \operatorname{ht} \mathfrak{q}+1$. We are reduced to proving that $\mathfrak{q}$ is a minimal prime ideal of an ideal generated by $n - 1$ elements.

Clearly $\mathfrak{q}$ cannot contain all $x_i$, so assume that $x_1 \notin \mathfrak{q}$. Moreover, $\mathfrak{p}$ is a minimal prime ideal of $(\mathfrak{q}, x_1)$ and it is maximal, so by Lemma 3.1.12 then $\operatorname{Rad}(\mathfrak{q}, x_1) = \mathfrak{p}$. Therefore, for each $i \geq 2$ then $x_i \in \mathfrak{p}$, so there exist $r_i \in R$, $y_i \in \mathfrak{q}$ and $n_i \in \mathbb{N}$ such that $x_i^{n_i} = y_i + r_i x_1$.

It follows that $(x_1, y_2, \ldots, y_n)$ will be contained in a *prime* ideal if and only if $(x_1, x_2, \ldots, x_n)$ is contained in that prime ideal. Hence using Exercise 4 (iv) then

$$\operatorname{Rad}(x_1, y_2, \ldots, y_n) = \operatorname{Rad}(x_1, x_2, \ldots, x_n) = \mathfrak{p}.$$

Furthermore, by Lemma 3.1.12 and the correspondence theorem we have that $\mathfrak{p}/(y_2, \ldots, y_n)$ is a minimal prime ideal of the principal ideal $(\overline{x_1}) =$

$(x_1, y_2, \ldots, y_n)/(y_2, \ldots, y_n)$. Now by the Krull principal ideal theorem the height of $\mathfrak{p}/(y_2, \ldots, y_n)$ is at most 1. Since $\mathfrak{q}/(y_2, \ldots, y_n) \subsetneq \mathfrak{p}/(y_2, \ldots, y_n)$ then $\mathfrak{q}/(y_2, \ldots, y_n)$ is a minimal prime ideal in the quotient ring. Finally, lifting back to $R$, $\mathfrak{q}$ is a minimal prime ideal of $(y_2, \ldots, y_n)$, an ideal generated by $n-1$ elements, so we are done. Indeed, using the induction hypothesis $\operatorname{ht}\mathfrak{p} = \operatorname{ht}\mathfrak{q} + 1 \leq n - 1 + 1 = n$. □

Let us analyze the behavior of the height in finite-dimensional rings. Being a local Noetherian ring is a sufficient condition in order to have a finite-dimensional ring, so we can restrict ourselves to that condition.

**Corollary 3.1.14.** *Let $R$ be a non-trivial Noetherian ring and let $\mathfrak{p}$ and $\mathfrak{q}$ be two prime ideals of $R$.*

*(i) The ideal $\mathfrak{p}$ has finite height. In particular, a local Noetherian ring has finite dimension.*

*(ii) If $\mathfrak{p} \subseteq \mathfrak{q}$. Then $\operatorname{ht}\mathfrak{p} \leq \operatorname{ht}\mathfrak{q}$. Moreover, when the inclusion is strict then $\operatorname{ht}\mathfrak{p} < \operatorname{ht}\mathfrak{q}$.*

*(iii) Suppose $\mathfrak{p} \subseteq \mathfrak{q}$. Then $\operatorname{ht}\mathfrak{p} = \operatorname{ht}\mathfrak{q}$ if and only if $\mathfrak{p} = \mathfrak{q}$.*

*Proof.* (i) Let $\mathfrak{p}$ be a prime ideal of $R$. Since $R$ is a Noetherian ring it is finitely generated by $n$ elements, say. Then by Theorem 3.1.13 $\operatorname{ht}\mathfrak{p} \leq n$, that is, $\mathfrak{p}$ has finite height. On the other hand, since $R$ is a local ring its dimension is the height of its unique maximal ideal, which is a finite number.

(ii) Set $\operatorname{ht}\mathfrak{p} = n$, then there exists a chain of prime ideals of $R$

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n,$$

such that $\mathfrak{p}_n = \mathfrak{p}$. Moreover, by hypothesis $\mathfrak{p} \subseteq \mathfrak{q}$. Then we consider the chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p} \subseteq \mathfrak{q}.$$

Therefore, $\operatorname{ht}\mathfrak{p} \leq \operatorname{ht}\mathfrak{q}$. Furthermore, when the inclusion is strict it is straightforward that $\operatorname{ht}\mathfrak{p} < \operatorname{ht}\mathfrak{q}$.

(iii) The *if* implication is obvious. On the other hand, the *only if* implication follows immediately from (ii). □

### 3.1.3 Height and systems of parameters

In Noetherian rings we are allowed to extend the concept of height to any ideal, prime or not. Furthermore, after extending that concept we will get also some results, which are by the way the reverses of the Krull's ideal theorems.

**Definition 3.1.15.** Let $R$ be a non-trivial Noetherian ring and let $\mathfrak{a}$ be a proper ideal of $R$. Clearly there exists a prime ideal containing $\mathfrak{a}$. Then the *height* of $\mathfrak{a}$, denoted by $\operatorname{ht}\mathfrak{a}$, is

$$\operatorname{ht}\mathfrak{a} = \min\{\operatorname{ht}\mathfrak{p} \mid \mathfrak{p} \text{ is prime and } \mathfrak{a} \subseteq \mathfrak{p}\}.$$

When we want to emphasize the ring $R$, we can write $\operatorname{ht}_R\mathfrak{a}$. Clearly the height of any proper ideal, is the minimun among the height of its minimal prime ideals. This definition is completely compatible with the one given for prime ideals some lines above.

**Lemma 3.1.16.** *Let $R$ be a non-trivial Noetherian ring and let $\mathfrak{a}$ and $\mathfrak{p}$ be two ideals such that $\mathfrak{a} \subseteq \mathfrak{p}$, $\mathfrak{p}$ is prime and $\operatorname{ht}\mathfrak{a} = \operatorname{ht}\mathfrak{p}$. Then $\mathfrak{p}$ is a minimal prime ideal of $\mathfrak{a}$.*

*Proof.* Suppose by contradiction that $\mathfrak{p}$ is not a minimal prime ideal of $\mathfrak{a}$. Then there exists a prime ideal, say $\mathfrak{q}$, such that $\mathfrak{a} \subseteq \mathfrak{q} \subsetneq \mathfrak{p}$, and so $\operatorname{ht}\mathfrak{a} \leq \operatorname{ht}\mathfrak{q} < \operatorname{ht}\mathfrak{p} = \operatorname{ht}\mathfrak{a}$, which is a contradiction. □

We also have the following similar result.

**Theorem 3.1.17.** *Let $R$ be a non-trivial Noetherian ring and let $\mathfrak{p}$ be a prime ideal such that $\operatorname{ht}\mathfrak{p} = n$. Then there exists an ideal $\mathfrak{a}$ generated by $n$ elements, such that $\operatorname{ht}\mathfrak{a} = n$ and $\mathfrak{a} \subseteq \mathfrak{p}$.*

*Proof.* We proceed by induction on $n$. In the case when $n = 0$ consider $\mathfrak{a} = \{0\}$ which is an ideal with the stated properties.

Suppose inductively that the statement holds for smaller values than $n$. Since $\operatorname{ht}\mathfrak{p} = n$ consider a saturated chain of prime ideals

$$\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n,$$

such that $\mathfrak{p} = \mathfrak{p}_n$. Then, $\operatorname{ht}\mathfrak{p}_{n-1} = n - 1$. Indeed, $\operatorname{ht}\mathfrak{p}_{n-1} \geq n - 1$ as shows the above chain, while $\operatorname{ht}\mathfrak{p}_{n-1} < \operatorname{ht}\mathfrak{p}_n = n$. Hence, there exists an ideal $\mathfrak{b} \subseteq \mathfrak{p}_{n-1}$ of height $n-1$, generated by $n-1$ elements, say $x_1, \ldots, x_{n-1}$.

According to Lemma 3.1.16, $\mathfrak{p}_{n-1}$ is a minimal prime ideal of $\mathfrak{b}$. However, since $\mathfrak{b}$ is proper there are finitely many minimal prime ideals of $\mathfrak{b}$, call them $\mathfrak{p}_{n-1}$ and $\mathfrak{q}_1, \ldots, \mathfrak{q}_s$. Observe that all of them have height $n - 1$. Indeed, by Krull's generalized ideal theorem and since $\operatorname{ht}\mathfrak{b} = n - 1$ then $n - 1 = \operatorname{ht}\mathfrak{b} \leq \operatorname{ht}\mathfrak{q}_i \leq n - 1$ for any $i = 1, \ldots, s$.

Now we have that

$$\mathfrak{p} \not\subseteq \mathfrak{p}_{n-1} \cup \mathfrak{q}_1 \cup \cdots \cup \mathfrak{q}_s,$$

because otherwise applying the prime avoidance theorem (Exercise 1) we would have $\mathfrak{p} \subseteq \mathfrak{p}_{n-1}$ or $\mathfrak{p} \subseteq \mathfrak{q}_i$ for some $i = 1, \ldots, s$. None of these posibilities can occur because $\operatorname{ht} \mathfrak{p} = n$, while

$$\operatorname{ht} \mathfrak{p} \leq \operatorname{ht} \mathfrak{p}_{n-1} = \operatorname{ht} \mathfrak{q}_i = n - 1.$$

Thus, there exists an element $x_n$ in $\mathfrak{p}$ but not in any minimal prime ideal of $\mathfrak{b} = (x_1, \ldots, x_{n-1})$. Finally, set $\mathfrak{a} = (x_1, \ldots, x_{n-1}, x_n)$. This ideal is generated by $n$ elements and $\mathfrak{a} \subseteq \mathfrak{p}$. If we prove that $\operatorname{ht} \mathfrak{a} = n$ the assertion follows.

Since $\mathfrak{b} \subseteq \mathfrak{a} \subseteq \mathfrak{p}$ we have $n - 1 = \operatorname{ht} \mathfrak{b} \leq \operatorname{ht} \mathfrak{a} \leq \operatorname{ht} \mathfrak{p} = n$. Suppose by contradiction that $\operatorname{ht} \mathfrak{a} = n - 1$, then there exists a minimal prime ideal $\mathfrak{p}'$ of $\mathfrak{a}$ such that $\operatorname{ht} \mathfrak{p}' = n - 1$. However, now we have that $\mathfrak{b} \subseteq \mathfrak{a} \subseteq \mathfrak{p}'$ and $\operatorname{ht} \mathfrak{p}' = n - 1 = \operatorname{ht} \mathfrak{b}$, it follows from Lemma 3.1.16 that $\mathfrak{p}'$ is one of the minimal prime ideals of $\mathfrak{b}$. But this is a contradiction, because $x_n \in \mathfrak{a} \subseteq \mathfrak{p}'$ whereas $x_n$ belongs to no minimal prime ideal of $\mathfrak{b}$. Thus the statement is proved. □

After all this work, a new definition of the dimension of a local Noetherian ring can be formulated, which is indeed related to the height concept.

**Proposition 3.1.18.** *Let $(R, \mathfrak{m})$ be a local Noetherian ring. Then,*

$$\dim R = \min \{n \mid \exists\ x_1, \ldots, x_n \in R \text{ such that } (x_1, \ldots, x_n) \text{ is } \mathfrak{m}\text{-primary}\}.$$

*That is, the dimension of $R$ is the least number of elements of $R$ needed to generate an $\mathfrak{m}$-primary ideal.*

*Proof.* Let us denote by $d$ the right hand side of the equality. First of all, since $\mathfrak{m}$ is an $\mathfrak{m}$-primary ideal the set is not empty, so the minimum is well defined. On the one hand, $\dim R = \operatorname{ht} \mathfrak{m} \leq d$. Indeed, by Lemma 3.1.12 the minimal prime ideal of any $\mathfrak{m}$-primary ideal is $\mathfrak{m}$. In particular $\mathfrak{m}$ is the minimal prime ideal of the one which can be generated with $d$ elements and the inequality follows from Theorem 3.1.13.

On the other hand, by Theorem 3.1.17 there exists an ideal $\mathfrak{q}$ which can be generated by $\dim R = \operatorname{ht} \mathfrak{m}$ elements and whose minimal prime ideal is $\mathfrak{m}$, i.e., an $\mathfrak{m}$-primary ideal. Hence, $d \leq \dim R$ and we are done. □

This particular set with $\dim R$ elements which generates an $\mathfrak{m}$-primary ideal is useful in order to characterize the ring $R$. It motivates the following definition.

**Definition 3.1.19.** Let $(R, \mathfrak{m})$ be a local Noetherian ring of dimension $d$. Then a *system of parameters* of the ring $R$ is a set of $R$ with $d$ elements which generates an $\mathfrak{m}$-primary ideal. Moreover, we say that $a_1, \ldots, a_d$ form a system of parameters of $R$ when $\{a_1, \ldots, a_d\}$ is a system of parameters of $R$.

It follows from Proposition 3.1.18 that any local Noetherian ring does indeed possess a system of parameters.

### 3.1.4 Dimension in quotient rings

Intuitively, the dimension of a quotient ring will be lower than the dimension of the initial ring. More precisely, these numbers are related with the number of elements needed to generate the ideal that factored with.

**Lemma 3.1.20.** *Let $R$ be a non-trivial Noetherian ring, let $\mathfrak{a}$ be a proper ideal of $R$ which can be generated by $n$ elements, and let $\mathfrak{p}$ be a prime ideal such that $\mathfrak{a} \subseteq \mathfrak{p}$. Then*

$$\operatorname{ht}_{R/\mathfrak{a}} \mathfrak{p}/\mathfrak{a} \leq \operatorname{ht}_R \mathfrak{p} \leq \operatorname{ht}_{R/\mathfrak{a}} \mathfrak{p}/\mathfrak{a} + n.$$

*Proof.* Firstly, notice that the ideal $\mathfrak{p}/\mathfrak{a}$ is prime in $R/\mathfrak{a} = \overline{R}$. On the one hand, it is immediate from the correspondence theorem that

$$\operatorname{ht}_{\overline{R}} \mathfrak{p}/\mathfrak{a} \leq \operatorname{ht}_R \mathfrak{p}.$$

Indeed, any prime ideal of $\overline{R}$ contained in $\mathfrak{p}/\mathfrak{a}$ corresponds to a prime ideal of $R$ which contains $\mathfrak{a}$ and which is contained in $\mathfrak{p}$. Thus there are more (or the same number) of prime ideals in any chain of prime ideals of $R$ finishing with $\mathfrak{p}$ than in any chain of prime ideals of $\overline{R}$ finishing with $\mathfrak{p}/\mathfrak{a}$. Then, the inequality follows from the definition of height.

On the other hand, let $b_1, \ldots, b_n$ generate $\mathfrak{a}$. Moreover, say $t = \operatorname{ht}_{\overline{R}} \mathfrak{p}/\mathfrak{a}$, by Theorem 3.1.17 and Lemma 3.1.16 there exist $a_1, \ldots, a_t \in R$ such that the ideal $\mathfrak{p}/\mathfrak{a}$ is a minimal prime ideal of $(\overline{a}_1, \ldots, \overline{a}_t)$. Hence, by the correspondence theorem $\mathfrak{p}$ is a minimal prime ideal of the ideal $(a_1, \ldots, a_t, b_1, \ldots, b_n)$, a proper ideal of $R$ that can be generated by $n+t$ elements. Thus, it follows from Theorem 3.1.13 that

$$\operatorname{ht}_R \mathfrak{p} \leq t + n = \operatorname{ht}_{\overline{R}} \mathfrak{p}/\mathfrak{a} + n.$$

Hence we are done. □

**Proposition 3.1.21.** *Let $(R, \mathfrak{m})$ be a Noetherian local ring and let $x_1, \ldots, x_t$ in $R$. Then*

$$\dim R - t \leq \dim R/(x_1, \ldots, x_t) \leq \dim R.$$

*Moreover, $\dim R - t = \dim R/(x_1, \ldots, x_t)$ if and only if $\{x_1, \ldots, x_t\}$ is a subset of a system of parameters of $R$.*

*Proof.* For notation simplicity denote $n = \dim R$, $\overline{\mathfrak{m}} = \mathfrak{m}/(x_1, \ldots, x_t)$ and $\overline{R} = R/(x_1, \ldots, x_t)$. According to Proposition 3.1.7, since both $R$ and $\overline{R}$ are

local rings, then $\dim R = \operatorname{ht}\mathfrak{m}$ and $\dim \overline{R} = \operatorname{ht}\overline{\mathfrak{m}}$.

By Lemma 3.1.20 we have that

$$\operatorname{ht}_{\overline{R}}\overline{\mathfrak{m}} \leq \operatorname{ht}_R \mathfrak{m} \leq \operatorname{ht}_{\overline{R}}\overline{\mathfrak{m}} + t.$$

That is,

$$\dim R/(x_1,\ldots,x_t) \leq \dim R \leq \dim R/(x_1,\ldots,x_t) + t.$$

Hence,

$$\dim R - t \leq \dim R/(x_1,\ldots,x_t) \leq \dim R.$$

Now, we shall prove the second part of the statement.

$\Rightarrow$) Suppose that $\dim \overline{R} = n - t \geq 0$. Then $t \leq n$ and by Proposition 3.1.18 there exist $x_{t+1},\ldots,x_n \in \mathfrak{m}$ such that $\{\overline{x}_{t+1},\ldots,\overline{x}_n\}$ is a system of parameters for $\overline{R}$. Then $(x_1\ldots,x_t,x_{t+1},\ldots,x_n)/(x_1,\ldots,x_t)$ is an $\overline{\mathfrak{m}}$-primary ideal of $\overline{R}$. Thus, $(x_1,\ldots,x_n)$ is an $\mathfrak{m}$-primary ideal of $R$. Hence, by Proposition 3.1.18 the set $\{x_1,\ldots,x_n\}$ is a system of parameters of $R$.

$\Leftarrow$) Suppose that there exist some elements $x_{t+1},\ldots,x_n \in \mathfrak{m}$ such that $\{x_1,\ldots,x_t,x_{t+1},\ldots,x_n\}$ is a system of parameters for $R$. Hence, $(x_1,\ldots,x_n)$ is an $\mathfrak{m}$-primary ideal of $R$, and so $(\overline{x}_1,\ldots,\overline{x}_n) = (\overline{x}_{t+1},\ldots,\overline{x}_n)$ is an $\overline{\mathfrak{m}}$-primary ideal of $\overline{R}$. Now according to Proposition 3.1.18 it follows that $\dim \overline{R} \leq n - t$, but we have from the first part that $\dim \overline{R} \geq n - t$. Hence, $\dim \overline{R} = \dim R - t$. □

## 3.2 Regular rings

When we work in a local ring $R$ whose unique maximal ideal is $\mathfrak{m}$, we can consider the ideals of $R$ as vector subspaces over the natural field $R/\mathfrak{m}$. Thus we have two distinct visions of the dimension, the one we have just introduced for rings in the previous section and the natural concept of the dimension of a vector space, that is, the number of elements that make up any basis. In this section we will try to link these two notions and introduce another property of local rings: *regularity*.

### 3.2.1 Definition and examples

Firstly, we ought to make sure that $\mathfrak{m}/\mathfrak{m}^2$ has $R/\mathfrak{m}$-vector space structure. There is no doubt about the sum of elements of $\mathfrak{m}/\mathfrak{m}^2$, so we are devoted to define de scalar product in order to get a vector space. We define the scalar product as follows $\cdot\colon R/\mathfrak{m} \times \mathfrak{m}/\mathfrak{m}^2 \to \mathfrak{m}/\mathfrak{m}^2$ where

$$(r+\mathfrak{m})\cdot(m+\mathfrak{m}^2) = (r+\mathfrak{m}^2)(m+\mathfrak{m}^2) = (rm+\mathfrak{m}^2).$$

Since the definition depends on the representatives in $R/\mathfrak{m}$ we shall prove that it is well defined, and it is straightforward because $\mathfrak{m}/\mathfrak{m}^2$ is annihilated by $\mathfrak{m}$. Hence for any $m + \mathfrak{m}^2 \in \mathfrak{m}/\mathfrak{m}^2$,

$$r_1 + \mathfrak{m} = r_2 + \mathfrak{m} \iff r_1 - r_2 \in \mathfrak{m} \implies (r_1 - r_2)m \in \mathfrak{m}^2.$$

Therefore $r_1 m + \mathfrak{m}^2 = r_2 m + \mathfrak{m}^2$. Now we can relate the two notions of dimension mentioned above.

**Proposition 3.2.1.** *Let $(R, \mathfrak{m})$ be a Noetherian local ring. Then*

$$\dim R \leq \dim \mathfrak{m}/\mathfrak{m}^2.$$

*Proof.* Notice that since $R$ is Noetherian $\mathfrak{m}$ is finitely generated. Firstly, we shall see that $\mathfrak{m} = (a_1, \ldots, a_n)$ if and only if

$$\mathfrak{m}/\mathfrak{m}^2 = \langle a_1 + \mathfrak{m}^2, \ldots, a_n + \mathfrak{m}^2 \rangle$$

(of course as $R/\mathfrak{m}$-vector space). The *only if* implication is clear. For the *if* implication define $\mathfrak{a} = (a_1, \ldots, a_n) \subseteq \mathfrak{m}$. Suppose by contradiction that for some $i$ we have $a_i \notin \mathfrak{m}$. Then $a_i$ will be a unit in $R$ and so $\mathfrak{m}/\mathfrak{m}^2 = R/\mathfrak{m}^2$ which is a contradiction.

Now for any $a \in \mathfrak{m}$ by initial hypothesis there exist $r_1, \ldots, r_n \in R$ such that

$$\begin{aligned} a + \mathfrak{m}^2 &= (r_1 + \mathfrak{m})(a_1 + \mathfrak{m}^2) + \cdots + (r_n + \mathfrak{m})(a_n + \mathfrak{m}^2) \\ &= r_1 a_1 + \mathfrak{m}^2 + \cdots + r_n a_n + \mathfrak{m}^2 = \sum_{i=1}^{n} r_i a_i + \mathfrak{m}^2. \end{aligned}$$

Then $a - \sum_{i=1}^{n} r_i a_i \in \mathfrak{m}^2$ and so $\mathfrak{m} \subseteq \mathfrak{a} + \mathfrak{m}^2$. The other inclusion is clear, i.e. $\mathfrak{m}^2 + \mathfrak{a} \subseteq \mathfrak{m}$. Then we have the equality. Therefore,

$$\mathfrak{m}\frac{\mathfrak{m}}{\mathfrak{a}} = \frac{\mathfrak{a} + \mathfrak{m}^2}{\mathfrak{a}} = \frac{\mathfrak{m}}{\mathfrak{a}}.$$

Finally, since $\operatorname{Jac} R = \mathfrak{m}$ and all the above ideals are finitely generated $R$-modules applying Nakayama's lemma $\mathfrak{m}/\mathfrak{a} = \{0\}$, so $\mathfrak{m} = \mathfrak{a} = (a_1, \ldots, a_n)$.

Hence, we have that $\dim \mathfrak{m}/\mathfrak{m}^2$ is the number of elements in each minimal generating set of $\mathfrak{m}$. As $\mathfrak{m}$ itself is an $\mathfrak{m}$-primary ideal it follows from Proposition 3.1.18 that $\dim R \leq \dim \mathfrak{m}/\mathfrak{m}^2$. □

**Remark 3.2.2.** In the right hand side expression we refer to the dimension as a vector space over the quotient field $R/\mathfrak{m}$.

**Definition 3.2.3.** Let $(R, \mathfrak{m})$ be a local ring. Then $R$ is said to be *regular* when $\dim R = \dim \mathfrak{m}/\mathfrak{m}^2$.

Furthermore, when $R$ is a Noetherian local ring, following the idea of the proof of Proposition 3.2.1 $\dim \mathfrak{m}/\mathfrak{m}^2$ is the number of elements of any minimal generating set of $\mathfrak{m}$ and according to Proposition 3.2.1 this number is at least $\dim R$. In particular, $R$ is regular if and only if $\mathfrak{m}$ can be generated exactly by $\dim R$ elements.

**Example 3.2.4.** Let $K$ be a field. Then its dimension is zero, $\dim K = 0$. Moreover, the unique maximal ideal of $K$ is $\{0\}$. Thus $\{0\}/\{0\}^2 \cong \{0\}$, which can be generated by the empty set, i.e., by zero elements. Therefore any field is a regular ring of dimension 0.

Finally, we should state one result concerning the power series rings, which is the main topic of these notes.

**Proposition 3.2.5.** *A power series ring $K[[X_1, \ldots, X_n]]$ in $n$ variables over a field $K$ is a regular ring.*

*Proof.* $K[[X_1, \ldots, X_n]]$ is a Noetherian local ring of dimension $n$ (see Exercise 5). Moreover its maximal ideal $(X_1, \ldots, X_n)$ can be generated by $n$ elements, so $K[[X_1, \ldots, X_n]]$ is a regular ring. □

### 3.2.2 Auslander-Buchsbaum's theorem

There is a very important theorem about regular rings, the Auslander-Buchsbaum theorem. Nevertheless, we are going to state some preliminary lemmas before approaching it.

**Lemma 3.2.6.** *Let $(R, \mathfrak{m})$ be a local ring and let $c \in \mathfrak{m} \setminus \mathfrak{m}^2$. Denote $\overline{R} = R/(c)$ and $\overline{\mathfrak{m}} = \mathfrak{m}/(c)$, the unique maximal ideal of the local ring $\overline{R}$. Then,*

$$\dim \mathfrak{m}/\mathfrak{m}^2 = \dim \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 + 1. \tag{3.1}$$

*Proof.* Call $n$ to the dimension of $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$. Consider $a_1, \ldots, a_n \in \mathfrak{m}$ such that their cosets form a basis of the vector space $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$. That is, the set $\{\overline{a}_1 + \overline{\mathfrak{m}}^2, \ldots, \overline{a}_n + \overline{\mathfrak{m}}^2\}$ is a basis of the vector space $\overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2$.

Thus, $\overline{\mathfrak{m}} = (\overline{a}_1, \ldots, \overline{a}_n, \overline{\mathfrak{m}}^2)$ and by the correspondence theorem we have that $\mathfrak{m} = (a_1, \ldots, a_n, c, \mathfrak{m}^2)$. Hence,

$$\{a_1 + \mathfrak{m}^2, \ldots, a_n + \mathfrak{m}^2, c + \mathfrak{m}^2\} \tag{3.2}$$

is a spanning set of the vector space $\mathfrak{m}/\mathfrak{m}^2$. We shall now see that (3.2) is linearly independent over the field $R/\mathfrak{m}$. In order to see that consider the linear combination

$$\sum_{i=1}^{n} (r_i + \mathfrak{m})(a_i + \mathfrak{m}^2) + (b + \mathfrak{m})(c + \mathfrak{m}^2) = 0 + \mathfrak{m}^2 \text{ where } r_i, b \in R.$$

That is, $\sum_{i=1}^{n} r_i a_i + bc \in \mathfrak{m}^2$ and so in the quotient ring $\overline{R}$ we have that $\sum_{i=1}^{n} \overline{r}_i \overline{a}_i \in \overline{\mathfrak{m}}^2$. However, by hypothesis this family is linearly independent over $\overline{R}/\overline{\mathfrak{m}}$. Thus, $\overline{r}_i \in \overline{\mathfrak{m}}$ and so $r_i \in \mathfrak{m}$ for any $i = 1, \ldots, n$. Indeed, for each $i$ there exist some $m_i \in \mathfrak{m}$ and some $s_i \in R$ such that $r_i = m_i + s_i c \in \mathfrak{m}$. Thus, $r_i + \mathfrak{m} = 0 + \mathfrak{m}$ in $R/\mathfrak{m}$ for any $i = 1, \ldots, n$.

Finally, $bc \in \mathfrak{m}^2$. Suppose by contradiction that $b \notin \mathfrak{m}$. Since $R$ is local $b \in \mathcal{U}(R)$ and so $c = b^{-1}bc \in \mathfrak{m}^2$, which is a contradiction with the initial hypothesis. Thus, $b \in \mathfrak{m}$ and so $b + \mathfrak{m} = 0 + \mathfrak{m}$. Hence (3.2) is a linearly independent family. Therefore,

$$\dim \mathfrak{m}/\mathfrak{m}^2 = n + 1 = \dim \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 + 1,$$

as we were required. □

**Lemma 3.2.7.** *Let $(R, \mathfrak{m})$ be a Noetherian regular ring and let $c \in \mathfrak{m} \setminus \mathfrak{m}^2$. Then $R/(c)$ is a Noetherian regular ring and* $\dim R/(c) = \dim R - 1$.

*Proof.* Firstly, we shall make sure that the formulas make sense. Since there exists $c \in \mathfrak{m} \setminus \mathfrak{m}^2$, then $\dim \mathfrak{m}/\mathfrak{m}^2 \geq 1$. Moreover, since $R$ is a regular ring then $\dim R = \dim \mathfrak{m}/\mathfrak{m}^2 \geq 1$, so $\dim R - 1$ is a non-negative integer.

Denote as before $\overline{R} = R/(c)$ and $\overline{\mathfrak{m}} = \mathfrak{m}/(c)$, the unique maximal ideal of the local ring $\overline{R}$. Since any ideal of $R$ can be generated by a finite number of elements, then any ideal of $\overline{R}$ can be generated by a finite number of elements, so $\overline{R}$ is Noetherian. Moreover, by Lemma 3.1.20 it follows that $\operatorname{ht} \overline{\mathfrak{m}} \geq \operatorname{ht} \mathfrak{m} - 1$, so

$$\dim \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 \geq \dim \overline{R} = \operatorname{ht} \overline{\mathfrak{m}} \geq \operatorname{ht} \mathfrak{m} - 1 = \dim R - 1. \tag{3.3}$$

However, on the other hand, from the regularity of $R$ and using the identity (3.1) we have that

$$\dim R - 1 = \dim \mathfrak{m}/\mathfrak{m}^2 - 1 = \dim \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2. \tag{3.4}$$

Therefore combining (3.3) and (3.4) we have that

$$\dim \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 \geq \dim \overline{R} \geq \dim R - 1 = \dim \overline{\mathfrak{m}}/\overline{\mathfrak{m}}^2 \tag{3.5}$$

Finally, it follows directly from (3.5) that $R/(c)$ is a regular ring such that $\dim R/(c) = \dim R - 1$. □

**Lemma 3.2.8.** *Let $(R, \mathfrak{m})$ be a Noetherian local ring that is not an integral domain, and let $\mathfrak{p}$ be a principal prime ideal. Then* $\operatorname{ht} \mathfrak{p} = 0$.

*Proof.* Suppose by contradiction that $\operatorname{ht}\mathfrak{p} > 0$. Then there exists a proper prime ideal $\mathfrak{q}$ such that $\mathfrak{q} \subsetneq \mathfrak{p} = (p)$. Of course, $p \notin \mathfrak{q}$ because otherwise $\mathfrak{p} = (p) \subseteq \mathfrak{q}$, which is impossible.

The procedure is to show that $\mathfrak{q} \subseteq \mathfrak{p}^n$ for any $n$ and then apply the Krull intersection theorem (it can be done because $R$ is local and so $\mathfrak{p} \subseteq \mathfrak{m} = \operatorname{Jac} R$). We proceed by induction on $n$. Since the case when $n = 1$ is clear, assume inductively $\mathfrak{q} \subseteq \mathfrak{p}^n$ for some $n$.

Consider any $a \in \mathfrak{q} \subseteq \mathfrak{p}^n = (p^n)$. Since $\mathfrak{p}^n$ is principal $a = bp^n$ for some $b \in R$. Hence $a = bp^n \in \mathfrak{q}$ and $\mathfrak{q}$ is a prime ideal which does not contain $p$, so $b \in \mathfrak{q} \subseteq \mathfrak{p}$ and so $a \in \mathfrak{p}^{n+1}$. Finally, applying Krull's intersection theorem $\mathfrak{q} \subseteq \cap_{i=1}^{\infty}\mathfrak{p}^i = \{0\}$ and so $\mathfrak{q} = \{0\}$, which is a contradiction. Indeed, since $R$ is not an integral domain $\{0\}$ is not a prime ideal. □

Now we are able to present the main theorem.

**Theorem 3.2.9** (Auslander-Buchsbaum)**.** *Any Noetherian regular ring is an integral domain.*

*Proof.* We proceed by induction on the dimension of $R$, denoted by $n$. In the case when $n = 0$ the ring $R$ is a field and so it is an integral domain. Indeed, let $(R, \mathfrak{m})$ be a regular ring of dimension 0, then by regularity $\dim \mathfrak{m}/\mathfrak{m}^2 = 0$, so $\mathfrak{m} = \mathfrak{m}^2$. Now, since $R$ is a local ring then $\operatorname{Jac} R = \mathfrak{m}$. Thus by Nakayama's lemma $\mathfrak{m} = \{0\}$. Therefore, since any proper ideal is contained in $\mathfrak{m} = \{0\}$, the unique ideals of $R$ are the trivial one and the total one. Thus $R$ is a field.

Assume the statement holds for $n - 1$, we will prove it for $n$. Suppose by contradiction that $R$ is not a domain. Since $\dim \mathfrak{m}/\mathfrak{m}^2 > 0$ we have that $\mathfrak{m} \setminus \mathfrak{m}^2 \neq \varnothing$, so choose $c \in \mathfrak{m} \setminus \mathfrak{m}^2$.

Since $R/(c)$ is a Noetherian regular ring of dimension $n-1$ (Proposition 3.2.7), by induction hypothesis $R/(c)$ is an integral domain and so $(c)$ is prime. Since $R$ is not an integral domain, according to Lemma 3.2.8 we have that $\operatorname{ht}(c) = 0$. Then $(c)$ is a minimal prime ideal of $\{0\}$, but there are finitely many minimal prime ideals of $\{0\}$, say $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. Thus, we have seen that

$$\mathfrak{m} \setminus \mathfrak{m}^2 \subseteq \bigcup_{i=1}^{s} \mathfrak{p}_i \implies \mathfrak{m} \subseteq \mathfrak{m}^2 \cup \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_s.$$

Finally by the prime avoidance theorem either $\mathfrak{m} \subseteq \mathfrak{m}^2$ which is a contradiction (we have said that the reverse inclusion is strict); or $\mathfrak{m} \subseteq \mathfrak{p}_{i_0}$ for some $i_0$. But then

$$n = \dim R = \operatorname{ht}\mathfrak{m} \leq \operatorname{ht}\mathfrak{p}_{i_0} = 0,$$

which is again a contradiction. Thus $R$ is an integral domain. □

### 3.2.3 Regular system of parameters

We have seen that the dimension of a Noetherian local ring $(R, \mathfrak{m})$ is the minimum number of elements that are needed to generate an $\mathfrak{m}$-primary ideal. However, when $R$ is regular $\mathfrak{m}$ itself can be generated with exactly $\dim R$ elements. Therefore, we can adapt the definition of system of parameters to the regular case.

**Definition 3.2.10.** Let $(R, \mathfrak{m})$ be a Noetherian regular ring of dimension $d$. Then a *regular system of parameters* of $R$ is a set of $d$ elements of $R$ which generate $\mathfrak{m}$, that is, a system of parameters which generate $\mathfrak{m}$.

**Example 3.2.11.** Let $K$ be a field. Then the unique maximal ideal of the regular ring $K[[X_1, \ldots, X_n]]$ is $(X_1, \ldots, X_n)$ and $K[[X_1, \ldots, X_n]]$ has dimension $n$. Then $\{X_1, \ldots, X_n\}$ is a regular system of parameters for $K[[X_1, \ldots, X_n]]$.

### 3.2.4 Regular rings of dimension one

Finally, we will try to characterize the regular rings of low dimension. Moreover, we can see that the analysis of domains of dimension one is quite simple.

**Theorem 3.2.12.** *Let $(R, \mathfrak{m})$ be a Noetherian local integral domain of dimension one. Then the following statements are equivalent:*

*(i) $R$ is regular,*

*(ii) every non-zero ideal of $R$ is a power of $\mathfrak{m}$,*

*(iii) there exists $a \in R$ such that each non-zero ideal of $R$ has the form $(a^h)$ for some $h \in \mathbb{N} \cup \{0\}$,*

*(iv) $R$ is a principal ideal domain.*

*Proof.* We shall prove the equivalence chain.

$(i) \implies (ii)$. Firstly since $R$ is regular $\dim \mathfrak{m}/\mathfrak{m}^2 = \dim R = 1$. Hence, the minimal generating set of $\mathfrak{m}$ has one element. In particular, $\mathfrak{m}$ is a principal ideal.

Let $\mathfrak{a}$ be a non-zero ideal of $R$. If $\mathfrak{a} = R$ then $\mathfrak{a} = \mathfrak{m}^0$, so we restrict ourselves to the case when $\mathfrak{a}$ is a proper ideal. Since $\mathfrak{m}$ is the unique maximal ideal of $R$, then $\mathfrak{a} \subseteq \mathfrak{m}$. Furthermore, because of the following inclusion chain

$$R \supseteq \mathfrak{m} \supseteq \mathfrak{m}^2 \supseteq \cdots \supseteq \mathfrak{m}^i \supseteq \ldots \tag{3.6}$$

there exists $n \in \mathbb{N} \cup \{0\}$ such that $\mathfrak{a} \subseteq \mathfrak{m}^n$ (this $n$ is at least one) and $\mathfrak{a} \nsubseteq \mathfrak{m}^{n+1}$. We shall see that really $\mathfrak{a} = \mathfrak{m}^n$. Consider one $y \in \mathfrak{a} \subseteq \mathfrak{m}^n$ such that $y \notin \mathfrak{m}^{n+1}$. Since $\mathfrak{m}$ is principal, then $y = rm^n$ for some $r \in R$ and for some $m \in \mathfrak{m}$ such that $\mathfrak{m} = (m)$. Moreover, since $y \notin \mathfrak{m}^{n+1}$, then $r \notin (m) = \mathfrak{m}$. Hence, since $R$ is local then $r \in \mathcal{U}(R)$. Thus, $m^n = r^{-1}y \in \mathfrak{a}$ and so $\mathfrak{m}^n \subseteq \mathfrak{a}$. Then the result follows.

*(ii)* $\implies$ *(iii)*. Since $\dim \mathfrak{m}/\mathfrak{m}^2 \geq \dim R = 1$, the inclusion $\mathfrak{m} \supseteq \mathfrak{m}^2$ is strict. Consider $a \in \mathfrak{m} \setminus \mathfrak{m}^2$, then by hypothesis $(a) = \mathfrak{m}^n$ for some $n \in \mathbb{N} \cup \{0\}$. Since $a \in \mathfrak{m}$, then $(a) \subseteq \mathfrak{m} \subsetneq R$, and so $n \geq 1$. Furthermore, since $a \notin \mathfrak{m}^2$, then $n \leq 1$ and so $n = 1$. Hence $\mathfrak{m} = (a)$. Moreover, every non-zero ideal of $R$ is a power of $\mathfrak{m}$. Therefore, any non-zero ideal of $R$ is of the form $(a^h)$ for some $h \in \mathbb{N} \cup \{0\}$.

*(iii)* $\implies$ *(iv)*. $R$ is an integral domain such that any proper ideal can be generated by one element of the form $a^h$ for some $a \in R$ and for some $h \in \mathbb{N} \cup \{0\}$, thus they are principal ideals. Trivially $R = (1)$ is a principal ideal. Thus, $R$ is a PID.

*(iv)* $\implies$ *(i)*. Since $R$ is a PID $\mathfrak{m}$ can be generated by one element. Moreover, this is the minimum number of elements which generate $\mathfrak{m}$, i.e., $\dim \mathfrak{m}/\mathfrak{m}^2 = 1$. Indeed, that number cannot be 0, since otherwise $\mathfrak{m} = \{0\}$ and $R$ would be a field, so $\dim R = 0$, which is a contradiction. Therefore, $\dim R = 1 = \dim \mathfrak{m}/\mathfrak{m}^2$ and $R$ is regular. □

For example the ring of $p$-adic integers $\mathbb{Z}_p$ is a local principal ideal domain of dimension one. Indeed, it is an integral domain which is not a field. Hence by the above theorem $\mathbb{Z}_p$ is a regular ring.

# Chapter 4

# Cohen's structure theorem

In this chapter the result that characterizes the power series rings will be presented. Expressed differently, we will formulate and demonstrate the Cohen structure theorem.

Throughout all of this chapter we will be working with finite-dimensional rings. Therefore, although it might not appear in the statements, the fact that we are working with local Noetherian rings should be assumed.

## 4.1 Field of representatives

**Definition 4.1.1.** Let $(R, \mathfrak{m})$ be a local ring. Then the field $R/\mathfrak{m}$ is called the *residue field* of $R$.

The residue field is the field which is defined in the natural way in any local ring $(R, \mathfrak{m})$, and now we should start with its analysis. In other words, we will study the characteristic of the residue field and the existence of a copy of that field contained in the ring $R$.

**Definition 4.1.2.** Let $(R, \mathfrak{m})$ be a local ring. Then, $R$ is said to be *equicharacteristic* when $R$ and the residue field $R/\mathfrak{m}$ have the same characteristic. Otherwise, it is said to have *mixed characteristic*.

Due to the complexity of the mixed characteristic case, on these notes we will limit ourselves to the equicharacteristic case. Moreover, for any field $K$ its characteristic is either zero or a prime number, $\operatorname{char} K = 0$ or $p$. Thus, we can forget about the local rings whose characteristic is not of that form.

**Examples 4.1.3.** (i) The ring of $p$-adic integers $\mathbb{Z}_p$ is a local ring of characteristic 0, but its residue field, $\mathbb{Z}_p/p\mathbb{Z}_p$, has characteristic $p$. Thus, $\mathbb{Z}_p$ has mixed characteristic.
(ii) Any field is an equicharacteristic ring. Indeed, $\{0\}$ is the unique maximal ideal of $K$ and so $K$ and its residue field are isomorphic. Hence, clearly both have the same characteristic.

From now on we will mainly work with fields, so we shall prove the following simple result concerning fields and injectivity.

**Lemma 4.1.4.** *Let $K$ be field, let $R$ be a non-trivial ring and let $\varphi : K \to R$ be a ring homomorphism. Then $\varphi$ is a monomorphism.*

*Proof.* For any ring homomorphism $\ker\varphi$ is an ideal of $K$ and $K$ is a field, so $\ker\varphi = \{0\}$ or $\ker\varphi = K$. However, $\varphi$ is a ring homomorphism, then $\varphi(1) = 1 \neq 0$ and so $1 \notin \ker\varphi$. Thus, $\ker\varphi = \{0\}$ and so $\varphi$ is injective. □

Now we should ask ourselves what the relation is between a local ring $R$ and its residue field, say $K$. Furthermore, we are going to see that the best situation will be that one in which we have an exact copy of $K$ within $R$. That is, there exists a subring of $R$ which is isomorphic to $K$. This idea is formalized in the next definition.

**Definition 4.1.5.** Let $(R, \mathfrak{m})$ be a local ring and let $\pi\colon R \to R/\mathfrak{m}$ be the canonical epimorphism. Suppose that there exists a subring $L$ of $R$ such that $\pi(L) = R/\mathfrak{m}$. Then $L$ is said to be a *field of representatives* or a *representative field* of $R$.

We conclude that the representative field of $R$ is isomorphic to the residue field $K = R/\mathfrak{m}$. Indeed, the restriction $\pi|_L$ is surjective and since $L$ is a field by Lemma 4.1.4 then $\pi|_L$ is also injective. When there exists such a field $L$ within $R$, $\pi(L)$ contains exactly one element of each residue class of $R/\mathfrak{m}$. And this is the motivation of its name, because it is a field made up by representatives of the quotient, one for each coset. In the following results we will study under what conditions such a field exists. We will see that completeness is an essential condition. Of course, in a Noetherian local ring $(R, \mathfrak{m})$ completeness is considered respect to the $\mathfrak{m}$-adic topology.

First, we shall discuss the zero-equicharacteristic case, using the famous Hensel's lemma; and then we will study the general equicharacteristic case. However, we ought to start by introducing some preliminary results and concepts.

**Lemma 4.1.6.** *Let $(R, \mathfrak{m})$ be a Noetherian complete local ring and let $f$ be a monic polynomial in $R[X]$. Suppose that there exist two coprime monic polynomials $G, H \in R/\mathfrak{m}[X]$ (of degree say $r$ and $n-r$ for some $r \geq 0$) such that $\overline{f} = GH$. Then there exist two monic polynomials $g, h \in R[X]$ such that $\overline{g} = G$, $\overline{h} = H$ and $f = gh$.*

**Notation.** Of course, $\overline{f}$ denotes the polynomial $f$ reduced modulo $\mathfrak{m}$. That is, if $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, then $\overline{f} = X^n + \overline{a_{n-1}}X^{n-1} + \cdots + \overline{a_0}$, where $\overline{a_i}$ is the residue of $a_i$ modulo $\mathfrak{m}$.

*Proof.* We have divided the proof into two steps and for notation simplicity we will denote $K = R/\mathfrak{m}$.

*Step 1.* We shall construct a sequence of polynomials $g_i$ and $h_i \in R[X]$, of degree $r$ and $n-r$ respectively, such that $f \equiv g_i h_i \pmod{\mathfrak{m}^i[X]}$ for any $i \geq 1$, where $\overline{g_i} = G$ and $\overline{h_i} = H$. And then we shall see that the polynomials $g_i, h_i$ are unique in the following way. If there exist some $g', h' \in R[X]$, of degree $r$ and $n-r$ respectively, such that $f \equiv g'h' \pmod{\mathfrak{m}^i[X]}$, $\overline{g'} = G$ and $\overline{h'} = H$, then $g_i \equiv g'$ and $h_i \equiv h' \pmod{\mathfrak{m}^i[X]}$. We will proceed inductively.

Given $G$ and $H$ choose representatives for the non-zero coefficients (make sure to choose 1 for $1 + \mathfrak{m}$). This defines two monic polynomials, say $g_1$ and $h_1 \in R[X]$, of degrees $r$ and $n-r$ respectively, where $\overline{g}_1 = G$ and $\overline{h}_1 = H$. Moreover, since $\overline{f} = GH = \overline{g}_1\overline{h}_1$, then $f \equiv g_1 h_1 \pmod{\mathfrak{m}[X]}$.

Now suppose inductively that $g_k$ and $h_k$ have been constructed and they are unique. We shall construct the polynomials $g_{k+1}$ and $h_{k+1}$ in $R[X]$ and show that they are unique.

Since $G$ and $H$ are coprime polynomials and $K[X]$ is a PID they generate the total ideal $K[X]$, i.e., $(G, H) = K[X]$. Hence, there exist two polynomials $\alpha, \beta \in R[X]$ such that

$$1 \equiv \alpha g_k + \beta h_k \pmod{\mathfrak{m}[X]}. \tag{4.1}$$

By induction hypothesis $\zeta = f - g_k h_k \in \mathfrak{m}^k[X]$. So multiplying (4.1) by $\zeta$, then

$$\zeta \equiv \zeta\alpha g_k + \zeta\beta h_k \pmod{\mathfrak{m}^{k+1}[X]}.$$

Now applying the division algorithm and dividing $\zeta\alpha$ with $h_k$ in $R[X]$ (it is monic so it makes sense), then there exist some $\gamma, \epsilon \in R[X]$ such that $\zeta\alpha = \gamma h_k + \epsilon$ and $\deg \epsilon < n - r$. Now since $\zeta\alpha \in \mathfrak{m}^k[X]$, then $0 \equiv \gamma h_k + \epsilon \pmod{\mathfrak{m}^k[X]}$. Since $h_k$ is monic then it has degree $n-r$ in $R/\mathfrak{m}^k[X]$, so $\gamma, \epsilon \in \mathfrak{m}^k[X]$. Then define $\delta = \gamma g_k + \zeta\beta \in \mathfrak{m}^k[X]$ (because $\gamma$ and $\zeta \in \mathfrak{m}^k[X]$) and so by (4.1)

$$\zeta \equiv \zeta\alpha g_k + \zeta\beta h_k \equiv \epsilon g_k + \gamma g_k h_k + \zeta\beta h_k = \epsilon g_k + \delta h_k \pmod{\mathfrak{m}^{k+1}[X]} \tag{4.2}$$

Since both $\zeta$ and $\epsilon g_k$ have degree strictly less than $n$ ($\deg \epsilon < n - r$), then so does $\delta h_k$ and so $\deg \delta < r$. Therefore, we can define the polynomials $h_{k+1} = h_k + \epsilon$ and $g_{k+1} = g_k + \delta \in R[X]$, whose degrees are $n-r$ and $r$ respectively. Furthermore, since $\delta, \epsilon \in \mathfrak{m}^k[X]$ then $\delta\epsilon \in \mathfrak{m}^{k+1}[X]$, so

$$g_{k+1}h_{k+1} \equiv g_k h_k + \epsilon g_k + \delta h_k + \delta\epsilon \equiv g_k h_k + \zeta + 0 \equiv f \pmod{\mathfrak{m}^{k+1}[X]}.$$

Moreover, since $\epsilon, \delta \in \mathfrak{m}^k[X]$, then $\overline{g_{k+1}} = \overline{g_k + \delta} = \overline{g_k} = G$ and in a similar way $\overline{h_{k+1}} = H$. Finally, we shall prove the uniqueness. Suppose that

there exist $h', g'$ in $R[X]$, of degree $r$ and $n-r$ respectively, such that $f \equiv g'h' \pmod{\mathfrak{m}^{k+1}[X]}$, $\overline{g'} = G$ and $\overline{h'} = H$. Then by inductive hypothesis $g_k$ and $h_k$ are unique, so define $\delta' = g' - g_k$ and $\epsilon' = h' - h_k$. Then $\delta', \epsilon' \in \mathfrak{m}^k[X]$ and so $\delta'\epsilon' \equiv 0 \pmod{\mathfrak{m}^{k+1}[X]}$. Now,

$$\begin{aligned} 0 &\equiv f - g'h' \\ &\equiv f - g_k h_k - \epsilon' g_k - \delta' h_k - \delta'\epsilon' \\ &\equiv \zeta - (\delta' h_k + \epsilon' g_k) \pmod{\mathfrak{m}^{k+1}[X]}. \end{aligned}$$

Hence subtracting this from (4.2) we obtain

$$0 \equiv (\delta - \delta')g_k + (\epsilon - \epsilon')h_k \pmod{\mathfrak{m}^{k+1}[X]},$$

where $\delta - \delta'$ (call it $\mu$) and $\epsilon' - \epsilon$ (call it $\nu$) have degree stricly less that $r$ and $n-r$ respectively. Now using identity (4.1) then $\alpha g_k + \beta h_k - 1 = m \in \mathfrak{m}[X]$. Hence, since $\nu h_k \equiv \mu g_k \pmod{\mathfrak{m}^{k+1}[X]}$

$$\begin{aligned} \mu = 1\mu &\equiv (\beta h_k + \alpha g_k - m)\mu \\ &\equiv \beta\mu h_k + \alpha\mu g_k - m\mu \\ &\equiv (\beta\mu + \alpha\nu)h_k - m\mu \pmod{\mathfrak{m}^{k+1}[X]}. \end{aligned}$$

However, $m\mu \in \mathfrak{m}^{k+1}[X]$, so $\mu$ is a multiple of $h_k$ in $R/\mathfrak{m}^{k+1}[X]$. But $h_k$ has degree $n-r$ and $\deg \mu < n-r$, so $\mu \equiv 0 \pmod{\mathfrak{m}^{k+1}[X]}$. Thus we have that $\delta \equiv \delta' \pmod{\mathfrak{m}^{k+1}[X]}$. In a similar way $\epsilon \equiv \epsilon' \pmod{\mathfrak{m}^{k+1}[X]}$. Hence, it follows that

$$h' \equiv h_k + \epsilon' \equiv h_k + \epsilon \equiv h_{k+1} \pmod{\mathfrak{m}^{k+1}[X]}$$

$$g' \equiv g_k + \delta' \equiv g_k + \delta \equiv g_{k+1} \pmod{\mathfrak{m}^{k+1}[X]}.$$

This completes the uniqueness.

*Step 2.* We shall find the desired polynomials $g, h \in R[X]$. Consider two integers $1 \leq i \leq j$, then $f - g_j h_j \in \mathfrak{m}^j[X] \subseteq \mathfrak{m}^i[X]$. So, $f - g_j h_j \in \mathfrak{m}^i[X]$ and by the uniqueness $g_i \equiv g_j \pmod{\mathfrak{m}^i[X]}$. Thus, if $g_i = g_{i0} + g_{i1}X + \cdots + X^r$ then for each $l = 0, \ldots, r-1$ we have that $g_{il} - g_{jl} \in \mathfrak{m}^i$, so the sequences $(g_{il})_{i\in\mathbb{N}}$ of coefficients of the $g_i$'s are Cauchy sequences. In a similar way, the sequences $(h_{il})_{i\in\mathbb{N}}$ $(l = 0, \ldots, n-r-1)$ of coefficientes of the $h_i$'s are Cauchy sequences. (There are $r + n - r = n$ different sequences.)

Since $R$ is a complete ring, then all the sequences are convergent to some values $a_0, \ldots, a_{r-1}$ (the sequences of the coefficients of the $g_i$'s) and to some $b_0, \ldots, b_{n-r-1}$ (the sequences of the coefficients of the $h_i$'s). Then define the monic polynomials

$$g(X) = a_0 + a_1 X + \cdots + a_{r-1}X^{r-1} + X^r \in R[X] \text{ and}$$

$$h(X) = b_0 + b_1 X + \cdots + b_{n-r-1}X^{n-r-1} + X^{n-r} \in R[X].$$

Now, $\overline{g_k} = G$ for any $k \geq 1$. Indeed, $\pi$ (the natural epimorphism $R$ onto $R/\mathfrak{m}$) is a continuous function and the coefficients are convergent. Hence for each $l = 0, \ldots, r-1$ we have $\pi(a_l) = \pi(\lim_{i\to\infty} g_{il}) = \lim_{i\to\infty} \pi(g_{il}) = G_l$, the $l$th coefficient of $G$. Therefore $\overline{g} = G$ and in the same way $\overline{h} = H$. Finally we shall see that $f = gh$.* Notice that for any $0 \leq i \leq n-1$, then

$$\begin{aligned}(gh)_i - (g_k h_k)_i &= \sum_{j=0}^{i} (g_j h_{i-j} - (g_k)_j (h_k)_{i-j}) \\ &= \sum_{j=0}^{i} (g_j - (g_k)_j) h_{i-j} + \sum_{j=0}^{i} (g_k)_j (h_{i-j} - (h_k)_{i-j}).\end{aligned}$$

When $k$ tends to the infinity $(g_k)_i \to g_i$ and $(h_k)_i \to h_i$, then by the above identity we have that $(g_k h_k)_i \to (gh)_i$. That is for any $\varepsilon > 0$, there exists $n_1 \in \mathbb{N}$ such that when $k \geq n_1$, then $|(gh)_i - (g_k h_k)_i| < \varepsilon/2$.

Moreover, by construction $f_i - (g_k h_k)_i \in \mathfrak{m}^k$, so $\lim_{k\to\infty} f_i - (g_k h_k)_i = 0$ (by Krull's intersection theorem). Thus, for any $\varepsilon > 0$, there exists some $n_2 \in \mathbb{N}$ such that when $k \geq n_2$, then $|f_i - (g_k h_k)_i| < \varepsilon/2$. Then if we choose $k \geq \max\{n_1, n_2\}$,

$$|f_i - (gh)_i| \leq |f_i - (g_k h_k)_i| + |(g_k h_k)_i - (gh)_i| < \varepsilon.$$

Therefore, $f_i = (gh)_i$ for any $i = 0, \ldots, n-1$ and so $f = gh$. □

Now it will be very easy to prove Hensel's lemma.

**Lemma 4.1.7** (Hensel)**.** *Let $(R, \mathfrak{m})$ be a Noetherian complete local ring and let $f \in R[X]$ be a monic polynomial. Suppose that there exists a simple root $\alpha \in R/\mathfrak{m}$ of the reduced polynomial $\overline{f}$. Then there exists an element $a \in R$, such that $\alpha \equiv a \pmod{\mathfrak{m}}$ and $f(a) = 0$. Moreover, the root $a$ of $f(X)$ is simple.*

*Proof.* Since $\alpha \in R/\mathfrak{m}$ is a root, $\overline{f}(X) = (X - \alpha)G(X) \in R/\mathfrak{m}[X]$ and since the root is simple $X - \alpha$ and $G$ are coprime polynomials. Then, by the preceding lemma there exist some polynomials $X - a,\ g(X) \in R[X]$ such that $\overline{g} = G$, $\overline{X - a} = X - \overline{a} = X - \alpha$ and $f(X) = (X - a)g(X)$. In particular, $a \equiv \alpha \pmod{\mathfrak{m}}$.

Furthermore, since $f(X) = (X-a)g(X)$, then $f(a) = 0$ and $a$ is a root of $f$ in $R[X]$. Finally, suppose by contradiction that $a$ is not a simple root, then $f(X) = (X-a)^2\tilde{g}(X)$. Thus, going to the quotient $\overline{f}(X) = (X-\alpha)^2\tilde{G}(X)$ and so $\alpha$ is not a simple root of $\overline{f}$, which is a contradiction. □

*Denote by $f_i$ the $i$th coefficient of $f$.

Hensel's lemma is a very important result. One of its practical applications is the factorization of polynomials. Indeed, the search of roots is simpler when we operate with reduced polynomials whose coefficients lie in the field $R/\mathfrak{m}$.

Now we are going to present a new concept that is linked with the separability of polynomials in field extensions, and which eventually will ensure the existence of a field of representatives.

**Definition 4.1.8.** Let $L : K$ be an algebraic field extension. Then the extension is *purely inseparable* if for any $\alpha \in L \setminus K$, the minimal polynomial of $\alpha$ is not a separable polynomial.

**Remark 4.1.9.** Let $L : K$ be a field extension which is both separable and purely inseparable at the same time. Then $L = K$. Clearly, suppose by contradiction that $L \setminus K \neq \varnothing$, then there exists an element in $L$ whose minimal polynomial over $K$ is at the same time separable and non-separable, which is impossible.

**Corollary 4.1.10** (Corollary of Hensel's lemma)**.** *Let $R$ be a Noetherian complete equicharacteristic local ring such that its characteristic is zero. Then there exists a subfield $L$ of $R$ such that $R/\mathfrak{m}$ is purely inseparable over the image of $L$ in $R/\mathfrak{m}$.*

*Proof.* Firstly, we shall prove that $R$ contains at least one field. Consider the *primary subring* of $R$

$$\mathbb{Z}[1] = \{n \cdot 1 \mid n \in \mathbb{Z}\},$$

where 1 is the identity of $R$. Since $\operatorname{char} R = 0$, then $\mathbb{Z}[1]$ is isomorphic to the ring of integers, $\mathbb{Z}[1] \cong \mathbb{Z}$. Moreover, since $\operatorname{char} R/\mathfrak{m} = 0$ we can assert that for any integer $n \neq 0$, then $n \cdot 1 \notin \mathfrak{m}$. Indeed, suppose by contradiction that there exists $n \in \mathbb{Z}$ such that $n \cdot 1 = 1 + \cdots + 1 \equiv 0 \mod \mathfrak{m}$, then $\operatorname{char} R/\mathfrak{m} = 0$ divides $n$, which is a contradiction. Hence, $n \cdot 1$ is a unit in $R$, with inverse say $(n \cdot 1)^{-1}$. Thus, consider

$$E = \{(n \cdot 1)(m \cdot 1)^{-1} \mid n \in \mathbb{Z} \text{ and } m \in \mathbb{Z} \setminus \{0\}\} \subseteq R,$$

which is a field and it is isomorphic to the field of rational numbers, $E \cong \mathbb{Q}$.

Now consider the set $\Phi$ of all subfields of $R$, which is not empty because it contains $E$. This set is partially ordered with respect to inclusion. Hence it admits by the Zorn lemma a maximal element say $L$.

Now consider the canonical epimorphism $\pi \colon R \to R/\mathfrak{m}$. We shall see that $R/\mathfrak{m}$ is purely inseparable over $\pi(L)$.

First, we discard that the extension $R/\mathfrak{m} : \pi(L)$ is transcendental. If it were true then we would have an element $x \in R$ such that $\pi(x)$ is transcendental over $\pi(L)$. Thus all the non-zero elements of $L[x]$ would be outside $\mathfrak{m}$ and so they would be units. Indeed, consider $a \neq 0 \in L[x]$ and suppose by contradiction that $a \in \mathfrak{m}$. Since $a \neq 0 \in L[x]$ then

$$a = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

for some $a_i \in L$. Therefore, since $a \in \mathfrak{m}$

$$0 = \pi(a) = \pi(a_n)\pi(x)^n + \cdots + \pi(a_1)\pi(x) + \pi(a_0).$$

Thus $\pi(x)$ is algebraic over $\pi(L)$, which is a contradiction. Therefore, $R$ contains contains the field $L[x]$, which is a contradiction with the maximality of $L$.

Thus, $R/\mathfrak{m}$ is algebraic over $\pi(L)$. Now, suppose by contradiction that there exists an element $\lambda$ which is separable over $\pi(L)$. Let $\overline{f}(X) = X^n + \alpha_{n-1}X^{n-1} + \cdots + \alpha_0$ be the minimal polynomial of $\lambda$ over $\pi(L)$ and let $a_i$ be a representative of each $\alpha_i$ for $i = 0, \ldots, n-1$. The polynomial $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in L[X]$ is a monic polynomial such that $\lambda$ is a simple root of $\overline{f}$. Hence, by Hensel's lemma there exists a simple root $x \in R$ such that $\pi(x) = \lambda$ and $f(x) = 0$.

Furthermore, $\pi$ induces a field-isomorphism from $L$ onto $\pi(L)$, which carries $f$ to $\overline{f}$, which is irreducible. Then, since isomorphisms keep irreducibility $f$ is irreducible over $L[X]$.

$$\begin{array}{ccc} R & \xrightarrow{\pi} & R/\mathfrak{m} \\ | & & | \\ L[x] & \xrightarrow{\pi} & \pi(L)[\lambda] \\ | & & | \\ L & \xrightarrow{\pi} & \pi(L) \end{array}$$

Finally, with the preceding isomorphism $L[x]$ is isomorphic with $\pi(L)[\lambda]$, which is a field. Indeed, $\lambda$ is an algebraic element, so $\pi(L)[\lambda] = \pi(L)(\lambda)$. Then, $L[x]$ is a field and by the maximality of $L$ we have that $x \in L$. Therefore, $\pi(x) = \lambda \in \pi(L)$. Thus, $R/\mathfrak{m}$ is purely inseparable over $\pi(L)$. □

**Remark 4.1.11.** It is clear that $\mathbb{Z}$ may not be contained in $R$, so in the proof of the preceding corollary $n \cdot 1$ cannot be viewed as the product of two elements inside $R$, but as the finite sums $n \cdot 1 = 1 + \ldots^n + 1$ (when $n > 0$), $n \cdot 1 = -(1 + \ldots^n + 1)$ (when $n < 0$) and $0$ (when $n = 0$).

Now after all this work we obtain the desired result in the zero equicharacteristic case.

**Corollary 4.1.12** (Existence of a field of representatives for equicharacteristic zero)**.** *Let $R$ be a Noetherian complete equicharacteristic local ring such that its characteristic is zero. Then $R$ admits a field of representatives.*

*Proof.* By Corollary 4.1.10 there exists a subfield $L$ of $R$ such that the field extension $R/\mathfrak{m} : \pi(L)$ is purely inseparable. However, since the characteristic of $R/\mathfrak{m}$ is 0 the field extension is perfect and so the preceding extension is separable. Now an extension $E : K$ can be both purely inseparable and separable if and only if $E = K$, so $R/\mathfrak{m} = \pi(L)$. Therefore $L$ is a field of representatives. □

Finally, we are going to generalize the preceding result to any equicharacteristic ring.

**Theorem 4.1.13** (Existence of a field of representatives)**.** *Let $R$ be a Noetherian complete equicharacteristic local ring. Then $R$ admits a field of representatives.*

*Proof.* The case when $R$ and $R/\mathfrak{m}$ have both characteristic 0 has been proved in Corollary 4.1.12 as a consequence of Hensel's lemma. Thus, we restrict ourselves to the case when $\operatorname{char} R = \operatorname{char} R/\mathfrak{m} = p$ (a prime number). We shall divide the proof into two cases.

*Case 1.* We first turn to the case when $\mathfrak{m}^p = \{0\}$. Let us consider

$$R^p = \{x^p \mid x \in R\},$$

which is a subring of $R$, because $\operatorname{char} R = p$. If $x^p \neq 0$, then $x \notin \mathfrak{m}$ and it is invertible, with inverse say $y$. Then $x^p$ has inverse $y^p$ in $R^p$ and so $R^p$ is a subfield of $R$. Now consider the set of subfields of $R$ which contain $R^p$. That set is non-empty and partially ordered with respect to inclusion. Thus Zorn's lemma asserts the existence of a maximal subfield $L$ among those containing $R^p$. Secondly, consider the canonical epimorphism $\pi$ from $R$ onto $R/\mathfrak{m}$ and consider its restriction to $L$, $\pi|_L$, which is a monomorphism.

We proceed to prove that $\pi(L) = R/\mathfrak{m}$. Suppose by contradiction that there exists $\alpha \in R/\mathfrak{m}$ such that $\alpha \notin \pi(L)$. Since $\alpha^p \in \pi(R^p) \subseteq \pi(L)$ the minimal polynomial of $\alpha$ over $\pi(L)$ is $X^p - \alpha^p$.

Indeed, since $p$ is a prime number we know that a polynomial of the type $X^p - b$ is irreducible or it has a root. Hence, the polynomial $X^p - \alpha^p$ is irreducible, otherwise since we have that $X^p - \alpha^p = (X - \alpha)^p$ (in $R/\mathfrak{m}$) then $\alpha \in \pi(L)$ which is a contradiction. We take the representative $a \in R$

of $\alpha$, that is $\pi(a) = \alpha$, then $a \notin L$, because otherwise $\alpha = \pi(a) \in \pi(L)$. Now $\pi|_L \colon L \to \pi(L)$ is an isomorphism, and it induces another isomorphism $\tilde{\pi} \colon L[X] \to \pi(L)[X]$. Since isomorphisms preserve irreducibility and $X^p - \alpha^p$ is irreducible in $\pi(L)[X]$, then $X^p - a^p$ is irreducible in $L[X]$. Therefore,

$$L[a] \cong \frac{L[X]}{(X^p - a^p)}$$

is a field. Thus $L[a] = L(a)$ is a subfield of $R$ containing properly $L$ and thus $R^p$, in contradiction with the maximality of $L$. Hence, the restriction of $\pi$ is surjective and so it is an isomorphism. Therefore $\pi(L) = R/\mathfrak{m}$ and so $R$ admits a field of representatives.

*Case 2.* For the general case, denote $K = R/\mathfrak{m}$ and consider the local ring $R/\mathfrak{m}^2$ and its unique maximal ideal $\overline{\mathfrak{m}} = \mathfrak{m}/\mathfrak{m}^2$. It satisfies the condition $\overline{\mathfrak{m}}^2 = \{\overline{0}\}$ and so $\overline{\mathfrak{m}}^p = \{\overline{0}\}$. Hence $R/\mathfrak{m}^2$ admits a field of representatives, say $K_2$. Furthermore the natural epimorphism $\pi_1 \colon R/\mathfrak{m}^2 \to R/\mathfrak{m}$ induces an isomorphism $\pi_1 \colon K_2 \to K$.

Let $\pi_n \colon R/\mathfrak{m}^{n+1} \to R/\mathfrak{m}^n$ be the canonical epimorphism defined by $\pi_n(x + \mathfrak{m}^{n+1}) = x + \mathfrak{m}^n$, with kernel $\ker \pi_n = \mathfrak{m}^n/\mathfrak{m}^{n+1}$.

We construct by induction on $n$, a representative field $K_n$ of $R/\mathfrak{m}^n$ such that the canonical epimorphism $\pi_n$ induces an isomorphism from $K_{n+1}$ into $K_n$.

Suppose that $K_n$ has already been constructed for $n$. Firstly, $A = \pi_n^{-1}(K_n)$ is a subring of $R/\mathfrak{m}^{n+1}$ and

$$\mathfrak{m}^n/\mathfrak{m}^{n+1} = \ker \pi_n = \pi^{-1}(\overline{0}) \subseteq \pi^{-1}(K_n).$$

Secondly, for any $\beta \in A$ such that $\beta \notin \mathfrak{m}^n/\mathfrak{m}^{n+1}$ it is a unit in $R/\mathfrak{m}^{n+1}$. Indeed, $\beta \notin \ker \pi_n$ so $0 \neq \pi_n(\beta) = \lambda \in K_n$ and $K_n$ is a field, so $\lambda$ is a unit in $K_n$. Therefore, $\lambda$ is also a unit in the local ring $R/\mathfrak{m}^n$, so $\lambda \notin \mathfrak{m}/\mathfrak{m}^n$. Thus $\beta = \pi^{-1}(\lambda) \notin \mathfrak{m}/\mathfrak{m}^{n+1}$. Suppose by contradiction that $\beta \in \mathfrak{m}/\mathfrak{m}^{n+1}$. Then $\beta = m + \mathfrak{m}^{n+1}$ for some $m \in \mathfrak{m}$, so $\lambda = \pi_n(\beta) = \pi_n(m + \mathfrak{m}^{n+1}) = m + \mathfrak{m}^n \in \mathfrak{m}/\mathfrak{m}^{n+1}$, which is a contradiction. Thus, $\beta \notin \mathfrak{m}/\mathfrak{m}^{n+1}$ and so it is a unit in $R/\mathfrak{m}^{n+1}$ as we have stated previously. Let $\eta$ be the inverse of $\beta$ in $R/\mathfrak{m}^{n+1}$, that is, $\eta\beta = 1 + \mathfrak{m}^{n+1}$. Then $\pi_n(\eta\beta) = \pi_n(\eta)\pi(\beta) = 1 + \mathfrak{m}^n$ and so $\pi_n(\eta) = \pi_n(\beta)^{-1} \in K_n$. Since $\pi_n(\eta) \in K_n$ and $A = \pi_n^{-1}(K_n)$ we have that $\eta \in A$. Thus $\beta$ is a unit in $A$ and so $\mathfrak{m}^n/\mathfrak{m}^{n+1}$ is the unique maximal ideal of $A$.

Now $(\mathfrak{m}^n/\mathfrak{m}^{n+1})^2 = \{0\}$ and so $(\mathfrak{m}^n/\mathfrak{m}^{n+1})^p = \{0\}$. Indeed, $\mathfrak{m}^{2n} \subseteq \mathfrak{m}^{n+1}$ and the result follows. Then the proof runs as before and it shows the existence of a field of representatives $K_{n+1}$ of $A$. We shall prove that that the

epimorphism $\pi_n$ induces an isomorphism and that $K_{n+1}$ is the representative field of $R/\mathfrak{m}^{n+1}$. Denote $\mathfrak{p} = \mathfrak{m}^n/\mathfrak{m}^{n+1}$ the unique maximal ideal of $A$, then $A/\mathfrak{p} \equiv K_{n+1}$. Furthermore, $\ker_{\pi_n|_A} = \mathfrak{m}^n/\mathfrak{m}^{n+1} = \mathfrak{p}$, so by the first isomorphism theorem $K_n \equiv A/\mathfrak{p}$. Therefore, $\pi_n$ induces an isomorphism $K_{n+1}$ onto $K_n$.

Finally, for each $n$ we have an epimorphism $\psi_n$ $R/\mathfrak{m}^{n+1}$ onto $R/\mathfrak{m}$, which is the composition of the canonical epimorphisms $\pi_i\colon R/\mathfrak{m}^{i+1} \to R/\mathfrak{m}^i$, i.e., $\psi_n = \pi_1 \circ \cdots \circ \pi_n$. Moreover, $K_n$ is the field of representatives of $R/\mathfrak{m}^n$, so $\psi_{n-1}(K_n) = K$, $\psi_{n-1}$ is an isomorphism (composition of isomorphisms) and $\psi_{n-1} \circ \pi_n = \psi_n$. Thus,

$$\psi_n(K_{n+1}) = \psi_{n-1}(\pi_n(K_{n+1})) = \psi_{n-1}(K_n) = K.$$

Hence $K_{n+1}$ is a field of representatives for $R/\mathfrak{m}^{n+1}$.

We continue the proof stating one property of $R$. Let $(\alpha_n + \mathfrak{m}^n)_{n\in\mathbb{N}}$ be a sequence[†] such that $\pi_n(\alpha_{n+1} + \mathfrak{m}^{n+1}) = \alpha_n + \mathfrak{m}^n$ for any $n \in \mathbb{N}$. Then there exists a unique element $a \in R$ such that

$$\forall k \in \mathbb{N}\ \exists n_0 \in \mathbb{N} \text{ s.t. } \forall n \geq n_0 \text{ then } a \equiv \alpha_n \mod \mathfrak{m}^k.$$

To see that, consider the sequence $(\alpha_n)_{n\in\mathbb{N}} \subseteq R$. Since $\pi_n(\alpha_{n+1} + \mathfrak{m}^{n+1}) = \alpha_n + \mathfrak{m}^n$ then $\alpha_{n+1} \equiv \alpha_n \mod \mathfrak{m}^n$. Hence by Proposition 1.4.7 $(\alpha_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in $R$. Since $R$ is complete the sequence is convergent and let us denote its limit by $a$. Then by the definition of convergence

$$\forall k \in \mathbb{N}\ \exists n_0 \in \mathbb{N} \text{ s.t. } \forall n \geq n_0 \text{ then } a \equiv \alpha_n \mod \mathfrak{m}^k.$$

Moreover the uniqueness of $a$ is given by the Krull intersection theorem. Indeed, suppose that there are two values $a, b \in R$ satisfying the above condition then for any $k$ there exists some $n$ big enough such that

$$a \equiv \alpha_n \equiv b \mod \mathfrak{m}^k \implies a - b \in \mathfrak{m}^k.$$

Hence $a - b \in \bigcap_{n=0}^{\infty} \mathfrak{m}^n = \{0\}$, so $a = b$. This shows that the value $a$ does not depend on the choice of the associated sequence $(\alpha_n)_{n\in\mathbb{N}}$.

Now we define the map $u\colon K \to R$ given as follows: for any $\eta \in K$ consider the coherent sequence

$$(\eta_1 = \eta, \eta_2 = \pi_1|_{K_2}^{-1}(\eta), \ldots, \eta_{n+1} = \pi_n|_{K_{n+1}}^{-1}(\eta_n), \ldots)$$

and let $u(\eta)$ be its limit. Each $\pi_n|_{K_{n+1}}$ is an isomorphism so for each $\eta \in K$ the above sequence exists and it is unique, so $u$ is well-defined.

[†]This type of sequence is called *coherent sequence.*

Furthermore, $u$ is a ring homomorphism. Firstly the ring isomorphisms $\pi_n^{-1}$ and limits preserve sum and multiplication. Therefore we have that $u(\eta+\eta') = u(\eta)+u(\eta')$ and $u(\eta\eta') = u(\eta)u(\eta')$ for any $\eta, \eta' \in K$. Moreover, the uniqueness forces that $u(1) = 1$. Indeed, consider the coherent sequence

$$(1, \pi_1^{-1}(1) = 1 + \mathfrak{m}, \dots, \pi_n^{-1}(1) = 1 + \mathfrak{m}^{n+1}, \dots),$$

one of whose associated sequences in $R$ is $(1, 1, \dots, 1, \dots)$, a sequence whose limit is 1. Finally by the uniqueness of the limit $u(1) = 1$. Therefore $u\colon K \to R$ is a ring homomorphism and $u(K) \subseteq R$ is a subring.

Futhermore, any $\eta \neq 0$ in $K$ is a unit and it has an inverse say $\eta'$. Then, $u(\eta)u(\eta') = u(\eta\eta') = u(1) = 1$ and the inverse of $u(\eta)$ in $u(K)$ is $u(\eta')$. Thus, $u(K) \subseteq R$ is a field. Therefore $\pi\colon u(K) \to K$ is a ring monomorphism.

We shall prove the surjectivity of the restricted $\pi$. Indeed, consider $x + \mathfrak{m} \in R/\mathfrak{m}$. Then $(x + \mathfrak{m}, \dots, x + \mathfrak{m}^n, \dots)$ is a coherent sequence and $(x, x, \dots, x, \dots)$ is an associated sequence in $R$. Then the previous constant sequence converges to $x \in R$. So $u(x + \mathfrak{m}) = x \in u(K)$ and hence we have $\pi(x) = x+\mathfrak{m} \in \pi(u(K))$. Since the reverse inclusion is clear then $\pi(u(K)) = K$ and so $\pi$ is an isomorphism. Hence $u(K) \subseteq R$ is the representative field of $R$. □

The chapter has started from the analysis of Noetherian local rings. However, in order to ensure the existence of a field of representatives, it is enough to impose a third condition to the ring: completeness; of course with respect to the $\mathfrak{m}$-adic topology. Finally, let us analyze how to join in the fourth property analyzed in this notes: regularity.

## 4.2 Non-regular case

Even though we have insisted repeatedly that regularity is a condition in the Cohen structure theorem, firstly we can study what happens if we dispense with that condition.

### 4.2.1 General case

When $R$ is a Noetherian, local and complete ring, but not regular, it is hardly the same as a power series ring. In fact, it is just the quotient of a power series ring by a suitable ideal. Let us see it.

**Lemma 4.2.1.** *Let be $R$ a Noetherian complete equicharacteristic local ring, let $K$ be one of its field of representatives and let $\{a_1, \dots, a_n\}$ be a generator*

*set for* $\mathfrak{m} \subseteq R$. *Then* $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ *is a finitely generated* $K$*-vector space and*

$$\mathfrak{m}^i/\mathfrak{m}^{i+1} = \langle Q(a_1, \ldots, a_n) + \mathfrak{m}^{i+1} |\ Q \in \mathcal{Q}_i \rangle_K,$$

*where* $\mathcal{Q}_i = \{Q \in K[X_1, \ldots, X_n] \mid Q$ *is a monomial of degree* $i\}$.

*Proof.* Observe that we can ensure the existence of a finite generator set for the ideal $\mathfrak{m}$, because $R$ is a Noetherian ring. Moreover, it is easy to verify that the quotient $\mathfrak{m}^i/\mathfrak{m}^{i+1}$ has $K$-vector space structure. Indeed, since $\mathfrak{m}$ is an ideal of $R$.

- $(m_1 + \mathfrak{m}^{i+1}) + (m_2 + \mathfrak{m}^{i+1}) = (m_1 + m_2) + \mathfrak{m}^{i+1} \in \mathfrak{m}^i/\mathfrak{m}^{i+1}$, $\forall m_1, m_2 \in \mathfrak{m}^i$.
- Since $am \in \mathfrak{m}^i$, for all $a \in K \subseteq R$ and $m \in \mathfrak{m}^i$, then

$$a(m + \mathfrak{m}^{i+1}) \in \mathfrak{m}^i/\mathfrak{m}^{i+1},\ \forall a \in K,\ \forall m + \mathfrak{m}^{i+1} \in \mathfrak{m}^i/\mathfrak{m}^{i+1}.$$

On the other hand, since $\mathfrak{m} = (a_1, \ldots, a_n)$ then

$$\mathfrak{m}^i = (x_1 \ldots x_i \mid x_k \in \{a_1, \ldots, a_n\}),$$

so

$$\mathfrak{m}^i = \left\{ \sum_{j=1}^{l} \lambda_j Q_j(a_1, \ldots, a_n) \mid \lambda_j \in K,\ Q_j \in \mathcal{Q}_i, l \in \mathbb{N} \right\}.$$

Therefore,

$$\mathfrak{m}^i/\mathfrak{m}^{i+1} = \left\{ \sum_{j=1}^{l} \lambda_j Q_j(a_1, \ldots, a_n) + \mathfrak{m}^{i+1} \mid \lambda_j \in K, Q_j \in \mathcal{Q}_i, l \in \mathbb{N} \right\}$$

and so

$$\mathfrak{m}^i/\mathfrak{m}^{i+1} = \langle Q(a_1, \ldots, a_n) + \mathfrak{m}^{i+1} \mid Q \in \mathcal{Q}_i \rangle_K.$$

Moreover, it is easy to see that the vector space is finitely generated, and so it is finite dimensional. Indeed, the set of monomials $X_1^{i_1} \ldots X_n^{i_n}$ in $n$ variables and of total degree $i$ (i.e. $i_1 + \cdots + i_n = i$) is a finite set. □

**Lemma 4.2.2.** *Let* $R$ *be a Noetherian complete equicharacteristic local ring, let* $K$ *be a field of representatives of* $R$ *and let* $\{a_1, \ldots, a_d\}$ *be a generator set for* $\mathfrak{m}$. *Then, any element of* $R$ *can be written as a power series in the* $a_i$*'s with coefficients in* $K$.

*Proof.* Take $x \in R$, then we can write it as $x = x_0 + y_1$ where $x_0 \in K$ and $y_1 \in \mathfrak{m}$. Now, repeating the process and according to Lemma 4.2.1 then $y_1 = x_1 + y_2$, where $x_1$ is a $K$-linear combination of the $a_i$'s and $y_2 \in \mathfrak{m}^2$. Thus, $x = x_0 + x_1 + y_2$. Repeating this process $n$ times, we get $x = x_0 + x_1 + \cdots + x_n + y_{n+1}$, where each $x_j$ is a $K$-linear combination of monomials of degree $j$ in the $a_i$'s and $y_{n+1} \in \mathfrak{m}^{n+1}$. Set $u_n = x_1 + \cdots + x_n$. Clearly, by construction $(u_n)_{n\in\mathbb{N}}$ is a Cauchy sequence. Since $R$ is complete there exists $\lim_{n\to\infty} u_n$ and then according to Krull's intersection theorem

$$x - \lim_{n\to\infty} u_n = \lim_{n\to\infty} (x - u_n) = \lim_{n\to\infty} y_{n+1} = 0.$$

Therefore,

$$x = \lim_{n\to\infty} u_n = \sum_{k=0}^{\infty} x_k = \sum_{k=0}^{\infty} \lambda_k Q_k(a_1, \ldots, a_d),$$

where $Q_k \in K[X_1, \ldots, X_d]$ is a homogeneous polynomial of degree $k$ and $\lambda_k \in K$. Thus, $x$ is a power series in the $a_i$'s. □

**Theorem 4.2.3** (Cohen's structure theorem I)**.** *Let $R$ be a Noetherian complete equicharacteristic local ring. Then $R$ is isomorphic to the quotient of a power series ring over the field of representatives with a suitable ideal $\mathfrak{I}$. That is,*

$$R \cong K[[X_1, \ldots, X_n]]/\mathfrak{I}.$$

*Proof.* Let $\{a_1, \ldots, a_n\}$ be a generator set for $\mathfrak{m}$ and let $K$ be a field of representatives of $R$. Firstly, we consider the map $\psi$ which is defined by the universal property ($R$ is complete with the $\mathfrak{m}$-adic topology), imposing the following:

$$\psi \colon K[[X_1, \ldots, X_n]] \to R$$

$$X_1 \mapsto a_1$$

$$\ldots$$

$$X_n \mapsto a_n$$

And naturally $\psi|_K = 1_K$.

This is a well-defined evaluation homomorphism and following Lemma 4.2.2 then $\psi$ is surjective. Indeed, any element of $R$ can be written as a power series in the $a_i$'s with coefficients in $K$. Indeed, for any $a \in R$ there exists some polynomials $Q_j$ such that

$$a = \sum_{j=0}^{\infty} \lambda_j Q_j(a_1, \ldots, a_n).$$

Hence, if we consider

$$a(X_1,\dots,X_n)=\sum_{j=0}^{\infty}\lambda_j Q_j(X_1,\dots,X_n)\in K[[X_1,\dots,X_n]],$$

then

$$\psi(a(X_1,\dots,X_n))=\sum_{j=0}^{\infty}\lambda_j Q_j(a_1,\dots,a_n)=a.$$

Secondly, denote $\mathfrak{J}=\ker\psi$ and according to the first isomorphism theorem we get

$$R\cong K[[X_1,\dots,X_n]]/\mathfrak{J}.$$

Hence, we are done. □

Note that since $\mathfrak{m}$ is an $\mathfrak{m}$-primary ideal, then by Proposition 3.1.18 the above integer $n$ satisfies $n\geq\dim R$. Moreover, we conclude that every Noetherian complete equicharacteristic local ring is the homomorphic image of a complete regular ring, i.e., a power series ring over a field.

### 4.2.2 Cohen's structure theorem in integral domains

If we add the condition that $R$ is an integral domain (which in a local ring is less than being regular) to the above conditions, we are even closer to the structure of power series rings. Indeed, $R$ contains a copy of a power series ring over a field. As usually we ought to start by proving some lemmas.

**Lemma 4.2.4.** *Let $(R,\mathfrak{m})$ be a Noetherian complete local ring and let $M$ be an $R$-module such that $\mathfrak{m}M$ satisfies Krull's intersection theorem. If $M/\mathfrak{m}M$ is a finitely generated $R$-module. Then $M$ is a finitely generated $R$-module.*

*Proof.* We shall prove that whenever the residue classes of $m_1,\dots,m_s$ generate $M/\mathfrak{m}M$ then the elements $m_1,\dots,m_s$ generate $M$.

We begin by defining $A=\{\sum_{i=1}^{s}rm_i\mid r\in R\}\subseteq M$. Now in order to prove the reverse inclusion, we consider any $c\in M$. By assumption there are some elements $\alpha_{i1}\in R$, $(i=1,\dots,s)$ for which $c-\sum_{i=1}^{s}\alpha_{i1}m_i\in\mathfrak{m}M$. Indeed, if $\overline{c}$ denotes the residue class modulo $\mathfrak{m}M$ of $c$, then by hipothesis $\overline{c}=\sum_{i=1}^{s}\alpha_{i1}\overline{m_i}$, for some $\alpha_{i1}\in R$.

Thus, we define $a_1=\sum_{i=1}^{s}\alpha_{i1}m_i$. Consider $k>1$ and suppose inductively that we have defined elements $a_1,\dots,a_k$ satisfying

- $a_l=\sum_{i=1}^{s}\alpha_{il}m_i$, $\alpha_{il}\in\mathfrak{m}^{l-1}$.
- $c-\sum_{j=1}^{l}a_j\in\mathfrak{m}^lM$.

(notice that $a_1$ satisfies both conditions). Then because of the second condition

$$c - \sum_{j=1}^{k} a_j = \sum_{l \in L} \alpha_l b_l, \quad \alpha_l \in \mathfrak{m}^k \text{ where and } b_l \in M.$$

Now we can repeat the argument used in the case of $k = 1$ for each $b_l$. Hence, for each $l \in L$ there exists $d_l \in A$ such that $b_l - d_l \in \mathfrak{m}M$. Now we will consider $a_{k+1} = \sum_{l \in L} \alpha_l d_l$. Then both conditions are satisfied. On the one hand, since $\alpha_l \in \mathfrak{m}^k$, there exist some suitable $\alpha_{i,k+1} \in \mathfrak{m}^k$ such that

$$a_{k+1} = \sum_{i=1}^{s} \alpha_{i,k+1} m_i, \ \alpha_{i,k+1} \in \mathfrak{m}^k M.$$

On the other hand,

$$c - \sum_{j=1}^{k+1} a_j = \sum_{l \in L} \alpha_l b_l - \sum_{l \in L} \alpha_l d_l = \sum_{l \in L} \alpha_l (b_l - d_l) \in \mathfrak{m}^k \mathfrak{m} M = \mathfrak{m}^{k+1} M.$$

Therefore, we have a sequence $(a_k)_{k \in \mathbb{N}}$. Since $R$ is complete, for each $i = 1, \ldots, s$ according to Proposition 1.4.8 we are allowed to define the values $\alpha_i^* = \sum_{j=1}^{\infty} \alpha_{ij} \in R$ and $a = \sum_{i=1}^{s} \alpha_i^* m_i \in A$. Furthermore,

$$\begin{aligned} c - a &= \lim_{k \to \infty} \left( c - \sum_{i=1}^{s} \left( \sum_{j=1}^{k} \alpha_{ij} \right) m_i \right) \\ &= \lim_{k \to \infty} \left( c - \sum_{j=1}^{k} \left( \sum_{i=1}^{s} \alpha_{ij} m_i \right) \right) \\ &= \lim_{k \to \infty} \left( c - \sum_{j=1}^{k} a_j \right) = 0. \end{aligned}$$

Using the conditions over the coefficients $a_i$ and Krull's intersection theorem for the ideal $\mathfrak{m}M$. Thus, $c = a \in A$ and so $M = A$. Hence, $M$ is finitely generated over $R$. □

**Lemma 4.2.5.** *Let $A$ and $B$ be $R$-modules. Suppose that there exists a $R$-module epimorphism $f \colon A \to B$ and that $A$ is finitely generated as an $R$-module. Then $B$ is a finitely generated $R$-module.*

*Proof.* We shall see that if $A$ is generated by $\{a_1, \ldots, a_s\}$ as $R$-module, then $B$ is generated by $\{f(a_1), \ldots, f(a_s)\}$ as $R$-module.

Consider $b \in B$, since $f$ is surjective then there exists $a \in A$ such that $f(a) = b$. There exist some $r_1, \ldots, r_s$ such that $a = r_1 a_1 + \cdots + r_s a_s$. Then $b = f(a) = f(r_1 a_1 + \cdots + r_s a_s) = r_1 f(a_1) + \cdots + r_s f(a_s)$. Hence we are done. □

**Lemma 4.2.6.** *Let $(R, \mathfrak{m})$ be a Noetherian complete equicharacteristic local integral domain of dimension $d$, let $K$ be one of its field of representatives, let $\{a_1, \dots, a_d\}$ be a system of parameters of $R$ and consider the map*

$$\varphi\colon K[[X_1, \dots, X_d]] \to R,$$

*defined by $\varphi(X_i) = a_i$ for all $i = 1, \dots, d$ and $\varphi|_K = 1_K$. Then,*

(i) *$R$ is a finitely generated $\varphi(R)$-module and*

(ii) *$\varphi$ is a monomorphism.*

*Proof.* Denote $S = \operatorname{im}\varphi$ and notice that $K \subseteq S$. Firstly, notice that $R$ is complete with the $\mathfrak{m}$-adic topology and $a_i \in \mathfrak{m}$, so $\varphi$ is a well defined evaluation homomorphism.

(i) Define the ideal $\mathfrak{n} = (a_1, \dots, a_d) \subseteq R$. Firstly $S$ is complete with the $\mathfrak{n}$-adic topology. Indeed, let $(y_n)_{n\in\mathbb{N}}$ be a Cauchy sequence in $S$. Since $S = \operatorname{im}\varphi$ for each $y_n$ there exists a $Y_n \in K[[X_1, \dots, X_d]]$ such that $\varphi(Y_n) = y_n$. Moreover, since $y_n \in \mathfrak{n}^k$ we can choose $Y_n \in \mathfrak{M}^k$. Hence by construction $(Y_n)_{n\in\mathbb{N}}$ is a Cauchy sequence in $K[[X_1, \dots, X_d]]$ with respect to the $\mathfrak{M} = (X_1, \dots, X_d)$-adic topology.

Moreover, $K[[X_1, \dots, X_d]]$ is complete with the $\mathfrak{M}$-adic topology. Thus, $(Y_n)_{n\in\mathbb{N}}$ converges to some $Y$, that is,

$$\forall k \in \mathbb{N} \;\; \exists n_0 \in \mathbb{N} \text{ such that } \forall n \geq n_0 \;\; Y_n - Y \in \mathfrak{M}^k.$$

Thus consider $y = \varphi(Y) \in S$, then

$$\forall k \in \mathbb{N} \;\; \exists n_0 \in \mathbb{N} \text{ such that } \forall n \geq n_0$$

$$y_n - y = \varphi(Y_n) - \varphi(Y) = \varphi(Y_n - Y) \in \varphi(\mathfrak{M}^k) = \mathfrak{n}^k.$$

Therefore, the sequence $(y_n)_{n\in\mathbb{N}}$ converges to $y \in S$, so $S$ is complete with the $\mathfrak{n}$-adic topology.

Furthermore, $\mathfrak{m}^k \subseteq \mathfrak{n} \subseteq \mathfrak{m}$, for some $k > 0$. Indeed, $\mathfrak{n}$ is an $\mathfrak{m}$-primary ideal and $\mathfrak{m} = (x_1, \dots, x_n)$ is finitely generated. Hence, $\operatorname{Rad}\mathfrak{n} = \mathfrak{m}$ and for each $i = 1, \dots, n$ there exists $k_i$ such that $x_i^{k_i} \in \mathfrak{n}$. Consider the integer $l = \max_{i=1,\dots,n} k_i$, then for any $x \in \mathfrak{m}$ we have that $x^{(n-1)l+1} \in \mathfrak{n}$. Indeed, since $x \in \mathfrak{m}$, there exists $i = 1, \dots, n$ such that $x^{(n-1)l+1} = x_i^l y \in \mathfrak{n}$. Hence, choose $k = (n-1)l + 1$ such that $\mathfrak{m}^k \subseteq \mathfrak{n}$.

Thus the exists a surjective map from $R/\mathfrak{m}^k$ onto $R/\mathfrak{n}$. Therefore, applying Lemma 4.2.5 in order to prove that $R/\mathfrak{n}$ is a finitely generated $S$-module,

it is enough to prove the same for $R/\mathfrak{m}^k$. It can be done by induction on $k$.

When $k = 1$, then $R/\mathfrak{m} \cong K$. Moreover, it is a finitely generated $K$-module and $K \subseteq S$, so $R/\mathfrak{m}$ is a finitely generated $S$-module. Suppose inductively that the hypothesis is fulfilled for $k$. Then, $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ is a finitely generated $K$-vector space, by Lemma 4.2.1. In particular it is a finitely generated $S$-module. Hence, since $R/\mathfrak{m}^k$ and $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ are finitely generated $S$-modules so is $R/\mathfrak{m}^{k+1}$. Indeed, we know that both $R/\mathfrak{m}^k$ and $\mathfrak{m}^k/\mathfrak{m}^{k+1}$ are finitely generated $S$-modules and by the third isomorphism theorem

$$R/\mathfrak{m}^k \cong (R/\mathfrak{m}^{k+1})/(\mathfrak{m}^k/\mathfrak{m}^{k+1}).$$

Hence, $R/\mathfrak{m}^{k+1}$ is also finitely generated as an $S$-module.

Therefore, according to Lemma 4.2.4 since $R/\mathfrak{n}$ is a finitely generated $S$-module, $(S, \mathfrak{n})$ is complete and $\mathfrak{n}R$ satisfies the Krull intersection theorem, then $R$ is finitely generated as an $S$-module.

(ii) Since $R$ is a finitely generated $S$-module then $S \subseteq R$ is an integral ring extension. By Exercise 6 $\dim S \geq \dim R$. Furthermore, since $R$ is an integral domain then $\ker\varphi$ is a prime ideal. Indeed, by the first isomorphism theorem $K[[X_1, \ldots, X_d]]/\ker\varphi$ is isomorphic to $S \subseteq R$, which is an integral domain (as a subring of the integral domain $R$) and so $\ker\varphi$ is a prime ideal.

Now if $\ker\varphi \neq \{0\}$, then

$$\dim K[[X_1, \ldots, X_d]]/\ker\varphi < \dim K[[X_1, \ldots, X_d]].$$

Indeed, say $d' = \dim K[[X_1, \ldots, X_d]]/\ker\varphi$, then there exists a chain of prime ideals

$$\tilde{\mathfrak{p}}_0 \subsetneq \tilde{\mathfrak{p}}_1 \subsetneq \cdots \subsetneq \tilde{\mathfrak{p}}_{d'}.$$

Obviously $\tilde{\mathfrak{p}}_0 = \{0\}$. Indeed, the quotient ring $K[[X_1, \ldots, X_d]]/\ker\varphi$ is an integral domain. Hence, by the correspondence theorem there exist some ideals $\mathfrak{p}_i$ of $K[[X_1, \ldots, X_d]]$ such that $\ker\varphi \subseteq \mathfrak{p}_i$ and $\mathfrak{p}_i/\ker\varphi = \tilde{\mathfrak{p}}_i$. Therefore,

$$\{0\} \subsetneq \ker\varphi \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_{d'}$$

is a chain of prime ideals and so

$$\dim K[[X_1, \ldots, X_d]] \geq d' + 1 > \dim K[[X_1, \ldots, X_d]]/\ker\varphi.$$

Finally, the result follows directly from the fact $\dim K[[X_1, \ldots, X_d]] = \dim R$. Indeed, both have dimension $d$. Suppose by contradiction that $\ker\varphi \neq \{0\}$, then by the two previous remarks

$$\dim R \leq \dim S = \dim K[[X_1, \ldots, X_d]]/\ker\varphi < \dim K[[X_1, \ldots, X_d]],$$

which is a contradiction. Hence, $\ker\varphi = \{0\}$ and $\varphi$ is injective. □

Now proving the second version of Cohen's structure theorem is straightforward.

**Theorem 4.2.7** (Cohen's structure theorem II)**.** *Let $R$ be a Noetherian complete equicharacteristic local integral domain of dimension $d$. Then there exists a subring $S \subseteq R$ such that the following holds:*

*(i) $S$ is isomorphic to $K[[X_1, \ldots, X_d]]$ where $K$ is the field of representatives.*

*(ii) Both $R$ and $S$ have the same residue field.*

*(iii) $R$ is a finitely generated $S$-module.*

*Proof.* Let $\{a_1, \ldots, a_d\}$ be a system of parameters of $R$ and consider the ring homomorphism $\varphi : K[[X_1, \ldots, X_d]] \to R$ defined in Lemma 4.2.6. Then $S = \varphi(R)$ is a subring of $R$ that satisfies the following:

(i) By Lemma 4.2.6, $\varphi$ is injective, so according to the first isomorphism theorem

$$S = \operatorname{im} \varphi \cong K[[X_1, \ldots, X_d]] / \ker \varphi \cong K[[X_1, \ldots, X_d]].$$

(ii) Once we know that $S \cong K[[X_1, \ldots, X_d]]$ its residue field is $K$.

(iii) By Lemma 4.2.6, $R$ is a finitely generated $S$-module.

Hence we are done. □

## 4.3 Regular case

An ideal situation will be the one in which the above maps are bijective. Well, regularity will provide us that result. In this theorem we can combine the two previous results, taking into account that when $R$ is regular, a system of parameters of $R$ at the same time generates $\mathfrak{m}$. Therefore, we have the surjectivity and the injectivity together.

Before starting, remember that by definition regularity implies locality.

**Theorem 4.3.1** (Cohen's structure theorem III)**.** *Let $R$ be a Noetherian complete equicharacteristic regular ring of dimension $d$. Then $R$ is isomorphic to the power series ring of $d$ indeterminates over a field of representatives:*

$$R \cong K[[X_1, \ldots, X_d]].$$

*Proof.* Since $R$ is a regular ring we have a system of parameters $\{a_1, \dots a_d\}$ which generates $\mathfrak{m}$. Now, if we define the ring homomorphism

$$\psi \colon K[[X_1, \dots, X_d]] \to R$$

as in Theorem 4.2.3 or as in Lemma 4.2.6, then $\psi$ is an isomorphism. Indeed, since the system of parameters generates $\mathfrak{m}$, then $\psi$ is surjective (Lemma 4.2.2). Moreover, since $R$ is a Noetherian regular ring by Theorem 3.2.9 it is an integral domain. Thus, according to Lemma 4.2.6 then $\psi$ is injective. Therefore,

$$R \cong K[[X_1, \dots, X_d]].$$

□

**Corollary 4.3.2.** *Let $R$ be a Noetherian complete equicharacteristic regular ring. Then $R$ is a unique factorization domain.*

*Proof.* By the above theorem $R$ is isomorphic to a power series ring over a field. Since power series rings over a field are unique factorization domains (Theorem 2.4.9), then $R$ is also a unique factorization domain. □

This corollary, which is a direct consequence of Cohen structure theorem, was independently proved by Auslander, Buchsbaum and Nagata in the 1950s.

Finally, it is important to highlight the fact that the Cohen's structure theorem is much more extensive, since it covers the non-equicharacteristic case. Unfortunately, the development of this theory exceeds the limits of this work both in difficulty and extension.

In the non-equicharacteristic case, $R$ may not contain any subring isomorphic to the residue field. Nevertheless, it contains a special subring, called Cohen-Macaulay subring, and the overall result could be expressed as:

**Theorem 4.3.3** (Cohen's structure theorem IV)**.** *Let $R$ be a Noetherian complete local ring of dimension $d$. Then,*

*1) there exists a Cohen-Macaulay ring $\Lambda$ such that*

$$R \cong \Lambda[[X_1, \dots, X_n]]/\mathfrak{I}$$

*for a suitable ideal $\mathfrak{I} \subseteq \Lambda[[X_1, \dots, X_n]]$ and a suitable integer $n$. Moreover, in the equicharacteristic case $\Lambda$ is a field of representatives.*

*2) In addition, when $R$ is an integral domain, then there exists a subring $S \subseteq R$ such that the following holds:*

*(i)* *$S$ is isomorphic to $\Lambda[[X_1, \ldots, X_d]]$ where $\Lambda$ is a Cohen-Macaulay ring. Moreover, in the equicharacteristic case $\Lambda$ is a field of representatives.*

*(ii)* *Both $R$ and $S$ have the same residue field.*

*(iii)* *$R$ is a finitely generated $S$-module.*

*3) In addition, when $R$ is regular then $R$ is isomorphic to $\Lambda[[X_1, \ldots, X_d]]$ where $\Lambda$ is a Cohen-Macaulay ring. Moreover, in the equicharacteristic case $\Lambda$ is a field of representatives.*

To alleviate the curiosity of the reader, the demonstration of this theorem can be read in [1].

# Appendix A

# Solved exercises

The prime avoidance theorem is a basic result of Commutative Algebra, which is used several times in these notes. It will be proved here, as an exercise.

**Exercise 1** (Prime avoidance theorem)**.** Let $R$ be a commutative ring, let $\{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$ $(s \geq 2)$ be a set of ideals such that at most two of them ($\mathfrak{p}_1$ and $\mathfrak{p}_2$) are not prime and let $\mathfrak{a}$ be an ideal of $R$, such that

$$\mathfrak{a} \subseteq \bigcup_{i=1}^{s} \mathfrak{p}_i.$$

Prove that $\mathfrak{a} \subseteq \mathfrak{p}_j$ for some $j \in \{1, \ldots, s\}$.

*Solution.* We proceed by induction over $s$. When $s = 2$, suppose by contradiction that $\mathfrak{a} \subseteq \mathfrak{p}_1 \cup \mathfrak{p}_2$ but $\mathfrak{a} \nsubseteq \mathfrak{p}_i$ for all $i = 1, 2$. Then there exist two elements $a_i$ such that $a_i \in \mathfrak{a} \setminus \mathfrak{p}_i$, so $a_1 \in \mathfrak{p}_2$ and $a_2 \in \mathfrak{p}_1$. Then, $a_1 + a_2 \in \mathfrak{a} \subseteq \mathfrak{p}_1 \cup \mathfrak{p}_2$. Hence, $a_1 + a_2$ belongs either to $\mathfrak{p}_1$ or to $\mathfrak{p}_2$. In the first case

$$a_1 = (a_1 + a_2) - a_2 \in \mathfrak{p}_1,$$

which is a contradiction. In the second case ($a_1 + a_2 \in \mathfrak{p}_2$), in a similar way we get that $a_2 \in \mathfrak{p}_2$, which is also a contradiction. Thus, $\mathfrak{a} \subseteq \mathfrak{p}_j$ for some $j = 1, 2$.

Now, suppose inductively that the result has been proved for $s = k$ and $\mathfrak{a} \subseteq \bigcup_{i=1}^{k+1} \mathfrak{p}_i$. Then suppose by contradiction that for any $j = 1, \ldots, k+1$

$$\mathfrak{a} \nsubseteq \bigcup_{i \neq j} \mathfrak{p}_i,$$

so for each $j = 1, \ldots, k+1$, there exists

$$a_j \in \mathfrak{a} \setminus \bigcup_{i \neq j} \mathfrak{p}_i.$$

Clearly, $a_j \in \mathfrak{p}_j$ for each $j$ and $a_j \notin \mathfrak{p}_i$ for any $i \neq j$. Now define $b = a_1 \dots a_k + a_{k+1}$. Then $b \notin \mathfrak{p}_{k+1}$, otherwise

$$a_1 \dots a_k = a_1 \dots a_k + a_{k+1} - a_{k+1} = b - a_{k+1} \in \mathfrak{p}_{k+1}.$$

Since $\mathfrak{p}_{k+1}$ is a prime ideal (indeed $k+1 \geq 3$), then there exists an element $a_j \in \mathfrak{p}_{k+1}$ for some $j = 1, \dots, k$, which is impossible. On the other hand, $b \notin \mathfrak{p}_j$ for any $j \neq k+1$. Otherwise,

$$a_{k+1} = b - a_1 \dots a_k \in \mathfrak{p}_j,$$

which is impossible. But since $b \in \mathfrak{a}$ is not contained in $\bigcup_{i=1}^{k+1} \mathfrak{p}_i$, we have a contradiction with the initial hypothesis. Hence, there exists $j = 1, \dots, k+1$ such that

$$\mathfrak{a} \subseteq \bigcup_{i \neq j} \mathfrak{p}_i.$$

Therefore, by induction hypothesis there exists $l = 1, \dots k+1$ such that

$$\mathfrak{a} \subseteq \mathfrak{p}_l.$$

This completes the inductive step and so the statement is proved. □

**Exercise 2.** Let $K$ be a field. Show that

$$K[[X_1, \dots, X_n]]/(X_1, \dots, X_n) \cong K$$

and conclude that $(X_1, \dots, X_n)$ is a maximal ideal.

*Solution.* Denote $R_n = K[[X_1, \dots, X_n]]$. Firstly we shall prove this identity

$$(X_1, \dots, X_n) = \{a \in R_n \mid a_{0,\dots,0} = 0\}. \tag{A.1}$$

$\subseteq$) Consider $a \in (X_1, \dots, X_n)$. Then there exist some $b_i(X_1, \dots, X_n) \in R_n$ $(i = 1, \dots, n)$ such that

$$a(X_1, \dots, X_n) = b_1(X_1, \dots, X_n)X_1 + \dots + b_n(X_1, \dots, X_n)X_n,$$

so by comparing constant terms

$$a_{0,\dots,0} = \sum_{i=1}^{n} b_i(0, \dots, 0)0 = 0.$$

$\supseteq$) Consider some $a \in R_n$ such that $a_{0,\dots 0} = 0$. Then we can separate the powers in which $X_1$ appears and those where it does not appear, that is,

$$a = a_1(X_1, \dots, X_n)X_1 + \tilde{a}_2(X_2, \dots, X_n).$$

Repeating the process in $\tilde{a}_2$ for $X_2$, then

$$a = a_1(X_1, \ldots, X_n)X_1 + a_2(X_2, \ldots, X_n)X_2 + \tilde{a}_3(X_3, \ldots, X_n).$$

Hence, in a finite number of steps, we obtain some $a_1, \ldots, a_n \in R_n$, such that,

$$a = a_1X_1 + \cdots + a_nX_n \implies a \in (X_1, \ldots, X_n).$$

Now we are ready to prove the isomorphism. Since $K$ is a field, it is complete with respect to the $\{0\}$-adic topology, and so the following evaluation homomorphism $\varphi$ is well-defined by Proposition 2.3.10:

$$\varphi\colon K[[X_1, \ldots, X_d]] \to K$$

$$X_1 \mapsto 0$$

$$\ldots$$

$$X_n \mapsto 0.$$

Moreover, this map is surjective. Indeed, set $k \in K$, and consider $k = k + \sum_{i_1,\ldots i_n \geq 0} 0X_1^{i_1} \ldots X_n^{i_n} \in K[[X_1, \ldots, X_n]]$ such that $\varphi(k) = k$. Then $K \subseteq \operatorname{im}\varphi$ and so $\varphi$ is an epimorphism.

On the other hand, $\ker\varphi = (X_1, \ldots, X_n)$.

$\subseteq$) Consider $a \in \ker\varphi$, then

$$0 = \varphi(a) = \sum_{i_1,\ldots,i_n \geq 0} a_{i_1,\ldots,i_n} 0^{i_1} \ldots 0^{i_n} = a_{0,\ldots,0},$$

so by (A.1) then $a \in (X_1, \ldots, X_n)$.

$\supseteq$) Consider $a \in (X_1, \ldots, X_n)$. Then, $a = a_1X_1 + \ldots a_nX_n$ for some $a_i \in R_n$. Thus $\varphi(a) = a_10 + \cdots + a_n0 = 0$. Hence $(X_1, \ldots, X_n) \subseteq \ker\varphi$.

Finally according to the first isomorphism theorem,

$$K[[X_1, \ldots, X_n]]/(X_1, \ldots, X_n) \cong K.$$

Now since the quotient is a field, it follows that $(X_1, \ldots, X_n)$ is a maximal ideal. □

**Exercise 3.** Let $K$ be a field and say $R_n = K[[X_1, \ldots, X_n]]$. The aim of this exercise is to show that for any power series $f$ there exists an automorphism $\varphi\colon R_n \to R_n$ such that $\varphi(f)$ is regular. Hence, this exercise is fundamental in order to prove Theorem 2.4.9.

(i) Show that the map $\varphi\colon R_n \to R_n$ sending $X_i$ to $X_i + X_n^{m_i}$ for $1 \leq i < n$ and fixing $X_n$ defines an automorphism of $R_n$ (the $m_i \in \mathbb{N} \cup \{0\}$ are fixed).

(ii) Fix $f \in R_n$, which is non-zero and which is not a unit. Show that one can choose $m_1, \ldots, m_{n-1}$ such that $f$ is mapped to a regular element.

*Solution.* (i) First of all notice that $R_n$ is complete with the $(X_1, \ldots, X_n)$-adic topology and for each $i = 1, \ldots, n-1$ then $X_i + X_n^{m_i} \in (X_1, \ldots, X_n)$. Thus, according to Proposition 2.3.10 the preceding map $\varphi$ is a well-defined evaluation homomorphism.

Moreover, the evaluation homomorphism defined by $\psi(X_i) = X_i - X_n^{m_i}$ for all $i = 1, \ldots, n-1$ and $\psi(X_n) = X_n$ is the inverse of $\varphi$. Therefore, $\varphi$ is an automorphism of $R_n$.

(ii) Let $f$ be a power series which is not zero or a unit. Now we shall fix the values of $m_i$ for $\tilde{f} = \varphi(f)$ be a regular power series. We are going to consider two cases.

*Case 1.* When $f$ is a regular power series of order $s$, it is enough considering $m_i = 0$ for all $i = 1, \ldots, n-1$ and $\varphi = 1_{R_n}$.

*Case 2.* In this case $f$ is not a regular power series. We have

$$\tilde{f} = \varphi(f) = f(X_1 + X_n^{m_1}, \ldots, X_{n-1} + X_n^{m_{n-1}}, X_n)$$

Hence,

$$\tilde{f}(0, \ldots, 0, X_n) = f(X_n^{m_1}, \ldots, X_n^{m_{n-1}}, X_n)$$

will be a power series in $X_n$. Moreover, define $\mathcal{I} = \{(i_1 \ldots, i_n) \mid a_{i_1,\ldots,i_n} \neq 0\}$, then $\tilde{f}$ will be a regular power series of order $s$, where

$$s \geq \min\{i_1 m_1 + \cdots + i_{n-1} m_{n-1} + i_n \mid (i_1 \ldots, i_n) \in \mathcal{I}\}. \tag{A.2}$$

Well, $\tilde{f}(0, \ldots, 0, X_n)$ is a power series in $X_n$, but is it a non-zero power series? Define

$$\mathcal{A}_j = \{a_{i_1,\ldots,i_n} \mid i_1 m_1 + \cdots + i_{n-1} m_{n-1} + i_n = j\}.$$

This is finite, because the natural number $j$ is fixed. Then the coefficient of $X_n^j$ is $\sum_{a \in \mathcal{A}_j} a$. Hence, even though there are monomials of total degree $j$, then their sum can be 0 and so $\tilde{f}(0, \ldots, 0, X_n)$ can be the zero power series. However, we can find a combination of $(m_1, \ldots, m_{n-1}) \in (\mathbb{N} \cup \{0\})^{n-1}$ such that $\tilde{f}(0, \ldots, 0, X_n) \neq 0$.

Indeed, we will define an order relation in the monomials such that $X_1^{i_1}\dots X_n^{i_n} < X_1^{j_1}\dots X_n^{j_n}$ if and only if there exists $k \in \mathbb{N}$ such that $i_l = j_l$ for $l = 1, \dots, k-1$ and $i_k < j_k$. Then let $a_{d_1,\dots,d_n}$ be the minimum (with the above order) non-zero coefficient of $f$. Since $f$ is not a unit, then $a_{0,\dots,0} = 0$ and so $(d_1, \dots, d_n) \neq (0, \dots, 0)$.

Consider $d = \max_{i=1,\dots,n} d_i > 0$ and choose $m_i = (nd)^{n-i}$. Then the image of the monomial term $a_{d_1,\dots,d_n} X_1^{d_1}\dots X_n^{d_n}$ by $\varphi$ (evaluated in $(0, \dots, 0, X_n)$) is

$$a_{d_1,\dots,d_n} X_n^{d_1 m_1 + \dots + d_{n-1} m_{n-1} + d_n}. \tag{A.3}$$

We shall prove that this term is not cancelled with any other term. So proving that for any $(i_1, \dots, i_n) \in (\mathbb{N} \cup \{0\})^n$

$$i_1 m_1 + \dots + i_{n-1} m_{n-1} + i_n > d_1 m_1 + \dots + d_{n-1} m_{n-1} + d_n \tag{A.4}$$

is enough. By the election of the $d_i$'s there exists an $l = 1, \dots, n$ such that $i_j = d_j$, when $j < l$ and $i_l > d_l$. Then subtracting both expressions in (A.4), since $i_j = d_j$ when $j < l$, we get

$$(i_l - d_l) m_l + \sum_{j=l+1}^{n} (i_j - d_j) m_j = (i_l - d_l) m_l + \sum_{j=l+1}^{n} i_j m_j - \sum_{j=l+1}^{n} d_j m_j,$$

where $m_n = 1$. Since $i_l > d_l$ then $(i_l - d_l) m_l \geq m_l$, so we should take care about the negative terms only.

$$\sum_{j=l+1}^{n} d_j m_j \leq (n-1) d \max_{j \geq l+1} m_j < n d m_{l+1} = n d (nd)^{n-l-1} = (nd)^{n-l} = m_l.$$

Hence,

$$(i_l - d_l) m_l + \sum_{j=l+1}^{n} i_j m_j - \sum_{j=l+1}^{n} d_j m_j > m_l + \sum_{j=l+1}^{n} i_j m_j - m_l \geq 0.$$

Therefore, the term (A.3) is not cancelled. Then $\tilde{f}(0, \dots, 0, X_n)$ is a non-zero power series ring in $X_n$, so it is a regular power series in $X_n$. □

**Exercise 4.** Let $R$ be a ring and let $\mathfrak{a}$ be an ideal of $R$. The goal of this exercise is to describe the main properties of the radical of $\mathfrak{a}$ defined as

$$\operatorname{Rad} \mathfrak{a} = \{r \in R \mid \exists n \in \mathbb{N} \text{ such that } r^n \in \mathfrak{a}\}.$$

Prove that:

(i) $\operatorname{Rad} \mathfrak{a}$ is an ideal.

(ii) If $\mathfrak{a} \subseteq \mathfrak{b}$ then $\operatorname{Rad}\mathfrak{a} \subseteq \operatorname{Rad}\mathfrak{b}$.

(iii) $\operatorname{Rad}\mathfrak{a} = R$ if and only if $\mathfrak{a} = R$.

(iv) $\operatorname{Rad}(\mathfrak{a}+\mathfrak{b}) = \operatorname{Rad}(\operatorname{Rad}\mathfrak{a} + \operatorname{Rad}\mathfrak{b})$.

(v) If $\mathfrak{a}$ is a primary ideal then $\operatorname{Rad}\mathfrak{a}$ is prime.

(vi) The radical of $\mathfrak{a}$ is the intersection of all the prime ideals containing $\mathfrak{a}$.

$$\operatorname{Rad}\mathfrak{a} = \bigcap_{\mathfrak{p} \text{ prime s.t. } \mathfrak{a}\subseteq\mathfrak{p}} \mathfrak{p}.$$

(vii) For any prime ideal $\mathfrak{p}$ and any $n \in \mathbb{N}$ then $\operatorname{Rad}(\mathfrak{p}^n) = \mathfrak{p}$.

(viii) Let $\mathfrak{a}$ be an ideal such that $\operatorname{Rad}\mathfrak{a} = \mathfrak{m}$ is a maximal ideal. Then $\mathfrak{a}$ is $\mathfrak{m}$-primary. In particular, if $\mathfrak{m}$ is a maximal ideal then $\mathfrak{m}^n$ is an $\mathfrak{m}$-primary ideal for any $n \in \mathbb{N}$.

(ix) Let $\mathfrak{p}$ be a prime ideal. Then conclude from (viii) that the ideal of $R$ defined as $\mathfrak{p}^{(i)} = \mathfrak{p}^i R_{\mathfrak{p}} \cap R$ is a $\mathfrak{p}$-primary ideal.

(x) (Proof of Lemma 3.1.12) Let $(R, \mathfrak{m})$ be a local ring. Then the following conditions are equivalent

(a) $\operatorname{Rad}\mathfrak{a} = \mathfrak{m}$,

(b) $\mathfrak{m}$ is a minimal prime ideal of $\mathfrak{a}$ and

(c) $\mathfrak{a}$ is an $\mathfrak{m}$-primary ideal.

*Solution.* (i) It is straightforward because the conditions that define an ideal are satisfied:

- For any $a \in \mathfrak{a}$, then $a^1 \in \mathfrak{a}$ and so $\mathfrak{a} \subseteq \operatorname{Rad}\mathfrak{a}$. In particular $\operatorname{Rad}\mathfrak{a} \neq \varnothing$.
- Let $a, b \in \operatorname{Rad}\mathfrak{a}$. Then there exist $n, m \in \mathbb{N}$ such that $a^n, b^m \in \mathfrak{a}$. Therefore using Newton's binomial formula

$$\begin{aligned}(a+b)^{n+m} &= \sum_{i=0}^{n+m} \binom{n+m}{i} a^i b^{n+m-i} \\ &= b^m \sum_{i=0}^{n} \binom{n+m}{i} a^i b^{n-i} \\ &+ a^n \sum_{i=n+1}^{n+m} \binom{n+m}{i} a^{i-n} b^{n+m-i} \in \mathfrak{a}.\end{aligned}$$

Hence $a + b \in \operatorname{Rad}\mathfrak{a}$.

- Let $a \in \operatorname{Rad}\mathfrak{a}$ and let $r \in R$. Then there exists $n \in \mathbb{N}$ such that $a^n \in \mathfrak{a}$. Hence $(ar)^n = a^n r^n \in \mathfrak{a}$ and so $ar \in \operatorname{Rad}\mathfrak{a}$.

(ii) Let $\mathfrak{a} \subseteq \mathfrak{b}$ be two ideals of $R$. Let $a \in \operatorname{Rad}\mathfrak{a}$, then there exists $n \in \mathbb{N}$ such that $a^n \in \mathfrak{a} \subseteq \mathfrak{b}$. By definition $a \in \operatorname{Rad}\mathfrak{b}$ and so $\operatorname{Rad}\mathfrak{a} \subseteq \operatorname{Rad}\mathfrak{b}$.

(iii) We shall prove both implications.
$\Rightarrow$) Suppose that $\operatorname{Rad}\mathfrak{a} = R$. Then $1 \in \operatorname{Rad}\mathfrak{a}$, so there exists $n \in \mathbb{N}$ such that $1^n = 1 \in \mathfrak{a}$, so $\mathfrak{a} = R$.
$\Leftarrow$) Suppose that $\mathfrak{a} = R$. Then $R = \mathfrak{a} \subseteq \operatorname{Rad}\mathfrak{a}$, so $\operatorname{Rad}\mathfrak{a} = R$.

(iv) We shall prove both inclusions.
$\subseteq$) Consider $x \in \operatorname{Rad}(\mathfrak{a}+\mathfrak{b})$, then there exists $n \in \mathbb{N}$ such that

$$x^n \in \mathfrak{a}+\mathfrak{b} \subseteq \operatorname{Rad}\mathfrak{a} + \operatorname{Rad}\mathfrak{b}.$$

Therefore $x \in \operatorname{Rad}(\operatorname{Rad}\mathfrak{a} + \operatorname{Rad}\mathfrak{b})$.
$\supseteq$) Consider $x \in \operatorname{Rad}(\operatorname{Rad}\mathfrak{a} + \operatorname{Rad}\mathfrak{b})$. Hence there exists $n \in \mathbb{N}$ such that $x^n \in \operatorname{Rad}\mathfrak{a} + \operatorname{Rad}\mathfrak{b}$. That is, $x^n = y_1 + y_2$, where there exist some $n_1, n_2 \in \mathbb{N}$ such that $y_1^{n_1} \in \mathfrak{a}$ and $y_2^{n_2} \in \mathfrak{b}$. Hence using the Newton binomial formula

$$\begin{aligned} x^{n(n_1+n_2)} = (y_1+y_2)^{n_1+n_2} &= \sum_{i=0}^{n_1+n_2} \binom{n_1+n_2}{i} y_1^i y_2^{n_1+n_2-i} \\ &= y_2^{n_2} \sum_{i=0}^{n_1} \binom{n_1+n_2}{i} y_1^i y_2^{n_1-i} \\ &+ y_1^{n_1} \sum_{i=n_1+1}^{n_1+n_2} \binom{n_1+n_2}{i} y_1^{i-n_1} y_2^{n_1+n_2-i} \in \mathfrak{a}+\mathfrak{b}. \end{aligned}$$

Hence $x \in \operatorname{Rad}(\mathfrak{a}+\mathfrak{b})$.

(v) Let $\mathfrak{a}$ be a primary ideal. Since $\mathfrak{a}$ is proper $1^n = 1 \notin \mathfrak{a}$ for any $n \in \mathbb{N}$, so $1 \notin \operatorname{Rad}\mathfrak{a} = \mathfrak{p}$. Hence $\mathfrak{p}$ is a proper ideal.

Let $ab \in \mathfrak{p}$ but $a \notin \mathfrak{p}$. Then there exists $n \in \mathbb{N}$ such that $(ab)^n = a^n b^n \in \mathfrak{a}$. However $a \notin \operatorname{Rad}\mathfrak{a}$, so $a^n \notin \mathfrak{a}$. Thus since $\mathfrak{a}$ is $\mathfrak{p}$-primary, then there exists $m \in \mathbb{N}$ such that $(b^n)^m = b^{nm} \in \mathfrak{a}$. Hence, $b \in \mathfrak{p}$ and so $\mathfrak{p}$ is prime.

(vi) We shall prove both inclusions.
$\subseteq$) Consider $a \in \operatorname{Rad}\mathfrak{a}$. Then there exists $n \in \mathbb{N}$ such that $a^n \in \mathfrak{a} \subseteq \mathfrak{p}$ for any prime ideal such that $\mathfrak{a} \subseteq \mathfrak{p}$. Since $\mathfrak{p}$ is prime $a \in \mathfrak{p}$ and

$$\operatorname{Rad}\mathfrak{a} \subseteq \bigcap_{\mathfrak{p} \text{ prime s.t. } \mathfrak{a}\subseteq\mathfrak{p}} \mathfrak{p}.$$

$\supseteq$) Consider $a$ in the above intersection and suppose by contradiction that $a \notin \operatorname{Rad}\mathfrak{a}$. Then $\mathfrak{a} \cap S = \varnothing$, where $S$ is the multiplicatively closed subset $S = \{a^n \mid n \in \mathbb{N}\}$. Thus the set

$$\Psi = \{\mathfrak{b} \text{ ideal of } R \mid \mathfrak{a} \subseteq \mathfrak{b} \text{ and } \mathfrak{b} \cap S = \varnothing\}$$

is a partially ordered non-empty set. Hence by the Zorn Lemma it admits a maximal element, say $\mathfrak{p}$. Now we shall prove that $\mathfrak{p}$ is a prime ideal. Consider $c, b \in R \setminus \mathfrak{p}$, we shall prove that $cb \notin \mathfrak{p}$. Since $c \notin \mathfrak{p}$ then $\mathfrak{p} \subsetneq (\mathfrak{p}, c)$. Hence by the maximality of $\mathfrak{p}$ and since $\mathfrak{a} \subseteq (\mathfrak{p}, c)$, we have that $(\mathfrak{p}, c) \cap S \neq \varnothing$. Hence, there exist some $s_1 \in S$, $r_1 \in R$ and $p_1 \in \mathfrak{p}$ such that $s_1 = p_1 + r_1 c$. In a similar way there exist some $s_2 \in S$, $r_2 \in R$ and $p_2 \in \mathfrak{p}$ such that $s_2 = p_2 + r_2 b$. Therefore, $s_1 s_2 = a^{n_1} a^{n_2} = a^{n_1+n_2} \in S$ and

$$s_1 s_2 = (p_1 p_2 + p_1 r_2 b + p_2 r_1 c) + r_1 r_2 cb \in S.$$

Since $p_1 p_2 + r_1 p_2 c + r_2 p_1 b \in \mathfrak{p}$ and $S \cap \mathfrak{p} = \varnothing$, then $cb \notin \mathfrak{p}$. Indeed, if $cb \in \mathfrak{p}$ then $s_1 s_2 \in S \cap \mathfrak{p}$. Thus $\mathfrak{p}$ is a prime ideal such that $\mathfrak{a} \subseteq \mathfrak{p}$, so $a \in \mathfrak{p}$. Thus $a \in S \cap \mathfrak{p} = \varnothing$, which is a contradiction.

(vii) We shall prove both inclusions.
$\supseteq$) Let $p \in \mathfrak{p}$. Then $p^n \in \mathfrak{p}^n$ and so $\mathfrak{p} \subseteq \operatorname{Rad}(\mathfrak{p}^n)$.
$\subseteq$) Let $a \in \operatorname{Rad}(\mathfrak{p}^n)$. Then there exists some $m \in \mathbb{N}$ such that $a^m \in \mathfrak{p}^n \subseteq \mathfrak{p}$. Now $\mathfrak{p}$ is a prime ideal, so $a \in \mathfrak{p}$.

(viii) Since $\mathfrak{a} \subseteq \operatorname{Rad}\mathfrak{a} = \mathfrak{m}$ and $\mathfrak{m}$ is a maximal ideal then $\mathfrak{a}$ is a proper ideal. Now let $a, b \in R$ such that $ab \in \mathfrak{a}$ and $b \notin \operatorname{Rad}\mathfrak{a} = \mathfrak{m}$. Then by the maximality condition $\mathfrak{m} + (b) = R$. Since $\mathfrak{m} + (b) \subseteq \mathfrak{m} + \operatorname{Rad}(b)$ then

$$R = \operatorname{Rad} R = \operatorname{Rad}(\mathfrak{m} + (b)) \subseteq \operatorname{Rad}(\mathfrak{m} + \operatorname{Rad}(b)),$$

so $\operatorname{Rad}(\mathfrak{m} + \operatorname{Rad}(b)) = R$. On the other hand,

$$\operatorname{Rad}(\mathfrak{a} + (b)) = \operatorname{Rad}(\operatorname{Rad}\mathfrak{a} + \operatorname{Rad}(b)) = \operatorname{Rad}(\mathfrak{m} + \operatorname{Rad}(b)) = R,$$

so by (iii) then $\mathfrak{a} + (b) = R$. Hence, there exist some $c \in \mathfrak{a}$ and $r \in R$ such that $1 = c + br$. Therefore,

$$a = a \cdot 1 = ac + abc \in \mathfrak{a},$$

because both $c$ and $ab$ are in $\mathfrak{a}$. Hence $\mathfrak{a}$ is $\mathfrak{m}$-primary.

Furthermore, consider $n \in \mathbb{N}$. When $\mathfrak{m}$ is a maximal ideal by (v) then $\operatorname{Rad}\mathfrak{m}^n = \mathfrak{m}$ which is a maximal ideal, so $\mathfrak{m}^n$ is an $\mathfrak{m}$-primary ideal.

(ix) Let $\mathfrak{p}$ be a prime ideal, let $i \in \mathbb{N}$ and consider the ideal $\mathfrak{p}^{(i)} = \mathfrak{p}^i R_{\mathfrak{p}} \cap R$ of $R$. Firstly, for any $i$ the ideal $\mathfrak{p}^{(i)}$ is proper. Suppose by contradiction

that for some $i \in \mathbb{N}$, $\mathfrak{p}^{(i)}$ is not proper. Then $1 \in \mathfrak{p}^i R_\mathfrak{p} \cap R$ so there exists $x \notin \mathfrak{p}$ such that $x = 1x \in \mathfrak{p}^i \subseteq \mathfrak{p}$, which is clearly a contradiction. Thus, $\mathfrak{p}^{(i)}$ must be a proper ideal.

On the one hand, since $R_\mathfrak{p}$ is a local ring with $\mathfrak{p}R_\mathfrak{p}$ as unique maximal ideal, then by (viii) $\mathfrak{p}^i R_\mathfrak{p}$ is a $\mathfrak{p}R_\mathfrak{p}$-primary ideal. Consider $a, b \in R$ such that $ab \in \mathfrak{p}^{(i)}$ and $a \notin \mathfrak{p}^{(i)}$. Then $ab \in \mathfrak{p}^i R_\mathfrak{p}$ and $a \notin \mathfrak{p}^i R_\mathfrak{p}$, because $a \in R$. Hence, since $\mathfrak{p}^i R_p$ is a primary ideal then there exists $n \in \mathbb{N}$ such that $b^n \in \mathfrak{p}^i R_p$. Therefore, $b^n \in \mathfrak{p}^i R_\mathfrak{p} \cap R$ and so $\mathfrak{p}^{(i)}$ is primary. If we prove that $\operatorname{Rad} \mathfrak{p}^{(i)} = \mathfrak{p}$, we are done.

One inclusion is obvious. Consider $p \in \mathfrak{p}$, then $p^i = p^i \cdot 1 \in \mathfrak{p}^i$ so $p^i \in \mathfrak{p}^i R_\mathfrak{p} \cap R$. Thus $p \in \operatorname{Rad} \mathfrak{p}^{(i)}$. On the other hand, consider $x \in \operatorname{Rad} \mathfrak{p}^{(i)}$, then there exists $n \in \mathbb{N}$ such that $x^n \in \mathfrak{p}^i R_\mathfrak{p} \cap R$. In particular, $x \in \operatorname{Rad} \mathfrak{p}^i R_\mathfrak{p} = \mathfrak{p}R_\mathfrak{p}$. Therefore, there exists some $u \notin \mathfrak{p}$ such that $xu \in \mathfrak{p}$. Finally since $\mathfrak{p}$ is a prime ideal, $u \notin \mathfrak{p}$ and $xu \in \mathfrak{p}$ then $x \in \mathfrak{p}$ and we are done.

(x) We shall prove the equivalence chain.

(a) $\implies$ (b). Firstly $\mathfrak{m}$ is a prime ideal that contains $\mathfrak{a}$. By (vi) it follows that

$$\mathfrak{m} = \operatorname{Rad} \mathfrak{a} = \bigcap_{\mathfrak{p} \text{ prime s.t. } \mathfrak{a} \subseteq \mathfrak{p}} \mathfrak{p}.$$

Then $\mathfrak{m}$ is contained in any prime ideal which contains $\mathfrak{a}$. Let $\mathfrak{p}$ be a minimal prime ideal of $\mathfrak{a}$. Then $\mathfrak{m} \subseteq \mathfrak{p}$ and since $\mathfrak{m}$ is maximal in $R$ then $\mathfrak{m} = \mathfrak{p}$.

(b) $\implies$ (c). Suppose that $\mathfrak{m}$ is a minimal prime ideal of $\mathfrak{a}$, then since the ring is local $\mathfrak{m}$ is the unique minimal prime ideal of $\mathfrak{a}$. Moreover it is the unique prime ideal that contains $\mathfrak{a}$ and so

$$\operatorname{Rad} \mathfrak{a} = \bigcap_{\mathfrak{p} \text{ prime s.t. } \mathfrak{a} \subseteq \mathfrak{p}} \mathfrak{p} = \mathfrak{m}.$$

Now since the radical of $\mathfrak{a}$ is a maximal ideal then by (viii) $\mathfrak{a}$ is an $\mathfrak{m}$-primary ideal.

(c) $\implies$ (a). It is straightforward. Since $\mathfrak{a}$ is an $\mathfrak{m}$-primary ideal, then $\operatorname{Rad} \mathfrak{a} = \mathfrak{m}$. □

**Exercise 5.** Let $K$ be a field. Prove that $\dim K[[X_1, \ldots, X_n]] = n$.

*Solution.* On the one hand, as in Exercise 2 it is easy to see that

$$K[[X_1, \ldots, X_n]]/(X_1, \ldots, X_i) \cong K[[X_{i+1}, \ldots X_n]].$$

On the other hand, $K$ is an integral domain. Thus $K[[X_{i+1},\dots,X_n]]$ is an integral domain for all $i=0,\dots,n-1$. Hence $K[[X_1,\dots,X_n]]/(X_1,\dots,X_i)$ is an integral domain, and so $(X_1,\dots,X_i)$ is a prime ideal for any $1\leq i<n$. Moreover, by Exercise 2 $(X_1,\dots,X_n)$ is a maximal ideal, so it is a prime ideal. Hence the following is a chain of prime ideals of lenght $n$.

$$\{0\}\subsetneq (X_1)\subsetneq (X_1,X_2)\subsetneq\cdots\subsetneq (X_1,\dots,X_n)$$

(note that $\{0\}$ is a prime ideal because $K[[X_1,\dots,X_n]]$ is an ID). Since all the inclusions are strict $\dim K[[X_1,\dots,X_n]]\geq n$.

Furthermore, $K[[X_1,\dots,X_n]]$ is a Noetherian ring and $(X_1,\dots,X_n)$ is a proper ideal which can be generated by $n$ elements. Therefore by Theorem 3.1.13 $\operatorname{ht}(X_1,\dots,X_n)\leq n$. Finally since $K[[X_1,\dots,X_n]]$ is a local ring with maximal ideal $(X_1,\dots,X_n)$, so $\dim K[[X_1,\dots,X_n]]=\operatorname{ht}(X_1,\dots,X_n)\leq n$. Hence $\dim K[[X_1,\dots X_n]]=n$. □

**Exercise 6.** Let $S\subseteq R$ be an integral ring extension. Prove that $\dim R\leq \dim S$. Is it true when the extension $S\subseteq R$ is not integral?

*Solution.* On the one hand, denote $r=\dim R$ and let

$$\mathfrak{p}_0\subsetneq\mathfrak{p}_1\subsetneq\cdots\subsetneq\mathfrak{p}_r$$

be a saturated chain of prime ideals of $R$. Then each $\mathfrak{q}_i=\mathfrak{p}_i\cap S$ is a prime ideal of $S$, and

$$\mathfrak{q}_0\subseteq\mathfrak{q}_1\subseteq\cdots\subseteq\mathfrak{q}_r$$

is a chain of prime ideals of $S$. We shall prove that all the inclusions are strict. Suppose by contradiction that $\mathfrak{q}_{i+1}=\mathfrak{q}_i$ for some $i$, then $\mathfrak{p}_{i+1}=\mathfrak{p}_i$, which is a contradiction. Consider $a\in\mathfrak{p}_{i+1}$. Since $R/\mathfrak{p}_i$ is integral over $S/\mathfrak{q}_i$ then there exist some coefficients $s_i\in S$ such that

$$a^n+s_{n-1}a^{n-1}+\cdots+s_0\equiv 0 \mod \mathfrak{p}_i,$$

and we can assume that $n$ is the lowest possible degree of that polynomial combination. Then $s_0\in S$ and $s_0\equiv -a^n-s_{n-1}a^{n-1}-\cdots-s_1a \mod \mathfrak{p}_i$. Moreover, $a\in\mathfrak{p}_{i+1}$, and it is an ideal so $-a^n-s_{n-1}a^{n-1}-\cdots-s_1a\in\mathfrak{p}_{i+1}$. Therefore $s_0\equiv -a^n-s_{n-1}a^{n-1}-\cdots-s_1a\equiv 0 \mod \mathfrak{p}_{i+1}$. Hence,

$$s_0\in S\cap\mathfrak{p}_{i+1}=\mathfrak{q}_{i+1}=\mathfrak{q}_i=S\cap\mathfrak{p}_i,$$

so $s_0\equiv 0 \mod \mathfrak{p}_i$. Thus,

$$a(a^{n-1}+s_{n-1}a^{n-2}+\cdots+s_1)\equiv 0 \mod \mathfrak{p}_i,$$

i.e., $\overline{a}\overline{(a^{n-1}+s_{n-1}a^{n-2}+\cdots+s_1)}=\overline{0}$ in the integral domain $R/\mathfrak{p}_i$. Now by the minimality of the above polynomial combination, then $\overline{a}=\overline{0}$ and so

$a \in \mathfrak{p}_i$. Hence, $\mathfrak{p}_i = \mathfrak{p}_{i+1}$.

Thus the preceding was a chain of prime ideals of $S$ and $\dim S \geq \dim R$.

If $S \subseteq R$ is not an integral ring extension then the result may not be true. Indeed, consider the ring extension $\mathbb{Q} \subseteq \mathbb{Q}[X]$, which is not integral. Then $\mathbb{Q}$ is a field so $\dim \mathbb{Q} = 0$ and $\mathbb{Q}[X]$ is a PID which is not a field, so $\dim \mathbb{Q}[X] = 1$. Hence $\dim \mathbb{Q} < \dim \mathbb{Q}[X]$. □

**Note.** The result is more general. Indeed, when the extension $S \subseteq R$ is integral, then $\dim S = \dim R$. However, proving the reverse inequality is much more difficult. Moreover, in order to prove that inequality we ought to use the Going Up theorem, which has not been studied in these notes.

# Bibliography


[1] S. Balcerzyk, T. Józefiak, *Commutative Rings. Dimension, multiplicity and homological methods*, Ellis Horwood Limited, Warszawa, 1989.

[2] N. Bourbaki, *Commutative algebra. Volume II*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1960.

[3] J. Dieudonnè, *Topics in local algebra*, University of Notre Dame Press, Notre Dame, Indiana, 1967.

[4] J. Duoandikoetxea, *Espazio Metrikoen Topologia*, UEU, Iruñea, 1982.

[5] S. Lang, *Algebra*, Graduate Texts in Mathematics, 3. ed., Springer-Verlag, New York, 1993.

[6] J.R. Munkres, *Topology: a first course*, Prentice Hall, Englewood Cliffs, New Jersey, 1975.

[7] H. Perdry, An Elementary Proof of Krull's Intersection Theorem, The American Mathematical Monthly. Vol. 111 **4** (2004), 356-357.

[8] R.Y. Sharp, *Steps in commutative algebra*, Cambrigde University Press, Cambridge, 1990.

[9] O. Zariski, P. Samuel, *Commutative algebra. Volume II*, Graduate Texts in Mathematics, Springer-Verlag, New York, 1960.

# Index