Universitat de Barcelona

Facultat de Matemàtiques i Informàtica

GRAU DE MATEMÀTIQUES

Treball final de grau

Krull Dimension and the Nullstellensatz: From Classical Foundations to Constructive Mathematics

Autor: Saad Boulaich Marso

Director: Carlos D'Andrea
Realitzat a: Departament d'Àlgebra
Barcelona, June 9, 2025

Abstract

This work presents a comprehensive study of fundamental concepts in commutative algebra through both classical and constructive approaches. The first chapter focuses on affine algebraic varieties, the Zariski topology, and Hilbert's Nullstellensatz. This chapter analyzes foundational notions in detail, explaining why they are defined as such and exploring their deep interrelations. Special emphasis is placed on the geometric intuition behind these concepts (for instance, studying the T_2 separability of the Zariski topology depending on the underlying ring), and on linking algebraic definitions to their geometric counterparts.

The second chapter develops the notion of Krull dimension. The effort is placed on deeply understanding how this dimension works, especially in relation to prime ideals. Each theorem is studied carefully, examining the ideas and tools used in the proofs. A completely geometric study of different ideals and their associated varieties is carried out, where the Krull dimension plays a central role in determining the geometric dimension of these varieties. Concepts like symbolic powers and primary decomposition are explored not just as technical tools, but as meaningful objects that help understand the structure of algebraic spaces.

The third chapter is the core and most extensive part of the work, centered on the constructive approach to commutative algebra developed by H. Lombardi, T. Coquand, and collaborators. This methodology seeks to avoid classical non-constructive principles like the law of excluded middle or the axiom of choice, instead providing explicit, algorithmic formulations of concepts and proofs. The chapter highlights the notion of 'collapse' in dynamic algebraic structures, such as potential primes, which impose more computationally verifiable conditions on classical prime ideals. Applying this approach implies that classical results such as the Nullstellensatz and Krull dimension are redefined in a fully constructive framework. The effort here lies not only in understanding these new definitions and their formal development but also in filling gaps in the literature by proving many propositions that are stated without proof in foundational texts. This chapter illustrates how constructive algebra enables explicit computations and verifications that classical algebra approaches without fully specifying the elements involved.

Finally, the fourth chapter offers a historical overview of the development of the Nullstellensatz theorem, summarizing key contributions from figures such as Kronecker and Noether. This retrospective contextualizes the earlier technical chapters by showing the evolution of ideas and terminology leading up to modern formulations.

In conclusion, this work bridges classical theory and modern constructive methods, providing detailed conceptual, geometric, and algebraic insight into the core structures of commutative algebra.

2020 Mathematics Subject Classification. 13-03, 13C15, 13E05, 13L99, 03F65

Agradecimientos

Quiero agradecer, ante todo, a mis padres (Samira y Adil), por su amor incondicional, su confianza y la educación que me han dado. Por estar siempre a mi lado, acompañarme en cada paso, empujarme cuando lo necesitaba y abrazarme cuando dudaba. Por consolarme en mis errores, celebrar conmigo mis logros y, sobre todo, por ser mi refugio constante y una fuente inagotable de alegría y fuerza. No hay palabras suficientes para expresar lo que significan para mí.

También quiero agradecer a mi hermana (Amani), por ser indispensable, una compañera constante y un apoyo incondicional a lo largo de este camino. A mis abuelos (Mohammed, Mustafa, Amina y Hachouma), por cuidarme, ser un ejemplo vital y seguir de cerca mi trayectoria personal y académica. A mis familiares (tíos y primos), por su cariño y su presencia.

Quisiera expresar mi más profundo agradecimiento a mi tutor, Carlos d'Andrea, por su apoyo constante, por confiar en mí durante todo el proceso de elaboración de este trabajo, y por hacer que mi iniciación en el álgebra conmutativa haya sido una experiencia enriquecedora y agradable, pese a su alta exigencia académica.

Y finalmente, a mis amigos de la infancia y de mi barrio (Almoustakbal, Tánger), por creer en mí, permitirme soñar, mantenerme con los pies en la tierra y apoyarme independientemente de las circunstancias. También a todas las amistades que han ido apareciendo en el camino y que han contribuido a forjar la persona que soy hoy.

Que esto sea solo el comienzo de una larga aventura...

Contents

Introduction

The Project

This work explores key concepts in commutative algebra through both classical and constructive perspectives. The classical approach relies on principles like the law of excluded middle and the axiom of choice, which often allow elegant but sometimes non-constructive proofs. In contrast, the constructive approach avoids these principles, aiming to provide explicit, algorithmic methods that can be effectively followed and verified.

This distinction shapes the entire thesis, which revisits classical notions such as affine algebraic varieties, Krull dimension, and the Nullstellensatz, and then reinterprets them constructively. The goal is to show how constructive algebra can offer deeper insight and practical tools while maintaining the core results of the classical theory.

Structure of the Thesis

The thesis is divided into four main chapters:

- **Chapter 1** Introduces the foundational concepts, introducing affine algebraic varieties, the Zariski topology, and the classical Nullstellensatz. It carefully explains how these ideas relate, with an emphasis on geometric intuition, such as studying when the Zariski topology is Hausdorff.
- **Chapter 2** focuses on the Krull dimension, its definitions, and properties. It goes beyond standard presentations by giving a thorough geometric study of various ideals and their associated varieties. The Krull dimension is central to defining a geometric dimension for these objects. The chapter also interprets important concepts like symbolic powers and primary decomposition both algebraically and geometrically.
- **Chapter 3** develops the constructive approach to commutative algebra. Based on works by H. Lombardi and others, it presents explicit, algorithmic methods to define and prove classical results without relying on non-constructive axioms. The chapter introduces dynamic algebraic structures and the key notion of collapse to rebuild notions like the Nullstellensatz and Krull dimension constructively.
- **Chapter 4** offers a historical overview of early developments related to the Nullstellensatz, highlighting the work of Kronecker, Noether, and others, to provide context for the modern theory.

This structure allows the thesis to build progressively from classical foundations to new constructive perspectives, while also situating the study in its historical framework. The references used in each section are specified in the corresponding introductory texts to avoid redundancy and to ensure a more fluent reading experience.

1 Chapter 1: Foundations, The Nullstellensatz and Zariski Topology

In this chapter we will introduce some basic concepts that are required to define properly the structure of a **constructive algebra** and that conduct to all the results, in this case the different Nullstellensatz obtained by the development of this theory. These are mainly three: **The Zariski Topology**, **The Hilbert Nullstellensatz** and **Krull Dimension**. As we explained in the abstract, all these results are useful in the context of **Commutative Algebra**, that is why we will only consider at all times a **commutative ring with identity**, A (unless we specify otherwise).

1.1 Algebraic Varieties

1.1.1 Prime and Maximal Ideals

Before pretending to define the points of such an elementary Topology, we need a deep understanding of the elements of its space. Unlike the common topological spaces we are used to, like the Euclidean spaces or the Riemannian Manifolds, this one is specifically based on the algebraic structure of polynomial rings, and of course, this implies to take in account the different kind of ideals we could construct and their role in this space.
Let's consider first of all the **prime** and **maximal** ideals, and the ideals related to their **spectrum** (cf. [1, 2, 3]).

Definition 1.1 (Prime Ideal)**.** *An ideal $\mathfrak{P}$ of A with $\mathfrak{P} \neq A$ is said to be prime if for any product $xy \in \mathfrak{P}$ (where $x, y \in A$) then $x \in \mathfrak{P}$ or $y \in \mathfrak{P}$.*

An immediate and useful property of prime ideals is the following one.

Proposition 1.2. *An ideal $\mathfrak{P}$ of A is a prime ideal if and only if $A/\mathfrak{P}$ is an **integral domain** (that is, it has no zero divisors).*

Defining $Spec(A)$ as the set of all the prime ideals of A, in our further analysis we shall see that it is interesting to consider the result of intersecting all the prime ideals. However, before that, we need to define the **nilradical** of a ring.

Definition 1.3 (Nilradical)**.** *The **nilradical** of an ring A is defined as the set of elements $f \in A$ such that there exists an $n \in \mathbb{N}$ for which $f^n = 0$. We denote it by η, and its elements are named **nilpotent**.*

Two immediate results from this definition are the following ones. We will prove the second one due to its importance.

Proposition 1.4. *A/η has no nilpotent elements except the 0.*

Proposition 1.5. *The nilradical η of a ring A is the intersection of all the elements of $Spec(A)$.*

Proof. Let us prove the inclusion $\eta \subseteq \bigcap_{\mathfrak{P} \in \mathrm{Spec}(A)} \mathfrak{P}$. If $f \in \eta$, then there exists $n \in \mathbb{N}$ such that

$$f^n = 0 \in \mathfrak{P}, \quad \forall \mathfrak{P} \in \mathrm{Spec}(A).$$

To prove the reverse inclusion, suppose there exists $f \in \bigcap_{\mathfrak{P}\in \text{Spec}(A)} \mathfrak{P}$ such that $f^n \neq 0, \quad \forall n \in \mathbb{N}$. We define the set $X = \{I \text{ ideal of } A \mid f^n \notin I, \ \forall n\} \neq \emptyset$. This set is partially ordered by inclusion, and since $(0) \in X$, by Zorn's Lemma there exists a maximal element $P_0 \in X$. Notice that $f \notin P_0$. We will show that P_0 is a **prime ideal**. Suppose $x, y \notin P_0$. Then $P_0 \subsetneq P_0 + (x)$ and $P_0 \subsetneq P_0 + (y)$. By maximality of P_0, there exist integers $m, n \in \mathbb{N}$ such that $f^m \in P_0 + (x)$ and $f^n \in P_0 + (y)$. Hence, there exist $p, q \in P_0$ and $a, b \in A$ such that $f^m = p + ax$ and $f^n = q + by$. Multiplying these two expressions, we get $f^{m+n} = (p+ax)(q+by) = pq + pby + axq + abxy$. Since P_0 is an ideal, and $p, q \in P_0$, the terms pq, pby, and axq all lie in P_0, so $f^{m+n} - abxy \in P_0$. Since $f^{m+n} \notin P_0$, it follows that $abxy \notin P_0$, hence $xy \notin P_0$. Therefore, if $xy \in P_0$, then $x \in P_0$ or $y \in P_0$, showing that P_0 is prime, contradicting the fact that $f \in \bigcap_{\mathfrak{P}\in \text{Spec}(A)} \mathfrak{P}$, therefore

$$\bigcap_{\mathfrak{P}\in \text{Spec}(A)} \mathfrak{P} \subseteq \eta.$$

Combining both inclusions, we conclude that

$$\eta = \bigcap_{\mathfrak{P}\in \text{Spec}(A)} \mathfrak{P}.$$

□

Definition 1.6 (Maximal Ideals)**.** *An ideal $\mathfrak{M}$ of A is said to be maximal if $\mathfrak{M} \neq A$ and if J is an ideal of A such that $\mathfrak{M} \subseteq J \subseteq A$ then $\mathfrak{M} = J$ or $J = A$.*

The following property of maximal ideals is really useful in order to make the geometrical interpretations easier.

Proposition 1.7. *An ideal $\mathfrak{M}$ of A is a maximal ideal if and only if $A/\mathfrak{M}$ is a* ***field****.*

As we did for the case of prime ideals, it is always useful to check what happens when we intersect all the maximal ideals of a given ring A.

Definition 1.8 (Jacobson Ideal)**.** *We define the* ***Jacobson Ideal*** *of a commutative ring with identity A as the intersection of all the ideals of $\mathfrak{M} - Spec(A)$.*

$$\mathfrak{J} = \bigcap_{\mathfrak{N}\in \mathfrak{M}-Spec(A)} \mathfrak{N}$$

The following property allows to charactrize all the elements of this ideal.

Proposition 1.9. *An element $x \in \mathfrak{J}$ if and only if $1 - xy \in U(A)$ for all the elements $y \in A$, where $U(A)$ denotes the set of invertible elements of A.*

Proof. In order to check the first implication, let's suppose that $1 - xy \notin U(A)$. That means that this element is contained in some maximal ideal M_0, but then by definition $x \in M_0$, so $xy \in M_0$ and by the properties of ideals $1 = 1 - xy + xy \in M_0$ contradicting the fact that M_0 is a maximal ideal.
In order to check the other implication, consider that $x \notin \mathfrak{J}$, then there exists a maximal ideal M_0 such that $x \notin M_0$, thus, by maximality $M_0 + (x) = A$. Due to the presence of the identity in the ring A, $1 = m_0 + xy \in A$ and therefore $1 - xy = m_0 \notin U(A)(\in M_0)$. □

Finally, we gather up some important and necessary definitions and results.

Definition 1.10 (Radical Ideal). *The radical ideal of a given ideal I of A has as elements those for which there exists some natural power belonging to I.*

$$\mathrm{Rad}(I) := \{f \in A | \exists n \in \mathbb{N}, f^n \in I\}$$

It also can be defined, equivalently, as the intersection of all prime ideals in A containing I.

Lemma 1.11 (Nakayama's Lemma). *If M is a finitely generated module (i.e. $M = (m_1, \dots, m_k), m_i \in M$) and $\mathfrak{I} \subset \mathfrak{J}_A$ then if also $\mathfrak{I}M = M$ therefore $M = 0$.*

Lemma 1.12. *Let R be a ring and M a finitely generated module. Suppose $\mathfrak{I} \subseteq R$ is an ideal contained in the Jacobson radical of R, and $N \subseteq M$ is a submodule such that $M = \mathfrak{I}M + N$, then $M = N$.*

Lemma 1.13. *Let R be a local ring with maximal ideal $\mathfrak{m}$, and let M be a finitely generated R-module. If $\mathfrak{m}M = M$, then $M = 0$.*

1.1.2 Localization of a Prime Ideal

In order to better understand the behavior of specific **prime ideals**, it is useful to find a way to concentrate the relevant properties of the ring around them, disregarding elements that do not belong to the ideal, and studying their structure through the relations (such as operations, inclusions, and maximality) that pertain to them. This objective is achieved through the technique of localization, which we will define precisely and formally, accompanied by illustrative examples to demonstrate its application (cf. [3, 4, 5]).

To this end, let us assume that the ring A is an **integral domain**. Intuitively, the idea of "focusing" in the algebraic structures of rings and modules often corresponds to taking quotients via an equivalence relation or an ideal. In this case, however, although an equivalence relation is involved, the construction takes inspiration from the structure of the field of fractions $Frac(A)$, which provides a more direct framework for localizing at a prime ideal. For this reason, we first recall the definition of a **multiplicative set** and the associated equivalence relation.

Definition 1.14 (Multiplicative Set). *Given a subset S of A, we say it is a multiplicative set if the following conditions hold:*

1. $1 \in S$.
2. *if $s, t \in S$, then $s \cdot t \in S$.*

Now, let us consider the Cartesian product set $A \times S$. We can define an equivalence relation in it, which is similar to the definition of the fraction field of A. Indeed, it is a subring of that field.

Definition 1.15. *Let $(a, s), (b, t) \in A \times S$, we say they are related if and only if there exists $u \in S$ such that $u(at - bs) = 0$.*

It is trivial that is reflexive and symmetric (just by taking $u = 1$), let's prove the transitivity.

Proposition 1.16. *The given relation is transitive. That is, it is an* ***equivalence relation****.*

Proof. Let us consider that $(a, s) \sim (a', s')$ and $(a', s') \sim (a'', s'')$. Then by defintion:

$$u(as' - a's) = 0$$
$$u'(a's'' - a''s') = 0$$

Then combining both expressions we get

$$uu's'(as'' - a''s) = u's''(u(as' - a's)) + us(u'(a's'' - a''s')) = 0$$

because $uu's \in S$.

□

Notation 1. *We write $a/s \equiv [(a, s)]$. The resulting quotient ring: $S^{-1}A \equiv (A \times S)/\sim$.*

Before introducing the definition of the localization ring, let's take a look at the units of this ring in general. Firstly, it is a ring because if we take the sum and the product to be of the same form as the fractions we are used to, we confirm that it obeys them.

However, in this case, we say it is a ring, not a field, and that's due to the fact that not all the elements are invertible. For example, if we take a/s with $a \in A - S, s \in S$, then by the rules of the product and the definition provided above, if we want it to be invertible then $a \in S$, and its inverse would be s/a, but for obvious reasons that's a contradiction. However, this suggests that the invertible elements are those who have both elements in S, that is:

Proposition 1.17. *The set of units or invertible elements of $S^{-1}A$ is: $\{a/s \in S^{-1}A |\ a, s \in S\}$*

And as we know, the units can never belong to a proper ideal. For this specific reason, if we choose properly the set S we can get this idea of "focusing" the algebraic features of $S^{-1}A$ in a particular ideal. Specifically, it suits perfectly the prime ideals for two reasons that we are going to prove:

1. $S^{-1}\mathfrak{P}$ is also a **prime ideal**.
2. $S^{-1}A$ becomes a **local ring** with only one maximal ideal ($S^{-1}\mathfrak{P}$): all the other remaining ideals are subsets of this one.

And this situation is possible if we take the multiplicative set to be $S = A - \mathfrak{P}$. Notice that in this case the only non invertible elements are those of the form a/b with $a \in \mathfrak{P}$ and $b \in S$. Let's prove both statements:

Proof. 1. Let's suppose that $S^{-1}\mathfrak{P}$ is not prime, that is given $a/s, b/t \notin S^{-1}\mathfrak{P}$, then $ab/st \in S^{-1}\mathfrak{P}$. If that is true, then there exists $c/u \in S^{-1}\mathfrak{P}$ such that $c/u = ab/st$, and by definition, there is a $u_0 \in S$ such that $u_0(cst - uab) = 0$, and therefore $u_0cst = u_0uab$. The left term of the equation is in $\mathfrak{P}$ because $c \in \mathfrak{P}$ (definition of ideal). By equality, $u_0uab \in \mathfrak{P}$, and knowing that $u_0, u \in S = A - \mathfrak{P}$ then the remaining product is in $\mathfrak{P}$, that is $ab \in \mathfrak{P}$. By the definition of prime ideal in A, we conclude that either $a \in \mathfrak{P}$ or $b \in \mathfrak{P}$, which implies a contradiction with the first assumption.

2. As we indicated before, $U(S^{-1}A) = S^{-1}A - S^{-1}\mathfrak{P}$, we then know from the results of the Commutative Algebra that an ideal satisfying this property is the only existing maximal ideal in $S^{-1}A$ (which also implies locality).

□

As we suggested in the beginning of the section, we have now focused the structure and properties of the ring A on the ideal $\mathfrak{P}$ by making it the only maximal ideal. Every other proper ideal is contained in $S^{-1}\mathfrak{P}$ and outside $\mathfrak{P}$ all the elements are units, which is not a case of interest in our particular problem, nor affects the procedures significantly.

1.1.3 Algebraic Varieties in Affine Spaces

Let's consider a polynomial ring $K[x_1, \ldots, x_n]$, which are the main mathematical objects we are interested to dig in. It is important to know which are the points that cancel its ideals it in order to get information about the way they factorize, that is, the way we can describe them (cf. [3, 5, 6]).

Definition 1.18 (Algebraic variety)**.** *Let's $S \subseteq K[x_1, \ldots, x_n]$ and F an* ***algebraically closed extension field*** *of K. We define the* ***affine K-variety****, or simply its corresponding* ***algebraic variety****, as the set of points of F^n that cancel all of its elements*

$$V(S) := \{(x_1, \ldots, x_n) \in F^n | f(x_1, \ldots, x_n) = 0, \forall f \in S\}$$

Similarly, given a set of points $X \subseteq K^n$, we are interested in the set of polynomials that have all of them as roots.

Definition 1.19. *Given a set $X \subseteq F^n$ we define the following set of annihilators*

$$I(X) := \{f \in K[x_1, \ldots, x_n] | f(x_1, \ldots, x_n) = 0, \forall (x_1, \ldots, x_n) \in X\}$$

Proposition 1.20. *The set $I(X)$ is an ideal.*

Proof. The null polynomial belongs to it, $0 \in I(X)$. Denoting $\vec{x} = (x_1, \ldots, x_n) \in$X
If $f, g \in I(X)$, then $f(\vec{x}) + g(\vec{x}) = 0, \forall \vec{x} \in X$, getting $f + g \in I(X)$.
Finally, given $f \in I(X)$, and $r \in K[x_1, \ldots, x_n]$, we get $r(\vec{x}) \cdot f(\vec{x}) = r(\vec{x}) \cdot 0 = 0, \forall (\vec{x}) \in X$, therefore $r \cdot f \in I(X), \forall r \in K[x_1, \ldots, x_n], \forall f \in I(X)$. □

Observation 1.21. If $\mathfrak{I}$ is the ideal generated by S, then $V(\mathfrak{I}) = V(S)$.

We shall highlight certain properties that will be essential later in this chapter for endowing algebraic varieties with the structure of a topological space.

Proposition 1.22. *Using the same notation as the preceding definitions and theorems:*

1. $V(F^n) = \emptyset$ *and* $V(\emptyset) = K[x_1, \ldots, x_n]$.
2. $V(I) \cap V(J) = V(I + J)$
3. $V(I) \cup V(J) = V(IJ)$

Observation 1.23. The second property indicates that the intersection of algebraic varieties is **arbitrary**; nevertheless, the union must be **finite**.

Although these notions may initially appear to be closely tied to polynomial rings, they can naturally be extended to any commutative ring with identity A. However, to achieve this (and consequently define concluding structures such as a topology or a dimension), we must first establish a solid connection between the ideals of a ring and the corresponding varieties.

1.1.4 Prime Ideals and Irreducible Varieties

Let's revert our understanding of cancellation by introducing the following funcion (cf. [4, 5, 6]).

Definition 1.24. *Let A be a ring, and consider $Spec(A)$. By taking $f \in A$, we define:*

$$f|_{Spec(A)} : Spec(A) \longrightarrow \bigsqcup_{\mathfrak{P} \in Spec(A)} A/\mathfrak{P}, with\ \mathfrak{P} \mapsto [f]_{A/\mathfrak{P}}$$

This function implies that an element $f \in A$ leads to the null function, i.e, $f|_{Spec(A)} = 0$, if and only if, $f \in \eta(A)$, i.e, it is nilpotent (as we have seen in the section **??**, the nilpotent ideal is the intersection of all the elements of $Spec(A)$).
With this notion of cancellation, we could define a new kind of algebraic varieties, and show that those defined in Affine Spaces remain just as a particular case of these.

Definition 1.25 (Algebraic variety)**.** *Let $S \subseteq A$, we define its corresponding algebraic variety as,*

$$V(S) = \{\mathfrak{P} \in Spec(A) | \mathfrak{P} \supseteq S\} = \{\mathfrak{P} \in Spec(A) | f(\mathfrak{P}) = 0, \forall f \in S\}$$

Definition 1.26 (Generated Ideal)**.** *Given a subset $X \subseteq Spec(A)$, we define its corresponding **generated ideal** as*

$$I(X) = \bigcap_{\mathfrak{P} \in X} \mathfrak{P} = \{f \in A : f|_X = 0\}$$

Although this definition may initially seem quite different (since it is based on collections of ideals rather than points) it actually generalizes the previous one, which was formulated in affine spaces. To recognize the equivalence between these definitions, we must expect prime ideals to exhibit a form of minimality, meaning they should correspond one-to-one with minimal objects in the space of varieties. If this condition holds, we can conclude that defining algebraic varieties in terms of prime ideals is well-founded, with the case of polynomial rings and affine varieties serving as a particular instance that must also validate this approach. Let's check it with the following proposition.

Theorem 1.27. *Let X be a subset of $Spec(A)$ that can be written in the form $X = V(J)$ for some ideal J of A. The following statements are equivalent:*

1. *$X = V(\mathfrak{P})$ for some prime ideal $\mathfrak{P}$ of A.*
2. *$I(X)$ is a prime ideal of A.*
3. *X is non-empty and may not be written as $X = X_1 \cup X_2$, where X_1, X_2 are subsets of $Spec(A)$ that can be written in the form $X_i = V(I_i)$, where $i = 1, 2$ and I_i is an ideal of A.*

If X satisfies the preceding conditions, it's said to be ***irreducible*** *(by the third condition it cannot be decomposed in elements of the same nature).*

Proof. (1) $\Rightarrow$ (2) If $X = V(\mathfrak{P})$, for some $\mathfrak{P} \in Spec(A)$, then taking the ideal generated by X:

$$I(X) = I(V(\mathfrak{P})) = \mathfrak{P}$$

because $\mathfrak{P}$ is prime.
(2) $\Rightarrow$ (3) If $I(X) \equiv \mathfrak{P}$ is a prime ideal of A, then if we take the variety generated by this ideal:

$$V(I(X)) = V(\mathfrak{P}) = V(I(V(J))) = V(J) = X$$

Now, let's suppose we can write X as $X = X_1 \cup X_2$ satisfying the conditions stated in the point 3. Then:

$$X = V(I(X)) = V(I(X_1 \cup X_2)) = V(I(X_1) \cap I(X_2)) = V(\mathfrak{P})$$

now taking the ideal generated of both sides, and applying the Hilbert's Nullstellensatz (fully proved in the following section), then:

$$rad(I(X_1) \cap I(X_2)) = rad(I(X_1)) \cap rad(I(X_2)) = \mathfrak{P}$$

now using the properties of radical ideals and the inclusion reversing property of algebraic varieties:

$$I(X_1) \subseteq rad(I(X_1)) \subseteq \mathfrak{P} = I(X) \Rightarrow X \subseteq X_1$$

and similarly $X \subseteq X_2$ which contradicts the assumptions made.
(3) $\Rightarrow$ (1) Suppose $X = V(J)$ is irreducible. Then X cannot be written as the union of two proper closed subsets. Let $I(X)$ be the ideal of X, so that $X = V(I(X))$. If $I(X)$ is not prime, then there exist $f, g \in A$ such that $fg \in I(X)$ but $f \notin I(X)$ and $g \notin I(X)$. Consider the closed subsets:

$$X_1 = V(I(X) + (f)), \quad X_2 = V(I(X) + (g))$$

Then $X = V(I(X)) \subseteq V(I(X)+(f)) \cup V(I(X)+(g)) = X_1 \cup X_2$. Also, $f \notin I(X)$ implies $X_1 \subsetneq X$, and similarly $X_2 \subsetneq X$, contradicting the irreducibility of X. Hence, $I(X)$ must be prime, and so $X = V(I(X)) = V(\mathfrak{P})$ for some prime ideal $\mathfrak{P}$. $\square$

A set X satisfying the previous conditions is said to be **irreducible**, and specially with the condition 3., the minimality is reflected in the fact that X cannot be decomposed into two (or more) sets of the same nature. The condition 1. shows us how prime ideals are directly related to irreducible sets in $Spec(A)$, therefore the definition given is consistent: the prime ideals containing the set of polynomials S are in one-to-one correspondence with the irreducible components that cancel out all their elements. Furthermore, if these irreducible components are points (in the sense of affine spaces), then they keep a one-to-one correspondence with maximal ideals, which are a particular case of prime ideals. Finally, the condition 2. gives us a way to detect whether an algebraic variety V is irreducible or not (in the general case, of course) by checking if the ideal generated $I(V)$ is prime or not.

1.2 The Hilbert Nullstellensatz

The previous discussion on the connection between irreducible varieties and prime ideals becomes even clearer and is a direct consequence of the Hilbert Nullstellensatz, which we have already mentioned in Chapter 1. Let's state it definitely. We will consider k to be an **algebraically closed field** only in this section (cf. [1, 2, 4, 6]).

Theorem 1.28 (Weak Nullstellensatz). *If I is a (proper) ideal in $k[x_1, \ldots, x_n]$, then $V(I) \neq \emptyset$.*

Proof. We shall segment this proof in two parts.

1. **If I is a proper ideal, then it is contained in some maximal ideal J:** Consider the set C of all the proper ideals containing I. Since all of them are proper ($\forall R \in C, R \neq (1)$) then their union is also a proper ideal, and they can be ordered by inclusion. By **Zorn's Lemma**, there is un upper bound, that is, a **maximal proper ideal** in C containing I.

2. **Using J, then $\emptyset \neq V(J) \subseteq V(I)$:** If J is a maximal ideal then $k[x_1, \ldots, x_n]/J$ is a field, concretely a finite extension of k. However, we stated that k is algebraically closed, which implies that $k \cong k[x_1, \ldots, x_n]/J$ (since any finite extension of an algebraically closed field must be the field itself).. Therefore, this last condition implies that there exists some $(a_1, \ldots, a_n) \in k^n$ such that $J = (x_1 - a_1, \ldots, x_n - a_n)$ and for every polynomial $f \in J$, $f(a_1, \ldots, a_n) = 0$, obtaining that $V(J) \neq \emptyset$.

□

Theorem 1.29 (Hilbert's Nullstellensatz). *Let I be an ideal in $k[x_1, \ldots, x_n]$, then $I(V(I)) =$ Rad(I).*

In concrete terms, this means that if $F_1, F_2, \ldots, F_r$ and G are in $k[X_1, \ldots, X_n]$, and G vanishes wherever $F_1, F_2, \ldots, F_r$ vanish, then there exist $N \geq 0$ and polynomials $A_i \in k[X_1, \ldots, X_n]$ such that:

$$G^N = A_1F_1 + A_2F_2 + \cdots + A_rF_r.$$

Proof. That $\text{Rad}(I) \subseteq I(V(I))$ is straightforward. Let's suppose that G belongs to the ideal $I(V(F_1, \ldots, F_r))$, where $F_i \in k[X_1, \ldots, X_n]$. Define the ideal:

$$J = (F_1, \ldots, F_r, X_{n+1}G - 1) \subset k[X_1, \ldots, X_n, X_{n+1}].$$

Then $V(J) \subset k^{n+1}$ is empty, since G vanishes wherever all the F_i's are zero. By the Weak Nullstellensatz, we conclude that $1 \in J$, so there exist polynomials $A_i(X_1, \ldots, X_n, X_{n+1})$ and $B(X_1, \ldots, X_n, X_{n+1})$ such that:

$$1 = \sum_i A_i(X_1, \ldots, X_n, X_{n+1})F_i + B(X_1, \ldots, X_n, X_{n+1})(X_{n+1}G - 1).$$

Setting $Y = 1/X_{n+1}$ and multiplying by a suitable power of Y, we obtain an equation in $k[X_1, \ldots, X_n, Y]$ of the form:

$$Y^N = \sum C_i(X_1, \ldots, X_n, Y)F_i + D(X_1, \ldots, X_n, Y)(G - Y).$$

Substituting $Y = G$ gives the desired equation. □

Hilbert's Nullstellensatz has the following direct consequences, reinforcing our previous approach of treating ideals as varieties.

Corollary 1.30. *If I is a radical ideal in $k[x_1, \dots, x_n]$, then $I(V(I)) = I$. Therefore, there is a one-to-one correspondence between* ***radical ideals*** *and* ***algebraic varieties****.*

Corollary 1.31. *If $\mathfrak{P}$ is a prime ideal, then $V(\mathfrak{P})$ is irreducible. Therefore there is a one-to-one correspondence between* ***prime ideals*** *and* ***irreducible varieties*** *(as we have seen before). The special case of* ***maximal ideals*** *correspond to* ***points****.*

Corollary 1.32. *If I is an ideal in $k[x_1, \dots, x_n]$, then $V(I)$ is a finite set if and only if the quotient $k[x_1, \dots, x_n]/I$ is finite dimensional vector space over k.*

1.3 Zariski Topology

1.3.1 Definition and properties

In the previous sections of this chapter, we explored the fundamental properties of prime ideals and their localization, as well as their connection to algebraic varieties. Given the behavior of unions and intersections of algebraic varieties, it is natural to consider the possibility of defining a topology where these varieties serve as closed sets.
To achieve this, let us first recall the definitions of **topology** and, to ensure a complete understanding, of **continuous functions**. Then, we will examine whether algebraic varieties fit within this framework (cf. [3, 4, 5, 6]).

Definition 1.33 (Topology)**.** *A* ***topological space*** *is a nonempty set χ together with a collection of subsets called* ***closed****, τ, such that:*

1. *$\{\emptyset, \chi\}$ are closed.*
2. *The finite union of closed subsets is closed.*
3. *The arbitrary intersection of closed subsets is closed.*

Definition 1.34 (Continuous function)**.** *We say that a function between topological spaces X and Y, $f : X \longrightarrow Y$ is* ***continuous*** *if for every closed set C in Y, then $f^{-1}(C)$ is closed in X.*

These definitions differ from the usual ones involving **open sets**; however, they are more useful in our context since algebraic varieties naturally behave as **closed sets**. This perspective allows for a clearer understanding of the topology arising from their properties. The properties given in **Proposition 1.20** are naturally extended to the general case, allowing us to define the Zariski Topology as:

Definition 1.35. *The* ***Zariski Topology*** *of a ring A is the nonempty set $\chi = Spec(A)$ where the* ***closed sets*** *are the algebraic varieties $V(I)$, where I is an ideal of A.*

From our previous discussion, it satisfies the properties of a topology. Furthermore, we know from Hilbert's Nullstellensatz that if the ring is a polynomial ring $K[x_1, \dots, x_n]$, and K is algebraically closed, then we can identify $m - Spec(A)$ with K^n, therefore, the Zariski Topology can be viewed as the minimal topology that makes all the polynomial functions in K to be continuous.

1.3.2 Cases where Zariski Topology is T_2

Given a topological space, it is interesting to discuss its **separability**, for that, we shall restrict ourselves to polyonomial rings over an algebraically closed field F, that is $F[x_1, \ldots, x_n]$, and check in which cases we can affirm whether it is or not T_2.

Definition 1.36. *Given a topological space X, we say it is **Hausdorff** or T_2 if for any distinct points $x, y \in X$ there are disjoint neighborhoods, that is, there are open sets U containing x, V containing y such that $U \cap V = \emptyset$.*

As we have observed, the closed sets in Zariski topology can be interpreted as the preimages of a given set of polynomials. While the conditions determining whether the Zariski topology of a polynomial ring is T_2 or not may seem related to the number of variables, in reality, this separability property is dictated by the finiteness of the base field F. Let us examine both cases in detail.

1. F **finite**, $n \geq 1$: If we take an arbitrary subset $S \subseteq F^n$ we can define the polynomial:

   $$P_S(x) = \prod_{(a_1,\ldots,a_n) \notin S} (x_1 - a_1) \ldots (x_n - a_n)$$

   it vanishes at all points in $F^n - S$, which implies that S is **closed** in the Zariski topology. Therefore, every subset of F^n is closed, and in this case, the Zariski topology coincides with the **discrete topology**, which is always T_2 since all its points are both open and closed.

2. F **infinite**, $n = 1$: Due to the following theorem:

   Theorem 1.37. *A polynomial $p(x)$ of degree n with coefficients in a field F has at most n roots (counting multiplicities) in any extension of F (for example, in $\mathbb{C}$ if $F = \mathbb{C}$).*

   any polynomial $f \in F[x]$ of degree $m > 1$ has at most m roots. For this reason, any closed set of its Zariski Topology is finite, then the open sets are those who have a finite complementary set. Consequently, the Zariski Topology in this case is the **cofinite topology**, whose open sets are:

   (a) The total set F and the empty set $\emptyset$.
   (b) The subsets $V \subset F$ such that $F \setminus V$ is finite.

   And we know that cofinite topology **is not** T_2. This is because any two non-empty open sets have non trivial intersection. To prove briefely this statement, if we consider x and y two distinct points of F with respective open neighborhoods U, V, $X \setminus U$, $X \setminus V$ must be finite. Then the intersection:

   $$U \cap V = X \setminus ((X \setminus U) \cup (X \setminus V))$$

   Therefore, the intersection $U \cap V$ is not empty, since the set $(X \setminus U) \cup (X \setminus V)$ is finite, and $X \setminus ((X \setminus U) \cup (X \setminus V))$ is a non-empty set. This proves that in the cofinite topology, any pair of non-empty open sets has a non-trivial intersection, which implies that the topology is not T_2 (i.e., it is not Hausdorff).

3. F **infinite**, $n > 1$: By taking F^n, we can consider its projection in F, that is, $F \times \{0\} \times \ldots \times \{0\}$. This subspace is obviously homeomorphic to F, and from the previous point we know that it is not T_2, and this implies that if the Hausdorff property of separabilty isn't satisfied for some subspace of F^n, then globally F^n is not T_2.

This particular study aims to highlight how the Zariski topology can take different forms depending on the properties of the base field F and the number of unknowns x_i involved. If the general properties of separability are not guaranteed, especially in the case of T_2-separability (Hausdorff separability), then caution is required when handling the topological structure. We must consider the different cases carefully if we wish to make general topological assertions.

2 Chapter 2: Krull Dimension, definition and properties

As always we consider a commutative ring with identity A. The definition of the **Krull dimension** reflects the maximal length of proper chains of prime ideals that we are able to construct. As we shall see, it has an important application in geometric contexts.

2.1 Definition, height and coheight

We now present some standard definitions concerning Krull dimension within the framework of algebraic geometry (cf. [6, 7, 9]).

Definition 2.1 (Krull Dimension)**.** *Let A be a commutative ring with identity, we define its **Krull Dimension** as:*

$$\dim_K(A) \equiv \dim(A) := sup\{n \geq 0 | \exists \mathfrak{P}_0 \subsetneq \ldots \subsetneq \mathfrak{P}_n\}$$

where $\mathfrak{p}_i$ are prime ideals of A.

In order to generalize this concept to any ideal and to have a deeper insight of it, we can also define the concepts of **height** and **coheight**, each of them leading to the definition of dimension and codimension, respectively.

Definition 2.2 (Height and Coheight)**.** *Let $\mathfrak{P}$ be a **prime** ideal of the commutative ring with identity A, and $\mathfrak{I}$ a general ideal of the same ring. We define:*

1. *Height of $\mathfrak{P}$:* $\text{height}(\mathfrak{P}) = \sup\{n \geq 0 | \exists \mathfrak{P}_0 \subsetneq \ldots \subsetneq \mathfrak{P}_n = \mathfrak{P}\}$
2. *Coheight of $\mathfrak{P}$:* $\text{coheight}(\mathfrak{P}) = \sup\{n \geq 0 | \exists \mathfrak{P} = \mathfrak{P}_0 \subsetneq \ldots \subsetneq \mathfrak{P}_n\}$
3. *Height of $\mathfrak{I}$:* $\text{height}(\mathfrak{I}) := \inf_{\mathfrak{P} \supsetneq \mathfrak{I}} \text{height}(\mathfrak{P})$
4. *Coheight of $\mathfrak{I}$:* $\text{coheight}(\mathfrak{I}) := \sup_{\mathfrak{P} \supsetneq \mathfrak{I}} \text{coheight}(\mathfrak{P})$

Observation 2.3. We may also define the **height of $\mathfrak{P}$ over $\mathfrak{Q}$**, where $\mathfrak{Q} \subset \mathfrak{P}$, in a manner similar to the definition of the height of $\mathfrak{P}$, but with $\mathfrak{Q}$ being the first prime ideal in any chain of inclusions leading up to $\mathfrak{P}$. In that case, it coincides with $\dim((A/\mathfrak{Q})_{\mathfrak{P}})$. This is because the prime ideals in $(A/\mathfrak{Q})_{\mathfrak{P}}$ are precisely those prime ideals of $A/\mathfrak{Q}$ that are contained in $\mathfrak{P}$. On the other hand, the prime ideals of $A/\mathfrak{Q}$ are exactly those that contain $\mathfrak{Q}$. Therefore, the prime ideals in $(A/\mathfrak{Q})_{\mathfrak{P}}$ are the ones that are **contained** in $\mathfrak{P}$ and **contain** $\mathfrak{Q}$, reflecting the relationship between the ideals in the localization and the quotient ring.

Now, we will introduce some lemmas (with their proof) that allow to understand better the structure of the height and coheight.

Proposition 2.4. *If I is an ideal of a commutative ring with identity A:*

$$\text{height}(I) + \dim(A/I) \leq \dim(A)$$

Proof. Taking natural numbers $r, s \in \mathbb{N}$ such that $r \leq height(I)$ and $s \leq dim(A/I)$ we can deduce, by using the definitions introduced above that:

$$\text{height}(I) = \inf_{\mathfrak{P} \supsetneq \mathfrak{I}} \text{height}(\mathfrak{P}) \Rightarrow \mathfrak{P}_0 \subsetneq \ldots \subsetneq \mathfrak{P}_r = \mathfrak{P}$$

$$\dim(A/I) = \text{coheight}(I) = \sup_{\mathfrak{P} \supsetneq \mathfrak{I}} \text{coheight}(\mathfrak{P}) \Rightarrow \mathfrak{I} \subsetneq \mathfrak{P} = \mathfrak{Q}_0 \subsetneq \mathfrak{Q}_1 \subsetneq \ldots \subsetneq \mathfrak{Q}_s$$

Allowing us to construct a chain based on both chains, with lower bound length $r + s$:

$$\mathfrak{P}_0 \subsetneq \ldots \subsetneq \mathfrak{P}_r = \mathfrak{P} = \mathfrak{Q}_0 \subsetneq \mathfrak{Q}_1 \subsetneq \ldots \subsetneq \mathfrak{Q}_s$$

and this suits the definition of the Krull dimension of A. □

2.2 Relationship with localization of Prime ideals

If we consider I to be a prime ideal $\mathfrak{P}$, then we can prove the following (cf. [5, 7]):

Proposition 2.5. *Let $\mathfrak{P}$ be a prime ideal of a ring A, and let $A_{\mathfrak{P}}$ be its localization at $\mathfrak{P}$. Then, the Krull dimension of $A_{\mathfrak{P}}$ is equal to the height of $\mathfrak{P}$ in A, that is,*

$$\dim(A_{\mathfrak{P}}) = \text{height}(\mathfrak{P}).$$

Proof. The Krull dimension of $A_{\mathfrak{P}}$ is given by:

$$\dim(A_{\mathfrak{P}}) = \sup\{n \geq 0 \mid \exists \bar{\mathfrak{P}}_0 \subsetneq \bar{\mathfrak{P}}_1 \subsetneq \cdots \subsetneq \bar{\mathfrak{P}}_n\},$$

where the $\bar{\mathfrak{P}}_i$ are prime ideals of $A_{\mathfrak{P}}$. On the other hand, the height of $\mathfrak{P}$ in A is:

$$\text{height}(\mathfrak{P}) = \sup\{n \geq 0 \mid \exists \mathfrak{P}_0 \subsetneq \mathfrak{P}_1 \subsetneq \cdots \subsetneq \mathfrak{P}_n \subseteq \mathfrak{P}\},$$

where the $\mathfrak{P}_i$ are prime ideals of A. Since, when localizing at $\mathfrak{P}$, the prime ideals of $A_{\mathfrak{P}}$ correspond exactly to the prime ideals of A contained in $\mathfrak{P}$, the chains of prime ideals in $A_{\mathfrak{P}}$ come directly from chains of prime ideals in A contained in $\mathfrak{P}$. Therefore, both suprema are equal, proving the desired result. □

Corollary 2.6. *Let $\mathfrak{P}$ be a prime ideal, and let $A_{\mathfrak{P}}$ be its localization at $\mathfrak{P}$. Then,*

$$\dim(A_{\mathfrak{P}}) + \dim(A/\mathfrak{P}) \leq \dim(A)$$

We can also determine the Krull dimension of a ring A by using its **minimal primes**, that is, the (proper) prime ideals $\mathfrak{P}_i$ such that there does not exist any (proper) prime ideal $\mathfrak{Q}$ with $\mathfrak{Q} \subsetneq \mathfrak{P}_i$.

Proposition 2.7. *If $\{\mathfrak{P}_i\}$ are the minimal primes of a ring A, then*

$$\dim(A) = \sup_i \dim(A/\mathfrak{P}_i)$$

Proof. This proposition is proven for the following two reasons:

1. Any maximal chain of prime ideals in A begins with a minimal prime ideal $\mathfrak{P}$; otherwise, we could extend the chain by including prime ideals from below.

2. These maximal chains correspond one-to-one with chains of prime ideals in the quotient ring $A/\mathfrak{P}$, since the prime ideals in this quotient ring are precisely the prime ideals in A that contain $\mathfrak{P}$.

This one-to-one correspondence allows us to determine the Krull dimension of A by taking the supremum of the dimensions of each quotient ring. □

The results in this section highlight the relationship between the Krull dimension of a ring, its localization, and the behavior of prime ideals. By utilizing the concept of minimal prime ideals and applying localization at prime ideals, we can efficiently determine the Krull dimension of a ring and its quotient rings, offering a deeper understanding of the structure of the ring.

2.3 Relationship with integral extensions

One particular and interesting case is those of **integral extensions of rings**, specially useful for polynomial rings (cf. [5, 7]).

Definition 2.8 (extension of rings). *Given two rings A and B, we say that B is an **extension** of A if $A \subseteq B$, meaning that A is a subring of B.*

Definition 2.9 (integral extension). *Given an extension $A \subset B$, we say that $y \in B$ is **integral** over A if there exist $a_0, \dots, a_{n-1} \in A$ such that $y^n + a_{n-1}y^{n-1} + \dots + a_1 y + a_0 = 0$. B is an **integral extension** of A if every element of B is integral over A.*

Before reaching the main theorem of this section, it is useful to mention the **Going-Down** Theorem and the **Going-Up** Theorem for their importance in the proof.

Lemma 2.10 (Going-Down). *Let $A \subseteq B$ be an integral extension of rings. If $\mathfrak{p}$ is a prime ideal in A, then there exists a prime ideal $\mathfrak{q}$ in B such that*

$$\mathfrak{q} \cap A = \mathfrak{p}.$$

That is, every prime ideal of A has at least one prime ideal lying over it in B.

Lemma 2.11 (Going-Up). *Let $A \subseteq B$ be an integral extension of rings. If we have a chain of prime ideals in A:*

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

then there exists a chain of prime ideals in B:

$$\mathfrak{q}_0 \subseteq \mathfrak{q}_1 \subseteq \cdots \subseteq \mathfrak{q}_n$$

such that $\mathfrak{q}_i \cap A = \mathfrak{p}_i$ for each i.

Knowing these definitions and lemmas, we can set the following proposition.

Theorem 2.12. *Given $A \subset B$ integral extension of rings, then $\dim(A) = \dim(B)$.*

Proof. Consider a chain of prime ideals in B of length n, $\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_n$. Taking the contractions of these primes to A, define: $\mathfrak{p}_i = \mathfrak{q}_i \cap A$. By the Lying-Over theorem, no two $\mathfrak{q}_i$'s contract to the same ideal in A, which ensures that:

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

forms a chain in A of the same length. This implies: $\dim(B) \leq \dim(A)$.
Conversely, take a chain of prime ideals in A of length m: $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_m$. By the Going-Up theorem, for each $\mathfrak{p}_i$, there exists a prime ideal $\mathfrak{q}_i$ in B lying over $\mathfrak{p}_i$, forming a corresponding chain:

$$\mathfrak{q}_0 \subsetneq \mathfrak{q}_1 \subsetneq \cdots \subsetneq \mathfrak{q}_m.$$

This shows that: $\dim(A) \leq \dim(B)$. Since we have both $\dim(B) \leq \dim(A)$ and $\dim(A) \leq \dim(B)$, it follows that:

$$\dim(A) = \dim(B).$$

□

2.4 Primary decomposition and Symbolic power of a prime ideal

As outlined in the introduction, this chapter is devoted to the study of Krull's theorem and Krull dimension, which we approach through a constructive methodology. Prime ideals have been emphasized throughout as fundamental objects, whose irreducibility and minimality facilitate the generalization of numerous concepts, such as the Zariski topology, from particular cases to broader frameworks.

In addition to prime ideals, primary ideals also play a significant role. Although they did not originally occupy a central position in the foundational development of commutative algebra, their utility became evident as they provided more efficient pathways for establishing results that would otherwise require intricate arguments relying solely on prime ideals. Furthermore, primary ideals offer a natural framework for the study of decomposition phenomena, often paralleling, in specific contexts, the behavior exhibited by prime ideals.

In keeping with the general approach of this work, we will focus exclusively on definitions and results that are instrumental for the subsequent discussion (cf. [1, 2, 10]).

Definition 2.13. *An ideal $\mathfrak{Q}$ is* ***primary*** *if for any $xy \in \mathfrak{Q}$ then $x \in \mathfrak{Q}$ or $y^n \in \mathfrak{Q}$ for some $n > 0$.*

Proposition 2.14. *Given a primary ideal $\mathfrak{Q}$ of a ring A, the quotient ring $A/\mathfrak{Q}$ satisfies the property that every zero divisor is nilpotent. Conversely, if Q is an ideal such that in $A/\mathfrak{Q}$ every zero divisor is nilpotent, then $\mathfrak{Q}$ is a primary ideal.*

Proof. For the first statement, if $\bar{y} \in A/\mathfrak{Q}$ is a zero divisor, then there exists an $\bar{x} \in A/\mathfrak{Q}$, such that $\bar{x}\bar{y} = \bar{0}$, that is, such that $xy \in \mathfrak{Q}$. Knowing that $\mathfrak{Q}$ is primary, then either $\bar{x} = \bar{0}$, or $\bar{y}^n = \bar{0}$ (for some $n > 0$), that is, they satisfy the nilponent element condition.

Conversely, let $xy \in \mathfrak{Q}$, we want to see that $\mathfrak{Q}$ is primary. In $A/\mathfrak{Q}$, the classes $\bar{x}, \bar{y}$ are zero divisors, therefore nilpotent, that is, there exists a natural number $n > 0$ such that $\bar{y}^n = \bar{0}$, and in that case, $y^n \in \mathfrak{Q}$ (definition of primary ideal).

□

To establish the connection between the relevant properties of primary ideals and those of prime ideals, the following theorem provides an explicit formulation.

Theorem 2.15. *If $\mathfrak{Q}$ is a primary ideal, then* $\mathrm{Rad}(\mathfrak{Q})$ *is a prime ideal. Furthermore, it is the smallest prime ideal containing $\mathfrak{Q}$.*

Proof. The radical of a primary ideal $\mathfrak{Q}$, denoted $\mathrm{Rad}(\mathfrak{Q})$, consists of all elements $x \in A$ such that $x^m \in \mathfrak{Q}$ for some integer $m > 0$. In particular, if $xy \in \mathrm{Rad}(\mathfrak{Q})$, then $(xy)^m \in \mathfrak{Q}$ for some $m > 0$. Since $\mathfrak{Q}$ is a primary ideal, it follows that either $x^m \in \mathfrak{Q}$ or $(y^m)^n = y^{mn} \in \mathfrak{Q}$ for some $n > 0$. In both cases, at least one of the factors lies in $\mathrm{Rad}(\mathfrak{Q})$.

□

In this case, where $\mathfrak{P} = \mathrm{Rad}(\mathfrak{Q})$ is the corresponding prime ideal, we say that $\mathfrak{Q}$ is $\mathfrak{P}$-primary.

Example 2.16. Consider the ring $\mathbb{Z}[x, y]$: the ideals (x^i, y^j) with $i, j \in \mathbb{N}$ are $\mathfrak{P}$-primary, where $\mathfrak{P} = (x, y)$.

However, beyond their connection with prime ideals, primary ideals also preserve their properties under finite intersections in a specific case. Moreover, they allow for a (non-unique) decomposition of certain ideals into primary components.

Lemma 2.17. *Let $\mathfrak{Q}$ and $\mathfrak{P}$ be ideals. Then $\mathfrak{Q}$ is $\mathfrak{P}$-primary if and only if the following conditions are satisfied:*

1. $\mathfrak{Q} \subset \mathfrak{P} \subset \mathrm{Rad}(\mathfrak{Q})$
2. *if $xy \in \mathfrak{Q}$ and $x \notin \mathfrak{P}$, then $y \in \mathfrak{Q}$.*

Theorem 2.18. *If $\mathfrak{Q}_1, \mathfrak{Q}_2, \ldots, \mathfrak{Q}_n$ are all $\mathfrak{P}-$primary ideals, then $\mathfrak{Q} = \cap_{i=1}^n = \mathfrak{Q}_i$ is also a $\mathfrak{P}-$primary ideal.*

Proof. It is easy to show that the radical of $\mathfrak{Q} = \bigcap_{i=1}^n \mathfrak{Q}_i$ is $\mathfrak{P}$:

$$\mathrm{Rad}(\mathfrak{Q}) = \mathrm{Rad}\left(\bigcap_{i=1}^n \mathfrak{Q}_i\right) = \bigcap_{i=1}^n \mathrm{Rad}(\mathfrak{Q}_i) = \bigcap_{i=1}^n \mathfrak{P} = \mathfrak{P}.$$

The equality $\mathrm{Rad}\left(\bigcap_{i=1}^n \mathfrak{Q}_i\right) = \bigcap_{i=1}^n \mathrm{Rad}(\mathfrak{Q}_i)$ holds in general for any finite intersection of ideals in a commutative ring. This follows from the fact that if $x^m \in \bigcap_{i=1}^n \mathfrak{Q}_i$ for some $m > 0$, then $x^m \in \mathfrak{Q}_i$ for all i, so $x \in \mathrm{Rad}(\mathfrak{Q}_i)$ for each i, and thus $x \in \bigcap_{i=1}^n \mathrm{Rad}(\mathfrak{Q}_i)$.

Now suppose that $xy \in \mathfrak{Q}$. Then $xy \in \mathfrak{Q}_i$ for all $i = 1, \ldots, n$. Since each $\mathfrak{Q}_i$ is $\mathfrak{P}$-primary, we have that either $x \in \mathfrak{Q}_i$ or $y^{k_i} \in \mathfrak{Q}_i$ for some $k_i > 0$. If $x \in \mathfrak{Q}_i$ for all i, then clearly $x \in \mathfrak{Q}$. Otherwise, let $N = \max\{k_1, \ldots, k_n\}$. Since $y^{k_i} \in \mathfrak{Q}_i$ implies $y^N \in \mathfrak{Q}_i$ (because ideals are closed under powers), it follows that $y^N \in \mathfrak{Q}_i$ for all i, and thus $y^N \in \mathfrak{Q}$. Therefore, $\mathfrak{Q}$ is also a $\mathfrak{P}$-primary ideal.

□

Finally, certain ideals are decomposable in primary ideals.

Definition 2.19. *An ideal I is said to admit a* ***primary decomposition*** *if it can be written as an intersection $I = \bigcap_{i=1}^n \mathfrak{Q}_i$, where each $\mathfrak{Q}_i$ is a primary ideal (**components**). Moreover, if no $\mathfrak{Q}_j$ contains the intersection $\bigcap_{i \neq j} \mathfrak{Q}_i$, and the radicals $\mathrm{Rad}(\mathfrak{Q}_i)$ are all distinct, then the decomposition is called* ***minimal*** *or* ***irredundant****.*

Observation 2.20. Primary decompositions do not always exist, and when they do, they are not necessarily **unique**.

The main reason for having explored the properties of primary ideals in detail is that, in the next section, when we prove Krull's theorem, the most natural approach involves working with powers of ideals (though not in an arbitrary way). Since powers of prime ideals are not necessarily prime, this presents a serious obstacle when attempting to derive the desired result. However, by modifying the notion of the n-th power to obtain a primary ideal instead, the argument becomes significantly more tractable. Moreover, this modification is not only technically useful but also sheds light on the geometric meaning of ideal powers and highlights which algebraic features are preserved in the process.The modified powers we refer to in this context are precisely the **symbolic powers**.

Definition 2.21. *Let $\mathfrak{p} \subset A$ be a prime ideal. The n-**th symbolic power** of $\mathfrak{p}$ is defined as*

$$\mathfrak{p}^{(n)} := \mathfrak{p}^n A_{\mathfrak{p}} \cap A,$$

that is, the contraction of the n-th ordinary power of $\mathfrak{p}$ in the localization of A at $\mathfrak{p}$.

Proposition 2.22. *The symbolic power $\mathfrak{p}^{(n)}$ satisfies:*

$$\mathfrak{p}^{(n)} = \{f \in A \mid \exists s \notin \mathfrak{p} \text{ such that } sf \in \mathfrak{p}^n\}.$$

Proof. ($\subseteq$) Let $f \in \mathfrak{p}^n A_{\mathfrak{p}} \cap A$. Then there exists $\frac{a}{s} \in \mathfrak{p}^n A_{\mathfrak{p}}$ with $a \in \mathfrak{p}^n, s \notin \mathfrak{p}$ such that $f = \frac{a}{s} \in A$, so $sf = a \in \mathfrak{p}^n$, and hence $f \in \{f \in A \mid \exists s \notin \mathfrak{p}, sf \in \mathfrak{p}^n\}$.

($\supseteq$) Conversely, if $sf = a \in \mathfrak{p}^n$ for some $s \notin \mathfrak{p}$, then in the localization $A_{\mathfrak{p}}$, $f = \frac{a}{s} = \frac{sf}{s} \in \mathfrak{p}^n A_{\mathfrak{p}}$, and since $f \in A$, we conclude $f \in \mathfrak{p}^n A_{\mathfrak{p}} \cap A$. □

We can also comprehend the elements of $\mathfrak{p}^{(n)}$ by employing a canonical projection.

Proposition 2.23. *The symbolic power $\mathfrak{p}^{(n)}$ satisfies:*

$$\mathfrak{p}^{(n)} = \mathrm{Ker}(A \longrightarrow A_{\mathfrak{p}}/\mathfrak{p}^n A_{\mathfrak{p}})$$

Clearly, the elements of $\mathfrak{p}^n$ satisfy the definition of $\mathfrak{p}^{(n)}$, so we have $\mathfrak{p}^n \subset \mathfrak{p}^{(n)}$. The inclusion $\mathfrak{p}^{(n)} \subset \mathfrak{p}$ also holds. To see this briefly, let $f \in \mathfrak{p}^{(n)}$. Then there exists $s \notin \mathfrak{p}$ such that $sf \in \mathfrak{p}^n \subset \mathfrak{p}$. Since $\mathfrak{p}$ is prime and $s \notin \mathfrak{p}$, we must have $f \in \mathfrak{p}$. Therefore, $\mathfrak{p}^{(n)} \subset \mathfrak{p}$. Apart from the inclusion relationship property, both ideals can still be related by examining the primary-like properties of the symbolic power.

Theorem 2.24. *$\mathfrak{p}^{(n)}$ is a $\mathfrak{p}$-primary ideal (primary and $\mathrm{Rad}(\mathfrak{p}^{(\mathrm{n})}) = \mathfrak{p}$).*

Proof. The proof is almost straightforward by applying **Lemma 2.17**. We already know that $\mathfrak{p}^{(n)} \subset \mathfrak{p}$, and of course $\mathfrak{p} \subset \mathrm{Rad}(\mathfrak{p}) \subset \mathrm{Rad}(\mathfrak{p}^{(n)})$. Therefore, we get the chain of inclusions:

$$\mathfrak{p}^{(n)} \subset \mathfrak{p} \subset \mathrm{Rad}(\mathfrak{p}^{(n)}).$$

On the other hand, if $sf \in \mathfrak{p}^{(n)}$ and $s \notin \mathfrak{p}$, then by the definition of $\mathfrak{p}^{(n)}$ (**Proposition 1.57**), we must have $f \in \mathfrak{p}^{(n)}$.

□

Then, by taking any primary decomposition of $\mathfrak{p}^n$, the n-th symbolic power $\mathfrak{p}^{(n)}$ is the $\mathfrak{p}$-primary component.

The symbolic power, besides making it easier to handle chain inclusion conditions (since it restricts the behavior of ordinary powers to the localization of the ring) has also the advantage of being $\mathfrak{p}$-primary, which allows for a stronger and more intrinsic connection with the ideal $\mathfrak{p}$ itself. Moreover, it carries an interesting geometric-algebraic interpretation if we treat the corresponding algebraic varieties. Let's explore this features through some illustrative examples.

Example 2.25. Let us consider the ring $A = k[x, y, z]/(xy - z^2)$, where k is an algebraically closed field. Denote by $\mathfrak{p} = (x, z)$ the prime ideal in A (we will treat x, y, z as the images of the corresponding variables in the quotient ring). Computing the second power of $\mathfrak{p}$, we find:

$$\mathfrak{p}^2 = (x^2, xz, z^2 = xy).$$

First, we observe that $\mathfrak{p}^2$ is not a primary ideal. Indeed, $xy = z^2 \in \mathfrak{p}^2$, yet $x \notin \mathfrak{p}^2$, and $y \notin \sqrt{\mathfrak{p}^2} = \mathfrak{p}$. Hence, $\mathfrak{p}^2$ fails the definition of a primary ideal.

Now consider the element $x \notin \mathfrak{p}^2$. Since $xy = z^2 \in \mathfrak{p}^2$ and $y \notin \mathfrak{p}$, we conclude that $x \in \mathfrak{p}^{(2)}$, which implies the strict inclusion

$$\mathfrak{p}^2 \subsetneq \mathfrak{p}^{(2)}$$

2.5 Noetherian Rings and Krull Dimension

The study of chains in rings, and their natural connection to dimension, leads to a natural generalization in the case of necessarily finite length: Noetherian rings (cf. [3, 6, 7, 9]).

Definition 2.26 (Noetherian rings)**.** *A ring A is called* Noetherian *if it satisfies any (and hence all) of the following equivalent conditions:*

1. *Every ascending chain of ideals in A stabilizes, i.e., for any sequence of ideals*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots,$$

there exists $n \in \mathbb{N}$ such that $I_n = I_{n+1} = I_{n+2} = \cdots$.

2. *Every ideal of A is finitely generated.*

Generally speaking, Noetherian rings have particular features that make them algebraically interesting by themselves. In particular, the stabilization of ascending chains impacts all the concepts previously discussed in detail (height, coheight, Krull dimension, ...), giving rise to the **Krull Principal Ideal Theorem** and the **Height Theorem**.

In the following proofs, we will use of **Artinian rings**, as they satisfy the **Descending Chain Condition (DCC)** on ideals. This property makes them particularly well-suited for arguments involving powers of ideals, where descending chains often arise naturally.

Definition 2.27. *A ring R is called* Artinian *if it satisfies the* descending chain condition *(DCC) on ideals. That is, for every descending chain of ideals*

$$I_1 \supseteq I_2 \supseteq I_3 \supseteq \cdots$$

there exists an integer $n \geq 1$ such that

$$I_n = I_{n+1} = I_{n+2} = \cdots.$$

Equivalently, every non-empty collection of ideals of R has a minimal element with respect to inclusion.

Lemma 2.28. *A Noetherian Ring of Krull dimension 0 is Artinian.*

Theorem 2.29 (Krull Principal Ideal Theorem)**.** *Let A be a Noetherian ring and $x \in A$. If $\mathfrak{p}$ is a prime ideal in A minimal over (x) (there is no prime ideal q st $(x) \subset \mathfrak{q} \subsetneq \mathfrak{p}$), then* $\text{height}(\mathfrak{p}) \leq 1$.

Proof. Consider the following length two chain of prime ideals $\mathfrak{q}_0 \subset \mathfrak{q} \subset \mathfrak{p}$, with $(x) \subseteq \mathfrak{p}$ minimal over (x). We can always convert it into a length one chain by taking the quotient $A/\mathfrak{q}_0$ and work with the quotient ideals (they exist there becuase they contain $\mathfrak{q}_0$)

$$0 \subset \mathfrak{q}/\mathfrak{q}_0 \subset \mathfrak{p}/\mathfrak{q}_0$$

Furthermore, if we take the localisation $A_\mathfrak{p}$ (with A now the quotient), we obtain a local Noetherian ring $(A_\mathfrak{p}, \mathfrak{p}A_\mathfrak{p})$, with $\mathfrak{p}A_\mathfrak{p}$ maximal and minimal over the image of (x). In order to simplify the notation, we will write the ideals as if we were on $A/\mathfrak{q}_0$ and having the chain $0 \subset \mathfrak{q} \subset \mathfrak{p}$. If we prove that $\mathfrak{q} = 0$ we would have proven our theorem.

Now, consider the ring A/xA, there the only prime ideal is $\mathfrak{p}/xA$, because $\mathfrak{q}$ disappears (it doesn't contain (x)), and since it is a Noetherian ring with Krull dimension, it is also Artinian by **Lemma 2.28**.

As we have discussed in the previous section, the symbolic power $\mathfrak{q}^{(t)} = \mathfrak{q}^t A_\mathfrak{q} \cap A \subset A$ is $\mathfrak{q}-$primary for every $t \in \mathbb{N}$. If we take the quotient of these ideals to A/xA, we fall into an Artinian ideal, and even if they are not necessarily ideals, the descending chain $\{\bar{\mathfrak{q}}^{(t)} = xA + \mathfrak{q}^{(t)}\}_{t>0}$ satisfies the *DCC* (Artinian), therefore, there exists a $n > 0$ such that

$$xA + \mathfrak{q}^{(t)} = xA + \mathfrak{q}^{(t+1)}, \quad \forall t \geq n$$

This implies that for every $v \in \mathfrak{q}^{(t)}$, there exists $w \in \mathfrak{q}^{(t+1)}$ and $a \in A$, such that $v = w + xa$. Due to the inclusion $\mathfrak{q}^{(t+1)} \subset \mathfrak{q}^{(t)}$, $v - w = xa \in \mathfrak{q}^{(t)}$. Knowing that $x \notin \mathfrak{q} = \text{Rad}(\mathfrak{q}^{(t)})$ and applying **Lemma 2.17**, we obtain that $a \in \mathfrak{q}^{(t)}$ ($\mathfrak{q}^{(t)} \subseteq \mathfrak{q}^{(t+1)} + x\mathfrak{q}^{(t)}$). By using the chain inclusions, we obtain

$$\mathfrak{q}^{(t)} = \mathfrak{q}^{(t+1)} + x\mathfrak{q}^{(t)}$$

By applying **Lemma 1.12** ($x \in \text{Rad}(A_\mathfrak{q}) = A_\mathfrak{p}$), then $\mathfrak{q}^{(t)} = \mathfrak{q}^{(t+1)}$, and by the *DCC*, $\mathfrak{q}^{(t)} = \mathfrak{q}^{(t+1)} = \mathfrak{q}^{(n)}$.

By the discussion above, A is a domain, then the homomorphism $f : A \longrightarrow A_\mathfrak{q}$ is **injective**, otherwise, if $0 \neq y \in ker(f)$, then $\frac{y}{1}$ would be a zero divisor in $A_\mathfrak{q}$, and therefore in A, and $A_\mathfrak{q}$ is also a domain. In addition, the homomorphism $\mathfrak{q}^{(t)} \longrightarrow \mathfrak{q}^{(t)} A_\mathfrak{q}$ is surjective (all its elements are contained in $\mathfrak{q}$ before and after localizing).

After localizing to $A_\mathfrak{q}$, there the symbolic power and the usual power are the same by definition, $\mathfrak{q}^{(t)} A_\mathfrak{q} = (\mathfrak{q}A_\mathfrak{q})^t$: since $\mathfrak{q}^{(t)} \subseteq \mathfrak{q}^t A_\mathfrak{q}$, we have $\mathfrak{q}^{(t)} A_\mathfrak{q} \subseteq \mathfrak{q}^t A_\mathfrak{q} = (\mathfrak{q}A_\mathfrak{q})^t$, and conversely, any element $\frac{a}{s} \in (\mathfrak{q}A_\mathfrak{q})^t$, with $a \in \mathfrak{q}^t$ and $s \in \mathfrak{q}$, satisfies $a \in \mathfrak{q}^{(t)}$, hence $\frac{a}{s} \in \mathfrak{q}^{(t)} A_\mathfrak{q}$.

If we take $\mathfrak{J} = \bigcap \mathfrak{q}^{(t)} = \mathfrak{q}^{(n)} \subseteq \bigcap \mathfrak{q}^{(t)} A_\mathfrak{q} = \bigcap (\mathfrak{q}A_\mathfrak{q})^t$, and knowing that in a proper ideal $\mathfrak{q}A_\mathfrak{q}$ of a local ring, the intersection of all usual powers is zero $\bigcap (\mathfrak{q}A_\mathfrak{q})^t = 0$, then

$$\mathfrak{J} = \mathfrak{q}^{(n)} \subseteq \bigcap (\mathfrak{q}A_\mathfrak{q})^t = 0$$

Finally, because of $\mathfrak{q}^n \subset \mathfrak{q}^{(n)} = 0$, and knowing that in a domain if the power of an ideal is zero then the ideal is zero too, we obtain $\mathfrak{q} = 0$, as desired.

□

Corollary 2.30. *Let A be a ring of finite dimension and $f \in A$ such that it doesn't belong to any minimal prime ideal in A, then* $\dim(A/(f)) < \dim(A)$. *Furthermore, if A is Noetherian and f is not a unit then* $\dim(A/(f)) = \dim(A) - 1$.

Proof. As previously discussed, prime ideals in $A/(f)$ are in one-to-one correspondence with the prime ideals of A that contain (f). Suppose we have a chain of prime ideals in $A/(f)$ of length $\dim(A/(f))$, with $\mathfrak{p}$ being its minimal element. Given the assumption that f is not contained in any minimal prime of A, there must exist at least one minimal prime ideal $\mathfrak{q} \subseteq \mathfrak{p}$ in A. This implies that the corresponding chain of prime ideals in A has greater length, extending the original chain.

Now suppose we have a chain of prime ideals $\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \cdots \subset \mathfrak{p}_d$ in $A/(f)$ of length $d = \dim(A/(f))$. Consider the inverse image of this chain in A, all containing (f). By Krull's Principal Ideal Theorem, the height of any minimal prime over the principal ideal (f) is at most one. Therefore, it must be exactly one in this case, because $\mathfrak{p}_0$ is not minimal in A, i.e., $\mathrm{ht}(\mathfrak{p}_0) = 1$. This implies that the corresponding chain in A can be extended one step further below $\mathfrak{p}_0$, giving a chain of length $d + 1$ in A. Hence, $\dim(A) = d + 1$.

□

Theorem 2.31 (The Height Theorem)**.** *Let A be a Noetherian ring, and $\mathfrak{I}$ a finitely generated ideal (by n elements). If $\mathfrak{p}$ is the minimal prime ideal over $\mathfrak{I}$ in A, then* $\mathrm{height}(\mathfrak{p}) \leq n$.

Proof. We prove this by induction on n, assuming the case $n - 1$ holds (the case $n = 1$ is established by the Krull Principal Ideal Theorem).

Let $\mathfrak{I} = (x_1, \ldots, x_n)$. Upon localizing at $A_{\mathfrak{p}}$, the ideal $\mathfrak{p}$ becomes the unique maximal ideal of the localized ring. Since $\mathfrak{p}$ is minimal over $\mathfrak{I}$, we have $\mathfrak{p} = \mathrm{Rad}(\mathfrak{I}) = \mathrm{Rad}(x_1, \ldots, x_n)$.

Let $\mathfrak{q}$ be a prime ideal such that the chain $\mathfrak{q} \subsetneq \mathfrak{p}$ is saturated; that is, there is no prime ideal strictly between $\mathfrak{q}$ and $\mathfrak{p}$, and $\mathfrak{q} \neq \mathfrak{p}$. Then there must exist some $x_i \notin \mathfrak{q}$, say x_1. This implies that $\mathfrak{p}$ is minimal over $\mathfrak{q} + x_1 A$, and by a similar argument as for $\mathfrak{I}$, we get $\mathrm{Rad}(\mathfrak{q} + x_1 A) = \mathfrak{p}$. By the definition of the radical, for each $i \geq 2$, there exist $y_i \in \mathfrak{q}$, $n_i \in \mathbb{N}$, and $a_i \in A$ such that

$$x_i^{n_i} = y_i + a_i x_1$$

Using the following two properties of radical ideals (for ideals $I, J \subset A$):

1. $I \subset J \Rightarrow \mathrm{Rad}(I) \subset \mathrm{Rad}(J)$
2. $\mathrm{Rad}(\mathrm{Rad}(I)) = \mathrm{Rad}(I)$

we obtain the following inclusions:

1. $x_i^{n_i} \in (x_1, y_2, \ldots, y_n) \Rightarrow x_i \in \mathrm{Rad}(x_1, y_2, \ldots, y_n)$, hence $\mathfrak{I} = (x_1, \ldots, x_n) \subseteq \mathrm{Rad}(x_1, y_2, \ldots, y_n)$
2. $y_i = x_i^{n_i} - a_i x_1 \in (x_1, x_i) \subseteq (x_1, \ldots, x_n) = \mathfrak{I} \Rightarrow (x_1, y_2, \ldots, y_n) \subseteq \mathfrak{I}$

Taking radicals on both sides of these inclusions yields $\mathrm{Rad}(x_1, y_2, \ldots, y_n) \subseteq \mathrm{Rad}(\mathfrak{I}) = \mathfrak{p}$ and $\mathrm{Rad}(\mathfrak{I}) \subseteq \mathrm{Rad}(\mathrm{Rad}(x_1, y_2, \ldots, y_n)) = \mathrm{Rad}(x_1, y_2, \ldots, y_n)$, hence

$$\mathrm{Rad}(x_1, y_2, \ldots, y_n) = \mathrm{Rad}(\mathfrak{I}) = \mathfrak{p}$$

Now, consider the quotient ring $\bar{A} = A/(y_1, \ldots, y_n)$, where $\bar{y}_i = 0$ for all i, and define $\mathfrak{J} = (x_1, y_2, \ldots, y_n)$, so that $\bar{\mathfrak{J}} = (\bar{x}_1)$, a principal ideal in $\bar{A}$. Since $\text{Rad}(\mathfrak{J}) = \mathfrak{p}$, it follows that $\text{Rad}(\bar{\mathfrak{J}}) = \text{Rad}(\bar{x}_1) = \bar{\mathfrak{p}}$, and we can apply the Krull Principal Ideal Theorem. In this context, the existence of $\mathfrak{q} \subsetneq \mathfrak{p}$ implies $\text{height}(\bar{\mathfrak{p}}) = 1$. Specifically, the chain $0 \subsetneq \bar{\mathfrak{q}} \subsetneq \bar{\mathfrak{p}}$ holds, with $\bar{\mathfrak{q}}$ being a minimal prime in $\bar{A}$. Both $\mathfrak{p}$ and $\mathfrak{q}$ are prime ideals containing $(y_2, \ldots, y_n)$: $\mathfrak{p}$ does so as the radical of the ideal, while $\mathfrak{q}$ contains its generators explicitly, since $y_i \in \mathfrak{q}$ for all i. Thus, going back to A, $\mathfrak{q}$ is a minimal prime over $(y_2, \ldots, y_n)$, and by the induction hypothesis, $\text{height}(\mathfrak{q}) \leq n - 1$, yielding the desired conclusion:

$$\text{height}(\mathfrak{p}) = \text{height}(\mathfrak{q}) + 1 \leq n$$

□

Example 2.32. Consider the ring $k[x, y, z]$, where k is a field (not necessarily algebraically closed). Since k is Noetherian (it has only two ideals, (0) and k), the Hilbert Basis Theorem implies that $k[x, y, z]$ is also Noetherian.

Let us take the ideal $I = (x, y)$. This ideal is prime because the quotient ring satisfies

$$k[x, y, z]/(x, y) \cong k[z],$$

and $k[z]$ is a domain, since k is a domain.

Therefore, by the Height Theorem, we conclude that

$$\text{height}(I) \leq 2.$$

As an explicit example of a chain of prime ideals, we can take

$$(0) \subset (x) \subset (x, y),$$

which is a saturated chain of prime ideals. Here, (0) is prime because $k[x, y, z]$ is a domain.

2.6 Krull dimension of Polynomial Rings

To keep the development of this concept consistent with our interests, let's focus on the importance of these concepts in the particular case of polynomial rings. Among their particularities, the most illustrative one is that they are generated by variables that also have an intrinsic notion of independence, allowing us to treat any ring (or algebra) over a field as an extension of a polynomial subring. Before presenting the main results that show how Krull dimension behaves in such rings, it is necessary to provide a brief discussion and some definitions related to their algebra and some new concepts associated with them (cf. [2, 7, 8, 9]).

Definition 2.33 (Fraction Field)**.** *Given a ring A, its fraction field,* $\text{Frac}(A)$ *is given by $A \times (A - \{0\})/\sim$, where $\sim$ is the equivalence relation of **Definition 1.15**.*

Definition 2.34 (Trascendence Degree)**.** *Let K be a field extension of a field k. A subset $\{x_1, \ldots, x_n\} \subseteq K$ is called **algebraically independent** over k if there is no non-zero polynomial $f \in k[X_1, \ldots, X_n]$ such that $f(x_1, \ldots, x_n) = 0$. The **transcendence degree** of K over k, denoted* $\text{tr.deg}_k K$, *is the cardinality of a maximal algebraically independent subset of K over k.*

Observation 2.35. If $\{x_1, \ldots, x_n\} \subseteq K$ is an algebraically independent set over k, then the field extension $k(x_1, \ldots, x_n) \subseteq K$ is a purely transcendental extension of transcendence degree n. In this case, we can write $K = k(x_1, \ldots, x_n)$ if and only if K contains no further algebraic elements over $k(x_1, \ldots, x_n)$, that is, if K is a purely transcendental extension.

Lemma 2.36 (Noether Normalization). *Let A be a finitely generated k-algebra, where k is a field. Then there exist algebraically independent elements $y_1, \ldots, y_d \in A$ such that A is integral over the subalgebra $k[y_1, \ldots, y_d]$.*

In this context, "normalizing" a finitely generated k-algebra A means finding a polynomial subring $k[y_1, \ldots, y_d] \subseteq A$ such that A is integral over it. The variables y_i are algebraically independent, and the number d corresponds to the transcendence degree of the field of fractions of A over k. Thus, Noether's Normalization Lemma allows us to compare A with a polynomial ring of the same transcendence degree. We are now ready to use these tools to analyze the Krull dimension of polynomial rings through two complementary approaches.

We shall present two different proofs of the classical result that the Krull dimension of the polynomial ring $k[x_1, \ldots, x_n]$ is n. The first approach, presented here, is based on the conceptual framework developed so far. The second proof (analyzed in Chapter 3) takes a more elementary and direct path, relying on a different notion (the **boundary** of an element $a \in A$) reaching the same conclusion through alternative definitions. Together, these perspectives illustrate both the power and flexibility of the tools available in commutative algebra when studying dimension.

Theorem 2.37. *Let k be a field. Given the polynomial ring $k[x_1, \ldots, k_n]$, its Krull dimension is n.*

Proof. Given that the variables $x_1, \ldots, x_n$ are algebraically independent, then we can build the chain of prime ideals $(0) \subset (x_1) \subset (x_1, x_2) \subset \ldots \subset (x_1, x_2, \ldots, x_n)$ as we already know, Krull dimension refers to a supremum of heights, thus:

$$\dim(k[x_1, \ldots, x_n]) \geq n$$

In order to prove the equality, lets take a general prime ideals chain of arbitrary length d

$$(0) \subset \mathfrak{p}_1 \subset \mathfrak{p}_2 \subset \ldots \subset \mathfrak{p}_d$$

where $\mathfrak{p}_1$ is minimal over (0). Among the particularities of a polynomial ring, we will highlight the fact that it is a **unique factorization domain**. Therefore, any irreducible $f \in A$ generates a prime ideal because if $ab \in (f)$, then, by the unique factorization property, either $a \in (f)$ or $b \in (f)$, which satisfies the definition of a prime ideal. For this reason, if we take $f \in \mathfrak{p}_1$, then $(f) = \mathfrak{p}_1$ by appealing to the minimality of $\mathfrak{p}_1$ over (0).

Finally, let's work on $A = k[x_1, \ldots, x_n]/(f)$ to determine the value of d. If we take the fractions field of $k[x_1, \ldots, x_n]$, that is $\text{Frac}(k[x_1, \ldots, x_n]) = k(x_1, \ldots, x_n)$, its trascendence degree is n. By taking the quotient, we are imposing an **algebraic relationship** between the variables $(f = 0)$, reducing the trascendence degree of its fractions field, $\text{Frac}(A)$ at least by one, that is, $\text{tr.deg}_k\, Frac(A) \leq n - 1$. We can also, remark that A is a k-algebra, and by Noether Normalization Lemma, A is finite over a polynomial ring with at most $n - 1$ variables (by **Observation 2.35**). Therefore, by **Theorem 2.12**, $\dim(A) \leq n - 1$.

Now, the chain of prime ideals defined above, becomes (in A) $(0) \subset \mathfrak{p}_2/\mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_d/\mathfrak{p}_1$ implying $d-1 \leq \dim(A) \leq n-1$, giving $d \leq \dim(k[x_1,\ldots,x_n]) = \dim(A)+1 \leq n$, and therefore the desired result: $\dim(k[x_1,\ldots,x_n]) = n$.

□

Corollary 2.38. *Let k be a field, if $f \in k[x_1,\ldots,x_n]$ is irreducible, then*

$$\dim(k[x_1,\ldots,x_n]/(f)) = n-1$$

Example 2.39. Let $k = \mathbb{Q}$ and consider the polynomial ring $\mathbb{Q}[x,y]$. Then by Theorem 1.74, $\dim(\mathbb{Q}[x,y]) = 2$. Now take the irreducible polynomial $f = x^2+y^2-1$. By Corollary 1.75, the Krull dimension of the quotient ring becomes

$$\dim(\mathbb{Q}[x,y]/(x^2+y^2-1)) = 1.$$

Geometrically, this corresponds to the fact that the unit circle defined by $x^2+y^2=1$ is a 1-dimensional variety in the affine plane.

2.7 Application to affine varieties

2.7.1 Krull Dimension in Affine Spaces

After developing the ring-theoretic framework and tools based on prime ideals that naturally lead to the concept of Krull dimension and related results, it is useful to explore how this concept applies to geometric objects in familiar spaces (e.g., affine subsets of $\mathbb{R}^n$ or $\mathbb{C}^n$). The Nullstellensatz and Zariski topology allow us to describe such objects using polynomial rings, which (once the definition of Krull dimension is known) makes it possible to determine their dimension algebraically. This method is straightforward and avoids reliance on differentiability, requiring only the equations that define the objects. Moreover, the concept of the height of an ideal enables us to compute the dimension of objects whose geometric dimension is not immediately evident. As a first step, we present the following proposition, which connects the Krull dimension to the geometric dimension of a set (cf. [1, 3, 9]).

Proposition 2.40. *Let k be a field and let $I \subseteq k[x_1,\ldots,x_n]$ be a proper ideal. Then,*

$$\dim_K(k[x_1,\ldots,x_n]/I)$$

gives the geometric dimension of the affine algebraic set defined by I, that is, the number of independent parameters required to describe the set.

Let's explore some interesting examples.

Example 2.41 (The Parabola)**.** Consider the real affine plane $\mathbb{A}^2_{\mathbb{R}}$. The equation for a parabola in this space is $y-x^2=0$ which defines the algebraic variety $V(y-x^2)$, corresponding to the ideal $I=(y-x^2) \subset \mathbb{R}[x,y]$. We claim that this ideal is **prime**. To prove it, we show that the quotient ring $\mathbb{R}[x,y]/(y-x^2)$ is an integral domain. In fact, we will prove that there is a ring isomorphism $\mathbb{R}[x,y]/(y-x^2) \cong \mathbb{R}[x]$. Define a ring homomorphism

$$\varphi : \mathbb{R}[x,y] \longrightarrow \mathbb{R}[x]$$

by setting $\varphi(x) = x$ and $\varphi(y) = x^2$. Clearly, φ is a surjective ring homomorphism because any element of $\mathbb{R}[x]$ is of the form $f(x) = f(x, x^2) \in \text{Im}(\varphi)$, and any polynomial $f(x, y) \in \mathbb{R}[x, y]$ is sent to $f(x, x^2) \in \mathbb{R}[x]$.

Now, the kernel of φ consists of all polynomials $f(x, y)$ such that $f(x, x^2) = 0$. That is:

$$\ker \varphi = (y - x^2).$$

Hence, by the Isomorphism Theorem, $\mathbb{R}[x, y]/(y - x^2) \cong \text{Im}(\varphi) = \mathbb{R}[x]$, which is an integral domain. Therefore, $(y - x^2)$ is a prime ideal. Now, taking advantage from the proven isomorphism, and knowing from **Theorem 2.37** that $\dim(\mathbb{R}[x]) = 1$, then obviously,

$$\dim(\mathbb{R}[x, y]/(y - x^2) = 1$$

as expected. One can also consider the maximal ideal $\mathfrak{m} = (x, y)$ corresponding to the vertex of the parabola, getting the chain $(y - x^2) \subset (x, y)$ which corresponds, under the quotient by $(y - x^2)$, to the chain $(0) \subset (x)$ in the ring $\mathbb{R}[x]$, where (x) is a maximal ideal (by taking the quotient again, $\mathbb{R}[x]/(x) \cong \mathbb{R}$, we obtain a field, confirming that (x) is indeed maximal). This approach makes it especially clear that the Krull dimension of the **parabola** is 1, while the **vertex**, being a point (maximal ideal), has dimension 0. The use of ideal chains and successive quotients provides a direct algebraic pathway to these geometric intuitions.

Example 2.42 (Cone)**.** Consider the cone defined by the affine variety $V(xy - z^2)$ in the affine space $\mathbb{A}^3_{\mathbb{R}}$. By using the same arguments as for the parabola, we know that $\mathbb{R}[x, y, z]/(xy - z^2) \cong \mathbb{R}[x, y]$ based on the homomorphism $\varphi(xy) = z^2$ and $\varphi(z) = z$, and therefore $(xy - z^2)$ is a prime ideal. Let's take two different approaches that provide different and complementary information about this algebraic object:

1. **Irreducibility:** Since f is quadratic, if it is reducible it must factor as a product of two linear polynomials $xy-z^2 = (a_1x+b_1y+c_1z+d_1)(a_2x+b_2y+c_2z+d_2)$. Comparing coefficients, we get $a_1a_2 = 0, \quad b_1b_2 = 0, \quad a_1b_2+b_1a_2 = 1, \quad c_1c_2 = -1$ and all other coefficients zero. These conditions lead to contradictions, since for example $a_1 = 0$ implies $c_1 = 0$, contradicting $c_1c_2 = -1$. Hence, no such factorization exists and f is irreducible. By applying **Corollary 2.38**, we get by a straightforward application of the concluding results obtained before, that $\dim(\mathbb{R}[x, y, z]/(xy - z^2)) = 3 - 1 = 2$.

2. **Chain arguments:** As we know from basic geometry, a cone can be defined by its generatrices, which each one correspond naturally to a prime ideal. For any $\lambda \geq 0$, the ideal $P_\lambda = (y - \lambda x, \quad z - \sqrt{\lambda}x)$ is prime and satisfies $(xy - z^2) \subseteq P_\lambda$:

   1. *Containment:* Substitute $y = \lambda x$, $z = \sqrt{\lambda}x$ into $xy - z^2$:

   $$xy - z^2 = x(\lambda x) - (\sqrt{\lambda}x)^2 = \lambda x^2 - \lambda x^2 = 0,$$

   hence $xy - z^2 \in P_\lambda$.

   2. *Primality:* Since P_λ defines a line (an irreducible variety), it is a prime ideal.

   Therefore, $(xy - z^2) \subseteq P_\lambda$ and P_λ corresponds to a generatrix line of the cone $V(xy - z^2)$. Similarly, for each $\mu \geq 0$, the ideal $Q_\mu = (x - \mu y, \quad z - \sqrt{\mu}y)$ is prime and contains the ideal $(xy - z^2)$. Thus, we obtain chains of prime ideals

   $$(xy - z^2) \subset Q_\mu \subset (x, y, z) \quad ; \quad (xy - z^2) \subset P_\lambda \subset (x, y, z)$$

where the maximal ideal (x, y, z) corresponds to the vertex $(0, 0, 0)$. Considering the quotient ring $\mathbb{R}[x, y, z]/(xy - z^2)$ these chains show that its Krull dimension is 2, since (x, y, z) corresponds to a point of dimension 0 (the vertex), and P_λ, Q_μ correspond to lines of dimension 1 on the cone.

Example 2.43 (Non-prime ideal)**.** Consider the ideal $I = (x(x-1),\ x(y-1)) \subset \mathbb{R}[x, y]$. Its associated variety $V(I) \subset \mathbb{A}^2_{\mathbb{R}}$ is the union of the line $x = 0$ and the point $(1, 1)$ (see Figure 2). The ideal I is clearly not prime, for instance, the generator $x(x-1)$ is the product of two elements $x, x-1 \in \mathbb{R}[x, y]$, neither of which lies in I. To compute the height of I, we apply the general definition (**Definition 2.2**), which considers chains of prime ideals containing I, and selects the one with maximal length (where lengths are counted starting from 0, in line with the definitions of height and Krull dimension). We find the following two relevant chains,

$$I \subset (x-1, y-1),$$

$$I \subset (x) \subset (x, y-a), \quad a \in \mathbb{R}.$$

The first chain corresponds to the point $(1, 1)$, whose associated ideal is the maximal ideal $(x-1, y-1)$. The second chain corresponds to the line $x = 0$, that is, the prime ideal (x) represents the generic point of the line, and $(x, y-a)$ corresponds to the maximal ideals at the individual points $(0, a)$ on it. Therefore, the longest chain has length 2, and we conclude,

$$\dim(\mathbb{R}[x, y]/I) = 1.$$

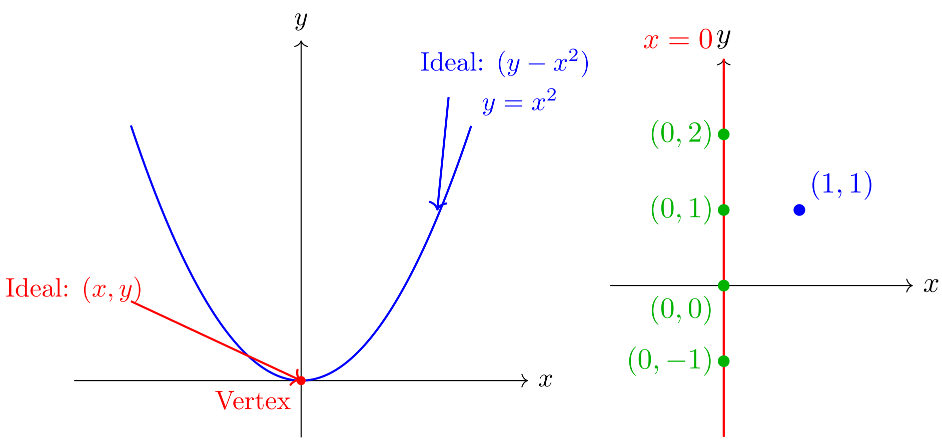


Figure 1: **Parabola**: Scheme of the parabola $y = x^2 \subset \mathbb{R}[x, y]$ as an affine variety, where the point $(x, y) = (0, 0)$ corresponds to the maximal ideal (x, y), and the entire parabola corresponds to the ideal $(y - x^2)$. **Non-prime ideal**: The variety $V(I)$ for $I = (x(x-1), x(y-1))$, consisting of the line $x = 0$ and the isolated point $(1, 1)$. The figure shows the line with several sample points $(0, a)$, illustrating the family of maximal ideals $(x, y-a)$, and highlights the point $(1, 1)$ corresponding to the maximal ideal $(x-1, y-1)$.

2.7.2 Nullstellensatz in Affine Spaces

We now explore a few illustrative examples to briefly and simply demonstrate how Hilbert's Nullstellensatz can be applied to study the irreducibility of ideals in a given ring, as well as the possibility of decomposing them, as discussed in detail in the previous sections.

Example 2.44 (Parabola)**.** The ideal $J = (y - x^2)$ is prime, and therefore radical. By the Nullstellensatz:

$$\mathrm{Rad}(J) = J, \quad \text{and} \quad I(V(J)) = J.$$

Example 2.45 (Maximal ideal)**.** Let $\mathfrak{m} = (x - a, y - b)$ be a maximal ideal. Then:

$$V(\mathfrak{m}) = \{(a, b)\}, \quad I(\{(a, b)\}) = \mathfrak{m}.$$

This is a radical ideal, and the Nullstellensatz ensures this correspondence between points and maximal ideals.

Example 2.46 (Non-radical ideal)**.** Let $J = ((y - x^2)^2)$. Then:

$$\mathrm{Rad}(J) = (y - x^2), \quad V(J) = V(y - x^2).$$

Since $J \neq \mathrm{Rad}(J)$, we have $I(V(J)) = \mathrm{Rad}(J) \neq J$, illustrating the necessity of passing to the radical ideal.

Example 2.47 (Reducible variety)**.** We have:

$$V(xy) = V(x) \cup V(y).$$

The ideal (xy) is radical but not prime:

$$I(V(xy)) = \mathrm{Rad}\,(xy) = (xy) = (x) \cap (y).$$

The Nullstellensatz still applies, and reflects the fact that the variety is reducible.

3 Chapter 3: Krull dimension and Nullstellensatz in Constructive Mathematics

3.1 Constructive Mathematics

In the previous chapter, we treated all the algebraic concepts with classical tools, starting from general definitions and properties of the different kinds of ideals, rings, and the consequent results such as the Hilbert Nullstellensatz, Zariski topology, and Krull dimension. Although the path followed has a logical sequence and the need for new concepts and theorems arises naturally, the explicit form of the mathematical objects is barely needed; instead, we focus on their algebraic properties.

For instance, even if we gave examples and a geometrical meaning to the n-th symbolic power of a prime ideal, $\mathfrak{p}^{(n)}$, in the proof of **Theorem 2.29** we only needed to apply its $\mathfrak{p}$-primarity and good behavior in descending inclusion chains. This procedure, where the explicit form of the object defined in the developed theory is not necessary to obtain meaningful and useful results, is what we name the **classical approach**.

In contrast, a **constructive approach** relies on building logical pathways by explicitly manipulating algebraic objects that may not carry strong intrinsic meaning and might even seem too elementary or of limited practical use. However, through a detailed treatment of their elements or algebraic form, more sophisticated objects, such as prime ideals or Krull dimension, emerge naturally as direct consequences. These can then be described precisely and explicitly, as they represent the culmination or completion of the initial constructive process. Consequently, this approach facilitates the computability of these concepts and gives a direct description where all the intermediate concepts introduced in the classical approach are not needed.

Nonetheless, following a constructive procedure may result in a lack of context for the objects being introduced or defined, context which is more thoroughly developed within the classical framework. On the other hand, remaining solely within the constructive perspective may lead to the omission of relevant results due to their explicit or computational nature. For this reason, and for the sake of completeness, we have chosen to contrast both frameworks, offering the reader two different yet complementary perspectives on the same underlying ideas.

This analysis is grounded in the work of H. Lombardi, T. Coquand, and collaborators, who established the methodology and foundations of constructive mathematics, particularly in their reformulation of Krull dimension and the Nullstellensatz within a framework that emphasizes explicit algorithms and avoidal of non-constructive principles (cf. [11, 12, 13, 14, 15]).

3.1.1 Differences between classical and constructive approaches

Before beginning the constructive treatment, it is necessary to state the concrete differences and to identify the classical axioms that will be excluded (or replaced by others) in order to obtain results consistent with the desired level of explicitness (cf. [12, 15]).

- **Law of excluded middle:** In classical algebra, reasoning often relies on the axiom that "a given proposition is either true or false." For instance, statements such as "a given ideal is either prime or not," or "a given polynomial is either irreducible or can be factored into lower-degree polynomials," illustrate this. However, this dichotomy is generally not algorithmically decidable, which becomes a limitation when attempting to develop computational versions of properties like irreducibility. For this reason, the law of excluded middle is only applied in contexts where the treated elements are given explicitly, prioritizing the direct provability of a given proposition.

- **Zorn's lemma and Axiom of Choice(AoC):** Since both rely on existential logic, they often do not provide an explicit characterization of the maximal element (in the case of Zorn's lemma) or the defined choice function between sets and elements (in the case of the Axiom of Choice), especially when dealing with infinite or non-countable indexing sets. In constructive contexts, their use is not entirely excluded, provided that the resulting objects are explicit and computable, for instance, Zorn lemma is applied when we treat with countable or finitely generated algebraic structures, or when ascending chains and inductive arguments are employable. AoC is preserved if the choice function is explicit and the indexed set is finite or countable.

Among the motivations for these changes, many authors highlight classical conclusions that defy intuition and physical reality, such as **the Banach-Tarski theorem**, which is a direct consequence of the Axiom of Choice within the **ZFC** (Zermelo-Fraenkel set theory with Choice) framework. Constructive approaches aim to replace such paradoxes with more practical statements that align better with intuition and observable reality.

3.2 Constructive version of prime ideals

Prime ideals constitute a central part of this work. One of their key properties is localization, which will also be addressed within this constructive framework. The fundamental objects from which prime ideals arise will be referred to as **potential primes** (cf. [11, 12]).

3.2.1 Potential Primes

Definition 3.1 (Potential Primes)**.** *Given a ring A, a potential prime is a pair $P = (R; T)$, where $R, T \subseteq A$.*

We define the following properties:

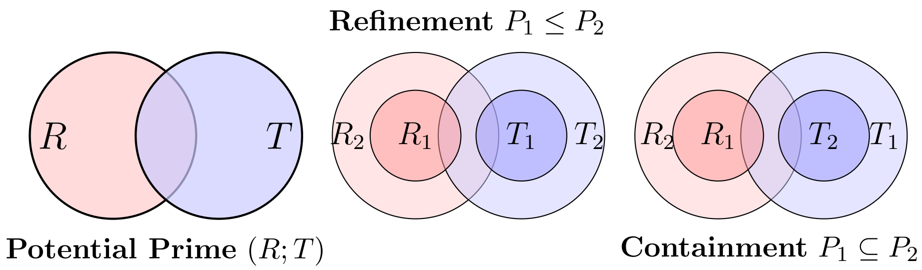
Definition 3.2. *Let $P = (R; T)$, $P_1 = (R_1; T_1)$ and $P_2 = (R_2; T_2)$ be a potential primes.*

1. *P_1 **refines** P_2 ($P_2 \leq P_1$) if $R_2 \subseteq R_1$ and $T_2 \subseteq T_1$.*
2. *P_1 **contains** P_2 ($P_2 \subseteq P_1$) if $R_2 \subseteq R_1$ and $T_1 \subseteq T_2$.*
3. *To each potential prime P we associate the monoid (multiplicative set with identity) $S(P) = \langle R \rangle + M(T)$, where $\langle R \rangle$ is the ideal generated by the set R in A, and $M(T)$ the monoid generated by T. The localization of the potential prime P in A is given by the same equivalence relation of **Definition 1.15**, that is $S(P)^{-1}A = (A \times S)/\sim$.*
4. *A potential prime **collapses** if $0 \in S(P)$.*
5. *A potential prime is said **complete** if R is an ideal, T is a monoid and $T = R + T$.*

6. *A potential prime is said* ***saturated*** *if given a $x \in A$ the following implications hold:*
   - *If $(R \cup \{x\}; T)$ collapses, then $x \in T$.*
   - *If $(R; T \cup \{x\})$ collapses, then $x \in R$.*

Using this general definitions, we define a prime ideal as follows.

Definition 3.3. *A prime ideal is a potential prime with the form $(\mathfrak{p}, S = A \setminus \mathfrak{p})$, where $\mathfrak{p}$ is a prime ideal.*



Actually, **Definition 3.3** only recovers the classical notion. Therefore, to construct a prime ideal using the concepts introduced in **Definition 3.2**, we must characterize it as a potential prime possessing elementary set-theoretic properties.

Theorem 3.4. *A prime ideal is a potential prime $P = (R, T)$ such that $R \cup T = A$ and that does not collapse.*

Proof.
- Given a prime ideal as defined in **Definition 3.3**, observe that $A = \mathfrak{p} \cup S = \mathfrak{p} \cup (A \setminus \mathfrak{p})$. We now verify that $0 \notin S(\mathfrak{p}; A \setminus \mathfrak{p})$. Suppose, for the sake of contradiction, that
$$0 = a \cdot r + s_1^{n_1} \cdot s_2^{n_2}$$
for some $a \in A$, $r \in \mathfrak{p}$, $s_1, s_2 \in S := A \setminus \mathfrak{p}$, and $n_1, n_2 \in \mathbb{N}$. This implies that $a \cdot r = -s_1^{n_1} \cdot s_2^{n_2}$. However, this is a contradiction: since $s_1^{n_1}, s_2^{n_2} \notin \mathfrak{p}$, their product cannot lie in $\mathfrak{p}$, as $\mathfrak{p}$ is a prime ideal. Therefore, $0 \notin S(\mathfrak{p}; A \setminus \mathfrak{p})$, and the ideal does not collapse.

- For the converse, suppose $P = (R, T)$ is a potential prime such that $R \cup T = A$ and $S(P)$ does not collapse. We aim to show that R is a prime ideal and that $R \cap T = \emptyset$.

  Assume for contradiction that $R \cap T \neq \emptyset$, and let $x \in R \cap T$. Then $x \in \langle R \rangle$ and $x \in M(T)$. Since $-x \in \langle R \rangle$, we obtain the identity $(-x) + x = 0 \in S(P)$, implying that $S(P)$ collapses, which is a contradiction. Hence, $R \cap T = \emptyset$, and since $R \cup T = A$, we conclude that $T = A \setminus R$.

  To show that R is an ideal, suppose there exist $x \in R$, $a \in A$ such that $a \cdot x \notin R$. Then $a \cdot x \in \langle R \rangle$ but also $a \cdot x \in T$, implying
$$-a \cdot x + a \cdot x = 0 \in S(P),$$
leading again to a contradiction. Thus, R is closed under multiplication by elements in A. Similarly, if $x_1, x_2 \in R$, but $x_1 + x_2 \in T$, then $-(x_1 + x_2) + (x_1 + x_2) = 0 \in S(P)$, and if $0 \notin R$, then $0 \in T$ and $0 + 0 = 0 \in S(P)$.

Finally, to show that R is prime, suppose $a \cdot b \in R$ for some $a, b \in A$ with $a, b \in T$. Then $a, b \in M(T)$, so $a \cdot b \in M(T)$, and since $a \cdot b \in \langle R \rangle$, we again have

$$-a \cdot b + a \cdot b = 0 \in S(P),$$

contradicting the assumption that $S(P)$ does not collapse. Therefore, R is prime.

□

Notice how the **constructive version** of a prime ideal is defined, it requires only two conditions: first, that the pair of sets collectively covers all elements of A, and second, that the associated structure does not collapse. Although classical notions such as ideals and monoids are implicitly involved in the construction, the definition itself remains explicit and direct. This approach provides a more elementary and flexible viewpoint, allowing us to work with pairs of subsets without assuming ideal or monoid properties *a priori*. To determine whether a given pair of subsets of A forms a prime ideal, it suffices to verify that their union equals A and that $0 \notin S(P)$, where $S(P)$ is the set generated by them. This simplicity highlights the elegance of the constructive framework, making it more accessible for constructive algebraic reasoning. The following proposition remarks their properties in this context according to **Definition 3.2**.

Proposition 3.5. *A prime ideal is complete and saturated as a potential prime.*

Proof.

- **Completeness:** $\mathfrak{p}$ is an ideal and according to **Section 1.1.2**, $A \setminus \mathfrak{p}$ is a multiplicative set, and therefore a monoid. Let's prove that $A \setminus \mathfrak{p} = \mathfrak{p} + (A \setminus \mathfrak{p})$. If $x \in A \setminus \mathfrak{p}$, then by taking $0 \in \mathfrak{p}$, $x = 0 + x \in \mathfrak{p} + (A \setminus \mathfrak{p})$, with $r \in \mathfrak{p}$ and $s \in A \setminus \mathfrak{p}$. Conversely, if $x = r + s \in \mathfrak{p} + (A \setminus \mathfrak{p})$, by complementarity, $x \in \mathfrak{p}$ or $x \in A \setminus \mathfrak{p}$. The first case, would imply that $x - r = (r + s) - r = s \in \mathfrak{p}$, therefore, by contradiction, $x \in A \setminus \mathfrak{p}$, obtaining the desired equality $S(\mathfrak{p}; A \setminus \mathfrak{p}) = A \setminus \mathfrak{p} = \mathfrak{p} + A \setminus \mathfrak{p}$. In this particular case, the constructive definition of the localization of a prime ideal coincides with the classical one for prime ideals.
- **Saturation:** Based on the definition of saturated potential primes, we need to check both conditions for a given $x \in A$:
  1. If $(\mathfrak{p} \cup \{x\}; A \setminus \mathfrak{p})$ collapses, then there are $r \in \mathfrak{p}$, $a \in A$ and $s \in A \setminus \mathfrak{p}$ such that $r + ax + s = 0$ ($r + ax \in \langle \mathfrak{p}, x \rangle$), then by isolating $ax = -(r + s) \in \mathfrak{p} + (A \setminus \mathfrak{p}) = A \setminus \mathfrak{p}$, therefore by defintion of prime ideal, $a, x \in A \setminus \mathfrak{p}$.
  2. Now, if $(\mathfrak{p}; (A \setminus \mathfrak{p}) \cup \{x\})$ collapses, then there are $r \in \mathfrak{p}$, $s \in A \setminus \mathfrak{p}$ and $n \in \mathbb{N}$ such that $r + s \cdot x^n = 0$, then $r = s \cdot x^n \in \mathfrak{p}$, and because $s \notin \mathfrak{p}$, then $x^n \in \mathfrak{p}$, therefore by primality, $x \in \mathfrak{p}$.

□

3.2.2 Constructive version of Krull's Theorem

An implicit result used during the classical approach developpement is the Krull's theorem (cf. [11, 12, 15]):

Theorem 3.6. *Let A be a ring, if I is a proper ideal of A then there exists a maximal ideal $\mathfrak{M}$ that contains I.*

It is proven using existential arguments, based on Zorn lemma. Knowing that all maximal ideals are prime, we can generalize its formulation to

Theorem 3.7. *Let A be a ring, if I is a proper ideal of A then there exists a prime ideal $\mathfrak{p}$ that contains I.*

For the sake of consistency, this result should have a counterpart within the constructive framework. However, the approach presented here does not depend explicitly on the classical notion of ideals, instead, it is formulated in terms of potential primes, which can be specialized to ideals but also provide a broader generalization of the theorem.

Theorem 3.8 (First version)**.** *Let $P = (R; T)$ be a potential prime that does not collapse. Then, there exists a prime ideal that refines it.*

Theorem 3.9 (Second version)**.** *Let $P = (R; T)$ be a potential prime and $x \in A$. If both $(R \cup \{x\}; T)$ and $(R; T \cup \{x\})$ collapse, then P collapses.*

Proof. The collapse of both new potential primes implies that $0 \in S(R \cup \{x\}; T) \cap S(R; T \cup \{x\})$, therefore, there are $r_1, r_2 \in \langle R \rangle$, $a \in A$, $t_1, t_2 \in M(T)$ and $n \in \mathbb{N}$ such that

$$-(r_1 + a \cdot x) + u_1 = -r_2 + u_2 \cdot x^n = 0$$

i.e, $r_1 + a \cdot x = u_1$ and $r_2 = u_2 \cdot x^n$. Inserting the first equality on the second one, we get:

$$a^n \cdot r_2 = u_2 \cdot (a \cdot x)^n = u_2 \cdot (u_1 - r_1)^n$$

implying that the element $u_2 \cdot u_1^n \in \langle R \rangle$, and therefore,

$$-(u_2 \cdot u_1^n) + (u_2 \cdot u_1^n) = 0 \in \langle R \rangle + M(T) = S(P)$$

making P collapse. □

Observation 3.10. The first version is an adaptation of the classical theorem to constructive objects, however, it is still based on existential logic, whereas the second version deals explicitly with the elements of potential primes. It is therefore insightful to prove the equivalence between both versions.

Corollary 3.11. *The first and second constructive versions of Krull's theorem are equivalent.*

Proof.

- Suppose the first one to be true: if P does not collapse then there exists a prime ideal that refines it. We shall prove the second one using a contrapositive argument. By the definition of a prime ideal in terms of potential primes, if $x \in A$ then either $x \in \mathfrak{p}$ or $x \in A \setminus \mathfrak{p}$, so in each case:

  1. If $x \in \mathfrak{p}$, then $(R \cup \{x\}; T) \leq (\mathfrak{p}, A \setminus \mathfrak{p})$, therefore $(R \cup \{x\}; T)$ does not collapse.
  2. Similarly, if $x \in A \setminus \mathfrak{p}$, then $(R; T \cup \{x\}) \leq (\mathfrak{p}, A \setminus \mathfrak{p})$, therefore $(R; T \cup \{x\})$ does not collapse.

  This is because if $P_1 \leq P_2$ then $S(P_1) \subseteq S(P_2)$.

- Now suppose the second version to be true: Given a potential prime $P = (R;T)$ that does not collapse, we can construct a countable refinement chain, that is $P = (R;T) \leq \ldots \leq P_i = (R_i;T_i) \leq P_{i+1} = (R_{i+1};T_{i+1}) \leq \ldots$ with $R_i \subseteq R_{i+1}, T_i \subseteq T_{i+1}$, denoted by $\{P_i\}_{i\in\mathbb{I}}$, where $\mathbb{I}$ is a countable set. Now, by applying the Zorn lemma, there exists a maximal potential prime of the chain $P_m = (R_m;T_m), m \in \mathbb{I}$. We need to verify that it is prime. It belongs to the chain therefore it does not collapse. Furthermore, if we consider that $A \neq R_m \cup T_m$, then there must exist a $x \in A\backslash(R_m \cup T_m)$, and by **Theorem 2.9**, if neither $(R_m \cup \{x\}; T_m)$ nor $(R_m; T_m \cup \{x\})$ collapse, we could add more refined potential primes to the chain contradicting the maximality of P_m, therefore one of them collapse, and P_m is a prime ideal.

□

With this discussion, we have described prime ideals with a solid constructive structure as maximal elements of refinement chains. Consequently, the definition of maximal ideals follows naturally in their constructive version.

Definition 3.12. *A potential prime $M = (R;T)$ is called a* ***maximal ideal*** *if it is prime (that is, it does not collapse and satisfies $A = R \cup T$) and there is no other prime ideal $M' = (R';T')$ such that M is properly contained in M', meaning $R \subsetneq R'$ and $T' \subsetneq T$.*

Observation 3.13. Notice that in the definition of maximal ideals we refer to containment rather than refinement, since all prime ideals are maximal with respect to refinement, but they can be properly contained in other prime ideals by enlarging R and shrinking T.

3.2.3 Potential Chains

Before fully characterizing prime ideals constructively, it is necessary to analyze their behavior under chain relations, hence leading naturally to the concept of Krull dimension. For this reason, we define Potential Chains as a generalization applied to potential primes, which inherently possess an underlying chain structure of associated prime ideals (cf. [11, 12]).

Definition 3.14 (Potential Chains)**.** *Given a ring A, a* potential chain *of length $n \in \mathbb{N}$ is defined as a sequence of potential primes $C = (P_0, P_1, \ldots, P_n)$, ordered by containment.*

Now, we introduce some important definitions associated to potential chains.

Definition 3.15.

1. *Given a potential chain $C = (P_0, \ldots, P_n)$, we say that C is* complete *if each P_i is complete and it is ordered by containment, $P_0 \subseteq P_1 \subseteq \ldots \subseteq P_n$. We denote by $\bar{C} = (\bar{P}_0 = (\langle R_0 \rangle; M(T_0)), \ldots, \bar{P}_n = (\langle R_n \rangle; M(T_n)))$ the complete chain associated to C, where $M(T_i)$ is a monoid containing T_i such that $M(T_i) = \langle R_i \rangle + M(T_i)$. We denote this completed chain by $\bar{C}$.*
2. *A potential chain C is said to collapse if, in its associated complete chain $\bar{C}$, the zero element belongs to the first monoid; that is, $0 \in M(T_0)$.*
3. *A potential chain $C' = (P'_0, \ldots, P'_n)$ is said to refine the chain $C = (P_0, \ldots, P_n)$, if for all $i \in \{0, \ldots, n\}$, $P_i \leq P'_i$.*
4. *A potential chain $C = (P_0, \ldots, P_n)$ is said to be saturated if each P_i is saturated.*

By translating the properties of potential primes to those of potential chains, one can correspondingly extend Theorems **2.8** and **2.9** by establishing a Krull's theorem of Potential Chains.

Theorem 3.16 (First version)**.** *Given a potential chain $C = (P_0, \dots, P_n)$ and an element $x \in A$, if the potential chains $(P_0, \dots, (R_i \cup \{x\}; T_i), \dots, P_n)$ and $(P_0, \dots, (R_i; T_i \cup \{x\}), \dots, P_n)$ collapse for some fixed $i \in \{0, \dots, n\}$, then the chain C collapses.*

Theorem 3.17 (Second version)**.** *Given a potential chain $C = (P_0, \dots, P_n)$ that does not collapse, there exists a chain of prime ideals $C_\mathfrak{p}$ that refines C.*

The proofs follow analogously from the corresponding results for potential primes by fixing an index $i \in \{0, \dots, n\}$. Furthermore, since prime ideals are complete and thus form complete chains, this framework naturally leads to a constructive definition of prime ideals chains ordered by contention, which in turn enables the definition of Krull dimension within this context.

3.3 Constructive versions of Krull dimension

Having established the foundational framework of constructive prime ideals through potential primes and potential chains, we now proceed to derive explicit results concerning Krull dimension without relying on the classical machinery developed in Chapter 1. This constructive perspective grants the notion of dimension a computational character, allowing for an algorithmic and operational treatment based on the elements of the commutative ring under consideration .

3.3.1 Krull dimension using potential chains

The following proposition describes an algorithmic description of the collapse of potential chains (cf. [11, 12, 13, 15]).

Proposition 3.18. *If a potential chain $C = (P_0, \dots, P_n)$ collapses, then for each $i = 0, \dots, n$ there exist elements $r_i \in \langle R_i \rangle$ and $t_i \in M(T_i)$ such that:*

$$0 = t_0 \cdot (t_1 \cdot (\cdots (t_n + r_n) + \cdots) + r_1) + r_0$$

Proof. As stated in **Definition 3.15**, a potential chain C collapses if $0 \in M(T_0)$. Given the completeness of the corresponding chain $\bar{C}$, we know that $M(T_i) = \langle R_i \rangle + M(T_i)$ for every i. Furthermore, the containment condition ensures that $M(T_n) \subseteq \cdots \subseteq M(T_0)$.

Since $0 \in M_0$, there exist $r_0 \in \langle R_0 \rangle$, $t_0 \in M_0$, and $w_1 \in M(T_1)$ such that

$$0 = t_0 \cdot w_1 + r_0.$$

For monoids, since $1 \in M(T_1)$ and $M(T_1) \subseteq M(T_0)$, every $x \in M(T_0)$ satisfies $x = x \cdot 1 \in M(T_1) \cdot M(T_0)$, hence $M(T_0) = M(T_1) \cdot M(T_0)$,the other inclusion is direct. Applying the same argument to $w_1 \in M(T_1) = \langle R_1 \rangle + M(T_1)$, we can write $w_1 = t_1 \cdot w_2 + r_1$ for some $r_1 \in \langle R_1 \rangle$, $t_1 \in M(T_1)$, and $w_2 \in M(T_2)$. Substituting this into the previous equation gives:

$$0 = t_0 \cdot (t_1 \cdot w_2 + r_1) + r_0.$$

Repeating this process iteratively, we obtain the desired expression. □

Now, let's have a first constructive description of Krull dimension.

Theorem 3.19. *Given a ring A, the following properties are equivalent:*

1. *The Krull dimension of A is $\leq n-1$.*
2. *For all $x_1, \ldots, x_n \in A$, the potential chain*

$$C = ((0; \{x_1\}), (\{x_1\}; \{x_2\}), \ldots, (\{x_{n-1}\}; \{x_n\}), (\{x_n\}; \{1\}))$$

   collapses.

3. *For all $x_1, \ldots, x_n \in A$, there exist $a_1, \ldots, a_n \in A$ and $m_1, \ldots, m_n \in \mathbb{N}$ such that*

$$x_1^{m_1}(x_2^{m_2}(\cdots(x_n^{m_n}(1 + a_n x_n) + \cdots + a_2 x_2) + a_1 x_1) = 0.$$

Proof.

- Firstly, let's prove the equivalence ($2 \iff 3$). If C collapses, then by **Proposition 2.18**, there exist $a_1x_1 \in \langle x_1 \rangle, a_2x_2 \in \langle x_2 \rangle, \ldots, a_nx_n \in \langle x_n \rangle$ and $t_i \in M(T_i)$ and $x_1^{m_1} \in M(x_2), x_2^{m_2} \in M(x_2), \ldots, x_n^{m_n} \in M(x_n)$ and substituting in the corresponding t_i and r_i:

$$x_1^{m_1}(x_2^{m_2}(\cdots(x_n^{m_n}(1 + a_n x_n) + \cdots + a_2 x_2) + a_1 x_1) = 0.$$

  Conversely, if 3. holds, then by constructing a chain of the form of C, it collapses because the equality implies that $0 \in \bar{P}_0 = (\langle 0 \rangle; M(x_1))$.

- Now, let's prove the implication ($3 \Rightarrow 1$): Suppose $\dim A \geq n$, so there exists a chain of prime ideals $p_0 \subsetneq \cdots \subsetneq p_n$. We select $x_i \in p_i \setminus p_{i-1}$ and define recursively:

$$E_n = x_n^{m_n}(1 + a_n x_n), \quad E_i = x_i^{m_i}(E_{i+1} + a_i x_i) \text{ for } i < n$$

  Notice that $E_i \notin p_{i-1}$, because $x_n^{m_n} \notin p_{n-1}$ and $1 + a_n x_n \notin p_{n-1}$ (since $1 \notin p_n \supset p_{n-1}$), so $E_n \notin p_{n-1}$.For $i < n$, if $E_{i+1} \notin p_i$, then $E_{i+1} + a_i x_i \notin p_{i-1}$ (as $p_{i-1} \subsetneq p_i$) and $x_i^{m_i} \notin p_{i-1}$, hence $E_i \notin p_{i-1}$. Finally, for $i = 1$, we have $0 = E_1 \notin p_0$, a contradiction. Thus $\dim A \leq n-1$.

- Finally, let's prove ($1 \Rightarrow 2$): Suppose $\dim A \leq n-1$. Let $x_1, \ldots, x_n \in A$ be arbitrary. Consider the chain

$$C = \big((0; \{x_1\}), (\{x_1\}; \{x_2\}), \ldots, (\{x_{n-1}\}; \{x_n\}), (\{x_n\}; \{1\})\big).$$

  Let's suppose that C does not collapse. Then we can define a proper chain of prime ideals that refine each potential prime (Krull's Theorem), giving rise to a saturated chain of prime ideals

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

  where $x_i \in \mathfrak{p}_i \setminus \mathfrak{p}_{i-1}$ for each i, contradicting the assumption that $\dim A \leq n-1$. Therefore, the chain must collapse.

□

3.3.2 Constructive Krull dimension in Polynomial Rings

In this section, we develop a constructive characterization of Krull dimension of polynomial rings using the notion of boundary, which excludes trivial elements and enables dimension bounds via algebraic relations. This leads to a purely algebraic proof of the classical result $\dim(k[x_1, \ldots, x_l]) = n$ (cf. [12, 14]).

Theorem 3.20. *Let K be a field extension of k. Then all transcendence bases of K over k have the same cardinality.*

If we adopt the convention that a ring A has Krull dimension -1 if and only if it is the zero ring (0), we can employ an inductive procedure to determine its dimension. To facilitate inductive proofs, we introduce a definition that depends on the choice of elements in A and, in particular, excludes nilpotent and invertible elements.

Definition 3.21. *The* ***boundary*** *$A_{\{x\}}$ of x in A is the localized ring $S_{\{x\}}^{-1}A$ where*

$$S_{\{x\}} = \{x^n(1 + ax) \mid n \in \mathbb{N}, a \in A\}$$

Proposition 3.22. *$A_{\{x\}}$ is trivial if x is* ***nilpotent*** *or* ***invertible****.*

Proof. 1. If x is **nilpotent**, then there exists $m \in \mathbb{N}$ such that $x^m = 0$, and for this m, $0 = x^m(1 + 0x) \in S_{\{x\}}$, therefore, $A_{\{x\}} = (0)$.

2. If x is **invertible**, then by taking $a = -x^{-1}$, $0 = x^n(1 + (-x^{-1})x) \in S_{\{x\}}$, therefore $A_{\{x\}} = (0)$.

□

By using these results, we can set up a upper bound for the Krull dimension of any commutative ring.

Theorem 3.23. *Let A be a commutative ring, and $n \in \mathbb{N}$, the following statements are equivalent.*

1. *The Krull dimension of A is at most n.*
2. *For all $x \in A$, the Krull dimension of $A_{\{x\}}$ is at most $n - 1$.*
3. *Given any elements $x_0, \ldots, x_n$ in A, there exist $a_0, \ldots, a_n$ in A and $m_0, \ldots, m_n$ in $\mathbb{N}$ such that*

$$x_0^{m_0}(\ldots(x_n^{m_n}(1 + a_l x_l) + \ldots) + a_0 x_0) = 0$$

Proof. To prove the equivalence between 1. and 2. we need the following two results

(a) **For all $x \in A$, every maximal ideal $\mathfrak{m}$ intersects $S_{\{x\}}$**: If $x \in \mathfrak{m}$ then the result is obvious, otherwise, from **Proposition 1.7.** we know that $A/\mathfrak{m}$ is a field, then the class $\bar{x}$ is invertible there, meaning that there is a $\bar{a} \in A/\mathfrak{m}$ such that $\bar{x}\bar{a} = \bar{1}$, implying $1 - xa \in \mathfrak{m}$, and therefore $(1 + xA) \cap \mathfrak{m} \neq \emptyset$ (thus $S_{\{x\}} \cap \mathfrak{m} \neq \emptyset$).

(b) **If $\mathfrak{m}$ is a maximal ideal of A and $x \in \mathfrak{m} - \mathfrak{p}$, where $\mathfrak{p}$ is a prime ideal contained in $\mathfrak{m}$, then $\mathfrak{p} \cap S_{\{x\}} = \emptyset$**: Let's assume the intersection is not empty, thus there is an element $x^k(1 + ax) \in \mathfrak{p}$, since $x \notin \mathfrak{p}$, then $1 + ax \in \mathfrak{p}$, which would imply that $1 \in \mathfrak{m}$, contradicting its maximality, obtaining the desired result.

Now, with (a), we prove that, knowing that every chain ends in a maximal ideal, it is shortened when we pass to $A_{\{x\}}$, and (b) implies that having a chain $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_{n-1} \subsetneq 1$, if we chose $x \in \mathfrak{m} - \mathfrak{p}_{n-1}$ it is shortened by 1, proving the equivalence.

The equivalence with 3. is proved by using induction over n. For $n = 0$, then it is clear that $x_0^{m_0}(1 + a_0x_0) = 0$ holds for any $x_0 \in A$, giving $S_{\{x\}} = 0$, and therefore $\dim(A_{\{x\}}) = -1$.

Let's assume the equivalence is true for all integers smaller than n and all A. By the inductive hypothesis, if we take any localization $S^{-1}A$, then $\dim(S^{-1}A) \leq n - 1$ if and only if, for any $x_0, \ldots, x_{n-1}$ in $S^{-1}A$, there are $a_0, \ldots, a_{n-1}$ in $S^{-1}A$, a unit $s \in S^{-1}A$ and $m_0, \ldots, m_{n-1} \in \mathbb{N}$ such that

$$x_0^{m_0}(\ldots(x_{n-1}^{m_{n-1}}(s + a_{n-1}x_{n-1}) + \ldots) + a_0x_0) = 0$$

The fact of taking s it's because the equality stated for 1 in the case of the global ring A holds also for all units in A. Now, by taking specifically the localization $S^{-1}A$, an element $s \in S^{-1}$ is of the form $x_n^{m_n}(1 + a_nx_n)$, proving this way the desired equivalence.

□

Before proving the following result we need to highlight an important definition, specially to know its formal meaning.

Definition 3.24. *Let $k[x_1, x_2, \ldots, x_n]$ be a polynomial ring over a field k. The* ***lexicographic order*** *on the set of monomials is defined as follows: given two monomials*

$$x^\alpha = x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_n^{\alpha_n}, \quad x^\beta = x_1^{\beta_1}x_2^{\beta_2}\cdots x_n^{\beta_n},$$

we say that

$$x^\alpha <_{\text{lex}} x^\beta$$

if the first index i where $\alpha_i \neq \beta_i$ satisfies $\alpha_i < \beta_i$.

Theorem 3.25. *Let k be a field and A a $k-$algebra. If any sequence $x_0, \ldots, x_n$ in A is algebraically dependent over k, then* $\dim(A) \leq n$.

Proof. If they are algebraically dependent, there exists a algebraic relation between them through a polynomial over k

$$f(x_0, \ldots, x_n) = 0$$

If we order the monomials $\alpha_{p_0,\ldots,p_n}x_0^{p_0}\ldots x_n^{p_n}$ by lexicographic order and we make the leader coefficient to be 1, then f can be written as:

$$f = x_0^{m_0}\ldots x_\ell^{m_n} + \sum_{j=1}^{N} \alpha_j x_0^{a_{0j}}x_1^{a_{1j}}\ldots x_n^{a_{nj}},$$

where each $(a_{0j}, \ldots, a_{nj})$ is strictly less than $(m_0, \ldots, m_n)$ in the lexicographic order.

Now, regroup this expression according to powers of x_0. For instance, we write:

$$Q = x_0^{m_0}\left(x_1^{m_1}\cdots x_\ell^{m_n} + x_1^{m_1}\cdots x_\ell^{m_n-1}R_n + \cdots + R_1\right) + R_0,$$

where each R_j belongs to $K[x_k : k \geq j]$ and involves only monomials of lexicographically smaller weight.

This expression is now in a form compatible with the previous Theorem. Indeed, the identity $l = 0$ gives:

$$x_0^{m_0}\left(x_1^{m_1}\left(\cdots x_n^{m_n}(1 + a_n x_n) + \cdots + a_1 x_1\right) + a_0 x_0\right) = 0,$$

for some $a_0, \ldots, a_n \in R$, where the terms a_i absorb all the lower-degree parts from the regrouped R_j terms.

Therefore, such an identity implies that $\dim R \leq n$. □

Finally, using these previous theorems we get the Krull dimension of a polynomial ring.

Theorem 3.26. *If k is a field, then* $\dim(k[x_1, \ldots, x_l]) = n$.

Proof. We first show that the Krull dimension is at least l. Consider the chain of prime ideals:

$$(0) \subset (x_1) \subset (x_1, x_2) \subset \cdots \subset (x_1, x_2, \ldots, x_n),$$

which has length n. Therefore, $\dim(k[x_1, \ldots, x_n]) \geq n$. To prove the opposite inequality, consider the field of fractions

$$K = \text{Frac}(k[x_1, \ldots, x_n]) = k(x_1, \ldots, x_n)$$

By **Theorem 2.**, any transcendence basis of K over k has cardinality n, hence the transcendence degree of K over k is n. This means that any $n+1$ elements of $k[x_1, \ldots, x_n]$ are algebraically dependent over k. Now, applying **Theorem 1.82**, which asserts that if every $(n+1)$-tuple in a k-algebra is algebraically dependent over k, then its Krull dimension is at most n, we conclude:

$$\dim(k[x_1, \ldots, x_n]) \leq n$$

Since both bounds coincide, we conclude:

$$\dim(k[x_1, \ldots, x_n]) = n$$

□

The proofs given here are possible thanks to having introduced the notion of **boundary**. Even if its definition could seem arbitrary, besides the fact that it allows to exclude **nilpotent** and **invertible elements** from the treatment, it also contains a strong algebraic meaning that can be visualized through geometric examples, and provides a **methodology** in order to make a space shortened by at least one dimension.

Even if we have introduced it to give an alternative proof to the same fact about the Krull dimension, it is useful and convenient to make a specific treatment of this concept by itself.

Example 3.27. Consider the polynomial ring $k[x, y, z]$. By the characterization of $S_{\{x\}}$ given in parts (a) and (b) of the proof of **Theorem 3.23**, all maximal ideals are "excluded" when passing to the localization ring. Moreover, regarding prime ideals, the only ones that survive are those that do not contain x.

As we have done throughout this chapter, an equivalent way to understand ideals is to consider their corresponding varieties.

As an example, consider the polynomial $f(x, y, z) = x$ whose variety is the plane $V_{\{x\}} = \{(0, y, z) \in k^3\}$.

We can affirm from (a) that all maximal ideals disappear in $A_{\{x\}}$, and that a prime ideal $\mathfrak{p}$ survives in $A_{\{x\}}$ if and only if $x \notin \mathfrak{p}$ *and* $\overline{x}$ is not invertible in $A/\mathfrak{p}$. This can be understood as follows.

First, suppose $\mathfrak{p} \cap S_{\{x\}} = \emptyset$. Then in particular, $x \notin \mathfrak{p}$. If $x \in \mathfrak{p}$, taking $n = 1$ and $a = 0$, we have $x = x^1(1 + 0 \cdot x) \in S_{\{x\}} \cap \mathfrak{p}$, contradicting the assumption. Conversely, assume $x \notin \mathfrak{p}$. To show $\mathfrak{p} \cap S_{\{x\}} = \emptyset$, suppose for contradiction that $x^n(1 + ax) \in \mathfrak{p}$ for some $n \geq 0$, $a \in A$. Since $\mathfrak{p}$ is prime, either $x^n \in \mathfrak{p}$ or $1 + ax \in \mathfrak{p}$. If $x^n \in \mathfrak{p}$, then $x \in \mathfrak{p}$, a contradiction. If $1 + ax \in \mathfrak{p}$, then in $A/\mathfrak{p}$, we have $\overline{1} + \overline{ax} = 0$. Since $x \notin \mathfrak{p}$, $\overline{x} \neq 0$. If $\overline{x}$ were invertible in $A/\mathfrak{p}$, there would exist $\overline{a} = -\overline{x}^{-1} \in A/\mathfrak{p}$, contradicting that no such $\overline{a}$ exists (as $\overline{x}^{-1}$ need not lie in $A/\mathfrak{p}$). Thus, $\mathfrak{p} \cap S_{\{x\}} = \emptyset$.

Geometrically, this means that surviving varieties are those not contained in the plane $x = 0$ and where x has no inverse when passing to the quotient. The localization $A_{\{x\}}$ excludes all maximal ideals and primes where x acts invertibly, retaining only structures "transverse" to $x = 0$ in both vanishing and algebraic invertibility. Moreover, as discussed earlier, the Krull dimension of the localized ring $A_{\{x\}}$ is strictly less than that of the original polynomial ring $k[x, y, z]$. This reduction is a direct consequence of the elimination of all maximal ideals during the localization process (see Figure 2).

Example 3.28. Let $A = \mathbb{F}_p[x]$ and $f = x$. Define $S = \{x^n(1 + ax) \mid n \in \mathbb{N},\ a \in \mathbb{F}_p[x]\}$. The ideal (x) intersects S since $x \in S$, and is thus eliminated. For each $a \in \mathbb{F}_p^\times$, the maximal ideal $(x - a)$ is disjoint from S, as no element of the form $x^n(1 + ax)$ vanishes at $x = a$. The boundary is $\{(x - a) \mid a \in \mathbb{F}_p^\times\}$.

Example 3.29. Let $A = \mathbb{F}_p[x, y]$ and $f = x$. Define $S = \{x^n(1 + ax) \mid n \in \mathbb{N},\ a \in A\}$. Every prime ideal containing x, such as (x) or $(x, y - b)$, intersects S and is eliminated. Prime ideals of the form $(x - a, y - b)$, with $a \in \mathbb{F}_p^\times$, do not contain any $x^n(1 + ax)$, and thus survive. The boundary consists of all closed points off the line $x = 0$; that is, all $(a, b) \in \mathbb{F}_p^2$ with $a \neq 0$.

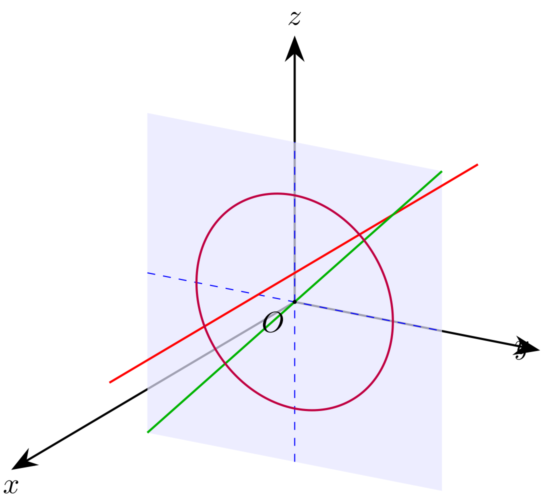


Figure 2: Geometric representation of various subvarieties of $\mathbb{A}_k^3$, illustrating the effect of localizing at x. The light blue plane corresponds to the variety $V(x)$, whose defining ideal is (x). The green diagonal line in the yz-plane represents the variety $V(x, y - z)$, defined by the ideal $(x, y - z)$. The purple circle lies entirely in the plane $x = 0$, and corresponds to the variety $V(x, y^2 + z^2 - 1)$, with ideal $(x, y^2 + z^2 - 1)$. All these varieties are annihilated upon localization at x, since their defining ideals contain x. In contrast, the red line $\{y = 1, z = 1\}$, defined by the ideal $(y - 1, z - 1)$, survives localization.

3.3.3 Krull Dimension in Distributive Lattices

In this section, we shall describe a more elemental pathway to deduce the Krull dimension, extending it to algebraic structures that are not necessarily rings, by developing some set-theoretical concepts consistent with the required constructivity (cf. [11, 12, 15]).

Definition 3.30 (Lattice)**.** *Let $(T, \leq)$ be a partially ordered set.*

1. *We say that $(T, \leq)$ is a **lattice** if for every finite subset in T, there exist a least upper bound and greatest lower bound, concretely for a ordered pair (a, b) they are denoted respectively by $a \vee b$ and $a \wedge b$.*
2. *If, in addition, there exist a minimum element $0 = \bigwedge T := \bigwedge_{x \in T} x$ and a maximum element $1 = \bigvee T := \bigvee_{x \in T} x$, then $(T, \leq)$ is called a **bounded lattice**.*
3. *A lattice is called **distributive** if for all $a, b, c \in T$, the following distributive laws hold: $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$ and $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$.*

Example 3.31. The union and intersection of sets form a distributive lattice. Given the sets A, B, C:

1. If $A \subseteq B$, then $A, B \subseteq A \cup B$ and $A \cap B \subseteq A, B$.
2. Distributive laws are satisfied: $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$, and $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Definition 3.32. *Given a distributive lattice T, and $A, B \in \mathcal{P}(T)$ (power set of T), we define the following relation in $\mathcal{P}(T)$:*

$$\bigwedge A \leq \bigvee B \text{ (denoted by } A \vdash B\text{)}$$

Proposition 3.33. *The relation $\vdash$ is reflexive, monotone, and transitive.*

Proof.

- **Reflexive:** Given a subset $A \in \mathcal{P}(T)$ by the definition of partial ordering, a lower bound is lower than an upper bound, therefore:

$$\bigwedge A \leq \bigvee A \Rightarrow A \vdash A$$

- **Monotone:** Given $A, B \in \mathcal{P}(T)$ such that $\bigwedge A \leq \bigvee B$ $(A \vdash B)$. Then $\bigwedge(A \cup A') \leq \bigwedge A \leq \bigvee B \leq \bigvee(B \cup B')$ by the definition of partial ordering. Hence, $\bigwedge(A \cup A') \leq \bigvee(B \cup B')$, which means $A \cup A' \vdash B \cup B'$.
- **Transitive:** For finite subsets A, B of a distributive lattice T and $x \in T$, transitivity is defined as follows:

$$(A \cup x \vdash B) \text{ and } (A \vdash B \cup x) \Rightarrow A \vdash B.$$

  It's also called the **cutting condition**.

□

The underlying constructivity of this concept is based on its equational treatment. The way the operations $\wedge$ and $\vee$ are defined allows to set the following operational structure:

$$\begin{aligned} a \vee a &= a & a \wedge a &= a \\ a \vee b &= b \vee a & a \wedge b &= b \wedge a \\ (a \vee b) \vee c &= a \vee (b \vee c) & (a \wedge b) \wedge c &= a \wedge (b \wedge c) \\ (a \vee b) \wedge a &= a & (a \wedge b) \vee a &= a \\ a \vee 0 &= a & a \wedge 1 &= a \end{aligned}$$

The fact that distributive lattices constitute set-theoretical concept, quotient lattices could be defined and establish a direct relationship between lattices and ideals. In order to get a coherent condition on Krull dimension using lattices, the **quotient lattice** will be defined as follows:

Definition 3.34 (Power Set Definition)**.** *Let T be a distributive lattice and (J, F) a pair of finite subsets of T. The **quotient lattice** T' is defined by imposing the relations:*

$$x \equiv 0, \ \forall x \in J, \quad y \equiv 1, \ \forall y \in F,$$

with the order:

$$[a] \leq_{T'} [b] \iff \exists J_0 \subseteq J, F_0 \subseteq F \text{ (finite) such that } a \wedge \bigwedge F_0 \leq_{\mathbf{T}} b \vee \bigvee J_0.$$

Definition 3.35 (Partial order Definition)**.** *A* quotient lattice T' *is induced by a preorder $\preccurlyeq$ on T satisfying:*

$$\begin{aligned} &(1)\ a \leq b \Rightarrow a \preccurlyeq b, \\ &(2)\ a \preccurlyeq b, a \preccurlyeq c \Rightarrow a \preccurlyeq c, \\ &(3)\ a \preccurlyeq b, a \preccurlyeq c \Rightarrow a \preccurlyeq b \wedge c, \\ &(4)\ b \preccurlyeq a, c \preccurlyeq a \Rightarrow b \vee c \preccurlyeq a. \end{aligned}$$

The quotient is the set of equivalence classes $[a] = \{b \mid a \preccurlyeq b \text{ and } b \preccurlyeq a\}$.

Although these definitions are apparently different, they yield to the same quotient lattice. Equivalance is proven by the following proposition.

Proposition 3.36. *The Power Set Definition and Preorder Definition yield isomorphic quotient lattices.*

Proof.

- Let $[a] \leq_{T'} [b]$, i.e, $\exists J_0 \in P_f(J), F_0 \in P_f(F)$ such that $a \wedge \bigwedge F_0 \leq b \vee \bigvee J_0$. We need to verify that $\leq_{T'}$ satisfies the definition of $\preccurlyeq$:

  1. Take $J_0 = F_0 = \emptyset$. Then:

     $$a \wedge \bigwedge \emptyset = a \wedge 1 = a \leq b = b \vee 0 = b \vee \bigvee \emptyset.$$

  2. If $a \leq_{T'} b$ (via (J_1, F_1)) and $b \leq_{T'} c$ (via (J_2, F_2)), then:

     $$a \wedge \bigwedge (F_1 \cup F_2) \leq b \wedge \bigwedge F_2 \vee \bigvee J_2 \leq c \vee \bigvee (J_1 \cup J_2)$$

     using $\bigwedge F_1 \wedge \bigwedge F_2 = \bigwedge (F_1 \cup F_2)$.

3. If $a \leq_{T'} b$ and $a \leq_{T'} c$ (via (J_b, F_b) and (J_c, F_c) respectively), then with $J_0 = J_b \cup J_c$ and $F_0 = F_b \cup F_c$:

$$a \wedge \bigwedge F_0 \leq (b \vee \bigvee J_b) \wedge (c \vee \bigvee J_c) \leq (b \wedge c) \vee \bigvee J_0$$

by distributivity.

4. Similarly to 3. using $(b \vee c) \wedge \bigwedge F_0 = (b \wedge \bigwedge F_0) \vee (c \wedge \bigwedge F_0)$.

- By employing the operational conditions of $\preccurlyeq$, we need to provide a construction of J and F consistent with the Power Set Definition. suppose a partial order $\preccurlyeq$ on T satisfies conditions (1)-(4). Define $J := \{x \in T \mid x \preccurlyeq 0\}$ and $F := \{y \in T \mid 1 \preccurlyeq y\}$, and consider the quotient lattice defined via the Power Set method with this (J, F). Assume $a \preccurlyeq b$; since $1 \preccurlyeq y$ for all $y \in F$ and $x \preccurlyeq 0$ for all $x \in J$, by properties (3) and (4) there exist finite subsets $F_0 \subseteq F$, $J_0 \subseteq J$ such that $a \wedge \bigwedge F_0 \preccurlyeq a \preccurlyeq b \preccurlyeq b \vee \bigvee J_0$, and by monotonicity (1) this implies $a \wedge \bigwedge F_0 \leq b \vee \bigvee J_0$, hence $[a] \leq_{T'} [b]$. Therefore, the equivalence classes and order defined by $\preccurlyeq$ coincide with those defined by the Power Set construction, so the quotient lattices are isomorphic.

□

The first definition presents quotient lattice as a collapsing method by employing subsets of T, while the second one provides a preservation of the partial order when passing to the quotient lattice.

Definition 3.37 (Constructive Ideal)**.** *Given a quotient lattice T' from the Power Set Definition, the **canonical ideal** I is:*

$$I = \{a \in T \mid [a] = [0]\}.$$

such that:

1. *$a, b \in I \Rightarrow a \vee b \in I$ (if $[a] = [b] = [0]$, then $[a \vee b] = [0 \vee 0] = [0]$),*
2. *$a \in I, c \in T \Rightarrow a \wedge c \in I$, (from $a \preccurlyeq 0$ and $c \preccurlyeq c$, condition (3) gives $a \wedge c \preccurlyeq 0 \wedge c = 0$. Thus $[a \wedge c] = [0]$.*

The dual notion of the constructive ideal is the filter.

Definition 3.38 (Filter)**.** *Given a quotient lattice T' from the Power Set Definition, the **filter** F is (satisfying the conditions 1. and 2.):*

$$F = \{b \in T \mid [b] = [1]\}.$$

1. *$a, b \in F \Rightarrow a \wedge b \in F$,*
2. *$a \in F, c \in T \Rightarrow a \vee c \in F$,*

The concepts of **Section 3.2** (and their respective properties) can be rewritten in terms of distributive lattices, implicating a redefinition of prime ideals in terms of the partial ordering defining the corresponding lattice.

Definition 3.39 (Potential Primes in distributive lattices)**.** *Let T be a distributive lattice.*

1. *A **potential prime** is a pair (J, U) of subsets of T. It is called **finite** if both J and U are finite, and **trivial** if $J = U = T$.*
2. *A potential prime is **saturated** if J is an ideal, U is a filter, and J and U are conjugate, i.e, for a given $x \in T$, $(f \in F, x \wedge f \in I) \implies x \in I$ and $(j \in I, x \vee j \in F) \implies x \in F$.*
3. *A potential prime (J, U) is said to **collapse** if the saturated prime it generates is trivial, i.e, there exist finite subsets $J_0 \subseteq J$, $U_0 \subseteq U$ such that $U_0 \vdash J_0$.*

Observation 3.40. A prime ideal, in this context is a potential prime $\mathfrak{P} = (R, T)$ that does not collapse, such that for any prime potential $P = (J; U)$ with $J \subseteq R$, then $U \cap T = \emptyset$.

Second and third conditions are analogous to those stated in **Definition 3.2**: a potential prime collapses if $R \cap T \neq \emptyset$, and the saturation conditions imply that no external element can be added to the pair. With these definitions and by applying similar arguments, Krull theorems for distributive lattices follow naturally. To introduce a notion of Krull dimension, we now directly redefine the concept of potential chains.

Definition 3.41. *Let T be a distributive lattice:*

1. *A potential chain of length n is a list of $n + 1$ potential primes of T:*
$$C = ((J_0; U_0), \ldots, (J_n; U_n))$$
2. *A potential chain is called **saturated** if the $(J_i; U_i)$ are pairs of conjugate ideals and filters, and if we have the relations $J_i \subseteq J_{i+1}$, $U_{i+1} \subseteq U_i$ $(i = 0, \ldots, n-1)$.*
3. *We say that a potential chain $C' = ((J'_0; U'_0), \ldots, (J_n; U'_n))$ **refines** the potential chain $C = ((J_0; U_0), \ldots, (J_n; U_n))$ if we have $J_k \subseteq J'_k$, $U_k \subseteq U'_k$.*
4. *We say that a potential chain C collapses if the only saturated potential chain that refines C is the trivial potential chain $((T; T), \ldots, (T; T))$.*

With a similar procedure than potential chains in commutative rings, the notion of Krull dimension can be translated to distributive lattices.

Definition 3.42. *Given a distributive lattice T generated by a subset A is said to have **Krull dimension** $\leq n - 1$ if it satisfies the following condition: for all $x_1, \ldots, x_n \in A$, the potential chain $((0, x_1), (x_1, x_2), \ldots, (x_{n-1}, x_n), (x_n, 1))$ collapses. This is equivalent to the existence of elements $a_1, a_2, \ldots, a_\ell$ satisfying:*

$$a_1 \cup x_1 \vdash 0, \quad a_2 \cup x_2 \vdash a_1 \cup x_1, \quad \ldots \quad , \quad a_n \cup x_n \vdash a_{n-1} \cup x_{n-1}, \quad 1 \vdash a_n \cup x_n$$

As shown in the proof of **Theorem 3.19**, this last condition is directly related to the possibility of constructing a chain of length greater than $n - 1$ provided the chain does not collapse. The fact that every constructive ideal refines to a prime ideal leads to the requirement that the chain C must collapse in order to ensure a well-defined Krull dimension, consistent with the classical approach.

3.4 Constructive version of Nullstellensatz

This section presents a constructive version of the classical Nullstellensatz, using the concepts of dynamic fields and triangular algebras to avoid relying on the assumption that the base field is algebraically closed (cf. [11, 12, 13]).

3.4.1 Dynamic Fields

Definition 3.43 (Dynamic Field). *A **dynamic field** is a pair $K = (A, P)$ where A is a commutative ring and $P = (I, U)$ is a potential prime of A. If P collapses in A, then K is said to collapse.*

The following theorem captures the behavior of dynamic fields under collapse conditions.

Theorem 3.44. *Given a dynamic field $K = (A, P)$ and a monic polynomial $f \in A[X]$, we consider the $A-$algebra $B = A[X]/(f)$. If the extended dynamic field $K[X] = (B, P)$ collapses, then K collapses too.*

Proof. Let $f \in A[X]$ be a monic polynomial of degree d. B is a free A-module with basis $\{1, X, X^2, \dots, X^{d-1}\}$ (follows from the Euclidean division algorithm). Therefore every element of B can be uniquely expressed in terms of elements from A.

Suppose (B, P) collapses, i.e., there exist $r_1, \dots, r_k \in R$ and $t_1, \dots, t_m \in T$ with:

$$\sum_{i=1}^{k} a_i r_i + \prod_{j=1}^{m} t_j = 0 \quad \text{in } B$$

where $a_i \in B$. Since B is free over A with basis $\{1, x, \dots, x^{d-1}\}$, we can expand each $a_i = \sum_{n=0}^{d-1} c_{i,n} X^n$ with $c_{i,n} \in A$. Substituting into the collapse equation and using linear independence of the basis, we obtain for each $0 \le n \le d-1$:

$$\sum_{i=1}^{k} c_{i,n} r_i + \delta_{n0} \prod_{j=1}^{m} t_j = 0 \quad \text{in } A$$

where δ_{n0} is the Kronecker delta. The $n = 0$ case shows $0 \in \langle r \rangle_A + M(t)$ in A, proving (A, P) collapses.

□

3.4.2 Triangular Algebras

Triangular algebras organize field extensions hierarchically, simplifying factorization and enabling inductive algorithms in constructive treatments.

Definition 3.45. *Let L be a field.*

1. *A finitely presented L-algebra A is called **triangular with** n **stages** if it is isomorphic to an algebra $L_{(P_1,\dots,P_n)} := L[X_1, \dots, X_n]/\langle P_1, \dots, P_n \rangle$ where each P_i is a monic polynomial in $L[X_1, \dots, X_{i-1}][X_i]$.*

2. *Two triangular algebras $L_{(P_1,\dots,P_n)}$ and $L_{(Q_1,\dots,Q_m)}$ are called **orthogonal** if there exists k such that $P_1 = Q_1, \dots, P_k = Q_k$ and there are $A, B \in L_{(P_1,\dots,P_k)}[X_{k+1}]$ with $AP_{k+1} + BQ_{k+1} = 1$*

3. *For any triangular algebra A, we denote by $\widetilde{A} := A/\eta(A)$.*

Observation 3.46. 3. implies that passing to $\widetilde{A}$ preserves the set of prime ideals, i.e., $\mathrm{Spec}(A) \cong \mathrm{Spec}(\widetilde{A}))$, while eliminating all nilpotent elements.

Theorem 3.47. *Let L be a field with decidable equality, $A = L_{(P_1,\ldots,P_n)}$ a triangular L-algebra, and $a_1, \ldots, a_s \in A$. Then there exist triangular L-algebras $(A_j)_{j=1,\ldots,r}$ pairwise orthogonal such that:*

1. $\widetilde{A} \simeq \widetilde{A}_1 \times \cdots \times \widetilde{A}_r$
2. *In each $\widetilde{A}_j$, every a_i is either zero or invertible*

Proof.

- **Base Case ($n = 0$):** Consider $A = L[X]/\langle f(X) \rangle$ and an element $g \in A$. Since equality is decidable in L, we can compute $d = \gcd(f, g)$. If $d = 1$, then g is invertible in A. Otherwise, factor $f = f_1 f_2$ such that $\gcd(f_1, g) = 1$ and $f_2 \mid g^k$ for some k. This yields algebras $A_1 = L[X]/\langle f_1 \rangle$ where g is invertible, and $A_2 = L[X]/\langle f_2 \rangle$ where g is nilpotent. Then $\widetilde{A} \simeq \widetilde{A}_1 \times \widetilde{A}_2$.
- **Inductive step:** Write $A = B[X_n]/\langle P_n \rangle$ with $B = L[X_1, \ldots, X_{n-1}]/\langle P_1, \ldots, P_{n-1} \rangle$. Since computations in $B[X_n]$ may be ambiguous, we apply the inductive hypothesis to factor B into orthogonal components where gcd-based reasoning is valid. Then lift each factor to $A_j = B_j[X_n]/\langle P_n \rangle$ and apply the base case in each.
- At each split, components share initial polynomials $P_1, \ldots, P_k$ and differ via a Bezout identity $AP_{k+1} + BQ_{k+1} = 1$, ensuring orthogonality by pairs.

□

This constructive factorization process lets us split triangular algebras into simpler components where each element behaves clearly, being either zero or invertible.

3.4.3 Hilbert Nullstellensatz in Constructive Mathematics

Finally, the triangular algebra machinery allows to capture all algebraic zeros through orthogonal decompositions and the collapse property of potential primes allows the detection of radical membership via dynamic evaluation, concluding with the following constructive version of the Hilbert's Nullstellensatz.

Theorem 3.48. *Let $\mathbf{L}$ be a field with decidable equality and $P = (f_1, \ldots, f_n; g)$ a potential prime in $\mathbf{L}[X_1, \ldots, X_m]$. The following are equivalent:*

1. *P collapses (i.e., $g \in \mathrm{Rad}\,(f_1, \ldots, f_n)$).*
2. *g vanishes on all algebraic zeros of $(f_1, \ldots, f_n)$ in triangular L-algebras.*
3. *g vanishes on all zeros of $(f_1, \ldots, f_n)$ in reduced L-algebras.*

4 Chapter 4: Historical developpement of Nullstellensatz and Early Proofs

4.1 Historical Evolution of Terminology in Commutative Algebra

It is important to understand the evolving terminology and conceptual background in which the foundations of commutative algebra were developed. Many terms we use today, such as the *Nullstellensatz*, ideals, or homogeneous polynomials, have historical roots reflecting the transition from concrete computational tools to abstract algebraic structures.

This section provides a brief overview of how certain key notions were originally introduced and labeled by early pioneers, and how these terms gradually took their modern form. Understanding this terminological evolution clarifies historical sources and highlights the constructive motivations and notational conventions shaping the theory.

1. The term *Nullstellensatz* (German for "Theorem of Zeros") is relatively recent. Earlier, it was commonly called the *Theorem of Hilbert.* Other mathematicians contributed different names: Macaulay called it the "Hilbert-Netto Theorem", and van der Waerden referred to it as the "Well Known Theorem of Hilbert". The theorem evolved into a broad framework engaging many mathematicians, beyond a mere compilation of propositions.

2. Not only the main theorem but also algebraic concepts such as ideals experienced naming changes. For instance, Lasker called ideals in $\mathbb{C}[x_1, \ldots, x_n]$ *modules.* This influenced Kronecker's notion of a *Modular system* to express polynomial membership $G \equiv 0 \pmod{(F_1, \ldots, F_k)}$, meaning G belongs to the ideal $(F_1, \ldots, F_k)$ in modern terminology.

3. Polynomial types were also named differently. For example, *homogeneous polynomials* (all nonzero terms have the same degree) were known as *forms.*

4. While modern commutative algebra is developed over algebraically closed fields K, classical literature often used $\mathbb{C}$ as the reference field for deriving key results.

This chapter highlights the main contributions of mathematicians who laid the foundations of modern commutative algebra and algebraic geometry. Their combination of computational techniques, conceptual insights, and abstract formalism has shaped the current theoretical landscape. The exposition is primarily based on the works cited in (cf. [16, 17]).

4.2 Noether's Fundamental Theorem (Plane Curves)

The fundamental theorem of Max Noether for plane curves states that given three curves $V(f), V(\phi), V(\psi) \subset \mathbb{A}^2_{\mathbb{C}}$, the polynomial f belongs to the ideal (ϕ, ψ) if and only if locally at each intersection point $p \in V(\phi, \psi)$ we can express f as:

$$f = a\phi + b\psi \quad \text{in} \cong \mathbb{C}[[x, y]],$$

For transverse intersections, this reduces to the global polynomial expression $f = A\phi + B\psi$ with $A, B \in \mathbb{C}[x, y]$.

Netto's geometric interpretation connects this to Hilbert's Nullstellensatz: when $V(f)$ contains all intersection points of $V(\phi)$ and $V(\psi)$, there exists an integer ρ (bounded by the maximal intersection multiplicity) such that:

$$f^\rho \in (\phi, \psi).$$

Noether's theorem became a precursor to modern ideal theory, where the radical $\text{Rad}\,(\phi, \psi)$ captures all polynomials vanishing on $V(\phi, \psi)$.

The generalization to higher dimensions by van der Waerden and others replaces plane curves with schemes $X \subset \mathbb{A}^n_{\mathbb{C}}$. The modern formulation uses:

1. The completed local ring $\widehat{\mathcal{O}}_{\mathbb{A}^n,p} \cong \mathbb{C}[[x_1, \ldots, x_n]]$ to test membership
2. Primary decomposition $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_m$ for the algebraic condition
3. The correspondence between ideals and varieties via $V(I) \leftrightarrow I(V(I)) = \sqrt{I}$

This framework, developed by E. Noether and Grothendieck, shows how Noether's original insight evolved into the modern duality between algebra and geometry.

4.3 Kronecker (Elimination Theory)

The concept of *ideals* originated in Kummer's work on algebraic number factorization, was later developed by Kronecker and Dedekind. Kronecker's approach extended beyond number fields to polynomial rings, particularly in *Elimination Theory* a method for solving systems of algebraic equations through successive eliminations. The foundational work appeared in Kronecker's 1882 Festschrift for Kummer, with detailed treatments by his student Molk. The Key Mathematical contributions of his work are:

1. **Elimination Algorithm**: For a system $V(f_1, \ldots, f_k) \subset \mathbb{A}^n_{\mathbb{C}}$, Kronecker's method constructs a triangular system through iterated resultants, reducing the problem dimension by one at each step:

$$\text{Res}_{x_n}(f_i, f_j) \in \mathbb{C}[x_1, \ldots, x_{n-1}]$$

2. **Netto's Generalization**: For a complete intersection $V(\phi_1, \ldots, \phi_n)$, Netto proved that if f vanishes on $V(\phi_1, \ldots, \phi_n)$, then:

$$f^\rho \in (\phi_1, \ldots, \phi_n) \quad \text{for some } \rho \geq 1$$

This anticipated Hilbert's Nullstellensatz, though Netto's flawed extension to overdetermined systems required later correction.

3. **Konig's Synthesis**: In his 564-page treatise , Konig attempted to unify:
   (a) Kronecker's elimination methods
   (b) Noether-style ideal theory for higher dimensions
   (c) Early versions of the Nullstellensatz

   Despite its influence on contemporaries like Macaulay , Konig's work contained critical errors in divisibility arguments.

The theory evolved through distinct phases:

1. **Kummer's Ideals** (1847): Algebraic number factorization
2. **Kronecker's Vision** (1882): Polynomial rings and elimination
3. **Modern Reformulation** (Noether/Hilbert): Abstract ideal theory and scheme-theoretic generalizations

Konig's represents a transitional work that bridged 19th-century computational algebra (Bezout, Cayley) with 20th-century structural approaches. Though obsolete in methods, it preserved important historical connections between Elimination Theory, Ideal Theory, and of course, Algebraic Geometry.

4.4 Hilbert

Hilbert's landmark papers revolutionized invariant theory by introducing polynomial ideal theory. His work synthesized:

1. **Kronecker's elimination methods**
2. **Dedekind's abstract approach** (modules and ideals)
3. **Geometric insights** from Salmon and Cayley

Among the many contributions developed by Hilbert, several have already been mentioned and discussed throughout this work, as they represent foundational steps in the evolution of modern algebra and algebraic geometry:

1. **Basis Theorem (Modern Version)**: For any ideal $I \subset K[x_1, \ldots, x_n]$, there exist finitely many polynomials $f_1, \ldots, f_m \in I$ such that:

   $$I = (f_1, \ldots, f_m)$$

   Hilbert's original formulation concerned homogeneous polynomials (forms) in infinite sequences.

2. **Nullforms and Nullstellensatz**: A form f is a nullform if all invariants vanish on it. For binary d-forms:

   $$f \text{ nullform} \iff \exists \text{ zero with multiplicity } > d/2$$

   This led to Hilbert's proof of the Nullstellensatz: if invariants $I_1, \ldots, I_\mu$ vanish on f, then some power $f^\rho \in (I_1, \ldots, I_\mu)$.

3. **Finite Generation of Invariants**: For $G = SL_n(\mathbb{C})$ acting on $V = S^{d_1}\mathbb{C}^n \oplus \cdots \oplus S^{d_k}\mathbb{C}^n$, the invariant ring $\mathbb{C}[V]^G$ is finitely generated via:

   (a) Noether normalization: $\mathbb{C}[V]^G$ is integral over $\mathbb{C}[J_1, \ldots, J_\kappa]$

   (b) Primitive element: $\mathbb{C}(V)^G = \mathbb{C}(J_1, \ldots, J_\kappa)(J)$

Criticized for non-constructive proofs, Hilbert later developed computational methods using Cayley's Ω-process (precursor to Reynolds operators) Kronecker's arithmetic of algebraic functions.

4.5 Lasker

Emanuel Lasker studied in Berlin and later in Gottingen, though his academic path was interrupted by a successful chess career, during which he was World Champion from 1894 to 1921. He earned his doctorate in Erlangen in 1900 with a thesis on *Reihen auf der Convergenzgrenze*. Despite his achievements, he never held a permanent academic position and did most of his mathematical work independently between 1903 and 1905.

His major contributions include the introduction of the primary decomposition of ideals, expressed as $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$, with each $\mathfrak{q}_i$ a primary ideal, thus extending Noether's theorem to higher dimensions. He also developed a new perspective on the Hilbert polynomial using non-zero divisors, which led to a new proof of the Nullstellensatz, generalizations to convergent power series $\mathbb{C}[x_1, ..., x_n]$, and applications to Plucker formulas for singular curves. His ideal theory was developed in parallel and independently from Hilbert's.

He was a multidisciplinary thinker, bridging abstract reasoning across chess, philosophy, and mathematics. His intellectual approach was predominantly deductive, guided by a deep love of truth and knowledge.

4.6 Macaulay

Francis Sowerby Macaulay worked as a schoolteacher until 1911, yet made important independent contributions to ideal theory. His main goal was to develop computational methods for Lasker's primary decomposition, $I = \mathfrak{q}_1 \cap \cdots \cap \mathfrak{q}_n$, at a time when no practical algorithms were available for such a decomposition.

In his 1913 paper, Macaulay synthesized Kronecker's elimination methods, Hilbert's basis theorem, and Lasker's decomposition to address the structure of polynomial ideals in $\mathbb{C}[x_1, \ldots, x_n]$, marking a shift toward an algebraic theory of ideals. His 1916 tract offered the first systematic exposition that combined Kronecker's computational techniques, Hilbert's abstract approach, and Lasker's primary ideals. In this work, he introduced the innovative method of Inverse Systems, which would later have a lasting influence.

Macaulay's work was well received. Emmy Noether praised his use of concrete examples and counterexamples, and his ideas became a foundational reference in van der Waerden's *Moderne Algebra*. His legacy lies in bridging the 19th-century computational algebra of Kronecker with the emerging abstract framework of the 20th century, notably influencing modern computational algebra and software such as Macaulay2.

4.7 Noether

Kurt Hentzelt completed his thesis in 1914 under E. Fischer, where he developed explicit elimination techniques for polynomial ideals. Notably, his work included the first known example of a non-unique primary decomposition, which was later cited by Noether. His style was heavily notational, relying on expressions such as (Notation with 4–5 indices) $\gg$ Conceptual explanations a point of criticism raised by Noether.

Although documentation is scarce, Hentzelt was possibly a student of Noether in Erlangen, and his contributions were acknowledged in her papers from 1914 and 1915. In their joint 1922 paper, Noether and Hentzelt provided a conceptual reformulation of Hentzelt's earlier work. Noether identified several computational difficulties, which she later assigned to Grete Hermann as part of Hermann's doctoral research, completed in 1926. During her

Moscow lectures in 1928–1929, Noether introduced abstract algebraic methods to the Soviet mathematical community, likely influencing the work of J. L. Rabinowitsch on the Nullstellensatz.

In 1926, van der Waerden published a foundational paper redefining the notion of the zero set of an ideal, remarkably without relying on classical elimination theory. Instead, he introduced the method of generic points, closely paralleling ideas from Noether's unpublished lectures. A persistent historical inaccuracy has been the misattribution of "Rabinowitsch's trick" to "A. Rabinowitsch," which highlights the often uncredited but central role Noether played through her teaching.

5 Conclusions

This work covers important topics in commutative algebra from both classical and constructive viewpoints. In the first two chapters, we carefully analyze key concepts like affine algebraic varieties, the Zariski topology, and Krull dimension. The focus was on understanding why these concepts are defined the way they are and giving clear geometric interpretations to help understand them better.

The third chapter, which is the most detailed and important part, introduces constructive algebra. This approach avoids some classical logical principles and focuses on giving explicit, algorithmic ways to work with algebraic ideas. Using concepts like collapse and dynamic structures, this chapter presents constructive versions of important theorems like the Nullstellensatz and Krull dimension, showing how these can be checked and used in a more concrete way.

The final chapter gives a historical overview that helps place the ideas in context. It shows how the work of early mathematicians led to the development of these theories and the Hilbert program. This part helps to understand the background and the evolution of the subject.

In summary, this work aims to give a clear and deep understanding of commutative algebra by combining different approaches and viewpoints, helping both theory and applications.

References

[1] Hungerford, T. W.: *Algebra*. Graduate Texts in Mathematics, vol. 73, 8th ed., Springer, 2000.

[2] Lang, S.: *Algebra*. Graduate Texts in Mathematics, vol. 211, Springer, 3rd ed., 2002.

[3] Atiyah, M. F.; MacDonald, I. G.: *Introduction to Commutative Algebra*. Addison-Wesley Series in Mathematics, Addison-Wesley, 1969.
Reprint edition, 2019.

[4] Matsumura, H.: *Commutative Ring Theory*, Cambridge Studies in Advanced Mathematics, no. 8, Cambridge University Press, Cambridge, 1989.

[5] Lang, S.: *Introduction to Algebraic Geometry*. Dover Books on Mathematics, Illustrated Edition, Dover Publications, 2002.

[6] Fulton, W.: *Algebraic Curves: An Introduction to Algebraic Geometry*, January 28, 2008.

[7] Nelson, P.: *Commutative Algebra: Some Basics on Krull Dimension*, ETH Zürich, November 23, 2017.

[8] Goldie, A. W.; Small, L. W.: A Study in Krull Dimension, *J. Algebra*, vol. 25, 1973.

[9] Engelking, R.: *Dimension Theory*. The University of Edinburgh, 1978.

[10] Grifo, E.: *Topics in Commutative Algebra: Symbolic Powers*, May 7-11, 2018.

[11] Lombardi, H.; Quitté, C.: *Commutative Algebra: Constructive Methods, Finite Projective Modules. Course and Exercises*. English translation by T. K. Roblot, Last corrections September 20, 2024.

[12] Lombardi, H.: *Structures algébriques dynamiques, espaces topologiques sans points et programme de Hilbert*. Université de Franche-Comté, October 2003.

[13] Lombardi, H.: Dimension de Krull, Nullstellensatze et évaluation dynamique, *Mathematische Zeitschrift*, vol. 242, 2002.

[14] Coquand, T. and Lombardi, H.: *A Short Proof for the Krull Dimension of a Polynomial Ring*, American Mathematical Monthly, Vol. 112, No. 9 (2005), pp. 826–829.

[15] Coquand, T.; Lombardi, H.; Roy, M.-F.: *An Elementary Characterisation of Krull Dimension*, April 2004.

[16] Stevens, J.: *Early Proofs of Hilbert's Nullstellensatz*. arXiv:2309.14024 [math.AG], 2023.

[17] Zach, R.: *Hilbert's Program Then and Now*, submitted August 29, 2005.