A proof for the Hilbert's Nullstellensatz Theorems

Kevin Alves Vasconcellos

March, 2021

Contents

1 Introduction

In this article, we have as main purpose to prove the Hilbert's Nullstellensatz theorems, which are key theorems in the classic algebraic geometry. There are several ways to prove to prove these results. The route chosen in this article is using the concept of valuations rings and integral dependence. Before explain this theorem, let's talk about the structure of this article. In section 2, we'll talk about integral dependence and its main results. If the reader knows the basic theory about this subject, he can skip to the section 3, which treats about valuation rings. In this section, it'll be defined and proved the existence of valuations rings. Moreover, it'll be proved that the integral closure of domain integral R is the intersection of all valuations rings of $\text{Quot}(R)$ which contains R. Finally, in the section 4, it'll be proved the Zariski's Lemma, which will be the key result to prove the weak and normal versions of Hilbert's Nullstellensatz

Theorem. As a little gift, using the Zariski lemma, it'll be proved that the maximal ideals of polynomials rings over a algebraically closed field Ω have a well-behaved structure and are in one-to-one correspondence with Ω^n, where n is the number of variables of the polynomial ring.

In order to talk about the Hilbert's Nullstellensatz Theorem, we need some definitions.

Definition 1.1. *Let k be a field and Ω be the algebraic closure of k. we define the n-dimensional affine space the family of all n-tuples in Ω^n and it is denoted by $\mathbb{A}^n_\Omega$*

We used $\mathbb{A}^n_\Omega$ instead of Ω^n simply because we don't want consider the vector space structure of $(\Omega^n, \Omega, +, *)$

Definition 1.2. *Let k be a field and Ω be the algebraic closure of k. $S \subseteq \mathbb{A}^n_\Omega$ is said an affine algebraic set if there is $\Phi \subseteq k[X_1, \ldots, X_n]$ such that*

$$S = \{(\alpha_1, \ldots, \alpha_n) \in \mathbb{A}^n_\Omega \ ; \ f(\alpha_1, \ldots, \alpha_n) = 0 \text{ for all } f \in \Phi\}.$$

In this case, we denote $S = \mathrm{V}(\Phi)$.

It's an easy exercise to show that for any $\Phi \subseteq k[X_1, \ldots, X_n]$, then $\mathrm{V}(\Phi) = \mathrm{V}(\langle\Phi\rangle)$, where $\langle\Phi\rangle$ is the ideal of $k[X_1, \ldots, X_n]$ generated by the elements of Φ. Since $k[X_1, \ldots, X_n]$ is a Noetherian ring by Hilbert't Basis theorem, it's immediate that there is $g_1, \ldots, g_n \in \langle\Phi\rangle$ such that

$$\mathrm{V}(\Phi) = \mathrm{V}(\{g_1, \ldots, g_n\}) \coloneqq \mathrm{V}(g_1, \ldots, g_n).$$

Now, given $S \subseteq \mathbb{A}^n_\Omega$, a natural question would be what are the polynomials which vanish in S. Motivating with this question, we have the following definition

Definition 1.3. *Let k be a field and Ω be the algebraic closure of k. Given $S \subseteq \mathbb{A}^n_\Omega$, we define the following ideal*

$$\mathfrak{I} = \{P \in \Omega[X_1, \ldots, X_n] \ ; \ P(\alpha_1, \ldots, \alpha_n) = 0 \text{ for all } (\alpha_1, \ldots, \alpha_n) \in S\}.$$

The Nullstellesatz Hilbert Theorem says that if a polynomial $P(X_1, \ldots, X_n) \in R = k[X_1, \ldots, X_n]$ vanishes in an algebraic affine set $V(I)$, where I is an ideal of R, then $P(X_1, \ldots, X_n) \in \sqrt{I}$, that is, there is $m \in \mathbb{N}$ such that $P(X_1, \ldots, X_n)^m \in I$. Moreover, it's true that $\sqrt{I} = \mathfrak{I}(\mathrm{V}(I))$.

Theorem 1.4 (Hilbert's Nullstellensatz Theorem)**.** *Let k be a field, Φ be a subset of polynomial ring $k[X_1, X_2, \ldots, X_n]$. Given $P(X_1, \ldots, X_n) \in k[X_1, X_2, \ldots, X_n]$, if $P(X_1, \ldots, X_n)$ vanishes on $\mathrm{V}(\langle\Phi\rangle)$, then there is $r > 0$ such that $P(X_1, \ldots, X_n)^r \in \langle\Phi\rangle$. Moreover, denoting $I = \langle\Phi\rangle$, then*

$$\sqrt{I} = \mathfrak{I}(\mathrm{V}(I)).$$

2 Integral dependence and integral closure

2.1 Main definitions and results

This is a preliminary section where it'll be defined the concept of integral dependence of an element over a given ring. The reader who is acquainted with the basic theory of integral closure can skip this section and go directly to Section 2. Moreover, be aware that not all results of this section will be used on the remaining of this article.

Definition 2.1. *Let $R \subseteq S$ be rings. $x \in S$ is said be integral over R if there is a monic polynomial $p(X) \in R[X]$ such that $p(x) = 0$.*

Now let's state the main and basic result which gives a necessary and enough condition for $x \in S$ be an integral element over R.

Proposition 2.2. *Let $R \subseteq S$ be rings and $x \in S$. The following assertions are equivalent.*

(i) x is integral over R;

(ii) $R[x]$ is an R-module finitely generated;

(iii) $R[x]$ is contained in a subring C of S such that C is a finitely generated R-module;

(iv) There is a faithful $R[x]$-module M which is finitely generated as R-module.

Proof: $(i) \longrightarrow (ii)$: In fact, since x is integral over R, there is $n \in \mathbb{N}$, $a_0, \ldots, a_n \in R$ such that

$$x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0.$$

Thus, by simple induction, we can prove that $R[x] = \mathrm{Span}_R\{1, x, \ldots, x^{n-1}\}$.
$(ii) \longrightarrow (iii)$: Take $C = R[x]$. C is a finitely generated R-module.
$(iii) \longrightarrow (iv)$: Take $M = C$. Since $R[x]$ is contained in C, C naturally has structure of $R[x]$-module. Since $1 \in R[x]$, for $x \in C$, $1.c = 0$ implies $c = 0$, then C is a faithful $R[x]$-module. Moreover, by hypothesis, $M = C$ is a finitely-generated R-module.
$(iv) \longrightarrow (i)$: Let $\{m_1, \ldots, m_n\}$ a set of generators of C as R-module. Since C is also a $R[x]$-module, there are $a_{11}, \ldots, a_{n1}, a_{21}, \ldots, a_{21}, \ldots, a_{n1}, \ldots, a_{nn} \in R$ such that

$$xm_i = \sum_{j=1}^{n} a_{ij} m_j$$

Using the Kronecker delta, we conclude that

$$\sum_{j=1}^{n}(a_{ij} - x\delta_{ij})m_j = 0$$

using the matrix notation, we obtain

$$A\begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} a_{11}-x & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22}-x & \dots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn}-x \end{bmatrix}\begin{bmatrix} m_1 \\ m_2 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Multiplying by adjoint matrix, we conclude that $\det(A)m_1 = \cdots = \det(A)m_n = 0$. So $\det(A)m = 0$ for every $m \in C$. Since C is a faithful $R[x]$-module, we conclude $\det(A) = 0$. However, unless a signal, $\det(A) = 0$ is an equation of integral dependence of x over R. Then x is integral over R. □

From this Proposition, we can extract two very important corollaries. The first says that if, given $R \subseteq S$ rings, if $x_1, \dots, x_n \in S$ are integral elements over R, then $R[x_1, \dots, x_n]$ is a finitely generated R-module. The second says that the subset of S constituted by the integral elements over R has ring structure with the sum and product induced by S.

Corollary 2.3. *Let $R \subseteq S$ be rings and $x_1, \dots, x_n \in S$. If $x_1, \dots, x_n$ are integral elements over R, then $R[x_1, \dots, x_n]$ is a finitely generated R-module.*

Proof: We'll proceed by induction in n. If $n = 1$, it was already proved in Proposition 2.2. Suppose that this result is true for $n-1$ elements. So let's $x_1, \dots, x_n \in S$ be integral elements over R. Since $R[x_1, \dots, x_{n-1}, x_n] = (R[x_1, \dots, x_{n-1}])[x_n]$ and x_n is integral over R, then x_n is integral over $R[x_1, \dots, x_{n-1}]$. By Proposition 2.2, $R[x_1, \dots, x_n]$ is a finitely generated $R[x_1, \dots, x_{n-1}]$-module. Let $\{m_1, \dots, m_r\}$ be a system of generators of $R[x_1, \dots, x_n]$ as $R[x_1, \dots, x_{n-1}]$-module . Since $R[x_1, \dots, x_{n-1}]$ is a finitely generated R-module, then, considering $\{n_1, \dots, n_s\}$ a system of generators of $R[x_1, \dots, x_{n-1}]$ as R-module, we obtain that $R = \mathrm{Span}_R\{m_i n_j \ ; \ 1 \le i \le r, 1 \le j \le s\}$. Then $R[x_1, \dots, x_n]$ is a finitely generated R-module

Corollary 2.4. *Let $R \subseteq S$ be rings. Denoting $T := \{x \in S \ ; \ x \text{ is integral over } R\}$, then T is a subring of S containing R.*

Proof: Let $x, y \in T$. By Corollary 2.3, we have that $R[x, y]$ is a finitely generated R-module.

Since

$$R \subseteq R[x+y] \subseteq R[x,y]$$

$$R \subseteq R[-x] \subseteq R[x,y]$$

$$R \subseteq R[xy] \subseteq R[x,y]$$

By Proposition 2.2, we conclude that $(T,+)$ is an abelian group and T is closed by product. Since clearly $R \subseteq T$, T contains 1 hence $(T,+,*)$ is a subring of C. □

The Corollary 2.4 motivates the following definition:

Definition 2.5. *Let $R \subseteq S$ be rings. The ring of elements of S which are integral over R is called the integral closure of R in S and denoted by $\overline{R}^S$. R is called integrally closed in S if $\overline{R}^S = R$ and S is said be an integral extension of R if $\overline{R}^S = S$.*

Example 2.6. *$\mathbb{Z}$ is integrally closed in $\mathbb{Q}$. In fact, let $r/s \in \mathbb{Q}$ be an integral element over $\mathbb{Z}$, where we can assume r, s has no common prime divisor. Thus there are $n \in \mathbb{Z}$, $a_1, \ldots, a_n \in \mathbb{Z}$ such that*

$$\left(\frac{r}{s}\right)^n + \sum_{i=1}^{n} a_i \left(\frac{r}{s}\right)^{n-i} = 0$$

Multiplying by s^n, we obtain that

$$r^n = -\sum_{i=1}^{n} a_i s^i r^{n-i}$$

Thus we have that s divides r^n. If $s \neq \pm 1$, we would conclude that r, s has common prime divisor, which is a contradiction, so $s = \pm 1$ and $r/s \in \mathbb{Z}$. Thus $\mathbb{Z}$ is integrally closed in $\mathbb{Q}$.

Let $R \subseteq S$ be an integral extension of rings. In general, it's not true that S is a finitely generated R-module as we'll see in the following example.

Example 2.7. *Let $R = \mathbb{Q}(\{\sqrt[n]{2} \ ; \ n \in \mathbb{N}\})$. Then $\mathbb{Q} \subseteq R$ is an integral extension, but R isn't a finitely generated $\mathbb{Q}$-module.*

Let R be a ring and T the of non-zerodivisors of R. It's easy to show that T is multiplicatively closed subset of R and that the mapping

$$\phi_T : R \longrightarrow R_T$$

$$x \longmapsto \tfrac{x}{1}$$

is injective homomorphism ring, so R can be considered a subring of R_T.

Definition 2.8. *Let R be a ring. Consider the multiplicatively closed set*

$$T = \{x \in R \ ; \ x \text{ is a non-zerodivisor of } R\}.$$

The localization ring R_T is called the total ring of fractions of R and is commonly denoted by $\mathrm{Quot}(R)$. *The integral closure of R in* $\mathrm{Quot}(R)$ *is denoted by $\overline{R}$ and R is said integrally closed if $\overline{R} = R$.*

Example 2.9. *Mutadis Mutantis in the proof of Example 2.6, we can prove that every unique factorization domain is integrally closed.*

Proposition 2.10 (Transitivy of integral dependence)**.** *Let $R \subseteq S \subseteq T$ be rings. If S is an integral extension of R and T is an integral extension of S, then T is an integral extension of R.*

Proof: In fact, let $x \in T$. Since T is integral over S, there are $n \in \mathbb{N}$, $a_1, \ldots, a_n \in S$ such that

$$x^n + \sum_{i=1}^{n} a_i x^i = 0$$

Consider the ring $A = R[a_1, \ldots, a_n]$. Note that x is integral over A, hence $A[x]$ is a finitely generated A-module. Moreover, since $a_1, \ldots, a_n$ are integral over R, we also have that A is a finitely generated R-module. Then $A[x]$ is a finitely generated R-module. Since $R \subseteq R[x] \subseteq A[x]$, using the part (iii) of Proposition 2.2, we conclude x is integral over R. Since x was chosen arbitrarily, we conclude T is an integral extension of R. □

Corollary 2.11. *Let $R \subseteq S$ be rings and $\overline{R}^S$ be the integral closure in S. Then $\overline{\overline{R}^S}^S = \overline{R}^S$.*

Proof: Indeed, note that

$$R \subseteq \overline{R}^S \subseteq \overline{\overline{R}^S}^S$$

and both extension are integral extensions. By transitivy of integral dependence, we have that $R \subseteq \overline{\overline{R}^S}^S$ is an integral extension. Thus, if $x \in \overline{\overline{R}^S}^S$, x is integral over R, so $x \in \overline{R}^S$. Hence $\overline{\overline{R}^S}^S \subseteq \overline{R}^S$ and so $\overline{R}^S = \overline{\overline{R}^S}^S$. □

Corollary 2.12. *Let R be a ring and $\overline{R}$ be its integral closure in the total ring of fractions. Then $\overline{R}$ is integrally closed.*

Proof: Note that, since $R \subseteq \overline{R} \subseteq \overline{\overline{R}}$, using the Corollary 2.11, it's enough to show that $\mathrm{Quot}(R) = \mathrm{Quot}(\overline{R})$. Let

$$S = \{x \in \overline{R} \ ; \ x \text{ is a non-zerodivisor of } \overline{R}\}$$

Define the following ring homomorphism

$$\phi : \overline{R} \longrightarrow \text{Quot}(R)$$

$$a/b \longmapsto a/b$$

Note that if $x \in S$, then $x = a/b$, where a is a non-zerodivisor of R. Thus clearly $\phi(x)$ unit in $\text{Quot}(R)$. Note that if $\phi(a/b) = 0$, then then there is a non-zerodivisor s of R such that $sa = 0$. Since every non-zero divisor of R is a non-zerodivisor of $\overline{R}$, we conclude that there is $s \in S$ such that $sa = 0$. Finally, given $a/b \in \text{Quot}(R)$, then

$$a/s = \phi(a)\phi(s)^{-1} = \phi\left(\frac{a}{s}\right).$$

By universal property of localization, we conclude that $\text{Quot}(\overline{R}) = (\overline{R})_S = \text{Quot}(R)$. □

Proposition 2.13. *Let $R \subseteq S$ be rings such that S is an integral extension of R.*

(i) If J is an ideal of S and $I = J^c = J \cap R$, then S/J is an integral extension of R/I;

(ii) If T is a multiplicative closed subset of R, then S_T is an integral extension of R_T.

Proof: (i): Consider the ring homomorphism

$$\psi : R \longrightarrow \frac{S}{J}$$

$$x \longmapsto \overline{x}$$

Note that $\ker(\psi) = J \cap R = I$, thus ψ induces a ring monomorphism $\overline{\psi} : R/I \longrightarrow S/J$. So we can inject R/I in S/J naturally. Let $s + J \in S/J$. Since $s \in S$ and S is integral over R, there is $n \in \mathbb{N}$, $a_1, \ldots, a_n \in R$ such that

$$s^n + \sum_{i=1}^{n} a_i s^{n-i} = 0. \tag{1}$$

Viewing this equation in S/J, we get

$$(s + J)^n + \sum_{i=1}^{n} (a_i + J)(s + J)^{n-i} = 0.$$

Since $a_i + J = \overline{\psi}(a_i + I)$ and R/I can be identified as subring of S/J, there is no problem in representing the equation (1) as

$$(s + J)^n + \sum_{i=1}^{n} (a_i + I)(s + J)^{n-i} = 0.$$

Then S/J is an integral extension of R/I.

(2): It's clear that R_T is a subring of S_T. Let $x/s \in S_T$. Since $x \in S$ and S is integral over R, there is $n \in \mathbb{N}$, $a_1, \ldots, a_n \in R$ such that

$$x^n + \sum_{i=1}^{n} a_i x^{n-i} = 0.$$

Multiplying this equation by $1/s^n$, we get

$$\left(\frac{x}{s}\right)^n + \sum_{i=1}^{n} \frac{x}{s^i}\left(\frac{x}{s}\right)^{n-i} = 0.$$

Thus x/s is integral over R_T. Since x/s was chosen arbitrarily, we conclude S_T is an integral extension of R_S.

2.2 The Lying-over and Going-up Theorems

In this section, we'll prove, beyond other results, two important properties that the integral extensions satisfies. These properties are the Lying-over property and the Going-up property. Firstly we'll prove that the condition of to be a field is rigid when we are treating with integral extensions of integral domains.

Proposition 2.14. *Let $R \subseteq S$ be integral domains such that S is an integral extension of R. Then S is a field if and only if R is a field.*

Proof: Suppose that S is a field and let $x \in R \setminus \{0\}$. Since S is a field, there is $y \in S$ such that $xy = yx = 1$. In order to prove that R is a field, it's enough to show that $y \in R$. Indeed, since S is integral over R, there is $n \in \mathbb{N}$, $a_1, \ldots, a_n \in R$ such that

$$y^n + \sum_{i=1}^{n} a_i y^{n-i} = 0.$$

Multiplying the equation above by x^{n-1}, we get

$$y = -\sum_{i=1}^{n} a_i x^i \in R.$$

Then $y \in R$ and so R is a field.

Now suppose that R is a field and let $x \in S \setminus \{0\}$. Since S is integral over R, there is $n \in \mathbb{N}$, $a_1, \ldots, a_n \in R$ such that

$$x^n + a_1 x^{n-1} + \cdots + a_{n-1} x + a_n = 0$$

Note that if $a_n = \cdots = a_{n-i} = 0$ for some $0 \leq i \leq n$, we can factor x^{i+1} and, using the fact that S is integral domain, obtain a new equation of integral dependence whose independent coefficient is non-zero. So we can suppose without lost of generality that $a_n \neq 0$ Assuming $a_n \neq 0$, thus we get

$$x(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1}) = -a_n$$

Since R is a field, we obtain that

$$x[(-a_n)^{-1}(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1})] = [(-a_n)^{-1}(x^{n-1} + a_1 x^{n-2} + \cdots + a_{n-1})]x = 1$$

Then x is unit and S is a field. □

An immediate consequence of this proposition is that, in an integral extension of rings, the contraction of an maximal ideal is always a maximal ideal.

Corollary 2.15. *Let $R \subseteq S$ be rings such that S is an integral extension of A. Let $\mathfrak{q}$ be a prime ideal of S and $\mathfrak{p} = \mathfrak{q}^c = \mathfrak{q} \cap R$. Then $\mathfrak{p}$ is a maximal ideal of R if and only if $\mathfrak{q}$ is a maximal ideal of S.*

Proof: Indeed, by Proposition 2.13 $S/\mathfrak{q}$ is an integral extension of $R/\mathfrak{p}$. Moreover, both rings are integral domains. Thus, by Proposition 2.14, $R/\mathfrak{p}$ is a field if and only if $S/\mathfrak{q}$ is field, that is, $\mathfrak{p}$ is a maximal ideal of R if and only if $\mathfrak{q}$ is a maximal ideal of S. □

Corollary 2.16 (incomparability)**.** *Let $R \subseteq S$ be rings such that S is an integral of R. Let $\mathfrak{q}, \mathfrak{q}'$ be prime ideals of S such that $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q}^c = \mathfrak{q}'^c = \mathfrak{p}$ say. Then $\mathfrak{q} = \mathfrak{q}'$.*

Proof: Indeed, consider $S_\mathfrak{p}$ the localization of S in the multiplicatively closed set $R \setminus \mathfrak{p}$. Since S is integral over R, then $S_\mathfrak{p}$ is integral over $R_\mathfrak{p}$. Note that $(\mathfrak{q}S_\mathfrak{p})^c = (\mathfrak{q}'S_\mathfrak{p})^c = \mathfrak{p}R_\mathfrak{p}$ which is the maximal ideal of $R_\mathfrak{p}$. Thus, by Corollary 2.15, we conclude that $\mathfrak{q}'S_\mathfrak{p}, \mathfrak{q}S_\mathfrak{p}$ are maximal ideals of $S_\mathfrak{p}$. Since $\mathfrak{q} \subseteq \mathfrak{q}'$, we conclude $\mathfrak{q}'S_\mathfrak{p} = \mathfrak{q}S_\mathfrak{p}$, so $\mathfrak{q} = \mathfrak{q}'$. □

Definition 2.17. *Let $R \subseteq S$ be a extension ring. This extension is said to satisfy the Lying-over property if, given a prime ideal $\mathfrak{p}$ of R, there is a prime ideal $\mathfrak{q}$ of S such that $\mathfrak{q}^c = \mathfrak{q} \cap R = \mathfrak{p}$*

The integral extension of rings always satisfies the Lying-over property, as we'll see in the next proposition. In particular, since the contraction of ideals maximal is always maximal in integral extensions, if S is a flat R-algebra and integral over R, we get immediately that S is a faithfully flat R-algebra.

Proposition 2.18. *Let $R \subseteq S$ be rings. If S is an integral extension of R, then this extension satisfies the Lying-over property.*

Proof: Indeed, consider $S_{\mathfrak{p}}$ the localization of S in the multiplicatively closed set $R \setminus \mathfrak{p}$. Since S is integral over R, then $S_{\mathfrak{p}}$ is integral over $R_{\mathfrak{p}}$. Let $\mathfrak{n} = \mathfrak{q}S_{\mathfrak{p}}$ be a maximal ideal of $S_{\mathfrak{q}}$. Note that $\mathfrak{n}^c = \mathfrak{p}R_{\mathfrak{p}}$ since $\mathfrak{p}R_{\mathfrak{p}}$ is the only maximal ideal of $R_{\mathfrak{p}}$ and $R_{\mathfrak{p}} \subseteq S_{\mathfrak{p}}$ is an integral extension. Since the following diagram

$$\begin{array}{ccc} R & \xrightarrow{i} & S \\ {\scriptstyle i_{R_{\mathfrak{p}}}}\downarrow & & \downarrow{\scriptstyle i_{S_{\mathfrak{p}}}} \\ R_{\mathfrak{p}} & \xrightarrow{i_{\mathfrak{p}}} & S_{\mathfrak{p}} \end{array}$$

is commutative, then $\mathfrak{q} := (i_{S_{\mathfrak{q}}})^{-1}(\mathfrak{n})$ is such that $\mathfrak{q} \cap R = \mathfrak{p}$. □

Definition 2.19. *Let $R \subseteq S$ be a extension ring. This extension is said to satisfy the Going-up property if, given prime ideals $\mathfrak{p}$, $\mathfrak{p}'$ of R with $\mathfrak{p} \subseteq \mathfrak{p}'$ and a prime ideal $\mathfrak{q}$ of S with $\mathfrak{q}^c = \mathfrak{p}$, then there is a prime ideal $\mathfrak{q}'$ of S such that $\mathfrak{q} \subseteq \mathfrak{q}'$ and $\mathfrak{q}'^c = \mathfrak{p}$*

The integral extension of rings always satisfies the Going-up property, as we'll see in the next proposition.

Proposition 2.20. *Let $R \subseteq S$ be rings. If S is an integral extension of R, then this extension satisfies the Going-up property.*

Proof: Indeed, consider the rings $R' = R/\mathfrak{p}$ and $S' = S/\mathfrak{q}$. Note that, by Proposition 2.13, S' is an integral extension of R'. Considering the prime ideal $P = \mathfrak{p}'/\mathfrak{p}$ of R', by Lying-over property, there is an ideal $Q = \mathfrak{q}'/\mathfrak{q}$ such that $Q \cap R' = P$. Considering the natural epimorphism $\pi_S : S \longrightarrow S'$, we have that $\mathfrak{q}' = \pi^{-1}(Q)$ is a prime ideal of S and $\mathfrak{q}' \cap R = \mathfrak{p}$ since the following diagram

$$\begin{array}{ccc} R & \xrightarrow{i} & S \\ {\scriptstyle \pi_R}\downarrow & & \downarrow{\scriptstyle \pi_S} \\ R' & \xrightarrow{\bar{i}} & S' \end{array}$$

is commutative. □

3 Valuation rings

In this section, we'll define a important class of rings which is the valuation rings. These rings appear frequently in commutative algebra and algebraic geometry.

3.1 Main definitions and properties

Definition 3.1. *Let R be an integral domain with total field of fractions K. R is said a valuation ring if, given $x \in K$, then $x \in R$ or $x^{-1} \in R$.*

An important characterization of these rings is that the family of all its ideals is totally ordered by inclusion.

Proposition 3.2. *Let R be an integral domain with total field of fractions K. The following assertions are equivalent:*

(i) R is a valuation ring;

(ii) If $\mathcal{I}$ is the family of all ideals of R, then $(\mathcal{I}, \subseteq)$ is totally ordered;

(iii) If $\mathcal{P}$ is the family of all principal ideals of R, then $(\mathcal{P}, \subseteq)$ is totally ordered.

Proof: $(i) \longrightarrow (ii)$: Let I, J be ideals of R and suppose that $I \nsubseteq J$. Thus let $y \in I \setminus J$ and let $x \in J$ be arbitrary. Consider the element $x/y \in K$. Since R is an valuation ring, then $x/y \in R$ or $y/x \in R$.

- Suppose that $y/x \in R$, then $y \in xR \subseteq J$, which is an contradiction since $y \notin J$.
- Thus it's true that $x/y \in R$. But so we have that $x \in yR \subseteq I$, which allows us to conclude that $J \subseteq I$.

$(ii) \longrightarrow (iii)$: Since every non-empty subset of a totally ordered set is totally ordered with the induced order, we conclude that, if $(\mathcal{I}, \subseteq)$ is totally ordered, then so is $(\mathcal{P}, \subseteq)$.

$(iii) \longrightarrow (i)$: Let $x \in K$, so $x = a/b$ for some $a, b \in R$. Consider the principal ideals $I = (a)$ and $J = (b)$. Since $(\mathcal{P}, \subseteq)$ is totally ordered, either $I \subseteq J$ or $J \subseteq I$.

- If $I = (a) \subseteq (b) = J$, then there is $z \in R$ such that $a = bz$, then $x = a/b = z \in R$.
- If $J = (b) \subseteq (a) = I$, then there is $z \in R$ such that $b = az$, then $x^{-1} = b/a = z \in R$.

So we conclude that R is a valuation ring. □

Corollary 3.3. *Let R be an integral domain. If R is a valuation ring, then R is a local ring.*

Proof: Let $\mathfrak{m}$ and $\mathfrak{m}'$ be maximal ideals of R. Since the family of ideals of R is totally ordered by inclusion, then we can assume without lost of generality that $\mathfrak{m} \subseteq \mathfrak{m}'$. However, since both ideals are maximal, we conclude $\mathfrak{m} = \mathfrak{m}'$. Hence R has only one maximal ideal, that is, R is a local ring. □

3.2 Existence of valuation rings

Until now, we defined the valuation rings and proved some important properties theses rings have. However there is a natural question still unasked: Do these rings, in fact, exist? Now we'll prove the existence of these rings. The proof is long and requires several results.

Proposition 3.4. *Let F be a field and Ω be an algebraically closed field. Given an algebraic extension K of F and $\phi : F \longrightarrow \Omega$ a field homomorphism, there is a field homomorphism $\psi : K \longrightarrow \Omega$ such that $\psi|_F = \phi$.*

Proof: This proof is Zorn's lemma based and it's divided in two parts:

Step 1: If $x \in K$ is algebraic over F and $L := F(x)$, then, given field homomorphism $\phi : F \longrightarrow \Omega$, there is a field homomorphism $\psi : L \longrightarrow \Omega$ such that $\psi|_F = \phi$.

In fact, since x is algebraic over F, there is a minimal monic polynomial $p(X) \in F[X]$ such that $p(x) = 0$. Denote

$$p(X) = X^n + a_1 X^{n-1} + \cdots + a_{n-1}X + a_n.$$

Consider $p^\phi(X) \in \Omega[X]$ the image of $p(X)$ under ϕ. Thus we have

$$p^\phi(X) = X^n + \phi(a_1)X^{n-1} + \cdots + \phi(a_{n-1})X + \phi(a_n).$$

Since Ω is an algebraically closed field, let $\zeta \in \Omega$ be a root of $p^\phi(X)$ and define

$$\psi : L \longrightarrow \Omega$$

$$\textstyle\sum_{i=0}^n a_i x^i \longmapsto \sum_{i=0}^n \phi(a_i)\zeta^i$$

Note that ψ is well-defined, because if $\sum_{i=0}^n a_i x^i = \sum_{i=0}^m b_i x^i$, then, defining the polynomials

$$g_1(X) = \sum_{i=0}^{n} a_i X^i \in F[X] \quad \text{and} \quad g_2(X) = \sum_{i=0}^{m} b_i X^i \in F[X]$$

we have that $(g_1 - g_2)(x) = 0$. Thus, since $p(X)$ is the minimal monic polynomial for x in $F[X]$, we obtain that $p(X)$ divides $(g_1 - g_2)(X)$, that is, there is $q(X) \in F[X]$ such that $(g_1 - g_2)(X) = p(X)q(X)$. Note that

$$(g_1^\phi - g_2^\phi)(X) = p^\phi(X)q^\phi.(X)$$

Thus

$$g_1^\phi(\zeta) - g_2^\phi(\zeta) = p^\phi(\zeta)q^\phi(\zeta) = 0$$

Then

$$\psi\left(\sum_{i=0}^{n} a_i x^i\right) = g_1^{\phi}(\zeta) = g_2^{\phi}(\zeta) = \psi\left(\sum_{i=0}^{m} b_i x^i\right).$$

Then ψ is a well-defined field homomorphism which extends ϕ.

Step 2: Let K be a algebraic extension of F and $\phi : F \longrightarrow \Omega$ be a field homomorphism, then there is a field homomorphism $\psi : K \longrightarrow \Omega$ which extends ϕ.

In fact, consider the following family:

$$\Delta = \{(L, f) \ ; \ L \text{ is a field with } F \subseteq L \subseteq K \text{ and } f : L \longrightarrow \Omega \text{ is a field homom. which extends } \phi \ \}.$$

Note that $\Delta \neq \varnothing$, because $(F, \phi) \in \Delta$. Define in Δ the following partial order:

$$(L, f) \leq (T, g) \qquad \Longleftrightarrow \qquad L \subseteq T \quad \text{and} \quad g|_L = f.$$

It's easy to prove that any chain in Σ has an upper bound, thus, by Zorn Lemma, Σ has maximal element (S, g). I claim that $L = K$. Indeed, if not, let $x \in K \setminus L$. Since x is algebraic over F and so over L, by Step 1, there is a field homomorphism $\overline{g} : S(x) \longrightarrow \Omega$ which extends g and, in particular, extends ϕ. Thus $(S(x), \overline{g}) \in \Delta$ and $(S, g) < (S(x), \overline{g})$, which contradicts the maximality of (S, g) in Δ. Then $S = K$, which proves the proposition. □

Proposition 3.5. *Let R be an integral domain with total field of fractions K and $\mathfrak{p}$ be a prime ideal of R. Given $x \neq 0 \in K$, then either $\mathfrak{p}R[x] \neq R[x]$ or $\mathfrak{p}R[x^{-1}] \neq R[x^{-1}]$*

Proof: Note that we can assume without lost of generality that $(R, \mathfrak{m})$ is a local domain and that $\mathfrak{p} = \mathfrak{m}$. Indeed, after localization in $\mathfrak{p}$, if we prove that either

$$\mathfrak{p}R_{\mathfrak{p}}[x] \neq R_{\mathfrak{p}}[x] \qquad \text{or} \qquad \mathfrak{p}R_{\mathfrak{p}}[x^{-1}] \neq R_{\mathfrak{p}}[x^{-1}],$$

then it's clear that

$$\mathfrak{p}R[x] \neq R[x] \qquad \text{or} \qquad \mathfrak{p}R[x^{-1}] \neq R[x^{-1}].$$

Thus suppose $(R, \mathfrak{m})$ is a local domain and $\mathfrak{p} = \mathfrak{m}$. Suppose that $\mathfrak{m}R[x] = R[x]$. Thus there $a_0, \ldots, a_n \mathfrak{m}$ such that

$$1 = a_0 + a_1 x + \cdots + a_n x^n$$

Since R is a local ring, then $1 - a_0$ is unit in R, then multiplying the equation above by $(1 - a_0)^{-1}$ and denoting $a_i(1 - a_0)^{-1}$ by b_i for each $1 \leq n$, we obtain

$$1 = b_1 x + \cdots + b_n x^n \tag{2}$$

Multiplying the equation (1) by x^{-n}, we obtain

$$(x^{-1})^n - \sum_{i=1}^{n} b_i (x^{-1})^i = 0.$$

Thus x^{-1} is integral over R and the ring extension $R \subseteq R[x^{-1}]$ is integral. Since the Lying-over property is true for integral extensions, there is a prime ideal $\mathfrak{m}$ of $R[x^{-1}]$ such that $\mathfrak{p} \cap R = \mathfrak{m}$. Then

$$\mathfrak{m}R[x^{-1}] = \mathfrak{m}[x^{-1}] = \mathfrak{m}^e = \mathfrak{p}^{ce} \subseteq \mathfrak{p} \subsetneq R[x^{-1}]$$

Thus $\mathfrak{m}R[x^{-1}] \neq R[x^{-1}]$. □

Now we proved these two propositions, we are almost ready to prove the existence of valuations rings. Let K be a field and Ω be an algebraically closed field. Consider the following family:

$$\Sigma = \{(A, f) \ / \ R \text{ is subring of } K \text{ and } f : R \longrightarrow \Omega \text{ is a ring homomorphism}\}$$

Note that $\Sigma \neq \varnothing$ since $(0, 0) \in \Sigma$. Define in Σ the following partial order:

$$(R, f) \leq (S, g) \qquad \Longleftrightarrow \qquad R \subseteq S \quad \text{and} \quad g|_R = f.$$

It's easy to prove that any chain in Σ has an upper bound, thus, by Zorn Lemma, Σ has maximal element (S, g).

Lemma 3.6. *Let (S, g) be a maximal element of Σ. Then S is a local ring and $\mathfrak{m} = \ker(g)$ is a maximal ideal of S.*

Proof: Indeed, by First Isomorphism Theorem, we have that

$$g(S) \cong \frac{S}{\ker(g)} = \frac{S}{\mathfrak{m}}.$$

Since $g(S)$ is a subring of a field, $g(S)$ is an integral domain and so $\mathfrak{m}$ is a prime ideal of S. Localizing S in $\mathfrak{m}$, we obtain the ring $S_{\mathfrak{m}}$ which contains S as subring. Moreover, the ring homomorphism

$$g_{\mathfrak{m}} : S_{\mathfrak{m}} \longrightarrow \Omega$$

$$\frac{r}{s} \longmapsto \frac{g(r)}{g(s)}$$

extends g. Thus $(S_{\mathfrak{m}}, g_{\mathfrak{m}}) \in \Sigma$ and $(S, g) \leq (S_{\mathfrak{m}}, g_{\mathfrak{m}})$. By maximility of (S, g) in Σ, we have $(S, g) = (S_{\mathfrak{m}}, g_{\mathfrak{m}})$. Thus S is a local ring and $\mathfrak{m}$ is a maximal ideal of S. □

Theorem 3.7. *Let (S, g) be a maximal element of Σ. Then S is valuation ring of the field K.*

Proof: We have to show that if $x \neq 0$ is an element of K, then either $x \in S$ or $x^{-1} \in S$. By Lemma 3.5, we can assume without lost of generality that $\mathfrak{m}[x] \neq S[x]$, where $\mathfrak{m} = \ker(g)$. Thus there is a maximal ideal $\mathfrak{m}'$ of $S[x]$ such that $\mathfrak{m}[x] \subseteq \mathfrak{m}'$. Note that $\mathfrak{m} = \mathfrak{m}' \cap S$. In fact, observe that

$$\mathfrak{m} = \mathfrak{m} \cap S \subseteq \mathfrak{m}' \cap S.$$

Since $\mathfrak{m}$ is an ideal maximal ideal of S and $\mathfrak{m}' \cap S$ is a prime ideal of S, then $\mathfrak{m} = \mathfrak{m}' \cap S$. Thus there is a natural embedding

$$\phi : \frac{S}{\mathfrak{m}} \longrightarrow \frac{S[x]}{\mathfrak{m}'}$$

$$\overline{x} \longmapsto \overline{x}$$

Moreover, denoting $S/\mathfrak{m}$ by k, note that $S[x]/\mathfrak{m}' = k[\overline{x}]$, where $\overline{x}$ is the image of x in $S[x]/\mathfrak{m}'$ Hence $\overline{x}$ is algebraic over k and $S[x]/\mathfrak{m}' = k[\overline{x}]$ is a finite algebraic extension of k.

Now observe that the homomorphism $g : S \longrightarrow \Omega$ induces a field homomorphism $\overline{g} : S/\mathfrak{m} \longrightarrow \Omega$ since $\mathfrak{m} = \ker(g)$ is a maximal ideal. By Proposition 3.4, since Ω is algebraically closed, we can extend $\overline{g}$ to $\hat{g} : S[x]/\mathfrak{m}' \longrightarrow \Omega$. Considering the natural epimorphism $\pi : S[x] \longrightarrow S[x]/\mathfrak{m}'$, we obtain the following ring homomorphism

$$\hat{g} \circ \pi : S[x] \longrightarrow \Omega$$

$$z \longmapsto \hat{g}(\overline{z})$$

Finally observe that if $z \in S$, then $(\hat{g} \circ \pi)(z) = g(z)$, thus $\hat{g} \circ \pi$ extends g and $(S[x], \hat{g} \circ \pi) \in \Sigma$. Since (S, g) is maximal element of Σ and $(S, g) \leq (S[x], \hat{g} \circ \pi)$, then $(S[x], \hat{g} \circ \pi) = (S, g)$. Thus $x \in S = S[x]$ and so S is a valuation ring of the field K.

Corollary 3.8. *Let R be a subring of the field K. Then the integral closure $\overline{R}$ of R in K is the intersection of all valuations rings of K which contain R.*

Proof: Let S be a valuation ring of K which contains R. Then, since S is integrally closed and $\mathrm{Quot}(R) = \mathrm{Quot}(S)$, then

$$\overline{R} \subseteq \overline{S} = S$$

Thus

$$\overline{R} \subseteq \bigcap_{S \text{ valuation of } K,\ R \subseteq S} S$$

Conversely, let $x \notin \overline{R}$, then $x \notin R' = R[x^{-1}]$. because if $x \in R'$, it's easy to conclude that $x \in \overline{A}$. Then x^{-1} is a non-unit in R', so there is a maximal ideal $\mathfrak{m}'$ containing x'. Let $k = R'/\mathfrak{m}'$ and $\Omega = \overline{k}$. Note that there is a natural mapping

$$\phi : R' \longrightarrow \Omega$$

$$x \longmapsto \overline{x}$$

Let $\psi = \phi|_R : R \longrightarrow \Omega$ be a ring homomorphism. By Theorem 3.7, ϕ can be extended a ring homomorphism $\Theta : S \longrightarrow \Omega$ such that S is a valuation ring of K containing R. Moreover, since $\Theta(x^{-1}) = 0$, then $x \notin S$, because if x also belongs to S, we would obtain

$$0 = \Theta(x)\Theta(x^{-1}) = \Theta(xx^{-1}) = \Theta(1) = 1$$

a contradiction, thus $x \notin S$, hence

$$\bigcap_{S \text{ valuation of } K,\ R \subseteq S} S \subseteq \overline{R}$$

□

4 Hilbert's Nullstellensatz Theorem and its versions

Now we are ready to prove the several versions of Hilbert's Nullstellesatz Theorems. Remember that there are several forms to prove theses results. In this text, we'll use Zariski's Lemma as main key.

Lemma 4.1. *Let $R \subseteq S$ be integral domains, S be a finitely generated R-algebra and Ω be an algebraically closed field. Let v be a non-zero element of S. Then there is $u \neq 0$ in R with the following property: Any ring homomorphism $f : R \longrightarrow \Omega$ such that $f(u) \neq 0$ can be extended to a ring homomorphism $g : S \longrightarrow \Omega$ such that $g(v) \neq 0$*

Proof: The proof consists by induction of number t of generators of S as R-algebra. Suppose $t = 1$. Then $S = R[x]$. We have two possibilities:

(i) Suppose x is transcedental over R and let $v = a_0x^n + \cdots + a_{n-1}x + a_n$ and take $u = a_0$. Then if $f : R \longrightarrow \Omega$ is ring homomorphism such that $f(a_0) \neq 0$. Then, denoting by $p(X)$, the polynomial

$$p(X) = f(a_0)X^n + \ldots f(a_{n-1})X + f(a_n)$$

we have clearly that $p(X)$ is a non-null polynomial in $\Omega[X]$. Since Ω is infinity, there is $\zeta \in \Omega$ such that $p(\zeta) \neq 0$. Let g be a ring extension of f such that

$$g : S \longrightarrow \Omega$$

$$x \longmapsto \zeta$$

Then $g(v) = f(a_0)\zeta^n + \ldots f(a_{n-1})\zeta + f(a_n) \neq 0$

(ii) Now suppose that x is algebraic over R, that is, x is algebraic over $\mathrm{Quot}(R)$. Since v is a polynomial in x, v is algebraic over R and so v^{-1} is integral over R. Hence we have equations of form

$$a_0 x^m + a_1 x^{m-1} + \cdots + a_m = 0 \tag{3}$$

$$a_0' v^{-n} + a_1' v^{-(n-1)} + \cdots + a_n' = 0 \tag{4}$$

Let $u = a_0 a_0'$ and $f : R \longrightarrow \Omega$ such that $f(a_0 a_0') \neq 0$ Then f can be extended , first to a homomorphism ring $f_1 : R[u^{-1}] \longrightarrow \Omega$ (with $f_1(u^{-1}) = f(u)^{-1}$), and then by Theorem 3.7 to a ring homomorphism $h : C \longrightarrow \Omega$, where T is a valuation ring of K containing $R[u^{-1}]$. From equation (3), we have that x is integral over $R[u^{-1}]$, then $x \in T0$ by Corollary 3.8, so that B is contained in T and, in particular, $v \in T$. On the other hand, from equation (4), v^{-1} is integral over $R[u^{-1}]$, and therefore by Corollary 3.8 again, $v^{-1} \in T$. Then v is unit in T and hence $h(v) \neq 0$. Take g the restriction of h to B.

Now suppose this result is true for S which is R-algebra generated by n elements. Let S be an R algebra generated by $n+1$ elements, that is, $R \subseteq R[x_1, \ldots, x_n] \subseteq R[x_1, \ldots, x_n, x_{n+1}] = S$ and $v \in S \setminus \{0\}$. By the case, $k = 1$, there is $u' \in R[x_1, \ldots, x_n] \setminus \{0\}$ with the following property: Any ring homomorphism $f : R[x_1, \ldots, x_n] \longrightarrow \Omega$ such that $f(u') \neq 0$ can be extended to a ring homomorphism $g : S \longrightarrow \Omega$ such that $g(v) \neq 0$. Using the induction hypothesis, we have that there is $u \in R \setminus \{0\}$ with the following property: Any ring homomorphism $f : R \longrightarrow \Omega$ such that $f(u) \neq 0$ can be extended to a ring homomorphism $g' : R[x_1, \ldots, x_n] \longrightarrow \Omega$ such that $g'(u') \neq 0$. □

Lemma 4.2 (Zariski's Lemma)**.** *Let k be a field and S be a finitely generated k-algebra. If S is a field, then it is a finite algebraic extension of k.*

Proof: Let S be a field which is a finitely generated k-algebra and consider the mapping

$$g : k \longrightarrow S$$

$$x \longmapsto x.1_S$$

It's easy to prove that g is a field homomorphism, so we naturally can see S as a field extension of k. Using the notation of previous Lemma, consider $\Omega = \overline{k}$, $R = k$ and $v = 1 \neq 0$. Since S is

finitely generated k-algebra, there exists $u \in R$, $u \neq 0$ satisfying the property of previous Lemma. Moreover, the field homomorphism

$$g : k \longrightarrow \overline{k} = \Omega$$

$$x \longmapsto x$$

is such that $f(u) \neq 0$, so there is an extension $g : S \longrightarrow \Omega$ such that $g(v) \neq 0$. Note g is injective since S is field. Now, given $x \in S$, we have $g(x) \in \Omega$. Since Ω is the algebraic closure of k, there is a polynomial

$$p(X) = \sum_{i=0}^{n} a_n X^n \in k[X].$$

such that $p(g(x)) = 0$. But

$$0 = \sum_{i=0}^{n} a_n g(x)^n = \sum_{i=0}^{n} g(a_n) g(x)^n = g\left(\sum_{i=0}^{n} a_n x^n \right).$$

Since g is injective, $\sum_{i=0}^{n} a_n x^n = 0$, thus x is algebraic over k. Then the field extension is $k \subseteq S$ is algebraic. Since it is finitely generated, it is finite algebraic extension. □

Finally we are ready to prove the weak version of Hilbert's Nullstellensatz Theorem.

Theorem 4.3 (Weak Hilbert's Nullstellensatz Theorem)**.** *Let k be a field and Φ be a subset of the polynomial ring $k[X_1, \ldots, X_n]$. If $\mathrm{V}(\Phi) = \varnothing$, then 1 belongs to the ideal I generated by the elements of Φ.*

Proof: Let I be the ideal generated by the elements of Φ. If I were a proper ideal of $k[X_1, \ldots, X_n]$, then there would be a maximal ideal $\mathfrak{m}$ such that $I \subseteq \mathfrak{m}$. Note that

$$K = \frac{k[X_1, \ldots, X_n]}{\mathfrak{m}} = k[\overline{x_1}, \ldots, \overline{x_n}].$$

is a finitely generated k-algebra. By Zariski's Lemma, K is an algebraic extension of k. Thus, by Proposition 3.4, there is a natural embedding

$$\phi : K \longrightarrow \overline{k}$$

$$x \longmapsto x$$

If we denote $\alpha_i = \phi(\overline{X_i})$ for each $i = 1, \ldots, n$, then, for all $g(X) \in \mathfrak{m}$, we get

$$0 = \phi(\overline{0}) = \phi(\overline{g}) = g(\phi(\overline{X_1}), \ldots, \phi(\overline{X_n})) = g(\alpha_1, \ldots, \alpha_n).$$

Thus $(\alpha_1, \ldots, \alpha_n) \in \mathrm{V}(\mathfrak{m}) \subseteq \mathrm{V}(\Phi)$, a contradiction. Hence $I = k[X_1, \ldots, X_n]$, that is, $1 \in I$. □

Now we are ready to prove the normal form of Hilbert's Nullstellensatz Theorem

Theorem 4.4 (Hilbert's Nullstellensatz Theorem)**.** *Let k be a field, Φ be a subset of polynomial ring $k[X_1, X_2, \ldots, X_n]$. Given $P(X_1, \ldots, X_n) \in k[X_1, X_2, \ldots, X_n]$, if $P(X_1, \ldots, X_n)$ vanishes on $\mathrm{V}(\langle\Phi\rangle)$, then there is $r > 0$ such that $P(X_1, \ldots, X_n)^r \in \langle\Phi\rangle$. Moreover, denoting $I = \langle\Phi\rangle$, then*

$$\sqrt{I} = \mathcal{I}(\mathrm{V}(I)).$$

Proof: Let $P(X_1, \ldots, X_n)$ be a polynomial which vanishes on the algebraic set $\mathrm{V}(\Phi)$, that is, $P(X_1, \ldots, X_n) \in \mathcal{I}(\mathrm{V}(I))$. Consider the polynomial ring $k[X_1, \ldots, X_n, Y]$ and $\Phi' = \Phi \cup \{1 - Y * P(X_1, \ldots, X_n)\}$. Since, $k[X_1, \ldots, X_n] \subseteq k[X_1, \ldots, X_n, Y]$, we have that $\Phi' \subseteq k[X_1, \ldots, X_n, Y]$. It's clear that $\mathrm{V}(\phi') = \varnothing$. Thus, by Weak Hilbert's Nullstellensatz Theorem, we have that $1 \in \langle\Phi\rangle$. Hence there are $G_1, \ldots, G_m \in \Phi$, $H, H_1, \ldots, H_m \in k[X_1, \ldots, X_n, Y]$ such that

$$H_1(X_1, \ldots, X_n, Y)G_1 + \cdots + H_m(X_1, \ldots, X_n, Y)G_m + H(1 - YP(X_1, \ldots, X_n)) = 1.$$

This is an algebraic expression. Switching Y by $1/P(X_1, \ldots, X_n)$, we obtain

$$H_1(X_1, \ldots, X_n, 1/P(X_1, \ldots, X_n))G_1 + \cdots + H_m(X_1, \ldots, X_n, 1/P(X_1, \ldots, X_n))G_m = 1.$$

Thus, multiplying the previous equation by $P(X_1, \ldots, X_n)^r$ for r sufficiently larger, we can write

$$\overline{H_1}(X_1, \ldots, X_n)G_1 + \cdots + \overline{H_m}(X_1, \ldots, X_n)G_m = P(X_1, \ldots, X_m)^r.$$

That is, $P(X_1, \ldots, X_n) \in \sqrt{I}$.

Moreover, given $P(X_1, \ldots, X_n) \in \sqrt{I}$, then $P^m \in I$ for some $m \in \mathbb{N}$. Then there are $G_1, \ldots, G_t \in I$ and $H_1, \ldots, H_t \in k[X_1, \ldots, X_n]$ such that P^m

$$G_1H_1 + \cdots + G_tH_t = P^m.$$

Thus, clearly we have that $P \in \mathcal{I}(\mathrm{V}(I))$. □

Using the Zariski's Lemma and the following Lemma, we can prove two important and interesting results about polynomial rings over algebraically closed fields

Lemma 4.5. *Let k be a field and consider $R = k[X_1, \ldots, X_n]$ the polynomial ring over R in n variables. Given $(r_1, \ldots, r_n) \in k^n$, the ideal $(X_1 - r_1, \ldots, X_n - r_n)$ is a maximal ideal of R.*

Proof: Consider the ring homomorphism

$$\phi : k[X_1, \ldots, X_n] \longrightarrow k$$

$$P(X_1, \ldots, X_n) \longmapsto P(r_1, \ldots, r_n)$$

Observe that ϕ is a surjective ring homomorphism, thus by, First Isomorphism Theorem, $\ker(\phi)$ is a maximal ideal of $k[X_1,\ldots,X_n]$. It's easy to see that $I := (X_1-r_1,\ldots,X_n-r_n) \subseteq \ker(\phi)$. Then it's enough to prove that $\ker(\phi) \subseteq I$. Let $P(X_1,\ldots,X_n) \in \ker(\phi)$ and write

$$P(X_1,\ldots,X_n) = \sum_{J=(i_1,\ldots,i_n)} a_J X_1^{i_1}\ldots X_n^{i_n}$$

It's clear that $\overline{X_i} = \overline{r_i}$ for each $i = 1,\ldots,n$ in R/I. Then it's easy to see that

$$\overline{P(X_1,\ldots,X_n)} = \overline{\sum_{J=(i_1,\ldots,i_n)} a_J X_1^{i_1}\ldots X_n^{i_n}} = \overline{\sum_{J=(i_1,\ldots,i_n)} a_J r_1^{i_1}\ldots r_n^{i_n}} = \overline{P(r_1,\ldots,r_n)}$$

Then, if $P(X_1,\ldots,X_n) \in \ker(\phi)$, we have that

$$\overline{P(X_1,\ldots,X_n)} = \overline{P(r_1,\ldots,r_n)} = \overline{0} \text{ in } R/I$$

This means that $P(X_1,\ldots,X_n) \in I$ and, so we conclude that $\ker(\phi) \subseteq I$. Hence $I = \ker(\phi)$ is a maximal ideal of R. □

Proposition 4.6. *Let Ω be an algebraically closed field and $\mathfrak{m}$ be maximal ideal of the polynomial ring $\Omega[X_1,\ldots,X_n]$. Then there is an ordered n−tuple $(\alpha_1,\ldots,\alpha_n) \in \Omega^n$ such that*

$$\mathfrak{m} = (X_1-\alpha_1,\ldots,X_n-\alpha_n).$$

Proof: Indeed, let $\mathfrak{m}$ be a maximal ideal of $\Omega[X_1,\ldots,X_n]$. Consider the field $K = \Omega[X_1,\ldots,X_n]/\mathfrak{m}$. Since K is a finitely generated Ω-algebra, K is an algebraic extension of Ω by Zariski's Lemma. As Ω is an algebraically closed field, we have that $\Omega = K$. This fact implies that each X_i is congruent mudulo $\mathfrak{m}$ to some $\alpha_i \in \Omega$, that is, $X_i - \alpha_i \in \mathfrak{m}$ for each $i = 1,\ldots,n$. Thus

$$(X_1-\alpha_1,\ldots,X_n-\alpha_n) \subseteq \mathfrak{m}$$

Since $(X_1-\alpha_1,\ldots,X_n-\alpha_n)$ is already a maximal ideal, we conclude that

$$(X_1-\alpha_1,\ldots,X_n-\alpha_n) = \mathfrak{m}.$$

□

Corollary 4.7. *Let Ω be an algebraically closed field. Then there is a one-to-one correspondence between the maximal ideals of $\Omega[X_1,\ldots,X_n]$ and Ω^n given by the following map*

$$\phi : \Omega^n \longrightarrow \operatorname{MaxSpec}(k[X_1,\ldots,X_n])$$

$$(\alpha_1,\ldots,\alpha_n) \longmapsto (X_1-\alpha_1,\ldots,X_n-\alpha_n)$$

Proof: it's immediate consequence of Lemma 4.5 and Proposition 4.6. □