國立臺灣大學理學院數學系
碩士論文
Department of Mathematics
College of Science
National Taiwan University
Master Thesis

關於零點定理的一些討論
On Nullstellensatz

研究生: 石勝吉
Student: SHENG - CHI, SHIH

指導教授: 朱樺 教授
Advisor: HUAH, CHU

中華民國九十七年六月
June, 2008

1

摘要

在第三節中, 我們給了兩個比較基本的零點定理的証明。在第四節中, 我們討論了不同形式的零點定理的相互關係, 並且我們也給了一些不同形式的零點定理的不同的証明。Alon 是組合的零點定理的主創者, 這個定理可以可以用來證明另一個定理 (定理 13) 並且在組合學和數輪上有很多的應用。在本篇論文中, 我們用另外一個觀點來證明此定理並將它推廣 (定理 12)。在例子 14 和例子 15 中, 我們也給了一些應用。

關鍵字: 零點定理, Gröbner 基底, 組合的零點定理, 零點定理的証明, 不同形式的零點定理

Abstract

In Section 4 we give two elementary proofs of Nullstellensatz. The first is due to Enrique Arrondo which is more brief. The second is due to Terrance Tao which is constructive. In Section 5 we will discuss different proofs of above theorems. The first is above three forms which are equivalent. The second we give two different proofs of strong form. The third we give four different proofs of field form.

Alon is the principal founder of the Combinatorial Nullstellensatz. This theorem can prove another theorem (see Theorem 13) which has many applications in combinatorics and number theory. In this paper we will give another view point to this proof and generalize this theorem (see Theorem 12). We also give some applications in Example 14 and Example 15.

Key words: Nullstellensatz, Combinatorial Nullstellensatz, Gröbner bases, different forms of Nullstellensatz, proofs of Nullstellensatz

Contents

1 Introduction

Gauss' fundamental theorem of algebra establish the basic link between algebra and geometry: It says that a polynomial in one variable over $\mathbb{C}$, an algebra object, is determined up to a scalar factor by the set of its roots, a geometry. Hilbert's Nullstellensatz (German: "Theorem of Zeros") extends this link to certain ideals of polynomial in many variables. Given an ideal I of a polynomial ring $F[X_1, \cdots, X_n]$, we define a corresponding algebra set of F^n to be

$$V(I) = \{(a_1, \cdots, a_n) \in F^n | f(a_1, \cdots, a_n) = 0, \forall f \in I\}.$$

Given a subset V of F^n, we also define a corresponding ideal of a polynomial ring to be

$$I(V) = \{f \in F[X_1, \cdots, X_n] | f(a) = 0, \forall a \in V\}.$$

Now we state the Hilbert's Nullstellensatz as follows:

Theorem 1. (*Strong form*)*Let L be an algebraically closed field. The assignment $V \to I(V)$ defines a bijection of the set of all L varieties $V \subset \mathbb{A}^n(L)$ onto the set of all ideals I of $L[X_1, \cdots, X_n]$ with $Rad(I) = I$. For any ideal I of $L[X_1, \cdots, X_n]$,*

$$Rad(I) = I(V(I)).$$

Nullstellensatz has another three different forms stated as follows:

Theorem 2. (*Weak form I*)[6][7] *Let L be an algebraically closed field. For an ideal I of $L[X_1, \cdots, X_n]$. If $I \neq L[X_1, \cdots, X_n]$, then $V(I)$ is not empty.*

Theorem 3. (*Field form*) *If A/F is an extension of field and A arises from F through ring adjunction of finite many elements, then A/F is an algebraic extension.*

Theorem 4. (*Weak form II*) *Let L be an algebraically closed field. For any maximal ideal M of $L[X_1, \cdots, X_n]$ there exist $a_1, \cdots, a_n$ in L such that*

$$M = (X_1 - a_1, \cdots, X_n - a_n).$$

In Section 4 we give two elementary proofs of Nullstellensatz. The first is due to Enrique Arrondo which is more brief. The second is due to Terrance Tao which is constructive. In Section 5 we will discuss different proofs of above theorems. The first is above three forms which are equivalent. The second we give two different proofs of strong form. The third we give four different proofs of field form.

Alon is the principal founder of the Combinatorial Nullstellensatz which has many applications in combinatorics and number theory. The theorem stated as follows:

Theorem 5. [1] *Let F be an arbitrary field, and let f be a polynomial in $F[X_1, \cdots, X_n]$. Let $S_1, \cdots, S_n$ be nonempty subset of F and let $S = S_1 \times \cdots \times S_n$. we define $g_i = \prod_{s \in S_i} (X_i - s)$. If $f(s) = 0$ for all s in S, then there are $h_1, \cdots, h_n$ in $F[X_1, \cdots, X_n]$ satisfing $\deg(h_i) \leq \deg(f) - \deg(g_i)$ such that*

$$f = \sum_{i=1}^{n} h_i g_i.$$

As a consequence of the above one can prove another theorem (see Corollary 13) which has many applications. In this paper we will give another view point to this proof and generalize this theorem (see Theorem 12). We also give some applications in Example 14 and Example 15.

2 Preliminaries on Gröbner bases

In this section we introduce some concepts about Gröbner bases, and all the material, except Lemma 10 are referred from [4 ,chapter 2].

Definition 6. *Let F be a field and $R = F[x_1, \cdots, X_n]$ be the polynomial ring over F.*

(1) *A monomial order $>$ in R is a totally order on monomial ideal in R satisfies the following properties:*

(i) *If $X^\alpha > X^\beta$, then $X^{\alpha+\gamma} > X^{\beta+\gamma}$ for all γ in $\mathbb{Z}^n_{\geq 0}$*

(ii) *$>$ is a well-ordering on monomials.*

(2) *A monomial order* $>_{gr}$ *is called graded if it satisfies*

$$X^{\alpha} >_{gr} X^{\beta} \Leftrightarrow |\alpha| > |\beta| \text{ or } |\alpha| = |\beta| \text{ and } \alpha > \beta$$

for some monomial order $>$.

(3) *The leading monomial of* f *is denoted by* $LM(f)$*, note that the coefficient of* $LM(f)$ *may not be* 1.

(4) *We note that* $R = k[X_1, \cdots, X_n]$ *can be regard as a graded ring graded by total degree, so for any* f *in* R, $f = f_0 + f_1 + \cdots + f_n$, $\deg f_i = i$ *and* $f_n \neq 0$. *We said that the leading term,* $LT(f)$*, of* f *is* f_n. *Note that* f_n *may not be a monomial.*

We introduce some notions of Grönber bases.

Definition 7. (1) *Fix a monomial order. A finite subset* $G = \{g_1, \cdots, g_s\}$ *of an ideal* I *is called a Gröbner basis if* $\langle LM(g_1), \cdots, LM(g_s)\rangle = \langle LM(I)\rangle$*, where* $LM(I)$ *means the set of leading monomial of element of* I.

(2) *Fix a monomial order and let* $G = \{g_1, \cdots, g_s\}$ *be a subset of* $k[X_1, \cdots, X_n]$. *Given* f *in* $k[X_1, \cdots, X_n]$*, we say that* f *reduces to zero modulo* G*, written*

$$f \to_G 0,$$

if f *can be written in the form*

$$f = a_1 g_1 + \cdots a_s g_s,$$

such that whenever $a_i g_i \neq 0$*, we have*

$$multideg\,(f) \geq multideg\,(a_i g_i).$$

There is a well-known criterion for deciding whether a generating set of deal is Gröbner basis, and the following is the criterion:

Proposition 8. *A basis* $G = \{g_1, \cdots, g_s\}$ *for an ideal* I *is a Gröbner basis if and only if* $S(g_i, g_i) \to_G 0$ *for all* $i \neq j$.

Lemma 9. *Let* G *be a finite subset of* $F[X_1, \cdots, X_n]$*, suppose that we have* f, g *in* G *such that the leading monomial of* f *and* g *are relatively prime. Then* $S(f, g) \to_G 0$.

Proof. Write $f = LM(f) + p,\ g = LM(g) + q$. Since $\text{LCM}(LM(f), LM(g)) = LM(f) \cdot LM(g)$, we have

$$\begin{aligned} S(f,g) &= LM(g) \cdot f - LM(f) \cdot g \\ &= (g-q) \cdot f - (f-p) \cdot g \\ &= g \cdot f - q \cdot f - f \cdot g + p \cdot g \\ &= p \cdot g - q \cdot f. \end{aligned}$$

We claim that

$$\text{multideg}(S(f,g)) = \max(\text{multideg}(p \cdot g),\ \text{multideg}(q \cdot f)).$$

Assume the claim holds, then by Definition 7.(2) $S(f,g) \to_G 0$. To prove the claim, we show that the leading monomial of $p \cdot g$ and $q \cdot f$ are distinct . For if the leading monomial are the same, we would have

$$LM(p) \cdot LM(g) = LM(f) \cdot LM(q).$$

Since $LM(g)$ and $LM(f)$ are relative prime, $LM(g)$ divide $LM(q)$ which is impossible because $g = LM(g) + q$. Hence leading monomial of $p \cdot g$ and $q \cdot f$ can not be canceled. □

Next we generalize the above lemma as follows:

Lemma 10. *Let G be a finite subset of $k[X_1, \cdots, X_n]$ and for f, g in G write $f = h \cdot p$ and $g = h \cdot q$, where $h = LCM(f,g)$. Suppose the leading monomial of p and q are relatively prime. Then $S(f,g) \to_G 0$.*

Proof. Write $p = LM(p) + p_1$ and $q = LM(q) + q_1$, then

$$\begin{aligned}
S(f,g) &= LM(q)\cdot f - LM(p)\cdot g \\
&= LM(q)\cdot p\cdot h - LM(p)\cdot q\cdot h \\
&= h(LM(q)\cdot p - LM(p)\cdot q) \\
&= h(LM(q)\cdot (LM(p)+p_1) - LM(p)\cdot (LM(q)+q_1)) \\
&= h\{LM(q)\cdot LM(p) + LM(q)\cdot p_1 - LM(p)\cdot LM(q) + LM(p)\cdot q_1\} \\
&= h(LM(q)\cdot p_1 - LM(p)\cdot q_1) \\
&= h(LM(q)\cdot p_1 - LM(p)\cdot q_1 + p_1\cdot q_1 - p_1\cdot q_1) \\
&= h((LM(q)+q_1)\cdot p_1 - (LM(p)+p_1)\cdot q_1) \\
&= h\cdot q\cdot p_1 - h\cdot p\cdot q_1 \\
&= g\cdot p_1 - f\cdot q_1.
\end{aligned}$$

We claim that

$$\text{multideg}(S(f,g)) = \max(\text{multideg}(g\cdot p_1),\ \text{multideg}(f\cdot q_1)).$$

Assume the claim holds, then by Definition 7.(2) $S(f,g) \to_G 0$. To prove the claim, we show that the leading monomial of $g\cdot p_1$ and $f\cdot q_1$ are distinct. For if the leading monomial are the same, we would have

$$LM(q)\cdot LM(p_1) = LM(p)\cdot LM(q_1).$$

Since $LM(p)$ and $LM(q)$ are relative prime, $LM(q)$ divide $LM(q_1)$ which is impossible because $q = LM(q) + q_1$. Hence the leading monomial of $g\cdot p_1$ and $f\cdot q_1$ cannot cancel. □

Lemma 11. *Fix a monomial order $>$ on R, and let $F = (f_1, \cdots, f_s)$ be an ordered $s-$tuple of polynomials in $F[X_1, \cdots, X_n]$. Then every f in $k[X_1, \cdots, X_n]$ can be written as*

$$f = a_1 f_1 + \cdots a_s f_s + r.$$

where a_i, r *in* $F[X_1, \cdots, X_n]$, *and either* $r = 0$ *or all monomials of* r *are not divided by any of* $LM(f_1), \cdots, LM(f_s)$. *Furthermore, if* $a_i f_i \neq 0$, *then we have*

$$multideg\,(f) \geq multideg\,(a_i f_i).$$

3 Main theorem

Recall that for a polynomial f, the leading term of f, $LT(f)$, is in the sense of definition 6.(4).

Theorem 12. *Given a polynomial* f *in* $F[X_1, \cdots, X_n]$, *where* F *is an arbitrary field, and a variety* V *in* F^n*with finite cardinality. Let* $I(V) = \langle g_1, \cdots, g_s \rangle$, *where* g_i *is in* $F[X_1, \cdots, X_n]$ *and* $\{g_1, \cdots, g_s\}$ *is a Gröbner basis under some graded monomial order. Assume* $LT(g_i)$ *is a monomial for all* i. *If* $LT(f)$ *contains a monomial which is not divisible by* $LT(g_i)$ *for all* i, *then* f *is not lie in* $I(V)$.

Proof. Suppose f is in $I(V)$, then $f = h_1 g_1 + \cdots + h_s g_s$ where h_i is in $F[X_1, \cdots, X_n]$ and by Lemma 11 we have

$$\text{multideg}\,(f) \geq \text{multideg}\,(h_i g_i).$$

This implies $\deg f \geq \deg h_i g_i$ for all i. Let $h_i = h_{i,0} + h_{i,1} + \cdots + h_{i,i_m}$ and $g_i = g_{i,0} + g_{i,1} + \cdots + g_{i,i_t}$, where $\deg g_{i,k} = k$ and $\deg h_{i,j} = j$ for $i = 1, 2, \cdots, s$. We denote the monomial of $LT(f)$ which is not divided by $LT(g_i)$ for all i by P. Then P occur in $h_i g_i$ for some i. Observing that if P occur in $h_{i,i_k} g_{i,i_j}$, for some $i_j < i_t$. Then $\deg P < \deg(h_{i,i_m} g_{i,i_t}) \leq \deg f$. This contradicts to that P is in $LT(f)$. Hence P occur in $h_{i,i_k} g_{i,i_m}$, then P is divided by $LT(g_i)$. this contradicts to that P is not divided by $LT(g_j)$ for all j. Therefore f is not in $I(V)$. □

As a corollary we proof the theorem due to Alon.

Corollary 13. [1] *Let* F *be an arbitrary field, and let* $S_1, \cdots, S_n$ *be nonempty subset of* F. *Let* f *be a polynomial in* $F[X_1, \cdots, X_n]$. *Suppose there exists a monomial in the* $LT(f)$ *say* $\prod_{i=1}^{n} X_i^{t_i}$ *such that* $|S_i| > t_i$ *for each* i, *then there exists* s *in* $V = S_1 \times \cdots \times S_n$ *such that* $f(s) \neq 0$.

Proof. Suppose $f(s) = 0$ for all s in S, then f is in $I(V)$. For $i = 1, \cdots, n$ let

$$g_i := \prod_{s \in S_i} (X_i - s).$$

By Proposition 8 and Lemma 9 $\{g_1, \cdots, g_n\}$ is a Gröbner basis. Since $|S_i|$ are grater than t_i for all i, Theorem 12 implies that f is not in $I(V)$, contradicts to that f is in $I(V)$. Therefore there exists s in V such that $f(s) \neq 0$. □

Alon just consider the case that V is a "rectangle". We will generalize this result to the case, which V is not a rectangle, but eliminate a subrectangle from a rectangle.

Example 14. *Let F be an arbitrary field, $S_1, \cdots, S_n$ be nonempty subset of F, $U_1, \cdots, U_n$ are subsets of $S_1, \cdots, S_n$ respectively. Consider a variety $V = S_1 \times \cdots \times S_n - U_1 \times \cdots \times U_n$. Let f be a polynomial in $F[X_1, \cdots, X_n]$. Suppose there exists a monomial in the $LT(f)$ say $\prod_{i=1}^{n} X_i^{t_i}$ such that $|S_i| > t_i$ for each i and there exists i such that $|S_i| - |U_i| > t_i$, then there exists s in S such that $F(s) \neq 0$.*

Proof. Let

$$I(V) = \langle \Pi_{s \in S_1}(X_1 - s), \Pi_{s \in S_2}(X_2 - s), \cdots, \Pi_{s \in S_n}(X_n - s), \Pi_{i=1}^{n} \Pi_{s \in S_i - U_i}(X_i - s) \rangle.$$

Using Proposition 8, Lemma 9 and Lemma 10 this generating set is a Gröbner basis. Since $|S_i|$ are greater than t_i for each i and there exists i such that $|S_i| - |U_i|$ is greater t_i, $\prod_{i=1}^{n} X_i^{t_i}$ is not divided by all of the leading terms of generators. Then Theorem 12 implies f is not lies in $I(V)$. In other words, there exists s in V such that $f(s) \neq 0$. □

Furthermore, we can also apply the theorem to the case of S being a "triangular".

Example 15. *Let F be an arbitrary field, $S = \{a_1, \cdots, a_n\}$ be a nonempty subset of F, and $S_1 \supseteq S_2 \supseteq \cdots \supseteq S_n$ also be nonempty subsets of F. Let f be a polynomial in $F[X_1, X_2]$ and let $V = \{(a_i, b) | a_i \in S, b \in S_i\}$. Suppose there exists a monomial in the $LT(f)$, say $X^{t_1} Y^{t_2}$ such that $t_1 < n$, $t_2 < |S_{t_1+1}|$ for all i, then there exist (a_i, b) in V such that $f(a_i, b) \neq 0$.*

Proof. Suppose $f(a_i, b) = 0$ for all (a_i, b) in V. Let

$$I(V) = \langle \prod_{s\in S_1}(y-s), (x-a_1)\prod_{s\in S_2}(y-s), \cdots, \prod_{i=1}^{n-1}(x-a_i)\prod_{s\in S_n}(y-s), \prod_{i=1}^{n}(x-a_i).\rangle$$

Using Proposition 8, Lemma 9 and Lemma 10 this generating set is a Gröbner basis. Since $t_1 < |S|$, $t_2 < |S_{t_1+1}|$ for all i, $X^{t_1}Y^{t_2}$ is not divided by all of the leading terms of generators. Then Theorem 12 implies f is not lies in $I(V)$. In other words, there exists s in V such that $f(s) \neq 0$. □

For example let $S = \{1, 2, 3, 4\}$, $S_1 = \{1, 2, 3, 4\} \supset S_2 = \{1, 2\} \supset S_3 = \{1\} = S_4$ and let $f(X, Y) = X^3 - 2X^2Y + Y^3$. Clearly f satisfies the condition of Example 15 and we have $f(1, 2) \neq 0$.

4 Elementary proofs of Nullstellensatz

The first proof of weak form of Nullstellensatz which is given by Arrondo.

Theorem 16. *Let I be a proper ideal of $L[X_1, \cdots, X_n]$. If L is an algebraically closed field, then $V(I)$ is nonempty.*

Proof. [2] If $I = 0$, then nothing to prove. So we may assume $I \neq 0$. We prove the theorem by induction on n. For the case $n = 1$, any non-zero ideal I of $L[X]$ is generated by a non-constant polynomial. Because L is a algebraically closed field, every generator of I has some root a in L. Therefore $f(a) = 0$ for all f in I.

We assume $n > 1$ and the theorem proved for the case $n - 1$. We claim that I contains a polynomial g which is monic in the variable X_n. To prove claim, given any polynomial f with degree d in I. Let f_d be the homogeneous component of f of degree d, then the coefficient of X_n^d in $f(X_1 + \lambda_1 X_n, \cdots, X_{n-1} + \lambda_{n-1}X_n, X_n)$ is $f_d(\lambda_1, \cdots, \lambda_{n-1}, 1)$. Since $f_d(X_1, \cdots, X_{n-1}, 1)$ is a non-zero polynomial in $L[X_1, \cdots, X_{n-1}]$ and L is infinite, there is a point $(\lambda_1, \cdots, \lambda_{n-1})$ in L^{n-1} such that $f_d(\lambda_1, \cdots, \lambda_{n-1}, 1)$ is non-zero. This proves the claim.

By claim after change of coordinates and scaling, we may assume that I contains a polynomial g which is monic in the variable X_n. Fixing such a polynomial

g, we consider the ideal $I' = \{f \in I | f \in L[X_1, \cdots, X_{n-1}]\}$ of $L[X_1, \cdots, X_{n-1}]$. Since 1 is not in I, I' is a proper ideal. Therefore, by induction hypothesis there is a point$(a_1, \cdots, a_{n-1})$ such that $h(a_1, \cdots, a_{n-1})$ for all h in I'. We now claim that the set $J = \{f(a_1, \cdots, a_{n-1}, X_n) | f \in I\}$ is a proper ideal of $L[X_n]$.

Now we show that J is an ideal of $L[X_n]$. Consider a homomorphism map $\varphi : L[X_1, \cdots, X_n] \to L[X_n]$ defined by $\varphi f(X_1, \cdots, X_n) = f(a_1, \cdots, a_{n-1}, X_n)$. For any h in $L[X_n]$ and any f in I, $\varphi^{-1}(hf(a_1, \cdots, a_{n-1}, X_n))$ in I. Hence $hf(a_1, \cdots, a_{n-1}, X_n)$ is in J. There J is an ideal of I

Now we show that J is a proper ideal of $L[X_n]$. Suppose to the contrary that there exists f in I such that $f(a_1, \cdots, a_{n-1}, X_n) = 1$. Thus we can write $f = f_0 + f_1 X_n + \cdots + f_d X_n^d$, with all the f_i in $L[X_1, \cdots, X_{n-1}]$,

$$f_1(a_1, \cdots, a_{n-1}) = \cdots = f_d(a_1, \cdots, a_{n-1}) = 0, \text{ and } f_0(a_1, \cdots, a_{n-1}) = 1. \qquad (*)$$

On the other hand, we can express the monic polynomial g in the form $g = g_0 + g_1 X_n + \cdots + g_{e-1} X_n^{e-1} + X_n^e$ with g_j in $L[X_1, \cdots, X_{n-1}]$ for $j = 1, \cdots, e-1$.

Let R be the resultant of f and g with respect to the variable X_n. In other words, R is the polynomial in $L[X_1, \cdots, X_{n-1}]$ given by the determinant

$$R = \begin{vmatrix} f_0 & f_1 & \cdots & f_d & 0 & 0 & 0 & 0 \\ 0 & f_0 & \cdots & f_{d-1} & 0 & 0 & \cdots & 0 \\ & & \ddots & & & & & \\ 0 & \cdots & 0 & f_0 & f_1 & \cdots & f_{d-1} & f_d \\ g_0 & g_1 & \cdots & g_{e-1} & 1 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{e-1} & 1 & \cdots & 0 \\ & & \ddots & & & & & \\ 0 & \cdots & 0 & g_0 & g_1 & \cdots & g_{e-1} & 1 \end{vmatrix}$$

which has $e + d$ rows. It is then well known that R is a linear combination of f and g and hence belongs to I. Therefore R is a member of I'. But direct inspection of determinant defining the resultant shows that, when we use (*) to evaluate R at $(a_1, \cdots, a_{n-1})$, it reduces to the determinant of lower-triangular

matrix whose entries on its main diagonal are all $1's$. Hence $R(a_1, \cdots, a_{n-1}) = 1$, which contradicts the fact that R is in I'. This proves the claim.

Therefore J is a proper ideal of $L[X_n]$, and since $L[X_n]$ is a principle ideal domain, J is generated either by polynomial $h(X_n)$ of positive degree or by $h = 0$. Since L is algebraically closed field, in the former case h has at least one root a_n in L. In either case this means that $f(a_1, \cdots, a_{n-1}, a_n) = 0$ for all f in I, which completes the proof. □

The second proof of strong form of Nullstellensatz which is given by Tao.

Theorem 17. *Let $P_1, P_2, \cdots, P_m, R \in L[X_1, X_2, \cdots, X_d] = L[X]$, where L is an algebraically closed field. Then the pair $(P_1, P_2, \cdots, P_m; R)$ satisfies exactly one of the following statements :*

(a) There exists $x \in L^d$ such that $P_1(x) = P_2(x) = \cdots = P_m(x) = 0, R(x) \neq 0$.

(b) There exists $Q_1, Q_2, \cdots, Q_m \in L[X]$ such that $P_1Q_1 + \cdots + P_mQ_m = R^r$ for some non-negative integer r.

Proof. [9] We proved by induction on d.

Step 1.: $d = 1$

Step 1.1.: Reduce to the case $m = 1$

Let $\gcd(P_1, \cdots .P_m) = D$, then there exists $U_1 \cdots, U_m \in L[X]$ such that

$$U_1P_1 + \cdots + U_mP_m = D. \tag{1}$$

We claim that $(P_1, \cdots, P_m; R)$ satisfies theorem if and only if $(D; R)$ satisfies the theorem.

Suppose $(P_1, \cdots, P_m; R)$ satisfies (a), then there exists $x \in F$ such that $P_1(x) = P_2(x) = \cdots = P_m(x) = 0, R(x) \neq 0$. Hence $D(x) = 0, R(x) \neq 0$ this implies $(D; R)$ satisfies (a). Suppose $(P_1, \cdots, P_m; R)$ satisfies (b), then there exist $Q_1, Q_2, \cdots, Q_m \in L[X]$ such that $P_1Q_1 + \cdots + P_mQ_m = R^r$ for some non-negative integer r. Let $P_i = V_i \cdot D$ for all $i = 1, \cdots, m$. So $R^r = P_1Q_1 + \cdots + P_mQ_m = D(V_1Q_1 + \cdots + V_mQ_m)$ and hence $(D; R)$ satisfies (b). Conversely, Suppose $(D; R)$ satisfies (a), then there exists $x \in L$ such that $D(x) = 0, R(x) \neq 0$. Since $D|P_i$,

$P_i(x) = 0$, for all $i = 1, \cdots, m$. Then $(P_1, \cdots, P_m; R)$ satisfies (a). Suppose $(D; R)$ satisfies (b), then there exists $Q \in L[X]$ such that $QD = R^r$ for some non-negative integer r. From (1) we have $(QU_1)P_1 + \cdots + (QU_m)P_m = QD = R^r$. Then $(P_1, \cdots, P_m; R)$ satisfies (b) and hence we proved the claim.

Step 1.2.:

So we have effectively reduced to the case $m = 1$. We will prove that the pair $(D; R)$ satisfies either (a) or (b) by induction on $\min\{\deg D,\ \deg R\}$. Let $\gcd(D, R) = D'$, then

$$D = D' \cdot S \ \text{ and } \ R = D' \cdot T \quad \text{ for some S}, T \in L[X].$$

On the other hand,

$$D' = DA + RB \quad \text{for some } A, B \in L[X].$$

Then $AS + BT = 1$. Clearly $D(X) = 0; R(X) \neq 0$ has a solution if and only if $S(X) = 0; R(X) \neq 0$ has a solution. Suppose $D'^r = QS$ for some is non-negative integer r and $Q \in L[X]$. Then

$$R^{r+1} = T^{r+1}D'^{r+1} = Q \cdot S \cdot T^{r+1} \cdot D' = D \cdot Q'. \tag{2}$$

Thus we see that if $(S; D')$ satisfies the theorem, then $(D; R)$ does also.

Now we have $\deg S \leq \deg D$ and $\deg D' \leq \deg R$. Suppose $\deg S = \deg D$, then $\deg D' = 0$. Since D' and R are relative prime, there exists $x \in F$ such that $D(x) = 0; R(x) \neq 0$. Thus $(D; R)$ satisfies (a). Suppose $\deg D' = \deg R$, then $D' = R$ and hence $D = R \cdot S$. If for all x in F with $D(x) = 0$ such that $R(x) = 0$, then $cD = R$ for some constant c. Thus $(D; R)$ satisfies (b). Hence there exists x in F with $D(x) = 0$ such that $R(x) \neq 0$. Then $(D; R)$ satisfies (a). Therefore we may assume $\min\{\deg D,\ \deg R\} < \min\{\deg S,\ \deg D'\}$. By induction, we can reduce to $\min\{\deg\ D, \deg\ R\} = 0$. Suppose D is zero. Since F is a infinity field, F is an infinity field. Then there exists a in L such that $R(a) \neq 0$ and hence $(D; R)$ satisfies (a). If D is a non-zero constant, then $\frac{R}{D} \cdot D = r$ and hence $(D; R)$ satisfies (b). Suppose D is not a constant. In this case, R is a constant. If $R = 0$,

then $0 \cdot D = 0$. Thus $(D; R)$ satisfies (b). If R is a non-zero constant. Since F is a algebraically closed field, D has at least one root. Then $(D; R)$ satisfies (a). Hence we proved the theorem for the case $d = 1$.

Step 2.: $d \geq 2$

Assume the theorem has been proved for $d-1$. Consider $P_i(X), R(X) \in L[\mathbf{X}][X_d]$, where $\mathbf{X} = (X_1, \cdots, X_{d-1})$. For any $y \in L^{d-1}, P_i(y, X_d), R(y, X_d) \in L[X_d]$. Suppose the equations

$$P_1(y, X_d) = \cdots = P_m(y, X_d) = 0, R(y, X_d) \neq 0$$

have no common solutions. By the case for $d = 1$ there exists $Q_1, \cdots, Q_m \in F[X_d]$ such that

$$P_1(y, X_d)Q_{1,y}(X_d) + \cdots + P_m(y, X_d)Q_{m,y}(X_d) = R(y, X_d)^{r_y} \tag{3}$$

for some $r^y \geq 0$. Note that $Q_{i,y}$ and r_y are depend on y.

Observing (2) in our argument for the case $d = 1$, we have r_y is uniform bounded in y (which has upper bounded $\max\{\deg_{x_d} D, \deg_{X_d} R\}$). So we can always multiply both side of (3) by suitable power of $R_y(X_d)$, and make $r = r_y$ is independent of y. Thus we get a equation

$$P_1(y, X_d)Q_{1,y}(X_d) + \cdots + P_m(y, X_d)Q_{m,y}(X_d) = R(y, X_d)^r$$

We will use an example to illustrate how to find the polynomial $Q_{i,y}$ by explicitly construct.

Example: Let $m = 2, R = 1$ and $P_{1,y}(t) = a(y) + b(y)t, P_{2,y}(t) = c(y) + d(y)(t)$. To find the $\gcd(P_{1,y}(t), P_{2,y}(t))$ for a given y.

Case 1: $b(y) = 0$

If $a(y) = c(y) = d(y) = 0$, then $\gcd(P_{1,y}(t), P_{2,y}(t)) = 0$ and hence (a) holds.

If $a(y) = d(y) = 0, c(y) \neq 0$, then $\gcd(P_{1,y}(t), P_{2,y}(t)) = P_{1,y} + \frac{1}{c(y)}P_{2,y}(t) = 1$. We take $Q_1 = 1$ and $Q_2 = \frac{1}{c(y)}$, then (b) holds.

If $a(y) = 0, c(y) \neq 0, d(y) \neq 0$,then $\gcd(P_{1,y}(t), P_{2,y}(t)) = P_{1,y}(t) + \frac{1}{d(y)}P_{2,y}(t) = t + \frac{c(y)}{d(y)}$ and hence (a) holds.

If $a(y) \neq 0$, then $\gcd(P_{1,y}(t), P_{2,y}(t)) = \frac{1}{a(y)} P_{1,y}(t) + 0 \cdot P_{2,y}(t) = 1$. We take $Q_1 = \frac{1}{a(y)}$ and $Q_2 = 0$, then (b) holds.

Case 2: $b(y) \neq 0$

If $a(y)d(y) - b(y)c(y) \neq 0$, then $\gcd(P_{1,y}(t), P_{2,y}(t)) = \frac{d(y)}{a(y)d(y)-b(y)c(y)} P_{1,y}(t) - \frac{b(y)}{a(y)d(y)-b(y)c(y)} P_{2,y}(t) = 1$. We take $Q_1 = \frac{d(y)}{a(y)d(y)-b(y)c(y)}$ and $Q_2 = -\frac{b(y)}{a(y)d(y)-b(y)c(y)}$, then (b) holds.

If $a(y)d(y) - b(y)c(y) = 0$, then $\gcd(P_{1,y}(t), P_{2,y}(t)) = \frac{1}{d(y)} P_{1,y}(t) + 0 \cdot P_{2,y}(t) = \frac{a(y)}{d(y)} + t$ and hence (a) holds.

So we see that even in the rather simple case of solving two linear equation in one unknown, there is a moderately complicated branching tree involved. Nevertheless, there are only finitely many branching paths. For any fixed complete path, it is defined by some conditions, we denote them as

$$T_1(\mathbf{X}) \neq 0, \cdots, T_a(\mathbf{X}) \neq 0, S_1(\mathbf{X}) = 0, \cdots, S_b(\mathbf{X}) = 0.$$

$T_1(\mathbf{X}) \neq 0, \cdots, T_a(\mathbf{X}) \neq 0$ define an open set U and $S_1(\mathbf{X}) = 0, \cdots, S_b(\mathbf{X}) = 0$ define a closed set W in L^{d-1}. Then this path define a quasi-variety $V = U \cap W$ Note that V may be empty. Now we consider any fixed nonempty quasi-variety V The above example show that in the equation (3), for all y in V all $R_{i,y}$ are the same and the polynomial $Q_{i,y}$ are in fact piecewise rational in the sense that $Q_{i,y} \in L(\mathbf{X})[X_d]$. Thus we write $R_{i,j} = R_{i,V}$ and $Q_{i,y} = Q_{i,V} = Q(\mathbf{X}, X_d)$ in V and hence we may write the equation (3) as

$$P_1(\mathbf{X}, X_d)Q_1(\mathbf{X}, X_d) + \cdots + P_m(\mathbf{X}, X_d)Q_m(\mathbf{X}, X_d) = R(\mathbf{X}, X_d)^r$$

in V. Then the denominators of the coefficient of $Q(\mathbf{X}, X_d)$ are product of $T_1(\mathbf{X}), \cdots, T_a(\mathbf{X})$. We may thus clear denominators and get an identity

$$P_1(\mathbf{X}, X_d)U_1(\mathbf{X}, X_d) + \cdots + P_m(\mathbf{X}, X_d)U_m(\mathbf{X}, X_d) = (T_1(\mathbf{X}) \cdots T_a(\mathbf{X})R(\mathbf{X}, X_d))^r \tag{4}$$

for some $U_1, \cdots, U_m \in F[\mathbf{X}, X_d]$. Let

$$G = P_1(\mathbf{X}, X_d)U_1(\mathbf{X}, X_d) + \cdots + P_m(\mathbf{X}, X_d)U_m\mathbf{X}, X_d) - (T_1(\mathbf{X}) \cdots T_a(\mathbf{X})R(\mathbf{X}, X_d))^r.$$

Therefore (4) holds in W, by induction hypothesis G lies in $I(W) = \mathrm{rad}I(W)$. Then there exists nonnegative integer s such that $G^s \in (S_1, \cdots, S_n)$. Thus we have an equation

$$P_1(\mathbf{X}, X_d)U_1(\mathbf{X}, X_d) + \cdots + P_m(\mathbf{X}, X_d)U_m(\mathbf{X}, X_d) =$$

$$(T_1(\mathbf{X}) \cdots T_a(\mathbf{X})R(\mathbf{X}, X_d))^r + S_1(\mathbf{X}, X_d)V_1(\mathbf{X}, X_d) + \cdots + S_b(\mathbf{X}, X_d)V_b(\mathbf{X}, X_d). \quad (5)$$

for some $U_1, \cdots, U_m, V_1, \cdots, V_b \in L[\mathbf{X}, t]$.

Now We consider $L^{d-1} \supseteq V_1 \supseteq \cdots \supseteq V_l = V$ and fix a path such that V_l is nonempty. Note that for any V_i is defined by $T_1(\mathbf{X}) \neq 0, \cdots, T_a(\mathbf{X}) \neq 0, S_1(\mathbf{X}) = 0, \cdots, S_b(\mathbf{X}) = 0$ and the defining condition of V_{i+1} is more then one of V_i.

Now we inductive backward on the length of $a+b$ to show that we can eliminate conditions until conditions are empty and then we proved the theorem. In V_l we have known that it has a relation of the form (5). So we assume that the path is not complete say V_i. Hence there is another condition say $H\mathbf{X})$ and assume in V_j has relation (5) for all $j > i$. Then for any y in V either $H(y) = 0$ or $H(y) \neq 0$. Now we have three possibility and discuss in the following.

Case 1: Assume $H(y) = 0$ for all y in V. Then by inductive hypothesis, we have

$$P_1U_1 + \cdots + P_mU_m = (T_1 \cdots T_aR)^r + S_1V_1 + \cdots + S_bV_b + HV. \quad (6)$$

On the other hand

$$S_1(\mathbf{X}) = \cdots = S_b(\mathbf{X}) = 0; T_1 \cdots T_aH(\mathbf{X}) \neq 0$$

has no common solution. Since the nullstellensatz is assumed to hold for dimension $d-1$, there exists $G_1, \cdots, G_a$ such that

$$G_1S_1 + \cdots + G_aS_a = (T_1 \cdots T_bH)^{r'}$$

for some r'. Then we multiply (6) by $(T_1 \cdots T_bR)^{r'}$ to eliminate the role of H. Then we have a relation of the form (5).

Case 2: Assume $H(y) \neq 0$ for all y in V. Then we have

$$P_1U_1 + \cdots + P_mU_m = (T_1 \cdots T_aHR)^{r'} + S_1V_1 + \cdots + S_bV_b \quad (7)$$

On the other hand the equation

$$S_1(\mathbf{X}) = \cdots = S_b(\mathbf{X}) = H(\mathbf{X}) = 0; T_1 \cdots T_a(\mathbf{X}) \neq 0 \tag{8}$$

has no common solutions and so by nullstellensatz in dimension $d-1$ there exists $G_1, \cdots, G_a, Z$ such that

$$G_1 S_1 + \cdots + G_a S_a + HZ = (T_1 \cdots T_b W)^{r''}$$

for some r''. then we multiply (7) by $Z^{r'}$ and using (8) to eliminate H, we obtain the relation of the form (5).

Case 3: There exist y_1, y_2 in V such that $H(y_1) = 0$ and $H(y_2) \neq 0$. In this case we obtain relation of the form (6) and (7). Multiplying (6) by Z^r to eliminate H and we get a relation of the form (5).

The above induction show that we can elimination conditions until condition is empty and hence we find $Q_1, Q_2, \cdots, Q_m$ are in $F[X]$ such that

$$P_1 Q_1 + \cdots + P_m Q_m = R^r$$

for some non-negative integer r. □

5 Different forms of Nullstellensatz

In this section we discuss various proofs of the Nullstellensatz. First we show that weak form I, II and field form are equivalent.

Theorem 18. [8] *Let L be a algebraically closed field, then the following are equivalent*

(a) (Weak form I) For an ideal I of $L[X_1, \cdots, X_n]$. If $I \neq L[X_1, \cdots, X_n]$, then $V(I)$ is not empty.

(b) (Field form) If A/F is an extension of field and A arises from F through ring adjunction of finite many elements, then A/F is a algebraic extension.

(c) (Weak form II) For any maximal ideal M of $L[X_1, \cdots, X_n]$ there exist $a_1, \cdots, a_n \in L$ such that

$$M = (X_1 - a_1, \cdots, X_n - a_n)$$

Proof. $(b) \Rightarrow (a)$ For I there is a maximal ideal M of $L[X_1, \cdots, X_n]$ such that $I \subset M$. Let $A := L[X_1, \cdots, X_n]/M$ is then a field which arises from L through ring adjunction of the residue classes a_i of X_i for $i = 1, \cdots, n$. By (b) A/L is an algebraic extension, so there is a $L-$ homomorphism $\phi : A \to L$, since L is algebraically closed field. Then $(\phi(a_1), \cdots, \phi(a_n)) \in L^n$ is a root of M, and hence so is I.

$(a) \Rightarrow (b)$ If the field A arises from F through ring adjunction of finite many elements, then $A \simeq F[X_1, \cdots, X_n]/M$ for some maximal ideal M. By (a) M has a zero in $\overline{F}^n$, where $\overline{F}$ is the algebraic closure of F. One has a $F-$homomorphism $\phi : A \to \overline{F}$, $\phi(X_i) = \xi_i$ with kernel M and thus $A \simeq F[\xi_1, \cdots, \xi_n]$. Since ξ_i is algebraic over F, A/F is an algebraic extension.

$(c) \Rightarrow (a)$ For I there is a maximal ideal M of $L[X_1, \cdots, X_n]$ such that $I \subset M$. Since $M = (X_1 - a_1, \cdots, X_n - a_n)$ for some a_i in L, $V(I) \supset V(M) = (a_1, \cdots, a_n)$. Therefore $V(I) \neq \phi$

$(a) \Rightarrow (c)$ Given any maximal ideal M, by (a) there exist $a_1, \cdots, a_n$ such that $(a_1, \cdots, a_n)$ in $V(M)$. The polynomial not belong to M then do not have $(a_1, \cdots, a_n)$ as a zero; otherwise, every polynomial would have this zero. It follows that $(X_1 - a_1, \cdots, X_n - a_n) \subset M$. Since $(X_1 - a_1, \cdots, X_n - a_n)$ is a maximal ideal, $(X_1 - a_1, \cdots, X_n - a_n) = M$. □

Now we use Hilbert basis Theorem and Fundamental Theorem of algebra to proof the strong form by Rabinowitsch trick.

Theorem 1. *(Strong form)Let L is an algebraically closed field. The assignment $V \to I(V)$ defined a bijection of the set of all L varieties $V \subset \mathbb{A}^n(L)$ onto the set of all ideals I of $L[X_1, \cdots, X_n]$ with $Rad(I) = I$. For any ideal I of $L[X_1, \cdots, X_n]$,*

$$Rad(I) = I(V(I)).$$

Proof. [6][8] Let f in $I(V(I)), f \neq 0$. In the polynomial ring $L[X_1, \cdots, X_n, T]$ with one more variable T, we form the ideal J generated by I and $f \cdot T - 1$. If

$(a_1, \cdots .a_n, t)$ in L^{n+1} is a zero of J, then $(a_1, \cdots, a_n)$ lie in $V(I)$, so $f(a_1, \cdots, a_n) \cdot t - 1 = -1$. But since $(a_1, \cdots, a_n, t)$ is also a zero of $f \cdot T - 1$, this is a contradiction. Since J has no zeros, $J = L[X_1, \cdots, X_n, T]$. Then we have an equation

$$1 = \sum_{i=1}^{s} R_i F_i + S(fT - 1)$$

with R_i, S in $L[X_1, \cdots, X_n, T]$ and $F_i \in I$. Now take $T = \frac{1}{f}$, then we have

$$1 = \sum_{i=1}^{s} \frac{A_i}{F^{\alpha_i}} F_i$$

for some A_i in $L[X_1, \cdots, X_n]$ and for some integer α_i. We can elimination the denominator by multipling F^{α} for some suitable α. Thus we get

$$f^{\alpha} = \sum_{i=1}^{m} A_i F_i.$$

Therefore we proved the theorem. □

In the special case for L has infinite transcendental degree over prime field k. We have the fastest proof[5].

Theorem 19. *Let L is an algebraically closed field with infinite transcendental degree over prime field k. For any ideal I of $L[X_1, \cdots, X_n]$,*

$$Rad(I) = I(V(I)).$$

Proof. We claim that for each prime ideal P of $L[X_1, \cdots, X_n] = R$ is the intersection of maximal ideal which is containing P. To prove the claim we have two steps.

Step1.: There exist $\alpha_1 \cdots, \alpha_n$ in L such that for $P' = P \bigcap K'[X_1, \cdots, X_n]$, then $P = P'L[X_1, \cdots, X_n]$, where $K' = k(\alpha_1 \cdots, \alpha_s)$.

Since $L[X_1, \cdots, X_n]$ is a Noetherian ring, $P = (f_1, \cdots, f_m)$. Let α_j be all the coefficient of f_i for $i = 1, \cdots, m$. Let $K' = k(\alpha_1 \cdots, \alpha_s)$ and let $P' = P \bigcap K'[X_1, \cdots, X_n]$. Thus f_i lie in $K'[X_1, \cdots, X_n]$ and hence for any f in P, $f = g_1 f_1 + \cdots + g_m f_m$ where g_i in $L[X_1, \cdots, X_n]$. Therefore f lie in $P'L[X_1, \cdots, X_n]$. So $P \subset P'L[X_1, \cdots, X_n]$. Conversely, $P'L[X_1, \cdots, X_n] \subset P$ is obviously. Then

we have $P = P'L[X_1, \cdots, X_n]$.

Step2.: Let K be the quotient field of $K'[X_1, \cdots, X_n]/P'$. Since L has infinite transcendental degree over prime field k, we can embedded K into L. Let a_i be the image of X_i for this embedded, and let $a = (a_1, \cdots, a_n)$. Then clearly for any f does not lie in P $f(a) \neq 0$. Thus we prove the claim. By definition of radical ideal we have

$$\mathrm{Rad}(I) = \bigcap_{I \subset P} P = \bigcap_{I \subset P \subset M,\ M \in MaxR} M = I(V(I)).$$

□

Next we will give four different proof of Field form. The first we give a proof by Artin Tate Lemma.

Lemma 20. [8](*Artin Tate Lemma*) *Let $R \subset S \subset T$ be rings, let R be Noetherian and $T = R[x_1, \cdots, x_n]$ with $x_1, \cdots, x_n$ in T. Assume $T$is finitely generated as an $S-$module. Then S is also finitely generated as a ring over R.*

First proof of field form: Suppose A/F is transcendental and $\{Z_1, \cdots, Z_t\}$, $t > 0$ is a transcendence basis, then by Lemma 20 $S := F(Z_1, \cdots, Z_t)$ is finitely generated as a ring over F. On the other hand, let $\{x_1, \cdots, x_m\}$ be a generating set of S/F, where $x_i = \frac{f_i(Z_1, \cdots, Z_t)}{g_i(Z_1, \cdots, Z_t)}$ with polynomials f_i, g_i for $i = 1, \cdots, m$. Because $S = F[x_1 \cdots, x_m]$, every element of S can be represented as a quotient of two polynomials in $F[Z_1 \cdots, Z_m]$. But for $p = g_1 \cdots g_m \in S$ $\frac{1}{p}$ does not lie in S, this is a contradiction. Therefore A/F is algebraic.

The second we give another proof by the version of integral extension.

Proposition 21. [8]*Let S/R be an extension of ring, where R is non-zero, and let I be an ideal of R. For x lie in S the following statements are equivalent.*

(a) x is integral over I.

(b) $R[x]$ is finitely generated as an $R-$module and x is in $Rad(IR[x])$.

(c) There is a subring S' of S with $R[x] \subset S$ such that S' is finitely generated as an $R-$module and x lie in $Rad(IS')$.

Second proof of field form: Let L/F be an extension of field, where $L = F[x_1, \cdots, x_n]$ for some x_i in L. We show by induction on n that L/F is algebraic. For $n = 1$ this i clear. Suppose that $n \geq 2$ and the assertion has been proved for $n-1$ elements, but that it is false for n elements. Say x_1 is transcendental over F. Since $L = F(x_1)[x_2, \cdots, x_n]$, L is algebraic over $F(x_1)$ by induction hypothesis. Let u_i in $F[x_1]$ be the leading coefficient of an algebraic equation of x_i over $F[x_1]$. and $u := \prod_{i=2}^{n} u_i$. Then by Proposition 21 L is integral over $F[x_1, \frac{1}{u}]$. Let p be a prime polynomial in $F[x_1]$ that does not divide u. $\frac{1}{p}$ satisfies an equation

$$(\frac{1}{p})^m + a_1(\frac{1}{p})^{m-1} + \cdots + a_m = 0 \quad (m > 0, a_i \in F[x_1, \frac{1}{u}])$$

After multiplying by p^m and suitable power of u, we get an equation

$$u^\rho + b_1 p + \cdots + b_m p^m = 0 \quad (\rho \in \mathbb{N},\ b_i \in F[x_1]).$$

But then p is a divisor of u^ρ in $F[x_1]$, a contradiction.

The third we use valuation ring version to proof field form. Let R be an integral domain and let K be the field of fractions. R is called valuation ring of K if, for each $x \neq 0$, either x in R or x^{-1} in R. Let K be a field and let L be the algebraically closed field. Let $\sum$ be the set of all pairs (A, f) where A is a subring of K and f is a homomorphism of A into L. We difine a partial order on the $\sum$ as follows:

$$(A, f) \leq (A', f') \Leftrightarrow A \subset A' and f'|_A = f.$$

By Zorn's Lemma there is a maximal element of $\sum$. To proof the theorem we need following lemma which lemmas we refered from [2].

Lemma 22. *Let (B, g) be a maximal element of $\sum$. Then B is a valuation ringof the field K*

Corollary 23. *Let A be a subring of a field K. Then the integral closure $\overline{A}$ of A in K is the intersection of all the valuation rings of K contain A.*

Proposition 24. *Let $C \subset B$ be a integral domain, B is finitely generated over C. Let v be a non-zero element of B. Then there exist a non-zero element u of*

C with the following property: any homomorphism f of C into an algebraically closed field Lsuch that $f(u) \neq 0$ can be extended to a homomorphism g of B into L such that $g(v) \neq 0$.

Third proof of field form: In Proposition 3 We take $C = K,\ v = 1$ and L be the algebraically closure of K. Then we can get the result of the theorem.

Last we give the fastest proof for a special case that K is a uncountable field.

Theorem 25. *(Field form) Suppose K is a uncountable field. If A/K is an extension of field and A arises from K through ring adjunction of finite many elements, then A/K is an algebraic extension.*

Proof. **Step 1.** $\dim_K K(X) \geq |K|$.

For

$$\frac{b_1}{X - a_1} + \cdots + \frac{b_n}{X - a_n} = 0.$$

We claim that $b_i = 0$ for all i. We Proof the claim by induction on n. For $n = 1$ nothing to proof. Now we assume the assertion hold for $n = 1$.

$$\begin{aligned} &\frac{b_1}{X - a_1} + \cdots + \frac{b_n}{X - a_n} = 0 \\ \Rightarrow &\sum_{i=1}^{n} \prod_{j \neq i} (X - a_j) = 0 \end{aligned}$$

Now take $X = a_1$ we have $b_1 = 0$ and by induction hypothesis we get $b_i = 0$ for all i. Thus $\dim_K K(X) \geq |K|$

Step 2. If E is an field extension of K and $\dim_K E < |K|$, then E is algebra over K.

Suppose E is transcendental over K and let $\{S_1, \cdots, S_m\}$ be a transcendental basis of E. Then

$$\dim_K E \geq \dim_K K(S_1, \cdots, S_m) \geq \dim_K K(S_1) \geq |K|.$$

This contradicts to that $\dim_K E < |K|$. Therefore E is algebra over K.

Step 3. Let $A = K[a_1, \cdots, a_n]$ be a finitely generated K algebra. Then $\dim_K A$

is at most countable.

Observing that one of bases of R over K is of the form $B = \{a_i^s | i = 1, \cdots, n \; s \in \mathbb{N}$. Thus $|B|$ is at most countable and hence $\dim_K A$ is at most countable.

Step 4 Now suppose A is transcendental over K. By step 1 $\dim_K A > |K|$, but K in a uncountable field this contradicts to $\dim_K A$ is at most countable. Therefore A os algebra over K. □

References

[1] Noga Alon, *Combinatorial Nullstellensatz*, combin. probab. comput. 8 (1999), no1-2,7-29.

[2] Enrique Arrondo, *Another Elementary Proof of the Nullstellensatz* ,Amer. Monthly 113 (2006), 169-170.

[3] M. F. Atiyah, I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-WesleyPublishing , 1969.

[4] David Cox, John Little, Donal O'shea, *Ideals, Varities, and Algorithms: An Introduction to Computational Algebraic Geometry and Commutative Algebra*, ,Springer-Verlag, New York, Heidelberg, Berlin, 1992.

[5] David Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Springer-Verlag, 1995.

[6] William Fulton, *Algebra Curves*, Addison-Wesley Publishing, 1989.

[7] Irving Kaplansky,*Commutative Rings*, Allyn and Bacon, 1970

[8] Ernst Kunz, *Introduction to commutative Algebra and Algebraic Geometry*, Birkhauser, 1980.

[9] Terrance Tao, *http://terrytao.wordpress.com/2007/11/26/hilberts-nullstellensatz*