4.5 Hilbert's Nullstellensatz (Zeros Theorem)

We develop a deep result of Hilbert's, relating solutions of polynomial equations to ideals of polynomial rings in many variables.

Notation: Put $A = F[x_1, \ldots, x_n]$ where F is a field. Write

$$\mathbf{x} = (x_1, \ldots, x_n) \quad \text{and} \quad \lambda = (\lambda_1, \ldots, \lambda_n)$$

if $\lambda_1, \ldots, \lambda_n \in F$. Suppose $p(\mathbf{x}) \in A$. Then

$$\boxed{\begin{array}{c} p(\lambda) \text{ is the result of evaluating } p(\mathbf{x}) \text{ in } F \\ \text{after substituting } \lambda_i \text{ for } x_i \text{ for each } i \ , \end{array}}$$

and if $p(\lambda) = 0$ then call λ a **zero** of $p = p(\mathbf{x})$. Put

$$\mathcal{Z}\big(p(\mathbf{x})\big) \ = \ \{ \ \lambda \in F^n \ \mid \ p(\lambda) \ = \ 0 \ \} \ ,$$

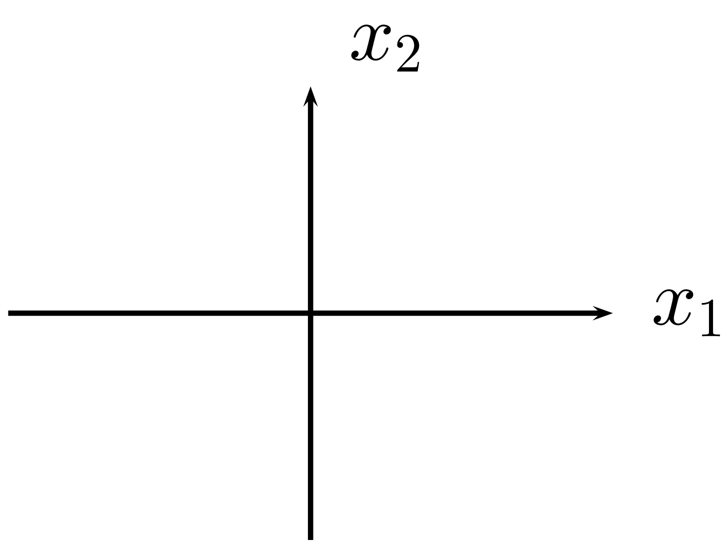
called the **zero set** of $p(\mathbf{x})$.

e.g. If $n = 1$ and $p(\mathbf{x})$ is nonzero then

$$|\mathcal{Z}\big(p(\mathbf{x})\big)| \le \text{ degree of } p(\mathbf{x}) .$$

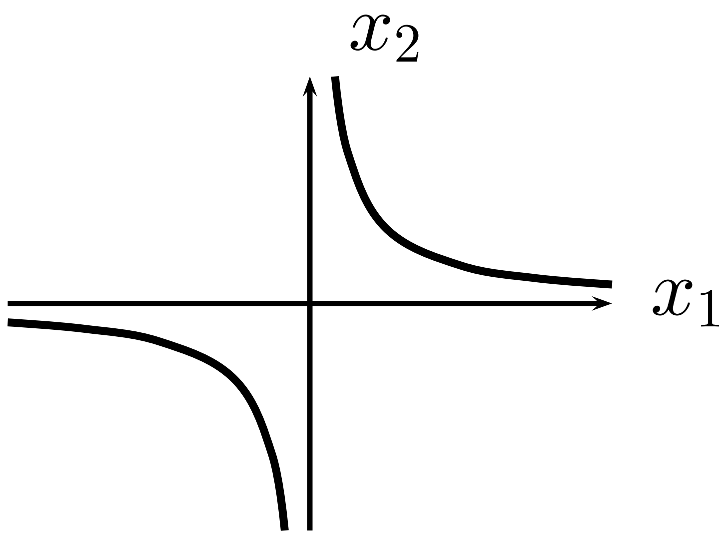
If $n = 2$ and $F = \mathbb{R}$, then

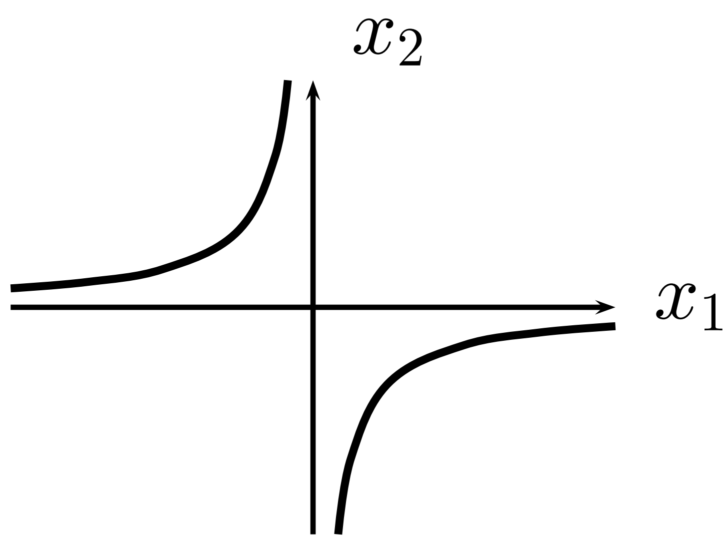
$$\mathcal{Z}\big(x_1 x_2\big) = \text{ union of } x_1 \text{ and } x_2 \text{-axes } :$$



$\mathcal{Z}\big(x_1 x_2 - 1\big) \ = \ $ hyperbola 1st and 3rd quadrants :

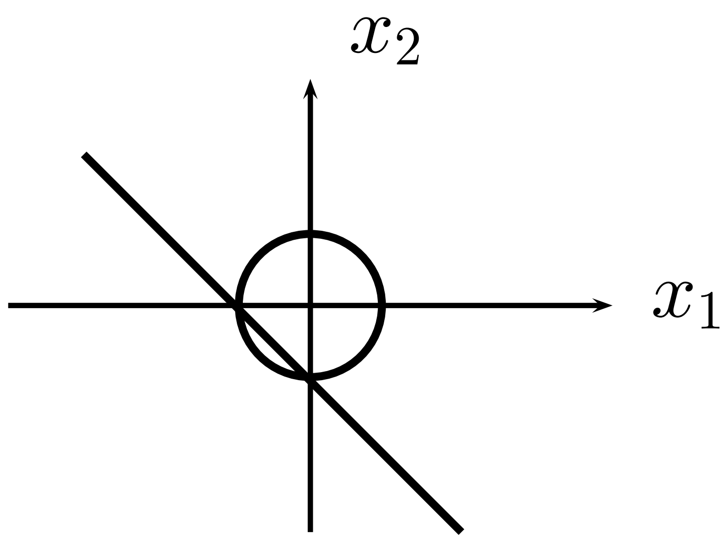
$\mathcal{Z}\big(x_1 x_2 + 1\big) \ = \ $ hyperbola 2nd and 4th quadrants :





$$\mathcal{Z}\big((x_1^2 + x_2^2 - 1)(x_1 + x_2 - 1)\big)$$

is the union of a circle and a line:



The circle and line separately correspond to irreducible factors of the polynomial.

If $T \subseteq A$ put

$$\mathcal{Z}(T) = \{ \lambda \mid p(\lambda) = 0 \qquad \forall p(\mathbf{x}) \in T \} ,$$

called the **zero set** of T .

$$\boxed{\begin{array}{c}\text{Clearly, if } T \subseteq A \text{ and } I = \langle T \rangle_{\text{ideal}} \text{ then} \\[2ex] \mathcal{Z}(T) = \mathcal{Z}(I) \, .\end{array}}$$

A subset Y of F^n is called **algebraic** if

$$(\exists T \subseteq A) \qquad Y = \mathcal{Z}(T)\,,$$

that is, if Y is the solution set of some system of polynomial equations.

But all ideals of A are finitely generated (Hilbert's Basis Theorem), so

Y is algebraic iff Y is the solution set of some **finite** system of polynomial equations.

Given $Y \subseteq F^n$, define the **ideal of** Y to be

$$\mathcal{I}(Y) = \{ p(\mathbf{x}) \in A \mid p(\lambda) = 0 \qquad \forall \lambda \in Y \},$$

the set of polynomials which vanish at all points of Y. Clearly

$$\mathcal{I}(Y) \lhd A .$$

It is easy to see that

$$\boxed{Y_1 \subseteq Y_2 \subseteq F^n \quad \Longrightarrow \quad \mathcal{I}(Y_1) \supseteq \mathcal{I}(Y_2)}$$

and also that

$$\boxed{T_1 \subseteq T_2 \subseteq A \quad \Longrightarrow \quad \mathcal{Z}(T_1) \supseteq \mathcal{Z}(T_2)\ .}$$

Further, it is clear that

$$Y \subseteq F^n \quad \Longrightarrow \quad Y \subseteq \mathcal{Z}\big(\mathcal{I}(Y)\big)$$

and

$$T \subseteq A \quad \Longrightarrow \quad T \subseteq \mathcal{I}\big(\mathcal{Z}(T)\big)\ .$$

Corollary: If Y is algebraic then

$$\mathcal{Z}\big(\mathcal{I}(Y)\big) \;=\; Y \,.$$

Proof: If $Y = \mathcal{Z}(T)$ for some $T \subseteq A$, then

$$Y \subseteq \mathcal{Z}\big(\mathcal{I}(Y)\big) = \mathcal{Z}\Big(\mathcal{I}\big(\mathcal{Z}(T)\big)\Big) \subseteq \mathcal{Z}(T) = Y\,,$$

at the second last step because $T \subseteq \mathcal{I}\big(\mathcal{Z}(T)\big)$, whence equality holds.

Question: Under what conditions is it the case, for $I \lhd A$, that

$$I = \mathcal{I}\big(\mathcal{Z}(I)\big)\ ?$$

Answer: . . . when $I = r(I)$, and F is algebraically closed (see below).

Hilbert's Nullstellensatz (Zeros Theorem):

If

$$I \lhd A = F[x_1, \ldots, x_n]$$

where F is an algebraically closed field, and $p(\mathbf{x}) \in A$ where

$$p(\lambda) = 0 \qquad (\forall \lambda \in \mathcal{Z}(I)) ,$$

then $p(\mathbf{x}) \in r(I)$.

This will be proved shortly after some preparation.

Corollary: If $I \lhd A$ and F is algebraically closed then

$$\mathcal{I}\big(\mathcal{Z}(I)\big) \;=\; r(I)\;.$$

Proof: If $I \lhd A$ then it is easy to see that

$$r(I) \;\subseteq\; \mathcal{I}\big(\mathcal{Z}(I)\big)\;,$$

so if, further, F is algebraically closed then, by the

Nullstellensatz, $\mathcal{I}\big(\mathcal{Z}(I)\big) \subseteq r(I)$, whence equality.

Corollary: Let F be algebraically closed. Then there is a one-one **inclusion-reversing** correspondence between algebraic sets in F^n and ideals of A which coincide with their radicals:

$$Y \;\mapsto\; \mathcal{I}(Y) \quad , \quad Y \text{ algebraic;}$$
$$I \;\mapsto\; \mathcal{Z}(I) \quad , \quad I \;=\; r(I) \lhd A \,.$$

Proof: If Y is algebraic then by an earlier Corollary,

$$\mathcal{Z}\big(\mathcal{I}(Y)\big) \;=\; Y\ .$$

If $I \;=\; r(I) \;\lhd\; A$ then, by the previous Corollary,

$$\mathcal{I}\big(\mathcal{Z}(I)\big) \;=\; I\ .$$

Injectivity and surjectivity follow quickly. The inclusion-reversing property has already been noted.

Before proving the Nullstellensatz, we review and develop some theory of **field extensions**: recall that if F is a subfield of a field K then we call

K an **extension** of F ,

in which case

$\boxed{K \text{ may be regarded as a vector space over } F\,.}$

If this vector space is finite dimensional then we call the extension **finite**.

Theorem: If K is a finite extension of F of dimension m, and L is a finite extension of K of dimension n, then

L is a finite extension of F of dimension mn.

Proof: left as an **exercise**.

Suppose K is an extension of F. Say that

$\alpha \in K$ is **algebraic over** F

if $p(\alpha) = 0$ for some nonzero $p(x) \in F[x]$.

Call K **algebraic over** F if all elements of K are algebraic over F .

If $\alpha_1 , \ldots , \alpha_n \in K$ then write

$$F[\alpha_1 , \ldots , \alpha_n] = \text{subring of } K \text{ generated by } F \text{ and } \alpha_1 , \ldots , \alpha_n$$

$$= F\text{-subalgebra of } K \text{ generated by } \alpha_1 , \ldots , \alpha_n .$$

$\boxed{\text{note: } \textbf{square brackets} \text{ denote } \textbf{subring},}$

and write

$$F(\alpha_1\,,\ \ldots\ ,\ \alpha_n) \;=\; \text{subfield of } K \text{ generated by } F \text{ and } \alpha_1\,,\ \ldots\ ,\ \alpha_n$$

$\boxed{\text{note: } \textbf{round brackets} \text{ denote } \textbf{subfield}.}$

Call $\alpha_1 , \ldots , \alpha_n \in K$

algebraically independent over F

if

$$p(\alpha_1, \ldots, \alpha_n) \neq 0 ,$$

for all nonzero $p(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$,

in which case the evaluation map

$$p(x_1, \ldots, x_n) \mapsto p(\alpha_1, \ldots, \alpha_n)$$

defines a ring isomorphism:

$$F[x_1, \dots, x_n] \longrightarrow F[\alpha_1, \dots, \alpha_n]$$

(where the latter is a **subring** of K), whence

$F(\alpha_1, \dots, \alpha_n)$ is the ring of fractions of $F[\alpha_1, \dots, \alpha_n]$ isomorphic to the ring

$F(x_1, \dots, x_n)$ of rational functions in indeterminates $x_1, \dots, x_n$.

Theorem: Let K be an extension of a field F and suppose $\alpha \in K$ is algebraic over F . Then

$$F[\alpha] \;=\; F(\alpha)$$

is a finite (and hence algebraic) extension of F .

Proof: Certainly $F[\alpha] \;\subseteq\; F(\alpha)$.

To prove the reverse set containment, suppose $p(x) \in F[x]$ such that

$$p(\alpha) \neq 0 \qquad \text{(evaluated in } K \text{)}\,.$$

$$\boxed{\text{It is sufficient to show } p(\alpha)^{-1} \in F[\alpha]\,.}$$

Since α is algebraic, let $m(x) \in F[x]$ be the **minimum** polynomial of α , that is, the nonzero polynomial of least degree such that $m(\alpha) = 0$. Then

$$p(x) = m(x)\,q(x) + r(x)$$

for some polynomials $q(x)$, $r(x)$ such that $r(x)$ has degree $<$ degree of $m(x)$. Hence

$$\boxed{p(\alpha) = r(\alpha) .} \qquad (*)$$

But $m(x)$ is irreducible (because it is minimal), so

$$\big(\exists\, a(x) , b(x)\big) \qquad r(x)a(x) + m(x)b(x) = 1 .$$

Evaluating in K yields

$$1 = r(\alpha)\, a(\alpha) + m(\alpha)\, b(\alpha) = p(\alpha)\, a(\alpha) ,$$

so that $p(\alpha)^{-1} = a(\alpha) \in F[\alpha]$.

It follows that

$$\boxed{F(\alpha) = F[\alpha] .}$$

Also $(*)$ shows that $F[\alpha]$ is spanned by 1 , α , $\ldots$, α^{d-1} over F where $d =$ degree of $m(x)$. Thus

$$\boxed{F(\alpha) \text{ is finite dimensional over } F \,.}$$

Finally, if $\beta \in F[\alpha]$ then

$$\{\, 1 \,,\ \beta \,,\ \ldots \,,\ \beta^d \,\}$$

is linearly dependent (being of size $> d$), so $g(\beta) = 0$ for some nonzero polynomial $g(x)$.

This proves $F(\alpha)$ is algebraic over F .

Theorem: Suppose α_1 , ... , $\alpha_n \in K$ are algebraic over F . Then

$$F[\alpha_1, \ldots, \alpha_n] \;=\; F(\alpha_1, \ldots, \alpha_n)$$

is a finite (and hence algebraic) extension of F .

Proof: If $n = 1$ this is the result of the previous Theorem, which starts an induction.

Suppose $n > 1$. By an inductive hypothesis,

$$F[\alpha_1, \ldots, \alpha_{n-1}] \;=\; F(\alpha_1, \ldots, \alpha_{n-1})$$

is a finite extension of F . Then

$$\begin{aligned} F[\alpha_1, \ldots, \alpha_n] &= F[\alpha_1, \ldots, \alpha_{n-1}][\alpha_n] \\ \\ &= F(\alpha_1, \ldots, \alpha_{n-1})[\alpha_n] \,, \end{aligned}$$

and certainly α_n is algebraic over $F(\alpha_1, \ldots, \alpha_{n-1})$, being algebraic over F .

By the previous Theorem,

$$\begin{aligned} F(\alpha_1, \dots, \alpha_n) &= F(\alpha_1, \dots, \alpha_{n-1})(\alpha_n) \\ &= F(\alpha_1, \dots, \alpha_{n-1})[\alpha_n] \\ &= F[\alpha_1, \dots, \alpha_n] \end{aligned}$$

is a finite extension of $F[\alpha_1, \dots, \alpha_{n-1}]$.

By the Theorem on extensions of extensions,

$F(\alpha_1, \ldots, \alpha_n)$ is a finite extension of F , and we are done.

Theorem: Let F be a field and E a finitely generated F-algebra.

If E is a field then E is a finite (and hence algebraic) extension of F .

Proof: Suppose E is a field and

$$E = F[\alpha_1, \ldots, \alpha_n]$$

for some $n \geq 1$ and $\alpha_1, \ldots, \alpha_n \in E$.

By the previous Theorem, it suffices to prove that

$$\boxed{\alpha_1, \ldots, \alpha_n \text{ are algebraic over } F.} \qquad (*)$$

Suppose $(*)$ is false, so WLOG we may suppose α_1 is not algebraic over F. Hence

$\boxed{\{\alpha_1\} \text{ is an algebraically independent set over } F\,.}$

Suppose we have $1 \leq m < n$ such that

$$\boxed{\begin{array}{l}\{\ \alpha_1\ ,\ \ldots\ ,\ \alpha_m\ \}\ \text{is algebraically independent} \\ \text{over}\ \ F\ ,\ \text{yet not all of}\ \ \alpha_{m+1}\ ,\ \ldots\ ,\ \alpha_n\ \ \text{are} \\ \text{algebraic over}\ \ F(\alpha_1\ ,\ \ldots\ ,\ \alpha_m)\ .\end{array}} \quad (**)$$

WLOG we may suppose α_{m+1} is not algebraic over $F(\alpha_1, \ldots, \alpha_m)$.

$$\boxed{\text{We will verify that } \{ \alpha_1, \ldots, \alpha_{m+1} \} \text{ is algebraically independent over } F .}$$

Let

$$p(x_1, \ldots, x_m, x_{m+1})$$

be a nonzero polynomial in $F[x_1, \ldots, x_{m+1}]$.

Then

$$\begin{aligned} p(x_1, \dots, x_{m+1}) \;\; &= \;\; p_0(x_1, \dots, x_m) + \\ & \qquad p_1(x_1, \dots, x_m) x_{m+1} \; + \; \dots \\ & \qquad \quad + \; p_N(x_1, \dots, x_m)\, x_{m+1}^N \end{aligned}$$

for some $N \geq 0$ and coefficient polynomials in $F[x_1, \dots, x_m]$ with $p_N(x_1, \dots, x_m)$ nonzero.

Certainly

$$p_0(\alpha_1, \ldots, \alpha_m) \ , \ \ldots \ , \ p_N(\alpha_1, \ldots, \alpha_m) \\ \in \ F(\alpha_1, \ldots, \alpha_m)$$

and

$$p_N(\alpha_1, \ldots, \alpha_m) \ \neq \ 0 \ ,$$

since α_1 , ... , α_m are algebraically independent over F .

Hence

$$p(\alpha_1, \ldots, \alpha_m, x_{m+1})$$

is a nonzero polynomial with coefficients in $F(\alpha_1, \ldots, \alpha_m)$, so,

since α_{m+1} is not algebraic over $F(\alpha_1, \ldots, \alpha_m)$,

$$p(\alpha_1, \ldots, \alpha_{m+1}) \neq 0 .$$

This proves $\{\alpha_1, \ldots, \alpha_{m+1}\}$ is algebraically independent over F .

Thus, continuing this way from $(**)$, we get to a stage where

for some r such that $1 \leq r \leq n$

$\{ \alpha_1 , \ \ldots \ , \alpha_r \}$ is algebraically independent over F

and each of $\alpha_{r+1} , \ \ldots \ , \alpha_n$ is algebraic over $F(\alpha_1, \ldots, \alpha_r)$.

Put

$$K = F(\alpha_1, \ldots, \alpha_r) \; ,$$

so, by earlier remarks (page 871),

$$\boxed{K \cong F(x_1, \ldots, x_r) \; ,}$$

the field of rational functions. Certainly

$$\begin{aligned} E &= F[\alpha_1, \ldots, \alpha_n] \subseteq F(\alpha_1, \ldots, \alpha_r)[\alpha_{r+1}, \ldots, \alpha_n] \\ &= K[\alpha_{r+1}, \ldots, \alpha_n] \subseteq E \; , \end{aligned}$$

so

$$E = K[\alpha_{r+1}, \ldots, \alpha_n] \; .$$

By the previous Theorem,

$$\boxed{E \text{ is a finite (algebraic) extension of } K \; .}$$

But $F \subseteq K \subseteq E$,

E is finitely generated as an F-algebra, and

E is finitely generated as a K-module (being a finite dimensional vector space over K).

Hence, by the last theorem we proved on Noetherian rings (page 845),

K is finitely generated as an F-algebra, say

$$K = F[\beta_1, \ldots, \beta_s]$$

for some $\beta_1, \ldots, \beta_s \in K$.

For each $i = 1, \ldots, s$, we may write

$$\beta_i \;=\; \frac{f_i(\alpha_1, \ldots, \alpha_r)}{g_i(\alpha_1, \ldots, \alpha_r)}$$

for some polynomials

$$f_i \;=\; f_i(x_1, \ldots, x_r) \;\;, \quad g_i \;=\; g_i(x_1, \ldots, x_r)$$

where we may suppose

f_i , g_i have no irreducible factors in common.

The proof now splits:

$\boxed{\textbf{Case (i):} \quad \text{Suppose } g_i \text{ is constant for each } i \text{ .}}$

WLOG we may suppose $g_i = 1$ for each i .

Now $0 \neq \alpha_1 \in K$, so $\alpha_1^{-1} \in K$, yielding

$$\alpha_1^{-1} = p(\beta_1, \ldots, \beta_s)$$

for some nonzero polynomial $p(x_1, \ldots, x_s)$.

But then

$$\alpha_1^{-1} \;=\; p\big(\, f_1(\alpha_1, \ldots, \alpha_r)\,,\ \ldots\ ,\ f_s(\alpha_1, \ldots, \alpha_r)\,\big)$$

$$=\; q(\alpha_1, \ldots, \alpha_r)$$

where

$$q(x_1, \ldots, x_r) \;=\; p\big(\, f_1(x_1, \ldots, x_r)\,,\ \ldots\ ,\ f_s(x_1, \ldots, x_r)\,\big)$$

is a nonzero polynomial.

Hence

$$\alpha_1 \, q(\alpha_1, \ldots, \alpha_r) \; - \; 1 \;\; = \;\; 0 \, .$$

But

$$x_1 \, q(x_1, \ldots, x_r) \; - \; 1$$

is a nonzero polynomial.

This yields a contradiction, since

$\{ \, \alpha_1 \, , \; \ldots \; , \; \alpha_r \, \}$ is algebraically independent.

Case (ii): Suppose $g_1 \dots g_s$ is not constant.

Put

$$\boxed{h = h(x_1, \dots, x_r) = \big(g_1 \dots g_s\big) + 1}$$

so

h is a nonconstant polynomial which is not divisible by any irreducible factor of $g_1 \dots g_s$.

Put

$$\gamma = h(\alpha_1, \ldots, \alpha_r) \neq 0$$

since $\{ \alpha_1 , \ldots , \alpha_r \}$ is algebraically independent over F .

But γ and hence γ^{-1} lie in $K = F[\beta_1, \ldots, \beta_s]$, so

$$\gamma^{-1} = p(\beta_1, \ldots, \beta_s)$$

for some nonzero $p(x_1, \ldots, x_s) \in F[x_1, \ldots, x_s]$.

Hence

$$\gamma^{-1} \;=\; p\left(\frac{f_1(\alpha_1, \ldots, \alpha_r)}{g_1(\alpha_1, \ldots, \alpha_r)} \,, \;\ldots\; , \frac{f_s(\alpha_1, \ldots, \alpha_r)}{g_s(\alpha_1, \ldots, \alpha_r)} \right)$$

$$= \;\frac{q_1(\alpha_1, \ldots, \alpha_r)}{q_2(\alpha_1, \ldots, \alpha_r)}$$

for some polynomials

$$q_1 \;=\; q_1(x_1, \ldots, x_r) \;, \;\; q_2 \;=\; q_2(x_1, \ldots, x_r) \;\in\; F[x_1, \ldots, x_r]$$

such that

(a) q_1 , q_2 have no common irreducible factors;

(b) either q_2 is constant, or q_2 is a product of (powers of) irreducible divisors of $g_1 \dots g_s$.

Then

$$1 \;=\; \gamma\gamma^{-1} \;=\; h(\alpha_1, \dots, \alpha_r)\, \frac{q_1(\alpha_1, \dots, \alpha_r)}{q_2(\alpha_1, \dots, \alpha_r)} \,,$$

so

$$q_2(\alpha_1, \ldots, \alpha_r) \; - \; h(\alpha_1, \ldots, \alpha_r)\, q_1(\alpha_1, \ldots, \alpha_r)$$
$$= \; 0 \, .$$

But $\{ \alpha_1 \, , \, \ldots \, , \, \alpha_r \}$ is algebraically independent, so, in $F[x_1, \ldots, x_r]$

$$\boxed{q_2 - hq_1 \; = \; 0 \, ,}$$

yielding

$$\boxed{hq_1 \;=\; q_2\,.} \qquad (\dagger)$$

If q_2 is constant then h is constant, contradicting that h is nonconstant.

Hence q_2 is nonconstant so, by **(b)** above,

$$q_3 \text{ divides } q_2$$

for some irreducible factor q_3 of $g_1 \dots g_s$.

But q_3 does not divide $h = (g_1 \dots g_s) + 1$ so, by $(\dagger)$ and the fact that $F[x_1, \ldots, x_n]$ is a UFD (Gauss' Theorem, see below),

$$q_3 \text{ must divide } q_1$$

which contradicts **(a)** above.

This proves $(*)$ and completes the proof of the Theorem.

Corollary: Let F be a field, A a finitely generated F-algebra, and M a maximal ideal of A.

Then A/M is a finite algebraic extension of (an embedding) of F.

In particular, if F is algebraically closed then

$$A/M \;\cong\; F\,.$$

Proof: Let $\phi : F \longrightarrow A/M$ where

$$\phi(\lambda) = \lambda + M \qquad (\lambda \in F) .$$

Clearly ϕ is a homomorphism and

$$\ker\phi = \{ \lambda \in F \mid \lambda \in M \} = \{0\} ,$$

since $M \neq A$. Hence ϕ is an embedding.

But A is finitely generated as an F-algebra, so A/M is finitely generated as a $\phi(F)$-algebra.

Also A/M is a field, so, by the previous Theorem,

$$\boxed{\begin{array}{c} A/M \text{ is a finite algebraic extension of} \\ \phi(F) \ \cong \ F \, . \end{array}}$$

If F is algebraically closed, then so is $\phi(F)$, so $\phi(F)$ contains all roots of all polynomial equations over itself, so

$$A/M \ = \ \phi(F) \ \cong \ F \, .$$

Finally we come to the

Proof of Hilbert's Nullstellensatz:

Here F is an algebraically closed field,

$$A \;=\; F[x_1, \ldots, x_n] \qquad (n \geq 1)$$

and $I \lhd A$.

We are given $p(\mathbf{x}) \in A$ such that

$$\boxed{\quad p(\lambda) \;=\; 0 \qquad \big(\forall \lambda \in \mathcal{Z}(I)\big) \quad} \qquad (*)$$

where

$$\mathcal{Z}(I) \;=\; \{\, \lambda \,\in\, F^n \;\mid\; q(\lambda) \,=\, 0 \quad \big(\forall\, q(\mathbf{x}) \,\in\, I\big)\,\}\,.$$

We need to prove

$$p(\mathbf{x}) \;\in\; r(I)\;,$$

that is, some power of $p(\mathbf{x})$ lies in I .

We argue by contradiction.

Suppose $p(\mathbf{x}) \notin r(I)$.

$\boxed{\text{But } r(I) \text{ is the intersection of all prime ideals of } A \text{ containing } I \text{ (see page 220).}}$

Hence

$$p(\mathbf{x}) \notin P$$

for some prime ideal $P \lhd A$ where $I \subseteq P$.

Consider the ring of fractions

$$\boxed{B \;=\; S^{-1}(A/P)}$$

where

$$\boxed{S \;=\; \{\, p(\mathbf{x})^m + P \;\mid\; m \geq 0 \,\}}$$

(which is clearly multiplicatively closed).

If B is the zero ring then

$$1 + P \;/\; 1 + P \;\; = \;\; 0 + P \;/\; 1 + P$$

so

$$(1 + P)(p(\mathbf{x})^m + P) \;\; = \;\; P \qquad\qquad (\exists m \geq 0)$$

so

$$p(\mathbf{x})^m + P \;\; = \;\; P$$

so $p(\mathbf{x})^m \in P$, whence $p(\mathbf{x}) \in P$, contradicting that $p(\mathbf{x}) \notin P$.

Hence B is not a zero ring, so there is some maximal ideal M of B, and

$$\boxed{B/M \text{ is a field.}}$$

Define mappings

$$\phi \;:\; A \longrightarrow B \qquad \text{by}$$

$$f(\mathbf{x}) \;\mapsto\; \big(f(\mathbf{x}) + P\big) \;/\; \big(1 + P\big)$$

and

$$\psi \; : \; A \longrightarrow B/M \qquad \text{by}$$

$$f(\mathbf{x}) \mapsto \phi\big(f(\mathbf{x})\big) + M \; .$$

Clearly

$$\boxed{\phi \text{ and } \psi \text{ are ring homomorphisms.}}$$

$$\boxed{\text{We check that } \psi|_F \text{ and } \phi|_F \text{ are injective.}}$$

Let $\lambda \in \ker \psi|_F$. Then

$$M = \psi(\lambda) = \phi(\lambda) + M ,$$

so

$$(\lambda + P)/(1 + P) = \phi(\lambda) \in M .$$

If $\lambda \neq 0$ then

$$\frac{1+P}{1+P} = \left(\frac{\lambda+P}{1+P}\right)\left(\frac{\lambda^{-1}+P}{1+P}\right) \in M$$

so $M = B$, contradicting that $M \neq B$.

Hence $\lambda = 0$, so

$$\ker \psi|_F = \ker \phi|_F = \{0\} ,$$

so both $\psi|_F$ and $\phi|_F$ are injective.

Hence

$\boxed{\phi(F) \text{ and } \psi(F) \text{ are copies of } F \text{ in } B \text{ and } B/M \text{ respectively.}}$

Notation: If $f = f(\mathbf{x}) \in A$ then denote by

$$\widehat{f} = \widehat{f}(\mathbf{x}) \qquad \text{and} \qquad \widetilde{f} = \widetilde{f}(\mathbf{x})$$

the polynomials obtained from f by replacing any coefficient $\gamma \in F$ by $\phi(\gamma)$ and $\psi(\gamma)$ respectively.

Clearly, then, since ϕ and ψ are ring homomorphisms, if $f = f(\mathbf{x}) \in A$ and

$$\alpha = (\alpha_1, \ldots, \alpha_n) \in A^n$$

then

$$\boxed{\begin{array}{l} \phi\big(f(\alpha)\big) = \widehat{f}\big(\phi(\alpha_1), \ldots, \phi(\alpha_n)\big) \\ \text{and} \\ \psi\big(f(\alpha)\big) = \widetilde{f}\big(\psi(\alpha_1), \ldots, \psi(\alpha_n)\big) \end{array}}$$

We now verify that

$$\boxed{B \text{ is a finitely generated } \phi(F)\text{-algebra.}}$$

If $b \in B$ then, for some $f(\mathbf{x}) \in A$ and $m \geq 0$

$$b = \frac{f(\mathbf{x}) + P}{p(\mathbf{x})^m + P} = \left(\frac{f(\mathbf{x}) + P}{1 + P}\right)\left(\frac{1 + P}{p(\mathbf{x})^m + P}\right)$$

$$= \widehat{f}\left(\frac{x_1 + P}{1 + P}, \ \ldots \ , \frac{x_n + P}{1 + P}\right)\left(\frac{1 + P}{p(\mathbf{x}) + P}\right)^m .$$

This verifies that B is generated, as a $\phi(F)$-algebra, by

$$\frac{x_1 + P}{1 + P}\,,\ \ldots\ ,\ \frac{x_n + P}{1 + P}\,,\ \frac{1 + P}{p(\mathbf{x}) + P}\,,$$

so

$$\boxed{B \ \text{ is finitely generated as a } \ \phi(F)\text{-algebra,}}$$

whence also

$$\boxed{B/M \ \text{ is finitely generated as a } \ \psi(F)\text{-algebra.}}$$

But F , and hence $\psi(F)$, are algebraically closed, so, by our last Corollary (page 902), since B/M is a field,

$$\boxed{B/M \ = \ \psi(F)\ .}$$

Hence, for each $i = 1, \ldots, n$,

$$\boxed{(\exists\, \lambda_i \ \in \ F) \qquad \psi(x_i) \ = \ \psi(\lambda_i)\ .}$$

Put

$$\boxed{\lambda \;=\; (\lambda_1 \,,\; \ldots \;,\; \lambda_n)\;.}$$

We now prove that

$$\lambda \;\in\; \mathcal{Z}(I) \qquad \text{but} \qquad p(\lambda) \;\neq\; 0\;.$$

For all $f(\mathbf{x}) \in I$ we have $f(\mathbf{x}) \in P$, so

$$
\begin{aligned}
\psi\big(f(\lambda)\big) &= \widetilde{f}\big(\psi(\lambda_1)\ ,\ \ldots\ ,\ \psi(\lambda_n)\big) \\
&= \widetilde{f}\big(\psi(x_1)\ ,\ \ldots\ ,\ \psi(x_n)\big) \;=\; \psi\big(f(\mathbf{x})\big) \\
&= \left(\frac{f(\mathbf{x}) + P}{1+P}\right) +\ M \\
&= \left(\frac{P}{1+P}\right) +\ M \;=\; M
\end{aligned}
$$

so $f(\lambda) = 0$, since $\psi|_F$ is injective.

This proves $\boxed{\lambda \in \mathcal{Z}(I) .}$

But

$$\psi\big(p(\lambda)\big) = \widetilde{p}\big(\psi(\lambda_1) , \ldots , \psi(\lambda_n)\big)$$

$$= \widetilde{p}\big(\psi(x_1) , \ldots , \psi(x_n)\big) = \psi\big(p(\mathbf{x})\big)$$

so

$$\psi\big(p(\lambda)\big) \;=\; \left(\frac{p(\mathbf{x}) + P}{1+P}\right) \;+\; M \;.$$

If $\psi\big(p(\lambda)\big) \;=\; M$ then

$$\frac{p(\mathbf{x}) + P}{1+P} \;\in\; M$$

so

$$\frac{1+P}{1+P} \;=\; \left(\frac{p(\mathbf{x}) + P}{1+P}\right)\left(\frac{1+P}{p(\mathbf{x}) + P}\right) \;\in\; M \;,$$

so $M \;=\; B$, contradicting that $M \;\neq\; B$.

Hence

$$\psi\big(p(\lambda)\big) \neq M .$$

so

$$\boxed{\quad p(\lambda) \neq 0 \quad}$$

since ψ is a homomorphism.

This contradicts that $p(\lambda) = 0$ by $(*)$,

and the proof of Hilbert's Nullstellensatz is complete.