ARITHMETIC NULLSTELLENSÄTZE AND APPLICATIONS

Teresa Krick - UBA & CONICET - Mvd, Dec 2014.

(I) Hilbert NSS ("Weak" form) ~ 1890 (David Hilbert, 1862-1943)

$f_1, \dots, f_s \in K[x_1, \dots, x_n]$ where $K = \overline{K}$ algebraically closed

$$\nexists\ x = (x_1, \dots, x_n) \in K^n \text{ s.t. } f_1(x) = \dots = f_s(x) = 0$$

$$\Updownarrow$$

$$\exists\ g_1, \dots, g_s \in K[x_1, \dots, x_n] \text{ s.t. } 1 = g_1 f_1 + \dots + g_s f_s$$

"Bézout identity"
(Etienne Bézout, 1730 - 1793)

Comments

1 - K algebraically closed is essential:

$\nexists\ x \in \mathbb{R}$ s.t. $x^2 + 1 = 0$ but $\nexists\ g \in \mathbb{R}[x]$ s.t. $1 = g \cdot (x^2+1)$

2 - Geometry vs Algebra:

Geometry: the common zero locus of $f_1, \dots, f_s$ is empty

i.e. if $V(\underline{f}) = \{ \underline{x} \in K^n : f_1(\underline{x}) = \dots = f_s(\underline{x}) = 0 \}$

is the algebraic variety defined by $f_1, \dots, f_s$, then $V(\underline{f}) = \emptyset$

Algebra: the polynomial 1 can be written as a polynomial combination of $f_1, \dots, f_s$. i.e. if $I = \langle f_1, \dots, f_s \rangle \subseteq K[x_1, \dots, x_n]$ is the ideal generated by $f_1, \dots, f_s$, then $1 \in I$

(Here $I = \langle f_1, \dots, f_s \rangle = \{ g_1 f_1 + \dots + g_s f_s ;\ g_i \in K[x_1, \dots, x_n],\ 1 \le i \le s \}$)

Ideals matter because $V(\underline{f}) = V(I)$ for $I = \langle f_1, \dots, f_s \rangle$

HNSS: $V(I) = \emptyset \iff 1 \in I$ (K alg. closed)

Note that since $K[x_1, \dots, x_n]$ is Noetherian (Hilbert Basis Theorem) every ideal $I \subseteq K[x_1, \dots, x_n]$ is finitely generated

3 - On the proof: ($\Leftarrow$) is easy:

$I = \langle f_1, \dots, f_s \rangle$: $1 \in I \Rightarrow \exists g_1, \dots, g_s \in K[X_1, \dots, X_n]$ st

$1 = g_1 f_1 + \dots + g_s f_s$.

Suppose $\exists \underline{x} \in K^n$ st $\underline{x} \in V(I)$, i.e $f_1(\underline{x}) = \dots = f_s(\underline{x}) = 0$

then $1 = g_1(\underline{x}) f_1(\underline{x}) + \dots + g_s(\underline{x}) f_s(\underline{x}) = 0$, contradiction

($\Rightarrow$) seems less obvious ...

Examples :

1 - Case $n = 1$, $\deg(f_i)$ arbitrary, $1 \le i \le s$:

$V(I) = \emptyset \Rightarrow \gcd(f_1, \dots, f_s) = 1$ since if $h := \gcd(f_1, \dots, f_s) \neq 1$,

then $\deg h \geq 1$ and since $K = \overline{K}$, $\exists x \in K$ s.t $h(x) = 0 \Rightarrow x \in V(I)$

$\Rightarrow \exists g_1, \dots, g_s \in K[X]$ st $1 = g_1 f_1 + \dots + g_s f_s$ since $\gcd(f_1, \dots, f_s)$ can be written as a polynomial combination of $f_1, \dots, f_s$

(because $K[X]$ is a PID (principal ideal domain) which comes from the fact that $K[X]$ is an Euclidean domain (division algorithm))

Note that the argument doesn't work for $n > 1$, since for instance $K[X,Y]$ is not a PID : $\langle X, Y \rangle \subseteq K[X,Y]$ is not a principal ideal

¿Why? and $1 = \gcd(X, Y)$ cannot be written as $1 = g_1 \cdot X + g_2 \cdot Y$

2 - Case n arbitrary, $\deg(f_i) = 1$, $1 \le i \le s$:

$f_1 = a_{11} X_1 + \dots + a_{1n} X_n - b_1$, ..., $f_s = a_{s1} X_1 + \dots + a_{sn} X_n - b_n$

$$\begin{cases} a_{11} X_1 + \dots + a_{1n} X_n = b_1 \\ \vdots \\ a_{s1} X_1 + \dots + a_{sn} X_n = b_n \end{cases} \quad \langle = \rangle \quad \begin{bmatrix} a_{11} & \dots & a_{1n} \\ a_{s1} & & a_{sn} \end{bmatrix} \begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = \begin{pmatrix} b_1 \\ \vdots \\ b_s \end{pmatrix}$$

doesn't have a sol $\Leftrightarrow$ $\operatorname{rk} \begin{bmatrix} a_{11} & \dots & a_{1n} \\ a_{s1} & & a_{sn} \end{bmatrix} \neq \operatorname{rk} \left[\begin{array}{ccc|c} a_{11} & \dots & a_{1n} & b_1 \\ a_{s1} & & a_{sn} & b_s \end{array}\right]$

$\langle = \rangle$ Gaussian elimination :

$$\left[\begin{array}{ccc|c} & * & & * \\ 0 & & & \\ & & & * \end{array}\right] \leftarrow \neq 0$$

a linear combination of the rows gives a non-zero constant.

i.e $1 = c_1 f_1 + \dots + c_s f_s$.

The general case

There are several ≠ proofs of HWSS at different levels
Surprisingly none is completely elementary as it is in the case $n = 1$ or $\deg(f_1) = 1$

For example

1 - Consequence of Tarski's lemma (Oscar Tarski, 1899-1986)

A finitely generated algebra over a field K which is itself a field is a finite field extension of the field K

which implies how are the maximal ideals of $K[x_1, \dots, x_n]$ when $K = \overline{K}$: $\langle x_1 - a_1, \dots, x_n - a_n \rangle$, $a_1, \dots, a_n \in K$

2 - Consequence of the "extension theorem":

$I = \langle f_1, \dots, f_s \rangle \subseteq K[x_1, \dots, x_n]$, $I_1 := I \cap K[x_2, \dots, x_n]$

Write $f_1 = c_1(x_2, \dots, x_n)\, x_1^{N_1} + \dots$

$\vdots$

$f_s = c_s(x_2, \dots, x_n)\, x_1^{N_s} + \dots$

Suppose $\exists\, \underline{x}' := (x_2, \dots, x_n) \in V(I_1) - V(c_1, \dots, c_s)$,

then $\exists\, x_1 \in K$ s.t. $\underline{x} := (x_1, \underline{x}') \in V(I)$

i.e: $V(I_1) - V(c_1, \dots, c_s) \neq \emptyset \Rightarrow V(I) \neq \emptyset$

We'll focus on this last, as a good excuse to introduce the important theory in Elimination Theory of Resultants which will often appear in different ways in these lectures.
Moreover the resultant is an essential tool in Number theory (through the discriminant) and in Computer Algebra

II Sylvester's matrix and Resultant (James Joseph Sylvester, 1814 - 1897)

Let $f, g \in K[X]$ of exact degrees m and n.

$f = a_m X^m + \dots + a_0$ with $a_m \neq 0$ and $g = b_n X^n + \dots + b_0$ with $b_n \neq 0$

The Sylvester matrix for f and g is defined as

$$S_{m,n}(f,g) := \begin{bmatrix} a_m & & & b_n & & \\ \vdots & \ddots & & \vdots & \ddots & \\ a_0 & & a_m & b_0 & & b_n \\ & \ddots & \vdots & & \ddots & \vdots \\ & & a_0 & & & b_0 \end{bmatrix} \begin{matrix} \uparrow \\ m+n \\ \downarrow \end{matrix} \in K^{(m+n)\times(m+n)}$$

$\leftarrow n \rightarrow \quad \leftarrow m \rightarrow$

and $\operatorname{Res}_{m,n}(f,g) := \det\left(S_{m,n}(f,g)\right) \in K$

Examples

1) $f = X - \alpha$, $g = X - \beta \Rightarrow S_{1,1}(f,g) = \begin{bmatrix} 1 & 1 \\ -\alpha & -\beta \end{bmatrix}$ and $\operatorname{Res}_{1,1}(f,g) = \alpha - \beta$

2) $f = a_m X^m + \dots + a_0$ with $a_m \neq 0$ and $g = X - \beta$:

$$S_{m,1}(f,g) = \begin{bmatrix} a_m & 1 & & \\ \vdots & -\beta & \ddots & \\ a_0 & & \ddots & 1 \\ & & & -\beta \end{bmatrix} \text{ and } \operatorname{Res}_{m,1}(f,g) = (-1)^m f(\beta)$$

Importance: Given $f, g \in K[X]$ with $\deg(f) = m$, $\deg(g) = n$, define the linear map

$$\phi : K[X]_{<n} \times K[X]_{<m} \longrightarrow K[X]_{<m+n}$$

$$(s,t) \longmapsto sf + tg$$

and consider the following ordered bases

$\mathcal{B} = \left((X^{n-1}, 0), \dots, (1,0), (0, X^{m-1}), \dots, (0,1)\right)$ of $K[X]_{<n} \times K[X]_{<m}$

$\mathcal{B}' = \left(X^{m+n-1}, \dots, 1\right)$ of $K[X]_{<m+n}$

Then

$$[\phi]_{\mathcal{B}\mathcal{B}'} = \begin{bmatrix} a_m & & & b_n & \\ \vdots & \ddots & & & \ddots \\ a_0 & & a_m & & b_n \\ & \ddots & \vdots & \ddots & \vdots \\ & & a_0 & & b_0 \end{bmatrix} \begin{matrix} \\ \\ \\ \\ \\ \end{matrix} = S_{m,n}(f,g)$$

$\underbrace{\qquad\qquad}_{n}$ $\underbrace{\qquad\qquad}_{m}$

Therefore:

ϕ is an isomorphism $\iff$ $[\phi]_{\mathcal{B}\mathcal{B}'}$ is an isomorphism $\iff$ $\mathrm{Res}_{m,n}(f,g) \neq 0$

Theorem Let $f, g \in K[X]$ with $\deg(f) = m$, $\deg(g) = n$. Then

$$\mathrm{Res}_{m,n}(f,g) = 0 \iff \gcd(f,g) \neq 1 \iff f \text{ and } g \text{ share a root in } \overline{K}$$

Proof

$\mathrm{Res}_{m,n}(f,g) = 0 \iff \exists\, s,t \in K[X]$ not both 0

with $\deg(s) < n$ and $\deg(t) < m$ s.t. $sf + tg = 0$.

i.e. $sf = -tg$

($\Rightarrow$) $sf = -tg$ with $\deg(s) < n$ and $\deg(t) < m \Rightarrow$

$\gcd(f,g) \neq 1$ since $\gcd(f,g) = 1 \Rightarrow f \mid t$ and $g \mid s$,

a contradiction because $(s,t) \neq (0,0)$ and degrees ...

($\Leftarrow$) $\gcd(f,g) = h \neq 1 \Rightarrow \mathrm{lcm}(f,g) = \dfrac{f \cdot g}{h} = sf = -tg \Rightarrow$

$sf + tg = 0$

where $\deg(s) = \deg(g/h) < n$ and $\deg(t) = \deg(-f/h) < m$ ☒

Properties of the resultant

① $\exists\, s,t \in K[X]$ with $\deg(s) < n$ and $\deg(t) < m$ s.t.

$$\mathrm{Res}_{m,n}(f,g) = sf + tg$$

Moreover $\mathrm{Res}_{m,n}(f,g) = \det$

$$\begin{bmatrix} a_m & & & & b_n & & \\ \vdots & \ddots & & & & \ddots & \\ a_0 & & a_m & & b_n & & b_n \\ & \ddots & \vdots & & \vdots & & \vdots \\ & & a_0 & & b_0 & & b_0 \\ X^{n-1}f & \cdots & f & & X^{m-1}g & \cdots & g \end{bmatrix}$$

In particular $\mathrm{Res}_{m,n}(f,g) \in \langle f, g \rangle$

② Poisson formula Let $g = b_m(x-\beta_1)\cdots(x-\beta_m)$,

then $\mathrm{Res}_{m,n}(f,g) = (-1)^{mn} b_m^n \prod_{1\le i\le m} f(\beta_i)$

③ The theorem of resultant holds if one (but only one) of the leading coefficients of f and g vanishes:

$f = a_m x^m + \cdots + a_0$ with $a_m \neq 0$

$g = b_{n'} x^{n'} + \cdots + b_0$ with $n' < n$

Then $\mathrm{Res}_{m,n}(f,g) = a_m^{n-n'} \mathrm{Res}_{m,n'}(f,g)$

and therefore $\mathrm{Res}_{m,n}(f,g) = 0 \iff \mathrm{Res}_{m,n'}(f,g) = 0$

But if $a_m = 0$, $\mathrm{Res}_{m,n}(f,g) = 0$ and f, g may not share any root

④ Universal property

Let $F = A_m X^m + \cdots + A_0$, $G = B_n X^n + \cdots + B_0 \in \mathbb{Z}[\underline{A}, \underline{B}, X]$

Then $\mathrm{Res}_{m,n}(f,g) \in \mathbb{Z}[\underline{A}, \underline{B}]$ satisfies that

$\forall\, \underline{a} = (a_m, \cdots, a_0) \in K^{m+1}$ and $\underline{b} = (b_n, \cdots, b_0) \in K^{n+1}$ with $a_m \neq 0$ or $b_n \neq 0$, one has

$\mathrm{Res}_{m,n}(F,G)(\underline{a}, \underline{b}) = 0 \iff F(\underline{a}, X)$ and $G(\underline{b}, X)$ have a common root in $\overline{K}$

But actually this is not the right setting the right setting is by homogeneization

$F = A_m X^m + A_{m-1} X^{m-1} Y + \cdots + A_1 X Y^{m-1} + A_0 Y^m$

$G = B_n X^n + B_{n-1} X^{n-1} Y + \cdots + B_1 X Y^{n-1} + B_0 Y^n \in \mathbb{Z}[\underline{A}, \underline{B}, X, Y]$

homogeneous polynomials in (X, Y). Define

$\mathrm{Res}(F,G) = \mathrm{Res}_{m,n}(F(X,1), G(X,1)) \in \mathbb{Z}[\underline{A}, \underline{B}]$ (in fact bihomogeneous polynomial in $(\underline{A}, \underline{B})$ of degree n in $\underline{A}$ and m in $\underline{B}$)

Then $\mathrm{Res}(F,G) \in \langle F, G\rangle$ satisfies

$\forall\, \underline{a} \in \mathbb{P}^m(K)$, $\underline{b} \in \mathbb{P}^n(K)$,

$\mathrm{Res}(F,G)(\underline{a},\underline{b}) = 0 \iff F(\underline{a},X,Y)$ and $G(\underline{b},X,Y)$ have a common root in $\mathbb{P}^1(\overline{K})$

for if $a_m = b_n = 0$, then the common root is $(0:1)$ (root at ∞)

Comments

(1) All constructions hold starting with a domain A with fraction field K

(2) The resultant generalizes for $n+1$ homogeneous polynomials in $n+1$ variables in 1902 (Francis Macaulay, 1862-1937)

Let

$$F_0 = \sum_{|\alpha| = d_0} A_{0\alpha} X_0^{\alpha_0} \cdots X_n^{\alpha_n}, \ldots, F_n = \sum_{|\alpha| = d_n} A_{n\alpha} X_0^{\alpha_0} \cdots X_n^{\alpha_n} \in \mathbb{Z}[\underline{A}, \underline{X}]$$

be homogeneous polynomials in $\underline{X}$.

Then there exists a multihomogeneous polynomial

$\mathrm{Res}(F_0, \ldots, F_n) \in \mathbb{Z}[\underline{A}_0, \ldots, \underline{A}_n]$ of degree $\prod_{j \neq i} d_j$ in the var. $\underline{A}_i$;

which satisfies

$$\mathrm{Res}(F_0, \ldots, F_n) \in \langle F_0, \ldots, F_n\rangle$$

$\forall\, (\underline{a}_0) \in \mathbb{P}^{\binom{d_0+n}{n}-1}(K), \ldots, \forall\, (\underline{a}_n) \in \mathbb{P}^{\binom{d_n+n}{n}-1}(K)$, one has

$\mathrm{Res}(F_0, \ldots, F_n)(\underline{a}_0, \ldots, \underline{a}_n) = 0 \iff F_0(\underline{a}_0, \underline{X}), \ldots, F_n(\underline{a}_0, \underline{X})$ share a common root in $\mathbb{P}^n(\overline{K})$

There is a matrix construction for this resultant (but not as neat as in the case of 2 polynomials)

The discriminant

$$D(f) = \frac{1}{a_m} \mathrm{Res}(f, f')$$

III Back to the Nullstellensatz

1) Extension theorem for 2 polynomials

Let $I = \langle f, g \rangle \subseteq K[x_1, \dots, x_n]$ with $K = \overline{K}$

$I_1 = I \cap K[x_2, \dots, x_n]$

Write $f = a_d(x_2, \dots, x_n) x_1^d + \dots$ with $a_d \neq 0$

$g = b_e(x_2, \dots, x_n) x_1^e + \dots$ with $b_e \neq 0$

Suppose $\underline{x}' = (x_2, \dots, x_n) \in V(I_1) - V(a_d, b_e) \subseteq K^{n-1}$

Then $\exists x_1 \in K$ st $\underline{x} := (x_1, \underline{x}') \in V(I)$

Proof: $\mathrm{Res}_{d,e}(f, g; x_1) \in \langle f, g \rangle \cap K[x_2, \dots, x_n] = I_1$

$\Rightarrow \mathrm{Res}_{d,e}(f, g; x_1)(\underline{x}') = 0$

but since $a_d(\underline{x}') \neq 0$, or $b_e(\underline{x}') \neq 0$, one has

$\mathrm{Res}_{d,e}(f, g; x_1)(\underline{x}') = c \, \mathrm{Res}_{d',e'}(f(x_1, \underline{x}'), g(x_1, \underline{x}'))$

for $c \neq 0$, d', e' the correct degrees

Therefore $f(x_1, \underline{x}')$ and $g(x_1, \underline{x}')$ share a root in K:

$\exists x_1$ st $f(x_1, \underline{x}') = g(x_1, \underline{x}') = 0$. ☒

This generalizes to s polynomials considering for instance f_1 and $f := u_2 f_2 + \dots + u_s f_s$, where $u_2, \dots, u_s$ are new indeterminates.

2) Hilbert NSS proof: by induction on n.

- $n = 1$ ✓
- $n-1 \Rightarrow n$: by a linear change of variables (how?) we can assume f_1 is "monic" of degree ≥ 1 in x_1: ⊛ (Page 9')

$f_1 = c_d x_1^N + \dots$, $f_2, \dots, f_s$ where $c_1 \in K$

If $V(I_1) \neq \emptyset$, then $V(I) \neq \emptyset$ (since $c_1(x_2, \dots, x_n) = c_1 \in K$)

Therefore $V(I) = \emptyset \Rightarrow V(I_1) = \emptyset \Rightarrow 1 \in I_1 = I \cap K[x_2, \dots, x_n]$

$\Rightarrow 1 \in I$ ☒

3) "Weak" and "strong" NSS :

Weak NSS : $V(I) = \emptyset \iff 1 \in I$ $\quad (K = \overline{K})$

Strong NSS : If $f \in K[x_1, \dots, x_n]$ satisfies $f|_{V(I)} = 0$,
then there exists $N \in \mathbb{N}$ st $f^N \in I$

Strong NSS $\Rightarrow$ Weak NSS :

$$V(I) = \emptyset \Rightarrow 1|_{V(I)} = 0 \Rightarrow 1 = 1^N \in I$$

Weak NSS $\Rightarrow$ Strong NSS : Rabinowitsch trick (1929)

- $f^N \in I \Rightarrow f|_{V(I)} = 0$ ✓
- $f|_{V(I)} = 0$. Consider a new variable Y and the ideal

$J := I + \langle 1 - Y f(x) \rangle \subset K[x, Y]$

Then $V(J) = \emptyset$ since $(x, y) \in V(J) \Rightarrow x \in V(I)$
$\Rightarrow f(x) = 0$ and therefore $\nexists y$ st $1 - y f(x) = 0$

By the weak NSS, $1 \in J$:

$$1 = g_1(x, Y) f_1(x) + \dots + g_s(x, Y) f_s(x) + g(x, Y)\,(1 - Y f(x))$$

Specializing $Y \mapsto 1/f(x)$ gives

$$1 = g_1\left(x, \frac{1}{f(x)}\right) f_1(x) + \dots + g_s\left(x, \frac{1}{f(x)}\right) f_s(x)$$

And thus taking a common denominator gives

$$f(x)^N = \tilde{g}_1(x) f_1(x) + \dots + \tilde{g}_s(x) f_s(x)$$

□

→ (9.1)

Bezout theorem

Change of variables (for NSS)

Assume $\deg(f) = N$, and $f_N = \sum_{|\alpha|=N} c_\alpha X_1^{\alpha_1} \dots X_n^{\alpha_n}$ is it homogeneous part of degree N

Consider the change of variables

$$\begin{cases} X_1 = \tilde{X}_1 \\ X_2 = \tilde{X}_2 + a_2 \tilde{X}_1 \\ \vdots \\ X_n = \tilde{X}_n + a_n \tilde{X}_1 \end{cases} \quad \text{then}$$

$$f_N(\underline{X}) = \tilde{f}_N(\underline{\tilde{X}}) = \left(\sum_{|\alpha|=N} c_\alpha a_2^{\alpha_2} \dots a_n^{\alpha_n} \right) \tilde{X}_1^N + \dots$$

where $\sum c_\alpha \tilde{X}_2^{\alpha_2} \dots \tilde{X}_n^{\alpha_n} \neq 0$ (why?)

and therefore $\exists (a_2, \dots, a_n) \in \mathbb{C}^{n-1}$ s.t. $\sum c_\alpha a_2^{\alpha_2} \dots a_n^{\alpha_n} \neq 0$

$\Rightarrow \tilde{f}$ is monic in X_1

---

(3) Bézout theorem (Etienne Bézout)

Classic statement: Let $f, g \in \mathbb{C}[X, Y]$ two curves with no common factor, then $V(f, g)$ is finite, and

$$\#(V(f,g)) \leq \deg(f) \deg(g)$$

Modern statement: Let $f, g \in \mathbb{C}[X, Y, Z]$ two homogeneous polynomials with no common factor, then

$V_{\mathbb{P}^2(\mathbb{C})}(f, g)$ is finite, and $\#(V(f,g)) = \deg(f) \deg(g)$

where each pt in V is given the correct multiplicity

In general: Let $f_1, \dots, f_n \in \mathbb{C}[X_0, \dots, X_n]$ be homogeneous polynomials such that $V(f_1, \dots, f_n) \subseteq \mathbb{P}^n(\mathbb{C})$ is finite,

then $V_{\mathbb{P}^n(\mathbb{C})}(f_1, \dots, f_n) = \prod_{i=1}^{n} \deg(f_i)$ (with correct multiplicities)

We prove via resultants the classic statement (M. Waldschmidt 9" 2004)

Let $f(X,Y), g(X,Y) \in \mathbb{C}[X,Y]$ of d° m, n.

① By a linear change of variables we can assume that f (or g) has a constant leading coefficient in Y, and also that if $\{(x_1,y_1), \dots, (x_t,y_t)\}$ is a set of $\neq$ pts in $V_{\mathbb{C}}(f,g)$, then $x_i \neq x_j$ (for $i \neq j$).

Since if not consider $Q(z) = \prod_{1 \le i < j \le t} \left((x_i - x_j) + z(y_i - y_j) \right)$

which is non-zero (why?): $\exists\, \lambda \in \mathbb{C}$ st $Q(\lambda) \neq 0 \Rightarrow$

$x_i + \lambda y_i \neq x_j + \lambda y_j$, $\forall i \neq j$

and then consider the polynomials $\tilde{f}(X,Y) = f(X - \lambda y, Y)$ ...

② Then $t = \#\{x_i\}$

Consider $\mathrm{Res}_Y(f(X,Y), g(X,Y))$.

We have, since f is "monic" in Y, that

① $\mathrm{Res}_Y(f(X,Y), g(X,Y))(x_i) = \mathrm{Res}_Y(f(x_i,Y), g(x_i,Y))$

$= 0$ since $f(x_i,Y)$ and $g(x_i,Y)$ have a common root

② but $\mathrm{Res}_Y(f(X,Y), g(X,Y)) \in \mathbb{C}[X]$ is non-zero

since $f(X,Y), g(X,Y)$ do not have a common non-trivial factor in $\mathbb{C}(X)[Y]$ (they would have a common non-trivial factor in $\mathbb{C}[X,Y]$)

So $\#\{x_i\} = t \le \deg \mathrm{Res}_Y(f(X,Y), g(X,Y))$

It suffices to show that

$\deg \mathrm{Res}_Y(f,g) \le mn$ if $\deg(f) = m$ & $\deg(g) = n$

$f = a_m(x) y^m + \dots + a_0(x)$, $g = b_n(x) y^n + \dots + b_0(y)$

To simplify the argument we homogeneite f and g,

so that $F = A_m y^m + \dots + A_0$, $G = B_n y^n + \dots + B_0$

where $A_k, B_j \in \mathbb{C}[x,z]$ homogeneous of degrees $m-k$ (resp $n-j$)

And we show that $\mathrm{Res}_y(F,G)$ is a homogeneous pol. of degree mn, showing that $\mathrm{Res}_y(F,G)(tx,tz) = t^{mn}\mathrm{Res}_y(F,G)(x,t)$

(we recover $\mathrm{Res}(f,g)$ setting $z=1$)

$$\mathrm{Res}_y(F,G)(x,z) = \det \begin{bmatrix} A_m & & & B_n & & \\ \vdots & \ddots & & B_0 & \ddots & \\ A_0 & & A_m & & & B_n \\ & \ddots & \vdots & & \ddots & \vdots \\ & & A_0 & & & B_0 \end{bmatrix}$$

$$\Rightarrow \mathrm{Res}_y(F,G)(tx,tz) = \det \begin{bmatrix} A_m & & & B_n & & \\ tA_{m-1} & \ddots & & t^n B_0 & \ddots & \\ t^m A_0 & & A_m & & & B_n \\ & \ddots & \vdots & & \ddots & \vdots \\ & & t^m A_0 & & & t^n B_0 \end{bmatrix}$$

Multiply the 1st column by 1, the 2nd col by t, ..., the m-th column by t^{m-1}, the $(m+1)$-col by 1, ..., the last column by t^m:

You get $t^{1+\dots+m-1} \cdot t^{1+\dots+m-1} \mathrm{Res}_y(F,G)(tx,tz) =$

$$\det \begin{bmatrix} A_m & 0 & & B_n & & \\ tA_{m-1} & tA_m & & tB_{n-1} & tB_n & \\ & t^2 A_{m-1} & & & & \\ t^m A_0 & & & & & t^{m+n-1} B_0 \\ & t^{m+1} A_0 & & & & \\ & & t^{m+n-1} A_0 & & & \end{bmatrix}$$

$$= t^{1+\dots+m+n-2} \mathrm{Res}_y(f,g)(x,y)$$

$$\frac{(m+n)(m+n-1)}{2} - \frac{m(m-1)}{2} - \frac{n(n-1)}{2}$$

$$\Rightarrow \mathrm{Res}(tx,tz) = t^{\frac{2mn}{2}} \mathrm{Res}(x,z)$$

exponent: $\dfrac{m^2+n^2+2mn-m-n-m^2+m-n^2+n}{2} = \dfrac{2mn}{2} = mn$