On a simple proof of Nullstelensatz

Vladimir Dotzenko wrote the article [1] where he described a simple proof of Nullstellensatz for the field **C** of complex numbers. As it is claimed in this article, this proof is "a part of mathematical folklore". (The standard proof of this Theorem possesses a "difficult part". (See e.g. the excellent book "Algebraic geometry for pedestrians" of Miles Read [2].))

I would like to retell this proof, paying little bit more attention on its crucial non-standard part.

Theorem 1 Let $M = \{f_1, f_2, \dots, f_k\}$ be a set of polynomials in the ring of polynomials of n complex variables.

Then or these polynomials have common root or there exist polynomials $g_1, \dots, g_n$ (over complex numbers) such that $f_1 g_1 + \dots + f_k g_k \equiv 1$.

In other words an ideal I generated by polynomials $\{f_1, f_2, \dots, f_k\}$ in the ring $\mathbf{K} = \mathbf{C}[x_1, \dots, x_n]$ of polynomials on $\mathbf{C}^n$ equals to $\mathbf{K}$ if these polynomials have not common root.

It is famous Hilbert's *Nullstelensatz.*

One can consider another formulation of this theorem:

Theorem 1′ Let $M = \{f_1, f_2, \dots, f_k\}$ be a set of polynomials over complex numbers. Then if for an arbitrary polynomial $F \in \mathbf{K}$ set of common roots of polynomials $\{f_1, f_2, \dots, f_k\}$ belongs to the set of roots of polynomial F:

$$f_1(x_0) = f_2(x_0) = \dots = f_n(x_0) \Rightarrow F(x_0) = 0\,,$$

then there exists natural m such that F^m belongs to the ideal $I = (f_1, \dots, f_n)$.

This Theorem is equivalent to previous one (see any standard textbook)

The proof of the Theorem 1 follows from the following

Lemma Let $\mathbf{K} : \mathbf{C}$ be a field extension of the field **C**. Let $\{a_i\}$ $(i = 1, 2, 3, \dots)$ be a set of elements of **K** such that the span of these elements over **C** is **K**, i.e. for an arbitrary $x \in \mathbf{K}$ there exists a finite set $\{a_{i_1}, \dots, a_{i_p}\}$ such that $x = \lambda_1 a_{i_1} + \lambda_2 a_{i_2} + \dots + \lambda_p a_{i_p}$. Then $\mathbf{K} = \mathbf{C}$.

In other words an arbitrary field **K** which is an extension of the field **C** of complex numbers coincides with **C** *or* degree of the extension is uncountable*.

Theorem follows from the lemma by means of the following standard textbook considerations:

Proof (of Theorem 1'). Let $I = (f_1, \dots, f_n)$ be an ideal generated by the polynomials $\{f_1, \dots, f_n\}$.

Suppose $I \neq \mathbf{C}[x_1, \dots, x_n]$. Consider the maximal ideal J ($J \neq \mathbf{K}$) in $\mathbf{C}[x_1, \dots, x_n]$ which contains I and a field $\mathbf{L} = \mathbf{C}[x_1, \dots, x_n] \backslash J$.

Consider the countable set of polynomials (e.g. polynomials $\{x_1^{m_1} x_2^{m_2} \dots x_k^{m_k}\}$ which span the ring $\mathbf{C}[x_1, \dots, x_n]$. Hence equivalence classes of these polynomials span the field $\mathbf{L} = \mathbf{C}[x_1, \dots, x_n] \backslash J$. It follows from the lemma that the field **L** is isomorphic to the field **C** of complex numbers. Let $a_i \in \mathbf{C}$ be the image of equivalence class $[x_i]$ of monomial x_i. Since $f_i \in J$ image of an equivalence class of polynomial f_i is equal to zero. Hence the point $x_i = a_i$ is a common root of polynomials $\{f_i\}$. x_i. Contradiction.

Now we go to the central part of this topic, we prove the **Lemma**.

Proof of the **Lemma**

Let field extension $\mathbf{K} : \mathbf{C}$ be spanned by the countable set of vectors $\{a_i\}$ $(i = 1, 2, 3, \dots)$.

Prove that for arbitrary $\theta \in \mathbf{K}$, $\theta \in \mathbf{C}$.

Consider the following uncountable set of elements in **K**:

$$\mathcal{M} = \left\{ \frac{1}{\theta - z} \right\}\,,$$

* In the paper [2] author gives this second formulation equivalent formulation of the lemma:

We prefer the first formulation above , since the case when algebraic dimension is more than finite could be little bit confusing for a reader.

where the set z runs over all complex numbers except a number θ (if $\theta \in \mathbf{C}$). (If $\theta \in \mathbf{C}$ we have nothing to prove but we consider this case too.)

Claim: There exists a finite subset of elements in $\mathcal{M}$ which are linear dependent elements (over $\mathbf{C}$.)

This claim implies the lemma. Indeed let $\left\{\frac{1}{\theta - z_i}\right\}$ be a finite subset of linear dependant vectors, i.e.

$$\sum_i \frac{c_i}{\theta - z_i} = 0\,,$$

where all coefficients $\{c_i\}$ are complex numbers and at least one of the complex numbers c_i is not equal to zero. This is an algebraic equation on θ over algebraically closed field $\mathbf{C}$. Hence $\theta \in \mathbf{C}$.

It remains to prove the claim.

Denote by $\mathbf{K}_r$ the span of the first r vectors $\{a_1, a_2, \ldots, a_r\}$. We have a sequence of $\{\mathbf{K}_k\}$ of finite-dimensional space $\mathbf{K}_1 \subseteq \mathbf{K}_2 \subseteq \ldots \mathbf{K}_i \subseteq \mathbf{K}_{i+1} \subseteq \ldots$ and $\cup_{r=1}^{\infty} \mathbf{K}_r = \mathbf{K}$.

Consider the subsets $\mathcal{M}_k = \mathcal{M} \cap \mathbf{K}_r$. At least one of these subsets, say $\mathcal{M}_k$ possesses infinite number of elements (in fact incountable number of elements) since the set $\mathcal{M} = \cup_k \mathcal{M}_k$ is uncountable. The infinite subset $\mathcal{M}_k$ belongs to finite-dimensional space $\mathbf{K}_k$. We see that there exists $N+1$ linear dependent elements $\left\{\frac{1}{\theta - z_i}\right\}$ $(i = 1, z \ldots, N+1)$ in $\mathbf{K}_k$ (N is dimension of the space $\mathbf{K}_k$). Claim is proved.

References

[1] V. Dotzenko "On a proof of Hilbert Nullstelensatz Theorem", *Matematicheskoje prosveshenije, 3, v6, pp.116—118, (2002)* (in Russian)

[2]