THE NULLSTELLENSATZ WITHOUT NOETHER NORMALISATION

Here is some terminology (which is standard in EGA but less standard in popular commutative algebra books). Let A be a ring and fix an A-algebra B. Note that there is an obvious A-module structure on B.

We say B is *finite* over A if the A-algebra B is finitely generated as an A-module. In other words there is a surjective map of A-modules

$$A^m \longrightarrow\!\!\!\!\!\rightarrow B.$$

Here, as always, the two headed right arrow " $\twoheadrightarrow$ " denotes a surjective map. A^m is the direct sum of m-copies of A.

We say that B is a *finite type* algebra over A if B is finitely generated as an A-algebra, i.e. B is of finite type over A if the natural map $A \to B$ giving B its A-algebra structure is a composite of ring homomorphisms of the form

$$A \xrightarrow{\text{natural}} A[X_1, \ldots, A_n] \longrightarrow\!\!\!\!\!\rightarrow B.$$

In other words, we have elements $b_1, \ldots, b_n$ in B such that every element of B can be written as a polynomial of the form $\sum_{\boldsymbol{\nu}} a_{\boldsymbol{\nu}} b_1^{\nu_1} \ldots b_n^{\nu_n}$, with $\boldsymbol{\nu} = (\nu_1, \ldots, \nu_n)$ varying in n-tuples of non-negative integers, $a_{\boldsymbol{\nu}}$ varying in A and such that all but a finite number of the $a_{\boldsymbol{\nu}}$ are zero.

It is clear that if B is finite over A, then it is of finite type over A.

1. The Nullstellensatz

1.1. **Artin-Tate.** The key to an elementary proof of Hilbert's Nullstellensatz is the the *Artin-Tate Lemma.*

Theorem 1.1.1. (The Artin-Tate Lemma) *Let $A \to B \to C$ be ring homomorphisms with $B \to C$ an inclusion. Suppose A is noetherian, and C a finite type algebra over A. If C is finite over B then B is of finite type over A.*

Proof. Let $c_1, \cdots, c_n \in C$ be a set of generators for C as an A-algebra. Let $\gamma_1, \ldots, \gamma_m$ be generators of C as a B-module. We have $b_{ij} \in B$, $1 \leq i \leq n$, $1 \leq j \leq m$ such that

$$c_i = \sum_{j=1}^{m} b_{ij}\gamma_j \qquad i = 1, \ldots, n. \tag{1.1.1.1}$$

We also have $\beta_{ijk} \in B$, $i, j, k = 1, \ldots, m$ such that

$$\gamma_i\gamma_j = \sum_{k=1}^{m} \beta_{ijk}\gamma_k \qquad i, j = 1, \ldots, m. \tag{1.1.1.2}$$

Let B_0 be the A-subalgebra of B generated by the b_{ij} and the β_{ijk}. Then B_0 is of finite type over A. By the *Hilbert Basis Theorem*, B_0 is Noetherian, since A is Noetherian.[1]

[1]See Theorem 2.1.1 of https://www.cmi.ac.in/~pramath/AGI/notes/hilb-basis.pdf.

We claim that C is a finite B_0 module. Indeed, given an element $c \in C$, it can be as a polynomial $p(c_1, \ldots, c_n)$ in $c_1, \ldots, c_n$ with coefficients in A, and whence by (1.1.1.1) as a polynomial in $\gamma_1, \ldots, \gamma_m$ with coefficients in the A-algebra generated by the b_{ij} defined above. Now any monomial in the γ_j can be written (using the relations in (1.1.1.2)) as a linear combination in the γ_j with coefficients in the A-algebra generated by the β_{ijk}. Putting these facts together, we see that c can be written as a linear combination of the γ_j with coefficients coming from B_0. This proves the claim for we have just shown that $\gamma_1, \ldots, \gamma_m$ are B_0-module generators for C.

Now B is a B_0-submodule of C, and since B_0 is Noetherian, and C is finite over B_0, therefore B is finite over B_0. It follows it is of finite type over B_0 whence over A. □

1.2. **Two lemmas.** The following lemma is useful in proving the Nullstellensatz.

Lemma 1.2.1. *Suppose k is a field, and t an element in a field extension of k which is transcendental over k. Then $k(t)$ is not a finite type $k[t]$-algebra.*

Proof. Since t is transcendental over k, $k[t]$ is the polynomial ring in one variable over k. Suppose $k(t)$ is of finite type over the polynomial ring $A = k[t]$. Let $b_1, \ldots, b_n \in k(t)$ be A-algebra generators for $k(t)$, say $b_i = a_i(t)/q_i(t)$, where $a_i(t)$ and $q_i(t)$ are in $k[t]$ with $q_i(t)$ non-zero. Since $k[t]$ has an infinite number of irreducible polynomials, we can find an irreducible polynomial $p(t) \in k[t]$ such that $p(t)$ is not a factor of any of the q_i, $i = 1, \ldots, n$. Since $b_1, \ldots, b_n$ generates $k(t)$ as an A-algebra, therefore $1/p(t)$ is a polynomial in $b_i = a_i(t)/q_i(t)$, $i = 1, \ldots, n$ with coefficients from A. This is not possible since $p(t)$ does not divide any of the $q_i(t)$. Thus $k(t)$ is not of finite type over $k[t]$. □

The following is also sometimes called the Nullstellensatz since it is essentially equivalent to (Zariski's version of) the Nullstellensatz.

Lemma 1.2.2. (Zariski's Lemma) *Let $k \to L$ be an extension of fields such that L is of finite type over k. Then L is finite over k.*

Proof. First note that if K is a field of the form $k[\theta]$ where θ is algebraic over k, then K is finite over k, since $1, \beta, \ldots, \beta^{d-1}$ is a k-vector space basis for K, where d is the degree of the irreducible polynomial of β. By iterating this process we see that if $K = k[\beta_1, \ldots, \beta_n]$ with every β_i algebraic over k, then K is finite over k. Thus if L is as in the hypothesis of the theorem, it is enough for us to prove that L is algebraic over k.

Suppose L is not algebraic over k. Using a transcendence basis, we have a tower of field extensions $k \subset K \subset L$ with K purely transcendental over k and L algebraic over K. In other words, K is isomorphic to the quotient field $k(X_\lambda \mid \lambda \in \Lambda)$ of a polynomial ring $k[X_\lambda \mid \lambda \in \Lambda]$ in possibly infinite number of variables (see Section 9.26 of [SP]). In fact the number of these variables is finite as the proof of Lemma 9.26.3 in [SP] shows (see the first paragraph of *loc.cit.* and let G be the finite set of generators of L over k). Thus we have $x_1, \ldots, x_m \in L$ which are algebraically independent, such that L is algebraic over $K = k(x_1, \ldots, x_m)$. By the Hilbert basis theorem (see e.g. Theorem 2.1.1 of the notes here), we see that K must be of finite type over k since L is of finite type over k. In particular, K must be of finite type over $k(x_1, \ldots, x_{m-1})[x_m]$. By Lemma 1.2.1 we have a contradiction since $K = k(x_1, \ldots, x_{m-1})(x_m)$. □

1.3. **Hilbert's Nullstellensatz.** The Nullstellensatz says that the zero set of a proper ideal of a polynomial ring over an algebraically closed field is non-empty. This is sometimes called the *weak Nullstellensatz*, but it is equivalent to the seemingly stronger version, which we will give later, and also equivalent to the seemingly weaker Zariski's lemma above.

Theorem 1.3.1. (Hilbert's Nullstellensatz-I) *Let k be an algebraically closed field, $A = k[X_1, \ldots, X_n]$ a polynomial ring in n-variables, with $n \geq 1$, and I a proper ideal of A. Then there exists at least one point $\boldsymbol{x} = (x_1, \ldots, x_n) \in k^n$ such that $f(\boldsymbol{x}) = 0$ for all $f \in I$.*

Proof. Let $\mathfrak{m}$ be a maximal ideal of A containing I. Then $L = A/\mathfrak{m}$ is of finite type over k, since it is a homomorphic image of the finite type k-algebra A. By Zariski's lemma, i.e. Lemma 1.2.2, the field extension $k \to L$ is finite. Since k is algebraically closed, this field extension is an isomorphism. Denote this isomorphism by $\psi\colon k \xrightarrow{\sim} L$ and let $\varphi = \psi^{-1}$. For $i \in \{1, \ldots, n\}$, let $\zeta_i \in L$ be the image of X_i under the surjective ring homomorphism $A \twoheadrightarrow A/\mathfrak{m} = L$ and let $x_i = \varphi(\zeta_i)$ and let $\boldsymbol{x} = (x_1, \ldots, x_n) \in k^n$. Clearly

$$X_i - x_i \in \mathfrak{m}$$

for $i = 1, \ldots, n$.

Let $f \in \mathfrak{m}$, say $f = \sum_{\boldsymbol{\nu}} c_{\boldsymbol{\nu}} X_1^{\nu_1} \ldots X_n^{\nu_n}$ with $c_{\boldsymbol{\nu}} \in k$. Then expanding f as a polynomial over k in the $X_i - x_i$ we get

$$f = f(\boldsymbol{x}) + \sum_{\boldsymbol{\mu}} d_{\boldsymbol{\mu}} (X_1 - x_1)^{\mu_1} \ldots (X_n - x_n)^{\mu_n}$$

where the $d_{\boldsymbol{\mu}} \in k$ and the index $\boldsymbol{\mu}$ is runs through n-tuples $(\mu_1, \ldots, \mu_n)$ of non-negative integers whose components are not all zero. Since f and $X_i - x_i$ lie in $\mathfrak{m}$ it follows that $f(\boldsymbol{x}) \in \mathfrak{m}$. This forces the relation $f(\boldsymbol{x}) = 0$, else $\mathfrak{m}$ would contain a unit, which is not possible since $\mathfrak{m}$ is a proper ideal. Thus all elements of $\mathfrak{m}$ vanish at $\boldsymbol{x} = (x_1, \ldots, x_n)$. Since $I \subset \mathfrak{m}$, we are done. □

1.3.2. Note that the argument towards the end shows that if $f \in \mathfrak{m}$ then $f \in \langle X_1 - x_1, \ldots, X_n - x_n \rangle$. Since $\mathfrak{m}$ is a maximal ideal, we have actually shown that $\mathfrak{m} = \langle X_1 - x_1, \ldots, X_n - x_n \rangle$, provided k is algebraically closed. This observation too is sometimes called Hilbert's Nullstellensatz.

1.3.3. The radical of an ideal. If A is a ring and I an ideal of A then *the radical* $\sqrt{I}$ of I is defined to be the set of elements $f \in A$ such that $f^n \in I$ for some $n \geq 0$ It is clear that $\sqrt{I}$ is an ideal of A. If I is a proper ideal, then I is contained in some maximal ideal, proving that that in this case $\sqrt{I}$ is a proper ideal of A.

There is a famous characterisation of $\sqrt{I}$. Let $V(I)$ be the set of prime ideals in A containing I, then

$$\sqrt{I} = \bigcap_{\mathfrak{p} \in V(I)} \mathfrak{p}. \tag{1.3.3.1}$$

A simple proof is as follows. If $I = A$ then both sides equal I since $V(I) = \emptyset$. Otherwise we proceed as follows. Since ideals of A/I are in one to one correspondence with ideals of A containing I and since prime ideals of A/I under this correspondence correspond to elements of $V(I)$, therefore by replacing A by A/I if necessary, we may assume $I = 0$ and we have to show that $\cap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$ is the ideal of nilpotent elements of A.

It is clear that every nilpotent element of A is in $\cap_{\mathfrak{p}\in\operatorname{Spec} A}\mathfrak{p}$. So suppose $f \in A$ is not a nilpotent element. Then A_f is a non-zero ring, else $1/1 = 0$, which means $f^n = 0$ for some $n \geq 0$. Since A_f is non-zero it has a prime ideal $\mathfrak{q}$. Let $\mathfrak{p}$ be the inverse image of $\mathfrak{q}$ under the natural map $A \to A_f$. Then $\mathfrak{p} \in \operatorname{Spec} A$ and $f \notin \mathfrak{p}$.

The following theorem is also called the Nullstellensatz. It is sometimes called the "strong Nullstellensatz" though it is no stronger than other versions of the theorem.

Theorem 1.3.4. (Hilbert's Nullstellensatz-II) *Let k be an algebraically closed field, and I a proper ideal of $A = k[X_1, \ldots, X_n]$, where $n \geq 1$. Let*

$$\mathfrak{V}(I) = \{\boldsymbol{x} \in k^n \mid g(\boldsymbol{x}) = 0 \text{ for all } g \in I\}.$$

If $f \in A$ is such that $f(\boldsymbol{x}) = 0$ for all $\boldsymbol{x} \in V(I)$, then there exists a positive integer m such that $f^m \in I$. In other words $f \in A$ vanishes at all points of $\mathfrak{V}(I)$ if and only if $f \in \sqrt{I}$.

Proof. Suppose $f \in A$ is such that $f^m \notin I$ for any positive integer m. By (1.3.3.1), there exists a prime ideal $\mathfrak{p}$ of A containing I such that $f \notin \mathfrak{p}$. Let $B = (A/\mathfrak{p})_f$. Then B is a finitely generated k-algebra since $B = ((A/\mathfrak{p})[Y])/\langle fY - 1\rangle$. Let $\mathfrak{m}$ be a maximal ideal of B and for $i = 1, \ldots, n$, let x_i be the image of X_i under the composite $A = k[X_1, \ldots, X_n] \twoheadrightarrow A/\mathfrak{p} \to B \to B/\mathfrak{m}$. By Zariski's lemma, i.e. Lemma 1.2.2, x_i may be regarded as elements of k since k is algebraically closed. It is clear that $f(x_1, \ldots, x_n) \neq 0$. □

References

[Ku] E. Kunz *Introduction to Commutative Algebra and Algebraic Geometry*, Birkhaüser, Boston, Basel, Berlin, 1985.

[SP] The Stacks project authors, *TheStacks project*, https://stacks.math.columbia.edu, 2021.