William Bae

Preliminary Work on the Nullstellansatz:

Algebraic vs. Transcendental:

We will first look at this setting in the traditional sense. We first take our base field as the rational numbers and we know that some numbers (not rational) can be gotten by solving some equation. Think first about the complex numbers and note that every equation has a solution there, but not every equation has a solution in the rationals. Now consider the equation: $x^2 - 2 = 0$, for example, which has no solution in the rationals and this yields two solutions that fall between the rationals and the complex numbers, in particular, $\sqrt{2}$ and $-\sqrt{2}$. These numbers are said to be algebraic.

Making a few observations before we move on, we note that there are infinitely many algebraic numbers because there are infinitely many equations that we can write and moreover, this infinity is countable. Here is the idea. Suppose some equation in the rationals and make every coefficient an integer by clearing denominators. Now, order your equations by the size of the integers and the degree, which allows you to arrange the equations in a countable list as well as the roots of each equation.

It is easy to show that the algebraic numbers form a field (I'm not going to do it, but this just amounts to showing that the field axioms hold.). We now ask: Can all algebraic numbers be written simply (in terms of radicals)? The answer is no and the counter examples come about when considering polynomials of degree 5, so you have algebraic numbers that can be expressed as radicals and algebraic numbers for which we can only express as a "root of" something.

We now talk about non-algebraic numbers, which are the transcendentals. This gives rise to an interesting situation where the transcendentals make up everything between the countable algebraics and the complexes, yet it is very difficult to prove a number is transcendental (this amounts to showing that a number is not a solution to any polynomial equation.).

Consider the following, suppose k is a field and let A be both a commutative ring and a k-vector space. An example of this is the matrices. Take 2x2 matrices over the rationals for example, and note that they form a ring, but we can also scale them by rational numbers. Another example is the ring of polynomials with coefficients in k, $A = k[x]$, which can be thought of as a k-vector space. Note here that the set $\{1, x, x^2, x^3, ...\}$ is linearly independent so we see that

$dim_k A = \infty$. Suppose now some $a \in A$ and we want to make a ring homomorphism $k[X] \to A$, which just sends $f(x)$ to $f(a)$ which is just an element of a. We can call this ev_a and we can ask for its kernel. We're taking every polynomial and we plug in a and the kernel is the set of polynomials that vanish at a.

So we write: $ker(ev_a) = \{Polynomials\ such\ that f(a) = 0\} = I(\{a\})$.

Note that this ideal is principal because we're in the space of polynomials in one variable so we can also write: $ker(ev_a) = < f_a >$, where f_a is some element of the ring of polynomials. Consider the case now when $f_a = 0$. This means that there is no polynomial having a as a root. So a is transcendental if and only if $f_a = 0$. Since the image under our transformation is just the polynomials in a and since the kernel is 0, we also point out that $k[a]$ is isomorphic to $k[x]$ in this setting. So if you have some transcendental number and evaluate polynomials of that number, you get the same structure as if you evaluated polynomials of x.

Now we look at the other equivalence. We see that a is algebraic if and only if $f_a \neq 0$. It is not hard to show also that f_a is irreducible. Notice that if f_a weren't, there would be a factor that is 0 at a, which implies that there would be a lower degree polynomial. So, f_a is irreducible and is the minimal polynomial for a. We add also that in this algebraic case, $k[a] \approx k[x]/ < f_a >$. Pushing further, look at our ring of polynomials of a, $k[a]$ and notice that for any $\alpha \in k[a]$, α is some linear combination of $\{1,\ a,\ a^2,\ a^3,\ ...\}$. So how many of these terms do we need to take? If $deg(f_a) = n,$ then as soon as we see some a^n term, we know that the polynomial is zero for some linear combination. Formalizing this, we observe that $\{1,\ a,\ a^2, ...,\ a^{n-1}, a^n\}$ is linearly dependent. Since f_a is minimal, we also get that $\{1,\ a,\ ...,\ a^{n-1}\}$ is linearly independent. So we see that there is a connection between a being algebraic and $k[a]$ being finite dimensional. We make a final comment that we can actually describe a ring as being algebraic in the following sense: A is algebraic over k if every $a \in A$ is algebraic over k. This idea of knowing when something is algebraic and when it's not will be crucial in proving the Nullstellansatz.

We now go over the different meanings of being "finitely generated". In the context of Linear Algebra, when we talk about being finitely generated, it implies that we have finitely many elements and everything can be gotten by taking linear combinations of those elements. In the context of a ring, we can think of being finitely generated in different ways. Let's entertain the question: Is $k[x]$ finitely generated? One answer to this question is **no** because there is no finite k-linear spanning set. In other words, $k[x]$ is infinite dimensional over k. This is the answer in the Linear Algebra sense. The other way to answer this is **yes** because $k[x]$ is generated by x. Since we're in a ring, we can think about multiplying elements together which gives us elements of the set, $\{1,\ x,\ x^2,\ x^3,\ ...\}$ and when we consider the smallest ring containing these elements, that just gives us the polynomials in x. When we talk about ideals, the idea of being finitely generated boiled down to having finitely many elements and getting all elements by multiplying and adding without squaring generators. We will use the following definition.

Suppose some ring $R \subset A$. We say that A is $R-finite$ if it's finitely generated in the Linear Algebra sense. In other words, if there exist generators $a_1, a_2, ..., a_k$ such that $Ra_1 + Ra_2 + ... + Ra_k = A$. We say A is finitely generated over R if there is a surjective ring homomorphism $R[x_1, ..., x_n] \to A$. What this tells us is that any element in A can be gotten by choosing where these n $x's$ go. One more note, if you look at the kernel of this ring homomorphism, it makes A be a quotient of the ring of polynomials. By modding out R by the kernel of our ring homomorphism and the result is isomorphic to A. So we say that being finitely generated as a ring over R means being a quotient of a ring of polynomials. We now come upon the "Big Hard Theorem" which will make proving the Nullstellansatz easy.

Big Hard Theorem: Suppose A is finitely generated over a field k. Then
$A\ is\ a\ field\ \Rightarrow A\ is\ algebraic\ over\ k$**.**

The idea is that for A to be algebraic over k, this means that elements in A when plugged into polynomials results in something finite dimensional. If A is also a field however, that means we can invert. So if A isn't algebraic and you take powers of $1/a$, we start to see that we're going to need infinitely many elements. We can start to see how things fall apart if A is not algebraic.
A canonical example is let $A = k[x]$ and we ask, is this finitely generated over $k[x]$? The answer is no because we would have to be able to put every possible irreducible polynomial in the denominator, but there are infinitely many of those. So it's impossible to get $k(x)/k[x]$ by inverting finitely many polynomials.

In the book, the statement of this theorem is in 3.8 and the proof takes place in 3.12-3.15. We will see that the main application is taking A to be the complex numbers and showing the complex numbers are algebraic. The other tool we will need is the Noether Normalization Theorem.