1 Nullstellensatz

1.1 Finite generation

Let R be a commutative ring with 1.

An *R-module* is an abelian group M that admits left multiplication by elements from R, where this multiplication is associative and distributive over addition.

The module M is called *module-generated* over R by a subset N if each element $m \in M$ has a representation $m = \sum r_i n_i$ with $r_i \in R$ and $n_i \in N$.

In other words, M is module-generated over R by a subset N if M is the smallest R-submodule of M containing N.

The module M is called *module-finite* over R if M is module-generated over R by a finite subset N.

Now let S be a commutative ring containing the ring R. The ring S is called *ring-generated* over R by a subset T if each element $s \in S$ has a representation $s = \sum r_i z_i$ with $r_i \in R$ and each z_i a monomial over T, that is, of the form $t_1^{e_1} ... t_m^{e_m}$ for certain $t_1, ..., t_m \in T$ and nonnegative integers $e_1, ..., e_m$.

In other words, S is ring-generated over R by a subset T if S is the smallest subring of S containing R and T.

The ring S is called *ring-finite* over R if S is ring-generated over R by a finite subset T.

For example, a finite-dimensional vector space V over a field k is module-finite over k. And a polynomial ring $k[x_1, ..., x_n]$ in finitely many variables is ring-finite over k.

Lemma 1.1 *Let $R \subseteq S \subseteq T$ be commutative rings. If T is module-finite over S, and S is module-finite over R, then T is module-finite over R.*

Proof: Exercise. $\square$

1.2 Integrality

Let S be a commutative ring containing the commutative ring R. An element $s \in S$ is called *integral* over R if it satisfies a monic equation $s^n + a_1 s^{n-1} + ... + a_n = 0$ with coefficients a_i in R.

Proposition 1.2 *Let S be a domain with subring R. Let T be the set of elements in S that are integral over R. Then T is a subring of S containing R.*

That T contains R is clear: $r \in R$ satisfies the equation $x - r = 0$. That T is a subring will follow from the following lemma.

Lemma 1.3 *Let S be a domain with subring R. Let $s \in S$. Equivalent are:*
(i) s is integral over R,
(ii) $R[s]$ is module-finite over R,
(iii) there is a subring R' of S containing $R[s]$ that is module-finite over R.

Proof: (i) implies (ii): an equation $s^n + a_1 s^{n-1} + ... + a_n = 0$ expresses s^n in terms of 1, s, ..., s^{n-1}, so $R[s]$ is module-generated by these finitely many elements.

(ii) implies (iii): take $R' = R[s]$.

(iii) implies (i): Suppose R' is module-generated over R by $t_1, ..., t_n$. Write the products st_i using these generators: $st_i = \sum c_{ij} t_j$ with $c_{ij} \in R$. Let $A = sI - C$ where I is the identity matrix and $C = (c_{ij})$. Then $At = 0$, where t is the column vector (t_j). In the quotient field of S we conclude that $\det A = 0$, and that is the required monic equation for s. □

Proof of the proposition: if $a, b \in S$ are integral over R, then $R[a]$ is module-finite over R, and $R[a, b]$ is module-finite over $R[a]$, so $R[a, b]$ is module-finite over R. Now let s be one of the elements $a + b$, $a - b$, ab. Take $R' = R[a, b]$ in the above lemma to find that s is integral over R. That means we proved that T is closed under addition, subtraction and multiplication. □

1.3 Weak Nullstellensatz

Theorem 1.4 *Let k be an algebraically closed field. Let I be an ideal of the polynomial ring $k[x_1, ..., x_n]$. If $1 \notin I$, then $V(I) \neq \emptyset$.*

In the proof of this theorem, we'll need the following proposition.

Proposition 1.5 *Let L be a field containing a field k. If L is ring-finite over k, then L is module-finite over k.*

Proof of the theorem: If I is made larger, $V(I)$ gets smaller. So, it suffices to show this for a maximal ideal I. If the ideal I is maximal, the quotient $L = k[x_1, ..., x_n]/I$ is a field. We have a natural embedding of k into L. If this embedding is an isomorphism, then there are elements $a_i \in k$ that map to the residue classes $x_i + I$, i.e., have the property that $x_i - a_i \in I$. Now $I = (x_1 - a_1, ..., x_n - a_n)$ since the right hand side is a maximal ideal contained in I. Consequently, $V(I) = \{(a_1, ..., a_n)\}$ is a single point, and therefore non-empty.

Remains to show that the embedding of k into L really is an isomorphism. This follows from Proposition 1.5. Indeed, let us identify k with its image in L. In our situation $L = k[x_1, ..., x_n]/I$ is ring-generated by the residue classes $x_i + I$, so by this proposition L is module-finite over k, and by Lemma 1.3 every element of L is integral (and in partiticular algebraic) over k. But k is algebraically closed, so $L = k$. □

Proof of the proposition: We have $L = k[s_1, ..., s_n]$ for certain elements $s_1, ..., s_n \in L$, and want to find a finite set module-generating L over k. Use induction on n.

If $n > 1$ then put $K = k(s_1)$. Then $L = K[s_2, ..., s_n]$, and by induction on n we see that L is module-finite over K. If K is also module-finite over k, then L is module-finite over k (by Lemma 1.1) and we are done.

So, suppose $K = k(s_1)$ is not module-finite over k, so that s_1 is transcendent over k, and $K \simeq k(x)$. Let us write x instead of s_1.

Since L is module-finite over K, every element of L is integral over K.

Now look at the subring T of L consisting of the elements of L that are integral over $k[x]$. If $s \in L$ has equation $s^n + a_1 s^{n-1} + ... + a_n = 0$ with coefficients a_i in $K = k(x)$, then these a_i are rational expressions $a_i = f_i(x)/g_i(x)$. Let $h = h(x)$ be a common multiple of all denominators $g_i(x)$. Then hs satisfies $(hs)^n + (ha_1)(hs)^{n-1} + ... + h^n a_n = 0$, a monic equation with all coefficients in $k[x]$, so that $hs \in T$.

If we do this for $s = s_2, ..., s_n$, and take for h the least common multiple (or just the product) of all denominators encountered for all s_j, then we find a single h such that $hs_j \in T$ for all j.

Let z be an arbitrary element of L. Since $L = k[x, s_2, ..., s_n]$ this element can be written as a sum of terms, each a monomial in the s_j. It follows that $h^N z \in T$ for sufficiently high exponent N.

Now that this holds for all elements $z \in L$, take a particular one, for example $z = 1/f$ where $f \in k[x]$ is an irreducible polynomial not dividing h. Now if $h^N/f \in T$, then we have an equation $(h^N/f)^m + c_1(h^N/f)^{m-1} + ... = 0$ with coefficients $c_i \in k[x]$. Multiplying by f^{m-1} we find that $h^{Nm}/f \in k[x]$. But that is false since f is irreducible and does not divide h.

So, the assumption that $K = k(s_1)$ is not module-finite over k leads to a contradiction, and this finishes the $n > 1$ part of the proof by induction.

Remains to look at $n = 1$. Given is $L = k[s]$. To show that L is module-finite over k.

Consider the map from $k[x]$ onto $k[s]$ sending x to s. Its kernel is some ideal I, and $k[x]/I \simeq k[s] = L$.

If $I \neq (0)$, then $I = (g(x))$ for some polynomial $g(x)$ since $k[x]$ is a PID. W.l.o.g. $g(x)$ is monic, and we see that s is integral over k because $g(s) = 0$, and hence L is module-finite over k as desired.

And if $I = (0)$, then $L \simeq k[x]$, but $k[x]$ is not a field since it does not contain $1/x$.

This proves everything. □

1.4 Nullstellensatz

Theorem 1.6 *Let k be algebraically closed. Let I be an ideal in $k[x_1, ..., x_n]$. Then $I(V(I)) = \mathrm{Rad}(I)$. That is, if $g \in k[x_1, ..., x_n]$ and g vanishes on $V(f_1, ..., f_m)$, then there is an N such that $g^N = \sum c_i f_i$ for certain $c_i \in k[x_1, ..., x_n]$.*

Proof: Apply the Weak Nullstellensatz in $n+1$ dimensions: Look at the ideal $J = (f_1, ..., f_m, x_{n+1}g - 1)$ in $k[x_1, ..., x_n, x_{n+1}]$. Since $V(J) = \emptyset$, it follows that $1 \in J$, i.e.,

$$1 = \sum a_i f_i + a.(x_{n+1}g - 1)$$

for certain $a, a_i \in k[x_1, ..., x_n, x_{n+1}]$. Put $x_{n+1} = 1/y$ and multiply by a power of y to remove denominators:

$$y^N = \sum b_i f_i + b.(g - y)$$

for certain $b, b_i \in k[x_1, ..., x_n, y]$. Now put $y = g$. □

One sees that for algebraically closed fields there is a 1-1 correspondence between closed sets (sets of the form $V(f_1, ..., f_m)$) and radical ideals of $k[x_1, ..., x_n]$ (ideals I that equal their radical).