2. Nullstellensatz

We will need the notion of localisation, which is a straightforward generalisation of the notion of the field of fractions.

Definition 2.1. *Let R be a ring. We say that a subset S of R is* ***multiplicatively closed*** *if for every s_1 and s_2 in S, $s_1 s_2 \in S$, that is,*

$$S \cdot S \subset S.$$

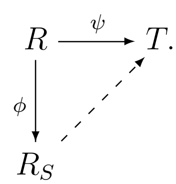
Definition-Lemma 2.2. *Let R be a ring and let S be a multiplicatively closed subset, which contains 1 but not zero. The* ***localisation of*** *R* ***at*** *S, denoted R_S, is a ring R_S together with a ring homomorphism*

$$\phi\colon R \longrightarrow R_S,$$

with the property that for every $s \in S$, $\phi(s)$ is a unit in R_S, which is universal amongst all such rings. That is, given any morphism

$$\psi\colon R \longrightarrow T,$$

with the property that $\psi(s)$ is a unit, for every $s \in S$, there is a unique ring homomorphism



Proof. This is almost identical to the construction of the field of fractions, and so we will skip most of the details. Formally we define R_S to be the set of all pairs (r, s), where $r \in R$ and $s \in S$, modulo the equivalence relation,

$$(r_1, s_1) \sim (r_2, s_2) \qquad \text{iff} \qquad s(r_1 s_2 - r_2 s_1) \text{ for some } s \in S.$$

We denote an equivalence class by $[r, s]$ (or more informally by r/s). Addition and multiplication are defined in the obvious way. □

Note that if R is an integral domain, then $S = R - \{0\}$ is multiplicatively closed and the localisation is precisely the field of fractions. Note also that as we are not assuming that R is an integral domain, we need to throw in the extra factor of s, in the definition of the equivalence relation and the natural map $R \longrightarrow R_S$ is not necessarily injective.

Example 2.3. *Suppose that $\mathfrak{p}$ is a prime ideal in a ring R. Then $S = R - \mathfrak{p}$ is a multiplicatively closed subset of R. The localisation is denoted $R_{\mathfrak{p}}$. It elements consist of all fractions r/f, where $f \notin \mathfrak{p}$. On* *the other hand, suppose that $f \in R$ is not nilpotent. Then the set of powers of f,*

$$S = \{ f^n \mid n \in \mathbb{N} \},$$

is a multiplicatively closed subset. The localisation consists of all elements of the form r/f^n.

For example, take $R = \mathbb{Z}$ and $f = 2$. Then $R_f = \mathbb{Z}[1/2] \subset \mathbb{Q}$ consists of all fractions whose denominator is a power of two.

Lemma 2.4. *Let F be a field and let $f \in F[x]$ be a polynomial.*

Then $F[x]_f$ is not a field.

Proof. Suppose not.

Clearly $\deg(f) > 0$ so that $1+f \neq 0$. Therefore we may find $g \in F[x]$ such that

$$(1+f)^{-1} = \frac{g}{f^n},$$

for some n. Multiplying out, we get that $(1+f)$ divides f^n.

So f^n is congruent to 0 modulo $(1+f)$. On the other hand, f is congruent to -1 modulo $(1+f)$. The only possibility is that $1+f$ is a unit, which is clearly impossible. □

Definition 2.5. *Let $R \subset F$ be a subring of the field F.*

*We say that $c \in F$ is **integral** over R if and only if there is a monic polynomial*

$$m(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in R[x],$$

such that $m(c) = 0$.

*If $R \subset S \subset F$ is an intermediary ring, we say that S is **integral over** R if every element of S is integral over R.*

*The **integral closure** of R in F is the set of all elements integral over R.*

Lemma 2.6. *Let $R \subset F$ be a subring of the field F.*

The following are equivalent:

1. *c is integral over R,*
2. *$R[c]$ is a finitely generated R-module,*
3. *there is an intermediary ring $R[c] \subset C \subset F$ which is a finitely generated R-module.*

Proof. Suppose that c is integral over R. Pick $m(x) \in R[x]$ monic such that $m(c) = 0$. If $m(x)$ has degree d it is easy to see that 1, c, c^2, …, c^{d-1} generate $R[c]$ as an R-module. Thus (1) implies (2).

(2) implies (3) is clear.

Now suppose that C is a finitely generated R-module. Multiplication by c defines an R-linear map

$$\phi\colon C \longrightarrow C.$$

Pick generators $c_1, c_2, \dots, c_k$ for the R-module C. Then we may find $A = (a_{ij}) \in M_k(R)$ such that

$$\phi(c_i) = \sum a_{ij} c_j.$$

Then $m(x) = \det(A - \lambda I) \in R[x]$ is a monic polynomial and $m(\phi) = 0$, by Cayley-Hamilton. But then $m(c) = m(\phi(1)) = 0$. Hence (3) implies (1). □

Lemma 2.7. *Let $R \subset F$ be a subring of the field F.*

If $S = R[r_1, r_2, \dots, r_k]$ where each $r_1, r_2, \dots, r_k$ is integral over S then S is integral over R.

Proof. By (2.6) it suffices to prove that S is a finitely generated R-module. By induction on k we may assume that $S' = R[r_1, r_2, \dots, r_{k-1}]$ is a finitely generated R-module. As S is a finitely generated S'-module (r_k is integral over S' as it is integral over R) it follows that S is a finitely generated R-module. □

We will need the following result later:

Lemma 2.8. *Let $R \subset F$ be a subring of the field F.*

The integral closure S of R in F is a ring.

Proof. Let a and b be in S. It suffices to prove that $a \pm b$ and ab are in S. But $a \pm b$ and ab belong to $R[a, b]$ and this is finitely generated over R by (2.7). □

Lemma 2.9. *Let E be a field and let R be a subring.*

If E is integral over R then R is a field.

Proof. Pick $a \in R$ and let $b \in E$ be the inverse. As E is integral over R, we may find $r_1, r_2, \dots, r_n \in R$ such that

$$b^n + r_1 b^{n-1} + \dots + r_n = 0.$$

Multiply both sides by a^{n-1} and solve for b to get

$$b = -r_1 - r_2 a - \dots - r_n a^{n-1} \in A.$$ □

Lemma 2.10. *Let E/F be a field extension.*

If E is finitely generated as an F-algebra then E/F is algebraic.

Proof. By assumption $E = F[f_1, f_2, \dots, f_m]$. We proceed by induction on m.

Let $f = f_m$. By induction $E = F(f)[f_1, f_2, \dots, f_{m-1}]$ is algebraic over $F(f)$. Let $m_i(x) \in F(f)[x]$ be the minimal polynomial of f_i. Clearing denominators, we may assume that $m_i(x) \in F[f][x]$. Let a_i be the leading coefficient of $m_i(x)$ and let a be the product of the a_i. Then $(1/a_i)m_i(x) \in F[f]_a[x]$ is a monic polynomial, so that f_i is integral over $F[f]_a$.

By (2.9) $F[f]_a$ is a field. But then f is algebraic over F by (2.4). □

Theorem 2.11 (Weak Nullstellensatz)**.** *Let K be an algebraically closed field.*

Then an ideal $\mathfrak{m} \lhd R = K[x_1, x_2, \dots, x_n]$ is maximal if and only if it has the form

$$\mathfrak{m}_p = \langle x_1 - a_1, x_2 - a_2, \dots, x_n - a_n \rangle,$$

for some point $p = (a_1, a_2, \dots, a_n) \in K^n$.

Proof. Let $\mathfrak{m} \lhd R$ be an ideal and let $L = R/\mathfrak{m}$. Then $\mathfrak{m}$ is maximal if and only if $L = R/\mathfrak{m}$ is a field and $L = K$ if and only if $\mathfrak{m} = \mathfrak{m}_p$ for some point p.

So we may assume that L is a field and we want to prove that $L = K$. But L is a finitely generated algebra over K (generated by the images of $x_1, x_2, \dots, x_n$) so that by (2.10) L/K is algebraic. As K is algebraically closed, $L = K$. □

Corollary 2.12 (Weak Nullstellensatz)**.** *Let K be an algebraically closed field.*

If $f_1, f_2, \dots, f_m \in R = K[x_1, x_2, \dots, x_n]$ is a sequence of polynomials then either

(1) $f_1, f_2, \dots, f_m$ have a common zero, or
(2) there are polynomials $g_1, g_2, \dots, g_m \in K[x_1, x_2, \dots, x_n]$ such that

$$f_1 g_1 + f_2 g_2 + \dots + f_m g_m = 1.$$

Proof. Let $I = \langle f_1, f_2, \dots, f_m \rangle \trianglelefteq R$ be the ideal generated by the polynomials $f_1, f_2, \dots, f_m$. Note that (1) holds if and only if I is contained in one of the ideals $\mathfrak{m}_p$ for some $p = (a_1, a_2, \dots, a_n) \in K^n$. Indeed, in this case $f_1, f_2, \dots, f_n$ all vanish at p. On the other hand, note that (2) holds if and only if $I = R$.

So suppose that $I \neq R$. Pick a maximal ideal $\mathfrak{m}$ containing I. By (2.11) we may find $p \in K^n$ such that $\mathfrak{m} = \mathfrak{m}_p$. □

Theorem 2.13 (Strong Nullstellensatz)**.** *Let K be an algebraically closed field.*

If $f_1, f_2, \dots, f_m, g \in R = K[x_1, x_2, \dots, x_n]$ is a sequence of polynomials then either

(1) $f_1, f_2, \dots, f_m$ have a common zero, at a point where the polynomial g is not equal to zero, or

(2) there are polynomials $g_1, g_2, \dots, g_m \in K[x_1, x_2, \dots, x_n]$ such that

$$f_1g_1 + f_2g_2 + \dots + f_mg_m = g^r,$$

for some natural number r.

Proof. We use the *trick of Rabinowitsch*. Let

$$S = R[y] = K[x_1, x_2, \dots, x_n, y],$$

where y is an indeterminate and consider the polynomials

$$f_1, f_2, \dots, f_m, yg - 1.$$

If (1) does not hold then these equations don't have any solutions at all. By the weak Nullstellensatz (2.12) we may find polynomials $g_1, g_2, \dots, g_m, h \in S$ such that

$$f_1g_1 + f_2g_2 + \dots + f_mg_m + h(yg - 1) = 1.$$

Let $z = 1/y$. Clearing denominators by multiplying through some large power z^r of z, and relabelling, we get

$$f_1g_1 + f_2g_2 + \dots + f_mg_m + h(g - z) = z^r.$$

Now set $z = g$. □

Corollary 2.14 (Hilbert's Nullstellensatz). *Let K be an algebraically closed field and let I be an ideal.*

Then $I(V(I)) = \sqrt{I}$.

Proof. One inclusion is clear, $I(V(I)) \supset \sqrt{I}$.

Now suppose that $g \in I(V(I))$. Pick a basis $f_1, f_2, \dots, f_k$ for I. Suppose that the point x is a common zero for $f_1, f_2, \dots, f_k$, so that $f_i(x) = 0$, for $1 \leq i \leq k$. Then $f(x) = 0$ for all $f \in I$ and so $x \in V(I)$. But then $g(x) = 0$. So we may apply the strong Nullstellensatz to $f_1, f_2, \dots, f_n, g$ to conclude that $g^r \in I$, some $r > 0$, that is, $g \in \sqrt{I}$. □