5. Hilbert's Nullstellensatz

Gauss proved several times that the field of complex numbers $\mathbb{C}$ is algebraically closed, i.e., if $\mathbb{C} \subset K$ is any algebraic extension of fields then necessarily $\mathbb{C} = K$, or equivalently every non-constant polynomial $f(X) \in \mathbb{C}[X]$ has a root in $\mathbb{C}$. This is in contrast with the field of real numbers $\mathbb{R}$, where for example the polynomial $X^2 + 1$ has no real root.

Now consider a polynomial ring over a field k with several variables $k[X_1, \ldots, X_n]$ and I an ideal. We say that $v = (v_1, v_2, \ldots, v_n) \in k^n$ is a *common zero* of the ideal if every polynomial $f(X_1, \ldots, X_n)$ in I vanishes on v, i.e. when we substitute v_i for the variable X_i for all i, we obtain 0:

$$f(v) = f(v_1, \ldots, v_n) = 0.$$

The evaluation-at-v map

$$\mathrm{ev}_v : k[X_1, \ldots, X_n] \to k : f \mapsto f(v)$$

is a surjective ring homomorphism; its kernel $\mathfrak{M}_v$ is therefore a maximal ideal. Hence v is a common zero for I if and only if $I \subseteq \mathfrak{M}_v$.

Write $\mathcal{V}(I) \subset k^n$ for the collection of all the common zeros of I, called the *zero set* of I. This zero set $\mathcal{V}(I)$ can be empty, for example when I contains the constant function $\mathbf{1}$, i.e. when $I = k[X_1, \ldots, X_n]$. For the ideal $I = (X_1^2 + 1) \lhd \mathbb{R}[X_1]$ the zero set $\mathcal{V}(I)$ in $\mathbb{R}^1$ is empty. We can reformulate : A field k is algebraically closed if and only if the zero set $\mathcal{V}(I) \subset k^1$ is non-empty for any non-trivial ideal $I \subset k[X_1]$, i.e. $\mathbf{1} \notin I$.

One version of a theorem of Hilbert, called Hilbert's *Nullstellensatz*, generalizes this for all n.

Theorem 5.1. *A field k is algebraically closed if and only if the zero set $\mathcal{V}(I) \subset k^n$ is non-empty for any $n \geq 1$ and non-trivial ideal $I \subset k[X_1, \ldots, X_n]$, i.e. $\mathbf{1} \notin I$.*

In particular, if $I \subset \mathbb{C}[X_1, \ldots, X_n]$ is an ideal and $I \neq \mathbb{C}[X_1, \ldots, X_n]$ then there does exist a common zero for I in $\mathbb{C}^n$.

An algebraic version of this theorem is as follows.

Theorem 5.2. *A field k is algebraically closed if and only if for any $n \geq 1$ any maximal ideal $\mathfrak{M}$ of $k[X_1, \ldots, X_n]$ is of the form $\mathfrak{M} = \mathfrak{M}_v$ for some $v \in V$.*

The two theorems sound different, but are equivalent nevertheless.

Proof of equivalence of the two theorems. Let k be algebraically closed, $\mathfrak{M} \lhd k[X_1, \ldots, X_n]$ a maximal ideal and suppose Theorem 5.1 holds. Then there exists a $v \in k^n$ that is a common zero of $\mathfrak{M}$, or $\mathfrak{M} \subseteq \mathfrak{M}_v$. Since $\mathfrak{M}$ is maximal it follows that $\mathfrak{M} = \mathfrak{M}_v$.

On the other hand let I be a non-trivial ideal of $k[X_1, \ldots, X_n]$ and suppose Theorem 5.2 holds. By Krull's theorem there exist a maximal ideal $\mathfrak{M}$ containing I. By assumption there is a $v \in k^n$ such that $\mathfrak{M} = \mathfrak{M}_v$. So $I \subset \mathfrak{M}_v$, and so v is a common zero for I. □

To prove the theorems we will use two useful lemmas.

Lemma 5.1. *Let $R \subset S$ be an integral extension of integral domains. Then R is a field if and only S is a field.*

Proof. Suppose R is a field and $s \in S$, $s \neq 0$. Let $s^d + r_1 s^{d-1} + \ldots + r_d = 0$ be an integrality relation of smallest degree d, where $r_i \in R$. Put $s' := s^{d-1} + r_1 s^{d-2} + \ldots + r_{d-1}$ then $ss' + r_d = 0$ and by minimality of the degree $s' \neq 0$. Suppose $r_d = 0$ then $s's = 0$. But by assumption S has no zero divisors. So $r_d \neq 0$ and r_d has an inverse in R. We have $ss' = -r_d$ or $s^{-1} = -r_d^{-1}s'$ exists. So S is a field.

Suppose S is a field and $r \in R$, $r \neq 0$. Now $r^{-1} \in S$ exists and satisfies an integrality relation over R, say $(r^{-1})^d + r_1(r^{-1})^{d-1} + \ldots + r_d = 0$. Multiplying by r^{d-1} we obtain $r^{-1} = -(r_1 + r_2 r + \ldots + r_d r^{d-1}) \in R$. So R is a field. □

The second lemma uses Noether normalization.

Lemma 5.2. *Let $\mathfrak{M} \lhd k[X_1, \ldots, X_n]$ be a maximal ideal, where k is a field. Then the field extension $k \subset K := k[X_1, \ldots, X_n]/\mathfrak{M}$ is finite, i.e. $\dim_k K < \infty$ and hence in particular the extension is algebraic.*

Proof. Since K is an affine k-algebra, Noether normalization says that there is a $d \geq 0$ and $y_1, \ldots, y_d \in K$ that are algebraically independent over k and such that $k[y_1, \ldots, y_d] \subset K$ is integral. Since K is a field, by the previous lemma $k[y_1, \ldots, y_d]$ is a field. This is only possible when $d = 0$, hence $k \subset K$ is an integral extension. □

Now we are ready to prove the Nullstellensatz.

Proof of Theorem 5.2. Let k be algebraically closed and $\mathfrak{M}$ a maximal ideal of $k[X_1, \ldots, X_n]$. Put $K := k[X_1, \ldots, X_n]/\mathfrak{M}$ and x_i the class of X_i in K. By Lemma 5.2 the extension $k \subseteq K$ is algebraic. Let $s \in K$ have minimum polynomial $f \in k[X]$. Since k is algebraically closed $f(X)$ has a zero $c \in k$, so by polynomial division there is a monic polynomial $g(X) \in k[X]$ such that $f(X) = (X - c)g(X)$. If $s \neq c$ then $g(s) = 0$ and so g is divisible by f, contradiction. So $c = s$. We proved that $k = K$. In particular there are $v_i \in k$ such that $x_i = v_i$, and for any polynomial $f(X_1, \ldots, X_n)$ we get $f(x_1, \ldots, x_n) = f(v)$ or stated differently $f - f(v) = f(X_1, \ldots, X_n) - f(v) \in \mathfrak{M}$. In particular when $f \in \mathfrak{M}_v$ we get $f = f - f(v) \in \mathfrak{M}$, or $\mathfrak{M}_v \subseteq \mathfrak{M}$. Since $\mathfrak{M}_v$ is a maximal ideal, it follows that $\mathfrak{M}_v = \mathfrak{M}$. □

5.1. If $I \subseteq J \lhd k[X_1, \ldots, X_n]$ then clearly $\mathcal{V}(I) \supseteq \mathcal{V}(J)$. Different ideals can have the same zero set, for example $(f_1, f_2))$ and (f_1^{10}, f_2^2) have the same zero-set. Let $I \lhd R$ be an ideal, the *radical* of I, written $\sqrt{I}$, is defined as:

$$\sqrt{I} = \{f \in R;\ \exists n \geq 1 : f^n \in I\}.$$

It contains I and is an ideal itself and $\mathcal{V}(I) = \mathcal{V}(\sqrt{I})$.

Let $Y \subset k^n$ be any subset of the n-dimensional affine space over the field k. Then we define its *vanishing ideal*

$$I(Y) := \{f \in k[X_1, \ldots, X_n];\ \forall v \in Y : f(v) = 0\} = \cap_{v \in Y} \mathfrak{M}_v.$$

If $Y \subset X$ then $I(Y) \supseteq I(X)$. Associated to this ideal we have a zero set called the (Zariski)-*closure* of Y:

$$\overline{Y} := \mathcal{V}(I(Y)).$$

And we could repeat, but $\overline{\overline{Y}} = \overline{Y}$, by the next lemma.

Lemma 5.3. *Let k be any field, $Y \subset k^n$ a subset and $J \lhd k[X_1, \ldots, X_n]$ an ideal.*
(i) $I(Y) = I(\mathcal{V}(I(Y)))$;
(ii) $\mathcal{V}(J) = \mathcal{V}(I(\mathcal{V}(J)))$.

Proof. (i) It is clear from the definition (I hope) that $Y \subseteq \mathcal{V}(I(Y))$, hence $I(Y) \supseteq I(\mathcal{V}(I(Y)))$. Let $f \in I(Y)$ then $f(v) = 0$ for all $v \in \mathcal{V}(I(Y))$, hence $f \in I(\mathcal{V}(I(Y)))$.

(ii) It is clear from the definition (I hope) that $J \subseteq I(\mathcal{V}(J))$, hence $V(J) \supseteq \mathcal{V}(I(\mathcal{V}(J)))$. Let $v \in V(J)$ then $f(v) = 0$ for all $f \in I(\mathcal{V}(J))$, hence $v \in \mathcal{V}(I(\mathcal{V}(J)))$. □

Given a field k and an ideal $J \lhd k[X_1, \ldots, X_n]$ then at least $\sqrt{I} \subseteq I(\mathcal{V}(J)$. Another version of the Nullstellensatz is the following.

Theorem 5.3. *A field k is algebraically closed if and only if for any $n \geq 1$ and any ideal $J \lhd k[X_1, \ldots, X_n]$ we have that*

$$I(\mathcal{V}(J)) = \sqrt{J}.$$

Proof. Suppose k is not algebraically closed, then there is a non-constant $f \in k[X_1]$ without zeros in k. So $I(\mathcal{V}(f)) = I(\emptyset) = k[X_1] \neq \sqrt{(f)}$.

The other direction uses a trick due to Rabinovich, cf. [2, §15.3]. Let $g \in I(\mathcal{V}(J))$. By Hilbert's basis theorem J is finitely generated, say by $f_1, \ldots, f_m$. Consider the ideal $\tilde{J}$ of $k[X_1, \ldots, X_n, X_{n+1}]$ generated by $f_1, \ldots, f_m$ and $X_{n+1}g - 1$. Suppose $(v_1, \ldots, v_n, v_{n+1}) \in k^{n+1}$ is a common zero for the ideal $\tilde{J}$. Then $f_i(v_1, \ldots, v_n) = 0$ for all i and $v_{n+1} \cdot g(v_1, \ldots, v_n) - 1 = 0$. In particular $(v_1, \ldots, v_n) \in k^n$ is a common zero for J, so $g(v_1, \ldots, v_n) = 0$ as well. But then $-\mathbf{1} = v_{n+1} \cdot 0 - \mathbf{1} = v_{n+1} \cdot g(v_1, \ldots, v_n) - \mathbf{1} = 0$ gives a contradiction. We conclude that the ideal $\tilde{J}$ does not have a common zero in k^{n+1}. By the first version of the Nullstellensatz, Theorem 5.1, we conclude that $\mathbf{1} \in \tilde{J}$. So there are $h_i \in k[X_1, \ldots, X_{n+1}]$ such that

$$\mathbf{1} = \sum_{i=1}^{n} h_i f_i + h_{n+1}(X_{n+1}g - \mathbf{1}).$$

Let $N > 1$ be larger then the x_{n+1}-degree of any of the h_i's, then $g_i := \frac{h_i}{x_{n+1}^N}$ becomes a polynomial in $\frac{1}{x_{n+1}}$ with coefficients in $k[X_1, \ldots, X_n]$, i.e., g_i is an element of $k[X_1, \ldots, X_n, \frac{1}{X_{n+1}}]$. Say

$$\left(\frac{1}{X_{n+1}}\right)^N = \sum_{i=1}^{n} g_i(X_1, \ldots, X_n, \frac{1}{X_{n+1}}) \cdot f_i + g_{n+1}(X_1, \ldots, X_n, \frac{1}{X_{n+1}})(X_{n+1}g - 1).$$

Now substitute $X_{n+1} := \frac{1}{g}$ to get

$$g^N = \sum_{i=1}^{n} g_i(X_1, \ldots, X_n, g) \cdot f_i + g_{n+1}(X_1, \ldots, X_n, g)(\frac{1}{g}g - 1) = \sum_{i=1}^{n} g_i(X_1, \ldots, X_n, g) \cdot f_i,$$

where each $g_i \in k[X_1, \ldots, X_n]$. So a power of g is contained in the ideal $(f_1, \ldots, f_m) = J$, or $g \in \sqrt{J}$. □

Remark. So when k is not algebraically closed then generally $I(\mathcal{V}(J))$ is bigger than $\sqrt{J}$. Can we nevertheless give a description of $I(\mathcal{V}(J))$ for a given field? For the field of real numbers such a description is known. But for $\mathbb{Q}$?!

5.2. Generators of maximal ideals of polynomial rings. Any maximal ideal of a polynomial ring over a field with n variables can be generated by n polynomials, and can be constructed iteratively from minimal polynomials, as shown in the proof of the next proposition.

Proposition 5.1. *Let $\mathfrak{m} \subset k[X_1, \ldots, X_n]$ be a maximal ideal, where k is a field. Then $\mathfrak{m}$ can be generated by n polynomials.*

Proof. We shall use induction on n; the case $n = 0$ is trivial and if $n = 1$ every ideal is generated by one element. Suppose the result is true for less than n variables. Put $K = k[X_1, \ldots, X_n]/\mathfrak{m}$ and $x_i := \overline{X_i}$, the class of X_i in K. Put $\mathfrak{m}' := k[X_1, \ldots, X_{n-1}] \cap \mathfrak{m}$, then $k[X_1, \ldots, X_{n_1}]/\mathfrak{m}' \simeq k[x_1, \ldots, x_{n-1}]$. Since the x_i's are algebraic over k, each $k[x_1, \ldots, x_{n-1}] = k(x_1, \ldots, x_{n-1})$ is a field, by Lemma 5.1, and so $\mathfrak{m}'$ is even a maximal ideal of $k[X_1, \ldots, X_{n-1}]$.

By induction we know generators $F_1, \ldots, F_{n-1}$ for $\mathfrak{m}'$. Since x_n is algebraic over the field $k(x_1, \ldots, x_{n-1})$, it has a minimum polynomial

$$f(T) = T^d + r_1 T^{d-1} + \ldots + r_d \in k(x_1, \ldots, x_{n-1})[T].$$

Choose polynomials $h_1, \ldots, h_d \in k[X_1, \ldots, X_{n-1}]$ such that $h_i(x_1, \ldots, x_{n-1}) = r_i$, and put

$$F_n := X_n^d + h_1 X_n^{d-1} + \ldots + h_d.$$

Then $F_n(x_1, \ldots, x_n) = 0$, i.e., $F_n \in \mathfrak{m}$. We have $\mathfrak{m} \supseteq (F_1, \ldots, F_n)$ and shall prove that $\mathfrak{m} = (F_1, \ldots, F_n)$.

Let $F \in \mathfrak{m}$, hence $F(x_1, \ldots, x_n) = 0$. Expand F as a polynomial in X_n, say

$$F = f_0 X_n^m + f_1 X_n^{m-1} + \ldots + f_m,$$

with $f_i \in k[X_1, \ldots, X_{n-1}]$. Since $F(x_1, \ldots, x_{n-1}, X_n)$ is divisible by the minimal polynomial $f(X_n)$, there exists a polynomial $h(X_n) \in k(x_1, \ldots, x_{n-1})[X_n]$ such that

$$F(x_1, \ldots, x_{n-1}, X_n) = f(X_n)h(X_n).$$

We can choose a polynomial $H \in k[X_1, \ldots, X_n]$ such that $H(x_1, \ldots, x_{n-1}, X_n) = h(X_n)$. Furthermore, since F_m is a monic polynomial we can assume that H has the same main coefficient as F, i.e., H is of the form

$$H = f_0 X_n^{m-d} + \quad \text{plus lower order terms in } X_n.$$

So

$$F - F_n H \in \mathfrak{m}$$

and the X_n-degree of $F - F_n H$ is smaller than the X_n-degree of F. By repeating this procedure, we can find a polynomial G such that

$$F - F_n G \in \mathfrak{m}$$

has X_n-degree is 0, i.e., $F - F_n G \in \mathfrak{m}' = (F_1, \ldots, F_{n-1})$ or

$$\mathfrak{m} \subseteq (F_1, \ldots, F_n) \lhd k[X_1, \ldots, X_n].$$

□

6. Cohen-Seidenberg theorems and Noether normalisation

Integral extension of rings have more nice properties than we have already mentioned. We will need them to get more corollaries from the Noether normalization, Theorem 4.1, and Hilbert's Nullstellensatz.

We collect the needed results in one omnibus theorem, due to Cohen and Seidenberg (see also [2, §15.3, Theorem 26]).

Let R be a ring and

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_m \subset \ldots \subset \mathfrak{p}_n$$

a sequence of prime ideals. We shall call it a *chain of prime ideals* of length n (there are n chains) if for all $0 \leq i < n$ we have $\mathfrak{p}_i \neq \mathfrak{p}_{i+1}$. The chain is *saturated* if it has the property that if $\mathfrak{q}$ is any prime ideal such that $\mathfrak{p}_i \subseteq \mathfrak{q} \subseteq \mathfrak{p}_{i+1}$, for some $0 \leq i < n$, then $\mathfrak{q} = \mathfrak{p}_i$ or $\mathfrak{q} = \mathfrak{p}_{i+1}$. We shall say that R has finite *(Krull) dimension* d if R has a chain of prime ideals of length d, but no chain of length $> d$.

Theorem 6.1 (Cohen-Seidenberg)**.** *Let $R \subset S$ be an integral extension of rings.*

(i) Let $\mathfrak{P} \lhd S$ be a prime ideal, put $\mathfrak{p} = \mathfrak{P} \cap R$. Then $\mathfrak{P}$ is a maximal ideal in S if and only if $\mathfrak{p}$ is a maximal ideal of R.

(ii) (Incompatibility theorem) Suppose $\mathfrak{Q} \supseteq \mathfrak{P}$ are prime ideals of S such that $\mathfrak{Q} \cap R = \mathfrak{P} \cap R$. Then $\mathfrak{P} = \mathfrak{Q}$.

(iii) (Lying-over theorem) Suppose $\mathfrak{p}$ is a prime ideal of R. Then there is a prime ideal $\mathfrak{P}$ of S such that $\mathfrak{P} \cap R = \mathfrak{p}$.

(iv) (Going-up theorem) Let $m < n$. Suppose there is a chain of prime ideals in S

$$\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \ldots \subset \mathfrak{P}_m,$$

and a chain of prime ideals in R

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_m \subset \ldots \subset \mathfrak{p}_n$$

such that $\mathfrak{P}_i \cap R = \mathfrak{p}_i$ for $1 \leq i \leq m$. Then the chain of prime ideals in S can be extended to a chain

$$\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \ldots \subset \mathfrak{P}_m \subset \ldots \subset \mathfrak{P}_n$$

such that $\mathfrak{P}_i \cap R = \mathfrak{p}_i$ for all i.

(v)(Going-down theorem) Suppose S is an integral domain and that R is integrally closed in its fraction field and still $R \subset S$ an integral extension. Let $0 < m \leq n$. Suppose there is a chain of prime ideals in S

$$\mathfrak{P}_m \subset \mathfrak{P}_{m+1} \subset \ldots \subset \mathfrak{P}_n,$$

and a chain of prime ideals in R

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_m \subset \ldots \subset \mathfrak{p}_n$$

such that $\mathfrak{P}_i \cap R = \mathfrak{p}_i$ for $m \leq i \leq n$. Then the chain of prime ideals in S can be extended to a chain

$$\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \ldots \subset \mathfrak{P}_m \subset \ldots \subset \mathfrak{P}_n$$

such that $\mathfrak{P}_i \cap R = \mathfrak{p}_i$ for all i.

The following lemma provides examples of domains that are integrally closed in their field of fractions.

Lemma 6.1. *Let R be a factorial domain. Then R is integrally closed in its field of fractions. In particular, this is the case for a polynomial ring over a field.*

Proof. Let the fraction $\frac{a}{b}$ be integral over R, we can suppose that a and b have no common irreducible factors. There is an integrality relation over R:

$$(\frac{a}{b})^d + r_1(\frac{a}{b})^{d-1} + \ldots + r_d = 0,$$

where $r_i \in R$. So

$$a^d = -b(r_1 a^{d-1} + r_2 a^{d-2} b + \ldots + r_d b^{d-1}).$$

So any irreducible factor of b is also an irreducible factor of a, but a and b have no irreducible factors in common. We conclude that b is a unit in R, so $\frac{a}{b} = b^{-1}a \in R$. We proved that R is integrally closed in its field of fractions. □

Corollary 6.1. *Suppose $R \subset S$ is an integral extension. Then they have the same Krull-dimension.*

Proof. Suppose

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_d$$

is a chain of prime ideals in R. By Lying-over there is a prime ideal $\mathfrak{P}_0$ in S, such that $\mathfrak{P}_0 \cap R = \mathfrak{p}_0$, then by Going-up there is a chain of prime ideals in S

$$\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \ldots \subset \mathfrak{P}_d$$

lying over our chain. So the Krull-dimension of S is at least as big as the Krull-dimension of R.

On the other hand, suppose

$$\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \ldots \subset \mathfrak{P}_d$$

is a chain of prime ideals in S. Put $\mathfrak{p}_i := \mathfrak{P}_i \cap R$. Then $\mathfrak{p}_i$ is a prime ideal. If $\mathfrak{p}_i = \mathfrak{p}_{i+1}$ we get a contradiction with the Incompatibility theorem, so we get a chain on prime ideals in R.

$$\mathfrak{p}_0 \subset \mathfrak{p}_1 \subset \ldots \subset \mathfrak{p}_d$$

So the Krull-dimension of R is at least as big as the Krull-dimension of S. □

Corollary 6.2. *(i) If S is an affine ring over a field k, then the Krull-dimension of S equals the dimension of R as affine k-algebra.*

(ii) In particular, a polynomial ring over a field $k[X_1, \ldots, X_n]$ has Krull-dimension n. In fact every maximal saturated chain of prime ideals in $k[X_1, \ldots, X_n]$ has length n.

Proof. By Noether normalization there are elements $x_1, \ldots, x_n$ in S that are algebraically independent over k and such that $R := k[x_1, \ldots, x_n] \subset S$ is an integral extension of rings and we can apply the corollary. So it suffices to prove the special case of a polynomial ring with n-variables $S = k[X_1, \ldots, X_n]$.

Put $\mathfrak{P}_0 = (0)$ and $\mathfrak{P}_i = (X_1, \ldots, X_i)$, for $1 \leq i \leq n$. Then $S/\mathfrak{P}_i$ is itself isomorphic to a polynomial ring, so $\mathfrak{P}_i$ is a prime ideal. So we get a chain of prime ideals of length n

$$\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \ldots \subset \mathfrak{P}_n.$$

So the Krull-dimension of $k[X_1, \ldots, X_n]$ is at least n.

Let

$$\mathfrak{P}_0 \subset \mathfrak{P}_1 \subset \ldots \subset \mathfrak{P}_e$$

be any maximal saturated chain of prime ideals of S. By Noether normalisation, there are elements $x_1, \ldots, x_n$ algebraically independent over k, such that $R := k[x_1, \ldots, x_n] \subset S$ is integral and there are integers $n \geq d_0 \geq d_1 \geq \ldots \geq d_e \geq 0$ such that

$$\mathfrak{P}_i \cap R = (x_{d_i+1}, x_{d_i+2}, \ldots, x_n)$$

Since there are only $n+1$ different integers between 0 and n, if $e > n$ we have $e+1 > n+1$ ideals $\mathfrak{P}_i$, there must be therefore an i such that $\mathfrak{P}_i \cap R = \mathfrak{P}_{i+1} \cap R$. But that is a contradiction with the Incompatibility theorem.

Suppose now that $e < n$. If $d_0 < n$ then $(0) \neq \mathfrak{p}_0$. By Going-down there exists a prime ideal $\mathfrak{P}_{-1} \subset \mathfrak{P}_0$ such that $\mathfrak{P}_{-1} \cap R = (0)$, and we have extended our chain. But this is impossible, since the original chain was already a maximal saturated chain. So $d_0 = n$. Let $i \geq 1$ be minimal such that $d_i > n - i$; in particular $d_{i-1} = n - i + 1$, and there is a linear prime ideal, say $\mathfrak{q}$ strictly between $\mathfrak{p}_{i-1}$ and $\mathfrak{p}_i$. Now $R/\mathfrak{p}_{i-1} \subset S/\mathfrak{P}_{i-1}$ is also integral, and since $R/\mathfrak{p}_{i-1}$ also a polynomial ring we can use Going-down again starting with $0 \neq \mathfrak{q}/\mathfrak{p}_{i-1} \subset \mathfrak{p}_i/\mathfrak{p}_{i-1}$. By Going-down and the correspondence theorem we get a prime ideal $\mathfrak{Q}$ in S containing $\mathfrak{P}_{i-1}$ and contained in $\mathfrak{P}_i$, such that $\mathfrak{Q} \cap R = \mathfrak{q}$. We conclude again that our chain was not saturated, which is a contradiction. Hence $e = n$. □

We say that a ring is *catenary* if for every two prime ideals $\mathfrak{p} \subseteq \mathfrak{p}'$ every saturated chain of prime ideals starting at $\mathfrak{p}$ and ending in $\mathfrak{p}'$ has the same length.

Corollary 6.3. *Any affine ring over a field is catenary.*

Proof. Since any affine k-algebra is the quotient of a polynomial ring $k[X_1, \ldots, X_n]$, using the correspondence theorem it suffices to prove that polynomial rings are catenary rings. Fix two prime ideals $\mathfrak{p} \subseteq \mathfrak{p}'$ of the polynomial ring. Suppose there are two saturated chains between $\mathfrak{p}$ and $\mathfrak{p}'$ with different lengths. We can complete those two chains to two maximal saturated chains of different lengths. But we just proved, that two maximal saturated chains of prime ideals in a polynomial ring have the same length. Contradiction. □

6.1. Let $I \lhd k[X_1, \ldots, X_n]$ be an ideal. We proved that if k is algebraically closed, $\sqrt{(I)} = \cap_{\mathfrak{m} \subseteq I} \mathfrak{m}$, where the intersection is over all maximal ideal containing $\mathfrak{m}$. This remains true if k is not algebraically closed (we shall use some facts from field theory to prove this).

Proposition 6.1. *Let I be an ideal of an affine k-algebra S. Then the radical of I is the intersection of all maximal ideals containing I:*

$$\sqrt{I} = \cap_{\mathfrak{m} \supseteq I} \mathfrak{m}.$$

Proof. By the correspondence theorem we can assume that $S = k[X_1, \ldots, X_n]$ is a polynomial ring over the field k. Let I be generated by $f_1, \ldots, f_m$.

There exists an algebraic extension $k \subset L$, where L is an algebraically closed field. We shall not prove this here.

Then $k[X_1, \ldots, X_n] \subset L[X_1, \ldots, X_n]$ is an integral extension of rings. Let $h \in \cap_{\mathfrak{m} \supseteq I} \mathfrak{m}$. Let $\mathfrak{M}$ be a maximal ideal of $L[X_1, \ldots, X_n]$ that contains every f_i, then its intersection $\mathfrak{m} = \mathfrak{M} \cap k[X_1, \ldots, X_n]$ is a maximal ideal (by the Cohen-Seidenberg theorem) containing I. So if we write I^e for the ideal in $L[X_1, \ldots, X_n]$ generated by I, we get

$$f \in \cap_{\mathfrak{m} \supseteq I} \mathfrak{m} \subset \cap_{\mathfrak{M} \supseteq I^e} \mathfrak{M} = \sqrt{I^e}$$

by the Nullstellensatz. So there is an N and $h_1, \ldots, h_m \imath L[X_1, \ldots, X_n]$ such that

$$f^N = \sum_{i=1}^{m} h_i f_i.$$

Let K be the finite dimensional algebraic extension of k generated by the finitely many coefficients of the h_i's, so now $h_i \in K[X_1, \ldots, X_n]$. Let $b_1, \ldots, b_s$ be a k-basis for K, where $b_1 = \mathbf{1}$. Any $z \in K$ can be written uniquely as $z = \sum_{i=1}^{s} c_i b_i$, with $c_i \in k$. Extend the projection

$$\pi : K \to k : \pi(z) = c_1 b_1 = c_1$$

to a $k[X_1, \ldots, X_n]$-linear projection $\pi : K[X_1, \ldots, X_n$.

Now apply π to the equation of f^N, to obtain:

$$f^N = \sum_{i=1}^{m} \pi(h_i) f_i.$$

Hence $f \in \sqrt{I}$. (Compare this proof with the proof of Proposition 3.1). $\square$

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA