4. Algebraic spaces

We want to study zero sets of polynomial equations. The basic theorem is the Nullstellensatz. But first we need some preliminaries.

4.0. Preliminaries. First we need to know that any finitely generated ring over a field $K$ can be mapped to the algebraic closure $\overline{K}$. This is not true for finitely generated field extensions. For example, there is no homomorphism of $K(X)$ into $\overline{K}$ over $K$. I used Noether normalization which makes the proofs shorter.

**Lemma 4.1.** If $R$ is integral over $S$ and $R$ is a field then $S$ is a field.

*Proof.* We just need to show that if $x \neq 0 \in S$ then $x^{-1} \in S$. Since $R$ is a field, $x^{-1} \in R$. Since $R$ is integral over $S$, $x^{-1}$ satisfies a monic polynomial:

$$x^n = \sum_{i=0}^{n-1} a_i x^{-i}$$

where $a_i \in S$. Multiply by $x^{n-1}$ to get

$$x^{-1} = \frac{x^{n-1}}{x^n} = \sum_{i=0}^{n-1} a_i x^{n-i-1}$$

Since $n - i - 1 \geq 0$ for all $i \leq n - 1$, this is an element of $S$ and we are done. $\square$

**Theorem 4.2.** If $R = K[x_1, \ldots, x_n]$ is a field then $x_1, \ldots, x_n$ are algebraic over $K$.

*Proof.* By Noether normalization there is an algebraically independent set $Y = \{y_1, \ldots, y_r\}$ in $R$ so that $R$ is integral over $K[Y]$. Since $R$ is a field, the lemma says that $K[Y]$ must be a field. This is only possible if $r = 0$. So, $R$ is integral and thus algebraic over $K$. $\square$

**Corollary 4.3.** Suppose that $K$ is a field and $R = K[x_1, \ldots, x_n]$ is a finitely generated ring over $K$. Then there is a homomorphism

$$\varphi : R \to \overline{K}$$

of rings over $K$, i.e., so that $\varphi$ is the identity on $K$.

*Proof.* $R$ f.g. implies $R \cong K[X_1, \ldots, X_n]/I$ for some ideal $I$. ($I = \{f(X) \mid f(x) = 0\}$). Let $M$ be a maximal ideal containing $I$. Then we have an epimorphism of rings over $K$:

$$R \to K[X]/M = L$$

Since $M$ is maximal, $L$ is field. Since $L$ is an extension of $K$ which is finitely generated as a ring, the theorem says that $L$ is algebraic over
Therefore \( L \subseteq K \) and the homomorphism what we want is the composition:

\[
\varphi : R \rightarrow L \hookrightarrow K
\]

\[\square\]

Corollary 4.4. Suppose that \( R = K[x_1, \cdots, x_n] \) is a f.g. domain over \( K \). Suppose that \( y_1, \cdots, y_m \) are nonzero elements of \( R \). Then there is a homomorphism

\[
\psi : R \rightarrow K
\]

of rings over \( K \) so that \( \psi(y_i) \neq 0 \) for all \( i \).

Proof. In the quotient field \( Q(R) \) we have \( y_1^{-1}, \cdots, y_m^{-1} \). Let

\[
S = K[x_1, \cdots, x_n, y_1^{-1}, \cdots, y_m^{-1}] \subseteq Q(R)
\]

Then \( R \subseteq S \) and by the previous corollary there is a homomorphism

\[
\varphi : S \rightarrow K
\]

of rings over \( K \). \( \psi = \varphi|_R \) is the homomorphism that we want. \[\square\]

4.1. Hilbert’s Nullstellensatz. Now we can prove the theorem about zero sets of polynomials. First, I gave the definition and some examples.

Definition 4.5. Suppose that \( S \) is a subset of \( K[X] = K[X_1, \cdots, X_n] \) and \( L \) is a field extension of \( K \). Then let \( \mathcal{Z}_S(L) \) denote the set of all common zeroes of \( f_i \in S \) in \( L^n \):

\[
\mathcal{Z}_S(L) = \{ (a) = (a_1, \cdots, a_n) \in L^n \mid f_i(a) = 0 \ \forall f_i \in S \}
\]

One of the key features of the zero set is the duality between points and polynomials, namely, the equation

\[
f(a) = 0
\]

can be interpreted in two ways: \( (a) \in L^n \) is a zero of \( f \) or \( f \in K[X] \) lies in the kernel of the evaluation at \( (a) \) mapping

\[
\text{ev}_a : K[X] \rightarrow L
\]

The equivalence of these two statements gives the following lemma.

Lemma 4.6. \( (a) \in \mathcal{Z}_S(L) \iff S \subseteq \ker(\text{ev}_a) : K[X] \rightarrow L \).

Since \( S \subseteq \ker(\text{ev}_a) \) if the ideal \( (S) \) of \( K[X] \) generated by \( S \) is contained in the ideal \( \ker(\text{ev}_a) \), we get:

Proposition 4.7. \( \mathcal{Z}_S(L) = \mathcal{Z}(S)(L) \).
We are assuming the Hilbert basis theorem which implies that $K[X]$ is Noetherian. Therefore, every ideal of $K[X]$ is finitely generated. So, we may assume that $S$ is a finite set of polynomials.

Now comes the first version of the Nullstellensatz:

**Theorem 4.8.** Let $S = \{f_1, \cdots, f_m\} \subseteq K[X_1, \cdots, X_n]$ and suppose that $L \supseteq K$ is algebraically closed. Then either

1. $1 = \sum f_i \cdot g_i$ for some $g_i \in K[X]$ or
2. $\mathcal{Z}_S(L) \neq \emptyset$.

*Proof.* $(S) = \{\sum f_i \cdot g_i\}$ is either equal to $K[X]$ or it is an ideal in $K[X]$. In the first case we get $1 \in (S)$. So, $1 = \sum f_i \cdot g_i$. In the second case, $R = K[X]/(S)$ is a finitely generated ring over $K$. So, there is a homomorphism of rings over $K$:

$$\varphi : K[X]/(S) \rightarrow \overline{K} \hookrightarrow L$$

Let $a_i = \varphi(X_i)$. Then $\varphi(f) = f(a)$. Since each $f_i \in S$ is in the kernel of $\varphi$ we have $f_i(a) = 0$ for all $i$. i.e., $(a) \in \mathcal{Z}_S(L)$. \qed

**Theorem 4.9** (weak Nullstellensatz). The maximal ideals of $\overline{K}[X]$ are

$$(X_1 - a_1, X_2 - a_2, \cdots, X_n - a_n)$$

where $a_i \in \overline{K}$. (So, the maximal ideals of $\overline{K}[X]$ are in 1-1 correspondence with the points in $\overline{K}^n$.)

*Proof.* Take any ideal $I$ in $K[X]$. By the previous theorem, $\exists(a_1, \cdots, a_n) \in \mathcal{Z}_I(\overline{K})$. By the lemma, this is equivalent to:

$$I \subseteq (X_1 - a_1, \cdots, X_n - a_n)$$

If $I$ is maximal, these must be equal. \qed

**Theorem 4.10** (Hilbert’s Nullstellensatz). If $f \in K[X]$ so that $f(a) = 0$ for all $(a) \in \mathcal{Z}_S(\overline{K})$ then $f^m \in (S)$ for some $m \geq 1$.

*Proof.* Let $S = \{h_1, \cdots, h_r\}$. Introduce a new variable $Y$ and one more polynomial:

$$h_0 = 1 - Yf(X_1, \cdots, X_n)$$

Then

$$\mathcal{Z}_{h_0, h_1, \cdots, h_r} = \emptyset$$

since, for any common zero $(a_1, \cdots, a_n, b)$, we have $f(a) = 0$ by assumption and $0 = h_0(a, b) = 1 - bf(a) = 1$.
which is a contradiction. Therefore, there exist \( g_0, \ldots, g_n \in K[X,Y] \) so that
\[
1 = \sum_{i=0}^{n} g_i h_i
\]
Plugging in \( Y = 1/f(X) \) makes \( h_0 = 0 \) and we get
\[
1 = \sum_{i=1}^{n} g_i(1/f(X), X_1, \ldots, X_n) h_i(X)
\]
If \( m \) is sufficiently large then
\[
f(X)^m g_i(1/f(X), X) \in K[X]
\]
for all \( i \) and \( f^m \in (S) \). \qed
4.2. **Algebraic sets and varieties.** Now I just want to talk about the consequences of the Nullstellensatz. One formulation of the statement is that there is a 1-1 correspondence between algebraic sets and reduced ideals.

**Definition 4.11.** An *algebraic set* is a subset $A \subseteq L^n$ (where $L = \mathbb{T}$ is algebraically closed) which is defined by polynomial equations with coefficients in $K \subseteq L$. In other words, $$A = \mathcal{Z}_S(L)$$ where $S \subseteq K[X_1, \cdots, X_n], K \subseteq L$. We say that $A$ is *defined over* $K$.

**Definition 4.12.** If $A \subseteq L^n$ is an algebraic set defined over $K$ then the *associated ideal* $\mathfrak{a}$ is defined by $$\mathfrak{a} = \{ f \in K[X] \mid f(a) = 0 \ \forall (a) \in A \}$$

Hilbert’s Nullstellensatz says that if $L = \mathbb{C}$ and $\mathfrak{a} \subseteq K[X]$ is an ideal then the ideal associated to the algebraic set $\mathcal{Z}_\mathfrak{a}(L)$ is the radical $$\text{rad}(\mathfrak{a}) = \{ f \in K[X] \mid f^n \in \mathfrak{a} \text{ for some } n \geq 1 \}$$

**Definition 4.13.** The *radical* of an ideal $I$ in a ring $R$ is defined to be the set of all $f \in R$ so that some positive power of $f$ lies in $I$. The radical of $I$ is written $\text{rad}(I)$.

Some people write the radical of $I$ as $\sqrt{I}$. (But then we get silly things like: $\sqrt{(8)} = (2)$.)

**Definition 4.14.** The *radical* of the ring $R$ is defined to be the radical of the ideal $0$: $$\text{rad}(R) := \text{rad}(0) = \{ r \in R \mid r^n = 0 \text{ for some } n \geq 1 \}$$

**Proposition 4.15.** $\text{rad}(I) = \pi^{-1} \text{rad}(R/I)$ where $\pi : R \to R/I$ is the quotient map.

*Proof.* $x^n \in I \iff (x + I)^n = I$. $\square$

Now we can restate the Nullstellensatz again: It says that there is a 1-1 correspondence between algebraic subsets of $L^n$ defined over $K$ and ideals $\mathfrak{a}$ in $K[X_1, \cdots, X_n]$ so that $\text{rad}(\mathfrak{a}) = \mathfrak{a}$ (we call such ideals *reduced*).

$$\{\text{algebraic sets}\} \cong \{\text{reduced ideals}\}$$

$$A \subseteq L^n \text{ defined}/K \quad \mathfrak{a} \subseteq K[X_1, \cdots, X_n]$$

Note that
a) This bijection is inclusion reversing:
\[ a \subseteq b \iff Z_a \supseteq Z_b \]

Assuming the Hilbert basis theorem \((K[X] \text{ is Noetherian})\), this has the following immediate consequence.

**Proposition 4.16.** Algebraic sets satisfy the DCC.

**Proof.** Suppose that \( A_1 \supseteq A_2 \supseteq A_3 \supseteq \cdots \) is a descending sequence of algebraic subsets of \( L^n \). Then the associated ideals form an ascending sequence: \( a_1 \subseteq a_2 \subseteq a_3 \subseteq \cdots \). So, it eventually stops: \( a_N = a_{N+1} = \cdots \). And the corresponding algebraic sets must be equal: \( A_N = A_{N+1} = \cdots \). \( \square \)

One consequence of this is that every algebraic set decomposes as a finite union of irreducible sets.

4.2.2. **irreducible sets.**

**Definition 4.17.** An algebraic set defined over \( K \) is called \( K\text{-irreducible} \) if it is not the union of two proper algebraic subsets. An irreducible algebraic set is called an \( \text{affine variety} \) over \( K \).

When people talk about varieties they often view \( L \) as being variable. Lang formalizes this by saying calling the function \( L \mapsto Z_a(L) \) an algebraic space and defining a variety as an algebraic space rather than an irreducible algebraic set.

The field of definition is very important. For example, the two point set \( A = \{i, -i\} \subset \mathbb{C} \) is \( \mathbb{R}\text{-irreducible} \) but not \( \mathbb{C}\text{-irreducible} \). This has many explanations. It is because the polynomial \( f(X) = X^2 + 1 \) which defines this set is irreducible over \( \mathbb{R} \) but not over \( \mathbb{C} \). Another way to say it is that the Galois group of \( \mathbb{C}/\mathbb{R} \) acts transitively on the set.

**Corollary 4.18.** Every algebraic set is a finite union of irreducible sets.

**Proof.** Suppose that \( A \) is not a finite union of irreducible sets. Then it is not irreducible. So \( A = A_0 \cup A_1 \). Either \( A_0 \) or \( A_1 \) is not a finite union of irreducible sets (otherwise we get a contradiction). Suppose it is \( A_0 \). Then \( A_0 = A_{00} \cup A_{01} \) where one of the pieces is not a finite union of irreducibles, etc. This contradicts the DCC. So, the corollary holds. \( \square \)

Another feature of the algebraic set–reduced ideal correspondence:

b) It converts products into unions, e.g.
\[ Z_{fg} = Z_f \cup Z_g \]
if \( f, g \in K[X] \). We will discuss products of ideals later.

This has the following important consequence.

**Theorem 4.19.** A is \( K \)-irreducible iff the associated ideal \( a \subset K[X] \) is prime.

The proof is easy if you realize that the Nullstellensatz can be formulated in the following way:

**Lemma 4.20.** Suppose \( a \subset K[X] \) is a reduced ideal, \( f \in K[X] \) and \( K \subseteq L = \overline{L} \). Then \( f \in a \) iff \( \mathcal{Z}_a(L) \subseteq \mathcal{Z}_f(L) \).

4.2.3. coordinate ring. For the next subtopic I need to assume that \( K = \overline{K} = L \) and \( A \subset K^n \) is an irreducible algebraic set with associated (prime) ideal \( p \subset K[X] \). In that case the **coordinate ring of** \( A \) is defined by

\[
R := K[X]/p
\]

This can be interpreted as the ring of all polynomial functions

\[ A \to K \]

since two polynomials \( f, g \in K[X] \) give the same function \( A \to K \) iff \( f - g = 0 \) on \( A \). By the Nullstellensatz this is equivalent to saying that \( f - g \in \text{rad } p = p \).

**Lemma 4.21.** Suppose that \( I \) is an ideal in a ring \( R \). Then the maximal ideals of \( R/I \) are \( m/I \) where \( m \) is a maximal ideal of \( R \) containing \( I \).

**Proof.** What I said in class was that \( m \) is a maximal ideal in \( R \) iff \( R/m \) is a field. But

\[
\frac{R}{m} \cong \frac{R/I}{m/I}
\]

which is a field iff \( m/I \) is a maximal ideal in \( R/I \). This proof assumes that \( m \subseteq R \) is an ideal containing \( I \).

Suppose that \( M \) is a maximal ideal in \( R/I \). Then \( M \) is the kernel of an epimorphism \( \phi : R/I \to K \) where \( K \) is a field. Let \( m = \pi^{-1}(M) \) be the inverse image of \( M \) under \( \pi : R \to R/I \). Then \( m \subseteq R \) is an ideal containing the kernel \( I \) of \( \pi \). So the previous paragraph applies. \( \square \)

To apply this lemma to the coordinate ring \( R = K[X]/p \) we need to recall the weak Nullstellensatz which says that the maximal ideals of \( K[X] \) are \( (X_1 - a_1, \ldots, X_n - a_n) \) where \( (a) = (a_1, \ldots, a_n) \in K^n \). This ideal is the kernel of the evaluation map:

\[ \text{ev}_{(a)} : K[X] \to K \]
And you need to remember that $S$ is contained in this kernel iff $(a) \in \mathcal{Z}_S(K)$. Putting $S = p$ we see that $p$ is contained in $(X_1 - a_1, \ldots, X_n - a_n)$ iff $(a) \in A = \mathcal{Z}_p(K)$. This proves the following.

**Theorem 4.22.** There is a 1-1 correspondence between the points of $A$ and the maximal ideals of the coordinate ring $R$ of $A$. \qed