# M3P8 LECTURE NOTES 13: INTRODUCTION TO ALGEBRAIC GEOMETRY

## 1. Algebraically closed fields

**Definition 1.1.** Let $k$ be a field. We say $k$is *algebraically closed* if every polynomial $P(X) \in k[X]$ factors into linear factors.

The Fundamental Theorem of Algebra states that the field $\mathbb{C}$ is algebraically closed. We won't prove this in this course; ultimately it requires some analysis (this is unsurprising, since the construction of $\mathbb{C}$ is fundamentally an analytic one.) We have the following characterization of algebraically closed fields:

**Lemma 1.2.** *A field $k$ is algebraically closed if, and only if, every field extension $L/k$ is either trivial (i.e. $L = k$) or transcendental.*

*Proof.* Suppose $k$ is algebraically closed. Let $L/k$ be an algebraic extension, and $\alpha \in L$. Let $P(X)$ be the minimal polynomial of $\alpha$ over $k$. Then $P(X)$ is irreducible, hence linear. But then $\alpha \in k$, so $L = k$. Conversely, if every field extension $L/k$ is trivial or transcendental, then if $P(X)$ is an irreducible polynomial in $k[X]$ we must have $k[X]/\langle P(X)\rangle = k$, so $P(X)$ must have degree one. Since every polynomial in $k[X]$ factors into irreducibles, $k$ must be algebraically closed. □

## 2. Affine algebraic sets

Fix an algebraically closed field $k$. (In fact, it is harmless to take $k = \mathbb{C}$ throughout.)

Let $\mathbb{A}^n_k$ (*affine $n$-space over $k$*) denote the set $k^n$ of $n$-tuples of elements of $k$. For $S$ an arbitrary collection of elements of $k[X_1, \ldots, X_n]$, we let $Z(S)$ denote the subset of $\mathbb{A}^n_k$ consisting of all elements $(x_1, \ldots, x_n)$ of $k^n$ such that $P(x_1, \ldots, x_n) = 0$ for all $P(X_1, \ldots, X_n) \in S$. (In other words, $Z(S)$ is the set of *common zeros* of all the polynomials in $S$.) Note that we have:

**Lemma 2.1.** *Let $S$ be a subset of $k[X_1, \ldots, X_n]$ and let $I$ be the ideal of $k[X_1, \ldots, x_n]$ generated by $S$. Then $Z(I) = Z(S)$.*

*Proof.* Since $S \subseteq I$, we have $Z(I) \subseteq Z(S)$. On the other hand, let $(x_1, \ldots, x_n) \in Z(S)$. Then for all $P(X_1, \ldots, X_n) \in S$, we have $P(x_1, \ldots, x_n) = 0$. But then for any finite collection $P_1, \ldots, P_r$ of polynomials in $S$, and any polynomials $Q_1, \ldots, Q_r$ in $k[X_1, \ldots, X_n]$, we have $Q_1(x_1, \ldots, x_n)P_1(x_1, \ldots, x_n) + \cdots + Q_r(x_1, \ldots, x_n)P_r(x_1, \ldots, x_n) = 0$. Since any polynomial in $I$ can be expressed as $Q_1P_1 + \cdots + Q_rP_r$ we have that $(x_1, \ldots, x_n) \in Z(I)$. □

From this and the Hilbert basis theorem we deduce: For any set $S$ of polynomials in $k[X_1, \ldots, X_n]$ there is a finite collection $S'$ of polynomials such that $Z(S) = Z(S')$ (just let $S'$ be a generating set for the ideal generated by $S$).

**Definition 2.2.** A subset $X$ of $\mathbb{A}^n_k$ is called an *affine algebraic set* if $X$ is for the form $Z(I)$ for some ideal $I$ of $k[X_1, \ldots, X_n]$.

Conversely, subsets of $\mathbb{A}^n_k$ define ideals of $k[X_1, \ldots, X_n]$. For $X \subseteq \mathbb{A}^n_k$, let $I(X)$ denote the ideal consisting of all polynomials $P(X_1, \ldots, X_n)$ such that $P(x_1, \ldots, x_n) = 0$ for all $(x_1, \ldots, x_n) \in X$. Note that the operations $X \mapsto I(X)$ and $I \mapsto Z(I)$ are both inclusion-reversing: if $Y \subseteq X$ then $I(X) \subseteq I(Y)$ and if $I \subseteq J$ then $Z(J) \subseteq Z(I)$. We have:

**Lemma 2.3.** *Let $X$ be an affine algebraic set. Then $Z(I(X)) = X$.*

*Proof.* Certainly any element of $I(X)$ vanishes at all points of $X$, so $X \subseteq Z(I(X))$. On the other hand, since $X$ is an affine algebraic set, $X = Z(J)$ for some ideal $J$. Since any $P \in J$ vanishes on $X$ we have $J \subset I(X)$. Then $Z(I(X)) \subseteq Z(J) = X$, so $X = Z(I(X))$. □

If $X$ is not an affine algebraic set, then $Z(I(X))$ is the smallest affine algebraic set containing $X$. (If $Y = Z(J)$ contains $X$, then $I(Y) \subseteq I(X)$, so $Z(I(X)) \subseteq Z(I(Y)) = Y$.) We call $Z(I(X))$ the *Zariski closure* of $X$; this operation is the closure operation for a topology on $\mathbb{A}^n_k$ called the *Zariski topology* which we will define later.

One might thus hope that similarly $I(Z(J)) = J$ for any ideal $J$ of $k[X_1, \ldots, X_n]$. This can't be literally true, for the following reason: note that for any $X$, the ideal $I(X)$ is a radical ideal: if a polynomial $P$ satisfies $P^n \in I(X)$ then $P^n(x_1, \ldots, x_n) = 0$ for all $(x_1, \ldots, x_n) \in X$. But then $P(x_1, \ldots, x_n) = 0$ as well, so $P \in I(X)$. Thus if $J$ is not a radical ideal we can't have $I(Z(J)) = J$. However, one does have:

**Theorem 2.4.** *(Hilbert's Nullstellensatz): Let $k$ be an algebraically closed field. For any ideal $J$ of $k[X_1, \ldots, X_n]$, we have $I(Z(J)) = \operatorname{rad} J$.*

We will prove this theorem later on. For now, we note that since $\operatorname{rad} \operatorname{rad} J = \operatorname{rad} J$ for all ideals $J$, the maps $X \mapsto I(X)$ and $J \mapsto Z(J)$ define a bijection between *radical ideals* (that is, ideals $J$ such that $\operatorname{rad} J = J$) and affine algebraic sets. This bijection is inclusion-reversing, and it is interesting to ask what geometric properties of $X$ are carried to algebraic properties of $I(X)$ via this bijection.

For instance:

**Proposition 2.5.** *Let $I$ and $J$ be ideals. Then $Z(I + J) = Z(I) \cap Z(J)$ and $Z(I \cap J) = Z(I) \cup Z(J)$. Conversely, if $X$ and $Y$ are affine algebraic sets, then $I(X \cap Y) = \operatorname{rad}(I(X) + I(Y))$ and $I(X \cup Y) = I(X) \cap I(Y)$.*

*Proof.* Let $p \in \mathbb{A}^n_k$ be a point of $Z(I + J)$. Then every element of $I + J$ vanishes at $p$, so since $I \subseteq I + J$ we have that $p \in Z(I)$. Similarly $p \in Z(J)$,

so $Z(I+J) \subseteq Z(I) \cap Z(J)$. Conversely, if $p \in Z(I) \cap Z(J)$, then for any element $Q$ of $I+J$ we can write $Q = R+S$ with $R \in I$ and $S \in J$. Then $R(p) = S(p) = 0$, so $Q(p) = 0$ and $p \in Z(I+J)$. The proof that $Z(I \cap J) = Z(I) \cup Z(J)$ is similar, and will be omitted.

The remaining statements $I(X \cap Y) = \mathrm{rad}(I(X)+I(Y))$ and $I(X \cup Y) = I(X) \cap I(Y)$ follow from the first two using the Nullstellensatz. □

**Definition 2.6.** An affine algebraic set $X$ is *irreducible* if $X$ cannot be written as the union $Y \cup Z$ of two *proper* affine algebraic subsets $Y$ and $Z$.

**Proposition 2.7.** *An affine algebraic set $X$ is irreducible if, and only if, $I(X)$ is prime.*

*Proof.* Suppose $X$ is irreducible, and let $P, Q$ be elements of $k[X_1, \ldots, X_n]$ such that $PQ \in I(X)$. Then $X \subseteq Z(PQ) = Z(P) \cap Z(Q)$. In particular $X = (X \cap Z(P)) \cup (X \cap Z(Q))$. Since $X$ is irreducible we must have $X = X \cap Z(P)$ (in which case $P \in I(X)$) or $X = X \cap Z(Q)$ (in which case $Q \in I(X)$.) So $I(X)$ is prime.

Conversely, suppose $I(X)$ is prime, and that $X = Y \cup Z$, where $Y$ and $Z$ are affine algebraic subsets of $X$. Then $I(X) = I(Y) \cap I(Z)$, so $I(X)$ contains the product $I(Y)I(Z)$. Since $I(X)$ is prime, either $I(X)$ contains $I(Y)$ (in which case $X = Y$) or $I(X)$ contains $I(Z)$ (in which case $X = Z$). □

The Hilbert Basis Theorem then gives us:

**Proposition 2.8.** *Let $X$ be an affine algebraic set. Then $X$ can be written uniquely as a finite union $X_1 \cup X_2 \cup \cdots \cup X_r$ such that each $X_i$ is an irreducible affine algebraic set and no $X_i$ is contained in $X_j$ for $i \neq j$.*

*Proof.* We first show that if $X$ is not irreducible, then $X$ can be written as $Y \cup Z$ with $Y$ irreducible and $Z \neq X$ affine algebraic. Certainly we can write $X = Y_1 \cup Z_1$ with $Y_1, Z_1$ proper subsets of $X$. If $Y_1$ is irreducible we are done; otherwise write $Y_1 = Y_2 \cup Z_2$. Again, if $Y_2$ is irreducible we can write $X = Y_2 \cup (Z_1 \cup Z_2)$ and we are done. Otherwise, supposing this never terminates, we obtain:

$$Y_1 \supsetneq Y_2 \supsetneq Y_3 \ldots$$
$$I(Y_1) \subsetneq I(Y_2) \subsetneq I(Y_3) \ldots$$

which is impossible since $k[X_1, \ldots, X_n]$ is Noetherian.

Now given $X$, if $X$ is not irreducible we can write $X = Y_1 \cup Z_1$ with $Y_1$ irreducible and $Z_1 \neq X$. If $Z_1$ is not irreducible we write $Z_1 = Y_2 \cup Z_2$ with $Y_2$ irreducible and $Z_2 \neq Z_1$. If this process ever terminates we have written $X$ as a finite union of irreducibles. Otherwise, we have

$$Z_1 \supsetneq Z_2 \supsetneq Z_3 \ldots$$

and as above this is impossible since $k[X_1, \ldots, X_n]$ is Noetherian.

For uniqueness, suppose we have $X = Y_1 \cup \cdots \cup Y_r$ and $X = Z_1 \cup \cdots \cup Z_s$ with the $Y_i$ and $Z_j$ irreducible, and with no $Y_i$ (resp. $Z_i$) contained in $Y_j$ (resp. $Z_j$) when $i \neq j$. Then $I(Y_i)$ and $I(Z_i)$ are prime for all $i$. In particular

$I(Y_1)$ is prime. Since $Y_1 \subset X$, $I(X) \subset I(Y_1)$, so $I(Y_1)$ contains $I(Z_1 \cup \cdots \cup Z_s) = I(Z_1) \cap \cdots \cap I(Z_s)$. It follows that $I(Y_1)$ contains the product $I(Z_1)I(Z_2)\ldots I(Z_s)$. Thus $I(Y_1)$ contains $I(Z_j)$ for some $j$. Similarly $I(Z_j)$ contains $I(Y_i)$ for some $i$. Then $I(Y_1) \subseteq I(Y_i)$, so $Y_i \subseteq Y_1$ and we must have $i = 1$. Then $Y_1 = Z_j$. Proceeding we show that each $Y_i$ is equal to some $Z_j$ and vice versa, proving uniqueness. □

Translating this to a statement about ideals, we find:

**Corollary 2.9.** *Every radical ideal in $k[X_1, \ldots, X_n]$ is uniquely expressible as a finite intersection of prime ideals, none of which contains any of the others.*

This is a special case of a very general ring-theoretic phenomenon known as *primary decomposition*, which was discovered via the sort of geometric considerations we see above.

## 3. Proof of the Nullstellensatz

The ideas above rely heavily on the correspondence between radical ideals and affine algebraic sets, and thus ultimately on the Nullstellensatz. We now give a proof of the Nullstellensatz. The first step is to show that to prove the Nullstellensatz it suffices to prove the following, seemingly much weaker, special case (the so-called "Weak Nullstellensatz"):

**Theorem 3.1.** *Let $I$ be an ideal of $k[X_1, \ldots, X_n]$ such that $Z(I)$ is empty. Then $I$ is the unit ideal.*

*Proof that the weak Nullstellensatz implies the Nullstellensatz:* Let $J$ be an ideal of $k[X_1, \ldots, X_n]$. Clearly $I(Z(J))$ contains $\operatorname{rad} J$; we must show the reverse containment. Let $P$ be an element of $I(Z(J))$. We must show that $P^m$ lies in $J$ for some $m$. Consider the ring $k[X_1, \ldots, X_n, T]$, and let $\tilde{J}$ be the ideal of $k[X_1, \ldots, X_n, T]$ generated by the polynomials in $I$, together with the polynomial $1 - TP(X_1, \ldots, X_n)$. Consider the subset $Z(\tilde{J})$ of $\mathbb{A}_k^{n+1}$; this consists of elements $(x_1, \ldots, x_n, t)$ of $k^{n+1}$ such that $Q(x_1, \ldots, x_n) = 0$ for all $Q \in J$, and $1 - tP(x_1, \ldots, x_n) = 0$. In particular if $(x_1, \ldots, x_n, t)$ lies in $Z(\tilde{J})$, then $(x_1, \ldots, x_n)$ lies in $Z(J)$. Since $P \in I(Z(J))$ we have $P(x_1, \ldots, x_n) = 0$, so $1 - tP(x_1, \ldots, x_n) = 1$. Thus $Z(\tilde{J})$ is empty.

By the weak Nullstellensatz, $\tilde{J}$ is the unit ideal, so there are polynomials $Q_0, Q_1, \ldots, Q_s$ in $k[X_1, \ldots, X_n, T]$, and $R_1, \ldots, R_s \in I$, such that

$$1 = Q_0(1 - TP) + Q_1R_1 + \cdots + Q_sR_s.$$

Consider the map: $k[X_1, \ldots, X_n, T] \to k[X_1, \ldots, X_n, \frac{1}{P}]$ that is the identity on $k[X_1, \ldots, X_n]$ and sends $T$ to $\frac{1}{P}$. Applying this map we find that

$$1 = Q_1(X_1, \ldots, X_n, \frac{1}{P})R_1(X_1, \ldots, X_n) + \cdots + Q_s(X_1, \ldots, X - n, \frac{1}{P})R_s(X_1, \ldots, X_n)$$

in $k[X_1, \ldots, X_n, \frac{1}{P}]$. Multiplying by a sufficiently large power of $P$, we get

$$P^m = P^m Q_1(X_1, \ldots, X_n, \frac{1}{P}) R_1(X_1, \ldots, X_n) + \cdots + P^m Q_s(X_1, \ldots, X_n, \frac{1}{P}) R_s(X_1, \ldots, X_n).$$

Since for $m$ sufficiently large $P^m Q_s(X_1, \ldots, X_n, \frac{1}{P})$ is a polynomial in the $X_i$ we find that $P^m \in I$ for $m$ sufficiently large. $\square$

It remains to prove the weak Nullstellensatz. This requires some new ideas; the following approach is due to Emmy Noether.

**Definition 3.2.** Let $R$ be a $k$-algebra; that is a ring together with a map $k \to R$. We say that elements $y_1, \ldots, y_s$ of $R$ are *algebraically independent* over $k$ if there is no nonzero polynomial $P(X_1, \ldots, X_s) \in k[X_1, \ldots, X_s]$ such that $P(y_1, \ldots, y_s) = 0$. (Equivalently, $y_1, \ldots, y_s$ are algebraically independent if, and only if, the map $k[X_1, \ldots, X_s] \to R$ taking $X_i$ to $y_i$ is injective.)

**Proposition 3.3.** *(Noether's normalization lemma) Let $k$ be a field, and let $R$ be a finitely generated $k$-algebra. Then there exists a nonnegative integer $s$, and algebraically independent elements $y_1, \ldots, y_s$ of $R$ such that $R$ is integral over $k[y_1, \ldots, y_s]$.*

*Proof.* Write $R = k[X_1, \ldots, X_m]/I$. We proceed by induction on $m$. The base case $m = 0$ is clear. Fix $m$ and assume the claim is true for $m - 1$.

If $I = 0$ then the statement is also clear, with $y_i = X_i$ for all $i$. Otherwise let $P(X_1, \ldots, X_n) \in I$. Renumbering the variables if necessary, we may assume $f$ is a nonconstant polynomial in $X_m$ with coefficients in $X_1, \ldots, X_{m-1}$. Let $d$ be the *total degree* of $P$ (that is, the largest value of $a_1 + \cdots + a_m$ for any monomial $cX_1^{a_1} X_2^{a_2} \ldots X_m^{a_m}$ appearing in $P$.) Let $n_i = (1 + d)^i$ for $i$ in $1...m - 1$, and let $Y_i = X_i - X_m^{n_i}$ for each $i$ in $1...m - 1$. Define

$$Q(X_1, \ldots, X_m) = P(X_1 + X_m^{n_1}, \ldots, X_{n-1} + X_m^{n_{m-1}}, X_m).$$

Then $Q(Y_1, \ldots, Y_{m-1}, X_m)$ is zero in $R$.

We now claim that, up to a factor $c \in k^\times$, $Q(X_1, \ldots, X_m)$ is *monic* when considered as a polynomial in $X_m$. Let $cX_1^{a_1} \ldots X_m^{a_m}$ be a monomial appearing in $P(X_1, \ldots, X_m)$. This monomial contributes the following terms to $Q(X_1, \ldots, X_m)$:

$$c(X_1 - X_m^{n_1})^{a_1} \ldots (X_{m-1} - X_m^{n_{m-1}})^{a_{m-1}} X_m^{a_m}.$$

Moreover, each $n_i$ is greater than $d$ and hence greater than the *sum* of the $a_j$. It is thus clear that the term of higest degree in the above expression is $cX_m^N$, where

$$N = n_1 a_1 + \cdots + n_{m-1} a_{m-1} + a_m = a_1(1 + d) + \cdots + a_{m-1}(1 + d)^{m-1} + a_m.$$

Since $1 + d$ is greater than the sum of the exponents $a$ appearing in *any* monomial of $P(X_1, \ldots, X_m)$, the terms $cX_m^N$ appearing in different monomials are all of different degree and thus cannot cancel. It follows that the term of the form $cX_m^N$ of highest degree is the highest degree term in $Q(X_1, \ldots, X_n)$, so that $\frac{1}{c} Q(X_1, \ldots, X_m)$ is monic in $X^m$.

Write

$$\frac{1}{c}Q(X_1,\dots,X_m)=\sum_n H_n(X_1,\dots,X_{n-1})X_m^n.$$

Since $Q(Y_1,\dots,Y_{m-1},X_m)=0$, we have

$$\sum_n H_n(Y_1,\dots,Y_{m-1})X_m=0.$$

That is, $X_m$ is integral over the subalgebra $S=k[Y_1,\dots,Y_{m-1}]$ of $R$. Since $X_m$ generates $R$ over $S$, it follows that $R$ is integral over $S$.

On the other hand we have a map $k[Z_1,\dots,Z_{m-1}]\to S$ taking $Z_i$ to $Y_i$ for all $I$. Let $J$ be the kernel. Then $S=k[Z_1,\dots,Z_{m-1}]/J$. Then by the inductive hypothesis there are algebraically independent elements $y_1,\dots,y_s\in S$ such that $S$ is integral over $k[y_1,\dots,y_s]$. Since $R$ is integral over $S$, it follows that $R$ is integral over $k[y_1,\dots,y_s]$ and we are done. □

**Corollary 3.4.** *Every maximal ideal of $k[X_1,\dots,X_n]$ is of the form $\langle X_1-p_1,\dots,X_n-p_n\rangle$ for some $p_1,\dots,p_n\in k$.*

*Proof.* Let $I$ be a maximal ideal of $k[X_1,\dots,X_n]$, and consider $R=k[X_1,\dots,X_n]/I$. Then $R$ is a field. On the other hand, by Noether normalization, there exist $y_1,\dots,y_s$ algebraically independent such that $R$ is integral over $S=k[y_1,\dots,y_s]$. Let $x$ be a nonzero element of $k[y_1,\dots,y_s]$; then $x^{-1}$ lies in $R$. Since $R$ is integral over $S$ there is a monic polynomial $P$ with coefficients in $S$ such that $P(x^{-1})=0$. We thus have:

$$(x^{-1})^d=\sum_{i=0}^{d-1}a_ix^{-i}$$

with $a_i\in S$. Multiplying by $x^{d-1}$ we find that

$$x^{-1}=\sum_{i=0}^{d-1}a_ix^{d-i-1}$$

so that $x^{-1}$ is also in $S$. Thus $S$ is a field. But since the $y_i$ are algebraically independent, $S$ is also a polynomial ring in $s$ variables; since no such ring is a field unless $s=0$ we must have $s=0$ and $R$ is integral over $k$. But then $R$ is a finite-dimensional $k$-vector space, hence a finite extension of $k$. Since $k$ is algebraically closed, the inclusion of $k$ in $R$ is an isomorphism.

Thus for each $i$ there is an element $p_i$ of $k$ such that $X_i$ is equal to $p_i$ in $R$. Then $X_i-p_i$ is in $I$ for all $i$, so $I$ contains the ideal $\langle X_1-p_1,\dots,X_n-p_n\rangle$. Since the latter is clearly maximal it must be equal to $I$. □

*Proof of the Weak Nullstellensatz*: Let $I$ be an ideal of $k[X_1,\dots,X_n]$ such that $I$ is not the unit ideal. Then $I$ is contained in some maximal ideal of $k[X_1,\dots,X_n]$, and thus in some ideal of the form $\langle X_1-p_1,\dots,X_n-p_n\rangle$. Then $(p_1,\dots,p_n)$ lies in $Z(I)$.□