1. Lecture 1

In this course, we will work over an algebraically closed field k. Unless explicitly specified, we will always assume that the ground field is algebraically closed. We will assume that our rings are commutative with unit.

Definition 1.1. *Affine n-space over k, denoted by $\mathbb{A}^n_k$, is the space of n-tuples in k. A closed algebraic set is the zero locus of a set of polynomials in $k[x_1, \ldots, x_n]$. Given a set of polynomials $\{f_\alpha\}_{\alpha \in A}$, we will denote the algebraic set they define by $V(\{f_\alpha\}_{\alpha \in A})$. When the ground field is clear from the context we will omit it from the notation.*

When $n = 2$, it is customary to set $x_1 = x, x_2 = y$. Similarly when $n = 3$, it is common to use x, y, z as the variables.

Example 1.2. (1) Let $f \in k[x_1, \ldots, x_n]$ be a non-constant polynomial. Then $V(f) \subset \mathbb{A}^n$ is called the hypersurface defined by f. If the degree of f is one, then the corresponding hypersurface is called a hyperplane. If the degree of f is two, then the corresponding hypersurface is called a quadric hypersurface. You should be familiar with linear and quadric hypersurfaces from past courses. For example, describe the following quadric hypersurfaces

$$V(x^2 + y^2 - 1),\ V(xy - 1),\ V(x^2 + y^2 + z^2 - 1)$$

(2) A point $(\alpha_1, \ldots, \alpha_n)$ in $\mathbb{A}^n$ is an algebraic set. It can be defined as the simultaneous zero locus of the polynomials $x_i - \alpha_i$ for $i = 1, \ldots, n$. The set consisting of the pair of points $\{(0, 0), (1, 1)\}$ in $\mathbb{A}^2$ is an algebraic set. It is the zero locus of the set of polynomials $x - y$ and $x(x - 1)$. The set of three points $\Gamma_1 = \{(0, 0), (1, 1), (2, 2)\}$ is an algebraic set defined by the polynomials $x - y$ and $x(x - 1)(x - 2)$. The set of three points $\Gamma_2 = \{(0, 0), (0, 1), (1, 0)\}$ is also an algebraic set. It can be defined by the polynomials $x(x - 1), y(y - 1)$ and xy.

These simple examples already raise many questions. For instance, take the two sets Γ_1, Γ_2. Although they are both sets of three points in $\mathbb{A}^2$, their equations look very different. Try to answer the questions: Can Γ_1 be defined by equations of degree at most two? Did we need three equations to define Γ_2? Could we have done it with two? What is special about the three equations given in the example? We will return to these questions in the future.

There is a dictionary between algebra (sets of polynomials in $k[x_1, \ldots, x_n]$) and geometry (sets of points in $\mathbb{A}^n$). Next we would like to make this correspondence more precise.

Let X be an algebraic set. The set of polynomials vanishing on X

$$I(X) = \{f \in k[x_1, \ldots, k_n] \mid f(x) = 0 \ \text{ for all } \ x \in X\}$$

forms an ideal.

Our definition of algebraic set, a priori, does not preclude the possibility that it might require infinitely many polynomials to define it. In fact, the Hilbert basis theorem guarantees that every ideal in $k[x_1, \ldots, x_n]$, in particular $I(X)$, is finitely generated. Hence, any algebraic set can be defined as the zero locus of finitely many polynomials.

We will briefly sketch the proof of the Hilbert basis theorem. We begin with the definition of a Noetherian ring.

Definition 1.3. *A ring R is called Noetherian if it satisfies any of the following equivalent definitions:*

(1) *Every ascending chain of ideals*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$$

in R stabilizes (i.e., there exists N such that for all $n \geq N$, $I_n = I_N$).

(2) *Every ideal in R is finitely generated.*

(3) *Every non-empty set S of ideals has a maximal element (i.e., an ideal $I \in S$ with the property that if $I \subseteq J$ and $J \in S$, then $I = J$).*

Example 1.4. A field k is a Noetherian ring since it has only two ideals (0) and k.

Theorem 1.5 (Hilbert basis theorem)**.** *If R is a noetherian ring, then $R[x]$, the polynomial ring over R, is also Noetherian.*

By induction, we conclude that $k[x_1, \ldots, x_n]$ is Noetherian. Hence, every ideal in $k[x_1, \ldots, x_n]$ is finitely generated.

Proof. Let I be an ideal in $R[x]$. We show that I is finitely generated. The main trick is the following. Let I_i be the ideal consisting of 0 and the leading coefficients of the polynomials of degree i in I (Exercise: check that I_i is an ideal). By multiplying a polynomial of degree i with x we obtain a polynomial of degree $i+1$ with the same leading coefficient. Consequently, we have an ascending chain of ideals

$$I_1 \subset I_2 \subset \cdots$$

in R. Since R is Noetherian, this chain stabilizes at some N. Choose generators $a_{i,j}$ for the ideal I_i for $i \leq N$. Since R is Noetherian, these ideals are all finitely generated. Hence, we have a finite number of generators in total. For each $a_{i,j}$ pick a polynomial $f_{i,j}$ of degree i in I with leading coefficient $a_{i,j}$. We claim that these polynomials generate I. Let $f \in I$ have degree d, then we can construct an element g in the ideal generated by $f_{i,j}$ such that $f - g$ has degree at most $d-1$. By induction on the degree of f, we conclude that f is in the ideal generated by $f_{i,j}$. □

More generally, we can define a Noetherian module as a module that satisfies any of the following equivalent properties:

(1) Every ascending chain of submodules

$$M_1 \subseteq M_2 \subseteq M_3 \subseteq \cdots$$

of M stabilizes.
(2) Every submodule of M is finitely generated.
(3) Every non-empty set S of submodules of M has a maximal element.

The following properties are frequently used in algebraic geometry. You should verify them for yourself.

Proposition 1.6. (1) *Let M be a Noetherian module. Then every submodule and every factor module of M is also Noetherian.*
(2) *Let M be a module and let N be a submodule of M. If both N and M/N are Noetherian, then M is Noetherian.*
(3) *Let R be a Noetherian ring, then a finitely generated R module is Noetherian.*

Note that if X_α are closed algebraic sets indexed by a set A, then their intersection $\cap_{\alpha \in A} X_\alpha$ is also a closed algebraic set. It can be defined by the union of the sets of polynomials defining each X_α. The union of two closed algebraic sets $X_1 \cup X_2$ is also algebraic. If $f_1, \ldots, f_n$ define X_1 and $g_1, \ldots, g_m$ define X_2, then the set of polynomials $f_i g_j$, as i varies between 1 and n and j varies between 1 and m, define the union. By induction, any finite union of closed algebraic sets is also algebraic. Finally, note that $\emptyset = V(1)$ and $\mathbb{A}^n = V(0)$ are also algebraic. We conclude that if we define closed subsets of $\mathbb{A}^n$ as the closed algebraic sets, then we obtain a topology on $\mathbb{A}^n$ called the Zariski topology. Unless explicitly explicitly stated, we will always assume that $\mathbb{A}^n$ is endowed with the Zariski topology.

A word of caution is in order. The Zariski topology is drastically different than most topologies you have encountered thus far. For example, it is almost never Hausdorff. Consider $\mathbb{A}^1_k$. Since $k[x]$ is a principal ideal domain, if I is a proper, non-zero ideal in $k[x]$, then in is generated by a single polynomial

f. Since k is algebraically closed, f is a product of linear terms $\Pi_i(x-\alpha_i)$. Hence any non-empy, proper closed set of $\mathbb{A}^1_k$ is a finite set of points. In particular, note that any two non-empty open sets intersect non-trivailly. Hence, the topology is not Hausdorff. To note another unusual feature, note that the product topology on $\mathbb{A}^1 \times \mathbb{A}^1$ differs from the Zariski topology on $\mathbb{A}^2$.

Next we would like to better understand the dictionary between geometry and algebra.

Proposition 1.7. *We have the following inclusions.*

(1) *If $X_1 \subset X_2$, then $I(X_2) \subset I(X_1)$.*
(2) *If $I_1 \subset I_2$, then $V(I_2) \subset V(I_1)$.*
(3) *$V(I(X)) = X$.*
(4) *$I_0 \subset I(V(I_0))$*

Example 1.8. Different ideals may define the same zero set. For instance, consider the ideals (x^n, y^m) for positive n, m. The ideals generated by these polynomials are different for different pairs (n, m). However, they all vanish at the origin. This example raises the question of characterizing ideals that arise as $I(X)$. Hilbert's nullstellensatz provides the answer.

Definition 1.9. *The radical $\sqrt{I}$ of an ideal $I \subset R$ is defined as the set of $f \in R$ such that $f^m \in I$ for some positive m. An ideal I is called radical if $I = \sqrt{I}$.*

Check that the radical of an ideal is also an ideal. Show that prime ideals are radical.

Theorem 1.10 (Hilbert's Nullstellensatz: weak form)**.** *Let k be an algebraically closed field. Then the maximal ideals in $k[x_1, \ldots, x_n]$ have the form*

$$(x_1 - a_1, \ldots, x_n - a_n) \quad \text{for} \quad n \quad \text{elements} \quad a_1, \ldots, a_n \in k.$$

Note that this theorem gives a one-to-one correspondence between maximal ideals in $k[x_1, \ldots, x_n]$ and points in $\mathbb{A}^n_k$ provided that the field k is algebraically closed. The assumption that the field k is algebraically closed is necessary. For instance, that the ideal generated by $x^2 + 1$ in $\mathbb{R}[x]$ is maximal, but does not correspond to any points in $\mathbb{A}^1_{\mathbb{R}}$.

Using Rabinowitsch's trick one can deduce the following stronger statement.

Theorem 1.11 (Hilbert's Nullstellensatz: strong form)**.** *Let k be an algebraically closed field. For any ideal $I \subset k[x_1, \ldots, x_n]$, the ideal of functions vanishing on the common zero locus of I is the radical of I:*

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

There is a bijection between affine subvarieties of $\mathbb{A}^n$ and radical ideals in $k[x_1, \ldots, x_n]$.

Proof of the strong form of the Nullstellensatz using the weak form. The inclusion $\sqrt{I} \subset I(V(I))$ is clear. We have to show the reverse inclusion. If I is an ideal in $k[x_1, \ldots, x_n]$ such that $V(I) = \emptyset$, then I must be the unit ideal. Otherwise, I would be contained in a maximal ideal. By the weak form of the Nullstellensatz, every maximal ideal vanishes at a point. We conclude that the common zeros of I cannot be empty unless I is the unit ideal.

Suppose $f \in I(V(I))$, we would like to show that $f^m \in I$ for some $m > 0$.

Rabinowitsch's trick: In $k[x_1, \ldots, x_n, t]$ (notice we added an extra variable!) consider the ideal J generated by I and $tf - 1$. Note that the zero locus of J is empty since f vanishes on the zero locus of I, so $tf - 1$ does not. Hence, J must be the unit ideal. We can express 1 as

$$1 = \sum a_i(x_1, \ldots, x_n, t) g_i(x_1, \ldots, x_n) + b(x_1, \ldots, x_n, t)(tf - 1),$$

where g_i are the generators of I. Now set $t = 1/f$ and clear the denominators. The last term drops out and we express a power of f in terms of elements in the ideal I. We conclude that

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

□

Proof of the weak form of the Nullstellensatz. The proof requires some commutative algebra. Let m be a maximal ideal in $k[x_1, \ldots, x_n]$. Then $L = k[x_1, \ldots, x_n]/m$ is a field and it contains k. If we knew that L is an algebraic extension of k, we would be done. We are assuming that k is algebraically closed. Hence, the only algebraic extension of k is itself. We conclude that $L = k$, which is equivalent to the Nullstellensatz. Showing that L is algebraic over k requires some commutative algebra. The key fact is the following lemma.

Lemma 1.12. *Let R be a Noetherian ring. Let S be a subring of $R[x_1, \ldots, x_n]$ containing R. If $R[x_1, \ldots, x_n]$ is finitely generated as an S-module, then S is finitely generated as an R algebra.*

Proof. Let $y_1, \ldots, y_m$ be the generators of $R[x_1, \ldots, x_n]$ as an S-module. Hence, we can write

$$x_i = \sum a_{i,j} y_j.$$

Similarly,

$$y_i \cdot y_j = \sum_k b_{i,j,k} y_k.$$

Let T be the subring of S generated over R by the coefficients $a_{i,j}$ and $b_{i,j,k}$. Since R is Noetherian, T is also Noetherian. The elements y_i generate $R[x_1, \ldots, x_n]$ as a T module. A submodule of a finitely generated module over a Noetherian ring is finitely generated. Thus S is a finitely generated T module, hence a finitely generated R-algebra.

□

To conclude the proof, suppose $x_1, \ldots, x_r \in L$ are algebraically independent over k and $x_{r+1}, \ldots, x_n$ are algebraic over $k(x_1, \ldots, x_r)$. We would like to show that $r = 0$. By the lemma, $k(x_1, \ldots, x_r)$ is a finitely generated k-algebra. This is a contradiction unless $r = 0$. Suppose $k(x_1, \ldots, x_r)$ is generated by $z_1, \ldots, z_m$ as a K algebra, where

$$z_i = \frac{P_i(x_1, \ldots, x_r)}{Q_i(x_1, \ldots, x_r)}$$

for some polynomials P_i, Q_i. If f is any irreducible polynomial in $k[x_1, \ldots, k_r]$, then we can express $1/f$ as a polynomial in z_i. Clearing the denominators we deduce that f must divide one of the Q_i. But then there would be only finitely many irreducible polynomials in $k[x_1, \ldots, x_r]$ which is clearly false. This concludes the proof. □

Next we would like to understand some basic properties of the Zariski topology. Given an algebraic set X, the Zariski topology on X is the subspace topology induced from $\mathbb{A}^n$. Let $f \in k[x_1, \ldots, x_n]$ be a polynomial. Then the distinguished open set U_f associated to f is the complement of the zero locus of f in X. Note that the distinguished open sets give a basis of the topology.

A distinguished open set U_f can itself be realized as a closed algebraic set. If $X \subset \mathbb{A}^n$ is the zero locus of polynomials f_α, then U_f is naturally a closed algebraic set in $\mathbb{A}^{n+1}$ defined by the polynomials f_α and $1 - z_{n+1} f$. (What is the relation with Rabinowitsch's trick?)

The Zariski topology is a Noetherian topology. This property becomes important in proofs because it allows one to use Noetherian induction. We recall the definition.

Definition 1.13. *A topological space is called Noetherian if every descending chain of closed sets*

$$X_1 \supset X_2 \supset X_3 \supset \cdots$$

stabilizes.

Show that the Zariski topology is Noetherian. It follows that the Zariski topology is quasi-compact, i.e., every covering has a finite subcover. Note that because the Zariski topology is not Hausdorff, quasi-compactness does not have the full impact of compactness for spaces like metric spaces. Suppose $\cup U_i$ is an open cover of X. Then consider $X_i = X - (U_1 \cup \cdots \cup U_i)$. X_i is closed and

$$X_1 \supset X_2 \supset X_3 \supset \cdots$$

Hence by the Noetherian property, this sequence of closed sets must stabilize. We conclude that at that point the U_i's must cover X.

Definition 1.14. *A topological space X is called reducible if X can be written as the union $X = X_1 \cup X_2$ of two proper closed sets. A topological space is called irreducible if it is not reducible. An irreducible algebraic subset of $\mathbb{A}^n$ is called an affine variety.*

Example 1.15. The algebraic set $V(x_1x_2)$ in $\mathbb{A}^2$ is reducible. It can be expressed as the union of $V(x_1)$ and $V(x_2)$. On the other hand, $V(x_1)$ is irreducible (why?).

Proposition 1.16. *An algebraic set $X \subset \mathbb{A}^n$ is an affine variety if and only if its ideal $I(X) \subset k[x_1, \ldots, x_n]$ is prime.*

Proof. Suppose $fg \in I(X)$. Then we can write $X = (X \cap V(f)) \cup (X \cap V(g))$. If X is irreducible, then either $X \cap V(f) = X$ or $X \cap V(g) = X$. We conclude that either f or g is in $I(X)$. Hence, $I(X)$ is prime. Conversely, suppose that $I(X)$ is prime. Then if $X = X_1 \cup X_2$, we have $I(X) = I(X_1) \cap I(X_2)$. Since $I(X)$ is prime, we must have (possibly after renumbering) $I(X) = I(X_1)$. Then $X = X_1$. □

Note that $\mathbb{A}^n$ is an affine variety. Similarly, a hypersurface defined by an irreducible polynomial is an affine variety.

Proposition 1.17. *Any closed algebraic set X is a finite union of irreducible closed sets. Moreover, the decomposition of X into irreducible closed sets $X = \cup_i X_i$ is unique provided that the decomposition is not redundant (i.e., there does not exist two indices i, j such that $X_i \subset X_j$).*

Proof. Suppose a closed algebraic set X cannot be written as a finite union of irreducible closed sets. Then X is reducible, so $X = X_1 \cup Y_1$ and either X_1 or Y_1 cannot be written as a finite union of irreducible closed sets. Up to relabeling assume X_1 cannot be written this way. Then $X_1 = X_2 \subset Y_2$ and we can repeat the argument. We obtain a sequence of strictly decreasing closed sets.

$$X \supset X_1 \supset X_2 \supset \cdots$$

By taking the ideals of functions vanishing on these closed algebraic sets, we obtain an infinite sequence of ideals

$$I(X) \subset I(X_1) \subset I(X_2) \subset \cdots$$

Since $k[x_1, \ldots, x_n]$ is Noetherian, we obtain a contradiction. We conclude that X can be written as a union of finitely many closed irreducible sets.

Suppose $X = \cup X_i$ and $X = \cup Y_j$ are two non-redundant expressions for X as a union of finitely many irreducible closed algebraic sets. Then consider

$$X_i = X_i \cap X = \cup (X_i \cap Y_j).$$

Since X_i is irreducible, we conclude that $X_i = Y_j$ for some j. By symmetry, we see that the non-redundant decomposition is unique. □

Definition 1.18. *The coordinate ring $A(X)$ of a closed algebraic set is the ring $k[x_1, \ldots, k_n]/I(X)$.*

Note that X is an affine variety if and only if its coordinate ring $A(X)$ is a domain.

Definition 1.19. *Let $U \subset X$ be an open set. Let $p \in U$ be a point. A function f on U is regular at p if there exists an open neighborhood V of p such that f is expressible as a quotient g/h of polynomials $g, h \in k[x_1, \ldots, x_n]$ such that $h(p) \neq 0$. The function f is called regular on U if it is regular at every point of U.*

Proposition 1.20. *Let X be a closed algebraic set. A function ϕ is regular on X if and only if $\phi \in A(X)$. More generally, the regular functions on a distinguished open set U_f is the localization $A(X)[1/f]$.*

Proof. Because the Zariski topology is quasi-compact, we can find finitely many distinguished open sets U_{f_α} such that on each open set U_{f_α}, we can express the regular function $\phi = g_\alpha/h_\alpha$ such that h_α does not vanish on U_α. The common zero loci of h_α must be contained in the zero locus of f. By Hilbert's nullstellensatz, we conclude that

$$f^m = \sum p_\alpha h_\alpha.$$

But then

$$f^m \phi = \sum p_\alpha h_\alpha \frac{g_\alpha}{h_\alpha} = \sum p_\alpha g_\alpha,$$

concluding the proof.

□

Definition 1.21. *Let $X \subset \mathbb{A}^n$ and let $Y \subset \mathbb{A}^m$ be two affine varieties. A map $f : X \to Y$ between two affine varieties is regular if f is given as $f(x) = (f_1(x), \ldots, f_m(x)$, where f_i are regular functions on X.*

Example 1.22. A regular function is a regular map to $\mathbb{A}^1$.

Example 1.23. The map $t \mapsto (t, t^2, t^3)$ gives a regular map from $\mathbb{A}^1$ to $\mathbb{A}^3$.

Example 1.24. The projection $\mathbb{A}^{n+1} \to \mathbb{A}^n$ given by $(x_1, \ldots, x_{n+1}) \mapsto (x_1, \ldots, x_n)$ is a regular map.

Example 1.25. Assume that the characteristic of k is $p > 0$. Let X be an affine variety. Then the Frobenius morphism $F : X \to X$ given by $(a_1, \ldots, a_n) \mapsto (a_1^p, \ldots, a_n^p)$ is a regular map.

A regular function $f : X \to Y$ defines a pull-back map between the coordinate rings of these varieties. Conversely, every algebra homomorphism between $\phi : A(Y) \to A(X)$ is induced by a regular map. (Why?)

Definition 1.26. *A regular map is an isomorphism if it has a regular inverse. Two affine varieties admitting an isomorphism are called isomorphic.*

In particular, note that two affine varieties are isomorphic if and only if their coordinate rings are isomorphic.

Example 1.27. The regular map $t \mapsto (t^2, t^3)$ gives a one-to-one correspondence between the points of $\mathbb{A}^1$ and the plane curve $y^2 = x^3$. Note; however, this map is not an isomorphism. The inverse map y/x is not regular at the origin.

Example 1.28. The hyperbola $xy - 1$ is isomorphic to $\mathbb{A}^1 - \{0\}$ under the projection morphism.

Definition 1.29. *Let X be an affine variety. Since the coordinate ring $A(X)$ is a domain, we can form its function field. The fraction field $k(X)$ of $(A(X)$ is called the rational function field of X. The elements of $k(X)$ are called rational functions on X.*