1 Introduction

Instructor information: Martin Olsson,

Two motivating questions. Let k be a field. We want to understand the solutions of equations $f_1(x) = 0 = \ldots = f_r(x)$ where the f_i are polynomials in $k[x_1, \ldots, x_n]$. For example, $k = \mathbb{Q}$, and $f(X_1, X_2, X_3) = X_1^n + X_2^n - X_3^n$. This is Fermat's last theorem. If $n \geq 3$ then only trivial solutions exist to this equation. Over $k = \mathbb{C}$, solutions of $f_1(x) = \ldots = f_r(x) = 0$ is a subset of $\mathbb{C}^n$, which will be a complex manifold. Similarly, suppose we are given a manifold, is it an algebraic variety? Given a manifold M, can $\pi_1(M)$ occur as the fundamental group of a manifold defined by polynomials? (This is "Hodge theory"). For example, $SL_2(\mathbb{Z})$ cannot be the fundamental group of any algebraic variety.

We're going to focus on the topological side a bit, because for the algebraic/arithmetic side needs schemes, which won't come up in 18.725 but only in 18.726.

1.1 Notation

Throughout the class, k will generally denote an algebraically closed field. A ring will generally be a commutative ring with identity, and ring homomorphisms will take the unit to the unit.

2 First Goal

2.1 Introduction

We want to understand $S = \{\underline{a} \in k^n | f_1(\underline{a}) = \ldots = f_r(\underline{a}) = 0\}$. There is a bijection between this and $T = \{$ maximal ideals in $k[x_1, \ldots, x_r]/(f_1, \ldots, f_r)\}$.

We want to consider how to map between varieties, and the natural way to think about this is as ring homomorphisms in the correspondence between the maximal ideal sets.

Let us call ρ the map from S to T.

$$\rho : \underline{a} = (a_1, \ldots, a_r) \mapsto (x_1 - a_1, \ldots, x_r - a_r).$$

Another way of thinking about it is that ρ maps to a map:

$$\rho : \underline{a} \mapsto \left\{ \frac{k[x_1, \ldots, x_r]}{(f_1, \ldots, f_r)} \xrightarrow{x_1 \mapsto a_i} k. \right\}$$

Thm 1: ρ is a bijection.

It is injective. How do we prove it's surjective? We need that if $m \subset R = \text{Frac } k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$, then $R/m = k$. Equivalently, the transcendence degree $trdeg_k(R/m) = 0$.

We need two results from Commutative algebra. First, the Noether normalization lemma.

Lemma (Noether Normalization) Let k be a field, let A be a finitely-generated k-algebra and integral domain. Then there exist $y_1, \ldots, y_r \in A$ which are algebraically independent over k, such that A is integral over $k[y_1, \ldots, y_r]$.

Reminder: algebraically independent means that $F(y_1, \ldots, y_r) = 0$ implies that $F = 0$.

Reminder: $B \hookrightarrow A$ integral $\iff$ every $a \in A$ satisfies $a^n + \alpha_{n-1}a^{n-1} + \ldots + \alpha_0 = 0$ for some $\alpha_i \in B$.

Pf. (of lemma): A is finitely generated $\iff$ $A = k[x_1, \ldots, x_m]/P$ where P is a prime ideal. By induction on r, the transcendence degree of A over k (the maximal number of algebraically independent elements we can find).

If $m = r$, $P = 0$ and the lemma is true trivially. If $m > r$, we induct on m. It suffices to find $k[y_1, \ldots, y_r] \subset_i S \subset_i A$ where both extensions are integral ($\subset_i$). A theorem from 18.705 shows that A will then be integral over $k[y_1, \ldots, y_r]$. We know there exists some $f \in k[y_1, \ldots, y_m]$ with $f(y_1, \ldots, y_m) = 0$. We will change variables to get our intermediate ring extension, s.t. $f = y_1^N +$ lower order terms. Then, S will be the subring generated by $y_2, \ldots, y_m$, and by this equation we will see that y_1 is integral over this, and so we are done.

Define $z_2 = y_2 - y_1^{s_2}, \ldots, z_m = y_m - y_1^{s_m}$. So $f(y_1, \ldots, y_m) = f(y_1, z_2 + y_1^{s_2}, \ldots, z_m + y_1^{s_m})$. Now, a monomial $a\Pi_{i=1}^m y_i^{b_i}$ will have a large y_1 term, and we can choose the s_i large enough that this works.

Here's an example. Suppose we just have $y_1^{b_1}(z_2 + y_1^{s_2})^{b_2}$. This gives us $y_1^{b_1}(y_1^{s_2 b_2} + y^{s_2(b_2-1}z_2 + \ldots)$ which will work out to $y_1^{b_1+s_2 b_2} +$ lower order terms, as desired.

If $s_i >> 0$, then $f(Y_1, Z_2 + Y_1^{s_2}, \ldots) = Y_1^N +$lower terms. This concludes the proof of the lemma. Exercise 1.1 shows that we can do this with *linear* substitutions.

The other result we need from commutative algebra is the Going-up theorem.

Thm. (Going-up). Let R be an integral domain, $S \subset R$ a subring, such that R is integral over S. Then, for every prime ideal $P \subset S$, there is a prime ideal $P' \subset R$ such that $P' \cap S = P$.

Pf. (of Going-up theorem). Let $M = S - P$, replace $S \subset R$ by $S_M \subset R_M$ (ie, localize at M.) It is enough to prove the theorem for S_M and R_M. Let $P^* \subset R_M$ s.t $P^* \cap S_M = P_M$. Then $j^{-1}(P^*) \subset R$ is prime. $j^{-1}(P^* \cap S) = (P^* \cap S_M) \cap S = P_M \cap S = P$. Thus, we can assume that S is a local ring, and P is the maximal ideal. (Local means that it has only one maximal ideal.)

So let S be local, and let P be the maximal idea. Claim: for all maximal ideals $P' \subset R$, $P' \subset S = P$. Look at $S/P' \cap S \hookrightarrow R/P'$ which is an integral map into a field.

Lemma: Let L be a field, $B \subset L$ a subring, such that $B \hookrightarrow L$ is integral. Then B is a field.

Pf. (of lemma): We know B is an integral domain. Let $b \in B$. We know $b' = 1/b \in L$, we need $1/b \in B$. We know there is some polynomial $b'^n + \alpha_{n-1}b'^{n-1} + \ldots \alpha_0 = 0$. Multiply this on both sides by b^{n-1}. We get

$$b' + \alpha_{n-1} + \alpha_{n-2}b + \ldots + \alpha_0 b^{n-1} = 0,$$

and each of the other terms are in b, so b' is in b. Now returning to the proof of the going-up theorem: We now know that for any maximal ideal $P'inR$, if we restrict to S, we get P. Since R has a maximal ideal, we are done.

Pf. of theorem 1 continues. We can write $\pi : k[x_1, \ldots, x_n] \twoheadrightarrow R$. Then $R/m = k[\underline{x}]/pi^{-1}(m)$. It is enough to consider $k[x_1, \ldots, x_n]$. Look at $k' = R/m$, which is a field, and k is a subfield of k'. Noether normalization tells us we can find $k[y_1, \ldots, y_r] \hookrightarrow k'$ which is integral. This looks bad, because this must be a field, but that is good because it implies that $r = 0$ so $trdeg_k(k') = 0$, and then since k is algebraically closed and k' is integral over k, we must have $k = k'$. This concludes the proof.

Cor. Nullstellensatz. If k is algebraically closed, then maximal ideals of $k[x_1, \ldots, x_n]$ are $(x_1 - a_1, \ldots, x_n - a_n)$ for $a - i \in k$. (Note: this is our bijection ρ with $r = 0$.)

We will sometimes write $\mathbb{A}^\kappa$ for k^n (A for "affine space").

2.2 Category Theory

We have some "objects" and "morphisms" which map between the objects. The objects we want in this course are zero sets of polynomial equations. What are the morphisms that go with these?

There is a correspondence between {subsets of k^n} and {finintely generated integral domains} defined by $0 \subset I \subset k[x_1, \ldots, x_n] \twoheadrightarrow R \to 0$ we can also make this a commutative diagram

$$\begin{array}{rcl} k[x_1, ..x_n] & \twoheadrightarrow & R \\ \uparrow & & \uparrow \\ k[y_1, ..y_m] & \twoheadrightarrow & R' \end{array}$$

so y_i corresponds to a polynomial $g(\underline{x})$. To pull this back one step, we can map y_i to $g_i(\underline{a})$ since this is the specific map from $k[x_1, \ldots, x_n]$ onto R.

So our morphisms are restrictions of polynomial maps $k^n \to k^m$. This is all a bit clumsy: really, we need schemes, but we'll do without them.

Def. An algebraic subset Σ of k^n is a set of the form

$$\{(a_1, \ldots, a_n) | f_1(\underline{a}) = \ldots = f_m(\underline{a}) = 0\}$$

for some $f_i \in k[x_1, \ldots, x_n]$. Note, Σ depends only on the ideal $f_1, \ldots, f_m)$. in fact, $\Sigma = \{\underline{a} \in k^n | f(\underline{a}) = 0 \text{ for all } f \in I\}$. Thus, for any ideal we can create an algebraic subset, using this formula. Define $V(I)$ to be this algebraic subset.

An issue: two ideals may define the same algebraic subset. For example, $I_1 = (x)$, $I_2 = (x^2)$. In both cases, $V(I) = \{0\}$. However, the radical of I_2 is still I_1, and so this is only well-defined up to (at best) radical ideals. (Yay! I remember this!)

Recall: if I is an ideal, then $\sqrt{I} = \{f \in k[\underline{x}] | f^l \in I \text{ for some } l > 0\}$. We know $V(I) = V(\sqrt{I})$. It is clear that $V(I) \supset V(\sqrt{I})$ since $I \subset \sqrt{I}$. The other inclusion follows easily.

Next time we will prove that this *is* well-defined up to radical ideals.