Algebraic Geometry (Math 6130)

Utah/Fall 2016.

1. Introduction/Affine Varieties

Let k be a field, and consider the polynomial ring in n variables:

$$k[x_1, ..., x_n]$$

These are commutative algebras over k with unique factorization that are *Noetherian*; each submodule $N \subset M$ of a finitely generated module over $k[x_1, .., x_n]$ is itself finitely generated. This is a consequence of the **Hilbert Basis Theorem**. In particular, the *ideals* $I \subset k[x_1, ..., x_n]$ are each generated by finitely many polynomials.

Notation. When I is generated by polynomials $f_1, ..., f_m$, we write:

$$I = \langle f_1, ..., f_m \rangle$$

Another striking result of Hilbert characterizes the *maximal ideals* of $k[x_1, ..., x_n]$ when k is an algebraically closed field. Namely:

Hilbert's Nullstellensatz: If $k = \overline{k}$ is an algebraically closed field, then every maximal ideal ideal $m \subset k[x_1, ..., x_n]$ is one of the following:

$$m_{\underline{a}} = \langle x_1 - a_1, ..., x_n - a_n \rangle \text{ for } \underline{a} = (a_1, ..., a_n) \in k^n$$

Remarks. (i) These maximal ideals are exactly the kernels of the maps:

$$ev_{\underline{a}} : k[x_1, ..., x_n] \to k;\ ev_{\underline{a}}(f) = f(\underline{a})$$

evaluating a polynomial at $\underline{a} \in k^n$, and the point is that when k fails to be algebraically closed, there are more maximal ideals. For example:

(ii) The polynomial ring $k[x]$ is a principal ideal domain, and the maximal ideals are the principal ideals $\langle f \rangle$ for **prime** polynomials $f(x)$. When k is algebraically closed, the only prime polynomials are the linear polynomials, and so every maximal ideal is of the form $\langle x - a \rangle$.

Corollary 1.1. If k is algebraically closed and $I \subset k[x_1, ..., x_n]$ does not contain 1, then the set of common zeroes of the polynomials in I:

$$V(I) = \{\underline{a} \in k^n \mid f(\underline{a}) = 0 \text{ for all } f \in I\} \subset k^n$$

is nonempty, in bijection with the set of maximal ideals containing I. Conversely, if $f_1, ..., f_m \in k[x_1, ..., x_n]$ and $V(\langle f_1, ..., f_m \rangle) = \emptyset$, then there are polynomials $g_1, ..., g_m \in k[x_1, ..., x_n]$ such that:

$$1 = \sum_{i=1}^{m} g_i f_i$$

i.e. $1 \in I = \langle f_1, ..., f_m \rangle$.

Definition 1.1. A subset $X \subset k^n$ is **algebraic** if $X = V(I)$ for some ideal $I \subset k[x_1, ..., x_n]$.

When k is not algebraically closed, there is no hope of recovering the ideal I from the algebraic subset $X = V(I)$ since, for example, $\emptyset = V(I)$ for many maximal ideals. However, when $k = \overline{k}$, then:

Corollary 1.2. For any subset $S \subset k^n$:

$$I(S) = \{f \in k[x_1, ..., x_n] \mid f(\underline{a}) = 0 \text{ for al } s \in S\}$$

of functions vanishing on S. Then for all ideals $I \subset k[x_1, ..., x_n]$,

$$I(V(I)) = \sqrt{I} := \{h \in k[x_1, ..., x_n] | \ h^N \in I \text{ for some } N > 0\}$$

Proof. (Trick of Rabinowitz) Let $I = \langle f_1, .., f_m \rangle$ and $h \in I(V(I))$. Consider the new ideal in the polynomial ring with one more variable:

$$J = \langle f_1, ..., f_m, hx_{n+1} - 1 \rangle \subset k[x_1, ..., x_{n+1}]$$

Then by construction, $V(J) \subset k^{n+1}$ is empty, so:

$$1 = \sum_{i=1}^{m} g_i(f_i + g \cdot (hx_{n+1} - 1)$$

for some polynomials $g_1, ..., g_m, g \in k[x_1, ..., x_{n+1}]$ by Corollary 1.1. Now formally substitute $1/h$ for x_{n+1} in the equation. This gives:

$$1 = \sum_{i=1}^{m} g_i(x_1, ..., x_n, \frac{1}{h})f_i$$

and we may multiply through by h^N for some N to clear denominators:

$$h^N = \sum h_i f_i \text{ for } h_i \in k[x_1, ..., x_n]$$

to get $h^N \in I$, as desired. This proves that $I(V(I)) \subseteq \sqrt{I}$, but the other direction is obvious. $\square$

Definition 1.2. An ideal $I \subset k[x_1, ..., x_n]$ is **geometric** if $I = I(S)$ for some subset $S \subset k[x_1, ..., x_n]$.

Remark. A geometric ideal is clearly *radical*, i.e. it satisfies $I = \sqrt{I}$. By Corollary 1.2, every radical ideal is geometric, with $S = V(I)$.

The Nullstellensatz therefore gives a bijection (when $k = \overline{k}$):

$$\{\text{algebraic subsets } X \subset k^n\} \leftrightarrow \{\text{geometric ideals } I \subset k[x_1, ..., x_n]\}$$

$$X \to I(X)$$

$$V(I) \leftarrow I$$

that generalizes the bijection between points and maximal ideals.

Remark. You should convince yourself of the two identities:

$$X = V(I(X)) \text{ and } I = I(V(I))$$

for algebraic sets and geometric ideals, respectively.

You should also convince yourself that:

$$X \subset Y \Leftrightarrow I(Y) \subset I(X) \quad \text{and} \quad I \subset J \Leftrightarrow V(J) \subset V(I)$$

i.e. the correspondence between algebraic sets and geometric ideals is *inclusion reversing.*

Notice that prime ideals $P \subset k[x_1, ..., x_n]$ are geometric ideals.

Definition 1.3. An algebraic subset $X \subset k^n$ is a **variety** if the associated geometric ideal $I(X)$ is prime.

Thus we have a correspondence between (always assuming $k = \overline{k}$):

$$\{\text{maximal ideals } m\} \subset \{\text{prime ideals } P\} \subset \{\text{geometric ideals } I\}$$

$$\text{and } \{\text{points } p\} \subset \{\text{varieties } V\} \subset \{\text{algebraic sets } X\}$$

On the other hand, by the first isomorphism theorem for rings we also have a correspondence between ideals and quotient rings, which may be interpreted as rings of polynomial functions on sets $X = V(I)$. Thus:

$$X \leftrightarrow I(X) \leftrightarrow k[X] := k[x_1, ..., x_n]/I(X)$$

and this **coordinate ring** $k[X]$ of X is:

(i) A reduced k-algebra (no nilpotents) when X is an algebraic set.

(ii) A k-algebra domain when X is a variety.

(iii) k itself (the constant functions) when X is a point.

Conversely, any reduced (respectively integral domain, field) quotient ring $k[x_1, ..., x_n] \to R$ of the polynomial ring is the coordinate ring of an algebraic set (respectively variety, point) in k^n.

Notice that when X is a variety, then:

$$k(X) := \text{the field of fractions of the domain } k[X]$$

may be defined. This is the **field of rational functions** of X.

Definition 1.4. The **dimension** of X is the transcendence degree:

$$td\,(k(X)/k)$$

of the field extension $k(X)$ over k (when X is a variety).

Remark. We will later see that every algebraic set is a finite union of varieties, which may have differing dimensions, giving such algebraic sets an undefined dimension.

Example 1.1.(Cubic Curves) Consider the following curves in k^2:

(a) $f(x,y) = y^2 - x^3$; $X = V(f) \subset k^2$ is the cuspidal cubic.

(b) $g(x,y) = y^2 - x^2(x+1)$; $Y = V(g)$ is the nodal cubic.

(c) $h_\lambda(x,y) = y^2 - x(x+1)(x-\lambda), \lambda \neq 0, -1$; $C_\lambda = V(h_\lambda)$.

Then:

(a) $k[X] = k[x,y]/\langle y^2 - x^3\rangle \cong k[t^2, t^3]$ and

(b) $k[V(g)] = k[x,y]/\langle y^2 - x^2(x-1)\rangle \cong k[t(t^2-1), t^2-1]$

so the fields of rational functions in (a) and (b) are isomorphic to $k(t)$, which is also the field of rational functions of the *affine line* k.

On the other hand, we will see that:

(i) The fields $k(C_\lambda)$ are never isomorphic to $k(t)$, and:

(ii) There is a finite group acting on the λ line with $k(C_{\lambda_1}) \cong k(C_{\lambda_2})$ if and only if λ_1, λ_2 belong to the same orbit. In particular, there are infinitely many non-isomorphic fields $k(C_\lambda)$ (since $k = \overline{k}$ is infinite).

A key property of Example (c) is:

(*) The cubic curves C_λ are "nonsingular:"

$$V(h_\lambda) \cap V(\nabla h_\lambda) = V(h_\lambda) \cap V\left(\frac{\partial h_\lambda}{\partial x}\right) \cap V\left(\frac{\partial h_\lambda}{\partial y}\right) = \emptyset$$

By the implicit function theorem, if $k = \mathbb{C}$, this implies that C_λ are complex manifolds, whereas both X and Y fail to be manifolds at the origin, where the gradient and the equation of the curve both vanish.

Remark. The cubic polynomial $p(x,y) = y - x^3$ is both nonsingular and produces a cubic curve Z with $k(Z) \cong k(x)$. There is, however, a "hidden" cuspidal singularity of this curve that is only revealed when it is completed to a curve in the projective plane. The curves C_λ, on the other hand, will remain nonsingular when they are completed to projective plane curves.

Theorem/Definition 1.5. Suppose $X = V(\langle f_1, ..., f_m\rangle) \subset k^n$ is a variety, and $\dim(X) = d$. Then the rank of the $n \times m$ Jacobian matrix:

$$J(\underline{a}) = \left(\frac{\partial f_i}{\partial x_j}(\underline{a})\right) \text{ for each } \underline{a} \in X$$

is always at most $n - d =$ the *codimension of* X *in* k^n, and it is strictly less than $n - d$ on a (possibly empty) proper algebraic subset $Z \subset X$.

The points $\underline{a} \in X$ where the rank of the Jacobian matrix is exactly equal to the codimension of X in k^n are the **nonsingular** points of X.

The next two Hilbert theorems relate to *graded* polynomial rings. When we discuss graded polynomial rings, we will use variables $x_0, ..., x_n$ (for reasons that will become apparent later), and define:

$$S := k[x_0, ..., x_n] = \bigoplus_{d=0}^{\infty} k[x_0, ..., x_n]_d =: \bigoplus_{d=0}^{\infty} S_d$$

decomposing the polynomial ring $S = k[x_0, ..., x_n]$ as a direct sum of subspaces $S_d = k[x_0, ..., x_n]_d$ of *homogeneous* polynomials of degree d. This grading of S respects polynomial multiplication, in the sense that multiplication induces bilinear maps for each pair of degrees:

$$\mu : S_{d_1} \times S_{d_2} \mapsto S_{d_1+d_2}$$

Definition 1.6. A module M over $S = k[x_0, ..., x_n]$ is *graded* if:

$$M = \bigoplus_{d\in\mathbb{Z}} M_d \text{ and } \mu : S_d \times M_e \to M_{d+e} \text{ for all } d \geq 0 \text{ and } e \in \mathbb{Z}$$

An S-homomorphism $\phi : M \to N$ of graded modules is **graded** if:

$$\phi(M_d) \subset N_d \text{ for all } d \in \mathbb{Z}$$

Remark. Any element $m \in M$ is thus a finite sum of **homogeneous** elements $m_d \in M_d$. In particular, if M is finitely generated and graded as an S-module, then it is finitely generated *by homogeneous elements*. Also, the kernel, image (by definition) and cokernel of a graded S-homomorphism are graded S-modules.

Definition 1.7. For any $e \in \mathbb{Z}$, the graded S-module:

$$S(e) = \bigoplus_{d=-e}^{\infty} k[x_0, ..., x_n]_{d+e}$$

is freely generated by $1 \in S(e)_{-e}$. A graded S-module is **free** if it is isomorphic (as a graded module) to a direct sum of such modules.

Now suppose M is a finitely generated graded S-module. If:

$$m_{d_1}, ..., m_{d_r} \in M \text{ are homogeneous generators}$$

of degrees $d_1, ..., d_r \in \mathbb{Z}$ (with possible repetitions of degrees), then we obtain a surjective graded homomorphism of S-modules:

$$\phi : \bigoplus_{i=1}^{r} S(-d_i) \to M; \quad \phi(1, 0, ..., 0) = m_{d_1}, \phi(0, 1, 0, .., 0) = m_{d_2} \text{ etc.}$$

We may repeat this with the kernel of ϕ, which is graded and finitely generated, to get a surjective graded homomorphism:

$$\phi_1 : \bigoplus_{i=1}^{r_1} S(-d_{i,1}) \to K_0 := \ker(\phi)$$

and we may do this n times, at which point we have the:

Hilbert Syzygy Theorem (Graded Version). Let M be a finitely generated graded S-module where $S = k[x_0, ..., x_n]$. Then the kernel module K_n of any partial free resolution:

$$0 \to K_n \to \bigoplus_{i=1}^{r_n} S(-d_{i,n}) \stackrel{\phi_n}{\to} \cdots \to \bigoplus_{i=1}^{r_1} S(-d_{i,1}) \stackrel{\phi_1}{\to} \bigoplus_{i=1}^{r_0} S(-d_{i,0}) \stackrel{\phi_0}{\to} M \to 0$$

is a free module, isomorphic to:

$$\bigoplus_{i=1}^{r_{n+1}} S(-d_{i,n+1})$$

for unique values of $d_{i,n+1}$.

Example 1.2. The Koszul resolution of the graded quotient ring:

$$0 \to \langle x_0, ..., x_n \rangle \to S \to k \to 0$$

of S by the unique maximal graded ideal has the following shape:

$$0 \to S(-n-1) \to \cdots \to \bigoplus_{i=1}^{\binom{n+1}{m}} S(-m) \to \cdots \bigoplus_{i=1}^{n+1} S(-1) \to S \to k \to 0$$

and it is not possible to "shorten" this free module resolution of k.

Remark. There is a canonical minimal free resolution of M, obtained by choosing generators as efficiently as possible. For example, if $M_e = 0$ for $e < d$ and $\dim(M_d) = n$, then n (linearly independent) generators should be chosen in degree d. The integers $d_{i,j}$ in the minimal free resolution of M are thus numerical invariants of M. The free modules in the minimal free resolution are the **syzygies** of the module M.

Notice also that each graded homomorphism:

$$S(-e) \to S(-f)$$

is multiplication by a homogeneous polynomial $F \in k[x_0, ..., x_n]_{e-f}$, hence any free resolution is accomplished with a series of matrices of homogeneous polynomials.

More numerical invariants come from our final Hilbert theorem, which is an immediate consequence of the Syzygy Theorem.

Hilbert Polynomial Theorem. The dimensions $\dim(M_d)$ of the graded pieces of a finitely generated graded module over $S = k[x_0, ..., x_n]$ coincide with a polynomial $H_M(d)$ of degree $\leq n$ for all sufficiently large values of d. This is the **Hilbert polynomial** of the module M, measuring the (eventual) growth the graded parts of M.

Proof. This is true of the twisted modules $S(e)$, since:

$$\dim(S[x_0, ..., x_n]_{d+e}) = \binom{d+e+n}{n} \text{ for } d \geq -e-n$$

is a polynomial of degree n in d with leading term:

$$\frac{d^n}{n!}$$

(if $d < -e - n$, however, the two sides do not agree!)

But now by the Syzygy Theorem, there is a finite resolution of M by free modules F_i, each of which has polynomial growth (of degree n), and since the dimension of M_d is the alternating sum of the dimensions of $(F_i)_d$, it follows that the growth of the dimension of M_d is polynomial, of degree **at most** n. $\square$

Remark. The S-module $k = S/\langle x_0, .., x_n\rangle$ has the zero polynomial as its Hilbert polynomial, so evidently the degree can be less than n. In fact, we will associate a *projective variety* to a graded quotient domain $S \to R$, and the dimension of this variety will be defined to be the degree of the Hilbert polynomial of the graded S-module R. Reconciling this with Definition 1.3 for *affine* varieties will be done with Krull's Hauptidealsatz.

We have now seen (with Hilbert's first two theorems) that algebraic subsets $X \subset k^n$ are in bijection with geometric ideals in $k[x_1, ..., x_n]$, and that the latter can be used to define "local" geometric properties of X, such as dimension and nonsingularity (at a point) purely in terms of commutative algebra. With the second pair of Hilbert theorems, we see that numerical invariants can be associated to finitely generated modules over a graded polynomial ring S. These should be thought of as being analogous to the dimensions of (singular) cohomology spaces on a compact manifold, and in fact the cohomology of coherent sheaves, which is the subject of this course, will be harnessed to do just that. But first we have to see how "graded" rings and modules are seen as completions of ordinary rings and modules with one fewer variable.

Exercises. Here, k is an algebraically closed field.

1.1. (a) Show that the union of two varieties $X, Y \subset k^n$ is an algebraic set, but that $X \cup Y$ is only a variety if $X = X \cup Y$ or $Y = X \cup Y$. Give examples showing that a union of infinitely many varieties need not be an algebraic set.

(b) Show that the intersection of any collection of varieties in k^n is an algebraic set, and give an example of a pair of varieties $X, Y \subset k^n$ whose intersection is not a variety.

(c) Find the appropriate commutative algebra result to allow you to conclude that every algebraic set is the union of finitely many varieties, and that the component varieties $X_1, ..., X_m$ of X are uniquely determined provided that $X_i \not\subset X_j$ for any $i \neq j$.

1.2. Let $S = \{p, q, r\} \subset k^2$ be three non-collinear points.

(a) Show that $S = V(\langle f, g \rangle)$ for some $f, g \in k[x_1, x_2]$.

(b) Show that $I(S) \subset k[x_1, x_2]$ is not generated by two polynomials.

(c) How do matters change if the points are collinear?

(d) Are there finite sets $S \subset k^2$ such that $I(S)$ require arbitrarily many generators? Are there finite sets $S \subset k^2$ that require arbitrarily many polynomials to generate **any** ideal I with $S = V(I)$?

1.3. (a) Show that a conic $C = V(q) \subset k^2$ for a "true" quadratic polynomial $q(x, y) \in k[x, y]$ is singular if and only if q factors as a product of linearly independent linear factors. Give an example to show that this is not true in more variables.

(b) Show that the plane curve $V(y^d - f(x)) \subset k^2$ is nonsingular for $d \geq 2$ if and only if $f(x) \in k[x]$ has distinct roots.

1.4. Resolve the following homogenous ideals (as graded modules):

(a) The kernel of the map:

$$S = k[x_0, x_1, x_2] \to k[s^2, st, t^2]; \; x_0 \mapsto s^2, \text{ etc}$$

(b) The kernel of the map:

$$S = k[x_0, x_1, x_2, x_3] \to k[s^3, s^2t, st^2, t^3]; \; x_0 \mapsto s^3, \text{ etc}$$

(c) The kernel of the map:

$$S = k[x_0, x_1, x_2] \to k[s^3, s^2t - st^2, t^3]$$

(d) The kernel of the map:

$$S = k[x_0, x_1, x_2, x_3] \to k[s^4, s^3t, st^3, t^4]$$