Algebraic Geometry I (Math 6130)

Utah/Fall 2020

1. Algebraic Sets

A commutative ring A with 1 is **Noetherian** if for every chain of ideals:

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

there is an n such that $I_n = I_{n+1} = \cdots = \bigcup_{k=1}^{\infty} I_k$ (i.e. the chain *stabilizes*).

Lemma 1.1. A is Noetherian if and only if every ideal $I \subset A$ is finitely generated.

Proof. Exercise.

- All fields k are Noetherian.
- Any PID (e.g. $\mathbb{Z}$ or $k[x]$) is Noetherian.

Lemma 1.2. If A is Noetherian and M is a finitely-generated A-module, then every submodule $N \subset M$ is also finitely generated.

Proof. If M is finitely generated, there is a surjection $q : A^n \to M$, and if the submodule $q^{-1}(N) \subset A^n$ is a finitely generated A-module, then N is also finitely generated (by the images of generators of $q^{-1}(N)$). Thus it suffices to prove the lemma for free modules A^n. But this follows by induction on n via exact sequences:

$$0 \to A^{n-1} \to A^n \to A \to 0 \quad \square$$

Hilbert Basis Theorem. If A is Noetherian, then $A[x]$ is Noetherian.

Proof. Let $J \subset A[x]$ be an ideal, and consider the ideals $I_d \subset A$ of leading coefficients of polynomials $f(x) \in J$ of degree d. That is, $a \in I_d$ if and only if there is a polynomial $f(x) \in J$ of the form $ax^d +$lower order "representing" a. The ideals I_d form an ascending chain that stabilizes at some I_n since A is Noetherian. Each of the ideals $I_0, I_1, ..., I_n$ is finitely generated by Lemma 1.1, and then J itself is generated by any choice of $n+1$ collections of polynomials in J of degrees $0, ..., n$ that represent generators of each of the ideals $I_0, ..., I_n$. $\square$

Corollary 1.3. The polynomial rings $k[x_1, ..., x_n]$ are Noetherian.

Example. Let $X \subset k^n$ be an arbitrary subset. Then:

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

is an ideal, hence finitely generated by Corollary 1.3.

Let $X = \{(0,0), (1,0), (0,1)\} \subset k^2$ and view $k[x_1, x_2]$ as $k[x_1][x_2]$. Let $J = I(X)$. Then:

$$I_0 = \langle x_1^2 - x_1 \rangle, \ I_1 = \langle x_1 \rangle \text{ and } I_2 = \langle 1 \rangle$$

and the polynomials $x_1^2 - x_1, x_1x_2, x_2^2 - x_2 \in J$ generate J, as in the Basis Theorem.

Together with the definition of $X(I)$ from §0, we have mappings:

$$X : \ \{\text{ideals } I \subset k[x_1, ..., x_n])\} \to \ \{\text{subsets } X \subset k^n\} \text{ and}$$
$$I : \{\text{subsets } X \subset k^n\} \to \{\text{ideals } I \subset k[x_1, ..., x_n])\}$$

Definition 1.4. (a) X is *algebraic* if $X = X(I)$ for some $I \subset k[x_1, ..., x_n]$.

(b) I is *geometric* if $I = I(X)$ for some subset $X \subset k^n$.

Simple Observations. (i) If $I \subseteq J$, then $X(I) \supseteq X(J)$.

(ii) If $X \subseteq Y$, then $I(X) \supseteq I(Y)$.

(iii) $X \subseteq X(I(X))$ and $I \subseteq I(X(I))$.

Proposition 1.5. The algebraic sets $X(I) \subset k^n$ are the closed sets of a *topology.* This is the **Zariski Topology** on k^n..

Proof. We need to show that:

(i) $\emptyset$ and k^n are closed sets.

(ii) If X and Y are closed sets, then $X \cup Y$ is a closed set.

(iii) If $X_\lambda,\ \lambda \in \Lambda$ is any collection of closed sets, then $\cap_\lambda X_\lambda$ is a closed set.

These follow immediately from the corresponding properties of ideals.

(i) $\emptyset = X(\langle 1 \rangle)$ and $k^n = X(\langle 0 \rangle)$.

(ii) If $X = X(I)$ and $Y = X(J)$, then $X \cup Y = X(I \cdot J)$.

(iii) If $X_\lambda = X(I_\lambda)$ for $\lambda \in \Lambda$, then $\cap X_\lambda = X(\sum I_\lambda)$. □

Remark. It's often the **open** sets $U = X^c$ that are more natural to think about. When we study schemes, we'll see there are many closed subschemes of k^n with the same underlying set X, but only one open subscheme with the underlying set U.

Example. (a) Points $a \in k^n$ are always closed, via the maximal ideals:

$$\{a\} = X(\langle x_1 - a_1, ..., x_n - a_n \rangle)$$

so finite sets are also closed. These are the **only** closed subsets of k (other than k). In k^2, we also have the *plane curves* $X = X(f(x_1, x_2))$ which are never finite sets when k is algebraically closed.

(b) By the Noetherian property and observation (ii) above, any descending chain:

$$X_1 \supseteq X_2 \supseteq X_2 \supseteq \cdots$$

of closed sets of k^n eventually stabilizes. Complementarily, any ascending chain:

$$U_1 \subseteq U_2 \subseteq U_3 \subseteq \cdots$$

of open subsets of k^n eventually stabilizes.

Suppose now that $P \subset k[x_1, ..., x_n]$ is a **prime** ideal and let:

- $X = X(P) \subset k^n$
- $k[X] = k[x_1, ..., x_n]/P$ (the integral domain of regular functions on X)
- $k(X) =$ field of fractions of $k[X]$ (the field of rational functions on X)

Let d be the transcendence degree of the field extension $k \subset k(X)$. Then:

Noether Normalization. There are algebraically independent regular functions $y_1, ..., y_d \in k[X]$ such that $k[X]$ is finitely generated as a $k[y_1, ..., y_d]$-module.

Proof. We will prove this under the (unnecessary) assumption that k is infinite. With this assumption, we can in fact choose:

$$y_i = \sum_{j=1}^{n} a_{i,j} x_j \text{ for } i = 1, ..., d \text{ and } a_{i,j} \in k$$

to be *linear* combinations of the images of the coordinate functions x_i in $k[X]$.

If $n = d$, then $P = 0$ (otherwise $k(X)$ would have transcendence degree $< d$). Otherwise, $n < d$ and $x_1, ..., x_n \in k[X]$ satisfy a relation $f(x_1, ..., x_n) = 0$ for some polynomial $f \in P$ of degree $m > 0$. If

$$f = ax_n^m + \{\text{lower order in } x_n\}$$

for some non-zero constant $a \in k$, then $k[X]$ is generated by $1, x_n, ..., x_n^{m-1}$ as a module over the integral domain $k[x_1, ..., x_{n-1}]/P \cap k[x_1, ..., x_{n-1}]$.

In general f will not have this form, but we can change variables to put it in this form as follows. Let $y_i = x_i + a_i x_n$ for $i = 1, ..., n-1$. Then as a function of $y_1, y_2, ..., y_{n-1}, x_n$ we have

$$f = g(a_1, ..., a_{n-1})x_n^m + \{\text{lower order in } x_n\}$$

where g is a non-zero polynomial in the a_i. Because k is infinite, we can choose the constants $a_1, ..., a_{n-1}$ so that $g(a_1, ..., a_{n-1}) \neq 0$ and then in terms of the new coordinates $y_1, ..., y_{n-1}, x_n$, the relation f does have the desired form, and so $k[X]$ is finitely generated as a module over $k[Y] = k[y_1, ..., y_{n-1}]/P \cap k[y_1, ..., y_{n-1}]$ from which it follows that $k(Y)$ is a finite field extension of $k(Y)$, so they have the same transcendence degree over k, and then we can proceed by induction on n. $\square$

Example. Consider the prime ideal $P = \langle xy - 1 \rangle \subset k[x, y]$. Then:

- $X = X(P)$ is the *hyperbola* $\{(t, t^{-1}) \mid t \in k^*\}$.
- $k[x, x^{-1}]$ is **not** finitely generated as a $k[x]$-module, but
- $k[x, x^{-1}]$ is generated by 1 and x as a $k[x + x^{-1}]$-module.

Hilbert Nullstellensatz: If k is infinite and $m \subset k[x_1, ..., x_n]$ is a maximal ideal, then $k \subset K = k[x_1, ..., x_n]/m$ is a finite field extension.

Proof. If not, then $k \subset K$ is a field extension of transcendence degree $d > 0$, and then by by Noether Normalization, we have:

$$k \subset k[y_1, ..., y_d] \subset K$$

where K is a finitely generated $k[y_1, ..., y_d]$-module. But this is impossible when K is a field. For example, by Lemma 1.2 and 1.3, $k[y_1, y_1^{-1}, ..., y_d] \subset K$ would be a finitely generated $k[y_1, ..., y_d]$-module, which it isn't. $\square$

Corollary 1.6. If $k = \overline{k}$, then $m_a, a \in k^n$ are the maximal ideals in $k[x_1, ..., x_n]$.

Proof. Let $m \subset k[x_1, ..., x_n]$ be a maximal ideal. Then by the Nullstellensatz,

$$k \subset k[x_1, ..., x_n] \to k[x_1, ..., x_n]/m = K$$

is a finite field extension of k, hence **equal** to k. Thus, m is the kernel of the map:

$$x_i \mapsto a_i \in K = k;\ i = 1, ..., n$$

i.e. m is the maximal ideal $m_a = \langle x_1 - a_1, ..., x_n - a_n \rangle$. $\square$

Corollary 1.7. If $X(I) = \emptyset$ and $k = \overline{k}$, then $1 \in I$.

Proof. If $X(I) = \emptyset$, then by Corollary 1.6, I is contained in **no** maximal ideal, hence $1 \in I$, so if $I = \langle f_1, ..., f_m \rangle$, there are polynomials $g_1, ..., g_m$ so that:

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

(though finding the g_i can be challenging).

Definition 1.8. If $I \subset A$ is an ideal, then the **radical** of I is the ideal:

$$\mathrm{rad}(I) = \{f \in A \mid f^n \in I \text{ for some } n > 0\}$$

Note that if $I \subset k[x_1, ..., x_n]$, then $I \subseteq \mathrm{rad}(I) \subseteq I(X(I))$.

The following Corollary characterizes geometric ideals in $k[x_1, ..., x_n]$ when $k = \overline{k}$.

Corollary 1.9. If $k = \overline{k}$, then $I(X(I)) = \mathrm{rad}(I)$.

Proof. Let $I = \langle f_1, .., f_m \rangle$ and suppose $f \in I(X(I))$ and consider the ideal:

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

Then by construction, $X(J) = \emptyset$, so $1 \in J$ by Corollary 1.7 and

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

for some $g_1, ..., g_m, g \in k[x_1, ..., x_{n+1}]$. Now formally substitute f^{-1} for x_{n+1}. Then:

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

and multiplying through by f^N for large enough N gives:

$$f^N = \sum h_i f_i \in I \text{ for } h_i = f^N g_i(x_1, ..., x_n, f^{-1}) \in k[x_1, ..., x_n]$$

Thus $\mathrm{rad}(I) \subseteq I(X(I))$. □

Definition 1.10. An ideal I is *radical* if $\mathrm{rad}(I) = I$.

Example. If I is any ideal, then $\mathrm{rad}(\mathrm{rad}(I)) = \mathrm{rad}(I)$, so $\mathrm{rad}(I)$ is radical.

Corollary 1.11. If $k = \overline{k}$, *geometric* ideals are the same as *radical* ideals.

Proof. Clearly every ideal of the form $I(X)$ for any $X \subset k^n$ is a radical ideal. On the the other hand, if I is radical, then $I = I(X(I))$, so I is geometric. □

Notice also that if $I \neq J$ are radical ideals, then $X(I) \neq X(J)$. So:

$$X : \{\text{radical ideals } I \subset k[x_1, ..., x_n]\} \to \{\text{algebraic (closed) subsets } \; X \subset k^n\}$$

is a bijection, with inverse I (this follows from $X(I(X(I)) = X(\mathrm{rad}(I)) = X(I))$.

Note that a prime ideal P is also a radical ideal, so $I(X(P)) = P$ (when $k = \overline{k}$). The closed sets $X(P)$ corresponding to prime ideals are "irreducible."

Definition 1.12. A closed set $X \subset k^n$ in the Zariski topology is **reducible** if:

$$X = X_1 \cup X_2$$

for two nonempty closed subsets $X_1 \subset X$ and $X_2 \subset X$ (properly contained in X). If no such pair of closed subsets exists, then X is **irreducible**.

Announcement. Unless otherwise indicated, we will assume $k = \overline{k}$ from now on.

Proposition 1.13. (a) If $P \subset k[x_1, ..., x_n]$ is a prime ideal then $X(P)$ is irreducible.

(b) If $X \subset k^n$ is an irreducible closed set, then $I(X)$ is prime.

(c) Every closed set $X \subset k^n$ is a union of finitely many irreducible closed sets, and the minimal such union: $X = X_1 \cup \cdots \cup X_m$ (with $X_i \not\subset X - X_i$) is uniquely determined, up to permuting the **irreducible components** $X_1, ..., X_m$.

Proof. (a) Let I be a radical ideal. If $X(I)$ is reducible, let $X = X_1 \cup X_2$ as in Definition 1.12 and choose $x_1 \in X - X_2$ and $x_2 \in X - X_1$. Since $X_i = X(I(X_i))$, it follows that there are $f, g \in k[x_1, ..., x_n]$ such that $f(x_1) \neq 0$ but $f|_{X_2} \equiv 0$ and $g(x_2) \neq 0$ but $g|_{X_1} \equiv 0$. Then $fg \in I$, but $f, g \notin I$. So I is not prime.

(b) Conversely, if $I(X)$ is not prime, then there are $f, g \notin I(X)$ with $fg \in I(X)$. Then $X(\langle I(X), f\rangle) = X_2$ and $X(\langle I(X), g\rangle) = X_1$ satisfy Definition 1.12.

(c) Either X is irreducible and there is nothing to prove, or else:

$$X = X_1 \cup X_2$$

as in Definition 1.12. If X is **not** a union of finitely many irreducible closed subsets as in (c), then either X_1 or X_2 is also not a union of finitely many irreducible closed subsets and in particular, X_i is reducible for $i = 1$ or 2, and so $X_i = X_{i,1} \cup X_{i,2}$. Continuing, there is a decreasing chain of closed subsets $X \supset X_{i_1} \supset X_{i_1,i_2} \supset \cdots$ that does not stabilize, violating the Noetherian property.

The uniqueness of irreducible components is left as an exercise. □

Example. $k[x_1, ..., x_n]$ is a unique factorization domain (UFD). If:

$$f = f_1^{d_1} \cdots f_m^{d_m}$$

is a prime factorization of $f \in k[x_1, ..., x_n]$ with distinct irreducible polynomials $f_1, ..., f_m$, then $X(f) = X(f_1) \cup \cdots \cup X(f_m)$ and the irreducible **hypersurfaces** $X(f_i)$ are the irreduciuble components of $X(f)$.

Assignment 1. Assume $k = \overline{k}$ (as we announced earlier).

1. Prove Lemma 1.1.

2. (a) If $X \subset k^n$ is an algebraic set, show that $X(I(X)) = X$.
(b) If $I \subset k[x_1, ..., x_n]$ is a geometric ideal, show that $I(X(I)) = I$.
(c) Do we need the assumption $k = \overline{k}$ for (a) and (b) to be true?

3. Prove that the components of a reducible algebraic set are uniquely determined.

4. Show that for each $n > 0$ there are ideals in $k[x_1, x_2]$ that require n generators. (This is in contrast with $k[x_1]$, which is a PID).

5. Find embeddings of each of the following commutative rings in the ring $k[t]$ and conclude that the corresponding plane curves $X(\langle f\rangle)$ are irreducible.

(a) $k[x_1, x_2]/\langle x_2^2 - x_1^3\rangle$

(b) $k[x_1, x_2]/\langle x_2^2 - x_1^2(x_1 - 1)\rangle$

6. Find three prime quadratic polynomials $q_1, q_2, q_3 \in k[x_1, x_2, x_3]$ such that:

$$X(q_1) \cap X(q_2) \cap X(q_3) = \{(t, t^2, t^3) \mid t \in k\} \subset k^3$$

(this is the *twisted cubic curve*). What are the pairwise intersections $X(q_i) \cap X(q_j)$?

7. Prove that the intersection of any two non-empty open subsets of k^n is non-empty. Conclude that the Zariski topology is not Hausdorff.