C3.4 Algebraic Geometry

Lecture 1: Introduction

Balázs Szendrői, University of Oxford, Michaelmas 2020

What is algebraic geometry about?

Algebraic geometry is the study of geometric spaces given by polynomial equations. More precisely, it is the study of geometric spaces given by the **vanishing** of polynomial equations of (Cartesian) coordinates.

Polynomials: very natural notion. As soon as we have "numbers" that we can add and multiply, we can take a bunch of variables and write down polynomials.

We get polynomial rings $S[x_1, x_2, \ldots]$ over rings S.

In this course,

- we will consider polynomial rings over fields k, and
- we will have a finite number of indeterminates (variables), so

$$R = k[x_1, \ldots, x_n].$$

We will think of variables $x_1, \ldots, x_n$ as Cartesian coordinates on affine space

$$p = (x_1, \ldots, x_n) \in \mathbb{A}^n = \mathbb{A}^n_k = k^n.$$

Familiar examples

You already know some examples from earlier studies!

- Fix constants $a_1, \ldots, a_n, c \in k$. Then
$$H = \left\{ \sum_{i=1}^{n} a_i x_i - c = 0 \right\} \subset \mathbb{A}^n$$
is an **affine hyperplane**. If $c = 0$, then H is a **hyperplane** (codimension one linear subspace).
- More generally, if we take several such equations, we get **affine linear subspaces**, respectively (if all constants are zero) **linear subspaces**.
- Take $k = \mathbb{R}$. Then
$$\{x^2 + y^2 - 1 = 0\} \subset \mathbb{A}^2_{\mathbb{R}}$$
is a **circle**. More generally, any quadratic equation in (x, y) describes a (real) **plane conic** or **conic section**.

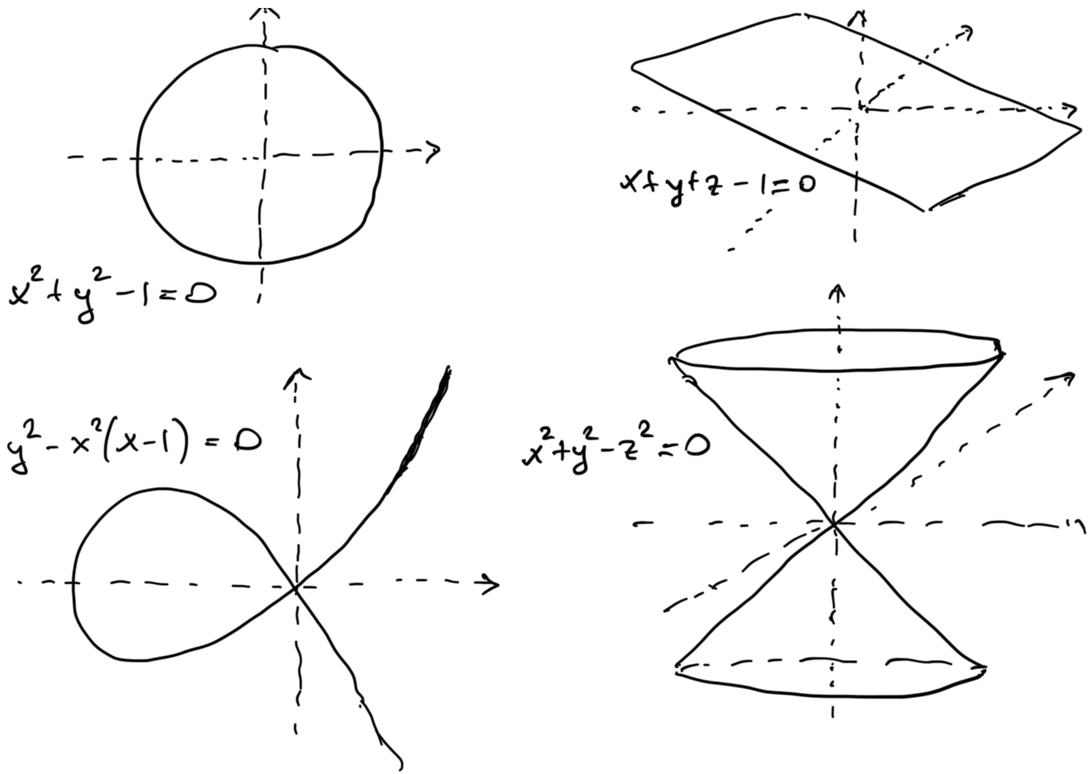
More familiar examples

- Take $k = \mathbb{C}$. Then
$$\{p(x, y) = 0\} \subset \mathbb{A}^2_{\mathbb{C}}$$
for any polynomial $p \in \mathbb{C}[x, y]$ is a (complex) **affine plane curve**, studied in the Oxford Part B course on Complex Algebraic Curves (and of course elsewhere).

- Take $k = \mathbb{R}$ again. Then
$$\{x^2 + y^2 - z^2 - c = 0\} \subset \mathbb{A}^3_{\mathbb{R}}$$
is a **hyperboloid**, with number of sheets depending on the sign of $c \neq 0$. For $c = 0$, we get the **quadric cone**.

- With $k = \mathbb{R}$ and arbitrary n, we have the (real) $(n-1)$**-sphere**
$$S^{n-1} = \left\{ \sum_{i=1}^{n} x_i^2 - 1 = 0 \right\} \subset \mathbb{A}^n_{\mathbb{R}}.$$

Familiar examples over $\mathbb{R}$ in pictures



General features

- A lot of the theory works for arbitrary fields k. We will assume
  - k has characteristic 0;
  - k is algebraically closed.
- Just take $k = \mathbb{C}$ if you wish!
- Number of variables will be arbitrary (finite!).
- Number of equations will also be arbitrary (finite! but now not a restriction).
- Drawing pictures remains a lot easier if $k = \mathbb{R}$ and $n \leq 3$...
- Don't forget other fields such as $\mathbb{F}_p, \mathbb{F}_q, \mathbb{Q}_p, \mathbb{C}(t), \ldots$ in further studies.

Applications of algebraic geometry

- Within pure mathematics: interacts with many different fields!
  - Key role in Wiles' proof of Fermat's Last Theorem
- Recent prominent role in theoretical physics
  - Spacetime models in string theory from algebraic geometry via supersymmetry
- Prominent applications in other areas
  - Algebraic robotics: describe motion of automate constrained by polynomial conditions.
  - Cryptography: cryptosystems from geometry (elliptic curves, abelian varieties...)
  - Algebraic systems biology: describe equilibria of complicated polynomial interaction systems

Sources of information

- Lecture notes by Prof Ritter on course website
  - Will follow the same notation.
  - The material in lectures forms a subset of the notes; will ignore categorical aspects but feel free to read those sections for a different, important point of view.
- Books
  - Many books around. Reid: UAG is perhaps the most useful. Hartshorne: Algebraic geometry is the “bible” but is too advanced just for this course.
- Problem sheets
  - There will be 5 problem sheets in total. Sheet 0 is not for handing in.

Commutative algebra in algebraic geometry

k denotes a field, algebraically closed and of characteristic 0, with unit $1 \in k$.

R a finitely generated, unital, commutative k-algebra: finitely generated as a commutative ring, has multiplication by elements of k, also has unit $1 \in R$. For example,

$$R = k[x_1, \ldots, x_n].$$

We will consider ideals $I \lhd R$, their intersections, products, quotient rings, etc. Also ring/algebra homomorphisms, kernels, images, etc.

I will quote results from Commutative Algebra. They can be taken without proof in this course; the Part B course Commutative algebra proves most of these results.

A simple but important proposition

Proposition Let k be a field, S a finitely generated commutative k-algebra. Then

$$S \cong k[x_1, \ldots, x_n]/I$$

for some n and an ideal $I \lhd k[x_1, \ldots, x_n]$.

Proof Let $s_1, \ldots s_n \in S$ be a set of k-algebra generators of S. Consider the ring homomorphism

$$\varphi \colon k[x_1, \ldots, x_n] \to S$$

defined by $\varphi(x_i) = s_i$. Then φ is surjective, since s_i generate S. Considering

$$I = \ker \varphi \lhd k[x_1, \ldots, x_n],$$

we get indeed

$$S \cong k[x_1, \ldots, x_n]/I$$

by the Isomorphism Theorem for rings. $\square$

Vanishing sets

We are working in the space $k^n = \{a = (a_1, \dots, a_n) : a_j \in k\}$.

This space corresponds to the polynomial ring $R = k[x_1, \dots, x_n]$.

$X \subset k^n$ is an **affine (algebraic) variety**, if $X = \mathbb{V}(I)$ for some ideal $I \subset R$, where

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

Examples

- For the zero ideal, $\mathbb{V}(0) = k^n$.
- For the ideal $\langle 1 \rangle = R$ generated by the identity, $\mathbb{V}(R) = \emptyset$.
- For some nonconstant $f \in R \setminus k$ generating principal ideal $\langle f \rangle \lhd R$, we get

$$V_f = \mathbb{V}(\langle f \rangle) = \{a \in k^n : f(a) = 0\},$$

  the **hypersurface** defined by f.

An easy but important example

Let $a = (a_1, \ldots, a_n) \in k^n$ and consider

$$\mathfrak{m}_a = \langle x_1 - a_1, \ldots, x_n - a_n \rangle \lhd R.$$

The following are all easy to check:

- $\mathbb{V}(\mathfrak{m}_a) = \{a\} \subset k^n$.
- The ideal $\mathfrak{m}_a \lhd R$ is the kernel of the evaluation homomorphism

  $$\mathrm{ev_a} \colon R \to k$$

  defined by $f \mapsto f(a)$.
- The ideal $\mathfrak{m}_a \lhd R$ is a maximal ideal of R.

Recall that an ideal $\mathfrak{m} \lhd R$ of a ring is **maximal** if it is not equal to R, nor is properly contained in another proper ideal of R. Remember that $\mathfrak{m} \lhd R$ is maximal if and only if the quotient $R/\mathfrak{m}$ is a field.

Some basic properties of vanishing sets

1. $I \subset J \Rightarrow \mathbb{V}(I) \supset \mathbb{V}(J)$.
2. $\mathbb{V}(I) \cup \mathbb{V}(J) = \mathbb{V}(I \cdot J) = \mathbb{V}(I \cap J)$.
3. $\mathbb{V}(I) \cap \mathbb{V}(J) = \mathbb{V}(I + J)$. (Note: $\langle I \cup J \rangle = I + J$.)
4. $\mathbb{V}(I), \mathbb{V}(J)$ are disjoint if and only if I, J are relatively prime (i.e. $I + J = \langle 1 \rangle$)

The proofs are easy exercises.

Hilbert's Basis Theorem

Hilbert's Basis Theorem $R = k[x_1, \ldots, x_n]$ is a Noetherian ring. In other words, it satisfies the following equivalent conditions.

1. Every ideal is **finitely generated** (f.g.)

$$I = \langle f_1, \ldots, f_m \rangle = Rf_1 + \cdots + Rf_m.$$

2. **ACC** (Ascending Chain Condition) on ideals:

$$I_1 \subset I_2 \subset \cdots \text{ ideals } \Rightarrow I_N = I_{N+1} = \cdots \text{ eventually all become equal.}$$

Equations of affine varieties

Corollary Any vanishing set $V = \mathbb{V}(I)$ is the common zero locus in k^n of a **finite** number of polynomials:

$$V = \{a \in \mathbb{A}^n \colon f_1(a) = \ldots = f_m(a) = 0\}.$$

Proof Use the Hilbert Basis Theorem: take a set of generators $f_1, \ldots, f_m$ of the ideal I. So

$$I = \langle f_1, \ldots, f_m \rangle \lhd R.$$

Then clearly $f(a) = 0$ for all $f \in I$ if and only if $f_i(a) = 0$ for all $i = 1, \ldots, m$. □

We will often refer to $f_1 \ldots, f_m$ as the "equations of V", even though the set of equations is not really well defined.

On Noetherian rings

Easy proposition If R is Noetherian, any quotient of R is also Noetherian.

Corollary A finitely generated k-algebra S is Noetherian.

Easy proposition If R is Noetherian, any ideal of I is contained in a maximal ideal $\mathfrak{m}$.

Proof Keep adding elements; eventually you must get to a maximal ideal by the ACC. $\square$

This statement is true in fact in arbitrary rings, but the proof is harder and requires Zorn's Lemma.

Hilbert's Weak Nullstellensatz

Theorem (Weak Nullstellensatz) Assume that k is algebraically closed. Then every maximal ideal of the ring $R = k[x_1, \ldots, x_n]$ is of the form $\mathfrak{m}_a \lhd R$ for some $a = (a_1, \ldots, a_n) \in k^n$.

This fails over fields that are not algebraically closed.

Example Let $k = \mathbb{R}$, $R = \mathbb{R}[x]$, and $I = \langle x^2 + 1 \rangle$.
Then $I = \ker \psi$ for $\psi \colon R \to \mathbb{C}$ given by $f \mapsto f(i)$.

So R/I is a field, and in particular $I \lhd R$ is maximal. But clearly I is a principal ideal not generated by degree one polynomial(s).

Corollary $\mathbb{V}(I) = \emptyset \Leftrightarrow 1 \in I \Leftrightarrow I = R$.

Proof If $1 \notin I$ then I is a proper ideal, so it lies inside some maximal ideal $\mathfrak{m}$.
By the Weak Nullstellensatz $\mathfrak{m} = \mathfrak{m}_a$ for some $a \in \mathbb{A}^n$.
But $I \subset \mathfrak{m}_a$ implies $\mathbb{V}(I) \supset \mathbb{V}(\mathfrak{m}_a) = \{a\}$. $\square$

The Zariski topology on k^n

The **Zariski topology** on k^n is defined by declaring that the closed sets are the sets of the form $\mathbb{V}(I)$.

Easy proposition This is indeed a topology!

Proof Use easy properties of vanishing sets listed above! □

The open sets of the topology look as follows:

$$\begin{aligned} U_I &= k^n \setminus \mathbb{V}(I) \\ &= k^n \setminus (\mathbb{V}(f_1) \cap \cdots \cap \mathbb{V}(f_m)) \\ &= (k^n \setminus \mathbb{V}(f_1)) \cup \cdots \cup (k^n \setminus \mathbb{V}(f_m)) \\ &= D_{f_1} \cup \cdots \cup D_{f_m}, \end{aligned}$$

where $I = \langle f_1, \ldots, f_m \rangle$ and the D_{f_i} are called the **basic open sets**

$$D_f = k^n \setminus \mathbb{V}(f) = \{a \in k^n : f(a) \neq 0\}.$$

Let $\mathbb{A}^n$ be **affine n-space**, the topological space k^n with the Zariski topology.

The Zariski topology on $\mathbb{A}^1$

Example. $\mathbb{A}^1 = k$ has the following closed sets: $\emptyset, \mathbb{A}^1$, and all finite subsets of $\mathbb{A}^1$.

Proof Let $I \lhd R = k[x]$. As R is a PID, we have $I = \langle f \rangle$ for some $f \in R$. If f is not constant, it has a finite set of roots.

Conversely, any finite subset of k is clearly the root set of some polynomial f.

$\square$

Correspondingly, the open sets in $\mathbb{A}^1$ are $\emptyset, \mathbb{A}^1$, and the complement of any finite set of points.

Some things to observe:

- This topology is not Hausdorff, since any two non-empty open sets intersect.
- The open sets are dense, as the only closed set with infinitely many points is $\mathbb{A}^1$ (note k is infinite).

The Zariski topology on $\mathbb{A}^2$

The following statement is not obvious; see Problem Sheet 1.

Example. $\mathbb{A}^2 = k$ has the following closed sets: $\emptyset, \mathbb{A}^2$, and finite unions of

- plane curves given by equations $p(x, y) = 0$, and
- points of $\mathbb{A}^2$.