Algebraic Geometry

Frank-Olaf Schreyer

Saarland University, Perugia July 2021

Overview

Algebraic Geometry is a huge area of mathematics, which went through several phases: Hilbert's fundamental paper from 1899, sheaves and cohomology introduced by Serre in the 1950's, Grothendieck's theory of schemes in the 1960's and so on.
In this course we will cover the state of affair after Hilbert's paper. We will give the proof of his important theorems with an emphasis on computational methods. In particular we will use Gröbner bases systematically.
The highlights of the course are the Nullstellensatz, Gröbner basis, Hilbert's syzygy theorem and the Hilbert function, Bézout's theorem, Mora division, semi-continuity of the fiber dimension, Bertini's theorem, Cremona resolution of plane curves and finally parametrization of rational curves. We will also take a glance at the Hilbert scheme and interpret lead term ideals as limits under one-parameter subgroups in $\mathrm{PGL}(n+1)$.

Weekly program

1-st week. Hilbert's Nullstellensatz and the ideal membership problem, Gröbner bases and Buchberger's criterion, the projection theorem, the algebra-geometry dictionary.
2-nd week. Component decomposition, noetherian rings and primary decomposition, localization, associated primes, the rational function field, dimension and transcendence degree, a Gröbner basis dimension criterium, the lying-over theorem, Krull dimension, constructive ideal and module theory.
3-rd week. $\mathbb{P}^n$, graded rings and the homogeneous coordinate ring, the syzygy theorem and the Hilbert polynomial, intersection multiplicities, multiplicity of points on plane curves, Bézout's theorem, local rings and the Lemma of Nakayama, completions and the ring of formal power series, Grauert division and the Weierstraß preparation theorem, Mora division, tangent space and tangent cone, Segre products, morphisms, linear projections, a dimension bound.

Weekly program

4-th week. Veronese embeddings, the fundamental theorem of elimination, projective morphisms, semi-continuity of the fiber dimension, the blow-up, resolution of singularities, Cremona transformations, linear systems of plane curves, Grassmannians, the Hilbert scheme, initial ideals and one-parameter subgroups, Bertini's theorem and the geometric interpretation of the degree, the dual variety, dynamical intersection numbers, a bound on the number of singular points of plane curves, rational curves, the geometric genus.

Further literature

Apart from the course notes in the form of slides the following books provide additional material.

- William Fulton: *Algebraic Curves: An Introduction to Algebraic Geometry*, Benjamin 1989, available online at CurveBook.pdf
- David A Cox; John Little; Donal O'Shea: *Ideals, Varieties, and Algorithm*, Springer 1990
- David A Cox;John Little;Donal O'Shea: *Using algebraic geometry*, GTM 185, Springer 1998
- M.F. Atiyah; I.G. Macdonald: *Introduction to Commutative Algebra*, Addison-Wesley 1969
- David Eisenbud: *Commutative Algebra with a View Toward Algebraic Geometry*, GTM 150, Springer 1995

These books gave inspiration for this course.

First lecture

The first lecture has the following topics:

1. Algebraic systems of equations
2. Basic questions and their answers
3. Ideals and residue rings
4. The ideal membership problem
5. Hilbert's Nullstellensatz
6. Algebraic sets and their $\mathbb{Q}$-rational points

Introduction

One of the basic tasks in mathematics is to solve algebraic systems of equations.

Example The equations

$$\frac{x^2}{2} + y^2 = 1, \quad x^2 + 4y^2 = 1$$

define two ellipses which intersect in four points.

The general set up

Let K be a field, for example $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$. The vanishing loci of a polynomial

$$f = f(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$$

in n variables $x_1, \dots x_n$ with coefficients in K is the set

$$V(f) = \{a = (a_1, \dots, a_n) \in K^n \mid f(a_1, \dots, a_n) = 0\} \subset K^n =: \mathbb{A}^n(K)$$

Given finitely many polynomials

$$f_1, \dots, f_r \in K[x_1, \dots, x_n]$$

we denote by

$$V(f_1, \dots, f_r) = \bigcap_{j=1}^{r} V(f_j)$$

the common solution space of the system of equations

$$f_1 = 0, \dots, f_r = 0.$$

Most basic questions

Given $f_1, \dots, f_r \in K[x_1, \dots, x_n]$ we may ask:

1. Has the corresponding system of equations a solution?

$$\text{Is } V(f_1, \dots, f_r) \neq \emptyset \quad ?$$

2. If $V(f_1, \dots, f_r) \neq \emptyset$, how many solutions are there?
3. If there are infinitely many solutions, what is the dimension of the solution space?
4. If there are infinitely many solutions, can we parametrize the solution space?

Examples of parametrizations

Example. $x^2 + y^2 = 1$

$$\Rightarrow x = \tfrac{2t}{1+t^2}, y = \tfrac{1-t^2}{1+t^2}.$$

Example. $y^2 = x^3 + x^2$

$$\Rightarrow x = t^2 - 1, y = t(t^2 - 1).$$

part 1

Basic answer to question 1

The answer to the first question depends very much on the nature of the field.

a) In case of $\mathbb{C}$, solvability can be decided with Hilbert's Nullstellensatz (1899)

b) In case of $\mathbb{R}$, quantifier elimination (Tarski 1948) leads to an answer.
Example. $\exists x \in \mathbb{R} : x^2 + px + q = 0 \iff p^2 - 4q \geq 0$

c) In case of $\mathbb{Q}$, there exists no general algorithm which decides whether a system of algebraic equations has a rational solution. (Matiyasevich's solution (1970) of Hilbert's 10-th problem)

Hilbert's Nullstellensatz uses the concept of ideals which we discuss next.

Ideals

Definition. Let R be a (commutative) ring (with 1). A non-empty subset $I \subset R$ is an **ideal** if

1) $a, b \in I \Rightarrow a + b \in I$, and
2) $r \in R, a \in I \Rightarrow ra \in I$

holds.

Example. Let

$$\varphi\colon R \to S$$

be a ring homomorphism. Then

$$\ker \varphi = \{a \in R \mid \varphi(a) = 0\}$$

is an ideal.

Example. Let $f_1, \dots, f_r \in R$ be elements of a ring. Then

$$(f_1, \dots, f_r) = \{f \mid \exists g_1, \dots, g_r \in R : f = g_1 f_1 + \dots + g_r f_r\}$$

is an ideal, **the ideal generated by** $f_1, \dots, f_r$.

Residue rings

Let R be a ring, $I \subset R$ an ideal. Then

$$a \equiv b \mod I \iff a - b \in I$$

is an equivalence relation on R. We denote with

$$\overline{a} = \{b \in R \mid b \equiv a\} = a + I \subset R$$

the residue class of a. The set of residue classes

$$R/I = \{\overline{a} \mid a \in R\} \subset 2^R$$

carries the structure of a ring defined by

$$\overline{a} + \overline{b} := \overline{a + b}, \overline{a} \cdot \overline{b} := \overline{ab}.$$

This is the unique ring structure on R/I which makes the map

$$\pi \colon R \to R/I, a \mapsto \overline{a}$$

into a ring homomorphism. $\ker \pi = I$.

Examples of residue rings

1) For $n \in \mathbb{Z}$ an integer, the residue ring $\mathbb{Z}/(n)$ has n elements

$$\{\overline{0}, \overline{1}, \dots, \overline{n-1}\}.$$

$\mathbb{Z}/(p)$ is a field iff p is a prime number. We denote by

$$\mathbb{F}_p := \mathbb{Z}/(p)$$

the field with p elements.

2) The polynomial $f = x^2 + x + 1 \in \mathbb{F}_2[x]$ has no zero in $\mathbb{F}_2$. The ring

$$\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$$

is a field with 4 elements.

3) All finite fields $\mathbb{F}_q$ can be constructed similarly. The number of elements $q = p^r$ is necessarily a prime power, and

$$\mathbb{F}_q \cong \mathbb{F}_p[x]/(f)$$

for f a monic irreducible polynomial of degree r in $\mathbb{F}_p[x]$.

Division with remainder

Theorem. *Let K be a field, $f \in K[x] \setminus \{0\}$ a univariate polynomial which is not the zero polynomial. For all $g \in K[x]$ there exist unique polynomials $q, r \in K[x]$ such that*

$$g = qf + r \text{ and } \deg r < \deg f.$$

r is called the **remainder** of g divided by f.

How to compute in $K[x]/(f)$?

Let K be a field, $f \in K[x] \setminus \{0\}$ a univariate polynomial. Suppose f is monic of degree $d = \deg f > 0$, i.e.

$$f = x^d + a_{d-1}x^{d-1} + \ldots + a_1 x^1 + a_0$$

Then every element $\overline{g} \in K[X]/(f)$ has a unique representative $r \in K[x]$ by a polynomial of degree $\leq d-1$. As a K-vector space the elements $1, x, \ldots, x^{d-1}$ represent a K-vector space basis of $K[x]/(f)$.

Given two elements $\overline{g}, \overline{h} \in K[x]/(f)$, we compute their product by taking representatives g, h and the remainder r of gh divided by f.

Example. $\overline{x} \in \mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$. Then

$$\overline{x}^2 = -\overline{x} - 1 = \overline{x} + 1$$

and

$$\overline{x}^3 = \overline{x}^2 \overline{x} = (\overline{x} + 1)\overline{x} = \overline{x}^2 + \overline{x} = 1.$$

Hence the multiplicative group $(\mathbb{F}_4^*, \cdot)$ is cyclic of order 3.

Affine K-algebras

Definition. Let K be a field. An **affine K-algebra** is a ring of the form

$$R = K[x_1, \dots, x_n]/(f_1, \dots, f_r).$$

One of the goals of the course is to learn how to compute in such rings. In particular we want to decide whether an element $\overline{f}$ is zero in this ring.

Ideal membership problem. Given a field K, an ideal $(f_1, \dots, f_r) \subset K[x_1, \dots, x_n]$ and an element $f \in K[x_1, \dots, x_n]$ decide

$$f \in (f_1, \dots, f_r) \quad ?$$

Hilbert's Nullstellensatz

Theorem. *Let K be an algebraically closed field. Let $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ be polynomials. Then*

$$V(f_1, \ldots, f_r) = \emptyset \iff 1 \in (f_1, \ldots, f_r).$$

Thus combined with an algorithm for the membership problem, we can decide whether an algebraic system of equations has a solution. One direction in Hilbert's Nullstellensatz is easy. Suppose $1 \in (f_1, \ldots, f_r)$, say $1 = g_1 f_1 + \ldots + g_r f_r$. If $a \in V(f_1, \ldots, f_r)$, then

$$1 = g_1(a) f_1(a) + \ldots + g_r(a) f_r(a) = 0,$$

a contradiction. Thus $V(f_1, \ldots, f_r) = \emptyset$.

part 3

Algebraically closed fields

Definition. A field K is algebraically closed if every non-constant univariate polynomial $f \in K[X]$ has a root in K.

The assumption K algebraically closed is clearly a necessary assumption in Hilbert's Nullstellensatz:
If $f \in K[x]$ is univariate polynomial of positive degree which has no root in K, then $V(f) = \emptyset \subset \mathbb{A}^1(K)$. But $1 \notin (f)$, since non-zero elements of (f) have degree $\geq \deg f$.

Fundamental theorem of algebra. *The field of complex numbers* $\mathbb{C}$ *is algebraically closed.*

Solvability with Computer Algebra

For $f_1, \ldots, f_r \in \mathbb{Q}[x_1, \ldots, x_n]$ we consider the vanishing loci

$$V(f_1, \ldots, f_r) := \{a \in \mathbb{C}^n \mid f_1(a) = 0, \ldots, f_r(a) = 0\} \subset \mathbb{A}^n(\mathbb{C})$$

over $\mathbb{C}$. Due to the Nullstellensatz we can decide $V(f_1, \ldots, f_r) = \emptyset$ with a computation over $\mathbb{Q}$:

The condition $1 = g_1 f_1 + \ldots + g_r f_r$ can be viewed as a linear system of equations for unknown coefficients of $g_1, \ldots, g_r$. If this system has a solution over $\mathbb{C}$, it also has a solution over $\mathbb{Q}$. Thus

$$V(f_1, \ldots, f_r) = \emptyset \subset \mathbb{A}^n(\mathbb{C}) \iff 1 \in (f_1, \ldots, f_r) \subset \mathbb{Q}[x_1, \ldots, x_n].$$

Implementing $\mathbb{C}$ into a computer requires numerical methods. But $\mathbb{Q}$ is accessible to exact computer algebra methods.

Algebraic sets

Let $\overline{K}$ be an algebraically closed field.
Definition. We denote by $\mathbb{A}^n = \overline{K}^n$ the affine n-space over $\overline{K}$. An **algebraic set** $X \subset \mathbb{A}^n$ is a set of the form

$$X = V(f_1, \ldots, f_r) \subset \mathbb{A}^n$$

for polynomials $f_1, \ldots, f_r \in \overline{K}[x_1, \ldots, x_n]$.
If $f_1, \ldots, f_r \in K[x_1, \ldots, x_n]$ for a subfield $K \subset \overline{K}$, then we call K a field of definition of X. In this case

$$X(K) = X \cap \mathbb{A}^n(K) \subset \mathbb{A}^n = \mathbb{A}^n(\overline{K})$$

denotes the set of K-rational points of X.

Diophantine equations

Let $f_1, \ldots, f_r \in \mathbb{Z}[x_1, \ldots, x_n]$ be polynomials with integral coefficients and

$$X = V(f_1, \ldots, f_r).$$

Then for any prime number p we can reduce the coefficients mod p to obtain equations in $\mathbb{F}_p[x_1, \ldots, x_n]$.
Thus $X(\mathbb{F}_p)$ makes sense, and the numbers

$$N_r = |X(\mathbb{F}_{p^r})|$$

of $\mathbb{F}_{p^r}$-rational points are defined.
We will see that for almost all prime numbers p, the growth of N_r determines the dimension of X over $\mathbb{C}$:

$$N_r = O(p^{rk}) \iff \dim_{\mathbb{C}} X = k.$$

If we want to study $X(\mathbb{Q})$, then the study of $X(\mathbb{F}_{p^r})$ and $X(\mathbb{R})$ gives some partial information. There is a huge branch of mathematics devoted to this approach to diophantine equations.