MAT4210—Algebraic geometry I: Notes 1

Closed algebraic sets and the Nullstellensatz

25th January 2018

These notes are just informal extensions of the lectures. As the course develops I'll now and then post new notes on the course's website, but this will certainly happen with irregular intervals. The idea with the notes is to give additional comments and examples which hopefully will make your reading of the book and the digestion of the lectures easier; and hopefully will widen your mathematical horizon.

I am certainly going to deviate from the book we use[1] at several points, and these notes will help you cope with the deviations. Another classic and inspiring book is Mumford's red book[2].

And of course: Exercises—doing exercises is of paramount importance for learning mathematics (or probably for learning anything). Many of the exercises in the book are in fact part of the theory. Without promising anything, I'll try to include if not proofs, at least serious hint or sketches of proofs, for those exercises.

Hot themes in Notes 1: The correspondence between ideals and algebraic sets—different versions, weak and strong, of Hilbert's Nullstellensatz—the Rabinowitsch trick—two proofs of the Nullstellensatz, one (very) elementary, and another totally different—radical ideals—drawings and figures

Preliminary version 1.2 as of 25th January 2018 at 11:22am—Prone to misprints and errors.

Changes from 1.1: Added an exercise about formal derivatives; problem 1.13. Small changes in two exercises *i.e.,* 1.4 and 1.7.

Geir Ellingsrud — ellingsr@math.uio.no

[1]

[2]

Introduction

Algebraic geometry has many ramifications, but roughly speaking there are two main branches. One could be called the "geometric" branch where the geometry is the main objective. One studies geometric objects like curves , surfaces, threefolds and varieties of higher dimensions, defined by polynomials (or more generally algebraic functions). The aim is to understand their geometry. Frequently techniques from several other fields are used like from algebraic topology, differential geometry or analysis, and the studies are tightly connected with these other fields. This makes it natural to work over the complex field $\mathbb{C}$, even though other fields like function fields are important.

The other main branch one could call "arithmetic". Superficially presented, one studies numbers by geometric methods. An ultra famous example is Fermat's last theorem, now Andrew Wiles' theorem, that the equation $x^n + y^n = z^n$ has no integral solutions except the trivial ones. The arithmetic branch also relies on techniques from

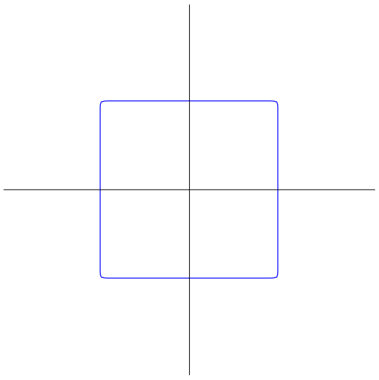


Figure 1: The affine Fermat curve $x^{50} + y^{50} = 1$.

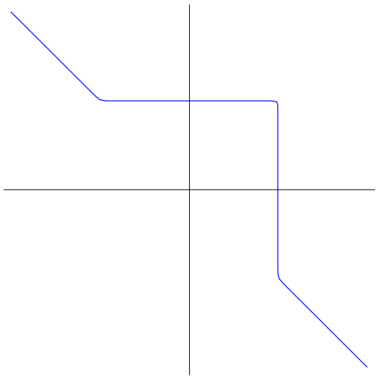


Figure 2: The affine Fermat curve $x^{51} + y^{51} = 1$.

other fields, like number theory, Galois theory and representation theory. One very commonly applied technique is reduction modulo a prime number p. Hence the importance of including fields of positive characteristic among the base fields. Of course another very natural base field for many of these "arithmetic" studies is the field $\overline{\mathbb{Q}}$ of algebraic numbers.

Algebraic geometry is to the common benefit in some sense a triple marriage of geometry, algebra and arithmetic. All of the spouses claim influence on the development of the field which makes the field quit abstract; but also a most beautiful part of mathematics.

Fields and the affine space

We shall almost exclusively work over an algebraic closed field which we shall denote by k. In general we do not impose further constraints on k, except for a few results that require the characteristic to be zero. A specific field to have in mind would be the field of complex numbers $\mathbb{C}$, but as indicated above, other important fields are $\overline{\mathbb{Q}}$ and $\overline{\mathbb{F}}_p$.

The affine space $\mathbb{A}^n$ is just the space k^n, but the name-change is there to underline that there is more to it than merely being a vector space—hopefully this will emerge from the fog during the course. Anyhow, in the beginning think about it as k^n. Often the ground field is tacitly understood, but when wanting to be precise about it, we shall write $\mathbb{A}^n(k)$. The ground will always be algebraically closed unless the contrary is explicitly stated.

Coordinates are certainly not God-given but man-made. So they are prone to being changed. General coordinate changes in $\mathbb{A}^n$ can be subtle, but translation of the origin and linear changes are unproblematic, and will be done unscrupulously. They are called *affine coordinate changes* and the affine spaces $\mathbb{A}^n$ are named after them.

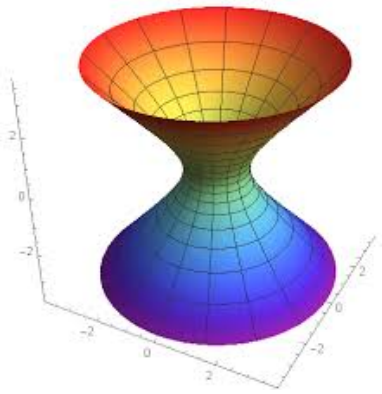


Figure 3: A one sheeted-hyperboloid.

Closed algebraic sets

ClosedAlgeSets

Closed algebraic sets

The first objects we shall meet are the so called *closed algebraic sets*. You have seen many examples of these already. They are just subsets of the affine space $\mathbb{A}^n$ given by a certain number of polynomial equations. You have probably seen a lot of curves in the plane and may be some surfaces in the space—like conic sections and hyperboloids and paraboloids, for example.

FORMALLY the definition of a closed algebraic set is as follows. If S is a subset of the polynomial ring $k[x_1, \ldots, x_n]$, one defines

$$Z(S) = \{\, x \in \mathbb{A}^n \mid f(x) = 0 \text{ for all } f \in S \,\},$$

$\mathfrak{a}, \mathfrak{A}$	$\mathfrak{b}, \mathfrak{B}$	$\mathfrak{c}, \mathfrak{C}$	$\mathfrak{d}, \mathfrak{D}$	$\mathfrak{e}, \mathfrak{E}$
$\mathfrak{f}, \mathfrak{F}$	$\mathfrak{g}, \mathfrak{G}$	$\mathfrak{h}, \mathfrak{H}$	$\mathfrak{i}, \mathfrak{I}$	$\mathfrak{j}, \mathfrak{J}$
$\mathfrak{k}, \mathfrak{K}$	$\mathfrak{l}, \mathfrak{L}$	$\mathfrak{m}, \mathfrak{M}$	$\mathfrak{n}, \mathfrak{N}$	$\mathfrak{o}, \mathfrak{O}$
$\mathfrak{p}, \mathfrak{P}$	$\mathfrak{q}, \mathfrak{Q}$	$\mathfrak{r}, \mathfrak{R}$	$\mathfrak{s}, \mathfrak{S}$	$\mathfrak{t}, \mathfrak{T}$
$\mathfrak{u}, \mathfrak{U}$	$\mathfrak{v}, \mathfrak{V}$	$\mathfrak{w}, \mathfrak{W}$	$\mathfrak{x}, \mathfrak{X}$	$\mathfrak{y}, \mathfrak{Y}$
$\mathfrak{z}, \mathfrak{Z}$				

Mathematicians are always in shortage of symbols and use all kinds of alphabets. The germanic gothic letters are still in use in some context, like to denote ideals in some text books.

and subsets of $\mathbb{A}^n$ obtained in that way are the *closed algebraic sets*. Notice that any linear combination of polynomials from S also vanishes at points of $Z(S)$, even if polynomials are allowed as coefficients. Therefore the *ideal* $\mathfrak{a}$ generated by S has the same zero set as S; that is, $Z(S) = Z(\mathfrak{a})$. We shall almost exclusively work with ideals and tacitly replace a set of polynomials by the ideal it generates.

Any ideal in $k[x_1, \ldots, x_n]$ is finitely generated, this is what Hilbert's basis theorem tells us, so that a closed algebraic subset is described as the set of common zeros of *finitely* many polynomials.

EXAMPLE 1.1 The polynomial ring $k[x]$ in one variable is a PID[3], so if $\mathfrak{a}$ is an ideal, it holds that $\mathfrak{a} = (f(x))$. Because polynomials in one variable merely have finitely many zeros, the closed algebraic subsets of $\mathbb{A}^1$ are just the finite subsets of $\mathbb{A}^1$. ☆

[3] A ring is a PID or a *principal ideal domain* if it is an integeral domain where every ideal is principal

EXAMPLE 1.2 A more spectacular example is the so called *Clebsch diagonal cubic*; a surface in $\mathbb{A}^3(\mathbb{C})$ with equation

$$x^3 + y^3 + z^3 + 1 = (x + y + z + 1)^3.$$

An old plaster model of its reals points; that is, the points in $\mathbb{A}^3(\mathbb{R})$ satisfying the equation, is depicted in the margin. ☆

The Clebsch diagonal cubic

EXAMPLE 1.3 The traditional conic sections are closed algebraic sets in $\mathbb{A}^2$. A *parabola* is given as the zeros of $y - x^2$ and a *hyperbola* as the zeros of $xy - 1$. ☆

THE MORE CONSTRAINTS one imposes the smaller the solutions set will be, so if $\mathfrak{b} \subseteq \mathfrak{a}$ are two ideals, one has $Z(\mathfrak{a}) \subseteq Z(\mathfrak{b})$. The *sum* $\mathfrak{a} + \mathfrak{b}$ of two ideals has the intersection $Z(\mathfrak{a}) \cap Z(\mathfrak{b})$ as zero set; remembering that

$$\mathfrak{a} + \mathfrak{b} = \{\, f + g \mid f \in \mathfrak{a} \text{ and } \; g \in \mathfrak{b} \,\}$$

one easily convinces oneself of this. In the same vein, the *product* $\mathfrak{a} \cdot \mathfrak{b}$ defines the union $Z(\mathfrak{a}) \cup Z(\mathfrak{b})$. With a little thought, this is clear since the products $f \cdot g$ of polynomials $f \in \mathfrak{a}$ and $g \in \mathfrak{b}$ generate $\mathfrak{a} \cdot \mathfrak{b}$. Sending $\mathfrak{a}$ to $Z(\mathfrak{a})$ is a order reversing map from the partially ordered sets of ideals in $k[x_1, \ldots, x_n]$ to the partially ordered set of subsets of $\mathbb{A}^n$.

IT MIGHT VERY well happen that two different ideals define the same algebraic set. The most stupid example being (x) and (x^2); they both define the origin in the affine line $\mathbb{A}^1$. More generally, powers $\mathfrak{a}^n$ of an ideal $\mathfrak{a}$ have the same zeros as $\mathfrak{a}$. Because $\mathfrak{a}^n \subseteq \mathfrak{a}$ it holds that $Z(\mathfrak{a}) \subseteq Z(\mathfrak{a}^n)$, and the other inclusion holds as well since $f^n \in \mathfrak{a}^n$ whenever $f \in \mathfrak{a}$. Recall that the *radical* $\sqrt{\mathfrak{a}}$ of an ideal is the ideal

whose members are the polynomials for which a power lies in $\mathfrak{a}$; that is,

$$\sqrt{\mathfrak{a}} = \{\, f \mid f^r \in \mathfrak{a} \text{ for some } r \,\}.$$

The argument above yields that $Z(\mathfrak{a}) = Z(\sqrt{\mathfrak{a}})$ (in fact, since all ideals in the polynomial ring are finitely generated, a power of the radical is contained in $\mathfrak{a}$). Ideals with the same radical therefore have coinciding zero sets, and we shall soon see that the converse is true as well. This is the content of the famous Hilbert's Nullstellensatz which we are about to formulate and prove, but first we sum up the present discussion in a proposition:

Proposition 1.1 *Let $\mathfrak{a}$ and $\mathfrak{b}$ be two ideals in $k[x_1, \ldots, x_n]$.*

- *If $\mathfrak{a} \subseteq \mathfrak{b}$, then $Z(\mathfrak{b}) \subseteq Z(\mathfrak{a})$;*
- $Z(\mathfrak{a} + \mathfrak{b}) = Z(\mathfrak{a}) \cap Z(\mathfrak{b})$;
- $Z(\mathfrak{a}\mathfrak{b}) = Z(\mathfrak{a}) \cup Z(\mathfrak{b})$;
- $Z(\mathfrak{a}) = Z(\sqrt{\mathfrak{a}})$.

By the way, this also shows that $Z(\mathfrak{a} \cap \mathfrak{b}) = Z(\mathfrak{a}) \cup Z(\mathfrak{b})$: Because of the inclusion $(\mathfrak{a} \cap \mathfrak{b})^2 \subseteq \mathfrak{a} \cdot \mathfrak{b}$ one has $Z(\mathfrak{a} \cap \mathfrak{b}) \subseteq Z(\mathfrak{a}) \cup Z(\mathfrak{b})$, and the other inclusion follows readily. Notice also that the argument for the second assertion remains valid, *mutatis mutandis*, for any family of ideals $\{\mathfrak{a}_i\}_{i \in I}$; that is, one has

- $Z(\sum_{i \in I} \mathfrak{a}_i) = \bigcap_i Z(\mathfrak{a}_i)$.

David Hilbert (1862–1943)
German mathematician.

The Nullstellensatz involves the ideal $I(X)$ of polynomials in $k[x_1, \ldots, x_n]$ that vanish along the subset X of $\mathbb{A}^n$, which acts as a partial converse to $Z(\mathfrak{a})$. To be precise, for any subset $X \subseteq \mathbb{A}^n$ one defines

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

When X is an arbitrary set, there is not much information about X in $I(X)$; for instance, if X is any infinite subset of $\mathbb{A}^1$, it holds that $I(X) = 0$ (polynomials have only finitely many zeros). However, if X *a priori* is known to be a closed algebraic subset, it is true that $Z(I(X)) = X$; in other words, one has

- $Z(I(Z(\mathfrak{a}))) = Z(\mathfrak{a})$.

The Nullstellensatz

Hilbert's Nullstellensatz is about the composition of I and Z the other way around, namely about $I(Z(\mathfrak{a}))$. Polynomials in the radical

$\sqrt{\mathfrak{a}}$ vanish along $Z(\mathfrak{a})$ and therefore $\sqrt{\mathfrak{a}} \subseteq I(Z(\mathfrak{a}))$, and the Nullstellensatz tells us that this inclusion is an equality. We formulate the Nullstellensatz here, together with two of its weak avatars, but shall come back with a thorough discussion of the proof(s) a little later.

StrongNSS

Theorem 1.1 (Hilbert's Nullstellensatz) *Assume that k is an algebraically closed field, and that $\mathfrak{a}$ is an ideal in $k[x_1, \ldots, x_n]$. Then one has $I(Z(\mathfrak{a})) = \sqrt{\mathfrak{a}}$.*

Notice that the ground field must be algebraically closed. Without this assumption the result is not true. The simplest example of an ideal in polynomial ring with empty zero locus is the ideal $(x^2 + 1)$ in $\mathbb{R}[x]$.

Obviously it holds true that $I(\emptyset)$ equals the entire polynomial ring, and if $\mathfrak{a}$ is a proper ideal, it is as obvious that $\sqrt{\mathfrak{a}}$ is not the entire polynomial ring, so in particular, the theorem asserts that $Z(\mathfrak{a}) = \emptyset$ if and only if $\mathfrak{a}$ equals the whole polynomial ring; that is, if and only if $1 \in \mathfrak{a}$. Hence we can conclude that $Z(\mathfrak{a})$ is not empty when $\mathfrak{a}$ is proper. This statement goes under the name of the Weak Nullstellensatz; and is despite the name equivalent to the Nullstellensatz, as we shall see later on .

WeakNullSS

Theorem 1.2 (Weak Nullstellensatz) *Assume that k is an algebraically closed field. For every proper ideal $\mathfrak{a}$ in $k[x_1, \ldots, x_n]$ there is a point $x \in Z(\mathfrak{a})$.*

Consider now the ideals $(x_1 - a_1, \ldots, x_n - a_n)$ where the a_i's are elements from k. It is easy to see that all these are maximal ideals; indeed, after a linear change of variables it suffices to see that $(x_1, \ldots, x_n)$ is maximal, which is clear since $(x_1, \ldots, x_n)$ obviously is the kernel of the map $k[x_1, \ldots, x_n] \to k$ evaluating a polynomial at the origin.

Amazingly, the converse follows from the Nullstellensatz: Every maximal ideal in the polynomial ring is of this form. If $\mathfrak{m}$ is a maximal ideal, it is certainly a proper ideal, and by the Nullstellensatz there is point $(a_1, \ldots, a_n)$ in $Z(\mathfrak{m})$. Consequently it holds that $(x_1 - a_1, \ldots, x_n - a_n) \subseteq \mathfrak{m}$, but since $(x_1 - a_1, \ldots, x_n - a_n)$ is also maximal, the two ideals coincide. Hence we have the following equivalent version of the Weak Nullstellensatz:

HilbNull2

Theorem 1.3 (Weak Nullstellensatz II) *Let k be an algebraically closed field. Then the maximal ideals in the polynomial ring $k[x_1, \ldots, x_n]$ are those of the form $(x_1 - a_1, \ldots, x_n - a_n)$ with $(a_1, \ldots, a_n) \in \mathbb{A}^n$.*

Radical ideals and algebraic subsets

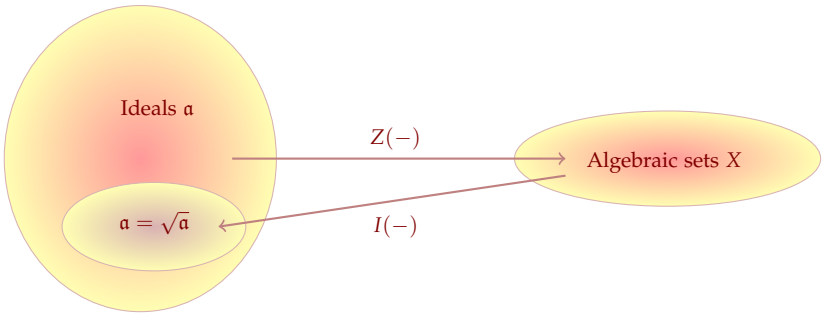
In view of the Nullstellensatz, it is natural to introduce the notion of a *radical ideal*. It is an ideal equal to its own radical; in other words, it

Radical ideals

satisfies $\mathfrak{a} = \sqrt{\mathfrak{a}}$. With this concept in place, the two constructions I and Z are mutually inverse mappings from the set of radical ideals to the set of closed algebraic sets.

Both sets are partially ordered under inclusion, and the two mappings both reverse the partial orders. Moreover, they take "sup's" to "inf's" and *vice versa*.

In a partial ordered set $\inf a, b$ is the greatest element less then both a and b, and $\sup a, b$ the smallest greater than both. In general they do not exists and do not need to be unique.



The radical of an intersection is the intersection of the radicals, so if $\mathfrak{a}$ and $\mathfrak{b}$ are two radical ideals, their intersection $\mathfrak{a} \cap \mathfrak{b}$ is as well, and it is the "inf" the two; that is, the greatest radical ideal contained in both.

On the other hand, the sum $\mathfrak{a} + \mathfrak{b}$ of two radical ideals is not in general radical. For instance, the ideals $(y - x^2)$ and (y) are both radical, but $(y - x^2) + (y) = (y - x^2, y) = (y, x^2)$ is not. Hence the "sup" of the two in the set of radical ideals will be $\sqrt{\mathfrak{a} + \mathfrak{b}}$. This means that for *radical ideals* one has the two relations:

- $I(Z(\mathfrak{a}) \cap Z(\mathfrak{b})) = \sqrt{\mathfrak{a} + \mathfrak{b}}$;
- $I(Z(\mathfrak{a}) \cup Z(\mathfrak{b})) = \mathfrak{a} \cap \mathfrak{b}$.

PROBLEM 1.1 Show that $(y - x^2)$ is radical. Let $\alpha \in k$ and let $\mathfrak{a} = (y - x^2, y - \alpha x)$. Show that $\mathfrak{a}$ is a radical ideal when $\alpha \neq 0$, but not when $\alpha = 0$. ★

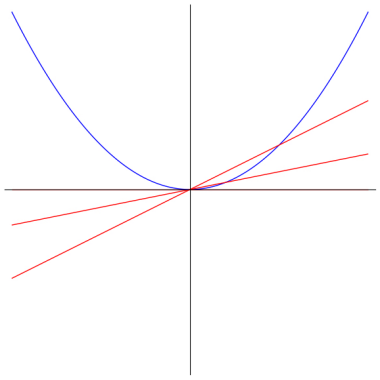


Figure 4: The parabola $y = x^2$ and some lines through the origin.

Affine coordinate rings

The coordinate ring

The ring $A(X) = k[x_1, \ldots, x_n]/I(X)$ is called the *affine coordinate ring* of X. If Y is a closed algebraic sets contained in X, it holds that $I(X) \subseteq I(Y)$, and conversely if $I(Y)$ contains $I(X)$, one has $Y \subseteq X$. Hence there is a one-to-one correspondence between radical ideals in the coordinate ring $A(X)$ and closed algebraic subsets contained in X. If $\mathfrak{a}$ is an ideal in $A(X)$, we denote by $Z(\mathfrak{a})$ the corresponding subvariety of X. And for a point $a = (a_1, \ldots, a_n) \in X$ we let $\mathfrak{m}_a$ denote the image in $A(X)$ of the maximal ideal $(x_1 - a_1, \ldots, x_n - a_n)$ of polynomials vanishing at x.

Hilbert's Nullstellensatz—proofs

In this section we discuss various proofs and various versions of the Nullstellensatz. The Nullstellensatz comes basically in two flavours, the strong Nullstellensatz and the weak one (of which we shall present three variations). Despite their names the different versions are equivalent. The strong version trivially implies the weak, but the reverse implication hinges on a trick frequently called the "Rabinowitsch"-trick.

The Rabinowitsch trick —– weak implies strong

We proceed to present the Rabinowitsch trick proving that the weak version of the Nullstellensatz (theorem 1.2 on page 5) implies the strong. That is, we need to demonstrate that $I(Z(\mathfrak{a})) \subseteq \sqrt{\mathfrak{a}}$ for any proper ideal $\mathfrak{a}$ in $k[x_1, \ldots, x_n]$.

The crux of the trick is to introduce a new variable x_{n+1} and for each $g \in I(Z(\mathfrak{a}))$ consider the ideal $\mathfrak{b}$ in the polynomial ring $k[x_1, \ldots, x_{n+1}]$ given by

$$\mathfrak{b} = \mathfrak{a} \cdot k[x_1, \ldots, x_{n+1}] + (1 - x_{n+1} \cdot g).$$

In geometric terms $Z(\mathfrak{b}) \subseteq \mathbb{A}^{n+1}$ is the intersection of the the subset $Z = Z(1 - x_{n+1} \cdot g)$ and the inverse image $\pi^{-1}Z(\mathfrak{a})$ of $Z(\mathfrak{a})$ under the projection $\pi\colon \mathbb{A}^{n+1} \to \mathbb{A}^n$ that forgets the last coordinate. This intersection is empty, since obviously g does not vanish on Z, but vanishes identically on $\pi^{-1}Z(\mathfrak{a})$.

The weak Nullstellensatz therefore gives that $1 \in \mathfrak{b}$, and hence there are polynomials f_i in $\mathfrak{a}$ and h_i and h in $k[x_1, \ldots, x_{n+1}]$ satisfying a relation like

$$1 = \sum f_i(x_1, \ldots, x_n) h_i(x_1, \ldots, x_{n+1}) + h \cdot (1 - x_{n+1} \cdot g).$$

We substitute $x_{n+1} = 1/g$ and multiply through by a sufficiently[4] high power g^N of g to obtain

$$g^N = \sum f(x_1, \ldots, x_n) H_i(x_1, \ldots, x_n),$$

where $H_i(x_1, \ldots, x_n) = g^N \cdot h_i(x_1, \ldots, x_n, g^{-1})$. Hence $g \in \sqrt{\mathfrak{a}}$.

[4] For instance the highest power of x_{n+1} that occurs in any of the h_i's.

The third version of the Weak Nullstellensatz

As already mentioned there are several variants of the weak Nullstellensatz. We have already seen two, and here comes number three, formulated for a general field k. This is the one we shall prove and subsequently deduce the other versions from. It has the virtue of

being general, and we shall bring it with us into Grothendieck's marvelous world of schemes.

HilbNullFinit

Theorem 1.4 (Weak Nullstellensatz III) *Let k a field and let $\mathfrak{m}$ be a maximal ideal in $k[x_1, \ldots, x_n]$. Then $k[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite field extension of k.*

Before proceeding to the proof of this version III we show how the Weak Nullstellensatz II (theorem 1.2 on page 5) can be deduced from version III (theorem 1.4 above).

PROOF OF II FROM III: Assume $\mathfrak{m}$ is a maximal ideal in $k[x_1, \ldots, x_n]$. The point is that the field $k[x_1, \ldots, x_n]/\mathfrak{m}$ is a finite extension of k after version III (theorem 1.4 above), and since k is algebraically closed by assumption, the two fields coincide. Thus there is an algebra homomorphism $k[x_1, \ldots, x_n] \to k$ having $\mathfrak{m}$ as kernel. Letting a_i be the image of x_i under this map, the ideal $(x_1 - a_1, \ldots, x_n - a_n)$ will be contained in $\mathfrak{m}$, and being maximal, it equals $\mathfrak{m}$. ❑

Proof of version III of the Nullstellensatz

The by far simplest proof of the Nullstellensatz I know, both technically and conceptually, was found by Daniel Allcock. It relies on no more sophisticated mathematics than the fact the polynomial ring $k[x]$ in one variable is a PID. Allcock establishes the following assertion, which obviously implies version III of the Weak Nullstellensatz (Theorem 1.4):

Lemma 1.1 *If $k \subseteq K$ is a finitely generated extension of fields which is not finite, and $a_1, \ldots, a_r$ are elements in K, then $k[a_1, \ldots, a_r]$ is not equal to K.*

PROOF: To begin with we treat the case that K is of transcendence degree one over k. Then there is a subfield $k(x) \subseteq K$ with x transcendental over which K is finite. Let $\{e_i\}$ be a basis for K over $k(x)$ with $e_0 = 1$ and let c_{ijk} be elements in $k(x)$ such that $e_i e_j = \sum_k c_{ijk} e_k$. Let s be the common denominator of the c_{ijk}. Then $A = \bigoplus_i k[x]_s e_i$ is a subalgebra of K free over $k[x]_s$. Now let $a_1, \ldots, a_r$ be elements in K, and express them in the basis $\{e_i\}$; that is, write $a_j = \sum d_{ij} e_i$ with $d_{ij} \in k(x)$. Let t be the common denominator of the d_{ij}'s.

Recall that $k[x]_s$ denotes the localization of $k[x]$ in the multiplicative set $\{1, s, s^2, \ldots\}$. Elements are of the form a/s^r with $a \in k[x]$.

Then $k[a_1, \ldots, a_r]$ is contained in A_t, and therefore can not be equal to K. Indeed, if $u \in k[x]$ is any irreducible element[5] neither being a factor in s nor in t, then u^{-1} will not lie in A_t.

[5] Even if k is a finite field, there are infinitely many irreducible polynomials in $k[x]$, see problem 1.12 on page 12.

Finally, if the transcendence degree of K is more than one, we let $k' \subseteq K$ be a field containing k over which K is of transcendence degree 1. Then K is never equal to $k'[a_1, \ldots, a_r]$, hence *a fortiori* neither to $k[a_1, \ldots, a_r]$. ❑

Figures and intuition

To have some geometric intuition one frequently have real pictures of algebraic sets in mind. Then the ground field must be $\mathbb{C}$ and the algebraic set must be defined by real equations. The object depicted is the subset of the points in $Z(\mathfrak{a})$ whose coordinates are real numbers.

These real pictures can be very instructive (and beautiful) and some times they are unsurpassed to explain what happens. But they can be deceptive and must be taken with a rather large grain of salt—often they do not tell the whole story, and sometimes they do not say any thing at all. For instance, $x^2 + y^2 + 1$ has no real zeros, so $V(x^2 + y^2 + 1)$ has no real points, but of course, complex zeros abound.

Performing complex coordinate shifts, which is perfectly legitimate when working over $\mathbb{C}$ and does not alter the complex geometric reality, can completely change the real picture. For instance, replacing y by iy in the above example, which is a simple scaling of one of the coordinates; gives the equation $x^2 - y^2 = -1$ whose real points constitute a hyperbola, and scaling both x and y by i gives the circle $x^2 + y^2 = 1$. So the real picture depends heavily on the coordinates one uses.

There is also a shift in dimension. The affine plane $\mathbb{A}^2(\mathbb{C})$ is as real manifold equal to $\mathbb{R}^4$, and a plane in $\mathbb{A}^2(\mathbb{C})$ is a linear subspace of real codimension two; that is, an $\mathbb{R}^2$ in $\mathbb{R}^4$. Complex algebraic sets will be of even (real) dimension and the (real) dimension of their real counterparts will be half that dimension.

Consider the curve $y^2 = x(x + a)(x - b)$ in $\mathbb{A}^3(\mathbb{C})$; with a and b both positive. The real points, depicted in Figure 6, has two components. One compact, which is homeomorphic to a circle, and one unbounded. The complex points turn out to form a space homeomorphic to a torus $\mathbb{S}^1 \times \mathbb{S}^1$ (in the topology induced from the standard topology on $\mathbb{C}^2$). Well, to be precise, it is homeomorphic to the torus minus one point.

To underline to what extent the real picture depends on the coordinate system, in figure 7 we depicted a cubic curve (almost the same as in Figure 6) viewed in another coordinate system.

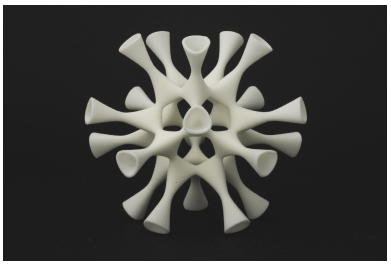


Figure 5: The famous surface of degree six constructed by Wolf Barth. It has 65 double points. The picture is of a 3D-print of the surface from http://math-sculpture.com.

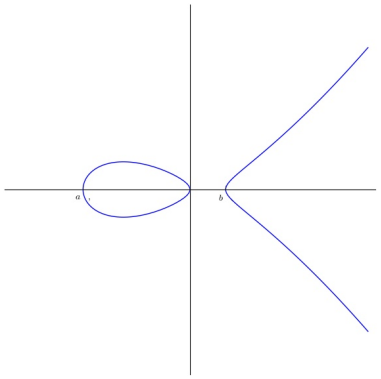


Figure 6: The real points of a cubic curve in the so called Weierstrass normal form.

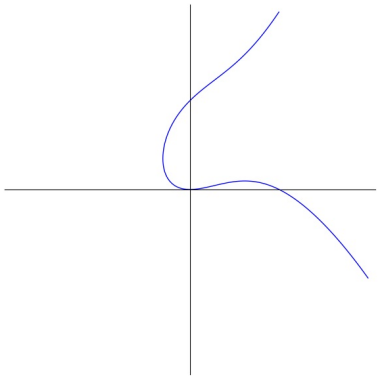


Figure 7: The real points of a cubic curve in the so called Tate normal form.

A second proof of the Nullstellensatz

It is worth while to ponder over another proof of the Nullstellensatz which follows a completely different path than the one of Daniel Allcock. We shall present it in a simplified form assuming that $k = \mathbb{C}$ and that $\mathfrak{a}$ is a *prime ideal*. The point is that the transcendence degree of $\mathbb{C}$ over $\mathbb{Q}$ is infinite (in fact it equals the cardinality $\mathfrak{c}$ of the continuum). It is not difficult to see that it is infinite; if not, $\mathbb{C}$ would

have been countable (it is more challenging to see it equals $\mathfrak{c}$). This implies:

Lemma 1.2 *Every field K of finite transcendence degree over $\mathbb{Q}$ can be embedded in $\mathbb{C}$.*

PROOF: Let $x_1, \ldots, x_r$ be a transcendence basis for K over $\mathbb{Q}$ so that K is algebraic over $\mathbb{Q}(x_1, \ldots, x_r)$. Chose algebraically independent complex numbers $z_1, \ldots, z_r$. Sending x_i to z_i gives an embedding of $\mathbb{Q}(x_1, \ldots, x_r)$ into $\mathbb{C}$ and because $\mathbb{C}$ is algebraically closed, it extends to K. ❑

Assume now that $\mathfrak{p}$ is a prime ideal in $\mathbb{C}[x_1, \ldots, x_n]$ and choose generators $f_1, \ldots, f_r$ for it. Let k be the field obtained by adjoining all the coefficients of the f_i's to $\mathbb{Q}$; it is clearly of finite transcendence degree over $\mathbb{Q}$. Let $\mathfrak{p}' = \mathfrak{p} \cap k[x_1, \ldots, x_n]$. Then the fraction field of the domain $k[x_1, \ldots, x_n]/\mathfrak{p}'$ is of finite transcendence degree over $\mathbb{Q}$ and therefore it embeds into $\mathbb{C}$. But this means that the images of the x_i's are coordinates for a point where all the f_i's vanish, and consequently $Z(\mathfrak{p})$ is not empty.

PROBLEM 1.2 Contrary to quadratic curves, show that a cubic curve in $\mathbb{A}^2(\mathbb{C})$ defined by an equation with real coefficients always have real points. Generalize to curves with real equations of odd degree. HINT: Intersect with real lines. ★

Examples

1.4 — QUADRATIC CURVES Curves in $\mathbb{A}^2$ given by irreducible quadratic equations can be classified. Up to an affine change of coordinates there are only two types. Either the equation can be brought on the form $y = x^2$ or on form $xy = 1$.

The quadratic polynomial can be written as $Q(x, y) + L(x, y) + c$ where Q and L are homogeneous polynomials of degree respectively two and one, and where c is a scalar. The quadratic form Q can be factored as the product of two linear form. We change coordinates so that the two factors become x and y; that is, $Q(x, y) = xy$, if they are different, or y if they coincide; that is, $Q(x, y) = y^2$. This brings the original quadratic polynomial on form

$$xy + ax + by + c = (x + a)(y + b) + c - ab$$

if $Q(x, y) = xy$, and

$$y^2 + ax + by + c$$

when $Q(x, y) = y^2$. The last necessary coordinate shifts are then easy to find and left as an exercise.

The following super-trivial lemma is nothing but Taylor expansion to the first order, but is now and then useful:

LittleLemma

Lemma 1.3 *Assume that R is any commutative ring. Let $P(z)$ be a polynomial in $R[z]$. Then $P(z+w) = P(z) + wQ(z,w)$ for some polynomial Q in $R[z,w]$.*

PROOF: Observe that by the binomial theorem one has $(z+w)^i = z^i + wQ_i(z,w)$; the rest of the proof follows from this. ❑

1.5 — THE AFFINE TWISTED CUBIC In this example we take a closer look at a famous curve called the *twisted cubic*, or rather an *affine* version of it (there is also a *projective* avatar of the curve which we come back to later). The word twisted in the name comes from that fact that the curve is a space curve and not contained in any plane.

The twisted cubic $C \subseteq \mathbb{A}^3$ is the image of the map $\phi\colon \mathbb{A}^1 \to \mathbb{A}^3$ given as $\phi(t) = (t, t^2, t^3)$. It is a closed algebraic set; indeed, we shall see that $C = Z(\mathfrak{a})$ where $\mathfrak{a}$ is the ideal

$$\mathfrak{a} = (z - x^3, y - x^2).$$

The inclusion $C \subseteq Z(\mathfrak{a})$ follows readily, and for the other inclusion, we observe that points in $Z(\mathfrak{a})$ are shaped like (x, x^2, x^3) so we can just take $t = x$. Moreover, it holds true that $I(X) = \mathfrak{a}$. To see this, notice that any polynomial f can be represented as

$$f(x,y,z) = f(x, x^2, x^3) + h(x,y,z),$$

where $h \in \mathfrak{a}$. This is just a repeated application of the little lemma (lemma 1.3) above; first with $y = x^2 - (x^2 - y)$ and then with $z = x^3 - (x^3 - z)$. That $f(x,y,z)$ vanishes on C means that $f(x, x^2, x^3)$ vanishes identically and hence $f \in \mathfrak{a}$.

As a by product of this reasoning, we obtain that the ideal $\mathfrak{a}$ is a prime ideal; indeed, it is the kernel of the restriction map

$$k[x,y,z] \to k[t]$$

that sends a polynomial to its restriction to C; in other words, x goes to t, y to t^2 and z to t^3.

☆

Problems

1.3 Let $f \in k[x_1, \ldots, x_n]$. Show that the ideal (f) is radical if and only if no factor of f is multiple.

For any two ideals $\mathfrak{a}$ and $\mathfrak{b}$ in a ring A recall that one denotes by $(\mathfrak{a} : \mathfrak{b})$ the ideal of those $a \in A$ such that $a \cdot \mathfrak{b} \subseteq \mathfrak{a}$; that is $(\mathfrak{a} : \mathfrak{b}) = \{\, a \in A \mid a \cdot \mathfrak{b} \subseteq \mathfrak{a} \,\}$.

1.4 Assume that the characteristic of k is zero. Let $f(x)$ be a polynomial in $k[x]$. Show that the relation $\sqrt{(f)} = (f : f')$ holds (where f' is the derivative of f; see exercise 1.13). Give a counterexample if k is of positive characteristic.

RadPoly

1.5 Let $\mathfrak{p}$ be a prime ideal in $k[x_1, \ldots, x_n]$. Show that $\mathfrak{p}$ is the intersection of all the maximal ideals containing it; that is, $\mathfrak{p} = \bigcap_{\mathfrak{p} \subseteq \mathfrak{m}} \mathfrak{m}$ HINT: Show that $I(Z(\mathfrak{p})) = \bigcap_{\mathfrak{p} \subseteq \mathfrak{m}} \mathfrak{m}$, then use the Nullstellensatz.

1.6 Consider the closed algebraic set in $\mathbb{A}^2$ given by the vanishing of the polynomial $P(x) = y^2 - x(x+1)(x-1)$. Let $\alpha \in \mathbb{C}$ and let $\mathfrak{a} = (x - \alpha, P(x))$. Determine $Z(\mathfrak{a})$ for all α. For which α's is $\mathfrak{a}$ a radical ideal?

1.7 With the same notation as in the previous problem. Let $\mathfrak{b}$ be the ideal $\mathfrak{b} = (y - \alpha, P(x))$. Determine $Z(\mathfrak{b})$ for all α and decide for which α the ideal $\mathfrak{b}$ is radical. HINT: The answer depends on the characteristic of k, characteristic three being special.

SnittKubikk

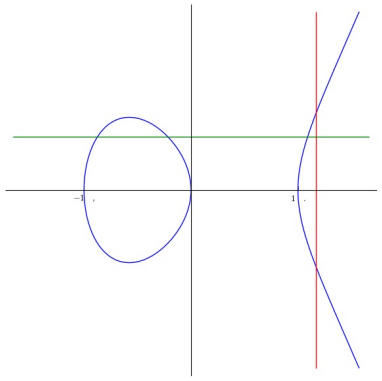


Figure 8: A cubic and two lines.

1.8 Let $F_1, \ldots, F_r$ be homogenous polynomials in $k[x_1, \ldots, x_n]$ and let $X = Z(F_1, \ldots, F_r)$ be the closed algebraic subset they define. Show that X is a *cone* with apex at the origin; that is, show that if x is a point in X, the line joining x to the origin lies entirely in X. HINT: Show that $t \cdot x$ lies in X for all $t \in k$.

1.9 Assume that X is a cone in $\mathbb{A}^n$ with apex at the origin, and assume that f is a polynomial that vanishes on X. Show that also all the homogenous components of f vanish along X.

1.10 Let $\mathbb{M}_{n,m}$ be the space of $n \times m$-matrices with coefficients from k. It can be identified with the affine space $\mathbb{A}^{nm}$ with coordinates x_{ij} where $1 \leq i \leq n$ and $1 \leq j \leq m$. Let r be a natural number less than both n and m, and let W_r be the set of $n \times m$-matrices of rank at most r. Show that W_r is a closed algebraic subset. Show that all the W_r's are cones over the origin. HINT: Determinants are polynomials.

1.11 Let $C_n \subseteq \mathbb{A}^n$ be the curve with parameter representation $\phi(t) = (t, t^2, \ldots, t^n)$, and let $\mathfrak{a}$ be the ideal $\mathfrak{a} = (x_i - x_1 x_{i-1} \mid 2 \leq i \leq n)$. Show that C_n is a closed algebraic set, that $I(C_n) = \mathfrak{a}$ and that $\mathfrak{a}$ is a prime ideal. The curves C_n are called *affine normal rational* curves and they are close relatives to the twisted cubic. For $n = 2$ we have a parabola in the plane and for $n = 3$ we get back the twisted cubic.

Affine normal rational curves

1.12 As usual $\mathbb{F}_p$ is the finite field with p elements. The aim of this exercise is to establish that there are infinitely many irreducible polynomials with coefficients in $\mathbb{F}_p$. If you are interested, there is a nice introduction to finite fields in Irelands and Rosen's book[6].

UendMangelrr

[6]

Let N_d be the number of irreducible, monic polynomials over $\mathbb{F}_p$ of degree d, and let F_d denote their product. Show that $x^{p^n} - x = \prod_{d|n} F_d(x)$ and that $p^n = \sum_{d|n} dN_d$. Conclude that there are infinitely many irreducible polynomials over $\mathbb{F}_p$. (If you know about Möbius inversion, show that $nN_d = \sum_{d|n} \mu(n/d)p^d$.)

1.13 *(The formal derivative)* Let $f(x) = \sum_i a_i x^i$ be a polynomial. Define the (formal) derivative of f to be $f'(x) = \sum_i i a_i x^{i-1}$. Show that the usual rules are still valid; *i.e.,* derivation is a linear operation and Leibnitz's product rule holds true. Show that f' vanishes identically if and only if either f is constant or the characteristic of k is p and $f(x) = g(x^p)$ for some polynomial $g(x)$. FormalDer

Geir Ellingsrud—25th January 2018