ALGEBRAIC GEOMETRY 1, WINTER TERM 2025/26. LECTURE NOTES.

ULRICH GÖRTZ

1. Introduction

Oct. 14, 2025

We will start with a relatively long *introductory chapter*, in order to …

- provide some motivation for the (partly more technical) content that will come later,
- give those participants who were not in the Algebra 2 class last term a little more time to brush up their commutative algebra knowledge:
  - (Prime) ideals, quotients
  - localization (with respect to a multiplicative subset; in particular with respect to one element and localization at a prime ideal),
  - spectrum of a ring, Zariski topology (this we will redo in the class, but ideally you are already a little familiar with the notion of *topological space*.

I will try to address the question *What is algebraic geometry?*, and at the same time give, towards the end of the chapter, a rough survey of this class.

(1.1) What Algebraic Geometry is about.

In one sentence: Study "geometric properties" of solution sets of systems of polynomial equations (over a field, or more generally a commutative ring).

Example 1.1.

$$\{(x, y) \in \mathbb{R}^2 \mid y^2 = x^2(x+1)\} \quad \subset \mathbb{R}^2.$$

Comparison with Previous/Other Courses

Linear Algebra	Systems of *linear* equations
Algebra	polynomial equations (1 variable, 1 polynomial)
Algebraic Geometry	systems of polynomial equations
Algebraic Number Theory	…coefficients/solutions in $\mathbb{Z}, \mathbb{Q}, K/\mathbb{Q}$ fin., $\mathbb{F}_q$

Here *algebraic* refers to the fact that we

- study solution sets (zero sets) of polynomials (not power series, differential/holomorphic functions, etc.),

Date: November 2, 2025.

- use algebraic methods (specifically commutative algebra) to study these objects.

In particular, at least in principle, we may hence work over an arbitrary field (not only $\mathbb{R}$ or $\mathbb{C}$).

(1.2) The Cayley–Hamilton Theorem: A Geometric View.

Theorem 1.2. [Cayley–Hamilton] *Let k be a field, $A \in M_n(k)$. Then* $\mathrm{charpol}_A(A) = 0$.

We want to look at this result from the perspective of an algebraic geometer, i.e., we view $M_n(k)$ as n-dimensional (vector) space.

Let us consider the case $k = \mathbb{R}$, $n = 2$ and restrict to matrices A with trace $\mathrm{tr}(A) = 0$. (This does not change the main argument, but simplifies the discussion a little bit and will allow us to draw a picture later.)

We want to use that the theorem is obviously true, if A is a diagonal matrix. From this, it follows easily that the theorem holds whenever A is diagonalizable. In fact, if $A = SDS^{-1}$ for a diagonal matrix D, then $\mathrm{charpol}_A = \mathrm{charpol}_D$. Since conjugation is a ring automorphism of the ring of matrices (over any ring), we may "pull it out" of any polynomial. Together we obtain

$$\mathrm{charpol}_A(A) = \mathrm{charpol}_D(SAS^{-1}) = S\,\mathrm{charpol}_D(D)S^{-1},$$

and the term on the right vanishes, since $\mathrm{charpol}_D(D) = 0$ by the case of diagonal matrices. Furthermore, in this argument we may just as well allow matrices S with entries in some extension field of k, and we see that it suffices to assume that A is *diagonalizable over* $\mathbb{C}$. But of course, there are also non-diagonalizable matrices.

So we consider a matrix

$$A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix} \in M_2(\mathbb{R})^{\mathrm{tr}=0} \cong \mathbb{R}^3,$$

where we use a, b, c as coordinates on $\mathbb{R}^3$. We then have

$$\mathrm{charpol}_A = (T - a)(T + a) - bc = T^2 - (a^2 + bc).$$

In particular we see that all matrices $A = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ with $a^2 + bc \neq 0$ are diagonalizable over $\mathbb{C}$. On the other hand, if $a^2 + bc = 0$, then A is not necessarily diagonalizable.

We now consider the map:

$$\chi : M_2(\mathbb{R})^{\mathrm{tr}=0} \to M_2(\mathbb{R}), \quad A \mapsto \mathrm{charpol}_A\,.$$

Our goal is to show that the map χ is constant with image the zero matrix. By what we have said, $\chi(A) = 0$ for all those A that are diagonalizable over $\mathbb{C}$.

Since the map $\chi\colon \mathbb{R}^3 \to \mathbb{R}^4$ is given by polynomials, it is continuous. Therefore for every closed subset of $\mathbb{R}^4$, its inverse image under χ is again closed. We apply this to the set $\{0\}$ containing only the zero matrix; clearly this is a closed set. Its inverse image contains, by what we know already, all those traceless matrices that are diagonalizable over $\mathbb{C}$, and in particular all matrices $\begin{pmatrix} a & b \\ c & -a \end{pmatrix}$ with $a^2 + bc \neq 0$. But this set is dense in $M_2(\mathbb{R})^{\mathrm{tr}=0}$, i.e., its closure is the whole space. It follows that $\chi^{-1}(\{0\}) = M_2(\mathbb{R})^{\mathrm{tr}=0}$, as we wanted to show.

The same argument, with small modifications, applies when we drop the condition on the trace, and also for square matrices of arbitrary size.

Question: How to deal with other fields?
For this, we need a *notion of continuous map* in a more general context.

(1.3) The Zariski topology on k^n.

Let k be a field. Since we want to study solution sets of systems of polynomial equations, we introduce the following notation:

Definition 1.3.

(1) *Given $f_1, \dots, f_m \in k[T_1, \dots, T_n]$, we define the* vanishing set *(in German:* Verschwindungsmenge*)*

$$V(f_1, \dots, f_m) := \{(t_i) \in k^n;\ f_j(t_1, \dots, t_n) = 0\ \forall j\}.$$

(2) *More generally, for any subset $\mathcal{F} \subset k[T_1, \dots, T_n]$, we define the* vanishing set *of $\mathcal{F}$ as*

$$V(\mathcal{F}) = \{(t_i) \in k^n;\ f(t_1, \dots, t_n) = 0\ \forall f \in \mathcal{F}\}.$$

If k'/k is a field extension, then we set

$$V(f_1, \dots, f_m)(k') := \{(t_i) \in (k')^n;\ f_j(t_i) = 0\ \forall j\},$$

and analogously define $V(\mathcal{F})(k')$.

Remark 1.4. Let $\mathcal{F} \subset k[T_1, \dots, T_n]$, and let $\mathfrak{a} \subset k[T_\bullet]$ be the ideal generated by $\mathcal{F}$. Then $V(\mathcal{F}) = V(\mathfrak{a})$, as is easily checked. From this it also follows that

$$V(\mathcal{F}) = V(\mathfrak{a}) = V(f_1, \dots, f_m),$$

whenever $f_1, \dots, f_m$ is a generating system for the ideal $\mathfrak{a}$. By Hilbert's Basis Theorem, every ideal in $k[T_1, \dots, T_n]$ admits a finite generating system. (We say that the polynomial ring in finitely many variables over a field, or more generally over any noetherian ring, is noetherian.) Therefore, every vanishing set $V(F)$ can be written in the form $V(f_1, \dots, f_m)$ for finitely many, suitably chosen polynomials f_j.

Proposition 1.5. *The sets $V(\mathcal{F})$, $\mathcal{F} \subset k[T_\bullet]$, form the closed sets of a topology on k^n, the* Zariski topology*.*

Spelled out explicitly, this means that
(1) $\emptyset$, k^n *are of this form,*
(2) *finite unions of such sets are again of this form,*
(3) *arbitrary intersections of such sets are of this form.*

Proof. (1) We have $\emptyset = V(1)$, $k^n = V(0)$.

(2) By induction, it is enough to consider the union of two closed subsets, say $V(\mathcal{F})$ and $V(\mathcal{G})$. But

$$V(\mathcal{F}) \cup V(\mathcal{G}) = V(fg;\ f \in \mathcal{F},\ g \in \mathcal{G}).$$

In fact, the inclusion $\subseteq$ is clear. For the other inclusion, take a point t in the right hand side which does not lie in $V(\mathcal{F})$. That means $f(t) \neq 0$ for some $f \in \mathcal{F}$. But since $f(t)g(t) = (fg)(t) = 0$ for all $g \in \mathcal{G}$, it follows, that $t \in V(\mathcal{G})$.

(3) For $\mathcal{F}_j \subseteq k[T_1, \ldots, T_n]$, $j \in J$, we have

$$\bigcap_{j \in J} V(\mathcal{F}_j) = V\left(\bigcup_{j \in J} \mathcal{F}_j\right).$$

□

Definition 1.6. *The topological space k^n with the Zariski topology is denoted by $\mathbb{A}^n(k)$ and called* affine space (over k, of dimension n).

(1.4) Bézout's Theorem.

Oct. 15, 2025

Next, let us look at *Bézout's theorem*, a relatively elementary, but still non-trivial result in algebraic geometry which at the same time illustrates a typical type of question asked in this theory and several methods that are crucial in (almost) all of algebraic geometry. In particular, it will serve as a motivation for introducing the so-called *projective space*, see Section (1.5).

Let k be a field. For a polynomial $f \in k[X, Y]$, as before we write

$$V(f) = \left\{(x, y) \in k^2;\ f(x, y) = 0\right\},$$

and call this set the *vanishing set of f*.

We want to study what we can say, given two such polynomials f, g, about the set $V(f) \cap V(g)$. More specifically, examples show that typically, this is a finite set, and it is a natural question whether we can determine its cardinality. We start with the following observations:

(1) For a polynomial $p \in k[X]$, $n = \deg(p) > 0$, we have

$$\#\{x \in k;\ p(x) = 0\} \leq n,$$

with equality if k is algebraically closed and if we count each zero x of p with its multiplicity $\operatorname{ord}_x(p) = \max\{r;\ (X - x)^r \mid p\}$.

(2) Let $p \in k[X]$ non-constant and let $f = Y - p(X)$, $g = Y$. We then have a bijection

$$\{x \in k;\ p(x) = 0\} \longleftrightarrow V(f) \cap V(g), \quad x \mapsto (x, 0).$$

Coming back to the general case, let $f, g \in k[X, Y]$. Recall that $k[X, Y]$ is a unique factorization domain. It is easy to see that in case f and g have a common divisor of positive degree, then $V(f) \cap V(g)$ is infinite, at least when k is algebraically closed. Since here we are interested in counting points, we rule out that case, and require that f, g are coprime. For a polynomial $f \in k[X, Y]$, we denote by $\deg(f)$ its *total degree*, i.e., for $f = \sum_{i,j} a_{ij} X^i Y^j$, $\deg(f) = \max\{i + j;\ a_{ij} \neq 0\}$.

Proposition 1.7. *Let k be a field, and let $f, g \in k[X, Y]$ be coprime, non-constant polynomials. Then*

$$\#(V(f) \cap V(g)) \leq \deg(f) \cdot \deg(g).$$

We will prove this result later, in an improved form. For now, our goal is to discuss this "improved form", by which we mean a refined statement where we actually have equality.

Looking back at the case of a single-variable polynomial p above, it is reasonable to require that k is algebraically closed, and also to expect that we will have to count intersection points with their correct "multiplicity". It is not so hard to write down the definition of multiplicity that will work; we will discuss this in more detail later.

Definition 1.8. [Local intersection multiplicity] *Let k be a field, $f, g \in k[X, Y]$, $P = (x, y) \in k^2$ a point. Let $\mathfrak{m} = (X - x, Y - y) \subset k[X, Y]$ (a maximal ideal of the polynomial ring). Then we define*

$$i_P(f, g) = \dim_k k[X, Y]_{\mathfrak{m}}/(f, g),$$

where $k[X, Y]_{\mathfrak{m}}$ denotes the localization at $\mathfrak{m}$ (i.e., the localization with respect to the multiplicative subset $k[X, Y] \setminus \mathfrak{m}$). (Note that the intersection multiplicity depends on the polynomials f, g; not just on their vanishing sets.)

However, looking at the case where $V(f)$ and $V(g)$ are parallel lines in k^2 (e.g., $f = Y$, $g = Y - 1$), we see that these changes are not enough in order to obtain equality.

(1.5) The projective plane $\mathbb{P}^2(k)$.

Idea. Add points to k^2 so that any two different lines intersect in a point. (While this at first may feel like cheating, it turns out that the resulting construction is extremely useful in algebraic geometry, far beyond Bézout's theorem, also in the sense that it will allow to come back and answer questions that do not mention the newly constructed space.) Setting up the theory

will also involve suitably modifying the notion of line; we will come to that later, and then also relate it to lines in k^2.

Definition 1.9. *Let k be a field. We define the* projective plane $\mathbb{P}^2(k)$ *over k, as a set, as*

$$\mathbb{P}^2(k) := \{L \subset k^3 \text{ linear subspace of dimension } 1\},$$

the set of all lines through the origin in k^3.

Viewing k^2 as the affine plane $\{(x, y, 1) \in k^3;\ x, y \in k\}$ in k^3, every line through the origin in k^3 which is not contained in the x-y-plane intersects k^2 in exactly one point. Thus we obtain an injective map $k^2 \to \mathbb{P}^2(k)$ which we may also write as

$$k^2 \longrightarrow \mathbb{P}^2(k), \quad (x, y) \mapsto \left\langle \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} \right\rangle.$$

In this way, we may view $\mathbb{P}^2(k)$ as "k^2 with some points added", namely the lines in the x-y-plane (note that thus for any equivalence class of parallel lines in k^2 we have one additional point, and it will turn out that this point "is" (in a sense that we yet must define) the missing intersection point of these parallel lines).

Usually we denote elements of $\mathbb{P}^2(k)$ in terms of their *homogeneous coordinates* which we are going to define next. (That also facilitates, hopefully, to think of elements of $\mathbb{P}^2(k)$, typically, as *points of some space* rather than as lines in some other space, similarly as we think of the elements of k^2 as points in the plane.)

For $(x, y, z), (x', y', z') \in k^3 \setminus \{0\}$, define:

$$(x, y, z) \sim (x', y', z') \iff \left\langle \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} \right\rangle$$

$$\iff \exists \lambda \in k^\times : (x', y', z') = \lambda(x, y, z).$$

This is an equivalence relation on $k^3 \setminus \{0\}$. We denote by $(x : y : z)$ the equivalence class of (x, y, z) and obtain a bijection

$$(k^3 \setminus \{0\})/\sim \quad \xrightarrow{1:1} \quad \mathbb{P}^2(k), \qquad (x : y : z) \mapsto \left\langle \begin{pmatrix} x \\ y \\ z \end{pmatrix} \right\rangle.$$

Our next task is to define a suitable notion of *line in the projective plane*. The resulting notion should satisfy (at least) the properties that through any two distinct points, there is a unique line; and that any two distinct lines intersect in a unique point (because our goal was a situation where there are no more "parallel lines"). For the definition, however, a general construction is better suited, namely an analog of the notion of vanishing set of polynomials. However, we have to be careful here, because for an

arbitrary polynomial $F \in k[X,Y,Z]$ the value on a point $(x:y:z)$ given in homogeneous coordinates is obviously not well-defined, but will depend on the choice of representative. On the other hand, in order to define vanishing sets, we do not need to compute values, but only need to check whether the outcome is $= 0$ or $\neq 0$. Even this is not possible for general polynomials, but it is possible for the class of *homogeneous* polynomials, which is still large enough to give all that we need. We give the definition in a general form.

Definition 1.10. *Let R be a ring. A polynomial $F \in R[X_0,\dots,X_n]$ is called* homogeneous of degree d*, if it can be written as a (finite) linear combination of monomials of degree d, i.e., in the form*

$$F = \sum_{i_0,\dots,i_n} a_{i_0,\dots,i_n} X_0^{i_0} \cdots X_n^{i_n}$$

with $a_{i_0,\dots,i_n} \in R$ and $a_{i_0,\dots,i_n} = 0$ whenever $i_0 + \cdots + i_n \neq d$.

Lemma 1.11. *Let R be a ring, and let $F \in R[X_0,\dots,X_n]$ be homogeneous of degree d. Then for all $\lambda, x_0,\dots,x_n \in R$, we have*

$$F(\lambda x_0,\dots,\lambda x_n) = \lambda^d F(x_0,\dots,x_n).$$

If R is an infinite field, then the converse is true, as well.

Proof. The first statement is clear. The second one follows (how?) from the fact that over an infinite field, the zero polynomial is the only polynomial in $n+2$ variables which vanishes at every point of k^{n+2}. □

Therefore we may define the vanishing set of a homogeneous polynomial, and more generally, the common vanishing set of a family of homogeneous polynomials (possibly of different degrees). We will look at several explicit examples soon.

Definition 1.12. *Let $\mathcal{F} \subseteq k[X,Y,Z]$ be a set of homogeneous polynomials. We define the* vanishing set *as*

$$V_+(\mathcal{F}) = \{(x:y:z);\ F(x,y,z) = 0 \text{ for all } F \in \mathcal{F}\} \quad \subseteq \mathbb{P}^2(k).$$

Similarly as for k^n, one proves the following. Oct. 21, 2025

Proposition 1.13. *The sets of the form $V_+(\mathcal{F})$, $\mathcal{F} \subseteq k[X,Y,Z]$ a set of homogeneous polynomials, form the closed sets of a topology on $\mathbb{P}^2(k)$, the so-called* Zariski topology*.*

Lines in $\mathbb{P}^2(k)$. We can now define the notion of line in the projective plane and conclude this section by stating the final form of Bézout't theorem.

Definition 1.14. *Let k be a field. A* line *in $\mathbb{P}^2(k)$ is a subset of the form $V_+(F)$ for a non-zero homogeneous polynomial of degree* 1*.*

Explicitly, F as in the definition has the form $aX+bY+cZ$, with $(a,b,c) \neq (0,0,0)$. For example $V_+(Z) = \mathbb{P}^2(k) \setminus \iota(k^2)$ (where $\iota\colon k^2 \to \mathbb{P}^2(k)$ is the

embedding defined above) is a line. This line is called the *line at infinity* (with respect to our chosen embedding $k^2 \subset \mathbb{P}^2(k)$).

Proposition 1.15.
(1) *Let $P_1, P_2 \in \mathbb{P}^2(k)$, $P_1 \neq P_2$. Then there exists $F \in k[X,Y,Z]$ homogeneous of degree 1, $F \neq 0$, such that $P_1, P_2 \in V_+(F)$, and F is uniquely determined up to multiplication by an element $\lambda \in k^\times$.*
(2) *For non-zero linear homogeneous polynomials $F_1, F_2 \in k[X,Y,Z]$, we have*

$$V_+(F_1) = V_+(F_2) \quad \Longleftrightarrow \quad \text{there exists } \lambda \in k^\times : F_2 = \lambda F_1.$$

(3) *Let $F_1, F_2 \in k[X,Y,Z]$ be non-zero linear homogeneous polynomials with $V_+(F_1) \neq V_+(F_2)$. Then the set $V_+(F_1) \cap V_+(F_2)$ consists of exactly one element.*

Proof. (1) Phrase the problem as a system of linear equations on the coefficients of F. We obtain a system with two linearly independent equations and three variables, so the space of solutions is 1-dimensional.

(2) This follows from Part (1) (because any $V_+(F_1)$ contains at least 2 points (more precisely: $\#k + 1$ points)).

(3) Similarly as Part (1) this can be shown by considering a suitable system of linear equations, where the coefficients are given by the coefficients of the equations of F_1 and F_2, and the variables correspond to the homogeneous coordinates of the point(s) we are looking for in the intersection. □

We can now state the final version of Bézout's theorem. Here, $i_P(F,G)$ is defined similarly as above. (As before, it depends on the actual polynomials F, G, not just on their vanishing sets.) We will come back to this, and also give a proof of the theorem, later in the course.

Theorem 1.16. [Bézout] *Let $F, G \in k[X,Y,Z]$ be non-constant coprime homogeneous polynomials. Then*

$$\sum_{P \in V_+(F) \cap V_+(G)} i_P(F,G) = \deg(F) \cdot \deg(G),$$

in particular $\#(V_+(F) \cap V_+(G)) \leq \deg(F) \cdot \deg(G)$.

Similarly to the projective plane, we can analogously define *projective space of dimension n over k*,

$$\mathbb{P}^n(k) = (k^{n+1} \setminus \{0\}) / \sim,$$

where $(x_0, \ldots, x_n) \sim (x_0', \ldots, x_n')$ if there exists $\lambda \in k^\times$ such that $x_i' = \lambda x_i$ for all i.

(1.6) Homogenization and dehomogenization of polynomials.

Let us look at the relationship between vanishing sets in k^2 and in $\mathbb{P}^2(k)$.

Remark 1.17. Let $F \in k[X,Y,Z]$ be a homogeneous polynomial. Then $V_+(F) \cap V_+(Z) = V_+(F,Z)$ and thus we can write $V_+(F)$ as the disjoint union

$$V_+(F) = (V_+(F) \cap \iota(k^2)) \sqcup V_+(F,Z).$$

Furthermore, under the identification $k^2 \xrightarrow{1:1} \iota(k^2)$, $V_+(F) \cap \iota(k^2)$ is in bijection with $V(f)$ for $f = F(x,y,1) \in k[x,y]$. Here f is a polynomial of degree $\leq \deg(F)$, with equality, if F is not divisible by Z.

Conversely, given a polynomial $f \in k[x,y]$ we can easily find a homogeneous polynomial such that $f(x,y) = F(X,Y,1)$ (and hence, by the above remark, $V(f) = V_+(F) \cap \iota(k^2)$, or in other words, $V_+(F)$ consists of $V(f)$ and (possibly) further points lying on the line at infinity $V_+(Z)$).

Namely, we just "fill in powers of Z" so as to construct a homogeneous polynomial of degree $\deg(f)$. For example, for $f = y^2 - x^3 + x + 1$, we would take $F = Y^2Z - X^3 + XZ^2 + Z^3$. Generally, given $f = \sum_{i,j} a_{i,j} x^i y^j$ of degree d, take $F = \sum_{i,j} a_{i,j} X^i Y^j Z^{d-i-j}$. We call F the dehomogenization (of degree d) of f.

Note that for f and F related in this way, the polynomial $G = Z \cdot F$ still has the property that $G(x,y,1) = f(x,y)$, however $V_+(G) = V_+(F) \cup V_+(Z)$, i.e., we get an "unnecessary" (and unwanted) copy of the line at infinity.

(1.7) More examples.

Let k be a field, $\mathrm{char}(k) \neq 2$. A vanishing set $V(f) \subset \mathbb{A}^2(k)$ for a polynomial f of degree 3 is called a *cubic curve*. Oct. 22, 2025

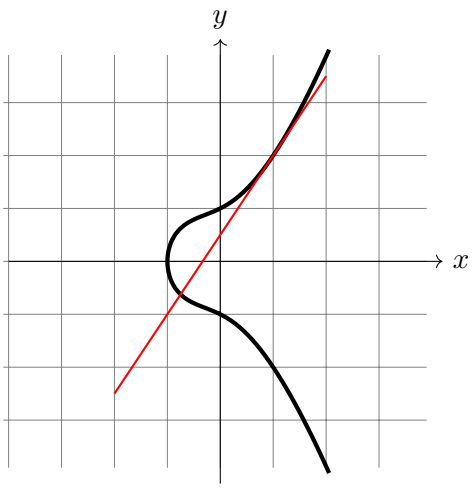
Example 1.18. Consider $C = V(f) \subset \mathbb{A}^2(k)$ with

$$f = y^2 - (x+1)(x^2+1).$$

We have

$$\frac{\partial f}{\partial x} = -3x^2 - 2x - 1, \qquad \frac{\partial f}{\partial y} = 2y.$$

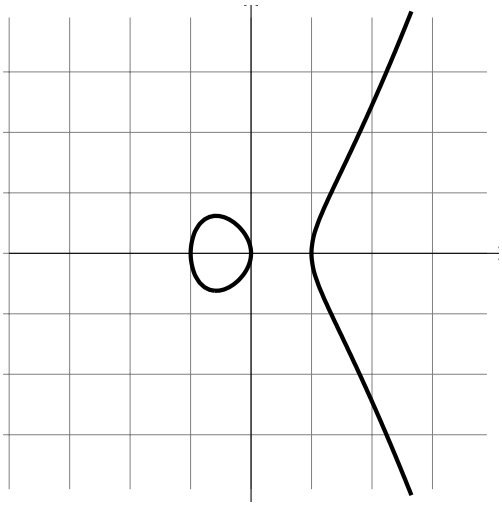
Let $P = (1, 2) \in C$. We have $\frac{\partial f}{\partial x}(P) = -6$, $\frac{\partial f}{\partial y}(P)4$. This implies that over $\mathbb{R}$ (and similarly over $\mathbb{C}$) the function $(x, y) \mapsto f(x, y)$ is approximated well by the linear function $(x, y) \mapsto -6x+4y-2$, and the zero set $V(f)$ is approximated, "in a small neighborhood of P" by the zero set of the above linear function, i.e., by the line $V(-6x + 4y - 2)$ (drawn in red).



Example 1.19.

Consider $C = V(f) \subset \mathbb{A}^2(k)$ with

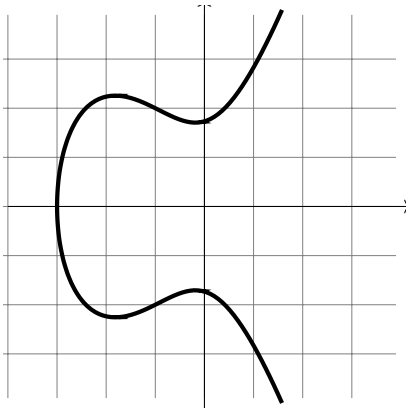
$$f = y^2 - x(x + 1)(x - 1).$$



Example 1.20.

Consider $C = V(f) \subset \mathbb{A}^2(k)$ with

$$f = y^2 - (x+3)(x^2+1).$$



Example 1.21. Consider $C = V(f) \subset \mathbb{A}^2(k)$ with

$$f = y^2 - x^2(x+1).$$

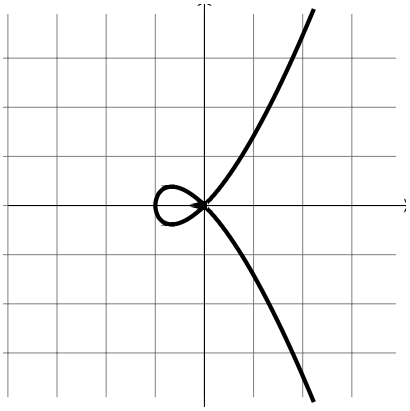
In this case,

$$\frac{\partial f}{\partial x} = -3x^2 - 2x, \quad \frac{\partial f}{\partial y} = 2y$$

and in particular

$$\frac{\partial f}{\partial x}(0,0) = \frac{\partial f}{\partial y}(0,0) = 0.$$

This corresponds to the fact that there is no well-defined tangent line to $V(f)$ at the point $(0,0)$.

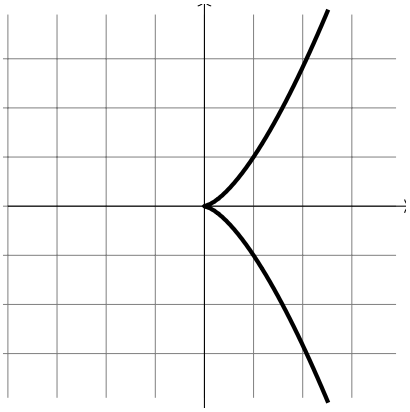


Example 1.22.

Consider $C = V(f) \subset \mathbb{A}^2(k)$ with

$$f = y^2 - x^3.$$

In this case once again both partial derivatives of f vanish at $(0,0)$.



(1.8) Singular and nonsingular points.

From the examples and the situation over the real and complex numbers, we would like to make the following definition, as one example that we can use some geometric insight, while formally "only manipulating algebraic expressions" (in this case, taking derivatives of polynomials).

Definition* 1.23. *Let k be a field and let $f \in k[X,Y]$ be a non-constant polynomial. We say that a point $P = (x_0, y_0) \in V(f)$ is* smooth *(or* non-singular*), if $\left(\frac{\partial f}{\partial X}(P), \frac{\partial f}{\partial X}(P)\right) \neq (0,0)$, and in this case call the line*

$$V\left(\frac{\partial f}{\partial X}(P) \cdot (X - x_0) + \frac{\partial f}{\partial X}(P) \cdot (Y - y_0)\right)$$

the tangent line *to $V(f)$ at P. Otherwise we call P a* singular point *of $V(f)$.*

Remark 1.24. This definition does not really make sense! (that's why I put a *) – more precisely, the property of being a smooth point *depends on the polynomial f*, not just on the subset $V(f) \subset k^2$. For example, $V(X) = V(X^2)$, and using the partial derivatives of $f = X$, all points are smooth, but using $f = X^2$ instead, all points are singular. This illustrates that the set $V(f)$ (even if we equip it with the induced topology for the embedding into k^2 with the Zariski topology) alone does not carry enough "structure" in order to really do geometry.

For now we will therefore view this as a "definition we would like to make for $V(f)$, but can currently only make after fixing f". A little later in the course we will be in a position to fix this problem.

If k is algebraically closed, then there is another option to proceed. (The fact that this is option is not viable for general fields is the reason that "classical" algebraic geometry, e.g., as in [GW1] Chapter 1 or [Ha] Chapter I, is done over an algebraically closed base field.)

To formulate this, recall that a ring R is called *reduced*, if it has no non-zero nilpotent elements, i.e., whenever $x^n = 0$ for some $x \in R$, $n \geq 1$, we must have $x = 0$. For a polynomial $f \in k[x,y]$, the quotient is reduced if and only if there does not exist an irreducible polynomial $g \in k[x,y]$ such that $g^2 \mid f$. In other words, in the decomposition of f into irreducible polynomials in the unique factorization domain $k[x,y]$ each irreducible factor occurs only once.

If $f \in k[x,y]$ is a non-constant polynomial and $f = f_1^{i_1} \cdot \cdots f_r^{i_r}$ is a decomposition of f with f_i irreducible and pairwise distinct, then clearly $V(f) = V(f_1 \cdot \cdots \cdot f_r)$, i.e., changing the exponents does not change the vanishing set. It is therefore clear that every $V(f)$ can also be written as the vanishing set of a polynomial for which $k[x,y]/(f)$ is reduced.

Over an algebraically closed field, we have the following strong converse: Given $V \subset k^2$ that has the form "vanishing set of one non-constant polynomial", there is a unique (up to multiplication by scalars in $k^\times$) polynomial $f \in k[x,y]$ such that $V = V(f)$ and such that the ring $k[x,y]/(f)$ is *reduced* (i.e., it has no non-trivial nilpotent elements). When we use this f, we get

the "right" notion of smooth points. (In fact, it is not difficult to show that for f such that $k[x,y]/(f)$ is *not* reduced, all points are non-smooth in the sense of the above definition applied to f.)

In fact, there is the following more general version of this statement. For an ideal $\mathfrak{a} \subset k[T_1, \dots, T_n]$ we denote by

$$\sqrt{a} = \{x \in k[T_\bullet];\ x^n \in \mathfrak{a} \text{ for some } n \geq 0\}$$

its radical. (With notation as above, $\sqrt{(f)} = (f_1 \cdot \dots \cdot f_r)$.) It is easy to see that $k[T_1, \dots, T_n]/\mathfrak{a}$ is reduced if and only if $\mathfrak{a} = \sqrt{\mathfrak{a}}$, and that $V(\mathfrak{a}) = V(\sqrt{\mathfrak{a}})$. Furthermore, we have:

Theorem 1.25. *Let k be an algebraically closed field, and let $\mathfrak{a}, \mathfrak{b} \subseteq k[T_1, \dots, T_n]$ be ideals. Then*

$$V(\mathfrak{a}) = V(\mathfrak{b}) \quad \iff \quad \sqrt{\mathfrak{a}} = \sqrt{\mathfrak{b}}.$$

This is (one version of) Hilbert's Nullstellensatz. The implication $\Leftarrow$ is easy, as indicated above, and does not require the assumption that k is algebraically closed. The other implication is non-trivial already in the case that $\mathfrak{a} = (1)$, so $V(\mathfrak{a}) = \emptyset$. In this case the statement is equivalent to saying that any family $f_1, \dots, f_r$ of polynomials that does not generate the unit ideal has a common zero, whence the name *Nullstellensatz* (*Nullstelle* is German for *zero (of a polynomial)*).

We will take up this discussion again, and in more detail, later.

Remark 1.26. Another perspective on the situation over the real numbers (and similarly over the complex numbers) is the Theorem on inverse functions. It implies, if P is a smooth point of $V(f)$ in the sense of the above definition, that locally (in the analytic, "usual", topology) around P the set $V(f)$ is diffeomorphic to an open interval in $\mathbb{R}$, i.e., there exists an open $U \subset V(f)$, $P \in U$, and an open interval $V \subset \mathbb{R}$, and bijective differentiable functions $U \to V$ and $V \to U$ that are inverse to each other.

More generally, there is a version for vanishing sets (or more generally, level sets) of continuously differentiable maps $\mathbb{R}^n \to \mathbb{R}$, and even more generally for fibers of continuously differentiable maps $f\colon \mathbb{R}^n \to \mathbb{R}^m$, $x \mapsto (f_1(x), \dots, f_m(x))$, such that the Jacobi matrix (at some point P),

$$\left(\frac{\partial f_j}{\partial x_i}(P)\right)_{i,j}$$

has rank m. Then locally around P, the fiber over $f(P)$ is a differentiable manifold, i.e., is diffeomorphic to an open of $\mathbb{R}^{n-m}$.

See Inverse function theorem (Wikipedia)[1], in particular the section Giving a manifold structure.

[1] `https://en.wikipedia.org/wiki/Inverse_function_theorem`

For the projective plane, we make the following analogous definition (which again depends on the polynomial F, not only on the vanishing set, cf. Remark 1.24

Definition 1.27. *Let k be a field and let $F \in k[X,Y,Z]$ be a non-constant homogeneous polynomial. We call a point $P \in V_+(F)$ a* smooth *(or* non-singular*) point of $V_+(F)$, if*

$$\left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right) \neq (0,0,0),$$

and in this case call the line

$$V_+\left(\frac{\partial F}{\partial X}(P)\cdot X + \frac{\partial F}{\partial Y}(P)\cdot Y + \frac{\partial F}{\partial Z}(P)\cdot Z\right)$$

the tangent line *to $V_+(F)$ at P. Otherwise, we call P a* singular *point.*

For the following remarks, the next lemma will be useful; we record it here in the general case of $n+1$ variables. Also note that for a homogeneous polynomial of degree d, all partial derivatives are homogeneous of degree $d-1$.

Lemma 1.28. (Euler identity) *Let $F \in k[X_0,\dots,X_n]$ be a homogeneous polynomial of degree d. Then*

$$\frac{\partial F}{\partial X_0}X_0 + \cdots + \frac{\partial F}{\partial X_n}X_n = dF.$$

Proof. Since both sides are k-linear in F, it is enough to check this in case $F = X_0^{\nu_0}\cdots X_n^{\nu_n}$ is a monomial. But then $\frac{\partial F}{\partial X_i}X_i = \nu_i F$ and the stated identity follows immediately. □

Remark 1.29.

(1) Euler's identity shows that the tangent line to a smooth point of $V_+(F)$ contains the point P.

(2) The two definitions of smooth point are related as follows. Let $F \in k[X,Y,Z]$ be a homogeneous polynomial, $f = F(x,y,1)$, so that $V_+(F) \cap \iota(k^2)$ may be identified with $V(f) \subset k^2$. Cf. Section (1.6). We assume that f is non-constant, and take $P \in V(f)$, say $P = (x_0, y_0)$, and $\iota(P) = (x_0 : y_0 : 1)$.

Then

$$\frac{\partial F}{\partial X}(x,y,1) = \frac{\partial f}{\partial x}, \quad \frac{\partial F}{\partial Y}(x,y,1) = \frac{\partial f}{\partial y}, \tag{1.8.1}$$

as is easily checked, and in particular

$$\frac{\partial F}{\partial X}(x_0,y_0,1) = \frac{\partial f}{\partial x}(P), \quad \frac{\partial F}{\partial Y}(x_0,y_0,1) = \frac{\partial f}{\partial y}(P).$$

This already shows that if $P \in V(f)$ is smooth (with respect to the polynomial f, that is), then $\iota(P)$ is a smooth point of $V_+(F)$ (i.e., for

F). To show the equivalence, assume that $\iota(P) \in V_+(F)$ such that the partial derivatives of F with respect to X and to Y both vanish. Then Euler's identity shows, since $F(\iota(P)) = 0$, that the partial derivative with respect to Z vanishes, as well, so $\iota(P)$ is not smooth.

Finally, for a smooth point with tangent line $V_+(L)$ to $V_+(F)$ at $\iota(P)$,

$$L = \frac{\partial F}{\partial X}(P) \cdot X + \frac{\partial F}{\partial Y}(P) \cdot Y + \frac{\partial F}{\partial Z}(P) \cdot Z,$$

equation (1.8.1) shows that $V(L(x, y, 1))$ is the tangent to $V(f)$ at P. In this sense, the two definitions are compatible.

(1.9) Smoothness for Cubic Curves.

Let us understand the notion of smoothness in the special case of cubic curves (compare the earlier examples), more precisely for $V(f)$ with f of the form

$$f = y^2 - (x^3 + ax^2 + bx + c) = y^2 - g(x).$$

As before, assume $\mathrm{char}(k) \neq 2$.

Then

$$\frac{\partial f}{\partial x} = -g'(x), \qquad \frac{\partial f}{\partial y} = 2y.$$

(This shows why the situation is different in characteristic 2, namely then the partial derivative with respect to y vanishes for all points.)

The points $(x_0, y_0) \in V(f)$ where both partial derivatives vanish satisfy

$$y_0 = 0, \quad g(x_0) = g'(x_0) = 0,$$

i.e. x_0 is a multiple root of g.

Proposition 1.30. *For f as above, $V(f)$ is smooth if and only if g is separable (i.e. g has no multiple roots in an algebraic closure $\overline{k}$).*

We may homogenize f to obtain

$$F(X, Y, Z) = Y^2Z - X^3 - aX^2Z - bXZ^2 - cZ^3.$$

homogeneous of degree 3. By Remark 1.29, $P \in V(f)$ is smooth if and only $\iota(P) \in V_+(F)$ is smooth, where as usual ι denotes the embedding $k^2 \to \mathbb{P}^2(k)$. Let us check smoothness at those points of $V_+(F)$ that lie on the line at infinity, i.e., points of the form $(x_0 : y_0 : 1) \in V_+(F)$. Then the vanishing of F amounts to $x_0 = 0$, and since this excludes the possibility of y_0 vanishing as well, and we can scale the homogeneous coordinates, we see that $V_+(F) \cap V_+(Z)$ consists of the one point $(0 : 1 : 0)$.

At this point, the partial derivative $\dfrac{\partial F}{\partial Z} = Y^2 - aX^2 - 2bXZ - 3cZ^2$ does not vanish, so it is a smooth point, independently of the choice of a, b, c. Therefore, for this special form of f and F, $V_+(F)$ is smooth if and only $V(f)$ is smooth, if and only if g is separable.

Oct. 28, 2025

(1.10) Elliptic Curves and the Group Law.

Definition* 1.31. *Let k be a field. An* elliptic curve over k *is given by a homogeneous polynomial F of degree 3 such that the vanishing set $V_+(F)$ is smooth ("for F", at all points of $V_+(F)(\overline{k})$, for an algebraic closure $\overline{k}$ of k), together with a fixed point $\mathcal{O} \in E$.*

Typical examples are the curves defined by homogenizations of polynomials of the form

$$y^2 - g(x), \quad g \in k[x] \text{ a separable polynomial of degree } 3$$

that we have studied above. In this case, we can (and typically do) choose the unique point $(0:1:0)$ of $V_+(F)$ on the line at infinity as the distinguished point $\mathcal{O}$.

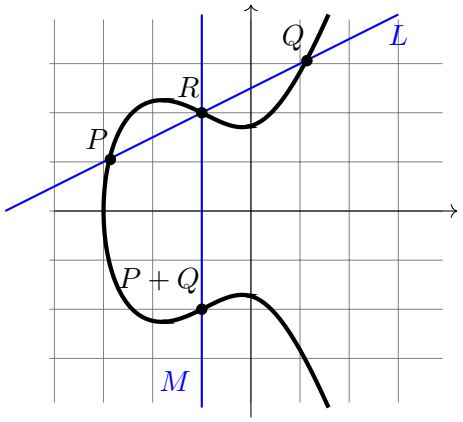
These elliptic curves have an extremely surprising additional structure, as shown by the next proposition. We will assume that k is algebraically closed, so that we can use Bézout's theorem; but see the following remark.

Proposition 1.32. *Let k be algebraically closed. Let $E = V_+(F) \subset \mathbb{P}^2(k)$ be smooth with $\deg F = 3$, and let $\mathcal{O} \in E$ be a fixed point. For $P, Q \in E$, let $L \subset \mathbb{P}^2(k)$ be the line through P, Q (or, in case $P = Q$, the tangent to $V_+(F)$ at $P = Q$).*

Then, counting with multiplicities, the intersection $E \cap L$ has three elements, among them P and Q; we express this, and give these points names, by saying that "$E \cap L = \{\{P, Q, R\}\}$ as a multiset". Let M be the line through $\mathcal{O}$ and R (or, in case of equality, the tangent to $V_+(F)$ at this point), write $E \cap M = \{\{\mathcal{O}, R, S\}\}$ and define

$$P + Q = S.$$

Then $(E, +)$ is a commutative group with neutral element $\mathcal{O}$.



Proof. All properties except for associativity are easy to check. The neutral element is the point $\mathcal{O}$. For a point P, its negative $-P$ is the third point in the intersection of $V_+(F)$ and the line through P and $\mathcal{O}$. The associativity

can, in principle, be checked by "direct computation" (write out equations for all the lines involved in terms of coordinates of the points for which one wants to check associativity), but this leads to long, complicated and tedious calculations which are not at all enlightening. For a better, but still elementary proof, see, e.g., [Kn] Section III.3 for a complete proof; cf. also the discussion in [ST] 1.2.

(We will later, but rather next term than this term, be able to give a more enlightening proof based on the Theorem of Riemann–Roch.) □

Remark 1.33. One can check that the proposition is still true without the assumption that k be algebraically closed. In fact, for any field extension k'/k, we obtain compatible group structures, i.e., $V_+(F)(k) \subseteq V_+(F)(k')$ is a subgroup. The key reason is that whenever a cubic polynomial in one variable over a field k has 2 zeros in k, then the third zero also lies in k (always counting zeros with multiplicity). To prove the statement, one way to proceed is to write down formulas for the coordinates of $P + Q$ in terms of the coordinates of P and of Q and see that whenever P, Q (and $\mathcal{O}$) have coordinates in k, then so does $P + Q$ and $-P$. See [ST] 1.4 or [Kn] III.4.

Outlook: Advanced results and some open conjectures.

Oct. 29, 2025

(1.11) The Mordell Conjecture (Faltings' Theorem).

From a number theoretic view, it is an interesting question to determine the number of points of a vanishing set $V_+(F) \subset \mathbb{P}^2(k)$ when k is a *number field*, i.e., a finite extension of $\mathbb{Q}$. For example, if F is linear, then $V_+(F)$ evidently has infinitely many points (whenever k is any infinite field; for a finite field of cardinality q, it has $q + 1$ points). For F homogeneous of degree 2 the situation is still relatively easy to understand (but we skip this here). However for F of degree ≥ 3, this is an extremely difficult question, and although a lot of progress has been made over the last 50 years, there are many questions that are still open. We first mention the Theorem of Mordell and Weil that dates back even further and gives some important information in the case of homogeneous cubic polynomials which define a smooth curve, i.e., an elliptic curve.

Theorem 1.34. [Mordell–Weil, Mordell 1922 für $K = \mathbb{Q}$; Weil 1928] *Let $K/\mathbb{Q}$ be a finite field extension and let E be an elliptic curve over K. Then the abelian group $E(K)$ is finitely generated.*

Depending on the choice of polynomial F, the group might be finite or infinite. By the general theory of finitely generated abelian group, we can find a group isomorphism $E(K) \cong \mathbb{Z}^r \times T$ for a finite group T and some natural

number $r \geq 0$, called the *rank* of E. Even in the case $K = \mathbb{Q}$, there are many open problems around the rank. For example, it is not known whether elliptic curves over $\mathbb{Q}$ of arbitrarily high rank exist. At the time of writing, the best result in this direction is by Elkies and Klagbrun who found (in 2024) an elliptic curve of rank ≥ 29. The Conjecture of Birch and Swinnerton-Dyer relates the rank of an elliptic curve to a natural number defined in analytic terms (the vanishing order of a certain holomorphic function, the so-called L-function of the elliptic curve).

For a proof of the theorem, see [ST] Chapter 3 (for $K = \mathbb{Q}$), or [Si] Chapter VIII.

For polynomials of higher degree Mordell conjectured that there are only finitely many solutions with coordinates in a fixed number field. This conjecture was proved in 1983 by Faltings, and he received the Fields medal in 1986 in recognition for this proof. We state the result in a slightly more general form (which you can ignore for now, and just read it in the case of the specific example of vanishing sets $V_+(F)$ in $\mathbb{P}^2(k)$).

Theorem 1.35. [Mordell Conjecture = Faltings's Theorem] *Let $K/\mathbb{Q}$ be a finite field extension and C/K a smooth projective curve of genus $g \geq 2$, e.g., $C = V_+(F) \subset \mathbb{P}^2(k)$ with F homogeneous of degree ≥ 4 such that $V_+(F)$ is smooth.*

Then $C(K)$ is a finite set.

(1.12) Fermat's Last Theorem and Modular Curves.

Theorem 1.36. ["Fermat's last theorem"; Wiles] *Let $p > 2$ be prime. Then*

$$V_+(X^p + Y^p + Z^p)(\mathbb{Q}) = \{(0:1:-1), (1:0:-1), (1:-1:0)\},$$

i.e. only the trivial (obvious) solutions exist.

It follows from Faltings's Theorem that the set on the left hand side is finite whenever $p > 3$, but that theorem does not give any information on the cardinality of this finite set. Wiles's contribution was the following more specific result about elliptic curves over $\mathbb{Q}$.

Theorem 1.37. [Taniyama–Shimura–Weil Conjecture; Wiles, 1995] *Every elliptic curve $E/\mathbb{Q}$ is modular.*

Actually, Wiles (together with Taylor) proved a slightly weaker than the theorem stated here; the proof was later completed by Breuil, Conrad, Diamond and Taylor. Ribet, based on an idea of Frey[2], had shown before that this modularity conjecture implies Fermat's Last Theorem. The key idea of Frey was that assuming that $a^p + b^p = c^p$ for $abc \neq 0$, the elliptic curve defined by the (homogenization of the) equation

$$y^2 = x(x - a^p)(y - b^p)$$

[2]Gerhard Frey was a professor at the University of Duisburg-Essen from 1990 to 2009.

has "strange" properties and is seemingly not modular; this was then shown by Ribet.

Remark 1.38. We do not explain here what *modular* means. Roughly, it asserts a strong relation between the elliptic curve and a certain "modular form".

For example, if E is given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$, then modularity implies a precise regularity for the numbers of points

$$\#\{(x, y) \in \mathbb{F}_q^2 \mid y^2 = x^3 + Ax + B\},$$

for each prime power q.

(1.13) The abc Conjecture.

We finish this chapter by a brief discussion of another famous conjecture which at first sight does not have much to do with algebraic geometry (but in fact, it does: for instance, it is equivalent to a conjecture by Szpiro on elliptic curves over $\mathbb{Q}$; indeed, Masser and Oesterlé made their conjecture after studying Szpiro's conjecture and its consequences).

We define the *radical* of a positive integer n as

$$\mathrm{rad}(n) := \prod_{p \text{ prime},\ p|n} p.$$

Conjecture 1.39. [abc conjecture, Masser–Oesterlé] *For every $\varepsilon > 0$ there are only finitely many coprime triples (a, b, c) of positive integers with $a+b = c$ and*

$$c > \mathrm{rad}(abc)^{1+\varepsilon}.$$

We also state the following stronger variant, an *explicit form of the abc conjecture*. If $a, b, c \in \mathbb{Z}_{>0}$ are coprime with $a + b = c$, then

$$c \leq \mathrm{rad}(abc)^2.$$

Example 1.40. $3+125 = 128 = c$, and $c > 30 = \mathrm{rad}(3 \cdot 125 \cdot 128)$ illustrates the inequality.

Remark 1.41.

(1) It is, somewhat surprisingly, not difficult to prove an analogous statement, where the ring $\mathbb{Z}$ of integers is replaced by the polynomial ring $\mathbb{C}[X]$. See the second problem sheet.
(2) The abc conjecture implies effective versions of the Mordell Conjecture/Faltings's Theorem.

Let us illustrate by showing that the above effective version of the abc conjecture easily implies Fermat's Last Theorem for exponents $n \geq 6$.

In fact, suppose there exist $n \in \mathbb{N}$ and coprime positive integers x, y, z with $x^n + y^n = z^n$. Then

$$z^n \leq \mathrm{rad}(xyz)^2$$

by the abc conjecture, but also

$$\mathrm{rad}(xyz)^2 \leq (xyz)^2 < z^6.$$

Putting both inequalities together, we obtain $n < 6$. The cases $n = 3, 4, 5$ are (relatively) easier and have long been known, so the (effective) *abc*-conjecture implies Fermat's Last Theorem.

(1.14) Problems with Our Approach So Far.

What we have discussed so far was intentionally introductory and not yet systematic. Beyond that, the "theory" so far has some serious problems. Some are easy to fix; others require more serious changes. Desiderata:

- The same vanishing set $V(f)$ (or more generally, $V(f_1, \ldots, f_m)$) can be defined by several different polynomials, and the set alone does not "contain enough information" (for example, in order to define smoothness). We would like to equip it with more "geometric structure" which will allow us to not carry around a specific choice of polynomial(s).
- Related to this: A definition of *morphisms* (and hence isomorphisms) between vanishing sets $V(f_1, \ldots, f_m)$.
- A more systematic use of *commutative algebra*.
- A theory that works well over *non-algebraically closed fields* (and even over arbitrary commutative rings).
- A more transparent *geometric meaning* of intersection multiplicities $i_P(V_+(F), V_+(G))$ in Bézout's theorem (see earlier sections).

2. The prime spectrum of a ring

References: [GW1] (2.1)–(2.4) (or other books that cover scheme theory, e.g., [Mu] Ch. II §1; [Ha] II.1). Nov. 4, 2025

(2.1) Motivation: Hilbert's Nullstellensatz.

One piece of motivation for the theory we are going to work out is *Hilbert's Nullstellensatz*. To start the discussion, we start with a simple observation.

Proposition 2.1. *Let k be a field, $(t_1, \dots, t_n) \in k^n$. Then*

$$(T_1 - t_1, \dots, T_n - t_n) \subset k[T_1, \dots, T_n]$$

is a maximal ideal. This ideal is the kernel of the evaluation homomorphism

$$k[T_1, \dots, T_n] \to k, \quad T_i \mapsto t_i,$$

i.e., a polynomial f lies in the above ideal if and only if $f(t_1, \dots, t_n) = 0$.

Proof. All statements are easy to check. □

Theorem 2.2. *Let k be a field, and $\mathfrak{m} \subset k[T_1, \dots, T_n]$ a maximal ideal. Then the field extension $k \subset k[T_1, \dots, T_n]/\mathfrak{m}$ is finite.*

Proof. See [GW1] Section (1.3), or [Mu] Ch. I §1, or [Alg2] 4.3[3] for proofs based on Noether Normalization, or, for instance, [AM] Ch. 5, Ch. 7 for (somewhat) different proofs. □

Corollary 2.3. *Let k be an algebraically closed field. Then the maximal ideals of the ring $k[T_1, \dots, T_n]$ are precisely the ideals of the form*

$$(T_1 - t_1, \dots, T_n - t_n), \quad (t_1, \dots, t_n) \in k^n,$$

and we obtain a bijection between k^n and the set of maximal ideals of $k[T_1, \dots, T_n]$.

Proof. Let $\mathfrak{m} \subset k[T_1, \dots, T_n]$ be a maximal ideal. By the theorem, the inclusion $k \to k[T_1, \dots, T_n]/\mathfrak{m}$ is a finite field extension, hence – since k is algebraically closed by assumption – an isomorphism. We define t_i as the image of (the residue class of) T_i under its inverse. Then clearly $(T_1 - t_1, \dots, T_n - t_n) \subset \mathfrak{m}$, and since the left hand side is a maximal ideal, equality follows. □

Under the bijection of the corollary (for k algebraically closed), a vanishing set $V(f_1, \dots, f_m)$ corresponds to the set of all maximal ideals that contain $f_1, \dots, f_m$.

[3] `https://math.ug/a2-ss23/sec-nullstellensatz.html`

(2.2) The spectrum of a ring.

Following Grothendieck, and in view of Hilbert's Nullstellensatz, we start a general theory of algebraic geometry by replacing polynomial rings over (algebraically closed) fields by arbitrary ring, and defining for a ring R, its prime spectrum

$$\operatorname{Spec}(R) = \{\mathfrak{p} \subset R \text{ prime ideal}\}.$$

(It is better to work with prime ideals than with maximal ideals. One reason is that otherwise the following definition of the map between spectra induced by a ring homomorphism would not work, since in general preimages of maximal ideals under a ring homomorphism are not maximal ideals.)

For an element $f \in R$, we denote by $f(\mathfrak{p})$ the image of f under the ring homomorphism

$$R \longrightarrow R/\mathfrak{p} \longrightarrow \operatorname{Frac}(R/\mathfrak{p}).$$

In particular, we have $f(\mathfrak{p}) = 0$ if and only if $f \in \mathfrak{p}$. (Compare the situation for polynomial rings over fields, and polynomials f.)

Proposition/Definition 2.4. [Zariski topology on $\operatorname{Spec}(R)$] *Let R be a ring.*

(1) *For a subset $M \subseteq R$, we define the "vanishing set"*

$$V(M) = \{\mathfrak{p} \in \operatorname{Spec}(R);\ M \subseteq \mathfrak{p}\}.$$

If $\mathfrak{a}$ is the ideal generated by M, then $V(M) = V(\mathfrak{a})$. For $M \subseteq M'$, we have $V(M') \subseteq V(M)$. For an element $f \in R$ we also write $V(f)$ for $V(\{f\})$.

(2) *We have $V(0) = \operatorname{Spec}(R)$, $V(1) = \emptyset$.*

(3) *For a family $\mathfrak{a}_i$ of ideals of R, we have*

$$\bigcap_i V(\mathfrak{a}_i) = V\left(\sum_i \mathfrak{a}_i\right).$$

(4) *For ideals $\mathfrak{a}_1, \mathfrak{a}_2 \subseteq R$ we have*

$$V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) = V(\mathfrak{a}_1 \cap \mathfrak{a}_2) = V(\mathfrak{a}_1\mathfrak{a}_2).$$

In particular, the subsets of $\operatorname{Spec}(R)$ of the form $V(\mathfrak{a})$ for ideals $\mathfrak{a} \subseteq R$ form the closed sets of a topology on $\operatorname{Spec}(R)$, the so-called Zariski topology*.*

Proof. Assertions (1), (2) and (3) are easy to check. For (4) note that

$$\mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{a}_1 \cap \mathfrak{a}_2 \cap \mathfrak{a}_1,$$

and likewise for $\mathfrak{a}_2$, so that we have

$$V(\mathfrak{a}_1) \cup V(\mathfrak{a}_2) \subseteq V(\mathfrak{a}_1 \cap \mathfrak{a}_2) \subseteq V(\mathfrak{a}_1\mathfrak{a}_2).$$

Now let $\mathfrak{p} \in V(\mathfrak{a}_1\mathfrak{a}_2)$ and assume that $\mathfrak{p} \notin V(\mathfrak{a}_1)$, say $f \in \mathfrak{a}_1 \setminus \mathfrak{p}$. But then for every $g \in \mathfrak{a}_2$, we have $fg \in \mathfrak{a}_1\mathfrak{a}_2 \subseteq \mathfrak{p}$, and since $\mathfrak{p}$ is a prime ideal and $f \notin \mathfrak{p}$, we get $g \in \mathfrak{p}$. We have shown that $\mathfrak{a}_2 \subseteq \mathfrak{p}$, i.e., that $\mathfrak{p} \in V(\mathfrak{a}_2)$. □

With the notation introduced above, we can also write

$$V(M) = \{\mathfrak{p} \in \operatorname{Spec}(R);\ f(\mathfrak{p}) = 0 \text{ for all } f \in M\}\,.$$

This in particular shows the analogy with the notation $V(M)$ introduced in Chapter 1. But note that this is only an analogy; we really *redefine* the notation $V(M)$ and from now on will use it only with the new meaning.

Example 2.5.
(1) $\operatorname{Spec}(k)$ for k a field,
(2) $\operatorname{Spec}(\mathbb{Z})$,
(3) $\operatorname{Spec}(k \times k)$ for k a field,
(4) $\operatorname{Spec}(k[T])$ for k a field.

We have attached to every ring R a topological space $\operatorname{Spec}(R)$. We extend this definition to a *contravariant functor* from the category of rings to the category of topological spaces, as follows. (This means simply that to each ring homomorphism $\varphi\colon R \to S$ we attach a continuous map $\operatorname{Spec}(S) \to \operatorname{Spec}(R)$ (note that it goes "in the other direction", whence the term *contravariant*), and this is compatible with composition of homomorphisms, and for the identity map an rings we get the identity map on topological spaces.)

Recall that the inverse image of a prime ideal under a ring homomorphism is a prime ideal.

Definition 2.6. *Let $\varphi\colon R \to S$ be a ring homomorphism. We define a map*

$$^a\varphi\colon \operatorname{Spec}(S) \to \operatorname{Spec}(R), \quad \mathfrak{q} \mapsto \varphi^{-1}(\mathfrak{q}).$$

This map is also denoted by $\operatorname{Spec}(\varphi)$.

It is immediate that this construction is compatible with composition of homomorphisms, and for the identity map an rings we get the identity map on topological spaces. Continuity is also easy to check:

Lemma 2.7. *Let $\varphi\colon R \to S$ be a ring homomorphism. Then the map $^a\varphi$ is continuous. More precisely, for every ideal $\mathfrak{a} \subseteq R$, we have*

$$(^a\varphi)^{-1}(V(\mathfrak{a})) = V(\varphi(\mathfrak{a})).$$

Proof. The second statement implies that for every closed subset of $\operatorname{Spec}(R)$ the inverse image under $^a\varphi$ is again closed, and hence that the map $^a\varphi$ is continuous. To prove it, note that for $\mathfrak{q} \in \operatorname{Spec}(S)$ we have

$$\begin{aligned}\mathfrak{q} \in (^a\varphi)^{-1}(V(\mathfrak{a})) &\iff {}^a\varphi(\mathfrak{q}) \in V(\mathfrak{a}) \iff \mathfrak{a} \subseteq \varphi^{-1}(\mathfrak{q}) \\ &\iff \varphi(\mathfrak{a}) \subseteq \mathfrak{q} \iff \mathfrak{q} \in V(\varphi(\mathfrak{a})).\end{aligned}$$

□

Note that it is easy (i.e., you should do it …) to construct examples of a ring R and ideals $\mathfrak{a} \neq \mathfrak{b}$ with $V(\mathfrak{a}) = V(\mathfrak{b})$. The following result clarifies the situation.

Proposition 2.8. *Let R be a ring. For $Y \subseteq \operatorname{Spec}(R)$, write $I(Y) = \bigcap_{\mathfrak{p}\in Y} \mathfrak{p}$.*

The maps $\mathfrak{a} \mapsto V(\mathfrak{a})$ and $Y \mapsto I(Y)$ satisfy

(1) $V(I(Y)) = \overline{Y}$,

(2) $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$,

and in particular induce a bijection between the set of all radical ideals of R and the set of all closed subsets of $\operatorname{Spec}(R)$.

Proof. It is clear that both $V(-)$ and $I(-)$ are inclusion reversing. Furthermore, $I(Y)$, being an intersection of radical ideals, is itself a radical ideal for every Y. Since $V(\mathfrak{a})$ is closed for every $\mathfrak{a}$, the final statement follows from (1) and (2).

Let us show that $V(I(Y)) = \overline{Y}$ for every subset $Y \subseteq \operatorname{Spec}(R)$. Clearly the left hand side is closed and contains Y, so we have $\supseteq$. To show $\subseteq$ we need to show that $V(I(Y))$ is the smallest closed subset containing Y, i.e., that whenever $Y \subseteq V(\mathfrak{a})$, then $V(I(Y)) \subseteq V(\mathfrak{a})$. But if $Y \subseteq V(\mathfrak{a})$, then $\mathfrak{a} \subseteq \mathfrak{p}$ for all $\mathfrak{p} \in Y$, so $\mathfrak{a} \subseteq I(Y)$, and hence $V(I(Y)) \subset V(\mathfrak{a})$ as desired.

Now we show that $I(V(\mathfrak{a})) = \sqrt{\mathfrak{a}}$ for every ideal $\mathfrak{a} \subset R$. But the radical of $\mathfrak{a}$ can be described as

$$\sqrt{\mathfrak{a}} = \bigcap_{\mathfrak{p}\in\operatorname{Spec}(R),\ \mathfrak{a}\subseteq\mathfrak{p}} \mathfrak{p},$$

and this is precisely $I(V(\mathfrak{a}))$. □

In particular, for every $\mathfrak{p} \in \operatorname{Spec}(R)$,

$$\overline{\{\mathfrak{p}\}} = V(\mathfrak{p}).$$

From this we see that a point $\mathfrak{p} \in \operatorname{Spec}(R)$ is closed (i.e., $\{\mathfrak{p}\}$ is a closed subset of $\operatorname{Spec}(R)$) if and only if $\mathfrak{p}$ is a maximal ideal.

Definition 2.9. *Let R be a ring. For $f \in R$ we define $D(f) = \operatorname{Spec}(R)\backslash V(f)$ and call the subsets of* $\operatorname{Spec}(R)$ *of this form* principal open subsets.

With the notation introduced above we may write

$$D(f) = \{\mathfrak{p} \in \operatorname{Spec}(R);\ f(\mathfrak{p}) \neq 0\},$$

and correspondingly we sometimes think of $D(f)$ as the *non-vanishing set of f*.

Proposition 2.10. *Let R be a ring.*

(1) *The sets $D(f)$ for $f \in R$ form a basis of the topology of* $\operatorname{Spec}(R)$, *i.e., every open subset of* $\operatorname{Spec}(R)$ *can be written as a union of subsets of this form.*

(2) *The family of sets $D(f)$ is stable under taking finite intersections.*

Proof. For (1) take $U \subseteq \operatorname{Spec}(R)$ open, say $U = \operatorname{Spec}(R)\backslash V(\mathfrak{a})$. Then $V(\mathfrak{a}) = \bigcap_{f\in\mathfrak{a}} V(f)$, hence $U = \bigcup_{f\in\mathfrak{a}} D(f)$. For (2) note that $D(f) \cap D(g) = D(fg)$ and that the intersection with empty index set, $\operatorname{Spec}(R)$ equals $D(f)$. □

References

[AM] M. Atiyah, I. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley.
[Alg2] U. Görtz, *Kommutative Algebra*, Vorlesungsskript[4], SS 2023.
[GW1] U. Görtz, T. Wedhorn, *Algebraic Geometry I: Schemes*, 2nd ed., Springer Spektrum (2020).
[Ha] R. Hartshorne, *Algebraic Geometry*, Springer Graduate Texts in Math.
[Mu] D. Mumford, *The Red Book on Varieties and Schemes*, 2nd expanded ed., Springer Lecture Notes in Math. 1358 (1999).
[Kn] A. Knapp, *Elliptic Curves*, Princeton Univ. Press 1992.
[Si] J. Silverman, *The Arithmetic of Elliptic Curves*, 2nd ed., Springer Graduate Textes in Math.
[ST] J. Silverman, J. Tate, *Rational Points on Elliptic Curves*, 2nd ed., Springer

[4] `https://math.ug/a2-ss23/`