Introduction to Algebraic Geometry

George Voutsadakis[1]

[1]Mathematics and Computer Science
Lake Superior State University

LSSU Math 500

Subsection 1

Functions

Linear Algebra

- *Linear algebra* is concerned with finding the solutions of a system of linear equations, that is, a system of the form

$$\begin{aligned} a_{11}x_1 + \cdots + a_{1m}x_m &= b_1 \\ &\vdots \\ a_{n1}x_1 + \cdots + a_{nm}x_m &= b_n \end{aligned}$$

  where a_{ij} and b_i are elements of some field k.

Quadratic Hypersurfaces

- Affine and projective quadratic hypersurfaces have the form

$$\sum_{i,j=1}^{n} a_{ij}x_ix_j + \sum_{i=1}^{n} b_ix_i + c = 0,$$

  where a_{ij} are the coefficients of a symmetric matrix.
- So the classification of affine and projective quadratic hypersurfaces can also be reduced to a problem in linear algebra.
- The properties of the ground field k do not play an important role in the theory of linear equations.
- For the classification of quadrics this is no longer the case.

Polynomials and Sets of Solutions

- In an elementary algebra course, we study the set of solutions of polynomials of arbitrary degree,

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 = 0, \quad a_i \in k.$$

- The existence of solutions $x \in k$, with $f(x) = 0$, depends on k.
- For example, to guarantee the existence of a solution, k must be algebraically closed.

Algebraic Geometry: Algebraic Sets

- *Algebraic geometry* is concerned with the study of **algebraic sets**.
- These are sets of solutions of polynomial equations in several variables,

$$\begin{aligned} f_1(x_1,\ldots,x_n) &= 0 \\ &\vdots \\ f_m(x_1,\ldots,x_n) &= 0 \end{aligned}$$

  where $f_i(x_1,\ldots,x_n)$ are polynomials.

Algebraic Geometry: Affine Spaces

- We fix an arbitrary ground field k.
- **Affine space** of dimension n over k is defined by

$$\mathbb{A}^n := \mathbb{A}^n_k := k^n = \{(a_1, \ldots, a_n) : a_i \in k\}.$$

- k^n and $\mathbb{A}^n$ are equal as sets.
- k^n is equipped with the standard vector space structure.
- $\mathbb{A}^n$ is affine space, i.e., it does not have an addition and there are no special points (e.g., the origin is not singled out).
- We will give $\mathbb{A}^n$ the structure of a topological space, by defining the *Zariski topology*.

Zero Loci

- Every polynomial $f \in k[x_1, \ldots, x_n]$ defines a map

$$\begin{array}{rcl} f: \mathbb{A}^n & \to & k; \\ (a_1, \ldots, a_n) & \mapsto & f(a_1, \ldots, a_n). \end{array}$$

- A point $P = (a_1, \ldots, a_n) \in \mathbb{A}^n$ is called a **zero** of f if

$$f(P) = 0.$$

- Note that unless k has infinitely many elements (e.g.,, when k is algebraically closed), several polynomials can define the same map.

Zero Loci (Cont'd)

- The **zero locus** of f is the set

$$V(f) := \{P \in \mathbb{A}^n : f(P) = 0\}.$$

- Let $T \subseteq k[x_1, \ldots, x_n]$ be a subset of the polynomial ring.

Definition (Zero Locus)

The **zero locus** of T is the set

$$V(T) := \{P \in \mathbb{A}^n : f(P) = 0, \text{ for all } f \in T\}.$$

Affine Algebraic Sets or Zariski Closed Sets

Algebraic Set or Zariski Closed Set

A subset $Y \subseteq \mathbb{A}^n$ is called an (**affine**) **algebraic set** (or a **closed**, or **Zariski closed set**) in $\mathbb{A}^n$ if there is a subset $T \subseteq k[x_1, \ldots, x_n]$, such that

$$Y = V(T).$$

- It is not necessary to consider arbitrary subsets T of $k[x_1, \ldots, x_n]$.
- We will now show that we can replace T by the *ideal* generated by T, namely
$$J := (T) \subseteq k[x_1, \ldots, x_n].$$
- Moreover, since $k[x_1, \ldots, x_n]$ is a Noetherian ring, there are finitely many polynomials $f_1, \ldots, f_m \in k[x_1, \ldots, x_n]$, such that
$$J = (f_1, \ldots, f_m).$$

Algebraic Sets are Finitely Generated

Lemma

For T and J as before, $V(T) = V(J) = V(f_1, \ldots, f_m)$.

- Clearly $V(J) \subseteq V(T)$.

  Let $g \in J$. There exist $h_1, \ldots, h_\ell \in T$ and $q_1, \ldots, q_\ell \in k[x_1, \ldots, x_n]$, such that
  $$g = h_1 q_1 + \cdots + h_\ell q_\ell.$$
  Suppose $P \in V(T)$. Then $h_1(P) = \cdots = h_\ell(P) = 0$.

  So $g(P) = 0$. Hence, $V(T) \subseteq V(J)$.

  A similar argument shows that $V(J) = V(f_1, \ldots, f_m)$.
- The lemma shows that we can restrict attention to finite systems of polynomial equations.

Examples of Degree 1 and 2

- The simplest possible algebraic subset of $\mathbb{A}_k^n$ is one given by a set of linear equations. Such an algebraic set is called an **affine subspace**. It is itself isomorphic to an affine space.
- The conic, given by an equation of the form

$$f(x,y) = a_1x^2 + a_2y^2 + a_3xy + a_4x + a_5y + a_6 = 0, \ a_1,\ldots,a_6 \in \mathbb{R},$$

  is a well known example of an algebraic set.

  The circle, parabola and hyperbola are special cases.

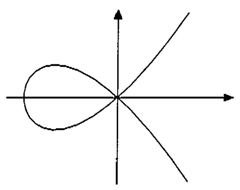
  In the degenerate case, that is, when f is reducible, we obtain pairs of lines.
- The example where $V(x) = V(x^2)$, demonstrates that the equations defining a given algebraic set are not uniquely determined.

The Nodal Cubic Curve

- The **nodal cubic curve** is defined by

$$C: \quad y^2 = x^3 + x^2, \quad x, y \in \mathbb{R}.$$

It has a "double point" at the origin.



Moreover, it can be parameterized as

$$\begin{array}{rrcl} \varphi: & \mathbb{R} & \to & \mathbb{R}^2; \\ & t & \mapsto & (t^2 - 1, t^3 - t). \end{array}$$

We have $\varphi(\mathbb{R}) = C$.

This map is injective, with the exception of $\varphi(1) = \varphi(-1) = (0,0)$.

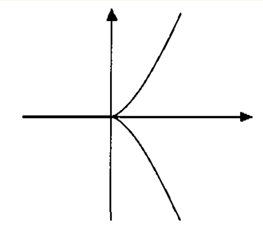
The Semicubical Parabola

- The **semicubical parabola**, also known as **Neile's parabola**, or as a **cuspidal cubic**, is given by the equation

  $$C: \quad y^2 = x^3, \quad x, y \in \mathbb{R}.$$

  This curve also admits a parametrization

  $$\begin{array}{rcl} \varphi : \mathbb{R} & \to & \mathbb{R}^2; \\ t & \mapsto & (t^2, t^3). \end{array}$$

  φ gives a bijection between $\mathbb{R}$ and C.

  However the partial derivatives of φ vanish at the origin, which is called a "cusp" of C.

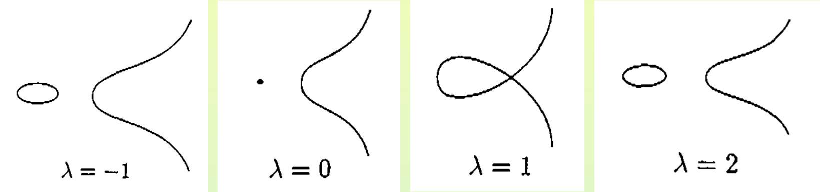
- In these examples the double point and the cusp are "singular" points on the curves. All other points are "smooth" (or "regular").

A Family of Plane Cubics

- We consider a family of plane cubics given by

$$C_\lambda : \quad y^2 = x(x-1)(x-\lambda) \quad \lambda \in \mathbb{R}.$$

- For $\lambda = 0$ and 1, we have a curve with a double point (at least over the complex numbers), and otherwise C_λ is smooth.



- Over $\mathbb{R}$, the curve C_1 has a rational parametrization.
- Over $\mathbb{C}$, both C_0 and C_1 have rational parametrizations.
- On the other hand, we will show that, for $\lambda \neq 0, 1$, the smooth curve C_λ does not have a rational parametrization over either $\mathbb{R}$ or $\mathbb{C}$.
- Thus, the latter behave very differently from C_0 and C_1.

A Technical Lemma

Lemma

Let $p, q \in \mathbb{C}[t]$ be coprime. If there are four distinct values of the ratio $\frac{\lambda}{\mu} \in \mathbb{C} \cup \{\infty\}$, such that $\lambda p + \mu q$ is a square in $\mathbb{C}[t]$, then $p, q \in \mathbb{C}$.

- We will use Fermat's method of infinite descent.

  The hypotheses are unchanged by a linear transformation

  $$p' = \alpha p + \beta q, \quad q' = \gamma p + \delta q, \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{Gl}(2, \mathbb{C}).$$

  Suppose that the result is false.

  Let $\{p, q\}$ be a counterexample with $\max\{\deg p, \deg q\}$ minimal.

  By a linear transformation, we can assume that the 4 ratios in question are $0, 1, \infty$ and λ, for some $\lambda \in \mathbb{C}$.

  That is $p, q, p - q, p - \lambda q \in \mathbb{C}[t]$ are squares.

A Technical Lemma (Cont'd)

- So $p = u^2$ and $q = v^2$ for some coprime u and v.

  Clearly
  $$\max\{\deg u, \deg v\} < \max\{\deg p, \deg q\}.$$
  For $\mu^2 = \lambda$, we have
  $$\begin{aligned} p - q &= u^2 - v^2 = (u - v)(u + v); \\ p - \lambda q &= u^2 - \lambda v^2 = (u - \mu v)(u + \mu v). \end{aligned}$$
  So $u - v, u + v, u - \mu v, u + \mu v$ are all squares.

  But then $\{w, v\}$ is also a counterexample.

  This contradicts the minimality of $\{p, q\}$.

Non-Parametrizability of $C_\lambda, \lambda \neq 0, 1$

Proposition

Let $k \in \{\mathbb{R}, \mathbb{C}\}$, and let $f, g \in k(t)$ be rational functions such that

$$g^2 = f(f-1)(f-\lambda), \quad \lambda \neq 0, 1.$$

Then f and g are constant, i.e., $f, g \in k$.

- Suppose

$$f = \frac{p}{q} \quad \text{and} \quad g = \frac{r}{s},$$

where r, s and $p, q \in k[t]$ are pairs of coprime polynomials.
After we multiply through by the denominators q and s, we get

$$\frac{r^2}{s^2} = \frac{p}{q} \frac{p-q}{q} \frac{p-\lambda q}{q}$$

$$r^2 q^3 = s^2 p(p-q)(p-\lambda q).$$

Non-Parametrizability of $C_\lambda, \lambda \neq 0,1$ (Cont'd)

- We got $r^2q^3 = s^2p(p-q)(p-\lambda q)$.
  Thus $s^2 \mid q^3$. Since p and q are coprime, we also have $q^3 \mid s^2$.
  So $s^2 = aq^3$, for some $a \in k$. Additionally, $aq = (\frac{s}{q})^2 \in k[t]$ is a square.
  Multiplying the preceding equation by a and dividing by s^2 gives
  $$r^2 = ap(p-q)(p-\lambda q).$$
  The right hand side is a square.
  Moreover, p and q are coprime.
  Hence, there must exist $b, c, d \in k$, such that $bp, c(p-q), d(p-\lambda q)$ are all squares in $k[t]$.
  By the lemma, $p, q \in k$. It follows that $f \in k$.
  We now get $g \in k$.

Parametrizability of $C_\lambda, \lambda \neq 0, 1$

Corollary

For $\lambda \neq 0, 1$, there is no nonconstant rational map

$$(f, g) : k \to C_\lambda, \quad f, g \in k(t).$$

In particular, there is no rational parametrization of C_λ for $\lambda \neq 0, 1$.

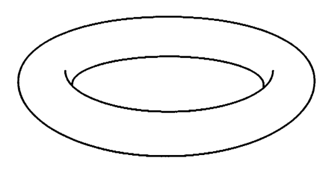
- C_λ is "rational" if and only if $\lambda = 0$ or 1.
- Over $\mathbb{C}$, there is an explicit parametrization in terms of meromorphic functions, which we develop next.

The Complex Curves $C_\lambda^{\mathbb{C}}$ and $\overline{C}_\lambda^{\mathbb{C}}$

- Consider the complex curves

$$\begin{aligned} C_\lambda^{\mathbb{C}} &= \{(x,y)\in\mathbb{C}^2 : y^2 = x(x-1)(x-\lambda)\}\subseteq\mathbb{C}^2;\\ \overline{C}_\lambda^{\mathbb{C}} &= C_\lambda^{\mathbb{C}}\cup\{\infty\}\subseteq\mathbb{C}^2\cup\{\infty\}\subseteq\mathbb{P}^2_{\mathbb{C}}, \end{aligned}$$

  where $\mathbb{P}^2_{\mathbb{C}}$ is the projective plane.
- The complex curve $\overline{C}_\lambda^{\mathbb{C}}$ may also be considered as a Riemann surface homeomorphic to a torus,



Homeomorphism of $\overline{C}_\lambda^{\mathbb{C}}$ and the Torus I

- Consider the projection

$$\begin{array}{rccl} \pi: & \overline{C}_\lambda^{\mathbb{C}} & \to & \mathbb{C} \cup \{\infty\} = S^2 \\ & (x,y) & \mapsto & x \\ & \infty & \mapsto & \infty. \end{array}$$

- This defines a 2:1 map, which corresponds to the projection of the graph of

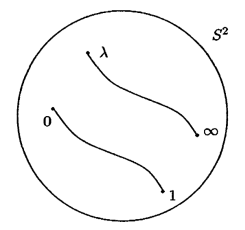
$$y = \pm\sqrt{x(x-1)(x-\lambda)}$$

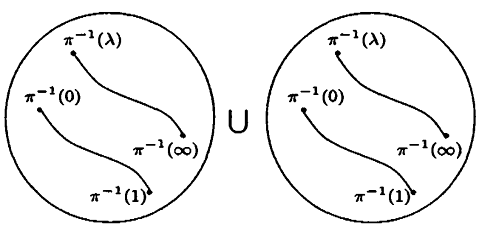
to the x-axis.

- Every point $x \in \mathbb{C} \cup \{\infty\}$ has two preimages, except for $0, 1, \lambda$ and ∞.

$\overline{C}_{\lambda}^{\mathbb{C}}$ and the Torus II

- We cut the sphere S^2 along two paths.





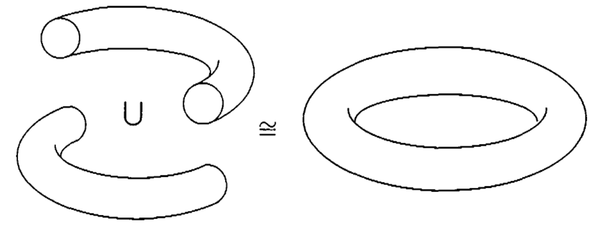
For every $x \in S^2 \backslash \{0, 1, \lambda, \infty\}$, $\pi^{-1}(x) \subseteq \overline{C}_{\lambda}^{\mathbb{C}}$ consists of two points.

Hence, the preimage under π^{-1} of S^2 minus the two paths connecting $0, 1$ and λ, ∞ decomposes into two disjoint components, each of which can be identified via π with S^2 minus the two given paths.

Each of these components is homeomorphic to "half a torus".

$\overline{C}_\lambda^{\mathbb{C}}$ and the Torus III

- If the slits are opened out to form the open ends of the "half tori", we obtain



The boundary of each piece is homeomorphic to two copies of S^1.

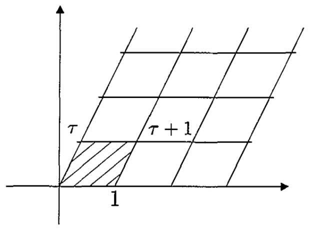
Each copy is equal to the preimage of one of the given paths in S^2.

The simultaneous inclusion of the preimage of each path in both components corresponds to gluing together the boundary circles.

The end result is a torus.

Another Definition of a Torus

- For any point $\tau \in \mathbb{C}$ in the upper half plane, i.e., with $\text{Im}\tau > 0$, there is a corresponding lattice,

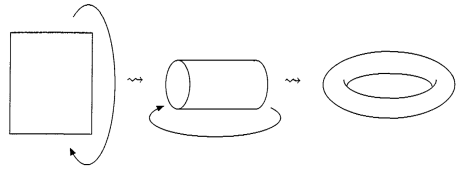


$$\Lambda_\tau := \mathbb{Z} + \mathbb{Z}\tau = \{m + n\tau : m, n \in \mathbb{Z}\}.$$

The quotient $E_\tau := \mathbb{C}/\Lambda_\tau$ is an abelian group.

It is also a topological space (with the quotient topology inherited from $\mathbb{C}$), with the structure of a compact Riemann surface.

Topologically E_τ is a torus



The Weierstaß $\wp$-Function

- To show that E_τ is isomorphic to the torus, we use the Weierstraß $\wp$-function

$$\wp(z) := \frac{1}{z^2} + \sum_{(m,n)\neq(0,0)} \left(\frac{1}{(z-(m\tau+n))^2} - \frac{1}{(m\tau+n)^2} \right).$$

- This is a meromorphic function on $\mathbb{C}$ which has poles of order 2 exactly at the lattice points in Λ_τ.
- Moreover, $\wp$ is periodic with respect to Λ_τ.
- That is, for all $z \in \mathbb{C}$, we have

$$\wp(z+w) = \wp(z), \quad \text{for all } w \in \Lambda_\tau.$$

The Weierstaß ℘-Function and a Plane Cubic

- It is well known that the Weierstraß ℘-function satisfies the differential equation
$$(\wp')^2 = 4\wp^3 - g_2\wp - g_3,$$
where
$$g_2 = 60 \sum_{(m,n)\neq(0,0)} \frac{1}{(m\tau+n)^4} \quad \text{and} \quad g_3 = 140 \sum_{(m,n)\neq(0,0)} \frac{1}{(m\tau+n)^6}$$
are complex numbers.
- We now consider the plane cubic and the projective curves
$$\begin{aligned} C_{g_2,g_3}^{\mathbb{C}} &= \{(x,y)\in\mathbb{C}^2 : y^2 = 4x^3 - g_2x - g_3\}; \\ \overline{C}_{g_2,g_3}^{\mathbb{C}} &= \{(x,y)\in\mathbb{C}^2 : y^2 = 4x^3 - g_2x - g_3\} \cup \{\infty\} \subseteq \mathbb{P}_{\mathbb{C}}^2. \end{aligned}$$

A Plane Cubic and a Projective Curve

- The Weierstraß $\wp$ function and its derivative give rise to a map

$$\varphi = (\wp, \wp') : \begin{array}{ccc} \mathbb{C} \setminus \Lambda_\tau & \to & C^{\mathbb{C}}_{g_2,g_3}; \\ z & \mapsto & (\wp(z), \wp'(z)). \end{array}$$

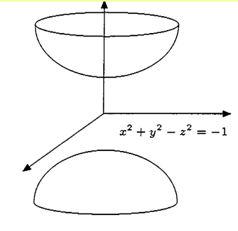
- φ has a continuation to $\mathbb{C}$, $\overline{\varphi} = (\wp, \wp') : \mathbb{C} \to \overline{C}^{\mathbb{C}}_{g_2,g_3}$, given by setting

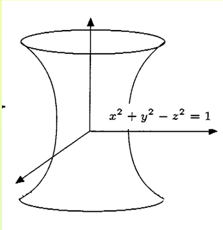
$$\overline{\varphi}(x) = \infty, \quad \text{for all } x \in \Lambda_\tau.$$

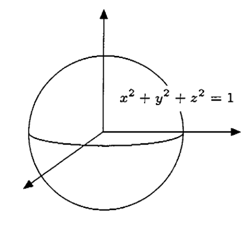
- The map $\wp$, and thus also $\wp'$, is periodic with respect to Λ_τ.
- So we get a map $\widetilde{\varphi} : E_\tau \to \overline{C}^{\mathbb{C}}_{g_2,g_3}$.
- One can show that this map is a bijection.
- A linear transformation of coordinates takes the curve $\overline{C}^{\mathbb{C}}_{g_2,g_3}$ to the curve $\overline{C}^{\mathbb{C}}_{\lambda}$ for a suitable choice of λ.
- Every curve $\overline{C}^{\mathbb{C}}_{\lambda}$, with $\lambda \neq 0, 1$, can be obtained in this way.

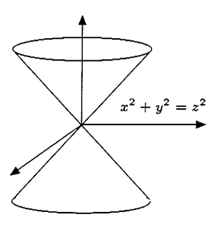
Quadratic Hypersurfaces

- Other higher dimensional examples are given by the quadratic hypersurfaces in $\mathbb{R}^3$ shown below:









A Determinantal Variety

- Consider the map

$$\begin{array}{rcl}\varphi : \mathbb{A}^1 & \to & \mathbb{A}^3, \\ t & \mapsto & (t, t^2, t^3).\end{array}$$

- The image $C = \varphi(\mathbb{A}^1)$ is an algebraic set, since C can be given as the intersection of two quadrics $C = Q_1 \cap Q_2$, where

$$\begin{array}{rrcl} Q_1 : & x_1^2 - x_2 & = & 0. \\ Q_2 : & x_1 x_2 - x_3 & = & 0.\end{array}$$

- We can also write C as a **determinantal variety**

$$C = \left\{ (x_1, x_2, x_3) \in \mathbb{R}^3 : \operatorname{rank} \begin{pmatrix} 1 & x_1 & x_2 \\ x_1 & x_2 & x_3 \end{pmatrix} < 2 \right\}.$$

The General Linear Group

- Another example of an algebraic set is the general linear group

$$\mathrm{Gl}(n,k) := \{A \in \mathrm{Mat}(n \times n, k) : \det A \neq 0\}.$$

- To see that $\mathrm{Gl}(n,k)$ is an algebraic set, we consider affine space $\mathbb{A}^{n^2+1}$ with coordinates $(x_{ij})_{1 \leq i,j \leq n}$ and t.
- The set

$$V := \{(x_{ij}, t) \in \mathbb{A}^{n^2+1} : \det(x_{ij})t - 1 = 0\}$$

  is clearly an algebraic set.
- The map

$$\begin{array}{rccc} \varphi : & \mathrm{Gl}(n,k) & \to & V; \\ & A = (a_{ij}) & \mapsto & ((a_{ij}), \frac{1}{\det A}) \end{array}$$

  defines a bijection from $\mathrm{Gl}(n,k)$ to V.
- This proves that $\mathrm{Gl}(n,k)$ is algebraic.

The General Linear Group

- Consider the multiplication map

$$\begin{array}{rrcl} \mu : & \mathrm{Gl}(n,k) \times \mathrm{Gl}(n,k) & \to & \mathrm{Gl}(n,k); \\ & (A,B) & \mapsto & AB. \end{array}$$

- Consider, also, the inverse map

$$\begin{array}{rrcl} \iota : & \mathrm{Gl}(n,k) & \to & \mathrm{Gl}(n,k); \\ & A & \mapsto & A^{-1}. \end{array}$$

- They are given in terms of the matrix entries by polynomial and rational maps respectively.
- Thus, $\mathrm{Gl}(n,k)$ is an *algebraic group*.

The General Linear Group is an Algebraic Group

- An **algebraic group** is an algebraic set which is also a group, and such that the group multiplication and inversion are given by rational functions.
- Further examples include:
  - The special linear group $\mathrm{Sl}(n, k)$;
  - The orthogonal group $O(n, k)$;
  - The symplectic group $\mathrm{Sp}(2n, k)$;
  - The torus E_τ.

The Fermat Curve

- The Fermat curve, given, for a positive integer n, by

$$F_n^{\mathbb{Q}} := \{(x,y,z) \in \mathbb{Q}^3 : x^n + y^n = z^n\}$$

  is a famous example of an algebraic set.
- A few points on this curve can be given immediately, e.g.:
  - $(1,0,1)$ and $(0,1,1)$, for all n;
  - $(1,-1,0)$, if n is odd;
  - $(1,0,-1)$ and $(0,1,-1)$, if n is even.
- Any rational multiple of any of these points is also a point on $F_n^{\mathbb{Q}}$.
- Fermat's Last Theorem states that these are the only points on $F_n^{\mathbb{Q}}$, for $n \geq 3$.

Theorem (Wiles, 1995)

There is no solution $(x,y,z) \in F_n^{\mathbb{Q}}$, with $xyz \neq 0$, for $n \geq 3$.

Diophantine Problems

- Fermat's Problem is a typical example of a **Diophantine problem**.
- If $n = 2$, then there are infinitely many nontrivial integral triples $(x, y, z) \in \mathbb{Z}^3$, with

$$x^2 + y^2 = z^2,$$

  known as **Pythagorean triples**.
- The distinction between $n = 2$ and $n \geq 3$ lies in the fact that $F_2^{\mathbb{C}}$ can be rationally parametrized, which is not the case for $F_n^{\mathbb{C}}$, when $n \geq 3$.

The Ground Field

- The problem of determining the solutions of a system of polynomial equations depends to a considerable extent on the ground field.

  Example: Consider the equation

  $$x^2 + y^2 + 1 = 0.$$

  It has no solution over $\mathbb{R}$.

  But over $\mathbb{C}$, or over any algebraically closed field, every nonconstant polynomial defines a nonempty algebraic set.

General Assumption

The ground field k is algebraically closed, i.e., $k = \overline{k}$.