Chapter 1
Algebraic sets

Notation

- k – alg closed base field ($\mathbb{C}$, $\overline{\mathbb{Q}}$, $\overline{\mathbb{F}}_p$)
- $\mathbb{A}^n$ (or $\mathbb{A}^n_k$) – n-dimensional affine space over k

as a set it is k^n, but $\mathbb{A}^n$ has more structure: it is a topological space (discuss later).

§ Algebraic sets

def. A (closed) algebraic set is a subset of $\mathbb{A}^n$, defined by polynomial equations.

$$S \subseteq k[x_1, .., x_n] \quad \rightsquigarrow \underbrace{Z(S)}_{\text{zero locus}} := \{x \in \mathbb{A}^n \mid f(x) = 0 \ \forall f \in S\}$$

Rem. 1). $Z(S) = Z(\mathfrak{a})$, where $\mathfrak{a}$ is the ideal generated by $f \in S$, since $f(x) = 0, g(x) = 0 \Rightarrow (f+g)(x) = 0$, $(\lambda \cdot f)(x) = 0$. We prefer ideals!

2) $\forall S \subseteq k[x_1, .., x_n] \quad \exists$ finite $S' \subset k[x_1, .., x_n]$: $Z(S) = Z(S')$, since every ideal is finitely generated by Hilbert's basis thm.

Ex. 1 algebraic sets in $\mathbb{A}^1$

$S \subseteq k[x]$ – PID $\Rightarrow Z(S) = Z(f(x)) = Z(a(x-\alpha_1) \cdot \ldots \cdot (x - \alpha_m))$,

so every algebraic set in $\mathbb{A}^1$ is either $\mathbb{A}^1$, or a finite set of points (possibly empty).

$n=2$: $S \subseteq k[x,y]$. What are $Z(x,y)$ and $Z(x\cdot y)$?

Let's draw some algebraic curves! But beware:

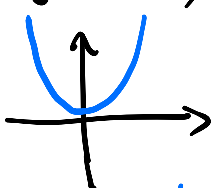
NB: 1) When you draw graphs of functions, you usually think about solutions $/\mathbb{R}$, which may be quite different $/\mathbb{C}$ even if coeffs of equations are real, e.g. $Z(x^2+1)$.

2) Dimension change:

$\mathbb{A}^n_{\mathbb{C}}$ as a real manifold is $\mathbb{R}^{2n}$.

② Conics in $\mathbb{A}^2$:

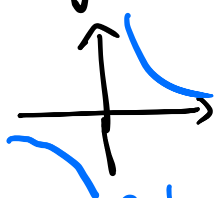
$Z(y-x^2)$



parabola

(pictures over $\mathbb{R}$)

$Z(xy-1)$



hyperbola

In fact, if $S=\{f(x,y)\}$ is any irreducible quadratic polynomial, then over $k=\bar{k}$ one can find a linear change of coords s.t. you get the parabola or the hyperbola.

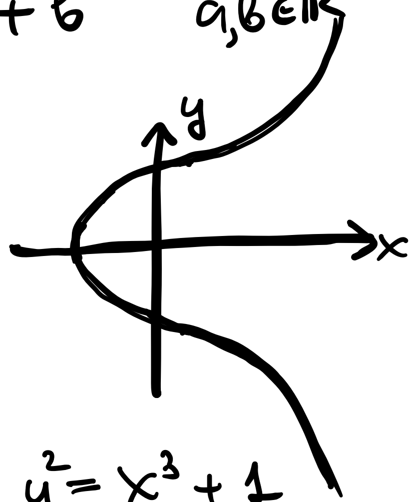
This classification of conics in $\mathbb{A}^2$ uses that $k=\bar{k}$:

$$\underset{\text{circle}}{x^2+y^2=1} \underset{y\mapsto iy}{\rightsquigarrow} \underset{\text{hyperbola}}{x^2-y^2=1}$$

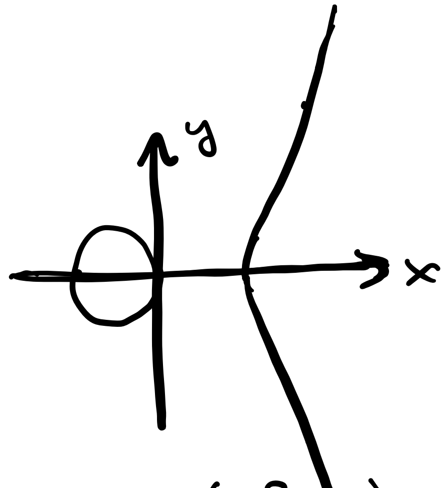
③ elliptic curves

$y^2 = x^3 + ax + b \quad a,b \in \mathbb{R}$

real points:



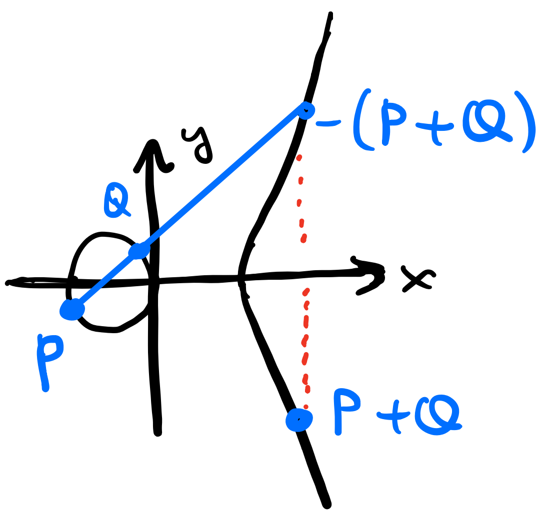
$y^2 = x^3 + 1$



$y^2 = x(x^2 - 1)$

Elliptic curves give applications of AG to real world: they are used in cryptography!

All thanks to the addition law on E, which can be geometrically depicted as follows:



(neutral element is the point at ∞ which isn't visible on the affine pic)

④ twisted cubic (affine)

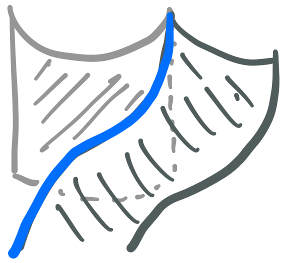
a curve in $\mathbb{A}^3$ which is not contained in $\mathbb{A}^2$:

$$C := \mathrm{Im}\left(\mathbb{A}^1 \xrightarrow{\varphi} \mathbb{A}^3\right) \quad \text{for} \quad \varphi(t) = (t, t^2, t^3).$$

As a closed algebraic set:

$$C = Z\left((y - x^2, z - x^3)\right) \subset \mathbb{A}^3.$$

(more about it in Exercises)



attempt of a 3-dimensional picture :)

Prop. (Properties of algebraic sets)

$\mathfrak{a}, \mathfrak{b} \subseteq k[x_1, \dots, x_n]$ ideals. Then:

1) $\mathfrak{a} \subseteq \mathfrak{b} \Rightarrow Z(\mathfrak{b}) \subseteq Z(\mathfrak{a})$
2) $Z(\mathfrak{a} + \mathfrak{b}) = Z(\mathfrak{a}) \cap Z(\mathfrak{b})$
3) $Z(\mathfrak{a} \cdot \mathfrak{b}) = Z(\mathfrak{a} \cap \mathfrak{b}) = Z(\mathfrak{a}) \cup Z(\mathfrak{b})$
4) $Z(\mathfrak{a}) = Z(\sqrt{\mathfrak{a}})$, where

$\sqrt{\mathfrak{a}} := \{ f \mid f^r \in \mathfrak{a} \text{ for some } r > 0 \}$ is the radical of $\mathfrak{a}$.

Proof: straightforward (check!), e.g.:

4): $Z(\sqrt{\mathfrak{a}}) \subseteq Z(\mathfrak{a})$ by 1) since $\mathfrak{a} \subseteq \sqrt{\mathfrak{a}}$

$Z(\mathfrak{a}) \subseteq Z(\sqrt{\mathfrak{a}})$ because for $x \in Z(\mathfrak{a})$ and $f \in \sqrt{\mathfrak{a}}$ holds $f^r(x) = 0$ for some $r \Rightarrow f(x) = 0 \Rightarrow x \in Z(\sqrt{\mathfrak{a}})$.

§ Nullstellensatz

$$\boxed{\text{ideals in } k[x_1, .., x_n]} \longleftrightarrow \boxed{\text{subsets in } \mathbb{A}^n}$$

$$\mathfrak{a} \longmapsto Z(\mathfrak{a}) = \left\{ x \mid f(x) = 0 \ \forall f \in \mathfrak{a} \right\}$$

$$\left\{ f \mid f(x) = 0 \ \forall x \in X \right\} = I(X) \longleftarrow X$$

ideal defined by a set

inclusion-reversing maps

This is NOT a bijection!

For example, $Z(x) = Z(x^2) = \{0\} \in \mathbb{A}^1$.

However, the maps $I(-)$ and $Z(-)$ induce a bijection:

$$\boxed{\begin{array}{l}\text{radical ideals} \\ \text{in } k[x_1, .., x_n], \\ \text{i.e. } \mathfrak{a} = \sqrt{\mathfrak{a}}\end{array}} \longleftrightarrow \boxed{\begin{array}{l}\text{algebraic sets} \\ \text{in } \mathbb{A}^n\end{array}}$$

inclusion-reversing bijection

This is thanks to

classical fact from commutative algebra

Thm (Hilbert's Nullstellensatz)

k alg. closed, $\mathfrak{a} \subset k[x_1, .., x_n]$ ideal. Then

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

Rem. false for non-alg. closed k,
e.g. over $\mathbb{R}$ we have
$$Z(x^2+1) = \emptyset \Rightarrow I(Z(x^2+1)) = k[x].$$

We recall the weaker forms of this theorem.

Cor. (Weak Nullstellensatz I)
k alg closed, $\mathfrak{a} \subsetneq k[x_1,..,x_n]$ ideal. Then $Z(\mathfrak{a})$ is non-empty.

Equivalently (check!):

Cor. (Weak Nullstellensatz II)
k alg closed. Then maximal ideals in $k[x_1,..,x_n]$ are exactly those of the form
$m = (x_1 - a_1, .., x_n - a_n)$, i.e. $Z(m) = \{(a_1,..,a_n)\}$ for some $a_1, ..., a_n \in k$.

Next time: some basic topology,
repeat: what a top. space, basis of open nbhds,...

§ Polynomial functions

def. $X \subseteq \mathbb{A}^n$ an algebraic set. The ring

$$k[X] := k[x_1, .., x_n] / I(X)$$

is the <u>coordinate ring</u> of X.

How to think about it:

- $f \in k[x_1, .., x_n]$ is a function $\mathbb{A}^n \to k$
- $f, g \in k[x_1, \ldots, x_n]$, then

$$f|_X = g|_X \iff f - g \in I(X)$$

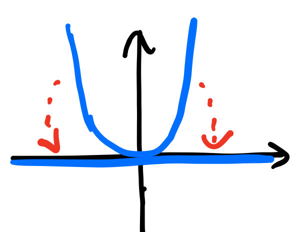
- hence, elements of $k[X]$ are <u>polynomial functions</u> $X \to k$.

(later we will call them „regular" functions)

Ex: $X = Z(y - x^2) \Rightarrow$

$$k[X] = k[x, y] / (y - x^2) \cong k[x]$$

So, functions on a parabola are the same as functions on a line:



For X an algebraic set, we have an induced bijection:

$$\{\text{radical ideals in } k[X]\} \leftrightsquigarrow \{\text{algebraic subsets of } X\}$$