1. Affine varieties

Recall: want to study the solution sets of systems of polynomial equations.

We work over a fixed alg. closed field k

ground field

$k = \mathbb{R}$, $\mathbb{F}_q$ finite field ✗

$k = \mathbb{C}$, $\overline{\mathbb{F}_q}$, ... ✓

Why alg. closed?

E.g. one variable, one equation

$f(x) = 0$
$\deg f = d \geq 1$ $\longrightarrow$ over $k = \overline{k}$: d solutions counted with multiplicity

over $k \neq \overline{k}$: ?

Recall:

- Affine n-space over k:

$$\mathbb{A}^n(k) = \mathbb{A}^n = \{(\underset{\substack{\cap \\ k}}{a_1}, \dots, \underset{\substack{\cap \\ k}}{a_n}) \in k^n\}$$

$\bullet$ A polynomial with coefficients in k in $\overbrace{x_1, \dots, x_n}^{\text{indeterminates}}$ is an expression of the form

$$f(x_1, \dots, x_n) = \sum_{\underline{I} = (i_1, \dots, i_n) \in \mathbb{N}^n} c_I \cdot \overbrace{x_1^{i_1} \cdots x_n^{i_n}}^{=: x^I} \quad \text{with } c_I \in k$$

$c_I = 0$ for all but finitely many I

$\bullet$ $k[x_1, \dots, x_n] := \{\text{polyn. in } x_1, \dots, x_n \text{ with } k\text{-coeff.}\}$

$+, \cdot$

<u>polynomial ring</u>

Def. $S \subset k[x_1, \dots, x_n]$

The zero set (or: vanishing locus) of S is

$$\mathbb{V}(S) = \mathcal{Z}(S) := \{p \in \mathbb{A}^n : f(p) = 0 \text{ for all } f \in S\} \subset \mathbb{A}^n$$

Subsets of $\mathbb{A}^n$ of the form $\mathbb{V}(S)$ are called (affine) algebraic sets.

Notation: for $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ we write

$$\mathbb{V}(f_1, \dots, f_m) := \mathbb{V}(\{f_1, \dots, f_m\}) =$$

$$= \{p \in \mathbb{A}^n \mid f_1(p) = \cdots = f_m(p) = 0\}.$$

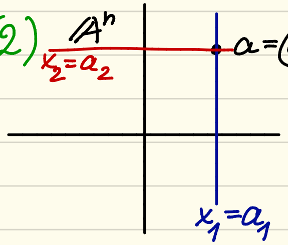
Examples:

(1) $1 \in k[x_1,\dots,x_n]$ $\quad \mathbb{V}(1)=\emptyset$

$0 \in k[x_1,\dots,x_n]$ $\quad \mathbb{V}(0)=\mathbb{A}^n$

the empty set and the whole space are algebraic sets

(2)



$\{a\}=\mathbb{V}(x_1-a_1, x_2-a_2, \dots, x_n-a_n)$

points are algebraic subsets

(3) All affine subspaces in $\mathbb{A}^n$ are algebraic sets.

(4) Curves in the affine plane $\mathbb{A}^2$.

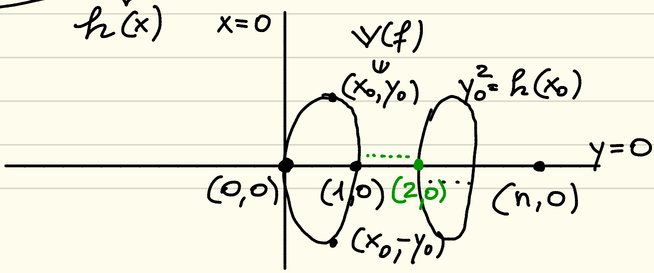
$f(x,y)\in k[x,y]$ non-constant polynomial

$\mathbb{V}(f) = \{f=0\}$ is an algebraic curve

E.g. • $f(x,y)=x^2+y^2-1$ $\quad \mathbb{V}(f)$ unit circle

• $f(x,y)=\underbrace{x(x-1)(x-2)\cdots(x-n)}_{h(x)}-y^2$

char $k\neq 2$



(5) If $X \subset \mathbb{A}^m$ and $Y \subset \mathbb{A}^n$ are alg. subsets, then $X \times Y \subset \mathbb{A}^m \times \mathbb{A}^n \cong \mathbb{A}^{m+n}$ is an alg. subset.
EXERCISE.

Remark: The set S defining the alg. subset $X = \mathbb{V}(S)$ is not unique. For instance:
- if f and g vanish on X, then $f+g$ vanishes on X
- if f vanishes on X, then hf vanishes on X for all $h \in k[x_1, \dots, x_n]$.

In particular, we have

$\mathbb{V}(S) = \mathbb{V}((S))$ $\qquad$ (S): ideal gen'd by S

$$(S) = \{h_1 f_1 + \cdots + h_r f_r \mid r \in \mathbb{N},\ f_1, \dots, f_r \in S,\ h_1, \dots, h_r \in k[x_1, \dots, x_n]\}$$

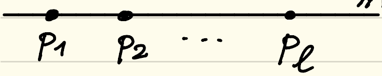
Recall: R ring (i.e. commutative ring with unity)
- an ideal $\mathfrak{I}$ is a subset $\mathfrak{I} \subset R$ closed under addition and satisfying $\underbrace{R \cdot \mathfrak{I} \subset R}$

i.e. $\alpha\beta \in \mathfrak{I}$ for all $\alpha \in R$ and $\beta \in \mathfrak{I}$

- (S) is the smallest ideal containing S
- ideals of the form (f) for some $f \in R$ are called principal ideals.

Example: Algebraic subsets in $\mathbb{A}^1$

Alg. subsets in $\mathbb{A}^1$ are: $\overset{\mathbb{V}(1)}{\overset{\shortparallel}{\emptyset}}$, finite sets of points, $\overset{\mathbb{V}(0)}{\overset{\shortparallel}{\mathbb{A}^1}}$



$\mathbb{A}^1 = k$

$$\{p_1, \dots, p_\ell\} = \mathbb{V}\big((x_1 - p_1)\cdot(x_2 - p_2)\cdots(x_\ell - p_\ell)\big) = \mathbb{V}(f)$$

All alg. subsets are of the form $\mathbb{V}(J)$ with $J \subset k[x]$ an ideal.

CA: $k[x]$ is a <u>principal ideal domain</u>: all ideals are principal.

Hence if $X \subset \mathbb{A}^1$ is an alg. subset, we have

$X = \mathbb{V}((f)) = \mathbb{V}(f)$ with $f \in k[x]$

Then $\deg f = 0 \implies X = \emptyset$ or $\mathbb{A}^1$

$\deg f = d \geq 1 \implies X$ consists of d points

However, $k[x_1, \dots, x_n]$ is <u>not</u> a PID if $n \geq 2$.

Hence in general we will need more than just one polynomial to define an alg. subset $X \subset \mathbb{A}^n$.

Is it enough to work with finitely many polynomials?

Answer from commutative algebra:

Lemma The following conditions are equivalent for a commutative ring R:

(*) every ideal in R is finitely generated

(ACC) ascending chain condition: every ascending chain of ideals in R is stationary, i.e.,

for all chains $I_1 \subset I_2 \subset I_3 \subset \dots \subset I_n \subset I_{n+1} \subset \dots$
with $I_j \subset R$ ideal
there is an N s.th. $I_m = I_N$ for all $m \geq N$.

Def. If R satisfies (ACC), then R is called Noetherian.

Thm (Hilbert basis theorem) If R is Noetherian, then $R[x]$ is Noetherian.

Cor. $k[x_1, \dots, x_n]$ is Noetherian.

In particular, every alg. set in $\mathbb{A}^n$ can be defined by the vanishing of finitely many polynomials.

Set-theoretical properties of alg. sets

Lemma If S_1, S_2 are sets of polynomials, then

$$\mathbb{V}(S_1) \cup \mathbb{V}(S_2) = \mathbb{V}(S_1 \cdot S_2)$$

with $S_1 \cdot S_2 = \{fg \mid f \in S_1,\ g \in S_2\}$.

Furthermore, for all families $\{S_i\}_{i \in I}$ with $S_i \subset k[x_1, \dots, x_n]$ we have:

$$\bigcap_{i \in I} \mathbb{V}(S_i) = \mathbb{V}\Big(\bigcup_{i \in I} S_i\Big).$$

Cor. Finite unions of alg. sets and arbitrary intersections of alg. sets are again algebraic.

Pf of lemma:
$S_1, S_2 \subset k[x_1, \dots, x_n]$

"$\subset$" $p \in \mathbb{V}(S_1) \cup \mathbb{V}(S_2)$, let $h \in S_1 S_2$.
Then $h = fg$ with $f \in S_1$, $g \in S_2$ and we have

$$h(p) = f(p)g(p) = \begin{cases} 0 \cdot g(p) = 0 & \text{if } p \in \mathbb{V}(S_1) \\ f(p) \cdot 0 = 0 & \text{if } p \in \mathbb{V}(S_2) \end{cases}$$

Hence $p \in \mathbb{V}(S_1 S_2)$.

"$\supset$" Let us assume $p \notin \mathbb{V}(S_1) \cup \mathbb{V}(S_2)$. Then there exist $f \in S_1$ and $g \in S_2$ s.th. $f(p) \neq 0$, $g(p) \neq 0$. Hence $(fg)(p) = f(p) \cdot g(p) \neq 0$, which implies $p \notin \mathbb{V}(S_1 S_2)$
$\square$

Def. Algebraic subsets satisfy the axioms for the closed subsets of a topology on $\mathbb{A}^n$.
We call this topology the Zariski topology.

Rem. The Zariski topology is not Hausdorff.
Take the case of $\mathbb{A}^1$. Let us take distinct points $p, q \in \mathbb{A}^1$

Every open subset containing p is of the form

$$U_p = \mathbb{A}^1 \setminus \{p_1, \dots, p_r\} \qquad p_1, \dots, p_r \neq p$$

and all open subsets containing q are of the form

$$U_q = \mathbb{A}^1 \setminus \{q_1, \dots, q_s\} \qquad q_1, \dots, q_s \neq q$$

Hence $U_p \cap U_q = \underbrace{\mathbb{A}^1}_{\text{infinite set}} \setminus \{\underbrace{p_1, \dots, p_r, q_1, \dots, q_s}_{\leq r+s \text{ points}}\} \neq \emptyset$