1. Affine varieties

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

We work over a fixed alg. closed field \( k \)

\[ k = \mathbb{R}, \quad \mathbb{F}_q \text{ finite field} \]

\[ k = \mathbb{C}, \quad \mathbb{F}_q, \ldots \]

Why alg. closed?

E.g. one variable, one equation

\[ f(x) = 0 \rightarrow \text{over } k = \overline{k}: \text{ d solutions counted with multiplicity} \]

\[ \text{over } k \neq \overline{k}: \quad ? \]

Recall:

- Affine n-space over \( k \):

\[ \mathbb{A}^n(k) = \mathbb{A}^n = \left\{ (a_1, \ldots, a_n) \in k^n \right\} \]
A polynomial with coefficients in \( k \) in \( x_1, \ldots, x_n \) is an expression of the form

\[
f(x_1, \ldots, x_n) = \sum_{I = (i_1, \ldots, i_n) \in \mathbb{N}^n} c_I x_1^{i_1} \cdots x_n^{i_n} \quad \text{with} \quad c_I \in k \quad \text{and} \quad c_I = 0 \text{ for all but finitely many } I.
\]

\[ k[x_1, \ldots, x_n] = \{ \text{polyn. in } x_1, \ldots, x_n \text{ with } k \text{- coeff.} \} +, \cdot \]

**Polynomial Ring**

**Def.** \( S \subseteq k[x_1, \ldots, x_n] \)

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

\[
V(S) = \mathbb{Z}(S) = \{ p \in \mathbb{A}^n \mid f(p) = 0 \text{ for all } f \in S \} \subseteq \mathbb{A}^n
\]

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

**Notation:** for \( f_1, \ldots, f_m \in k[x_1, \ldots, x_n] \) we write

\[
V(f_1, \ldots, f_m) = \bigcap \{ f \mid f(p) = 0 \} = \{ p \in \mathbb{A}^n \mid f_1(p) = \cdots = f_m(p) = 0 \}.
\]
Examples:

(1) \( 1 \in k[x_1,\ldots,x_n] \quad \forall (1) = \emptyset \) the empty set and
the whole space

\( 0 \in k[x_1,\ldots,x_n] \quad \forall (0) = \mathbb{A}^n \) are algebraic sets

(2) \( \mathbb{A}^n_{x_2=a_2} \)

\( \{a\} = \forall (x_1-a_1, x_2-a_2,\ldots, x_n-a_n) \) 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

\( \forall (f) = \{f=0\} \) is an algebraic curve

E.g. \( f(x,y) = x^2+y^2-1 \) \( \forall (f) \) unit circle

\( f(x,y) = x(x-1)(x-2)\ldots(x-n)-y^2 \)

\( \forall (f) \) unit circle

\( \text{char } k \neq 2 \)
If $X = A^n$ and $Y = A^m$, then $X \times Y = A^m \times A^n \cong A^{m+n}$ is an algebraic subset.

**Remark:** The set $S$ defining the algebraic subset $X = \bigvee(S)$ 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 $h \in k[x_1, \ldots, x_n]$.

In particular, we have

$$\bigvee(S) = \bigvee((S)) = \langle S \rangle: \text{ ideal generated by } S$$

$$\langle S \rangle = \{ h_1 f_1 + \cdots + h_r f_r \mid r \in \mathbb{N}, f_1, \ldots, f_r \in S, h_1, \ldots, h_r \in k[x_1, \ldots, x_n] \}$$

**Recall:** $R$ ring (i.e. commutative ring with unity)
- an ideal $I$ is a subset $I \subseteq R$ closed under addition and satisfying $RI = R$.
- i.e. $\alpha \cdot \beta \in I$ for all $\alpha \in R$ and $\beta \in I$.

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

**Example:** Algebraic subsets in $A^1$
Alg. subsets in $\mathbb{A}^1$ are: $\emptyset$, finite sets of points, $\mathbb{A}^1$

\begin{align*}
\mathbb{A}^1 &= k \\
\{p_1, \ldots, p_e\} &= \bigvee ((x_1-p_1) \cdot (x_2-p_2) \cdots (x_e-p_e))
\end{align*}

All alg. subsets are of the form $\bigvee(I)$ with $I = k[x]$ an ideal.

CA: $k[x]$ is a **principal ideal domain**: all ideals are principal.

Hence if $X \subset \mathbb{A}^1$ is an alg. subset, we have $X = \bigvee((f)) = \bigvee(f)$ with $f \in k[x]$.

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

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

However, $k[x_1, \ldots, x_n]$ is not 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 $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots = I_n \subseteq I_{n+1}$ with $I_i \subseteq \mathcal{R}$ ideal there is an $N$ s.t. $I_m = I_N$ for all $m \geq N$.

**Def.** If $\mathcal{R}$ satisfies (ACC), then $\mathcal{R}$ is called Noetherian.

**Thm (Hilbert basis theorem)** If $\mathcal{R}$ is Noetherian, then $\mathcal{R}[x]$ is Noetherian.

**Cor.** $k[x_1, \ldots, x_n]$ 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

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

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 $S_i \subseteq k[x_1, \ldots, x_n]$ we have:

$$\bigcap_{i \in I} \text{V}(S_i) = \text{V}(\bigcup_{i \in I} S_i).$$
Cor. Finite unions of alg. sets and arbitrary intersections of alg. sets are again algebraic.

Proof of lemma:
$S_1, S_2 \subset k[x_1, \ldots, x_n]$

"\subseteq" $p \in V(S_1) \cup V(S_2)$, let $h \in S_1S_2$.
Then $h = fg$ with $f \in S_1, g \in S_2$ and we have
$h(p) = f(p)g(p) = \begin{cases} 0 \cdot g(p) = 0 & \text{if } p \in V(S_1) \\ f(p) \cdot 0 = 0 & \text{if } p \in V(S_2) \end{cases}$
Hence $p \notin V(S_1S_2)$.

"\supseteq" Let us assume $p \notin V(S_1) \cup V(S_2)$. Then there exist $f \in S_1$ and $g \in S_2$ s.t. $f(p) \neq 0$, $g(p) \neq 0$. Hence $(fg)(p) = f(p)g(p) \neq 0$, which implies $p \notin V(S_1S_2)$.

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

Rem. The Zariski topology is not Hausdorff.
Take the case of $A^1$. Let us take distinct points $p, q \in A^1$.
Every open subset containing $p$ is of the form

$$U_p = A^1 \setminus \{p_1, \ldots, p_r\} \quad p_1, \ldots, p_r \neq p$$

and all open subsets containing $q$ are of the form

$$U_q = A^1 \setminus \{q_1, \ldots, q_s\} \quad q_1, \ldots, q_s \neq q$$

Hence $U_p \cap U_q = A^1 \setminus \{p_1, \ldots, p_r, q_1, \ldots, q_s\} \neq \emptyset$