# 4 Affine algebraic sets.

## 4.1 Affine algebraic sets and their ideals.

Let $k$ be any field.

**Definition 4.1.** *A **zero** of a polynomial $f \in k[x_1, \ldots, x_n]$ in the affine space $k^n$ is a point $(a_1, \ldots, a_n) \in k^n$ such that $f(a_1, \ldots, a_n) = 0$.*

*An **affine algebraic set** $V$ is a subset of the affine space $k^n$ consisting of all common zeros of some set of polynomials $\mathcal{S} \subseteq k[x_1, \ldots, x_n]$:*

$$V = \{(a_1, \ldots, a_n) \in k^n | \ f(a_1, \ldots, a_n) = 0 \ \text{ for all } f \in \mathcal{S}\}.$$

*We shall call the set $V$ to be defined by the set of polynomials $\mathcal{S}$ and denote by $V = \mathcal{Z}(\mathcal{S})$.*

**Remark 4.2.** Let $\mathcal{S} \subseteq k[x_1, \ldots, x_n]$ and let $\mathfrak{a}$ be the ideal of $k[x_1, \ldots, x_n]$ generated by $\mathcal{S}$. Then

$$\mathcal{Z}(\mathcal{S}) = \mathcal{Z}(\mathfrak{a}).$$

**Proof.** Since $S \subseteq \mathfrak{a}$, every common zero of polynomials from $\mathfrak{a}$ is also a zero of polynomials from $S$, so that $\mathcal{Z}(S) \supseteq \mathcal{Z}(\mathfrak{a})$. Conversely, if $(a_1, \ldots, a_n) \in k^n$ is a common zero of all polynomials from $S$, then it necessarily is a zero of every polynomial of the form

$$f_1 h_1 + \ldots + f_m h_m,$$

where $f_1, \ldots, f_m \in S$, $h_1, \ldots, h_m \in k[x_1, \ldots, x_n]$ and $m \in \mathbb{N}$. It is thus a zero of every polynomial from $\mathfrak{a}$ and hence $\mathcal{Z}(S) \subseteq \mathcal{Z}(\mathfrak{a})$. □

**Remark 4.3.** Let $\mathcal{S} \subseteq k[x_1, \ldots, x_n]$. Then there exists a finite set $\{f_1, \ldots, f_r\} \subseteq k[x_1, \ldots, x_n]$ such that

$$\mathcal{Z}(\mathcal{S}) = \mathcal{Z}(f_1, \ldots, f_r).$$

**Proof.** By Remark 4.2 $\mathcal{Z}(S) = \mathcal{Z}(\mathfrak{a})$, where $\mathfrak{a} = (S)$. By Hilbert's basis theorem, $\mathfrak{a}$ is finitely generated, so $\mathfrak{a} = (f_1, \ldots, f_r)$, for some $f_1, \ldots, f_r \in k[x_1, \ldots, x_n]$. Applying Remark 4.2 once again we obtain $\mathcal{Z}(\mathfrak{a}) = \mathcal{Z}(f_1, \ldots, f_r)$. □

**Remark 4.4.** Let $V \subseteq k^n$ be an affine algebraic set. The set $\mathcal{I}(V)$ of all polynomials whose common zeros coincide with $V$:

$$\mathcal{I}(V) = \{f \in k[x_1, \ldots, x_n] | \ f(a_1, \ldots, a_n) = 0 \ \text{ for all } (a_1, \ldots, a_n) \in V\}$$

is an ideal of $k[x_1, \ldots, x_n]$.

**Proof.** If $f, g \in \mathcal{I}(V)$, then

$$(f + g)(a_1, \ldots, a_n) = f(a_1, \ldots, a_n) + g(a_1, \ldots, a_n) = 0 + 0 = 0,$$

for all $(a_1, \ldots, a_n) \in V$. If, moreover, $h \in k[x_1, \ldots, x_n]$, then

$$(h \cdot f)(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot f(a_1, \ldots, a_n) = h(a_1, \ldots, a_n) \cdot 0 = 0,$$

for all $(a_1, ..., a_n) \in V$. □

**Definition 4.5.** *Let $V \subseteq k^n$ be an affine algebraic set. The ideal $\mathcal{I}(V)$ consisting of polynomials whose common zeros constitute $V$ shall be called the* ***ideal of the affine algebraic set*** *$V$.*

**Remark 4.6.** Let $V, V_1, V_2 \subset k^n$ be affine algebraic sets in $k^n$, let $\mathfrak{a}, \mathfrak{a}_1, \mathfrak{a}_2$ be ideals of $k[x_1, ..., x_n]$. Then:

1. $\mathfrak{a}_1 \subseteq \mathfrak{a}_2 \Rightarrow \mathcal{Z}(\mathfrak{a}_1) \supseteq \mathcal{Z}(\mathfrak{a}_2)$,
2. $\mathcal{I}(\mathcal{Z}(\mathfrak{a})) \supseteq \mathfrak{a}$,
3. $\mathcal{Z}(\mathcal{I}(V)) = V$,
4. $V_1 \subseteq V_2 \Leftrightarrow \mathcal{I}(V_1) \supseteq \mathcal{I}(V_2)$,
5. $V_1 = V_2 \Leftrightarrow \mathcal{I}(V_1) = \mathcal{I}(V_2)$.

**Proof.** 1. and 2. are obvious.

In order to show 3., observe that $\mathcal{Z}(\mathcal{I}(V)) \supseteq V$ is clear as well, and for the other inclusion assume that $V = \mathcal{Z}(\mathfrak{a})$, for some $\mathfrak{a} \lhd k[x_1, ..., x_n]$. But then $\mathcal{I}(V) = \mathcal{I}(\mathcal{Z}(\mathfrak{a})) \supseteq \mathfrak{a}$, and the result follows by 1.

4. is immediate.

For the proof of 5. it suffices to show that if $\mathcal{I}(V_1) \supseteq \mathcal{I}(V_2)$, then $V_1 \subseteq V_2$. But this is clear by 1. and 3. □

**Lemma 4.7.** *Let $f, g \in k[x_1, x_2]$ and assume that $f$ is irreducible in $k[x_1, x_2]$ and that $f \nmid g$. Then the system of equations*

$$f(x_1, x_2) = 0 \quad \textit{and} \quad g(x_1, x_2) = 0$$

*has only a finite number of solutions in the field $k$.*

**Proof.** If $\deg_{x_1} f = 0$, then $0 \neq f \in k[x_1]$ and the result is obvious, as a nonzero polynomial in one variable has only finitely many zeros. If $\deg_{x_1} f > 0$, consider $f \in k[x_1, x_2]$ as an element of the ring $k(x_2)[x_1]$. As $f$ is irreducible and does not divide $g$ in $k[x_1, x_2] \cong k[x_2][x_1]$, by Gauss lemma it is also irreducible and does not divide $g$ in $k(x_2)[x_1]$. Since $k(x_2)[x_1]$ is a PID, by the extended Euclidean algorithm there exist polynomials $\alpha, \beta \in k(x_2)[x_1]$ such that

$$\alpha f + \beta g = 1.$$

Multiplying both sides of the above equality by the least common multiple of denominators of coefficients of $\alpha$ and $\beta$, we yield

$$A(x_1, x_2) \cdot f + B(x_1, x_2) \cdot g = h(x_2),$$

for some $A(x_1, x_2), B(x_1, x_2) \in k[x_1, x_2]$ and $h(x_2) \in k[x_2]$. But $h$, as a nonzero polynomial in single variable, has only finitely many zeros, which implies that the system of equations $f(x_1, x_2) = 0$ and $g(x_1, x_2) = 0$ has at most finitely many solutions. □

**Theorem 4.8.** *Let $f \in k[x_1, x_2]$ be an irreducible polynomial in $k[x_1, x_2]$. If the curve $\mathcal{Z}(f)$ contains infinitely many points, then*

$$\mathcal{I}(\mathcal{Z}(f)) = (f).$$

**Proof.** By Remark 4.6.2 it suffices to show that $\mathcal{I}(\mathcal{Z}(f)) \subseteq (f)$. Fix $g \in \mathcal{I}(\mathcal{Z}(f))$. Then $g$ vanishes at infinitely many points of the curve $\mathcal{Z}(f)$, that is the system of equations $f(x_1, x_2) = 0$ and $g(x_1, x_2) = 0$ has infinitely many solutions. By Lemma 4.7 $f \mid g$, that is $g \in (f)$. □

## 4.2 Zariski topology.

**Lemma 4.9.** *A finite sum of affine algebraic sets is an affine algebraic set. To be more precise, let $\mathfrak{a}_1, ..., \mathfrak{a}_m$ be ideals of the ring $k[x_1, ..., x_n]$. Then*

$$\mathcal{Z}(\mathfrak{a}_1) \cup ... \cup \mathcal{Z}(\mathfrak{a}_m) = \mathcal{Z}(\mathfrak{a}_1 \cdot ... \cdot \mathfrak{a}_m),$$

*where* $\mathfrak{a}_1 \cdot ... \cdot \mathfrak{a}_m = \{\sum_{i=1}^{k} a_{i1}a_{i2}...a_{im} \mid k \in \mathbb{N}, a_{ij} \in \mathfrak{a}_j, j \in \{1, ..., m\}, i \in \{1, ..., k\}\}$.

**Proof.** Let $m = 2$ and let $\mathfrak{a}_1 = (f_1, ..., f_r)$, $\mathfrak{a}_2 = (g_1, ..., g_s)$. If $(a_1, ..., a_n) \in \mathcal{Z}(\mathfrak{a}_1) \cup \mathcal{Z}(\mathfrak{a}_2)$, then either $f_i(a_1, ..., a_n) = 0$ for all $i \in \{1, ..., r\}$, or $g_j(a_1, ..., a_n) = 0$ for all $j \in \{1, ..., s\}$. But then, for every selection of a pair $(i, j)$, $i \in \{1, ..., r\}$, $j \in \{1, ..., s\}$, $f_i g_j(a_1, ..., a_n) = 0$, that is $(a_1, ..., a_n) \in \mathcal{Z}(\mathfrak{a}_1 \cdot \mathfrak{a}_2)$.

Conversely, if $(a_1, ..., a_n) \notin \mathcal{Z}(\mathfrak{a}_1) \cup \mathcal{Z}(\mathfrak{a}_2)$, then $f_{i_0}(a_1, ..., a_n) \neq 0$, for some $i_0 \in \{1, ..., r\}$, and $g_{j_0}(a_1, ..., a_n) \neq 0$, for some $j_0 \in \{1, ..., s\}$. Hence $f_{i_0} g_{j_0}(a_1, ..., a_n) \neq 0$, that is $(a_1, ..., a_n) \notin \mathcal{Z}(\mathfrak{a}_1 \cdot \mathfrak{a}_2)$.

For $m > 2$ we proceed by induction. □

**Remark 4.10.** Let $\mathfrak{a}_1, ..., \mathfrak{a}_m$ be ideals of the ring $k[x_1, ..., x_n]$. Then

$$\mathcal{Z}(\mathfrak{a}_1 \cdot ... \cdot \mathfrak{a}_m) = \mathcal{Z}(\mathfrak{a}_1 \cap ... \cap \mathfrak{a}_m).$$

**Proof.** It suffices to observe that

$$\mathcal{Z}(\mathfrak{a}_1 \cdot ... \cdot \mathfrak{a}_m) \subseteq \mathcal{Z}(\mathfrak{a}_1) \cup ... \cup \mathcal{Z}(\mathfrak{a}_m) \subseteq \mathcal{Z}(\mathfrak{a}_1 \cap ... \cap \mathfrak{a}_m) \subseteq \mathcal{Z}(\mathfrak{a}_1 \cdot ... \cdot \mathfrak{a}_m).$$ □

**Lemma 4.11.** *Intersection of any number of affine algebraic sets is an affine algebraic set. To be more precise, let $\{\mathfrak{a}_i \mid i \in I\}$ be a family of ideals of the ring $k[x_1, ..., x_n]$. Then*

$$\bigcap_{i \in I} \mathcal{Z}(\mathfrak{a}_i) = \mathcal{Z}\left(\left(\bigcup_{i \in I} \mathfrak{a}_i\right)\right).$$

**Proof.** Let $\mathfrak{a} = (\bigcup_{i \in I} \mathfrak{a}_i)$. Then

$$\begin{aligned}
(a_1, ..., a_n) \in \mathcal{Z}(\mathfrak{a}) &\Leftrightarrow \forall f \in \mathfrak{a} \quad f(a_1, ..., a_n) = 0 \\
&\Leftrightarrow \forall f \in \bigcup_{i \in I} \mathfrak{a}_i \quad f(a_1, ..., a_n) = 0 \\
&\Leftrightarrow \forall i \in I \forall f \in \mathfrak{a}_i \quad f(a_1, ..., a_n) = 0 \\
&\Leftrightarrow \forall i \in I \quad (a_1, ..., a_n) \in \mathcal{Z}(\mathfrak{a}_i) \\
&\Leftrightarrow (a_1, ..., a_n) \in \bigcap_{i \in I} \mathcal{Z}(\mathfrak{a}_i).
\end{aligned}$$

□

**Remark 4.12.** Let $\mathfrak{a}_1, ..., \mathfrak{a}_m$ be ideals of the ring $k[x_1, ..., x_n]$. Then

$$\mathcal{Z}(\mathfrak{a}_1 + ... + \mathfrak{a}_m) = \mathcal{Z}(\langle \mathfrak{a}_1 \cup ... \cup \mathfrak{a}_m \rangle).$$

**Theorem 4.13.** *In $k^n$ there is a topology whose closed sets are affine algebraic sets in $k^n$.*

**Proof.** Observe that $\emptyset = \mathcal{Z}(\{\text{const.}1\})$ and $k^n = \mathcal{Z}(\{\text{const.}0\})$. The rest of the proof follows from Lemmas 4.9 and 4.11. □

**Definition 4.14.** *The topology of $k^n$ defined by affine algebraic sets is called the **Zariski topology** in $k^n$.*

**Remark 4.15.** In every nonempty family of affine algebraic sets there exists a minimal affine algebraic set.

**Proof.** Let $\mathcal{R} = \{V_i |\, i \in I\}$ be a family of affine algebraic sets. Let $\mathfrak{a}_i = \mathcal{I}(V_i)$. Since $k[x_1, ..., x_n]$ is Noetherian, the family of ideals $\{\mathfrak{a}_i |\, i \in I\}$ contains a maximal element, and, consequently, the family $\mathcal{R}$ contains a minimal element. □

**Remark 4.16.** Every affine algebraic set $V \subseteq k^n$ is compact in the Zariski topology.

**Proof.** Let $V \subseteq \bigcup_{i \in I} U_i$ be a covering of $V$ by open sets in the Zariski topology. Fix $i_1 \in I$. If $V \nsubseteq U_{i_1}$, then there exists $i_2 \in I$ such that $U_{i_1} \subsetneq U_{i_1} \cup U_{i_2}$. If $V \nsubseteq U_{i_1} \cup U_{i_2}$, then there exists $i_3 \in I$ such that $U_{i_1} \cup U_{i_2} \subsetneq U_{i_1} \cup U_{i_2} \cup U_{i_3}$. Proceeding by induction we eventually exhibit a finite covering $V \subseteq U_{i_1} \cup U_{i_2} \cup ... \cup U_{i_m}$, for otherwise we would have constructed an infinite ascending sequence of open sets, corresponding to an infinite descending sequence of closed sets, corresponding, in turn, to an infinite ascending sequence of ideals in a Noetherian ring – a contradiction. □