

Chapter 3

Algebraic sets and varieties

3.1 Affine Space and Algebraic Sets

Throughout this chapter let K be a field.

Def. 3.1.1. The n -dimensional affine space over K is defined as

$$\mathbb{A}^n(K) := \{ (a_1, \dots, a_n) \mid a_i \in K \}.$$

If K is clear from context, we simply write \mathbb{A}^n . The elements of \mathbb{A}^n are called *points*. \mathbb{A}^1 is called the *affine line*, and \mathbb{A}^2 is called the *affine plane*. \square

Def. 3.1.2. Let $f \in K[x_1, \dots, x_n]$. A point $P = (a_1, \dots, a_n) \in \mathbb{A}^n(K)$ is a *root* or *zero* of f iff $f(P) = f(a_1, \dots, a_n) = 0$.

A subset $V \subseteq \mathbb{A}^n(K)$ is an *affine algebraic set* iff there is a set of polynomials $S \subseteq K[x_1, \dots, x_n]$ such that

$$V = V(S) = \{ P \in \mathbb{A}^n(K) \mid f(P) = 0 \text{ for all } f \in S \}. \quad \square$$

We list a few facts about affine algebraic sets:

- (1) If $S \subseteq K[x_1, \dots, x_n]$ and $I = \text{ideal}(S) = \langle S \rangle$, then $V(S) = V(I)$. So every affine algebraic set is $V(I)$ for some ideal I in $K[x_1, \dots, x_n]$. Since the polynomial ring is Noetherian (see Hilbert's Basis Theorem, below), every ideal has a finite basis. So for every affine algebraic set V there is a finite set of polynomials $S = \{f_1, \dots, f_m\}$ such that $V = V(S) = V(f_1, \dots, f_m)$. The corresponding system of algebraic equations

$$f_1 = 0, \dots, f_m = 0$$

is called a *system of defining equations* for V .

(2) If I, J are ideals with $I \subseteq J$, then $V(I) \supseteq V(J)$.

(3) If $\{I_\alpha\}_{\alpha \in A}$ is an arbitrary family of ideals, then

$$V\left(\bigcup_{\alpha \in A} I_\alpha\right) = \bigcap_{\alpha \in A} V(I_\alpha).$$

Thus, the intersection of an arbitrary family of algebraic sets is an algebraic set.

(4) $V(f \cdot g) = V(f) \cup V(g)$ for polynomials f, g . This relation can be generalized to ideals I, J .

$$V(I) \cup V(J) = V(\{f \cdot g \mid f \in I, g \in J\}).$$

So if $B_I = \{f_1, \dots, f_m\}$ and $B_J = \{g_1, \dots, g_p\}$ are finite bases for the ideals I and J , respectively, then $B = \{f_i \cdot g_j \mid 1 \leq i \leq m, 1 \leq j \leq p\}$ is a finite basis for $I \cdot J$, the product of the ideals I, J , and

$$V(I) \cup V(J) = V(I \cdot J) = V(B).$$

By the way, we also have $V(I) \cup V(J) = V(I \cap J)$.

So every finite union of algebraic sets is an algebraic set.

(5) $V(0) = \mathbb{A}^n(K)$, and $V(1) = \emptyset$.

$V(x_1 - a_1, \dots, x_n - a_n) = \{(a_1, \dots, a_n)\}$ for all $a_i \in K$. So every finite set of points is an algebraic set.

(6) Collecting (3), (4), and (5) we get that $\mathbb{A}^n(K)$ is a topological space if we take the algebraic sets as the closed sets. This topology is called the *Zariski topology*.

Def. 3.1.3. The *Zariski topology* on $\mathbb{A}^n(K)$ is the topology in which the closed sets are exactly the algebraic sets in $\mathbb{A}^n(K)$. \square

Example 3.1.1. Some examples of affine algebraic sets:

(1) Linear algebraic sets: they are the solutions of systems of linear equations and are treated in linear algebra.

(2) Hypersurfaces: these are algebraic sets defined by a single equation $f(x_1, \dots, x_n) = 0$, where f is non-constant.

If f is linear, we have a hyperplane (a plane in \mathbb{A}^3 , a line in \mathbb{A}^2).

Hypersurfaces in \mathbb{A}^3 are just called surfaces.

By definition, every algebraic set is the intersection of finitely many hypersurfaces.

Over the field \mathbb{R} a hypersurface can be empty or consist of only finitely many points:

$$\begin{aligned} x^2 + y^2 + 1 = 0 &\longrightarrow \text{no point in } \mathbb{A}^2(\mathbb{R}) \\ x^2 + y^2 = 0 &\longrightarrow \text{only one point } (0, 0) \text{ in } \mathbb{A}^2(\mathbb{R}) \end{aligned}$$

This cannot happen over an algebraically closed field such as \mathbb{C} .

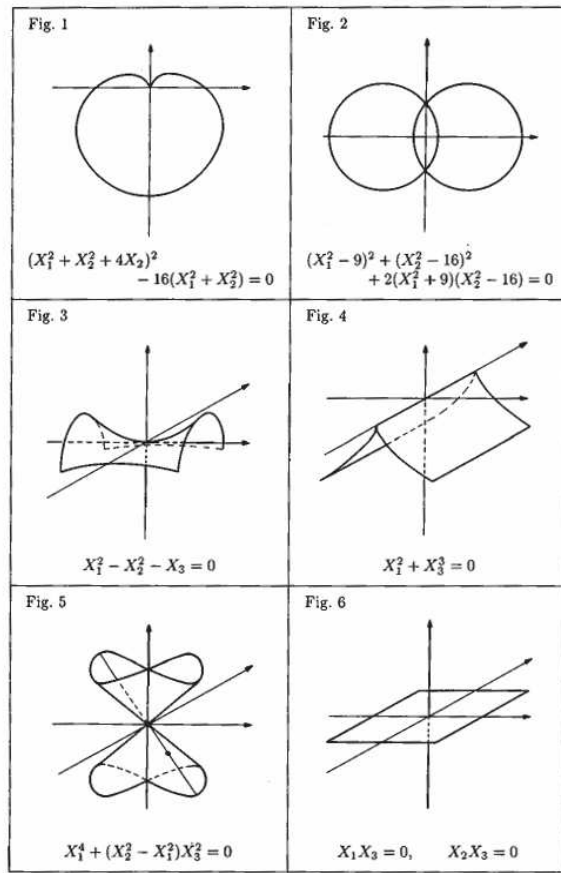


Figure 3.1: from [Kun85]

- (3) Plane algebraic curves: a plane algebraic curve \mathcal{C} is a hypersurfaces in \mathbb{A}^2 , i.e. the set of solutions of $f(x, y) = 0$.
- (4) Cones: if the defining system of equations consists only of homogeneous polynomials, then the corresponding algebraic set V has the property that for $P \in V$, $P \neq (0, 0)$, the whole line connecting P and the origin $O = (0, 0)$ is contained in V . Such an algebraic set is called a cone with vertex at the origin.
- (5) Product of affine algebraic sets:

$$\begin{array}{ll}
 V \subseteq \mathbb{A}^n(K) & \text{defined by } f_i(x_1, \dots, x_n) = 0, \quad i = 1, \dots, r \\
 W \subseteq \mathbb{A}^m(K) & \text{defined by } g_j(x_1, \dots, x_m) = 0, \quad i = 1, \dots, s
 \end{array}$$

The product $V \times W \subseteq \mathbb{A}^{n+m}(K)$ is defined by

$$\begin{aligned} f_i(x_1, \dots, x_n) &= 0, & 1 \leq i \leq r \\ g_j(y_1, \dots, y_m) &= 0, & 1 \leq j \leq s \end{aligned}$$

in $K[x_1, \dots, x_n, y_1, \dots, y_m]$.

- (6) Parametrizations are points in spaces over rational function fields: let $\mathcal{C} \subset \mathbb{A}^2(K)$ be a curve defined as the set of solutions of $f(x, y) = 0$ over the field K . Let \mathcal{C} be parametrized by $P(t) = (x(t), y(t))$ (compare Example 1.3.). So $f(x(t), y(t)) = 0$, which means that $P(t)$ is a point on the curve $\tilde{\mathcal{C}}$ defined by $f(x, y)$ over the bigger field $\mathbb{A}^2(K(t))$. In fact,

$$\tilde{\mathcal{C}} = \{P(t) \in \mathbb{A}^2(K(t)) \mid f(P(t)) = 0\}.$$

$\tilde{\mathcal{C}}$ contains all the points of \mathcal{C} and also all the parametrizations of \mathcal{C} (or of components thereof; compare Chap. 8).

Theorem 3.1.1. *Let the field K be infinite.*

- (a) *Let $n \geq 1$. Then for every hypersurface V in $\mathbb{A}^n(K)$ there are infinitely many points in $\mathbb{A}^n(K) \setminus V$, i.e. outside of V .*
- (b) *Let K be algebraically closed and $n \geq 2$. Then every hypersurface in $\mathbb{A}^n(K)$ contains infinitely many points.*

Proof: (a) We proceed by induction on n . For $n = 1$ the statement obviously holds. Now consider $n > 1$. The hypersurface V is defined by the non-constant polynomial $f(x_1, \dots, x_n)$. W.l.o.g. we may assume that x_n actually occurs in f , i.e.

$$f = \sum_{i=0}^m g_i(x_1, \dots, x_{n-1})x_n^i, \quad (*)$$

with $m > 0$ and $g_m \neq 0$.

By the induction hypothesis there is a point $(a_1, \dots, a_{n-1}) \in \mathbb{A}^{n-1}$ such that $g_m(a_1, \dots, a_{n-1}) \neq 0$. So $f(a_1, \dots, a_{n-1}, x_n)$ is a non-vanishing polynomial in $K[x_n]$, having only finitely many roots. Thus, there are infinitely many $a_n \in K$ such that $f(a_1, \dots, a_{n-1}, a_n) \neq 0$.

(b) Let V be defined by f as in (*). By (a), there are infinitely many points $P = (a_1, \dots, a_{n-1}) \in \mathbb{A}^{n-1}$ with $g_m(a_1, \dots, a_{n-1}) \neq 0$. Since K is algebraically closed, for every such point P there is a value $a_n \in K$ such that $f(a_1, \dots, a_{n-1}, a_n) = 0$. \square

We have seen how we can associate a geometric variety to a polynomial ideal. On the other hand, any set of points in space also determines a polynomial ideal, namely the set of polynomials vanishing on these points.

Def. 3.1.4. Let X be a subset of $\mathbb{A}^n(K)$. The set of all polynomials in $K[x_1, \dots, x_n]$ vanishing on all the points in X form an ideal. This ideal is the *ideal of X* , $I(X)$.

$$I(X) := \{ f \in K[x_1, \dots, x_n] \mid f(P) = 0 \text{ for all } P \in X \}. \quad \square$$

Theorem 3.1.2. Let K be algebraically closed and $n \geq 1$. Let $H \subset \mathbb{A}^n(K)$ be a hypersurface defined by the polynomial

$$f = c \cdot f_1^{\alpha_1} \cdot \dots \cdot f_s^{\alpha_s},$$

where $c \in K^*$, and the f_i are pairwise relatively prime irreducible polynomials. Then $I(H) = \langle f_1 \cdot \dots \cdot f_s \rangle$.

Proof: Obviously $f_1 \cdot \dots \cdot f_s \in I(H)$.

So it suffices to show that every $g \in I(H)$ is divisible by all the factors f_i , $1 \leq i \leq s$. Suppose for some i the factor f_i does not divide g . W.l.o.g. we may assume that x_n actually occurs in f_i , i.e.

$$f_i = \sum_{j=0}^m g_j(x_1, \dots, x_{n-1}) x_n^j,$$

with $m > 0$ and $g_m \neq 0$. By Gauss' Lemma, the polynomials f_i and g are also relatively prime in the Euclidean domain $K(x_1, \dots, x_{n-1})[x_n]$. So for some $h_1, h_2 \in K[x_1, \dots, x_n]$ and $d \in K[x_1, \dots, x_{n-1}]^*$ we can write

$$d(x_1, \dots, x_{n-1}) = h_1(x_1, \dots, x_n) \cdot f_i(x_1, \dots, x_n) + h_2(x_1, \dots, x_n) \cdot g(x_1, \dots, x_n).$$

By Theorem 3.1.1(a) there is a point $(a_1, \dots, a_{n-1}) \in \mathbb{A}^{n-1}$ such that

$$d(a_1, \dots, a_{n-1}) \cdot g_m(a_1, \dots, a_{n-1}) \neq 0.$$

Choose a value $a_n \in K$ such that $f_i(a_1, \dots, a_{n-1}, a_n) = 0$. Then $(a_1, \dots, a_n) \in H$, and therefore $g(a_1, \dots, a_n) = 0$. This, however, is a contradiction to $d(a_1, \dots, a_{n-1}) \neq 0$. \square

We list some relations between ideals and algebraic sets.

Lemma 3.1.3. *Let $X, Y \subseteq \mathbb{A}^n(K)$, $S \subseteq K[x_1, \dots, x_n]$.*

- (a) *If $X \subseteq Y$ then $I(X) \supseteq I(Y)$.*
- (b) $I(\emptyset) = K[x_1, \dots, x_n]$.
If K is infinite, then $I(\mathbb{A}^n) = \langle 0 \rangle$.
 $I(\{(a_1, \dots, a_n)\}) = \langle x_1 - a_1, \dots, x_n - a_n \rangle$ for all $a_i \in K$.
- (c) $I(V(S)) \supseteq S$.
 $V(I(X)) \supseteq X$.
- (d) $V(I(V(S))) = V(S)$.
 $I(V(I(X))) = I(X)$.
- (e) $I(X)$ is a radical ideal.

The proof is left to the reader as an exercise.

3.2 Noetherian rings and Hilbert's Basis Theorem

We have already used the fact that every ideal in the polynomial ring $K[x_1, \dots, x_n]$ is finitely generated. In this section we give a proof of this fact.

Def. 3.2.1. A commutative ring with identity R is called a *Noetherian ring* iff the *basis condition* holds in R , i.e. every ideal in R is finitely generated. \square

Lemma 3.2.1. A commutative ring with identity R is Noetherian if and only if there are no infinite properly ascending chains of ideals in R . I.e., if

$$I_1 \subseteq I_2 \subseteq \dots \subseteq R,$$

then there is an index k such that

$$I_k = I_{k+1} = \dots . \quad \square$$

Proof: Suppose that R is Noetherian. Let

$$I_0 \subseteq I_1 \subseteq I_2 \subseteq \dots$$

be an ascending chain of ideals in R . Consider

$$I := \bigcup_{i=0}^{\infty} I_i .$$

I is an ideal in R , so it has a finite basis. This basis must be contained in some I_k ; so

$$I_k = I_{k+1} = \dots .$$

On the other hand, suppose that an ideal I in R does not have a finite basis.

Choose a non-zero element $r_0 \in I$; then $I_0 := \langle r_0 \rangle \neq I$.

Choose $r_1 \in I \setminus I_0$; then $I_1 := \langle r_0, r_1 \rangle \neq I$.

This process can be continued indefinitely, yielding an infinite properly ascending chain of ideals in R . \square

Theorem 3.2.2. (Hilbert's Basis Theorem) *If R is a Noetherian ring then also the ring of polynomials $R[x]$ is Noetherian.*

Proof: Let I be an ideal in $R[x]$. We have to show that I has a finite basis.

For $f(x) = a_0 + a_1x + \dots + a_dx^d \in R[x]^*$, $a_d \neq 0$, we call a_d the *leading coefficient* of f , $\text{lc}(f)$, and a_dx^d the *leading term* of f , $\text{lt}(f)$. The leading coefficient of 0 is 0.

Let J be the set of all leading coefficients of polynomials in I . J is an ideal in R , and therefore has a finite basis. Let $f_1, \dots, f_k \in I$ be such that their leading coefficients generate J , i.e.

$$J = \langle \text{lc}(f_1), \dots, \text{lc}(f_k) \rangle .$$

Let N be the highest degree of the f_i 's,

$$N = \max_{1 \leq i \leq k} \deg(f_i).$$

For every $m, 0 \leq m < N$, let J_m be the ideal in R consisting of the leading coefficients of all polynomials $f \in I$ with $\deg(f) \leq m$. Let $\{f_{mj} | 1 \leq j \leq k_m\}$ be a finite set of polynomials in I with $\deg(f_{mj}) \leq m$, such that J_m is generated by the leading coefficients of the f_{mj} , i.e.

$$J_m = \langle \text{lc}(f_{m1}), \dots, \text{lc}(f_{mk_m}) \rangle.$$

Now let

$$I' := \langle \{f_1, \dots, f_k\} \cup \bigcup_{0 \leq m < N} \{f_{mj} | 1 \leq j \leq k_m\} \rangle.$$

We show that $I' = I$, so I has a finite basis.

Obviously $I' \subseteq I$. Suppose that I' is a proper subset of I . Let g be an element of least degree in $I \setminus I'$.

Case $\deg(g) \geq N$: There are polynomials q_i such that

$$\text{lt}\left(\sum q_i f_i\right) = \text{lt}(g).$$

So also $g - \sum q_i f_i \in I \setminus I'$ and $\deg(g - \sum q_i f_i) < \deg(g)$, in contradiction to the minimality of $\deg(g)$.

Case $\deg(g) < N$: Let $m = \deg(g)$. There are polynomials q_j such that

$$\text{lt}\left(\sum q_j f_{mj}\right) = \text{lt}(g).$$

So also $g - \sum q_j f_{mj} \in I \setminus I'$ and $\deg(g - \sum q_j f_{mj}) < \deg(g)$, in contradiction to the minimality of $\deg(g)$.

In any case we see that such a g cannot exist, i.e. $I = I'$ and I is finitely generated. \square

Corollary. For any n , $K[x_1, \dots, x_n]$ is a Noetherian ring.

Proof: K has only two ideals, namely $\langle 0 \rangle, \langle 1 \rangle$. Both are obviously finitely generated. The statement follows from the Theorem by induction on n . \square

Let us derive some further properties of Noetherian rings.

Theorem 3.2.3. Let \mathcal{S} be a non-empty set of ideals in the Noetherian ring R . Then \mathcal{S} contains a maximal element, i.e. there is an $I \in \mathcal{S}$ such that for all other ideals $J \in \mathcal{S}$ we have $I \not\subset J$.

Proof: Let $\mathcal{S}_0 := \mathcal{S}$. Choose an ideal $I_0 \in \mathcal{S}_0$. Now let

$$\mathcal{S}_1 := \{ I \in \mathcal{S} \mid I_0 \subset I \text{ and } I_0 \neq I \}.$$

If $\mathcal{S}_1 \neq \emptyset$, then choose an ideal $I_1 \in \mathcal{S}_1$ and let

$$\mathcal{S}_2 := \{ I \in \mathcal{S} \mid I_1 \subset I \text{ and } I_1 \neq I \}.$$

This process is continued as long as $\mathcal{S}_m \neq \emptyset$. The proof is complete if we can show that for some m the set \mathcal{S}_m is empty.

Suppose $\mathcal{S}_m \neq \emptyset$ for all m . Let

$$I := \bigcup_{m=0}^{\infty} I_m,$$

an ideal in R . Let $\{f_1, \dots, f_r\}$ be a finite basis of I . For a sufficiently big m we have $f_i \in I_m$ for all $1 \leq i \leq r$. So $I = I_m$ and therefore $I_{m+1} = I_m$, a contradiction. \square

Also the converse is true; see [ZaS58] I, p.199.

In a Noetherian ring we can use a certain form of induction based on ascending chains, the so-called *Principle of Divisor Induction*.

Def. 3.2.2. Let I, J be ideals in R , a commutative ring with 1. J is a *divisor* of I iff $I \subseteq J$.

For ideals I_1, I_2 in R , $I_1 + I_2$ is called the *greatest common divisor* of I_1 and I_2 . \square

Theorem 3.2.4. (The Principle of Divisor Induction) *Let R be a Noetherian ring. If a property E can be proved for any ideal I under the hypothesis that it is satisfied for all proper divisors of I , then all ideals have the property E .*

Proof: Suppose that some ideal does not have property E . Then by Theorem 3.2.3 there is a maximal ideal I which does not have property E . Because of the maximality, all proper divisors of I must have property E . Therefore, I also has property E ; which is a contradiction. \square

3.3 Irreducible Components of Algebraic Sets

Def. 3.3.1. An algebraic set $V \subseteq \mathbb{A}^n$ is *reducible* iff there are algebraic sets V_1, V_2 different from V such that $V = V_1 \cup V_2$. Otherwise V is *irreducible*. An irreducible algebraic set is also called a *variety*. \square

An ideal I is prime iff with the product $a \cdot b$ it must contain one of the factors a or b . Irreducible algebraic sets correspond to prime ideals.

Theorem 3.3.1. *An algebraic set V is irreducible if and only if $I(V)$ is a prime ideal.*

Proof: “ \implies ”: Suppose $I(V)$ is not prime. Then there are polynomials f_1, f_2 such that $f_1 \cdot f_2 \in I(V)$ but $f_1, f_2 \notin I(V)$. So $V = (V \cap V(f_1)) \cup (V \cap V(f_2))$, and $V \cap V(f_i) \neq V$ for $i = 1, 2$. Thus, V is reducible.

“ \impliedby ”: Suppose $V = V_1 \cup V_2$, where $V_i \neq V$ for $i = 1, 2$. By Lemma 3.1.3(d), also $I(V_i) \neq I(V)$ for $i = 1, 2$. Let $f_i \in I(V_i) \setminus I(V)$ for $i = 1, 2$. Then $f_1 \cdot f_2 \in I(V)$, and therefore $I(V)$ is not prime. \square

An algorithm for decomposing an algebraic set V into a finite union of irreducible algebraic sets could proceed as follows: first we decompose V into sets V_1, V_2 . Next we decompose V_1 and V_2 , and so on. We will reach a finite decomposition if this algorithm terminates. This is a consequence of the following theorem.

Theorem 3.3.2. *Every non-empty family $\mathcal{V} = \{V_\alpha\}_{\alpha \in A}$ of algebraic sets in \mathbb{A}^n contains a minimal element (w.r.t. to set inclusion “ \subset ”).*

Proof: Let $I(V_{\alpha_0})$ be a maximal element in $\{I(V_\alpha)\}_{\alpha \in A}$ (this exists because of Theorem 3.2.3). Then V_{α_0} is minimal in \mathcal{V} . \square

Theorem 3.3.3. *Let V be an algebraic set in \mathbb{A}^n . Then there is a unique decomposition, up to permutation of the components, of V into irreducible algebraic sets V_1, \dots, V_m such that*

$$V = V_1 \cup \dots \cup V_m \quad \text{and} \quad V_i \not\subseteq V_j \text{ for } i \neq j.$$

Proof: (a) Existence of decomposition: Let

$$\mathcal{V} := \{ V \subseteq \mathbb{A}^n \mid V \text{ is algebraic and } V \text{ is not the union of finitely many irreducible algebraic sets } \}.$$

We want to show that $\mathcal{V} = \emptyset$.

If this is not the case, then \mathcal{V} contains a minimal element, say \overline{V} . Since $\overline{V} \in \mathcal{V}$, \overline{V} can be decomposed into $\overline{V} = V_1 \cup V_2$, $V_i \neq \overline{V}$ for $i = 1, 2$. Because of the minimality

of \overline{V} , V_i cannot be in \mathcal{V} , so $V_i = V_{i1} \cup \dots \cup V_{im_i}$ for V_{ij} irreducible. But then

$$V = \bigcup_{i,j} V_{ij},$$

a contradiction.

(b) Uniqueness: In the decomposition $V = V_1 \cup \dots \cup V_m$ eliminate all components which are properly contained in another component and also double occurrences of components. The resulting decomposition is *reduced*.

Now consider two reduced decompositions

$$V = V_1 \cup \dots \cup V_m$$

and

$$V = W_1 \cup \dots \cup W_l.$$

Then

$$V_i = V \cap V_i = \bigcup_{j=1}^l (W_j \cap V_i).$$

Because of the irreducibility of the V_i, W_j , every $V_i \subseteq W_{j(i)}$ for some $j(i)$, and on the other hand $W_{j(i)} \subseteq V_k$ for some k . This is only possible for $V_i = W_{j(i)} = V_k$, i.e. $i = k$. Thus, every V_i is equal to some $W_{j(i)}$.

In the same way, we can show that every W_j is equal to some $V_{i(j)}$. \square

Def. 3.3.2. Let $V \subseteq \mathbb{A}^n$ be an algebraic set. Let $V = V_1 \cup \dots \cup V_m$ be the unique decomposition guaranteed by Theorem 3.3.3. This decomposition is called the *decomposition of V into irreducible components*. \square

In Section 4.3 we will compare this result on decomposition of algebraic sets with primary decomposition of polynomial ideals. The situation for primary decomposition is much more complicated.

Theorem 3.3.4. *If K is infinite, then $\mathbb{A}^n(K)$ is irreducible.*

Proof: Suppose $\mathbb{A}^n(K)$ were reducible, and $\mathbb{A}^n(K) = V_1 \cup V_2$ a decomposition. Consider non-zero polynomials $f_1 \in I(V_1) \setminus I(V_2)$, $f_2 \in I(V_2) \setminus I(V_1)$. $f_1 \cdot f_2 \in I(V_1) \cap I(V_2)$, so $0 \neq f_1 \cdot f_2$ vanishes on all points of $\mathbb{A}^n(K)$. This is a contradiction to Theorem 3.1.1. \square

We will take the affine plane $\mathbb{A}^2(K)$ as an example and give a complete classification of the algebraic subsets of the plane. Because of Theorem 3.3.3 it suffices to classify the irreducible algebraic sets. All others are constructed from these components.

Theorem 3.3.5. *Let $f, g \in K[x, y]$, f and g relatively prime. Then $V(f, g) = V(f) \cap V(g)$ is a finite set of points.*

Proof: f and g are relatively prime in $K[x][y]$, so by Gauss' Lemma they are also relatively prime in $K(x)[y]$. But $K(x)[y]$ is a Euclidean domain, so we can write the gcd as a linear combination

$$1 = r \cdot f + s \cdot g,$$

for some $r, s \in K(x)[y]$. After eliminating the denominators from this equation, we get

$$d = a \cdot f + b \cdot g,$$

for some $d \in K[x]$, $a, b \in K[x, y]$.

Now if $(c_1, c_2) \in V(f, g)$, then $d(c_1) = 0$. But d has only finitely many roots. So there are only finitely many possible values for the x -coordinate of points in $V(f, g)$. By an analogous consideration we determine that there are only finitely many possible values for the y -coordinate of points in $V(f, g)$. \square

Corollary. *If $f(x, y)$ is irreducible in $K[x, y]$ and $V(f)$ is infinite, then $I(V(f)) = \langle f \rangle$ and $V(f)$ is irreducible.*

Proof: If $g \in I(V(f))$, then $V(f, g) = V(f)$ is infinite. So, by the Theorem, f must divide g , and therefore $g \in \langle f \rangle$. The irreducibility of $V(f)$ follows from Theorem 3.3.1. \square

Theorem 3.3.6. (classification) *Let the field K be infinite. The following is a complete classification of the irreducible algebraic subsets of $\mathbb{A}^2(K)$:*

- (a) $\mathbb{A}^2(K)$ and \emptyset ,
- (b) single points,
- (c) irreducible algebraic curves $V(f)$, where f is an irreducible polynomial and $V(f)$ is infinite.

Proof: Let V be an irreducible algebraic set in $\mathbb{A}^2(K)$. If V is finite or $I(V) = \langle 0 \rangle$, then V is of type (a) or (b).

Otherwise, $I(V)$ contains a non-constant polynomial f . Since $I(V)$ is prime, it must also contain an irreducible factor of f . So w.l.o.g. let f be irreducible. Now we claim that $I(V) = \langle f \rangle$. To see this, let $h \in I(V) \setminus \langle f \rangle$. h and f are relatively prime, so by Theorem 3.3.5 $V \subset V(f, h)$ is finite. \square

Theorem 3.3.7. *Let K be algebraically closed, $f \in K[x, y]$. Let $f = f_1^{\alpha_1} \cdot \dots \cdot f_s^{\alpha_s}$ be the factorization of f . Then*

- (a) $V(f) = V(f_1) \cup \dots \cup V(f_s)$ is the decomposition of $V(f)$ into irreducible components, and
- (b) $I(V(f)) = \langle f_1 \cdot \dots \cdot f_s \rangle$.

Proof: obvious. □

Example 3.3.1. We consider the intersection of a sphere with radius 2 and a cylinder with radius 1 defined by

$$\begin{aligned}f_1 &= x^2 + y^2 + z^2 - 4 = 0 , \\f_2 &= y^2 + z^2 - 1 = 0 .\end{aligned}$$

$V = V(f_1, f_2)$ can be decomposed as

$$V = V(x - \sqrt{3}, y^2 + z^2 - 1) \cup V(x + \sqrt{3}, y^2 + z^2 - 1),$$

and these are the irreducible components of V . □