Introduction to algebraic geometry

Lecturer: Klemen Šivic

October 3, 2025

I. AFFINE VARIETIES (Afine raznoterosti)

1. Recap of basic notions

A polynomial over a ring R is a formal expression $p(x) = a_n x^n + a_{n-1}x^{n-1} + \dots + a_0$, where $a_i \in R$, n = degree of p (if $a_n \neq 0$). The set of all polynomials in x over R is denoted $R[x]$. All rings will be commutative and with 1. $R[x]$ is a ring for usual addition and multiplication of polynomials.

Suppose R is a subring of a ring S and $a \in S$. Then we can compute $a_n a^n + a_{n-1}a^{n-1} + \dots + a_0 \in S$. We denote this element $p(a)$ and call it the value of p at a. If $p(a) = 0$, then a is a root/zero of p. We have a polynomial function $S \longrightarrow S$, $a \longmapsto p(a)$.

Polynomial in two variables x and y with coefficients in a ring R is an expression $p(x,y) = \sum_{i=0}^{n}\sum_{j=0}^{m} a_{ij}x^i y^j$, where $a_{ij} \in R$. The expression $a_{ij}x^i y^j$ is called a monomial. The degree of a monomial $x^i y^j$ is $i+j$. The degree of the polynomial $p(x,y) = \max\{i+j \mid a_{ij} \neq 0\}$. The set of all polynomials in two variables is a ring. We denote it by $R[x,y]$.

$R[x,y] \cong R[x][y] \cong R[y][x]$.

Similarly we define polynomials in more variables.

$R[x_1, \dots, x_n] \cong R[x_1, \dots, x_{n-1}][x_n]$.

If R is a subring of S and $p \in R[x_1, \dots, x_n]$ and $a = (a_1, \dots, a_n) \in S^n$, we can compute $p(a_1, \dots, a_n) \in S$. We get a function $S^n \longrightarrow S$, $a \longmapsto p(a)$.

Let R be a ring. An ideal of R is a subset $I \subseteq R$ s.t.

i) If $x, y \in I$, then $x+y \in I$.
ii) If $a \in R$ and $x \in I$, then $ax \in I$.
$I \trianglelefteq R$.
If an ideal I contains an invertible element, then $I = R$.
If $M \subseteq R$ is some set, then
$(M) := \{ \sum_{i=0}^{n} a_i x_i \mid n \in \mathbb{N}, a_i \in R, x_i \in M \}$ is an ideal.
We call it the ideal generated by M. If $M = \{m_1, \dots, m_n\}$, we write $(x_1, \dots, x_n)$ instead of $(\{x_1, \dots, x_n\})$.
$I \trianglelefteq R$ is finitely generated if $I = (M)$ where M is a finite set. I is a principal ideal, if $I = (a)$ for some $a \in R$.
A domain where every ideal is principal is called a principal ideal domain (PID).

$F[x]$ is a PID if F is a field. A polynomial ring in more variables is not a PID.

Let R be a domain. An element $0 \neq a \in R$ is irreducible if it is not invertible and it cannot be written as a product of non-invertible elements. R is a unique factorization domain (UFD) if:
i) Each $0 \neq a \in R$ can be written in a form $a = up_1 \cdots p_n$, where u is invertible and $p_1, \dots, p_n$ are irreducible.
ii) If $a = v q_1 \cdots q_m$ is another such expression, then $m = n$ and there exists a permutation π of elements $w_1, \dots, w_n$ s.t. $q_i = w_i p_{\pi(i)}$ for each i. We say q_i and $p_{\pi(i)}$ are associated.
Polynomial rings in any number of variables over a field are UFD.

$$\text{PID} \Rightarrow \text{UFD}$$
$$\not\Leftarrow$$

Proposition: For a ring R the following are egivalent:
i) Each ideal is finitely generated.
ii) Each increasing sequence of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ terminates, i.e. $I_m = I_{m+1} = I_{m+2} = \cdots$ for some m.
iii) Each family of ideals in R has a maximal element (for inclusion).

Proof: Commutative algebra.

Definition: A ring satisfying the above properties is called a noetherian ring (noetherski kolobar).

1) Each PID is noetherian.
   $F[x]$ is noetherian if F is a field
2) Each quotient R/I of a noetherian ring R is noetherian.

Fact from commutative algebra:
Theorem [Hilbert basis theorem]: If R is noetherian, then $R[x]$ is noetherian.

Remark: If R is noetherian, then the power series ring $R[[x]]$ is noetherian.

Corollary: If F is a field, then $F[x_1, \dots, x_n]$ is noetherian.

Corollary: Every finitely generated algebra over a field is noetherian.

2. Affine varieties and Zariski topology

afine raznoterosti

October 6, 2025

We will always work over an algebraically closed field $\mathbb{k}$.

<u>Definition</u>: The n-dimensional affine space over $\mathbb{k}$ is $\mathbb{A}^n = \mathbb{A}^n_{\mathbb{k}} = \{(a_1, \dots, a_n) \mid a_i \in \mathbb{k} \text{ for each } i\}$.
As a set, $\mathbb{A}^n = \mathbb{k}^n$, but $\mathbb{k}^n$ has an additional structure of a vector space, so we use a different notation.

affine space - translated vec. space
- not important where the origin is

$n=1$: $\mathbb{A}^1$: affine line
$n=2$: $\mathbb{A}^2$: affine plane

<u>Definition</u>: Let $S \subseteq \mathbb{k}[x_1, \dots, x_n]$ be a set of polynomials. The (affine) zero locus of S is the set
$V(S) := \{(a_1, \dots, a_n) \in \mathbb{A}^n \mid \forall f \in S.\ f(a_1, \dots, a_n) = 0\}$.

This set contains the set off all common zeroes of polynomials in S. If $S = \{f_1, \dots, f_m\}$, then we write $V(f_1, \dots, f_n)$ instead of $V(\{f_1, \dots, f_n\})$.

<u>Definition</u>: A set $X \subseteq \mathbb{A}^n$ is an affine variety if $X = V(S)$ for some set $S \subseteq \mathbb{k}[x_1, \dots, x]$.
some authors also additionally assume irreducibility

<u>Examples</u>: i) $\emptyset = V(1)$
ii) $\mathbb{A}^n = V(0)$
iii) Each point is an affine variety:
$\{(a_1, \dots, a_n)\} = V(x_1 - a_1, \dots, x_n - a_n)$

iv) All affine spaces (and in particular all vector spaces) are affine spaces, as they are solutions of systems of linear equations.

v) Plane affine algebraic curves are affine varieties. They are defined as $\underbrace{\{(a,b) \in \mathbb{A}^2 \mid p(a,b) = 0\}}_{=V(p)}$ where $p \in \Bbbk[x,y]$.

vi) If $p \in \Bbbk[x_1, \dots, x_n]$, then $V(p) = \{(a_1, \dots, a_n) \in \mathbb{A}^n \mid p(a_1, \dots, a_n) = 0\}$ is called a hypersurface.

Lemma: If $S_1 \subseteq S_2 \subseteq k[x_1, \dots, x_n]$, then $V(S_2) \subseteq V(S_1)$.

Proof: Obvious.

Proposition: Let $S \subseteq k[x_1, \dots, x_n]$ and I the ideal generated by S. Then $V(I) = V(S)$.

Proof: $S \subseteq I$, so $V(I) \subseteq V(S)$ follows from the Lemma.

($\supseteq$): Assume we have $a \in V(S) \setminus V(I)$. Then there is $f \in I$ such that $f(a) \neq 0$. I is generated by S, so there exist $g_1, \dots, g_m \in \Bbbk[x_1 \dots, x_n]$ and $h_1, \dots, h_m \in S$ s.t. $f = g_1 h_1 + \dots + g_m h_m$.

$$0 \neq f(a) = g_1(a) \underbrace{h_1(a)}_{=0, \text{ because } a \in V(S)} + \dots + g_m(a) h_m(a) = 0 \quad \text{↯}$$

We get $V(S) = V(I)$. ▨

Corollary: Varieties in $\mathbb{A}^n$ are exactly sets of the form $V(I)$, where $I \trianglelefteq \Bbbk[x_1, \dots, x_n]$.

It may happen that $I_1 \neq I_2$, but $V(I_1) = V(I_2)$.

Example: in $\mathbb{A}^1$: $V(x^2) = \{0\} = V(x)$

$\mathbb{k}[x_1, \dots, x_n]$ is noetherian, so all ideals are finitely generated. If $I = (f_1, \dots, f_m)$, then $V(f_1, \dots, f_n) = V(I)$.

Corollary: Affine varieties in $\mathbb{A}^n$ are exactly the sets $V(S)$ where S is a finite set.

Lemma: (i) For any family $\{S_j\}_{j \in J}$ of subsets of $\mathbb{k}[x_1, \dots, x_n]$ we have $V(\bigcup_{j \in J} S_j) = \bigcap_{j \in J} V(S_j)$.

ii) For any polynomials $f_1, \dots, f_s, g_1, \dots, g_t \in \mathbb{k}[x_1, \dots, x_n]$ we have $V(f_1, \dots, f_s) \cup V(g_1, \dots, g_s) = V(f_i g_j \mid 1 \leq i \leq s,\ 1 \leq j \leq t)$.

Proof: $a \in V(\bigcup_{j \in J} S_j) \iff \forall f \in \bigcup_{j \in J} S_j .\ f(a) = 0$

$$\iff \forall j \in J.\ \forall f \in S_j .\ f(a) = 0$$

$$\iff \forall j \in J.\ a \in V(S_j)$$

$$\iff a \in \bigcap_{j \in J} V(S_j)$$

(ii): Assume $a \in V(f_1, \dots, f_s) \cup V(g_1, \dots, g_t)$. Then

$$a \in V(f_1, \dots, f_s) \quad \text{or} \quad a \in V(g_1, \dots, g_t).$$

$$\Rightarrow \quad \forall i.\ f_i(a) = 0 \quad \text{or} \quad \forall j.\ g_j(a) = 0$$

In both cases $f_i(a) g_j(a) = 0 \ \forall i. \forall j$

$\Rightarrow \quad a \in V(f_i g_j \mid 1 \le i \le s,\ 1 \le j \le t).$

Conversely, assume $a \notin V(f_1, \dots, f_s) \cup V(g_1, \dots, g_t)$.

$\exists i$. st. $f_i(a) \neq 0$ and $\exists j$ s.t. $g_j(a) \neq 0 \Rightarrow f_i(a) g_j(a) \neq 0$

$\Rightarrow a \notin V(f_i g_j \mid 1 \le i \le s,\ 1 \le j \le t).$ $\square$

Corollary: (1) $\emptyset, \mathbb{A}^n$ are affine varieties
(2) If $\{X_j\}_{j \in J}$ is any family of varieties, then $\bigcap_{j \in J} X_j$ is also an affine variety.
(3) If $X, Y \subseteq \mathbb{A}^n$ are affine varieties, then $X \cup Y$ is an affine variety.

(1)-(3) are axioms of closed sets of some topology, so affine varieties are exactly the closed sets of some topology on $\mathbb{A}^n$. This topology is called the Zariski topology on $\mathbb{A}^n$.

On subsets of $\mathbb{A}^n$ we define the Zariski topology as a relative topology: Let $X \subseteq \mathbb{A}^n$ be an arbitrary set. A subset $Z \subseteq X$ is Zariski closed in X if there exists an affine variety $Y \subseteq \mathbb{A}^n$ s.t. $Z = X \cap Y$. In particular, if X is an affine variety, then a set $Z \subseteq X$ is closed $\Leftrightarrow$ it is an affine variety.

If the topology is not mentioned explicitly, we will always mean the Zariski topology.

Examples: Zariski topology on $\mathbb{A}^1$:
Zariski closed sets are common zeroes of finitely many polynomials. Each nonzero in 1 variable has finitely many zeroes. $\Rightarrow$ All closed sets are finite.
Converse is clear: given a finite set in $\mathbb{A}^1$, it is easy to find a polynomial whose zeroes are precisely the elements of the given set.
$\Rightarrow$ On $\mathbb{A}^1$ the Zariski topology is equal to the topology of finite complements.

The example shows that the Zariski topology is NOT Hausdorff: every two open sets of $\mathbb{A}^1$ intersect (and the same holds for open subsets in $\mathbb{A}^n$).

Example: Zariski closed sets in $\mathbb{A}^2$ are $\mathbb{A}^2$, $\emptyset$, finite unions of points and affine algebraic curves.

Open sets in the Zariski topology are complements of varieties.

Definition: Let $p \in \mathbb{k}[x_1, \dots, x_n]$. The set $D(p) := \mathbb{A}^n \setminus V(p) = \{a \in \mathbb{A}^n \mid p(a) \neq 0\}$ is called a distinguished open set /subset (odlikovana odprta množica /podmnožica) of p in $\mathbb{A}^n$.

Example: Distinguished open sets in $\mathbb{A}^2$ are complements of algebraic curves.

$f, g \in \mathbb{k}[x_1, \dots, x_n]$
$D(f) \cap D(g) = \{a \in \mathbb{A}^n \mid f(a) \neq 0 \wedge g(a) \neq 0\}$

$= \{a \in \mathbb{A}^n \mid f(a)g(a) \neq 0\}$
$= D(f \cdot g)$

$\Rightarrow$ The intersection of distinguished open subsets is a distinguished open subset.

Distinguished open subsets form a basis of the Zariski topology: every open subset is a finite union of distinguished open subsets.

Let $U \subseteq \mathbb{A}^n$ be an open subset. Then $Z = \mathbb{A}^n \setminus U$ is closed, so an affine variety. Therefore there exist polynomials $f_1, \ldots, f_m$ s.t. $Z = V(f_1, \ldots, f_m) = \{a \in \mathbb{A}^n \mid \forall i.\ f_i(a) = 0\} =$
$= \bigcap_{i=1}^{m} V(f_i) \Rightarrow U = \bigcup_{i=1}^{m} D(f_i)$.

3. V-I correspondence and Nullstellensatz

„Če tega ne prevajajo v angleščino, tudi v slovenščino ne bomo."

<u>Definition</u>: For each subset $X \subseteq \mathbb{A}^n$ we define
$I(X) := \{f \in \mathbb{k}[x_1, \ldots, x_n] \mid \forall a \in X.\ f(a) = 0\}$. This is an ideal in $\mathbb{k}[x_1, \ldots, x_n]$ called the ideal of X. (easy exercise)

$$\{\text{varieties in } X\} \underset{V}{\overset{I}{\rightleftarrows}} \{\text{ideals in } \mathbb{k}[x_1, \ldots, x_n]\}$$

These two maps are not inverse to each other. For example, we know that $V(x^2) = V(x) \Rightarrow$
$I(V(x^2)) = I(V(x))$.

<u>Definition</u>: Let $I_1, I_2 \trianglelefteq R$. The product of ideals I_1, I_2 is
$I_1 I_2 = \{\sum_{i=1}^{m} a_i b_i \mid m \in \mathbb{N},\ a_i \in I_1,\ b_i \in I_2\}$.

Lemma: Product of ideals is an ideal.

Proof: exercise

Definition: Let $I \triangleleft R$. The radical of I is $\sqrt{I} = \mathrm{rad}(I) = \{a \in R \mid a^m \in I \text{ for some } m \in \mathbb{N}\}$. The ideal $I \triangleleft R$ is radical if $I = \sqrt{I}$.

Lemma: Radical of an ideal is an ideal.

Exercise: show that if $a^n \in I$ and $b^m \in I$, then $(a+b)^{m+n-1} \in I$.

Example: If $I = ((x-a_1)^{k_1}(x-a_2)^{k_2} \cdots (x-a_r)^{k_r})$, then $\sqrt{I} = ((x-a_1)(x-a_2) \cdots (x-a_r))$. Proof: exercise.

Proposition: (1) $I(\emptyset) = \Bbbk[x_1, \dots, x_n]$.

(2) $I(\mathbb{A}^n) = (0)$

(3) If $I_1 \subseteq I_2$, then $V(I_2) \subseteq V(I_1)$.

(4) If $X_1 \subseteq X_2$, then $I(X_2) \subseteq I(X_1)$.

(5) $X \subseteq V(I(X))$ for each $X \subseteq \mathbb{A}^n$.

(6) $S \subseteq I(V(S))$ for each $S \subseteq \Bbbk[x_1, \dots, x_n]$.

(7) $V(S) = V(I(V(S)))$ $\forall S \subseteq \Bbbk[x_1, \dots, x_n]$.

(8) If $X \subseteq \mathbb{A}^n$ is a variety, then $X = V(I(X))$.

(9) If $X \subseteq \mathbb{A}^n$ is any set, then $V(I(X)) = \overline{X}$ (Zariski closure of X), $I(X) = I(\overline{X})$.

(10) $I(X)$ is always a radical ideal.

(11) $I(X) = I(V(I(X)))$ $\forall X \subseteq \mathbb{A}^n$.

(12) $V(I) = V(\sqrt{I})$ for each ideal.

(13) $V(I_1) \cup V(I_2) = V(I_1 \cap I_2) = V(I_1 I_2)$ for all ideals I_1, I_2.

(14) $V(I_1) \cap V(I_2) = V(I_1 + I_2)$ for all ideals I_1, I_2.

(15) $I(X \cup Y) = I(X) \cap I(Y)$ $\forall$ varieties X, Y

(16) $I(X) + I(Y) \subseteq I(X \cap Y)$ $\forall$ varieties X, Y

Proof: (2) It is clear that 0 vanishes everywhere. We have to prove that it is the only such polynomial! We prove it with induction on n.

$\underline{n=1}$: Let f be a polynomial in 1 variable that vanishes everywhere on $\mathbb{A}^1$. Since $\mathbb{k}$ is algebraically closed, it is infinite and the only polynomial that vanishes everywhere it is the zero polynomial.

$\underline{n \mapsto n+1}$: Let $f \in \mathbb{k}[x_1, \dots, x_{n+1}]$ vanish everywhere on $\mathbb{A}^{n+1}$. Write $f(x_1, \dots, x_n) = \sum_{i=0}^{d} g_i(x_i, \dots, x_n) x_{n+1}^i$.

Take any $(a_1, \dots, a_n) \in \mathbb{A}^n$. Then $f(a_1, \dots, a_n, x_{n+1})$ is a polynomial in 1 variable that vanishes everywhere by the assumption. By case $n=1$, all coefficients of $f(a_1, \dots, a_n, x_{n+1})$ are zero.

$\Rightarrow \forall i \quad g_i(a_1, \dots, a_n) = 0 \quad \forall (a_1, \dots, a_n) \in \mathbb{A}^n$

$\underset{\text{ind. assumption}}{\Rightarrow} \quad g_i$ is the zero polynomial $\forall i$

$\Rightarrow f$ is the zero polynomial. ☒

October 10, 2025

(11): exercise class

(7): similar proof

(8): the same as 7

(9): $\bar{X} = V(I(X))$

Clear: $X \subseteq V(I(X))$

Suppose that Z is a variety such that $X \subset Z \quad | I$

$I(Z) \subseteq I(X) \quad | V$

$V(I(Z)) \subseteq \underset{\substack{\uparrow \\ Z \text{ is a variety}}}{V(I(Z)) = Z}$

$\Rightarrow V(I(X))$ is the smallest closed set that contains X

(13) $V(I_1) \cup V(I_2) = V(I_1 \cap I_2) = V(I_1 I_2)$

Suppose $I_1 = (f_1, \dots, f_s)$ and $I_2 = (g_1, \dots, g_t)$.

Then: $I_1 I_2 = (f_i g_j \,;\, 1 \le i \le s,\ 1 \le j \le t)$.

We know that $V(\overbrace{f_1, \dots, f_s}^{I_1}) \cup V(\underbrace{g_1, \dots, g_t}_{I_2}) =$

$$= V(\underbrace{f_i g_j \mid 1 \le i \le s,\ 1 \le j \le t}_{I_1 I_2})$$

If $a \in V(I_1) \cup V(I_2)$, then $f(a) = 0\ \forall f \in I$ or $g(a) = 0\ \forall g \in I_2$.
In both cases $h(a) = 0\ \forall h \in I_1 \cap I_2 \Rightarrow a \in V(I_1 \cap I_2) \Rightarrow$
$\Rightarrow V(I_1) \cup V(I_2) \subseteq V(I_1 \cap I_2)$.

$I_1 I_2 \subseteq I_1 \cap I_2 \quad \Rightarrow V(I_1 \cap I_2) \subseteq V(I_1 I_2)$

Other parts: exercise. ∎

$V(I(X)) = X$ for a variety X

$I(V(J)) \neq J$ for ideal J

in general

We will use the following result from commutative algebra.

Proposition: Let F be a field and let E be a finitely generated F-algebra which is also a field. Then E is a finite algebraic extension of F.

Corollary: Let A be a finitely generated commutative algebra over $\mathbb{k}$ ($\mathbb{k}$ alg. closed) and let M be some maximal ideal in A. Then $A/M \cong \mathbb{k}$.

Proof: A/M is finitely generated and a field, as M is a maximal ideal. By proposition A/M is a finite algebraic extension of $\mathbb{k}$. $\mathbb{k}$ is algebraically closed $\Rightarrow$ $A/M \cong \mathbb{k}$. ∎

Theorem [Weak Nullstellensatz]:

(1) Maximal ideals in the polynomial ring are exactly the ideals of the form $(x_1-a_1, \dots, x_n-a_n)$ for some $a_1, \dots, a_n \in \mathbb{k}$.

(2) If J is a proper ideal of $\mathbb{k}[x_1, \dots, x_n]$ then $V(J) \neq \emptyset$.

It is crucial to have an algebraically closed field:

- over $\mathbb{R}$: $V(x^2+1) = \emptyset$

  (x^2+1) is a maximal ideal in $\mathbb{R}[x]$

Proof: (1) Let $a_1, \dots, a_n \in \mathbb{k}$. We want to prove that $M = (x_1-a_1, \dots, x_n-a_n)$ is a maximal ideal.

Define a ring homomorphism

$$\varphi: \mathbb{k}[x_1, \dots, x_n] \longrightarrow \mathbb{k}$$
$$x_i \longmapsto a_i$$
$$f(x_1, \dots, x_n) \longmapsto f(a_1, \dots, a_n)$$

φ is surjective: for each $a \in \mathbb{k}$ the constant polynomial a maps to a

$\Rightarrow \underset{\text{field}}{\mathbb{k}} \cong \mathbb{k}[x_1, \dots, x_n]/\ker \varphi$

$\Rightarrow \ker \varphi$ is a maximal ideal

It is enough to show that $\ker \varphi = (x_1-a_1, \dots, x_n-a_n)$.

Obviously $(x_1-a_1, \dots, x_n-a_n) \subseteq \ker \varphi$.

For the other inclusion take $f \in \ker \varphi$.

We divide f by x_1-a_1 and the remainder belongs to $\mathbb{k}[x_2, \dots, x_n]$. We divide the remainder by x_2-a_2 and get the remainder in $\mathbb{k}[x_3, \dots, x_n]$, ...

$\Rightarrow f = \sum_{i=1}^{n} g_i (x_i - a_i) + b$ for some $g_i \in \mathbb{k}[x_i, x_{i+1}, \dots, x_n]$ and $b \in \mathbb{k}$

$f \in \ker \varphi \Rightarrow$

$0 = \varphi(f) = \sum_{i=1}^{n} \varphi(g_i) \varphi(x_i - a_i) + \varphi(b) = b \Rightarrow b = 0$

$\Rightarrow f \in (x_1-a_1,\dots, x_n-a_n)$

(We didn't use algebraic closure, $(x_1-a_1,\dots,x_n-a_n)$ is a maximal ideal in $F[x_1,\dots,x_n]$ for any field F.)

We have to prove there are no other maximal ideals.

Let $M \trianglelefteq \mathbb{k}[x_1,\dots,x_n]$ be an arbitrary maximal ideal.

$\mathbb{k}$ is alg. closed, $\mathbb{k}$ is fin. generated $\mathbb{k}$-algebra so $\mathbb{k}[x_1,\dots,x_n]/M \cong \mathbb{k}$ by previous corollary.

Define the maps $\pi : \mathbb{k}[x_1,\dots,x_n] \xrightarrow{\substack{\text{canonical}\\ \text{projection}}} \mathbb{k}[x_1,\dots,x_n]/M = \mathbb{k}$

Denote $a_i = \pi(x_i) \in \mathbb{k}$ for each i.

π is a ring homomorphism $\Rightarrow \pi(f) = f(\pi(x_1),\dots,\pi(x_n))$
$= f(a_1,\dots,a_n)$

We already proved $\ker\pi = (x_1-a_1,\dots,x_n-a_n)$. By the construction $\ker\pi = M$.

(2): If J is a proper ideal in $\mathbb{k}[x_1,\dots,x_n]$, it is contained in some maximal ideal M.

By (1), M is of the form $(x_1-a_1,\dots,x_n-a_n)$ for some $a_1,\dots,a_n \in \mathbb{k}$.

$$V(M) = V(x_1-a_1,\dots,x_n-a_n) = \{(a_1,\dots,a_n)\} \neq \emptyset$$

$\Rightarrow \emptyset \neq V(M) \subseteq V(J)$. ▨

<u>Corollary</u>: We have mutually inverse bijections

$$\{\text{points in } \mathbb{A}^n\} \underset{V}{\overset{I}{\rightleftarrows}} \left\{\begin{matrix}\text{maximal ideals}\\ \text{in } \mathbb{k}[x_1,\dots,x_n]\end{matrix}\right\}$$

$$(a_1,\dots,a_n) \longleftrightarrow (x_1-a_1,\dots,x_n-a_n)$$

<u>Theorem</u> [Hilbert's Nullstelensatz]:

$I(V(J)) = \sqrt{J}$ for each $J \trianglelefteq \mathbb{k}[x_1,\dots,x_n]$.

<u>Proof</u>: One inclusion is easy.

If $f \in \sqrt{J}$, then $f^m \in J$ for some m.

If $a \in V(J)$, then $f^m(a) = 0 \Rightarrow f(a) = 0 \Rightarrow f \in I(V(J))$.

($\subseteq$): Let $f \in I(V(J))$.

We consider the ring $\mathbb{k}[x_1, \dots, x_n, y]$ (with a variable added) and the ideal

$$\tilde{J} = (J) + (fy - 1) \trianglelefteq \mathbb{k}[x_1, \dots, x_n, y]$$

one generator is added to J

First we show that $V(\tilde{J})$ is empty.

Suppose $(a_1, \dots, a_n, a_{n+1}) \in V(\tilde{J})$.

$$\Rightarrow \forall g \in \tilde{J}.\ g(a_1, \dots, a_n, a_{n+1}) = 0$$

If $g \in J \trianglelefteq \mathbb{k}[x_1, \dots, x_n]$, we get $g(a_1, \dots, a_n) = 0$.

$\Rightarrow (a_1, \dots, a_n) \in V(J)$

$f \in (I(V(J))) \Rightarrow f(a_1, \dots, a_n) = 0$

$(a_1, \dots, a_n, a_{n+1}) \in V(fy - 1) \Rightarrow f(a_1, \dots, a_n) \cdot a_{n+1} = 1$

$\Rightarrow f(a_1, \dots, a_n) \neq 0$ ... contradiction $\Rightarrow V(\tilde{J}) = \emptyset$

By weak Nullstelensatz we get that $\tilde{J}$ is not proper, so $1 \in \tilde{J}$.

$\mathbb{k}[x_1, \dots, x_n]$ is noetherian $\Rightarrow$ there exist $g_1, \dots, g_m \in \mathbb{k}[x_1, \dots, x_n]$ such that $J = (g_1, \dots, g_m)$.

$1 \in (g_1, \dots, g_m, fy - 1) \Rightarrow \exists\ p_1, \dots, p_m, q \in \mathbb{k}[x_1, \dots, x_n, y]$.

$$1 = p_1 g_1 + \dots + p_m g_m + q(fy - 1) \qquad (*)$$

Let N be the largest number such that y^N appears in each $p_1, \dots, p_m$. We multiply $(*)$ with f^N and rearrange the terms in such a way that each y appears together with f as fy. We get

$$f^N = P_1(x_1, \dots, x_n, fy) g_1 + \dots + P_m(x_1, \dots, x_n, fy) g_m + Q(x_1, \dots, x_n, fy) \cdot (fy - 1)$$

We look at this equation modulo $(fy-1)$:

$$f^N \equiv p_1(x_1,\dots,x_n,fy)g_1 + \dots + p_m(x_1,\dots,x_n,fy)g_m$$

$$\equiv p_1(x_1,\dots,x_n,1)g_1 + \dots + p_m(x_1,\dots,x_n,1)g_m \pmod{(fy-1)}$$

$$\Rightarrow \underbrace{f^N - \sum_{i=1}^m p_i(x_1,\dots,x_n,1)g_i}_{\text{we don't have } y \text{ here}} \in (fy-1) \cap \mathbb{k}[x_1,\dots,x_n] = (0)$$

$$\Rightarrow f^N = \sum_{i=1}^m \underbrace{p_i(x_1,\dots,x_n,1)}_{\in \mathbb{k}[x_1,\dots,x_n]} \cdot g_i \in J \Rightarrow f \in \sqrt{J} \qquad \blacksquare$$

Corollary: V and J are mutually reverse bijections

$$\{\text{radical ideals}\} \underset{J}{\overset{V}{\rightleftarrows}} \{\text{affine varieties}\}.$$

Corollary: $I(X \cap Y) = \sqrt{I(X) + I(Y)}$ if X, Y are affine affine varieties.

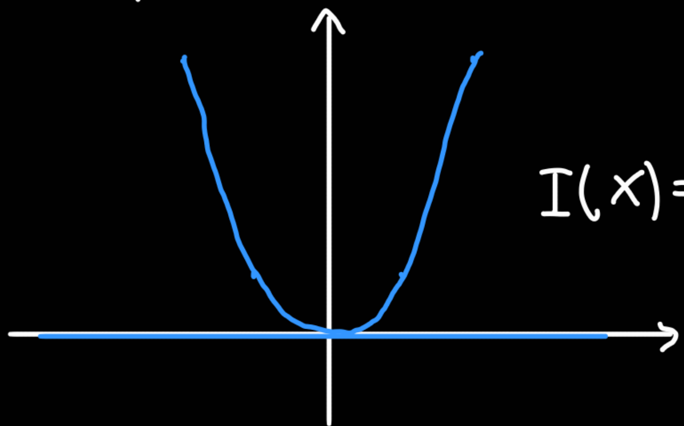
Proof: $I(X \cap Y) = I(V(I(X)) \cap V(I(Y)))$

$$= I(V(I(X) + I(Y)))$$

Nullstelensatz

$$= \sqrt{I(X) + I(Y)} \qquad \blacksquare$$

Example: $X = V(y^2 - x)$, $Y = V(y)$



$X \cap Y = \{(0,0)\}$

$I(X) = I(V(y-x^2)) = \sqrt{(y-x^2)} = (y-x^2)$

$I(Y) = (y)$

principal ideal generated by polynomials without multiple factors

$I(X) + I(Y) = (y - x^2, y) = (y, x^2)$

This ideal is not radical, as it contains x^2, but not x
$\Rightarrow I(X) + I(Y) \neq I(X \cap Y)$.

$$I(X \cap Y) = I(\{(0,0)\}) = (x, y) = \sqrt{(x^2, y)}$$

$I(X) + I(Y)$ is not radical, because X and Y have a common tangent in $(0,0)$.

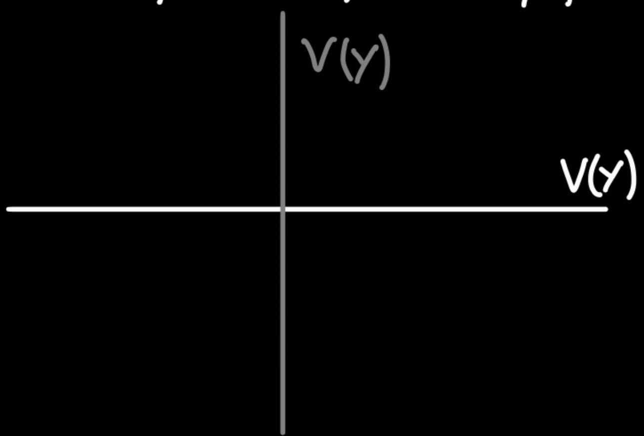
4. Irreducibility of varieties

A topological space X is disconnected if it is a union of two disjoint closed subsets. It is connected otherwise.

Definition: A topological space X is reducible if there exist proper closed subsets $X_1, X_2 \subsetneq X$ such that $X = X_1 \cup X_2$. X is irreducible otherwise.

Definition: An affine variety X is reducible if there exist varieties $X_1, X_2 \subsetneq X$ such that $X = X_1 \cup X_2$. X is irreducible otherwise.

Example: $V(xy) = V(x) \cup V(y)$ is reducible



Lemma: If X is an irreducible variety, then the following holds:

1) Each non-empty open subset of X is dense in X. (in the Zariski topology)
2) Every two non-empty open subsets of X intersect.

Proof: (1) If U is open and $\overline{U}=X$, then we have a decomposition $X=\overline{U}\cup(X\setminus U)$

(2): If U_1, U_2 are open, non-empty, and $U_1\cup U_2=\emptyset$, then $X=(X\setminus U_1)\cup(X\setminus U_2)$. $\blacksquare$

Definition: Let $I\triangleleft R$. slovene: „praideal"

(1) I is a prime ideal if $I\neq R$ and the following holds: If $ab\in I$ for some $a,b\in R$, then $a\in I$ or $b\in I$.

2) I is a primary ideal if $I\neq R$ and the following holds: If $ab\in I$ for some $a,b\in R$, then $a\in R$ or $b^m\in I$ for some $m\in\mathbb{N}$. slovene: „primarni ideal"

Lemma: A radical of a primary ideal is a prime ideal.

Proof: Let I be primary and $ab\in\sqrt{I}$. Then $(ab)^r=a^rb^r\in I$ for some $r\in\mathbb{N}$.

Since I is primary, we get $a^r\in I$ or $(b^r)^m=b^{rm}\in I$ for some m.

$$\underset{a\in\sqrt{I}}{\Downarrow} \qquad \underset{b\in\sqrt{I}}{\Downarrow}$$

$\blacksquare$

Corollary: A primary ideal which is radical is a prime ideal.

Theorem: $X \subseteq \mathbb{A}^n$ is an irreducible variety $\Leftrightarrow$ $I(X)$ is a prime ideal.

Proof: ($\Rightarrow$): Assume X is irreducible and let $fg \in I(X)$.
Define $X_1 = X \cap V(f)$ and $X_2 = X \cap V(g)$. Then $X_1, X_2 \subseteq X$
$\Rightarrow X_1 \cup X_2 \subseteq X$.
Let $a \in X$. $fg \in I(X)$ so $f(a)g(a) = 0$ so $f(a) = 0$ or $g(a) = 0$ $\Rightarrow a \in V(f)$ or $a \in V(g)$ $= X = X_1 \cup X_2$.
X_1, X_2 are closed, so by irreducibility of X one of them is equal to X.
WLOG: $X_1 = X$ $(X_1 = X \cap V(f))$
$\Rightarrow X \subseteq V(f) \Rightarrow \forall a \in X.\ f(a) = 0 \Rightarrow f \in I(X)$

($\Leftarrow$): Assume $I(X)$ is a prime ideal. Let $X = X_1 \cup X_2$ for some $X_1, X_2 \subseteq X$ varieties and suppose that $X_1 \neq X$.
We will show that $I(X) = I(X_2)$.
$X_2 \subseteq X \Rightarrow I(X) \subseteq I(X_2)$
For the other inclusion take $g \in I(X_2)$.

$$X_1 \subsetneq X \Rightarrow I(X) \subsetneq I(X_1) \Rightarrow \exists f \in I(X_1) \setminus I(X)$$

Let $a \in X$ be arbitrary. Then $a \in X_1$ or $a \in X_2$, so $f(a) = 0$ or $g(a) = 0$. So we have $f(a)g(a) = 0$ for each $a \in X$. $\Rightarrow fg \in I(X)$.
$I(X)$ is prime and $f \notin I(X)$, so $g \in I(X)$

$$\Rightarrow I(X_2) \subseteq I(X) \Rightarrow I(X_2) = I(X)$$

$$\Rightarrow \underbrace{V(I(X_2))}_{= X_2} = \underbrace{V(I(X))}_{= X} \Rightarrow X \text{ is irreducible.}$$

$\blacksquare$

Corollary: A hypersurface $V(f)$ where f is a square-free polynomial is irreducible $\Leftrightarrow$ f is irreducible.

$f = g_1^{k_1} \cdots g_r^{k_r}$, g_i irreducible $\Rightarrow k_i = 1 \ \forall i$

Corollary: $\mathbb{A}^n$ is irreducible

Proof: $I(\mathbb{A}^n) = (0)$ is a prime ideal. $\blacksquare$

Corollary: V and I are mutually inverse bijections

$$\left\{\begin{array}{c}\text{irreducible}\\ \text{varieties}\end{array}\right\} \underset{V}{\overset{I}{\rightleftarrows}} \left\{\text{prime ideals}\right\}.$$

Remark:

algebra	geometry
$\Bbbk[x_1, \dots, x_n]$	$\mathbb{A}^n$
maximal ideals	points
radical ideals	affine varieties
prime ideals	irreducible affine varieties

$$\underset{I}{\overset{V}{\rightleftarrows}}$$

Theorem: Each affine variety X can be decomposed as a union $X = X_1 \cup \dots \cup X_m$ where $m \in \mathbb{N}_0$ and $X_1, \dots, X_m$ are non-empty irreducible varieties.
Moreover, if $X_i \not\subseteq X_j$ whenever $i \neq j$, then the decomposition is unique up to permutation.

Definition: If $X = X_1 \cup \dots \cup X_m$ where $X_1, \dots, X_m$ are irreducible varieties and $X_i \not\subseteq X_j$, whenever $i \neq j$, then $X_1, \dots, X_m$ are called *irreducible components* of X.

slovene: nerazcepne komponente

Proof: If $X \neq \emptyset$, then the decomposition exists (for $m=0$) and it is unique.
Assume now that $X \neq \emptyset$.
Existance of the composition:
Assume that no decomposition $X = X_1 \cup \cdots \cup X_m$ where $X_1, \ldots, X_n$ are irreducible, exists. Then X is reducible (as otherwise $X = X$ is such decomposition for $m=1$).
$X = X_1 \cup X_1'$ for some varieties X_1 and X_1', and at least one of them is not a union of irr. varieties.
WLOG: this is X_1, X_1 has to be reducible: $X_1 = X_2 \cup X_2'$ for some var. X_2, X_2' and at least one of them is not a union of irr. variaties.

$\vdots$

We get a strictly decreasing chain of varieties:

$$X \supsetneq X_1 \supsetneq X_2 \supsetneq \cdots \qquad / I$$

$$I(X) \subsetneq I(X_1) \subsetneq I(X_2) \subsetneq \cdots$$

This is a strictly increasing sequence of ideals in $\mathbb{k}[x_1, \ldots, x_n]$, which contradicts the noetherian property.
$\Rightarrow X$ can be decomposed into a union of irreducible varieties.

Uniqness: $X = X_1 \cup \cdots \cup X_r = X_1' \cup \cdots \cup X_s'$ where X_i, X_i' are irreducible, $X_i \not\subseteq X_j$, $X_i' \subseteq X_j'$ whenever $i \neq j$.
Take arbitrary $i \in \{1, \ldots, r\}$.

$$X_i = X_i \cap X = X_i \cap (X_1' \cup \cdots \cup X_s')$$
$$= \bigcup_{j=1}^{s} (X_i \cap X_j'), \quad X_i \text{ is irreducible}$$

therefore $X_i = X_i \cap X_j'$ for some $j \Rightarrow X_i \subseteq X_j'$
The same argument shows that there exists $l \in \{1, \ldots, r\}$ such that $X_j' \subseteq X_l \Rightarrow X_i \subseteq X_j' \subseteq X_l$.

By assumption $l = i \Rightarrow X_j' = X_i$.
$\Rightarrow$ We get uniqness (and in particular, $r=s$). $\blacksquare$

<u>Remark</u>: The crucial part was to show the fact that there does not exist an infinite sequence of closed subsets, each properly contained in the previous one, $X \supsetneq X_1 \supsetneq X_2 \supsetneq$.
We say that varieties are noetherian topological spaces.

<u>Remark</u>: In commutative algebra an important theorem says that each ideal in a noetherian ring can be written as an intersection of primary ideals. Using this fact we could prove the theorem as follows:

$$I(X) = Q_1 \cap Q_2 \cap \cdots \cap Q_m, \quad Q_i \text{ primary } / V$$

$$X = V(I(X)) = V(Q_1 \cap \cdots \cap Q_m)$$

$$= V(Q_1) \cup \cdots \cup V(Q_m)$$

To show that $V(Q_i)$ are irreducible, apply I:
$I(V(Q_i)) = \sqrt{\underset{\substack{\uparrow \\ \text{primary}}}{Q_i}} = \text{prime ideal} \Rightarrow V(Q_i)$ irreducible.

If we use only minimal prime ideals over $I(X)$ then we also get the uniqueness statement.