Algebraic geometry

a desperate attempt to avoid failure

1. Blitzkrieg z GA

Noetherowskość, wymiary

For any $A \subseteq K[\overline{X}]$ we define

$$V(A) = \{\overline{x} \in K^n \ : \ \forall\ F \in A\ F(\overline{x}) = 0\}.$$

Let $I, J \trianglelefteq K[\overline{X}]$. Then

- $A_0 \subseteq A_1 \implies V(A_1) \subseteq V(A_0)$
- $V(\bigcup A_i) = \bigcap V(A_i)$
- $V(I \cap J) = V(IJ) = V(I) \cup V(J)$
- $V(I + J) = V(I) \cap V(J)$

For any $A \subseteq K[\overline{X}]$ there is a finite $A_0 \subseteq A$ such that $V(A) = V(A_0)$ (by the Hilbert's basis theorem).

Definicja 1.1: Noetherian ...

A topological space X is called **Noetherian** if any descending chain of closed subsets of X stabilizes. Meanwhile, a ring is Noetherian if any ascending chain of ideals stabilizes.

Definicja 1.2: irreducible space

A space X is irreducible if it is not a non-trivial union of its two closed subseteq, i.e. for any $Y_1, Y_2 \subseteq X$ closed $X = Y_1 \cup Y_2$ then $X = Y_1$ or Y_2.

If X is a Noetherian space then

- $X = X_1 \cup ... \cup X_k$ for some $X_1, ..., X_k \subseteq X$ irreducible such that $X_i \not\subseteq X_j$ for $i \neq j$
- this sequence is unique up to permutation of indices

An affinie algebraic set $V(A)$ is **affine variety** if it is irreducble as a topological space with the Zariski topology.

Definicja 1.3: dimension

$\dim(X) = n$ if there is a strictly decreasing sequence of irreducible closed subsets of X such that

$$X_n \subsetneq X_{n-1} \subsetneq \dots \subsetneq X_0 \subseteq X$$

For $V \subseteq \mathbb{A}^n$ we define the **affine coordinate ring of V** as

$$K[v] := \{f \in \text{Func}(V, K) \ : \ \exists F \in K[\overline{X}] \ : F|_V = f\}$$

$K(V)$ is the field of fractions of $K[V]$, called **the field of rational functions on V**.

The **ideal of V** is defined as

$$\ker\left(K[\overline{X}] \ni F \mapsto F|_V \in K[V]\right)$$

which is the same as

$$I(V) = \{F \in K[\overline{X}] \ : \ \forall\, \overline{x} \in V\ F(\overline{x}) = 0\}.$$

The **Zariski closure** of V_0 is the set $V(I(V_0))$.

Twierdzenie 1.4: Hillbert's Nullstellensatz

weak $I \trianglelefteq K[\overline{X}] \wedge; I \neq K[\overline{X}] \implies V(I) \neq \emptyset$
strong/regular $I \trianglelefteq K[\overline{X}] \implies I(V(I)) = \sqrt{I}$

If $V \subseteq \mathbb{A}^n$ is Zariski closed, then the following are equivalent

1. V is irreducible
2. $I(V)$ is prime
3. $\exists P \trianglelefteq K[\overline{X}]$ prime such that $V = V(P)$!!the field K needs to be algebraically closed!!
4. $K[V]$ is a domain

Twierdzenie 1.5

If $F \in K[\overline{X}]$ is irreducible, then $V(F)$ is an affine variety.

Let $V \subseteq \mathbb{A}^n$ be an affine algebraic set. Then there is a bijection between $\begin{matrix}\text{radical}\\ \text{prime}\end{matrix}$ ideals of $K[V]$ and the set of Zariski $\begin{matrix}\text{closed}\\ \text{irreducible closed}\end{matrix}$ subsets of V.

Definicja 1.6: Krull dimension

For a ring R we define its Krull dimension $\dim(R)$ as the supremum $k \in \mathbb{N}$ such that there is a strictly increasing (or decreasing) sequence of prime ideals

$$P_0 \subsetneq P_1 \subsetneq \ldots \subsetneq P_k$$

of R.

$$\mathbf{dim}(V) = \mathbf{dim}(K[V])$$

Twierdzenie 1.7

Let R be a finitely generated K-algebra which is a domain. Then

$$\dim(R) = \operatorname{trdeg}_K(R_0)$$

the dimension of R is equal to the transcendental degree of the field of fractions of R over K.

If $R = K[V]$ then $R_0 = K(V)$ and the above statement holds.

Kategoryje

Let $V \subseteq \mathbb{A}^n$ and $W \subseteq \mathbb{A}^m$ be affine algebraic sets. Then $\varphi : V \to W$ is a **morphism** if there are $f_1, \ldots, f_m \in K[V]$ such that

$$\varphi(v) = (f_1(v), \ldots, f_m(v)).$$

For such a morphism we define

$$\varphi^* : K[W] \to K[V]$$
$$\varphi^*(f) = f \circ \varphi.$$

1. The mapping $\varphi \mapsto \varphi^*$ is an isomorphism between the set of morphisms $V \to W$ and the set of morphisms $K[W]$ to $K[V]$.
2. Any finitely generated K-algebra R which is reduced (no nilpotent elements) is isomorphic over V to $K[V]$ for some affine algebraic V.

$$\boldsymbol{V \cong W \iff K[V] \cong_K K[W]}$$

For $f \in K(V)$, the **domain** of f, $\operatorname{dom} f$, is the set of points $v \in V$ such that there are $f_1, f_2 \in K[V]$, $f = \frac{f_1}{f_2}$ and $f_2(v) \neq 0$.

Definicja 1.8

Let $f \in K(V)$ and $v \in V$.

1. f is regular at v if $v \in \operatorname{dom} f$
2. $\mathcal{O}_{V,v} := \{f \in K(V) \ : \ v \in \operatorname{dom} f\}$
3. f is regular if f is regular at each $v \in V$, i.e. $\operatorname{dom} f = V$.

Fakt 1.9

For any $v \in V$

$$\mathcal{O}_{V,v} = K[V]_{I_V(v)} = \{\frac{a}{b} \ : \ a \in K[V], b \in K[V] - I_V(v)\}$$

Denote by

$$\mathfrak{m}_{V,v} \trianglelefteq \mathcal{O}_{V,v}$$

the maximal ideal of $\mathcal{O}_{V,v}$.

f is regular $\iff$ $f \in K[V]$

Lemat 1.10

For a morphism $\varphi : V \to W$ its dual φ^* is a monomorphism $\iff$ φ is **dominant**, i.e. $\varphi(V)$ is Zariski dense in W (is an epimorphism in its category).

A function $\varphi : U \subseteq V \to W$ is a **rational function** between V and W if there are $f_1, ..., f_m \in K(V)$ such that

$$U = \operatorname{dom} f_1 \cap ... \cap \operatorname{dom} f_m$$

and for all $v \in U$ there is $\varphi(v) = (f_1(v), ..., f_m(v))$.

$\varphi : V \dashrightarrow W$ denotes a **dominant rational function** from V to W.

For any field extension $K \subseteq L$ such that L is finitely generated over K there is an affine variety V such that $L \cong_K K(V)$.

The category of affine varieties and dominant rational maps is *entiequivalent* or *dually equivalent* to the category of finitely generated field extensions of K.

Smooooth *like the fur of a newborn goat*

Let R be a ring. The map $\partial R \to R$ is called a **derivation** on R if for all $a, b \in R$

$$\partial(a+b) = \partial(a) + \partial(b)$$

$$\partial(ab) = \partial(a)b + a\partial(b).$$

The **Jacobian matrix** of $\overline{F} = (F_1, ..., F_m)$, $F_i \in K[\overline{X}]$ is

$$J_{\overline{F}} := \begin{pmatrix} \frac{\partial F_1}{\partial X_1} & \cdots & \frac{\partial F_1}{\partial X_n} \\ \vdots & \ddots & \vdots \\ \frac{\partial F_m}{\partial X_1} & \cdots & \frac{\partial F_m}{\partial X_n} \end{pmatrix}$$

Fakt 1.11

If $(G_1, ..., G_k) = I = (F_1, ..., F_m) \trianglelefteq K[\overline{X}]$ and $v \in V(I)$, then

$$\operatorname{rank}(J_{\overline{G}}(v)) = \operatorname{rank}(J_{\overline{F}}(v)).$$

Definicja 1.12: non-singular variety

Let $V \subseteq \mathbb{A}^n$ and $F_1, ..., F_m \in I(V) = (F_1, ..., F_m)$. We say that $a \in V$ is a **non-singular** or smooth point of V if

$$\operatorname{rank}(J_{\overline{F}}(a)) = n - \dim(V).$$

We say that V is a non-singular variety or a smooth variety if V is irreducible and all points of V are smooth.

$F \in K[X, Y]$ and $V = V(F) \subseteq \mathbb{A}^2$

1. $F \notin K \implies |V| = \infty$
2. $|V(F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y})| < \infty \implies \sqrt{(F)} = (F) \ \wedge \ I(V) = (F)$
3. $V(F, \frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}) = \emptyset \implies V$ is smooth

Lemat 1.13

A point $a \in V$ is smooth $\iff \dim_K(I_V(a)/I_V(a)^2) = \dim(V)$.
If V is an affine variety and $a \in V$, then we have

$$I_V(a)/I_V(a)^2 \cong_K \mathfrak{m}_{V,a}/\mathfrak{m}_{V,a}^2$$

A Noetherian local ring $(R, \mathfrak{m})$ is **regular** if $\dim(R) = \dim_{R/\mathfrak{m}}(\mathfrak{m}/\mathfrak{m}^2)$.

The K-vector space $\mathfrak{m}_{V,a}/\mathfrak{m}_{V,a}^2$ is the **cotangent space** of V at a. The dual space is the *tangent space*.

DVR

A local ring $(R, \mathfrak{m})$ is a **discrete valuation ring** if

1. R is Noetherian domain
2. R is not a field
3. $\mathfrak{m}$ is principal (generated by a single element)

In any Noetherian domain R and any $I \lhd R$ we have

$$\bigcup_{n\geq 1} I^n = \{0\}.$$

Any DVR is PID (the generator of $\mathfrak{m}$ is the uniformizing parameter)

Let R be a UFD, $r \in R$ irreducible and R_0 be the field of fractions of R. Define

$$v_r : R_0^* \to \mathbb{Z}$$

$$v_r(r^n \frac{a}{b}) = n, \quad r \not| a,\ r \not| b.$$

We call v_r the **r-addic valuation** on R_0.

Fakt 1.14

R, r, R_0 and v_r as above. Then for all $\alpha, \beta \in R_0^*$

1. $\alpha + \beta \in R_0^* \implies v_r(\alpha + \beta) \geq \min\{v_r(\alpha), v_r(\beta)\}$
2. $v_r(\alpha\beta) = v_r(\alpha) + v_r(\beta)$
3. $v_r(R_0^*) = \mathbb{Z}$

For any irreducible $r, s \in R$ if $(r) = (s)$ then $v_r = v_s$.

Definicja 1.15: discrete valuation

Let L be a field. Any function $v : L^* \to \mathbb{Z}$ satisfying 1-3 from the fact above is called a **(discrete) valuation** on L. For any valuation $v : L^* \to \mathbb{Z}$

- $\mathcal{O}_v := \{\alpha \in L^* \ : \ v(\alpha) \geq 0\} \cup \{0\}$ -> *valuation ring* of v
- $\mathfrak{m}_v := \{\alpha \in L^* \ : \ v(\alpha) > 0\} \cup \{0\}$ -> *valuation ideal* of v

For a valuation $v : L^* \to \mathbb{Z}$, $(\mathcal{O}_v, \mathfrak{m}_n)$ is a DVR.

Twierdzenie 1.16

Let C be an affine curve and $a \in C$. Then a is smooth $\iff$ $(\mathcal{O}_{C,a}, \mathfrak{m}_{C,a})$ is a DVR.

Definicja 1.17

Let C be an affine curve and $a \in C$ be a smooth point

1. a uniformizing parameter $f \in \mathcal{O}_{C,a}$ is a **local parameter** for C at a
2. the unique valuation on $K(C)$ given by $(\mathcal{O}_{C,a}, \mathfrak{m}_{C,a})$ is denoted ord_a
3. for $f \in K(C) - \{0\}$ and $n \in \mathbb{N}_{>0}$
   - $\mathrm{ord}_a(f) = n \implies f$ has a zero at a of order n
   - $\mathrm{ord}_a(f) = -n \implies r$ has a pole at a of order n

$$\mathrm{ord}_a(f) = \dim_K(\mathcal{O}_{C,a}/f\mathcal{O}_{C,a})$$

$$\dim_K(K[X]/(F)) = \sum_{a \in V(F)} \mathrm{ord}_a(F)$$

Definicja 1.18: intersection number

The intersection number of F and G at $a = (x, y) \in \mathbb{A}^2$ is

$$I(a, F \cap G) := \dim_K(\mathcal{O}/(F, G)\mathcal{O}),$$

where

$$\mathcal{O} := K[X, Y]_{(X-x, Y-y)} = K[X, Y]_{I(a)} = \mathcal{O}_{\mathbb{A}^2, a}$$

For curves C_1, C_2 such that $F = I(C_1)$ and $G = I(C_2)$ we define $I(a, C_1 \cap C_2) := I(a, F \cap G)$.

$$I(a, F \cap G) > 0 \iff a \in V(F, G)$$

$$|V(F, G)| < \infty \implies I(a, F \cap G) < \infty$$

F irreducible and $a \in V(F)$ smooth then

$$I(a, F \cap G) = \mathrm{ord}_a(G|_{V(F)}).$$

$$I(a, F \cap G) = I(a, F \cap (G + HF).G, F, H \in K[X, Y]$$

$$I(a, F \cap GH) = I(a, F \cap G) + I(a, F \cap H)$$

$$I(a, F \cap G) > 0 \iff a \in V(F, G)$$

$L_X = V(Y)$, $L_Y = V(Y)$, $C_1 = V(Y^2 - x^3)$, $C_2 = V(Y - X^3)$

- $I(0, L_X \cap C_1) = \text{ord}_0((Y^2 - X^3)|L_X) = 3$
- $I(0, L_Y \cap C_1) = \text{ord}_0((Y^2 - X^3)|L_Y) = 2$
- $I(0, L_X \cap C_2) = \text{ord}_0((Y - X^3)|L_X) = 3$
- $I(0, L_X \cap C_2) = \text{ord}_0((Y - X^3)|L_Y) = 1$

Definicja 1.19

C - a plane curve, $a \in \mathbb{A}^2$
- $L \subseteq \mathbb{A}^2$ **line** if $\exists \alpha, \beta, \gamma \in K$ such that $L = V(\alpha X + \beta Y + \gamma)$ and $(\alpha, \beta) \neq (0, 0)$
- $L \subseteq \mathbb{A}^2$ is **tangent** to C at a if $I(a, L \cap C) > 1$
- $T_a C$ is the union of all tangent lines to C at a

Lemat 1.20

R - ring, $P \trianglelefteq R$ prime, $e \in R - P$ idempotent divisible by every element of $R - P$
$\varphi : R \to R_P$ induces an isomorphism of rings $eR \cong R_P$ preserving the unit elements.

Twierdzenie 1.21

$V = V(F, G)$ is finite

$$\dim_K(K[X, Y]/(F, G)) = \sum_{a \in V} I(a, F \cap G)$$

poprosić o notatki?

Projektywizujem siem

If $x = [a_1 : ... : a_{n+1}] \in \mathbb{P}^n$, then $a_1, ..., a_{n+1}$ are called the **projective** or **homogenous coordinates** of x.

Definicja 1.22: homogenous polynomial

$d, k, d_1, ..., d_k \in \mathbb{N}$ and $H \in K[X_1, ..., X_k]$
- $H = aX_1^{d_1}...X_k^{d_k}$ is a monomial $\implies$ $\deg H = d_1 + ... + d_k$
- H is **homogenous polynomial of degree** d if H is a sum of monomials of degree d

H of degree d is homogenous $\iff \forall\lambda \in K\ H(\lambda X_1, ..., \lambda X_k) = \lambda^d H$.

Definicja 1.23: projective algebraic

$V \subseteq \mathbb{P}^n$ is a **projective algebraic** set if there are homogenous polynomials $F_1, ..., F_k \in K[X_1, ..., X_{n+1}]$ such that

$$V = \{x \in \mathbb{P}^n \ : \ F_1(x) = 0, ..., F_k(x) = 0\}$$

$$\psi_i : \mathbb{A}^n \to \mathbb{P}^n$$
$$\psi_i(a_1, ..., a_n) = [a_1 : ... : a_{i-1} : 1 : a_i : ... : a_n]$$
$$U_i = \{[a_1 : ... : a_{n+1} \in \mathbb{P}^n \ : \ a_i \neq 0\}$$

A line in $\mathbb{P}^2$ is a subset V such that there exists $(\alpha, \beta, \gamma) \in K^3 - \{0\}$ such tat

$$V = \{[a : b : c] \ : \ \alpha a + \beta b + \gamma c = 0\}.$$

1. $\mathbb{P}^n$ with topology defined by closed algebraic subsets is a Noetherian topological space
2. $F_1, ..., F_k \in K[X_1, ..., X_{n+1}]$, $V = \{x \in \mathbb{P}^n \ : \ F_1(x) = 0, ..., F_k(x) = 0\}$
$$\psi^{-1}(V) = V(F_1|_{X_i=1}, ..., F_k|_{X_i=1})$$
$F_j|_{X_i=1}$ is called the **dehomogenization** of H with respect to X_i. Denote it by $\widetilde{F}_j$
3. $W = V(H_1, ..., H_l) \subseteq \mathbb{A}^n$, then
$$U_i \cap \{x \in \mathbb{P}^n \ : \ \widetilde{H}_1(x) = 0, ..., \widetilde{H}_l(x) = 0\} = \psi_i(W)$$
denote the $\{x \ : \ \widetilde{H}_i(x) = 0\}$ by W^*.
4. For closed $V \subseteq \mathbb{A}^n$ we have
   - $\dim V = \dim V^*$,
   - V irreducible $\iff$ V^* irreducible
5. $W \subseteq \mathbb{P}^n$ irreducible, $W \cap U_i \neq \emptyset$, then W is the Zariski closure of $W \cap U_i$

Definicja 1.24

Projective variety is an irreducible projective algebraic set.

Any projective plane curve can be expressed as $V = \{x \in \mathbb{P}^2 \ : \ F(x) = 0\}$ for some $F \in K[X, Y, Z]$. A point $x \in V$ is **smooth** if there is $i \leq n$ such that $x \in U_i$ and $\psi_i^{-1}(x)$ is a smooth point of the affine variety $\psi_i^{-1}(V)$. A point is **singular** if it is not smooth.

Bezout theorem, czyli intersection nr, divisors

Definicja 1.25: intersection number

$x \in \mathbb{P}^2$, $F, H, G \in K[X, Y, Z]$ are homogenous

- i such that $x \in U_i$

$$I(x, F \cap H) = I(\psi_i^{-1}(x), (F|_{X_i=1}) \cap (H|_{X_i=1}))$$

  is the **intersection number**
- F, H irreducible, $V, W \subseteq \mathbb{P}^2$ projective plane curves

$$V = \{x \in \mathbb{P}^2 \ : \ F(x) = 0\}$$

$$W = \{x \in \mathbb{P}^2 \ : \ H(x) = 0\}$$

$$I(x, V \cap G) = I(x, F \cap G)$$

$$I(x, W \cap V) = I(x, F \cap G)$$

Twierdzenie 1.26

$F, H \in K[X, Y, Z]$ homogenous such that

$$V = \{x \in \mathbb{P}^2 \ : \ F(x) = 0, H(x) = 0\}$$

is finite. Then

$$\sum_{x \in V} I(x, F \cap H) = \deg(F)\deg(H)$$

The group of divisors on V $\mathrm{Div}(V)$ is the free Abelian group with basis V, $\mathbb{Z}[V]$.

Definicja 1.27: intersection divisor

Let $F \in K[X, Y, Z]$ be homogenous with finite $\{x \ : \ F(x) = 0\}$. The **intersection divisor** of F is

$$V \cdot F = \sum_{x \in V} I(x, V \cap F) \cdot x \in Div(V).$$

For $D = n_1 x_1 + ... + n_k x_k \in \mathrm{Div}(V)$ we define $\deg(D) = n_1 + ... + n_k$.

Elliptic curves

Definicja 1.28

An **elliptic curve** is a pair (C, O) such that C is a projective plane curve of degree 3 and $O \in C$

We aim to show that there is a natural commutative group structure on C such that O becomes the neutral element.

Lemat 1.29

For any $x, y \in C$ there is a unique line L in $\mathbb{P}^2$ and unique $z \in C$ such that

$$C \cdot L = x + y + z \in Div(C)$$

$$\varphi : C \times C \to C$$

$\varphi(x, y) = z \iff$ there is a line L such that

$$C \cdot L = x + y + z.$$

For $x, y, z \in C$ we have $\varphi(x, y) = \varphi(y, x)$

$$\varphi(x, y) = z \iff \varphi(y, z) = x \iff \varphi(z, x) = y.$$

so this is almost a group action but lacks the neutral element.

Twierdzenie 1.30

$(C, \oplus, O)$ is a **commutative group**, where the multiplication is defined

$$x \oplus y = \varphi(O, \varphi(x, y)).$$

Definicja 1.31

$D, D' \in \mathrm{Div}(C)$

$$D = \sum_{P \in C} n_P P$$

$$D' = \sum_{P \in C} n'_P P$$

we write $D \leq D'$ if $\forall\ P \in C\ n_P \leq n'_P$.

Twierdzenie 1.32

$F, G \in K[X, Y, Z]$ homogenous such that each has finitely many zeros on C and

$$\forall x \in C \; I(x, C \cap F) \geq I(x, C \cap G)$$

Then there exists homogenous $H \in K[X, Y, Z]$

$$C \cdot F = C \cdot G + C \cdot H$$

Using assumptions from the theorem:

- $$C \cdot (FG) = C \cdot F + C \cdot G$$
- If $C \cdot F = x_1 + ... + x_s + y$ and $C \cdot G = x_1 + ... + x_s + z$, then $y = z$.

Twierdzenie 1.33

$$(C, \oplus, O_1) \cong (C, \oplus, O_2)$$

Definicja 1.34: inflection point

$x \in C$ is **inflection point** if

$$I(x, C \cap T_x C) > 2$$

For an elliptic curve C the following are equivalent

- x - inflection point
- $I(X, C \cap T_x C) = 3$
- $\varphi(x, x) = x$

$K \neq 3 \implies$ there are 9 inflection points on C