K je těleso, char K ≠ 2

$$y^2 = x^3 + Ax + B, \quad A, B \in K$$

$$E(K) = \{(x,y) \in K \times K,\ y^2 = x^3 + Ax + B\} \cup \{\infty\}$$

$$y^2 - x^3 - Ax - B \rightsquigarrow Y^2 Z - X^3 - AX^2 Z - BZ^3$$

$x = \alpha$

$$x - \alpha = 0 \rightsquigarrow X - \alpha Z = 0 \iff X = \alpha Z$$

$$Y^2 Z - \alpha^3 Z^3 - A\alpha^2 Z^3 - BZ^3 = 0$$

$$Z(Y^2 - \alpha^3 Z^2 - A\alpha^2 Z^2 - BZ^2) = 0$$

Př. Buď E eliptická křivka nad $\mathbb{Z}_{13}$ zadaná rovnicí

$$y^2 = x^3 - x = x(x-1)(x+1)$$

x	$x^3 - x$
0	0
1	0
2	6
3	-2
4	-5
5	3
6	2
-6	-2
-5	-3
⋮	

y	y^2
0	0
1	1
2	4
3	9
4	3
5	-1
6	-3

(0,0), (1,0), (-1,0), (5,4), (5,-4), (-5,-6), (-5,6)

$$E(\mathbb{Z}_{13}) = \{(-1,0), (0,0), (1,0), (5,4), (5,-4), (-5,6), (-5,-6)\} \cup \{\infty\}$$

$$|E(\mathbb{Z}_{13})| = 8$$

Pro bod $P = (x_0, 0)$, platí $P = -P$, tedy $2P = \infty$.

Grupa $E(\mathbb{Z}_{13})$ má právě 3 prvky řádu 2

$$\Rightarrow \quad E(\mathbb{Z}_{13}) \cong \mathbb{Z}_2 \times \mathbb{Z}_4$$

Dimenze

Def Buď $V \subseteq \mathbb{A}^2(K)$ afinní algebraická množina. Okruh

$$\overline{K}[V] := \overline{K}[x,y] / I(V)$$

se nazývá souřadnicový okruh afinní alg. množiny V.

$$I(V) = \{ f \in \overline{K}[x,y] \,;\, f(P) = 0 \text{ pro každé } P \in V \}.$$

Je-li V afinní varieta, pak $\overline{K}[V]$ je obor integrity. Jeho podílové těleso $\overline{K}(V)$ se nazývá těleso funkcí variety V.

Definice Buď R komutativní okruh. Výškou prvoideálu $\mathcal{P} \subseteq R$ rozumíme supremum všech nezáporných celých čísel n, pro která existuje rostoucí řetězec (po dvou různých) prvoideálů

$$\mathcal{P}_0 \subset \mathcal{P}_1 \subset \ldots \subset \mathcal{P}_n = \mathcal{P}.$$

Dimenzí (nebo též Krullovu dimenzí) okruhu R definujeme jako supremum výšek všech prvoideálů okruhu R.

Př. V oboru integrity je nulový ideál prvoideál výšky 0. Libovolné těleso má dimenzi 0. Okruh $\mathbb{Z}$ celých čísel má dimenzi 1, neboť každý nenulový prvoideál je maximální.

p prvočíslo

$$\{0\} \subset (p)$$

(p) má výšku

Př. Buď $\alpha \in \mathbb{C}$ celé algebraické číslo a označme $f_\alpha \in \mathbb{Z}[x]$ minimální polynom α nad $\mathbb{Q}$. Pro libovolný nenulový prvoideál $P \subset \mathbb{Z}[\alpha]$ je $P \cap \mathbb{Z}$ je nenulový prvoideál okruhu $\mathbb{Z}$. Označme p ono jediné prvočíslo, které leží v P. Pak

$\mathbb{Z}[\alpha]/(p)$ je konečný okruh, neboť platí

$$\mathbb{Z}[\alpha]/(p) \cong \mathbb{Z}[x]/(f_\alpha, p) \cong \mathbb{Z}_p[x]/(\overline{f_\alpha}),$$

$$\mathbb{Z}[\alpha] \cong \mathbb{Z}[x]/(f_\alpha)$$

kde $\overline{f_\alpha}$ je obraz f_α v homomorfismu $\mathbb{Z}[x] \longrightarrow \mathbb{Z}/p\mathbb{Z}[x]$.

Inkluze $(p) \subseteq P$ nám dává surjektivní homomorfismus okruhů

$$\mathbb{Z}[\alpha]/(p) \longrightarrow \mathbb{Z}[\alpha]/P$$

tedy $\mathbb{Z}[\alpha]/P$ je také konečný okruh. Prvoideál P je maximální, neboť $\mathbb{Z}[\alpha]/P$ je jakožto konečný obor integrity tělesem.

Závěr: Každý nenulový prvoideál okruhu $\mathbb{Z}[\alpha]$ má výšku 1, tedy dimenze $\mathbb{Z}[\alpha]$ je 1.

Př. Zřejmě $\dim \mathbb{Z}[x] \geq 2$, neboť $(x,2)$ je prvoideál, jehož výška je alespoň:

$$\{0\} \subset (x) \subset (x,2)$$

Př. Pro libovolné těleso K má okruh $K[x]$ dimenzi 1, neboť libovolný nenulový prvoideál je maximální.

Tvrzení Buď R noetherovský okruh. Pak platí

$$\dim R[x] = \dim R + 1.$$

Důsledek Buď K těleso. Pak

$$\dim K[x_1, x_2, \dots, x_n] = n.$$

Př. Buďte R a S komutativní okruhy. Předpokládejme, že existuje surjektivní homomorfismus $f: R \to S$. Pak

$$\dim S \leq \dim R.$$

$$\begin{tikzcd} R \arrow[r, two heads, "f"] \arrow[d, two heads] & S \arrow[d, two heads] \\ R/f^{-1}(P) \arrow[r, hook, two heads] & S/P \end{tikzcd}$$

$P \subseteq S$ prvoideál

$f^{-1}(P)$ je prvoideál v R

P má výšku n $\Rightarrow$ výška prvoideálu $f^{-1}(P)$ je alespoň n

Definice Buď V libovolná afinní algebraická množina. Pak dimenzí V rozumíme dimenzi okruhu $\overline{K}[V]$.

Pokud $V \subseteq \mathbb{A}^2(K)$, pak $\dim V \leq 2$, neboť

$$\dim \overline{K}[V] \leq \dim \overline{K}[x,y] = 2$$

Definice Afinní varieta dimenze 1 se nazývá křivka.

Pozn. Pro varietu V lze dimenzi definovat také jako stupeň transcendence $[\overline{K}(V) : \overline{K}]$.

Lokalizace

Buď $V \subseteq \mathbb{A}^2(K)$ afinní varieta. Pro libovolný bod $P \in V$ definujme ideál

$$M_P = \{ f \in \overline{K}[V] ; \; f(P) = 0 \}$$ okruhu $\overline{K}[V]$.

Ideál M_P je maximální ideál okruhu $\overline{K}[V]$, neboť zobrazení $\overline{K}[V]/M_P \to \overline{K}$ dané předpisem $f \longmapsto f(P)$ je izomorfismus.

Je-li $P = (x_0, y_0) \in V$, není těžké ukázat, že

$$M_P = (x - x_0, y - y_0).$$

Definice Lokálním okruhem variety V v P rozumíme lokalizaci $\overline{K}[V]$ v prvoideálu M_P a značíme jej $\overline{K}[V]_P$.

$$\overline{K}[V]_P = \left\{ F \in \overline{K}(V) ; \; F = \frac{f}{g} \text{ pro nějaké } f, g \in \overline{K}[V], \; g(P) \neq 0 \right\}.$$

Definice Okruh hlavních ideálů, který má jediný nenulový prvoideál se nazývá okruh diskrétní valuace.

Buď R okruh diskrétní valuace, $M \subseteq R$ je jediný nenulový prvoideál. Zřejmě M je maximální ideál okruhu R. Jednotkami okruhu R jsou právě ty prvky, které nepatří M, tj. $R^{\times} = R \setminus M$. V okruhu hlavních ideálů je každý nenulový prvoideál generovaný ireducibilním prvkem. Okruh R má až na pronásobení jednotkou jediný ireducibilní prvek. Tento prvek se nazývá uniformizér. Buď $\pi \in R$ uniformizér, pak libovolný nenulový prvek $x \in R$ lze zapsat jednoznačně ve tvaru

$$x = u \cdot \pi^n, \text{ kde } u \in R^{\times}, n \in \mathbb{N} \cup \{0\}.$$