$$\mathfrak{a}: E \longrightarrow Pic(E)$$
$$P \longmapsto \text{třída obsahující divizor } [P]-[\infty]$$

Tvrzení Buďte $P, Q \in E(\bar{K})$ a předpokládejme, že existuje funkce $f \in \bar{K}(E)$ taková, že
$$div(f) = [P]-[Q].$$
Pak $P = Q$.

$$D_1 = \sum_{P \in E(\bar{K})} a_P [P] \qquad D_2 = \sum_{P \in E(\bar{K})} b_P [P]$$

$$D_1 \geq D_2 \iff a_P \geq b_P \text{ pro každé } P$$

$$\mathcal{L}(D) = \{ f \in \bar{K}(E)^*, \ div(f) \geq -D \} \cup \{0\}$$

$$D = \sum a_P [P]$$

$$f \in \mathcal{L}(D) \iff ord_P(f) \geq -a_P \text{ pro každé } P$$

$f, g \in \mathcal{L}(D)$, $f \neq 0, g \neq 0$ $\qquad ord_P(f+g) \geq \min\{ \underbrace{ord_P(f)}_{\geq -a_P}, \underbrace{ord_P(g)}_{\geq -a_P} \} \geq -a_P$

$\mathcal{L}(D)$ je vektorový prostor nad $\bar{K}$, který má konečnou dimenzi $\ell(D)$.

$\mathcal{L}([Q])$ Pro libovolný bod $P \in E(\bar{K})$ je $\ell([P])$ rovna 1, tj. $\mathcal{L}([P]) \cong \bar{K}$

$$\mathcal{L}([P]) \longrightarrow \bar{K}$$
$$f \longmapsto (f \cdot \pi)(P)$$

$\pi \in \bar{K}(E)^*$ je uniformizér v bodě P, tj. $ord_P(\pi) = 1$.

Zobrazení $\mathcal{L}([P]) \to \bar{K}$

$f \mapsto (f \cdot \pi)(P)$

je lineární a jeho jádro je $\mathcal{L}(0)$

$\{f \in \mathcal{L}([P]);\ ord_P(f) \geq 0\} = \mathcal{L}(0)$

$\mathcal{L}(0) = \bar{K}$, neboť libovolná nekonstantní funkce má pól.

$$\mathcal{L}([P]) / \mathcal{L}(0) \longrightarrow \bar{K}$$

$$\ell([D]) - \ell(0) \leq \dim \bar{K} = 1$$

$$\Rightarrow \ell([P]) \leq \ell(0) + 1 = 2$$

Dk. Buď $f \in \bar{K}(\bar{E})^*$ takové, že

$$div(f) = [P] - [Q].$$

Pak $f \in \mathcal{L}([Q])$. Protože $\ell([Q]) = 1$, musí být f konstantní funkce, a proto

$$div(f) = 0, \text{ tedy } P = Q.$$

Eliptické křivky nad $\mathbb{Q}$

Věta (Mordell - Weil)
Buď E eliptická křivka definovaná nad $\mathbb{Q}$. Pak $E(\mathbb{Q})$ je konečně generovaná abelovská grupa.

Buď A konečně generovaná abelovská grupa. Pak existuje $r \in \mathbb{N} \cup \{0\}$ tak, že

$$A \cong A_{tors} \oplus \mathbb{Z}^r,$$

kde A_{tors} je podgrupa prvků konečného řádu.

Věta (Lutz - Nagell)
Buď E eliptická křivka daná rovnicí $y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$. Nechť $P = (x, y) \in E(\mathbb{Q})$ je bod konečného řádu. Pak $x, y \in \mathbb{Z}$. Pokud $y \neq 0$, pak

$$y^2 \mid 4A^3 + 27B^2.$$

Bod $P = (x, y)$ je řádu 2 $\Leftrightarrow$ $(x, y) = (x, -y)$ $\Leftrightarrow$ $y = 0$.
Pak x je kořenem polynomu $x^3 + Ax + B$ a platí,
$x \in \mathbb{Q} \Leftrightarrow x \in \mathbb{Z}$.

---

p prvočíslo

$$v_p : \mathbb{Q} \longrightarrow \mathbb{Z} \cup \{\infty\}$$

$a \in \mathbb{Z}, a \neq 0$ $\quad a = p^n \cdot b,\ p \nmid b,\ n \in \mathbb{N} \cup \{0\},\ b \in \mathbb{Z}$

$$v_p(a) = n$$

$\alpha \in \mathbb{Q}, \alpha \neq 0$ $\quad \alpha = \frac{a}{b},\ a, b \in \mathbb{Z}$

$$v_p(\alpha) = v_p(a) - v_p(b)$$

$$v_p(0) = \infty$$

$$v_p(\alpha\cdot\beta) = v_p(\alpha) + v_p(\beta)$$

$$v_p(\alpha+\beta) \geq \min\{v_p(\alpha), v_p(\beta)\}$$

Pokud $v_p(\alpha) < v_p(\beta)$, pak $v_p(\alpha+\beta) = v_p(\alpha)$.

Lemma
Buď $(x,y) \in E(\mathbb{Q})$ libovolný bod. Platí $v_p(x) < 0$ právě tehdy když $v_p(y) < 0$. Pokud $v_p(x) < 0$, pak existuje $r \in \mathbb{N}$ takové, že $v_p(x) = -2r$ a $v_p(y) = -3r$.

Dk. Platí

$$y^2 = x^3 + Ax + B,$$

pak

$$2v_p(y) = v_p(y^2) = v_p(x^3+Ax+B) \geq \min\{3v_p(x), \underbrace{v_p(A)}_{\geq 0} + v_p(x), \underbrace{v_p(B)}_{\geq 0}\}$$

$$v_p(x) < 0 \Rightarrow 3v_p(x) < v_p(x)$$

$$\Rightarrow v_p(x^3+Ax+B) = 3v_p(x) < 0$$

$$\Rightarrow v_p(y) < 0, \text{ přičemž}$$

$$2v_p(y) = 3v_p(x)$$

$$v_p(x) \geq 0 \Rightarrow v_p(x^3+Ax+B) \geq 0 \Rightarrow v_p(y) \geq 0$$

Pro libovolné $n \in \mathbb{N}$ definujme

$$E_n = \{(x,y) \in E(\mathbb{Q});\ v_p\left(\frac{x}{y}\right) \geq n,\ v_p(x) < 0\} \cup \{\infty\}$$

$m, n \in \mathbb{N}$, $m \leq n \Rightarrow E_n \subseteq E_m$.

$$\ldots \subseteq E_n \subseteq \ldots \subseteq E_3 \subseteq E_2 \subseteq E_1$$

$v_p(x) < 0 \quad \Rightarrow \quad v_p(x) = -2r,\ v_p(y) = -3r \quad$ pro $r \in \mathbb{N}$

$\Rightarrow v_p\left(\frac{x}{y}\right) = r$

$$\left\{(x,y) \in E(\mathbb{Q});\ v_p\left(\tfrac{x}{y}\right) \geq n\right\} \supseteq \left\{(x,y) \in E(\mathbb{Q});\ v_p(x) \leq -2n,\ v_p(y) \leq -3n\right\}$$

$y^2 = x^3 + 1, \quad p = 2 \qquad x = 2 \qquad v_2\left(\frac{x}{y}\right) = 1$

$y = 3$