Některé nezbytnosti z algebraické geometrie

Nechť K je těleso.

Definice. n-rozměrným afinním prostorem nad K rozumíme kartézskou mocninu K^n. Budeme jej značit $A^n(K)$, tj.

$$A^n(K) = \{(x_1, \ldots, x_n);\ x_1, \ldots, x_n \in K\}.$$

Definice. n-rozměrným projektivním prostorem nad K rozumíme rozklad na množině $K^{n+1} - \{(0, \ldots, 0)\}$ příslušný ekvivalenci $\sim$, kterou definujeme takto: pro libovolné $(n+1)$-tice $(x_1, \ldots, x_{n+1})$, $(y_1, \ldots, y_{n+1}) \in K^{n+1}$ položíme $(x_1, \ldots, x_{n+1}) \sim (y_1, \ldots, y_{n+1})$ právě tehdy, když existuje $\lambda \in K^\times$, které pro každé $i \in \{1, \ldots, n+1\}$ splňuje podmínku $x_i = \lambda y_i$. Tento n-rozměrný projektivní prostor nad K budeme značit $P^n(K)$, třídu rozkladu (tj. bod projektivního prostoru) obsahující $(n+1)$-tici $(x_1, \ldots, x_{n+1})$ budeme značit $[x_1, \ldots, x_{n+1}]$.

Afinní část projektivního prostoru

Nechť $x_1, \ldots, x_{n+1}$ jsou z tělesa K, přičemž alespoň jedno z nich je různé od nuly.

Jestliže $x_{n+1} \neq 0$, pak platí $[x_1, \ldots, x_{n+1}] = [\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}, 1]$, čímž je pevně dán bod $(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}) \in A^n(K)$.

Jestliže naopak $x_{n+1} = 0$, určuje $[x_1, \ldots, x_{n+1}]$ jednoznačně bod $[x_1, \ldots, x_n] \in P^{n-1}(K)$.

Lze tedy n-rozměrný projektivní prostor „rozdělit“ na n-rozměrný afinní prostor, který považujeme za množinu „vlastních bodů“ a na množinu „nevlastních bodů“, která tvoří $(n-1)$-rozměrný projektivní prostor.

Můžeme si představovat, že nevlastní body „leží v nekonečnu.“ Toto rozdělení však *není* kanonické – lze to provést mnoha způsoby. Tedy to, zda je bod vlastní nebo ne, je věc naší volby.

Nadplochy projektivního prostoru

Máme-li homogenní polynom $F(t_1, \ldots, t_{n+1}) \in K[t_1, \ldots, t_{n+1}]$ o $n+1$ proměnných nad K stupně k a bod $[x_1, \ldots, x_{n+1}] \in P^n(K)$, má smysl se ptát, zda $F(x_1, \ldots, x_{n+1}) = 0$. Je-li totiž $[x_1, \ldots, x_{n+1}] = [y_1, \ldots, y_{n+1}]$, pak existuje $\lambda \in K^\times$, které pro každé $i \in \{1, \ldots, n+1\}$ splňuje podmínku $x_i = \lambda y_i$. Pak ovšem $F(x_1, \ldots, x_{n+1}) = F(\lambda y_1, \ldots, \lambda y_{n+1}) = \lambda^k \cdot F(y_1, \ldots, y_{n+1})$, a tedy $F(x_1, \ldots, x_{n+1}) = 0$, právě když $F(y_1, \ldots, y_{n+1}) = 0$.

Definice. Nechť $F(t_1, \ldots, t_{n+1}) \in K[t_1, \ldots, t_{n+1}]$ je homogenní polynom stupně k. Množina

$$\mathcal{C} = \{[x_1, \ldots, x_{n+1}] \in P^n(K);\ F(x_1, \ldots, x_{n+1}) = 0\}$$

se nazývá nadplocha stupně k v $P^n(K)$. Je-li $n = 2$, hovoříme také o křivce stupně k v projektivní rovině $P^2(K)$.

Singulární bod nadplochy projektivního prostoru

Parciální derivací homogenního mnohočlenu je opět homogenní mnohočlen. Má proto smysl následující definice.

Definice. Nechť $F(t_1, \ldots, t_{n+1}) \in K[t_1, \ldots, t_{n+1}]$ je homogenní polynom stupně k a

$$\mathcal{C} = \{[x_1, \ldots, x_{n+1}] \in P^n(K);\ F(x_1, \ldots, x_{n+1}) = 0\}$$

příslušná nadplocha. Bod $[x_1, \ldots, x_{n+1}] \in \mathcal{C}$ se nazývá singulární, jestliže pro každé $i \in \{1, \ldots, n+1\}$ platí

$$\frac{\partial F}{\partial x_i}(x_1, \ldots, x_{n+1}) = 0.$$

Nadplocha $\mathcal{C}$ se nazývá singulární, existuje-li alespoň jeden její singulární bod.

Příklad

Uvažme reálnou projektivní rovinu $P^2(\mathbb{R})$.
Abychom se vyhnuli indexům, budeme psát x, y, z místo t_1, t_2, t_3.

Kubický mnohočlen $F_1(x, y, z) = x^3 + x^2z - y^2z$ nám definuje kubickou křivku $\mathcal{C}_1$ (tj. křivku stupně 3)

$$\mathcal{C}_1 = \{[x, y, z] \in P^2(\mathbb{R});\ F_1(x, y, z) = 0\}.$$

Jistě $[0, 0, 1] \in \mathcal{C}_1$. Tento bod je singulární, neboť

$$\frac{\partial F_1}{\partial x} = 3x^2 + 2xz, \quad \frac{\partial F_1}{\partial y} = -2yz, \quad \frac{\partial F_1}{\partial z} = x^2 - y^2.$$

Je tedy $\mathcal{C}_1$ singulární křivka.

Další příklad

Opět pracujme s reálnou projektivní rovinu $P^2(\mathbb{R})$.

Uvažme nyní mnohočlen $F_2(x, y, z) = x^3 + xz^2 - y^2z$ a příslušnou kubickou křivku

$$\mathcal{C}_2 = \{[x, y, z] \in P^2(\mathbb{R});\ F_2(x, y, z) = 0\}.$$

Hledejme singulární body na $\mathcal{C}_2$. Platí

$$\frac{\partial F_2}{\partial x} = 3x^2 + z^2, \quad \frac{\partial F_2}{\partial y} = -2yz, \quad \frac{\partial F_2}{\partial z} = 2xz - y^2.$$

Z $\frac{\partial F_2}{\partial x} = 0$ plyne $x = 0$ a $z = 0$, pak ale z $\frac{\partial F_2}{\partial z} = 0$ plyne i $y = 0$.

Ale trojice nul nedává žádný bod projektivní roviny. Singulární bod na $\mathcal{C}_2$ tedy neexistuje a proto $\mathcal{C}_2$ není singulární křivka.

Eliptické křivky

Definice. Eliptická křivka nad tělesem K je uspořádaná dvojice $(\mathcal{E}, O)$, kde $\mathcal{E}$ je nesingulární kubická křivka v $P^2(K)$ a $O \in \mathcal{E}$.

Poznámka. Je možné zavést pojem biracionální ekvivalence dvou křivek, spočívající v tom, že existují transformace prostoru převádějící jednu křivku na druhou a obráceně, přičemž tyto transformace jsou „pěkné“ v tom smyslu, že transformační rovnice jsou dány homogenními polynomy téhož stupně nad K.

Věta. *Libovolná eliptická křivka nad K je biracionálně ekvivalentní s nějakou eliptickou křivkou $(\mathcal{E}, O)$ následujícího tvaru (přičemž transformace převádějí vyznačený bod jedné křivky na vyznačený bod druhé křivky)*

$$\mathcal{E} = \{[x, y, z] \in P^2(K);\ F(x, y, z) = 0\},$$

kde

$$F(x, y, z) = y^2z + a_1xyz + a_2yz^2 - x^3 - a_3x^2z - a_4xz^2 - a_5z^3,$$

$a_1, \ldots, a_5 \in K$ *a* $O = [0, 1, 0]$.

Eliptické křivky dané Weierstrassovou rovnicí

V projektivní rovině zvolme za afinní část množinu těch bodů, které mají nenulovou třetí souřadnici, tedy bodů $[x, y, 1]$.

Každá eliptická křivka ve tvaru z předchozí věty má jeden nevlastní bod (totiž $O = [0, 1, 0]$) a v afinní části je dána rovnicí

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5.$$

Tato rovnice se nazývá **Weierstrassova rovnice**.

V dalším textu budeme předpokládat, že charakteristika tělesa K není ani 2 ani 3, tj. že 2 i 3 jsou invertibilní prvky v K.

Důvodem je to, že pro naše účely eliptické křivky nad tělesy charakteristiky 2 a 3 nejsou zapotřebí a že tento předpoklad dále zjednodušuje Weierstrassovu rovnici.

Můžeme pak totiž předpokládat, že $a_1 = a_2 = a_3 = 0$, a tedy Weierstrassova rovnice je tvaru $y^2 = x^3 + a_4x + a_5$.

Kdy Weierstrassova rovnice zadává eliptickou křivku?

Věta. *Nechť K je těleso charakteristiky různé od 2 a 3, $a, b \in K$. Rovnice $y^2 = x^3 + ax + b$ je Weierstrassovou rovnicí nějaké eliptické křivky, právě když platí $4a^3 + 27b^2 \neq 0$.*

Důkaz. Položme $F(x, y, z) = y^2z - x^3 - axz^2 - bz^3$. Platí

$$\frac{\partial F}{\partial x} = -3x^2 - az^2, \quad \frac{\partial F}{\partial y} = 2yz, \quad \frac{\partial F}{\partial z} = y^2 - 2axz - 3bz^2.$$

Předpokládejme, že $[x, y, z]$ je singulární bod. Pak $z = 0$ implikuje $x = y = 0$, spor. Je tedy $z \neq 0$. Proto $y = 0$ a pro $\gamma = \frac{x}{z}$ platí $3\gamma^2 = -a$, $2a\gamma = -3b$. Jestliže $a = 0$, pak také $b = 0$. Naopak pro $a = b = 0$ je bod $[0, 0, 1]$ singulární. Zabývejme se dále případem $a \neq 0$. Platí $\gamma = -\frac{3b}{2a}$, $\gamma^2 = -\frac{a}{3} = \frac{9b^2}{4a^2}$, tj. $4a^3 + 27b^2 = 0$. Naopak, je-li $4a^3 + 27b^2 = 0$, $a \neq 0$, ověřme, že pro $\gamma = -\frac{3b}{2a}$ je $[\gamma, 0, 1]$ singulární bod, což je snadné, například $\gamma^2 = \frac{9b^2}{4a^2} = -\frac{a}{3}$, dále

$$\gamma^3 + a\gamma + b = \left(-\tfrac{3b}{2a}\right)\left(-\tfrac{a}{3}\right) + a\left(-\tfrac{3b}{2a}\right) + b = \tfrac{b}{2} - \tfrac{3b}{2} + b = 0.$$

Eliptická křivka daná Weierstrassovou rovnicí

Nechť K je těleso charakteristiky různé od 2 a 3, $a, b \in K$, $4a^3 + 27b^2 \neq 0$. Pak Weierstrassova rovnice

$$y^2z = x^3 + axz^2 + bz^3$$

spolu s význačným bodem $O = [0, 1, 0]$ zadává v projektivní rovině $P^2(K)$ eliptickou křivku $\mathcal{E}$.

Tento význačný bod O je jediným bodem na nevlastní přímce $z = 0$. Platí dokonce, že nevlastní přímka $z = 0$ má s eliptickou křivkou $\mathcal{E}$ trojnásobný bod dotyku O, neboť dosazením $z = 0$ do rovnice křivky dostaneme $x^3 = 0$.

Ostatní body eliptické křivky jsou vlastní a jsou v afinní rovině $A^2(K) = K^2$ určeny rovnicí $y^2 = x^3 + ax + b$.

Je-li $A = [\alpha, \beta, 1] \in \mathcal{E}$, pak i $B = [\alpha, -\beta, 1] \in \mathcal{E}$. Přímka AB má v $P^2(K)$ rovnici $x = \alpha z$ a obsahuje ještě třetí bod na $\mathcal{E}$, totiž O.

Eliptická křivka $\mathcal{E}: \; y^2z = x^3 + axz^2 + bz^3$, $O = [0,1,0]$

Jsou-li $A = [\alpha, \beta, 1] \in \mathcal{E}$, $B = [\gamma, \delta, 1] \in \mathcal{E}$, přičemž $\alpha \neq \delta$, přímka AB má v $P^2(K)$ rovnici $y = \beta z + (x - \alpha z)k$, kde $k = \frac{\delta - \beta}{\gamma - \alpha}$.
Hledejme průsečíky přímky AB s eliptickou křivkou $\mathcal{E}$.

Dosazením této rovnice za y do rovnice $y^2z = x^3 + axz^2 + bz^3$ a vydělením z^3 dostaneme kubickou rovnici pro $\frac{x}{z}$ s koeficienty z K:

$$\left(\tfrac{x}{z}\right)^3 + a\tfrac{x}{z} + b - \left(\beta + (\tfrac{x}{z} - \alpha)k\right)^2 = 0.$$

Jde o normovaný kubický polynom v $\frac{x}{z}$, jehož dva kořeny α a γ už známe. Proto má ještě třetí kořen $\sigma \in K$ a z Viétových vztahů zjistíme, že platí $\alpha + \gamma + \sigma = k^2$.

Přímka AB a eliptická křivka $\mathcal{E}$ mají tedy ještě třetí průsečík $C = [\sigma, \tau, 1]$, kde $\sigma = k^2 - \alpha - \gamma$, $\tau = \beta + k(\sigma - \alpha)$.

Někdy může bod C splynout s některým z bodů A, B, v tom případě mluvíme o dvojnásobném průsečíku.

Eliptická křivka $\mathcal{E}: \; y^2z = x^3 + axz^2 + bz^3, \; O = [0,1,0]$

Podobně se odvodí, že pokud sestrojíme křivce $\mathcal{E}$ v jejím bodě A tečnu, protne tato tečna křivku $\mathcal{E}$ ještě v jednom bodě. Máme tedy operaci: pro libovolnou dvojici bodů $A, B \in \mathcal{E}$ je jejím výsledkem třetí průsečík, který nazveme $A \star B$. Tato operace však není „pěkná“: nemá neutrální prvek, není asociativní.

Proto operaci ještě trochu pozměníme pomocí pevně zvoleného bodu O. Definujeme součet bodů $A, B \in \mathcal{E}$ předpisem

$$A + B = (A \star B) \star O.$$

Tato operace sčítání bodů je zřejmě komutativní, $(\mathcal{E}, +)$ má neutrální prvek O a libovolný bod $A = [\alpha, \beta, 1] \in \mathcal{E}$ má opačná bod $-A = [\alpha, -\beta, 1] \in \mathcal{E}$. Je možné dokázat, že operace sčítání bodů je také asociativní, je tedy $(\mathcal{E}, +)$ komutativní grupa. Důkaz asociativity je mimo možnosti této přednášky.

Explicitní popis operace sčítání bodů

Věta. *Nechť K je těleso charakteristiky různé od 2 a 3, $a, b \in K$, $4a^3 + 27b^2 \neq 0$. Nechť $\mathcal{E}$ je eliptická křivka daná Weierstrassovou rovnicí $y^2z = x^3 + axz^2 + bz^3$ s význačným bodem $O = [0, 1, 0]$. Operaci $+$ na $\mathcal{E}$ je možné popsat takto:*

1. *Pro libovolné $A \in \mathcal{E}$ klademe $A + O = O + A = A$.*
2. *Pro libovolné $A = [\alpha, \beta, 1] \in \mathcal{E}$ je také $B = [\alpha, -\beta, 1] \in \mathcal{E}$ a klademe $A + B = O$. (Tento bod B pak označujeme $-A$.)*
3. *Pro libovolné $A = [\alpha, \beta, 1] \in \mathcal{E}$, $B = [\gamma, \delta, 1] \in \mathcal{E}$ takové, že $B \neq -A$, položme*

$$k = \begin{cases} \frac{\beta-\delta}{\alpha-\gamma} & \text{je-li } A \neq B, \\ \frac{3\alpha^2+a}{2\beta} & \text{je-li } A = B, \end{cases}$$
$$\sigma = k^2 - \alpha - \gamma,$$
$$\tau = -\beta + k(\alpha - \sigma),$$

pak platí $[\sigma, \tau, 1] \in \mathcal{E}$ a klademe $A + B = [\sigma, \tau, 1] \in \mathcal{E}$.

Věty o eliptických křivkách nad konečnými tělesy

Projektivní rovina nad konečným tělesem má konečně mnoho bodů, proto eliptická křivka nad konečným tělesem je konečná grupa.

Věta. (Hasse)

1. *Nechť p je prvočíslo a $(\mathcal{E}, O)$ je eliptická křivka nad $\mathbb{F}_p$. Pak $|\mathcal{E}| = p + 1 - a_p$, kde celé číslo a_p splňuje $|a_p| < 2\sqrt{p}$.*
2. *Označme $\alpha_p \in \mathbb{C}$ kořen rovnice $x^2 - a_p x + p = 0$. Pro libovolné $n \in \mathbb{N}$ nechť $(\mathcal{E}_n, O)$ je eliptická křivka nad $\mathbb{F}_{p^n}$ určená stejnou Weierstrassovou rovnicí jako $(\mathcal{E}, O)$ (to má smysl, neboť $\mathbb{F}_p \subseteq \mathbb{F}_{p^n}$). Pak platí $|\mathcal{E}_n| = p^n + 1 - 2\Re(\alpha_p^n)$, kde $\Re$ značí reálnou část komplexního čísla.*