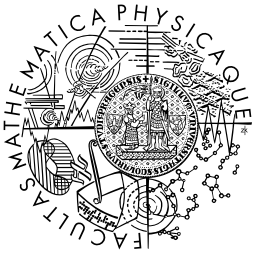


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Timea Jakubócyová

Cayleyovo kritérium pro řád bodu na eliptické křivce

Katedra algebry

Vedoucí bakalářské práce: doc. RNDr. Jan Šťovíček, Ph.D.

Studijní program: Obecná matematika

Studijní obor: MOMP

Praha 2024

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Chcela by som poďakovať svojmu vedúcemu práce doc. RNDr. Janovi Šťovíčkovi, Ph.D. za ochotu, trpezlivosť a čas strávený nad mojou bakalárskou prácou. A ďalej by som chcela poďakovať svojim rodičom a priateľovi za nekonečnú podporu a objatia.

Název práce: Cayleyovo kritérium pro řád bodu na eliptické křivce

Autor: Timea Jakubócyová

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. RNDr. Jan Šťovíček, Ph.D., Katedra algebry

Abstrakt: Hlavným cieľom tejto práce je dôkaz Cayleovho kritéria, ktoré popisuje nutnú a postačujúcu podmienku na to, aby rád bodu $(0, a_0)$ na danej eliptickej krivke delil dané prirodzené číslo n. V práci popisujeme potrebnú teóriu k diskrétnym valuačným okruhom, algebraickým množinám a polynomiálnym a racionálnym funkciám na ireducibilných algebraických množinách. Zaoberáme sa tiež vlastnosťami rovinných kriviek a eliptických kriviek, ktoré sú špeciálnym prípadom afinných rovinných kriviek. Na množine bodov projektívneho uzáveru eliptickej krivky definujeme grupovú štruktúru dvomi spôsobmi - geometricky a pomocou divizorov - a ukazujeme, že tieto dve grupové štruktúry si odpovedajú. Nakoniec sa venujeme samotnému dôkazu Cayleyovho kritéria.

Klíčová slova: algebraická množina, racionálna funkcia, eliptická krivka, grupa, Cayleyovo kritérium

Title: Cayley's criterion for the order of a point on an elliptic curve

Author: Timea Jakubócyová

Department: Department of Algebra

Supervisor: doc. RNDr. Jan Šťovíček, Ph.D., Department of Algebra

Abstract: The main goal of this work is to prove Cayley's criterion, which describes a necessary and sufficient condition for the order of the point $(0, a_0)$ on a given elliptic curve to divide a given natural number n. In the work, we explain the necessary theory for discrete valuation rings, algebraic sets, and polynomial and rational functions on irreducible algebraic sets. We also describe the properties of plane curves and elliptic curves, which are a special case of affine plane curves. We define a group structure on the set of points of the projective closure of an elliptic curve in two ways - geometrically and using divisors - and show that these two group structures correspond to each other. Finally, we focus on the proof of Cayley's criterion itself.

Keywords: algebraic set, rational function, elliptic curve, group, Cayley's criterion

Obsah

Úvod

V roku 1813 francúzsky matematik Jean-Victor Poncelet zistil, že pokiaľ si zoberieme dve kužeľosečky v projektívnej rovine a nájdeme n-uholník, ktorý je jednej z týchto dvoch kužeľosečiek vpísaný a druhej opísaný, potom takýchto n-uholníkov existuje nekonečne mnoho. V roku 1822 J.-V. Poncelet publikoval prácu *Traité sur les propriétés projectives des figures*, v ktorej dokázal toto tvrdenie dnes známe ako Ponceletovo porisma. Ponceletovo porisma zaujalo veľké množstvo matematikov, ktorí ho ďalej študovali, pracovali na nových alternatívnych dôkazoch a snažili sa ho zovšeobecniť. Jedným z týchto matematikov bol Arthur Cayley, ktorý v roku 1853 formuloval a dokázal kritérium, ktoré nám hovorí, kedy pre dané dve kužeľosečky existuje vôbec jeden n-uholník vpísaný jednej z týchto dvoch kužeľosečiek a opísaný druhej. Cayleyovo kritérium je možné preformulovať v jazyku eliptických kriviek a grupovej operácie na eliptických krivkách. Hlavným cieľom tejto práce je dôkaz práve tohto preformulovaného Cayleyovho kritéria.

Prvé tri kapitoly sa venujú spracovaniu teórie potrebnej k štúdiu eliptických kriviek a grupovej štruktúry na eliptických krivkách. V prvej kapitole sa zaoberáme pojmom diskrétneho valuačného okruhu, ktorý sa vyskytuje naprieč celou prácou. V druhej časti prvej kapitoly sa venujeme mocninovým radom a zavedeniu pojmu rozvoja prvku do mocninového radu, ktorý potrebujeme v dôkaze Cayleyovho kritéria. V tejto kapitole vychádzame najmä z práce Williama Fultona [1] a uvádzame tu dôkazy základných vlastností diskrétnych valuačných okruhov a mocninových radov, ktoré W. Fulton vo svojej práci formuluje, ale nedokazuje. V druhej kapitole sa zaoberáme afinnými a projektívnymi algebraickými množinami. Definujeme tu všetky potrebné pojmy ako napríklad pojem polynomiálnej či racionálnej funkcie na ireducibilnej algebraickej množine a rozoberáme vzťah medzi afinnými a projektívnymi algebraickými množinami. Tretia kapitola sa venuje afinným a projektívnym rovinným krivkám. Rozoberáme tu základné vlastnosti rovinných kriviek ako ireducibilita a singularita a ukazujeme, ako sa tieto vlastnosti prenášajú medzi afinnými a projektívnymi krivkami. Druhá časť tejto kapitoly sa venuje spracovaniu základnej teórie k divizorom. Divizory potrebujeme k definícii grupovej štruktúry na eliptických krivkách a k formulácii tvrdenia, ktoré nám hovorí, že za určitých predpokladov majú racionálne funkcie rovnaký počet núl a pólov až na násobnosť. V štvrtej kapitole sa už dostávame k eliptickým krivkám, ktoré sú špeciálnym prípadom afinných rovinných kriviek. V tejto kapitole formulujeme a dokazujeme potrebné vlastnosti eliptických kriviek. Následne dvoma rôznymi spôsobmi zavádzame grupovú štruktúru na množine bodov projektívneho uzáveru eliptickej krivky a dokazujeme, že tieto dve grupové štruktúry si odpovedajú. V poslednej, piatej, kapitole sa venujeme dôkazu samotného Cayleyovho kritéria. Vychádzame pritom z článku Olivera Nasha [2], v ktorom sú avšak uvedené len hlavné myšlienky tohto dôkazu bez potrebných detailov.

1 Rozvoj do mocninového radu

V tejto kapitole najskôr zavedieme pojem diskrétneho valuačného okruhu a uvedieme niekoľko jeho základných vlastností. Tieto vlastnosti následne použijeme k zadefinovaniu pojmu rozvoja prvku do mocninového radu. V celej kapitole vychádzame z práce Fultona [1, Kapitoly 2.4 a 2.5].

1.1 Diskrétny valuačný okruh

Definícia 1. *Nech R je okruh. Povieme, že R je* lokálny okruh*, pokiaľ spĺňa nasledujúce ekvivalentné podmienky:*

(1) Množina všetkých neinvertibilných prvkov v R tvorí ideál.

(2) Okruh R má práve jeden maximálny ideál, ktorý obsahuje všetky vlastné ideály v R.

Definícia 2. *Nech R je obor, ktorý nie je poľom. Povieme, že R je* diskrétny valuačný okruh*, píšeme DVR, pokiaľ spĺňa nasledujúce ekvivalentné podmienky:*

(1) Obor R je Noetherovský, lokálny a jeho maximálny ideál je hlavný.

(2) Existuje ireducibilný prvok $t \in R$ taký, že každý nenulový prvok $z \in R$ sa dá napísať jednoznačne v tvare $z = ut^n$, kde $u \in R$ je invertibilný prvok a $n \in \mathbb{N}_0$.

Prvok t z (2) sa nazýva uniformizačný parameter *pre R.*

Poznámka. Dôkaz ekvivalencie bodov (1) a (2) v definícii 2 môžeme nájsť v práci Fultona [1, Kapitola 2.5, Tvrdenie 4].

Poznámka. Nech R je diskrétny valuačný okruh, F je jeho podielové pole a t je jeho uniformizačný parameter. Potom každý nenulový prvok $z \in F$ sa dá jednoznačne zapísať v tvare $z = ut^n$, kde $u \in R$ je invertibilný prvok a $n \in \mathbb{Z}$. Exponent n sa nazýva *rád* prvku z a značí sa $\mathrm{ord}(z)$. Ďalej definujeme $\mathrm{ord}(0) = \infty$.

Aby sme mohli zaviesť pojem rozvoja prvku do mocninového radu, budeme potrebovať niekoľko nasledujúcich pomocných tvrdení. Tieto tvrdenia neskôr využijeme aj pri určovaní násobností núl a pólov racionálnych funkcií.

Tvrdenie 1. *Nech R je DVR a F je jeho podielové pole. Potom pre všetky $a, b \in F$ platí:*

(a) $\mathrm{ord}(ab) = \mathrm{ord}(a) + \mathrm{ord}(b)$.

(b) $\mathrm{ord}(a + b) \geq \min(\mathrm{ord}(a), \mathrm{ord}(b))$.

Dôkaz. Pokiaľ aspoň jeden prvok z a, b je nulový, tvrdenie zrejme platí. Predpokladajme teda, že $a, b \neq 0$. Nech $t \in R$ je uniformizačný parameter pre R a $a = ut^n, b = vt^m$, kde $u, v \in R$ sú invertibilné prvky a $n, m \in \mathbb{Z}$. Potom máme:

(a) $\mathrm{ord}(ab) = \mathrm{ord}(uvt^{n+m}) = n+m = \mathrm{ord}(ut^n)+\mathrm{ord}(vt^m) = \mathrm{ord}(a)+\mathrm{ord}(b)$, kde v druhej rovnosti využívame, že súčin invertibilných prvkov je invertibilný prvok.

(b) Bez ujmy na všeobecnosti nech $n \leq m$, teda $m - n \in \mathbb{N}_0$. Potom platí

$$a + b = ut^n + vt^m = t^n(u + vt^{m-n})$$

a výraz v zátvorke je prvkom R. Pokiaľ $u + vt^{m-n} = 0$, tak $a + b = 0$ a platí

$$\operatorname{ord}(a + b) = \infty \geq \min(n, m) = \min(\operatorname{ord}(a), \operatorname{ord}(b)).$$

Inak existuje invertibilný prvok $w \in R$ a $n' \in \mathbb{N}_0$ také, že $(u + vt^{m-n}) = wt^{n'}$. Takže

$$\begin{aligned}\operatorname{ord}(a + b) &= \operatorname{ord}(t^n(u + vt^{m-n})) = \operatorname{ord}(wt^{n+n'}) = \\ &= n + n' \geq n = \min(n, m) = \min(\operatorname{ord}(a), \operatorname{ord}(b)).\end{aligned}$$

□

Tvrdenie 2. *Nech R je DVR a F je jeho podielové pole. Potom platia nasledujúce tvrdenia:*

(a) Pre každé $a, b \in F$ také, že $\operatorname{ord}(a) < \operatorname{ord}(b)$, platí $\operatorname{ord}(a + b) = \operatorname{ord}(a)$.

(b) Nech $n \in \mathbb{N}$ a $a_0, a_1, \ldots, a_n \in F$. Pokiaľ exituje $i \in \{0, \ldots, n\}$ také, že $\operatorname{ord}(a_i) < \operatorname{ord}(a_j)$ pre všetky $i \neq j \in \{0, \ldots, n\}$, tak $a_0 + a_1 + \cdots + a_n \neq 0$.

Dôkaz. (a) (Dôkaz tohto bodu vychádza z Stichtenoth [3, Lema 1.1.11].) Z tvrdenia 1 máme, že pre všetky $a, b \in F$ platí $\operatorname{ord}(a + b) \geq \min(\operatorname{ord}(a), \operatorname{ord}(b))$ a $\operatorname{ord}(-a) = \operatorname{ord}(a)$. Pre spor predpokladajme, že existujú $a, b \in F$ také, že $\operatorname{ord}(a) < \operatorname{ord}(b)$ a $\operatorname{ord}(a + b) > \operatorname{ord}(a)$. Potom platí

$$\begin{aligned}\operatorname{ord}(a) &= \operatorname{ord}((a + b) - b) \geq \min(\operatorname{ord}(a + b), \operatorname{ord}(-b)) = \\ &= \min(\operatorname{ord}(a + b), \operatorname{ord}(b)) > \operatorname{ord}(a),\end{aligned}$$

čo je spor.

(b) Nech $a_0, a_1, \ldots, a_n \in F$ a existuje $i \in \{0, 1, \ldots, n\}$ spĺňajúce $\operatorname{ord}(a_i) < \operatorname{ord}(a_j)$ pre všetky $j \neq i$. Bez ujmy na všeobecnosti môžeme predpokladať, že $i = 0$. Potom platí

$$\begin{aligned}\operatorname{ord}(a_1 + a_2 + \cdots + a_n) &= \operatorname{ord}(a_1 + (a_2 + \cdots + a_n)) \\ &\geq \min(\operatorname{ord}(a_1), \operatorname{ord}(a_2 + \cdots + a_n)) \\ &\geq \min(\operatorname{ord}(a_1), \min(\operatorname{ord}(a_2), \operatorname{ord}(a_3 + \cdots + a_n))) \\ &= \min(\operatorname{ord}(a_1), \operatorname{ord}(a_2), \operatorname{ord}(a_3 + \cdots + a_n)) \\ &\geq \cdots \geq \min(\operatorname{ord}(a_1), \ldots, \operatorname{ord}(a_n)) > \operatorname{ord}(a_0).\end{aligned}$$

Potom $\operatorname{ord}(a_0)$ nemôže byť rovné ∞, teda platí $a_0 \neq 0$. Z (a) máme, že $\operatorname{ord}(a_0 + a_1 + \cdots + a_n) = \operatorname{ord}(a_0)$. Teda ani $\operatorname{ord}(a_0 + a_1 + \cdots + a_n) \neq \infty$, a preto $a_0 + a_1 + \cdots + a_n \neq 0$.

□

Tvrdenie 3. *Nech R je DVR s maximálnym ideálom $M \leqslant R$ a $K \subseteq R$ je pole. Uvažujme zobrazenie inklúzie $\varphi : K \hookrightarrow R$ a kanonickú projekciu $\pi : R \twoheadrightarrow R/M$. Predpokladajme, že zobrazenie $\pi \circ \varphi : K \to R/M$ je izomorfizmus. Potom platí:*

(a) *Pre každé $z \in R$ existuje práve jedno $\lambda \in K$ také, že $z - \lambda \in M$.*

(b) *Nech $t \in R$ je uniformizačný parameter pre R a $z \in R$. Potom pre každé $n \geq 0$ existujú jednoznačne určené $\lambda_0, \lambda_1, \ldots, \lambda_n \in K, z_n \in R$ také, že*

$$z = \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + z_n t^{n+1}.$$

Dôkaz. (a) Nech $z \in R$. Keďže zobrazenie $\pi \circ \varphi$ je na, existuje prvok $\lambda \in K$, ktorý sa zobrazí na prvok $\pi(z) \in R/M$. Potom

$$z + M = \pi(z) = \pi \circ \varphi(\lambda) = \pi(\lambda) = \lambda + M,$$

takže $z - \lambda \in M$. Teraz nech $\lambda \neq \lambda' \in K$ tiež spĺňa $z - \lambda' \in M$. Potom platí $\lambda' + M = z + M = \lambda + M$, teda $\pi \circ \varphi(\lambda') = \pi \circ \varphi(\lambda)$. To je spor s prostotou zobrazenia $\pi \circ \varphi$. Teda prvok $\lambda \in K$ je určený jednoznačne.

(b) Najskôr ukážeme existenciu, budeme postupovať induktívne podľa $n \geq 0$. Nech $z \in R$. Z (a) nájdeme $\lambda_0 \in K$ také, že $z - \lambda_0 \in M$. Teda existuje $m_0 \in M$ spĺňajúce $z - \lambda_0 = m_0$. Keďže t je uniformizačný parameter pre R, tak ideál (t) obsahuje práve všetky neinvertibilné prvky R. Teda (t) je maximálny ideál a $M = (t)$. Takže existuje $z_0 \in R$ také, že $m_0 = z_0 t$. Potom máme $z = \lambda_0 + z_0 t$.

Predpokladajme, že už sme našli $\lambda_0, \ldots, \lambda_n \in K$ a $z_n \in R$ spĺňajúce

$$z = \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + z_n t^{n+1}.$$

Potom z (a) existuje $\lambda_{n+1} \in K$ také, že $z_n - \lambda_{n+1} \in M$. Teda existuje $m_{n+1} \in M$ také, že $z_n - \lambda_{n+1} = m_{n+1}$. Nájdeme $z_{n+1} \in R$ spĺňajúce $m_{n+1} = z_{n+1} t$ a dostávame

$$z_n t^{n+1} = (\lambda_{n+1} + z_{n+1} t) t^{n+1} = \lambda_{n+1} t^{n+1} + z_{n+1} t^{n+2}.$$

Dokopy $z = \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + \lambda_{n+1} t^{n+1} + z_{n+1} t^{n+2}$.

Teraz ukážeme jednoznačnosť. Pre spor predpokladajme, že máme dva rôzne rozklady pre nejaké $z \in R$ a nejaké $n \geq 0$:

$$z = \lambda_0 + \lambda_1 t + \cdots + \lambda_n t^n + z_n t^{n+1} = \omega_0 + \omega_1 t + \cdots + \omega_n t^n + w_n t^{n+1}.$$

Potom platí

$$0 = z - z = (\lambda_0 - \omega_0) + (\lambda_1 - \omega_1) t + \cdots + (\lambda_n - \omega_n) t^n + (z_n - w_n) t^{n+1}. \tag{1.1}$$

Položme $i = \min(j \in \{0, 1, \ldots, n\} \mid \lambda_j - \omega_j \neq 0)$. Pre všetky $j \in \{0, \ldots, n\}$ platí $\lambda_j - \omega_j \in K$, teda pokiaľ $\lambda_j - \omega_j \neq 0$, tak $\lambda_j - \omega_j$ je invertibilný prvok R. Takže

$$\begin{aligned} &\operatorname{ord}((\lambda_i - \omega_i) t^i) = i < j = \operatorname{ord}((\lambda_j - \omega_j) t^j), \\ &\operatorname{ord}((\lambda_i - \omega_i) t^i) = i < n + 1 \leq \operatorname{ord}((z_n - w_n) t^{n+1}), \end{aligned}$$

pre všetky $i \neq j \in \{0, 1, \ldots, n\}$ také, že $\lambda_j - \omega_j \neq 0$. Z Tvrdenia 2 teda dostávame, že

$$(\lambda_0 - \omega_0) + (\lambda_1 - \omega_1) t + \cdots + (\lambda_n - \omega_n) t^n + (z_n - w_n) t^{n+1} \neq 0,$$

čo je spor s predpokladom (1.1).

□

1.2 Mocninové rady

Definícia 3. *Nech K je pole a $(a_i)_{i=0}^{\infty}$ je postupnosť prvkov z K. Potom rad*

$$\sum_{i=0}^{\infty} a_i x^i$$

nazývame formálny mocninový rad nad K. *Množinu všetkých formálnych mocninových radov nad K značíme $K[[x]]$.*

Nech $\sum_{i=0}^{\infty} a_i x^i$ a $\sum_{i=0}^{\infty} b_i x^i$ sú dva formálne mocninové rady nad K. Potom definujeme ich súčet ako

$$\sum_{i=0}^{\infty} a_i x^i + \sum_{i=0}^{\infty} b_i x^i = \sum_{i=0}^{\infty} (a_i + b_i) x^i$$

a ich súčin ako

$$\left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty}\left(\sum_{i=j+k} a_j b_k\right) x^i.$$

Poznámka. Rozpísaním z definície ľahko ukážeme, že $K[[x]]$ je komutatívny okruh, ktorý obsahuje $K[x]$ ako podokruh. Navyše $K[[x]]$ je aj obor. Nech $\sum_{i=0}^{\infty} a_i x^i$ a $\sum_{i=0}^{\infty} b_i x^i$ sú dva nenulové mocninové rady nad K. Uvažujme $j_1 = \min(i \mid a_i \neq 0)$ a $j_2 = \min(i \mid b_i \neq 0)$. Potom platí

$$\left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty} b_i x^i\right) = a_{j_1} b_{j_2} x^{j_1+j_2} + \sum_{i>j_1+j_2}^{\infty} c_i x^i$$

pre vhodné $c_i \in K$. Keďže K je obor, platí $a_{j_1} b_{j_2} \neq 0$. Z toho vyplýva, že aj súčin $(\sum_{i=0}^{\infty} a_i x^i)(\sum_{i=0}^{\infty} b_i x^i)$ je nenulový. Tým sme ukázali, že $K[[x]]$ je obor. Jeho podielové pole značíme $K((x))$.

Tvrdenie 4. *Nech K je pole. Potom $K[[x]]$ je diskrétny valuačný okruh s uniformizačným parametrom x.*

Toto tvrdenie je dôsledkom nasledujúceho tvrdenia, ktoré nám hovorí ako vyzerajú invertibilné prvky v $K[[x]]$.

Tvrdenie 5. *Nech K je pole a $\sum_{i=0}^{\infty} a_i x^i \in K[[x]]$. Potom $\sum_{i=0}^{\infty} a_i x^i$ je invertibilným prvkom $K[[x]]$ práve vtedy, keď $a_0 \neq 0$.*

Dôkaz. $\Longleftarrow$ Najskôr predpokladajme, že $a_0 \neq 0$. Hľadáme formálny mocninový rad $\sum_{i=0}^{\infty} b_i x^i \in K[[x]]$ taký, že

$$\left(\sum_{i=0}^{\infty} a_i x^i\right)\left(\sum_{i=0}^{\infty} b_i x^i\right) = \sum_{i=0}^{\infty}\left(\sum_{i=j+k} a_j b_k\right) x^i = 1 + 0x + 0x^2 + \dots$$

Teda riešime sústavu rovníc:

$$\begin{aligned} a_0 b_0 &= 1 \\ a_0 b_1 + a_1 b_0 &= 0 \\ &\vdots \\ a_0 b_k + a_1 b_{k-1} + \cdots + a_k b_0 &= 0 \\ &\vdots \end{aligned}$$

Keďže K je pole, existuje v K inverz k nenulovému prvku a_0. Riešením prvej rovnice dostávame $b_0 = a_0^{-1}$. Výsledok dosadíme do druhej rovnice a vyjadríme b_1: $b_1 = -a_0^{-1}a_1b_0$. Induktívne postupujeme ďalej, pokiaľ už máme vyjadrené koeficienty $b_0, b_1, \ldots, b_{k-1}$ z prvých $k-1$ rovníc, dosadíme výsledky do $k-$tej rovnice a vyjadríme b_k: $b_k = -a_0^{-1}(a_1b_{k-1} + \cdots + a_kb_0)$. Mocninový rad, ktorý dostaneme je hľadaným inverzným prvkom k $\sum_{i=0}^{\infty} a_ix^i$.

$\Longrightarrow$ Teraz predpokladajme, že $a_0 = 0$. Potom $\sum_{i=0}^{\infty} a_ix^i \in xK[[x]]$, ale $xK[[x]]$ je vlastný ideál v $K[[x]]$. To znamená, že neobsahuje žiadne invertibilné prvky $K[[x]]$. Teda ani prvok $\sum_{i=0}^{\infty} a_ix^i$ nie je invertibilný. □

Teraz už môžeme dokázať tvrdenie 4.

Dôkaz. Vieme, že $K[[x]]$ je obor. Navyše $K[[x]]$ nie je pole - napríklad prvok x nemá v $K[[x]]$ inverz podľa tvrdenia 5. Ďalej x je ireducibilný prvok v $K[[x]]$. Ukážeme, že x je uniformizačný parameter pre $K[[x]]$. Nech $0 \neq \sum_{i=0}^{\infty} a_ix^i \in K[[x]]$ a označme $n = \min(i \mid a_i \neq 0) \in \mathbb{N}_0$. Potom $\sum_{i=0}^{\infty} a_ix^{i-n}$ je invertibilný prvok v $K[[x]]$ a platí

$$\sum_{i=0}^{\infty} a_ix^i = \left(\sum_{i=0}^{\infty} a_ix^{i-n}\right) x^n. \tag{1.2}$$

Keďže každý mocninový rad je jednoznačne určený svojimi koeficientami, aj vyjadrenie (1.2) je určené jednoznačne. Pre spor nech

$$\sum_{i=0}^{\infty} a_ix^i = \left(\sum_{j=0}^{\infty} b_jx^j\right) x^m = \left(\sum_{k=0}^{\infty} c_kx^k\right) x^p,$$

kde $\sum_{i=0}^{\infty} b_jx^j, \sum_{k=0}^{\infty} c_kx^k$ sú invertibilné prvky v $K[[x]]$, teda $b_0 \neq 0 \neq c_0$. Potom sa jednotlivé členy na obidvoch stranách musia rovnať, špeciálne $b_0x^m = c_0x^p$. Keďže b_0, c_0 sú nenulové, tak $m = p$ a $b_0 = c_0$. Porovnaním jednotlivých členov zistíme, že všetky ďalšie koeficienty sa musia rovnať. Takže x je naozaj uniformizačný parameter pre $K[[x]]$ a $K[[x]]$ je DVR. □

Uvažujme diskrétny valuačný okruh R s uniformizačným parametrom t a s maximálnym ideálom $M \leqslant R$. Ďalej uvažujme pole $K \subseteq R$ a predpokladajme, že zobrazenie $K \hookrightarrow R \twoheadrightarrow R/M$ je izomorfizmus. Položíme zobrazenie

$$\begin{aligned} \iota\colon R &\to K[[t]] \\ z &\mapsto \sum_{i=0}^{\infty} \lambda_it^i, \end{aligned}$$

ktoré každému $z \in R$ priradí mocninový rad s jednoznačne určenými koeficientami $\lambda_0, \lambda_1, \ldots \in K$ z tvrdenia 3(b).

Ukážeme, že zobrazenie ι je prostý okruhový homomorfizmus. Zjavne 1_R sa zobrazí na $1_{K[[t]]}$. Nech $z, w \in R$. Uvažujme jednoznačne určené koeficienty $\lambda_0, \lambda_1, \ldots, \omega_0, \omega_1, \ldots \in K$ také, že pre každé $n \geq 0$ platí:

$$\begin{aligned} z &= \lambda_0 + \lambda_1t + \cdots + \lambda_nt^n + z_nt^{n+1}, \\ w &= \omega_0 + \omega_1t + \cdots + \omega_nt^n + w_nt^{n+1}, \end{aligned}$$

pre jednoznačne určené $z_n, w_n \in R$. Potom pre každé $n \geq 0$ platí:

$$z + w = \lambda_0 + \omega_0 + (\lambda_1 + \omega_1)t + \cdots + (\lambda_n + \omega_n)t^n + (z_n + w_n)t^{n+1},$$
$$zw = \lambda_0\omega_0 + (\lambda_0\omega_1 + \lambda_1\omega_0)t + \cdots + \left(\sum_{n=i+j} \lambda_i\omega_j\right) t^n + v_n t^{n+1},$$

pre vhodné, jednoznačne určené, $v_n \in R$. Takže platí

$$\iota(z + w) = \sum_{i=0}^{\infty}(\lambda_i + \omega_i)t^i = \sum_{i=0}^{\infty} \lambda_i t^i + \sum_{i=0}^{\infty} \omega_i t^i = \iota(z) + \iota(w),$$
$$\iota(zw) = \sum_{i=0}^{\infty} \left(\sum_{i=j+k} \lambda_j\omega_k\right) t^i = \left(\sum_{i=0}^{\infty} \lambda_i t^i\right) \left(\sum_{i=0}^{\infty} \omega_i t^i\right) = \iota(z)\iota(w).$$

Stačí teda už len ukázať, že zobrazenie ι je prosté. Pre spor predpokladajme, že existuje $0 \neq z \in R$ také, že $\iota(z) = 0$. Takže pre príslušné koeficienty platí $0 = \lambda_0 = \lambda_1 = \ldots$ a pre každé $n \geq 0$ existuje jednoznačne určené $0 \neq z_n \in R$ spĺňajúce $z = 0 + 0t + \cdots + 0t^n + z_n t^{n+1}$. Zo vzťahu $z_n t^{n+1} = z = z_{n+1}t^{n+2}$ dostávame, že $z_n = z_{n+1}t$ pre každé $n \geq 0$. To nám dáva nekonečný ostro rastúci reťazec ideálov $(z_0) \subsetneq (z_1) \subsetneq (z_2) \subsetneq \ldots$ v R, čo je spor s noetherovskosťou R. Takže $\ker(\iota) = 0$ a zobrazenie ι je prosté.

Často píšeme $z = \sum_{i=0}^{\infty} \lambda_i t^i$ a sumu napravo nazývame *rozvoj prvku z do mocninového radu.*

2 Algebraické množiny

V tejto kapitole si zadefinujeme afinné a projektívne algebraické množiny a niekoľko pojmov s nimi súvisiacimi. Následne rozoberieme vzťah medzi afinnými a projektívnymi algebraickými množinami. V celej kapitole bude K označovať algebraicky uzavreté pole.

Táto kapitola vychádza z práce Fultona [1, Kapitoly 1, 2 a 4] a zo skrípt predmetu Úvod do komutatívní algebry [4, Kapitola 3].

2.1 Afinné algebraické množiny

Definícia 4. *Nech $P = (a_1, \ldots, a_n) \in K^n$ a $F \in K[x_1, \ldots, x_n]$. Bod P sa nazýva* nula *polynómu F, pokiaľ $F(P) = 0$. Množinu všetkých núl polynómu F značíme $V(F)$.*

Definícia 5. *Nech $S \subseteq K[x_1, \ldots, x_n]$ je ľubovoľná množina polynómov. Položme množinu*

$$V(S) := \{P \in K^n \mid \forall F \in S : P \text{ je nula polynómu } F\}.$$

Množina $V \subseteq K^n$ sa nazýva afinná algebraická množina*, pokiaľ existuje množina polynómov $S \subseteq K[x_1, \ldots, x_n]$ taká, že $V = V(S)$.*

Definícia 6. *Nech $X \subseteq K^n$ je ľubovoľná množina. Potom definujeme* ideál množiny X *ako*

$$I(X) := \{F \in K[x_1, \ldots, x_n] \mid \forall P \in X : F(P) = 0\}.$$

Poznámka. Rozpísaním z definície ľahko ukážeme, že ideál množiny X je skutočne ideál v okruhu $K[x_1, \ldots, x_n]$.

Definícia 7. *Afinná algebraická množina $V \subseteq K^n$ sa nazýva* reducibilná*, pokiaľ existujú afinné algebraické množiny $V_1, V_2 \subseteq K^n$ také, že $V = V_1 \cup V_2$ a $V_1 \neq V \neq V_2$. Inak povieme, že V je* ireducibilná*. Ireducibilná afinná algebraická množina sa nazýva* afinná varieta*.*

Tvrdenie 6. *Neprázdna afinná algebraická množina $V \subseteq K^n$ je ireducibilná práve vtedy, keď $I(V)$ je prvoideál.*

Dôkaz. Fulton [1, Kapitola 1.5, Tvrdenie 1]. □

Tvrdenie 7. *Nech $F \in K[x_1, \ldots, x_n]$ je nekonštantný polynóm a $F = F_1^{n_1} \cdots F_r^{n_r}$ je ireducibilný rozklad polynómu F. Potom $V(F) = V(F_1) \cup \cdots \cup V(F_r)$ je rozklad afinnej algebraickej množiny $V(F)$ na ireducibilné afinné algebraické množiny a $I(V(F)) = (F_1 \cdots F_r)$.*

Dôkaz. Tvrdenie je dôsledkom Hilbertovej vety o nulách [1, Kapitola 1.7, Dôsledok 3]. □

Definícia 8. *Nech $V \subseteq K^n$ je neprázdna afinná varieta. Potom* súradnicový okruh V *definujeme ako faktorokruh $K[V] := K[x_1, \ldots, x_n]/I(V)$.*

Definícia 9. *Nech $V \subseteq K^n$ je neprázdna množina. Označme $\mathcal{F}(V,K)$ množinu všetkých funkcií z V do K. Na množine $\mathcal{F}(V,K)$ definujeme operácie sčítania a násobenia nasledovne: Pre všetky $f, g \in \mathcal{F}(V,K)$ a $x \in V$ položíme $(f+g)(x) = f(x) + g(x)$ a $(fg)(x) = f(x)g(x)$.*

Poznámka. Množina $\mathcal{F}(V,K)$ spolu so zadefinovanými operáciami sčítania a násobenia tvorí okruh. To sa ľahko ukáže rozpísaním z definície a využitím vlastností operácii sčítania a násobenia v okruhu K.

Definícia 10. *Nech $V \subseteq K^n$ je neprázdna afinná varieta. Funkcia $f \in \mathcal{F}(V,K)$ sa nazýva* polynomiálna funkcia*, pokiaľ existuje polynóm $F \in K[x_1, \ldots, x_n]$ spĺňajúci $f(a_1, \ldots, a_n) = F(a_1, \ldots, a_n)$ pre všetky $(a_1, \ldots, a_n) \in V$.*

Poznámka. Množina polynomiálnych funkcií tvorí podokruh okruhu $\mathcal{F}(V,K)$. Dva polynómy $F, G \in K[x_1, \ldots, x_n]$ určujú rovnakú polynomiálnu funkciu práve vtedy, keď pre všetky $(a_1, \ldots, a_n) \in V$ platí $F(a_1, \ldots, a_n) = G(a_1, \ldots, a_n)$, teda $(F - G)(a_1, \ldots, a_n) = 0$. To nastáva práve vtedy, keď $F - G \in I(V)$. Teda polynomiálne funkcie $1:1$ odpovedajú triedam ekvivalencie faktorokruhu $K[V]$ a okruh $K[V]$ môžeme stotožniť s okruhom všetkých polynomiálnych funkcií na V. Prvky K odpovedajú konštantným polynomiálnym funkciam určeným danými prvkami, teda K môžeme považovať za podpole $K[V]$.

Poznámka. Podľa tvrdenia 6 pre neprázdnu afinnú varietu V platí, že $I(V)$ je prvoideál. Teda súradnicový okruh $K[V]$ je obor a má podielové pole.

Definícia 11. *Nech $V \subseteq K^n$ je neprázdna afinná varieta.* Pole racionálnych funkcií na V*, značíme $K(V)$, definujeme ako podielové pole súradnicového okruhu $K[V]$. Prvky $K(V)$ nazývame* racionálne funkcie na V.

Definícia 12. *Nech $V \subseteq K^n$ je neprázdna afinná varieta, f je racionálna funkcia na V a $P \in V$. Povieme, že racionálna funkcia f je* definovaná *v bode P, pokiaľ existujú polynomiálne funkcie $a, b \in K[V]$ také, že $f = a/b$ a $b(P) \neq 0$. Množinu všetkých racionálnych funkcií na V definovaných v bode P značíme $O_P(V)$ a nazývame* lokálny okruh V v bode P.

Poznámka. Jednoducho overíme, že množina $O_P(V)$ tvorí podokruh poľa $K(V)$. Teda platí $K \subseteq K[V] \subseteq O_P(V) \subseteq K(V)$. Neskôr ukážeme, že $O_P(V)$ je skutočne lokálny okruh.

Tvrdenie 8. *Nech $\emptyset \neq V \subseteq K^n$ je afinná varieta. Potom $K[V] = \cap_{P \in V} O_P(V)$.*

Dôkaz. Fulton [1, Kapitola 2.4, Tvrdenie 2]. □

Definícia 13. *Nech $V \subseteq K^n$ je neprázdna afinná varieta, $P \in V$ a $f \in O_P(V)$.* Hodnotu funkcie f v bode P *definujeme ako $f(P) = a(P)/b(P)$, kde $a, b \in K[V]$ sú polynomiálne funkcie spĺňajúce $f = a/b$ a $b(P) \neq 0$.*

Poznámka. Je potrebné overiť, že hodnota funkcie f v bode P je dobre definovaná. Uvažujme polynomiálne funkcie $a, b, c, d \in K[V]$ také, že $f = a/b = c/d$ a $b(P) \neq 0 \neq d(P)$. Potom platí $ad = cb$, teda $a(P)d(P) = (ad)(P) = (cb)(P) = c(P)b(P)$. Takže $a(P)/b(P) = c(P)/d(P)$ a hodnota funkcie f v bode P nezávisí na voľbe polynomiálnych funkcií a, b.

Poznámka. Uvažujme množinu $M_P(V) = \{f \in O_P(V) \mid f(P) = 0\}$. Potom množina $M_P(V)$ je jadrom dosadzovacieho homomorfismu

$$\begin{aligned} \varphi\colon O_P(V) &\to K \\ f &\mapsto f(P). \end{aligned}$$

Teda množina $M_P(V)$ tvorí ideál v okruhu $O_P(V)$. Navyše homomorfizmus φ je na, pretože každý prvok K je obrazom konštantnej funkcie určenej daným prvkom. Z prvej vety o izomorfizme teda platí $O_P(V)/M_P(V) \cong K$. Teda faktorokruh $O_P(V)/M_P(V)$ je pole, z čoho dostávame, že $M_P(V)$ je maximálny ideál v $O_P(V)$. Ideál $M_P(V)$ nazývame *maximálny ideál V v bode P.*

Uvažujme teraz racionálnu funkciu $f \in O_P(V)$ a nech $a, b \in K[V]$ spĺňajú $f = a/b$ a $b(P) \neq 0$. Potom funkcia f je invertibilná práve vtedy, keď existuje racionálna funkcia $g = c/d \in O_P(V)$, kde $c, d \in K[V], d(P) \neq 0$, taká, že $fg = 1$, ekvivalentne $ac = bd$. To nastáva práve vtedy, keď $a(P) \neq 0$ alebo ekvivalentne $f(P) \neq 0$. Teda množina všetkých neinvertibilných prvkov $O_P(V)$ je práve ideál $M_P(V)$, a preto $O_P(V)$ je lokálny okruh a $M_P(V)$ je jeho jednoznačne určený maximálny ideál.

Keďže $O_P(V)$ je podokruh poľa $K(V)$, je to obor. Dokonca je to noetherovský obor, ako hovorí nasledujúce tvrdenie.

Tvrdenie 9. *Nech $\emptyset \neq V \subseteq K^n$ je afinná varieta a $P \in V$. Potom $O_P(V)$ je noetherovský obor.*

Dôkaz. Fulton [1, Kapitola 2.4, Tvrdenie 3]. □

Poznámka. Predpokladajme, že $O_P(V)$ je DVR s uniformizačným parametrom t. Nech $0 \neq f = a/b \in K(V)$, kde $a, b \in K[V] \subseteq O_P(V)$. Potom existujú $n, m \in \mathbb{N}_0$ a invertibilné prvky $u, v \in O_P(V)$ také, že $a = ut^n$ a $b = vt^m$. Teda $f = uv^{-1}t^{n-m}$. Takže každý nenulový prvok $f' \in K(V)$ vieme zapísať v tvare $f' = u't^{n'}$, kde $u' \in O_P(V)$ je invertibilný prvok a $n' \in \mathbb{Z}$, a toto vyjadrenie je určené jednoznačne. Keby $f' = u't^{n'} = v't^{m'}$, kde $n' \leq m'$, tak $u' = v't^{m'-n'}$, teda $u'v'^{-1} = t^{m'-n'}$. Ale prvok t nie je invertibilný, teda $n' = m'$ a z toho už máme, že $u' = v'$.

Definícia 14. *Nech $V \subseteq K^n$ je neprázdna afinná varieta, $P \in V$ a platí, že $O_P(V)$ je diskrétny valuačný okruh s uniformizačným parametrom t. Potom každú nenulovú racionálnu funkciu $f \in K(V)$ vieme jednoznačne vyjadriť v tvare $f = ut^n$, kde $u \in O_P(V)$ je invertibilný prvok a $n \in \mathbb{Z}$. Definujeme* valuáciu f v bode P *ako $v_P(f) = n$. Valuáciu nulovej funkcie položíme $v_P(0) = \infty$.*

Poznámka. Vieme, že $O_P(V)$ je obor, teda má podielové pole Q. Ukážeme, že $Q \simeq K(V)$. Uvažujme zobrazenie

$$\begin{aligned} \varphi\colon Q &\to K(V) \\ \frac{a/b}{c/d} &\mapsto \frac{ad}{bc} \end{aligned}$$

Rozpísaním z definície overíme, že zobrazenie φ je okruhový homomorfizmus. Pre každé $f = a/b \in K(V)$ platí $\varphi(\frac{a/1}{b/1}) = a/b$, teda φ je na. Stačí teda overiť, že zobrazenie φ je prosté. Vieme, že jadro okruhového homomorfizmu je ideál.

Keďže Q je pole, obsahuje práve dva ideály, a to nulový ideál a seba samo. Avšak $\ker\varphi \neq Q$, lebo napríklad $\varphi(1_Q) = 1_{K(V)} \neq 0$. Takže $\ker\varphi = 0$ a φ je prosté.

Z toho dostávame, že $K(V)$ je podielové pole oboru $O_P(V)$. Valuácia racionálnej funkcie f v bode P je teda rád funkcie f vzhľadom ku diskrétnemu valuačnému okruhu $O_P(V)$. Zobrazenie v_P má teda rovnaké vlastnosti ako zobrazenie ord.

Definícia 15. *Nech $V \subseteq K^n$ je neprázdna afinná varieta, $P \in V$, $O_P(V)$ je diskrétny valuačný okruh a $f \in K(V)$. Povieme, že*

- *P je* nula *f, pokiaľ $v_P(f) > 0$,*
- *P je* pól *f, pokiaľ $v_P(f) < 0$,*
- *P je* nula *f* násobnosti *m, pokiaľ $v_P(f) = m > 0$,*
- *P je* pól *f* násobnosti *m, pokiaľ $v_P(f) = -m < 0$.*

2.2 Projektívne algebraické množiny

Definícia 16. *Bod $P = (p_1 : p_2 : \cdots : p_{n+1}) \in \mathbb{P}^n(K)$ sa nazýva* nula *polynómu $F \in K[x_1, x_2, \ldots, x_{n+1}]$, pokiaľ*

$$F(p_1, p_2, \ldots, p_{n+1}) = 0$$

pre každú voľbu projektívnych súradníc $(p_1 : p_2 : \cdots : p_{n+1})$ bodu P. Píšeme $F(P) = 0$.

Lema 10. *Nech $F \in K[x_1, \ldots, x_{n+1}]$ a platí $F = F_0 + \cdots + F_d$, kde F_i je homogénny polynóm stupňa i pre každé $i \in \{0, \ldots, d\}$. Nech bod $P = (p_1 : \cdots : p_{n+1}) \in \mathbb{P}^n(K)$ je nulou polynómu F. Potom pre každé $i \in \{0, \ldots, d\}$ je bod P nulou polynómu F_i.*

Dôkaz. Pre každé $i \in \{0, \ldots, d\}$ a pre každé $0 \neq \lambda \in K$ platí

$$F_i(\lambda p_1, \ldots, \lambda p_{n+1}) = \lambda^i F_i(p_1, \ldots, p_{n+1}).$$

Takže $F_i(p_1, \ldots, p_{n+1}) = 0$ práve vtedy, keď $F_i(\lambda p_1, \ldots, \lambda p_{n+1}) = 0$. Stačí nám teda overiť, že $F_i(p_1, \ldots, p_{n+1}) = 0$ pre jednu voľbu homogénnych súradníc bodu P.

Položme polynóm

$$G(\lambda) = F(\lambda p_1, \ldots, \lambda p_{n+1}) = \sum_{i=0}^{d} \lambda^i F_i(p_1, \ldots, p_{n+1}).$$

Potom G je polynóm v premennej λ s koeficientami $F_i(p_1, \ldots, p_{n+1}), i \in \{0, \ldots, d\}$ z poľa K. Keďže bod P je nulou polynómu F, pre každé $0 \neq \lambda \in K$ platí $G(\lambda) = 0$. Každý nenulový polynóm $H \in K[\lambda]$ má len konečne mnoho koreňov a pole K je alegbraický uzavreté, teda je nekonečné. Z toho vyplýva, že G musí byť nulový polynóm a pre všetky jeho koeficienty platí $F_i(p_1, \ldots, p_{n+1}) = 0, i \in \{0, \ldots, d\}$. □

Definícia 17. *Nech $S \subseteq K[x_1, \ldots, x_{n+1}]$ je ľubovoľná množina polynómov. Položme množinu*

$$V(S) := \{P \in \mathbb{P}^n(K) \mid \forall F \in S : P \text{ je nula polynómu } F\}.$$

Množina $V \subseteq \mathbb{P}^n(K)$ sa nazýva projektívna algebraická množina*, pokiaľ $V = V(\{F_1, F_2, \ldots, F_m\})$, kde $m \in \mathbb{N}$ a $F_1, F_2, \ldots, F_m \in K[x_1, \ldots, x_{n+1}]$ sú homogénne polynómy.*

Poznámka. Nech $S \subseteq K[x_1, \ldots, x_{n+1}]$ je ľubovoľná množina a I je ideál generovaný množinou S. Pole K je noetherovský okruh, teda z Hilbertovej vety o báze aj $K[x_1, \ldots, x_{n+1}]$ je noetherovský okruh. Takže každý ideál v $K[x_1, \ldots, x_{n+1}]$ je konečne generovaný. Špeciálne, existujú polynómy $F_1, \ldots, F_m \in K[x_1, \ldots, x_{n+1}]$ také, že $I = (\{F_1, \ldots, F_m\})$. Pre každé $i \in \{1, \ldots, m\}$ uvažujme rozklady $F_i = F_i^0 + F_i^1 + \cdots + F_i^{d_i}$, kde $F_i^j, j \in \{0, \ldots, d_i\}$ je homogénny polynóm stupňa j. Potom

$$V(S) = V(I) = V(\{F_1, \ldots, F_m\}) = V(\{F_i^j \mid i \in \{1, \ldots, m\}, j \in \{0, \ldots, d_i\}\}),$$

kde v poslednej rovnosti sme využili lemu 10. Teda pre ľubovoľnú množinu S je $V(S)$ projektívna algebraická množina.

Poznámka. Pojem *ideálu množiny, projektívnej reducibilnej algebraickej množiny* a *projektívnej variety* sa definuje analogicky ako v afinnom prípade. Podobne ako v afinnom prípade sa ukáže tiež tvrdenie, že neprázdna projektívna algebraická množina V je ireducibilná práve vtedy, keď $I(V)$ je prvoideál. Následujúce pojmy sú teda dobre definované.

Definícia 18. *Nech $V \subseteq \mathbb{P}^n(K)$ je neprázdna projektívna varieta.* Homogénny súradnicový okruh V *definujeme ako* $K_h[V] := K[x_1, \ldots, x_{n+1}]/I(V)$. *Prvok $f \in K_h[V]$ sa nazýva* forma stupňa d, *pokiaľ existuje homogénny polynóm $F \in K[x_1, \ldots, x_{n+1}]$ stupňa d, ktorého trieda ekvivalencie je f.* Homogénne funkčné pole V, *značíme $K_h(V)$, definujeme ako podielové pole oboru $K_h[V]$.*

Definícia 19. *Nech $V \subseteq \mathbb{P}^n(K)$ je neprázdna projektívna varieta.* Funkčné pole V, *značíme $K(V)$, definujeme ako množinu všetkých prvkov $z \in K_h(V)$, pre ktoré existujú formy $f, g \in K_h[V]$ rovnakého stupňa spĺňajúce $z = f/g$. Prvky $K(V)$ nazývame* racionálne funkcie na V.

Poznámka. Vieme ľahko overiť, že funkčné pole $K(V)$ je naozaj pole.

Definícia 20. *Nech $V \subseteq \mathbb{P}^n(K)$ je neprázdna projektívna varieta, $z \in K(V)$ a $P \in V$. Povieme, že racionálna funkcia z je* definovaná *v bode P, pokiaľ existujú formy $f, g \in K_h[V]$ rovnakého stupňa spĺňajúce $z = f/g$ a $g(P) \neq 0$.*

Poznámka. Pojmy *lokálneho okruhu* $O_P(V)$ a *maximálneho ideálu* $M_P(V)$ v bode P a *hodnoty* racionálnej funkcie v bode P definujeme rovnako ako v afinnom prípade. Tu je však dôležité si uvedomiť, že hodnota racionálnej funkcie je dobre definovaná. Uvažujme bod $P \in V$ a racionálnu funkciu $z \in K(V)$, ktorá je definovaná v bode P. Nech $f, g \in K_h[V]$ sú formy rovnakého stupňa $d \in \mathbb{N}_0$ spĺňajúce $z = f/g$ a $g(P) \neq 0$. Potom pre každé $0 \neq \lambda \in K$ platí

$$z(\lambda P) = \frac{f(\lambda P)}{g(\lambda P)} = \frac{\lambda^d f(P)}{\lambda^d g(P)} = \frac{f(P)}{g(P)} = z(P),$$

teda hodnota funkcie z nezávisí na voľbe homogénnych súradníc bodu P.

Pokiaľ je $O_P(V)$ diskrétny valuačný okruh, definujeme ďalej pojmy *valuácie, nuly* a *pólu* racionálnej funkcie v bode P rovnako ako v afinnom prípade.

Poznámka. Môžeme si všimnúť, že v afinnom aj v projektívnom priestore používame rovnaké značenie. Z kontextu bude však vždy jasné či sa nachádzame v afinnom, alebo v projektívnom priestore.

2.3 Projektívny uzáver

V tejto podkapitole si ukážeme, aký je vzťah medzi afinnými a projektívnymi varietami. K tomu budeme potrebovať zadefinovať homogenizáciu a dehomogenizáciu polynómu.

Definícia 21. *Nech R je obor a $F \in R[x_1, \ldots, x_n]$ je nenulový polynóm stupňa d. Potom polynóm F vieme zapísať v tvare $F = F_0 + F_1 + \cdots + F_d$, kde F_i je homogénny polynóm stupňa i. Položme polynóm*

$$F^* = x_{n+1}^d F_0 + x_{n+1}^{d-1} F_1 + \cdots + x_{n+1} F_{d-1} + F_d.$$

Potom $F^* \in R[x_1, \ldots, x_n, x_{n+1}]$ je homogénny polynóm stupňa d. Tento proces sa nazýva homogenizácia polynómu F vzhľadom k premennej x_{n+1}.

Poznámka. Pre nulový polynóm F položíme $F^* = 0$.

Definícia 22. *Nech R je obor a $F \in R[x_1, \ldots, x_{n+1}]$ je homogénny polynóm. Položme polynóm $F_* = F(x_1, \ldots, x_n, 1)$. Tento proces sa nazýva* dehomogenizácia polynómu F vzhľadom k premennej x_{n+1}.

Lema 11. *Nech R je obor a $F, G \in R[x_1, \ldots, x_n]$ sú nenulové polynómy. Potom platí*

(a) $(FG)^* = F^* G^*$,

(b) $(F^*)_* = F$.

Dôkaz. Nech d_F je stupeň polynómu F a d_G je stupeň polynómu G. Uvažujme rozklady $F = F_0 + \cdots + F_{d_F}$ a $G = G_0 + \cdots + G_{d_G}$, kde F_i, G_i sú homogénne polynómy stupňa i.

(a) Máme $FG = F_0G_0 + F_0G_1 + \cdots + F_0G_{d_G} + \cdots + F_{d_F}G_0 + \cdots + F_{d_F}G_{d_G}$. Keďže sme v obore, pre ľubovoľné dva nenulové polynómy $F', G' \in R[x_1, \ldots, x_n]$ platí $\deg(F'G') = \deg(F') + \deg(G')$. Teda FG je polynóm stupňa $d_F + d_G$ a platí

$$\begin{aligned}(FG)^* = {} & x_{n+1}^{d_F+d_G} F_0G_0 + x_{n+1}^{d_F+(d_G-1)} F_0G_1 + \cdots + \\ & + x_{n+1}^{d_F} F_0G_{d_G} + \cdots + x_{n+1}^{d_G} F_{d_F}G_0 + \cdots + F_{d_F}G_{d_G}.\end{aligned} \tag{2.1}$$

Ďalej platí

$$\begin{aligned}F^* &= x_{n+1}^{d_F} F_0 + x_{n+1}^{d_F-1} F_1 + \cdots + x_{n+1} F_{d_F-1} + F_{d_F}, \\ G^* &= x_{n+1}^{d_G} G_0 + x_{n+1}^{d_G-1} G_1 + \cdots + x_{n+1} G_{d_G-1} + G_{d_G}.\end{aligned}$$

Takže

$$\begin{aligned}F^*G^* = {} & x_{n+1}^{d_F} F_0 x_{n+1}^{d_G} G_0 + x_{n+1}^{d_F} F_0 x_{n+1}^{d_G-1} G_1 + \cdots + \\ & + x_{n+1}^{d_F} F_0 G_{d_G} + \cdots + F_{d_F} x_{n+1}^{d_G} G_0 + \cdots + F_{d_F} G_{d_G}.\end{aligned} \tag{2.2}$$

Výrazy v (2.1) a (2.2) sa zjavne rovnajú.

(b) $(F^*)_* = (x_{n+1}^{d_F} F_0 + \cdots + x_{n+1} F_{d_F-1} + F_{d_F})_* = 1^{d_F} F_0 + \cdots + 1 F_{d_F-1} + F_{d_F} = F.$

□

Poznámka. Pokiaľ nejaké z polynómov F, G sú nulové, lema 11 zjavne platí.

Lema 12. *Nech R je obor a $F, G \in R[x_1, \ldots, x_{n+1}]$ sú homogénne polynómy. Potom platí:*

(a) $(FG)_* = F_* G_*$.

(b) $(F+G)_* = F_* + G_*$.

(c) Pokiaľ $F \neq 0$ a $r \in \mathbb{N}_0$ je najväčšie číslo také, že x_{n+1}^r delí F, tak $x_{n+1}^r (F_*)^* = F$.

Dôkaz. Označme d_F^1 stupeň polynómu F a d_G^1 stupeň polynómu G. Ďalej označme d_F^2 (resp. d_G^2) stupeň polynómu F (resp. G) ako polynómu premennej x_{n+1} s koeficientami z $R[x_1, \ldots, x_n]$. Zjavne $d_F^1 \geq d_F^2$ a $d_G^1 \geq d_G^2$. Potom máme

$$\begin{aligned} F &= F_{d_F^1} + x_{n+1} F_{d_F^1-1} + \cdots + x_{n+1}^{d_F^2} F_{d_F^1-d_F^2}, \\ G &= G_{d_G^1} + x_{n+1} G_{d_G^1-1} + \cdots + x_{n+1}^{d_G^2} G_{d_G^1-d_G^2}, \end{aligned}$$

pre vhodné $F_{d_F^1-d_F^2}, \ldots, F_{d_F^1}, G_{d_G^1-d_G^2}, \ldots, G_{d_G^1} \in R[x_1, \ldots, x_n]$ také, že F_i, G_i je homogénny polynóm stupňa i.

(a) Platí

$$\begin{aligned} (FG)_* &= ((F_{d_F^1} + x_{n+1} F_{d_F^1-1} + \cdots + x_{n+1}^{d_F^2} F_{d_F^1-d_F^2})(G_{d_G^1} + x_{n+1} G_{d_G^1-1} + \\ &\quad + \cdots + x_{n+1}^{d_G^2} G_{d_G^1-d_G^2}))_* = \\ &= (F_{d_F^1} G_{d_G^1} + x_{n+1} F_{d_F^1} G_{d_G^1-1} + \cdots + x_{n+1}^{d_G^2} F_{d_F^1} G_{d_G^1-d_G^2} + \cdots + \\ &\quad + x_{n+1}^{d_F^2} F_{d_F^1-d_F^2} G_{d_G^1} + \cdots + x_{n+1}^{d_F^2+d_G^2} F_{d_F^1-d_F^2} G_{d_G^1-d_G^2})_* = \\ &= F_{d_F^1} G_{d_G^1} + F_{d_F^1} G_{d_G^1-1} + \cdots + F_{d_F^1} G_{d_G^1-d_G^2} + \cdots + F_{d_F^1-d_F^2} G_{d_G^1} + \\ &\quad + \cdots + F_{d_F^1-d_F^2} G_{d_G^1-d_G^2} = \\ &= (F_{d_F^1} + F_{d_F^1-1} + \cdots + F_{d_F^1-d_F^2})(G_{d_G^1} + G_{d_G^1-1} + \cdots + G_{d_G^1-d_G^2}) \\ &= F_* G_* \end{aligned}$$

(b) Ukáže sa analogicky ako (a).

(c) Máme $F = x_{n+1}^r F_{d_F^1-r} + x_{n+1}^{r+1} F_{d_F^1-(r+1)} + \cdots + x_{n+1}^{d_F^2} F_{d_F^1-d_F^2}$. Takže

$$\begin{aligned} x_{n+1}^r (F_*)^* &= x_{n+1}^r (F_{d_F^1-r} + F_{d_F^1-(r+1)} + \cdots + F_{d_F^1-d_F^2})^* = \\ &= x_{n+1}^r (F_{d_F^1-r} + x_{n+1} F_{d_F^1-(r+1)} + \cdots + x_{n+1}^{d_F^2-r} F_{d_F^1-d_F^2}) = F \end{aligned}$$

□

Definícia 23. *Nech $V \subseteq K^n$ je afinná algebraická množina. Uvažujme ideál $I = I(V) \leqslant K[x_1, \ldots, x_n]$. Položíme ideál I^* v okruhu $K[x_1, \ldots, x_{n+1}]$ generovaný množinou $\{F^* \mid F \in I\}$.* Projektívny uzáver V *definujeme ako* $V^* := V(I^*) \subseteq \mathbb{P}^n(K)$.

Tvrdenie 13. *Pokiaľ $V \subseteq K^n$ je ireducibilná afinná algebraická množina, tak jej projektívny uzáver $V^* \subseteq \mathbb{P}^n(K)$ je ireducibilná projektívna algebraická množina.*

Dôkaz. Fulton [1, Kapitola 4.3, Tvrdenie 3]. □

Poznámka. Uvažujme neprázdnu afinnú varietu $V \subseteq K^n$ a jej projektívny uzáver V^*. Pre formu $f \in K_h[V^*]$ stupňa d označme F homogénny polynóm stupňa d, ktorého trieda ekvivalencie je f. Potom f_* bude značiť triedu ekvivalencie polynómu F_* vo faktorokruhu $K[V]$. Nie je ťažké overiť, že f_* nie je závislé na voľbe polynómu F.

Tvrdenie 14. *Nech $V \subseteq K^n$ je neprázdna afinná varieta. Položme zobrazenie $\alpha\colon K(V^*) \to K(V), f/g \mapsto f_*/g_*$, kde $f, g \in K_h[V^*]$ sú formy rovnakého stupňa. Potom zobrazenie α je izomorfizmus polí $K(V^*)$ a $K(V)$.*

Dôkaz. Zobrazenie α zjavne zobrazí $1_{K(V^*)}$ na $1_{K(V)}$. Nech $f_1, g_1 \in K_h[V^*]$ sú formy rovnakého stupňa d_1 a $f_2, g_2 \in K_h[V^*]$ sú formy rovnakého stupňa d_2. S využitím lemy 12 platí:

$$\alpha\left(\frac{f_1}{g_1} + \frac{f_2}{g_2}\right) = \alpha\left(\frac{f_1g_2 + f_2g_1}{g_1g_2}\right) = \frac{(f_1g_2 + f_2g_1)_*}{(g_1g_2)_*} = \frac{(f_1g_2)_* + (f_2g_1)_*}{(g_1g_2)_*} =$$
$$= \frac{(f_1)_*(g_2)_* + (f_2)_*(g_1)_*}{(g_1)_*(g_2)_*} = \frac{(f_1)_*}{(g_1)_*} + \frac{(f_2)_*}{(g_2)_*} = \alpha\left(\frac{f_1}{g_1}\right) + \alpha\left(\frac{f_2}{g_2}\right),$$

$$\alpha\left(\frac{f_1}{g_1}\frac{f_2}{g_2}\right) = \alpha\left(\frac{f_1f_2}{g_1g_2}\right) = \frac{(f_1f_2)_*}{(g_1g_2)_*} = \frac{(f_1)_*(f_2)_*}{(g_1)_*(g_2)_*} = \frac{(f_1)_*}{(g_1)_*}\frac{(f_2)_*}{(g_2)_*} = \alpha\left(\frac{f_1}{g_1}\right)\alpha\left(\frac{f_2}{g_2}\right).$$

Teda α je homomorfizmus polí $K(V^*)$ a $K(V)$.

Nech $f/g \in K(V)$ a $F, G \in K[x_1, \ldots, x_n]$ sú postupne reprezentanti tried ekvivalencie f, g v $K[V]$. Uvažujme homogenizáciu F^*, G^* polynómov F, G vzhľadom k premennej x_{n+1}. Bez ujmy na všeobecnosti môžeme predpokladať, že $\deg(F^*) \leq \deg(G^*)$. Polynóm F^* prenásobíme $x_{n+1}^{\deg(G^*)-\deg(F^*)}$ a dostaneme homogénny polynóm rovnakého stupňa ako polynóm G^*. Označme f^*, g^* postupne triedy ekvivalencie polynómov F^*, G^* vo faktorokruhu $K_h[V^*]$. Potom $(x_{n+1}^{\deg(G^*)-\deg(F^*)}f^*)/g^*$ leží v $K(V^*)$ a podľa lem 11 a 12 platí

$$\alpha\left(\frac{(x_{n+1}^{\deg(G^*)-\deg(F^*)}f^*)}{g^*}\right) = \frac{\left(x_{n+1}^{\deg(G^*)-\deg(F^*)}f^*\right)_*}{(g^*)_*} = \frac{\left(x_{n+1}^{\deg(G^*)-\deg(F^*)}\right)_*(f^*)_*}{(g^*)_*} = \frac{f}{g}.$$

Takže α je na.

Zostáva ukázať, že zobrazenie α je prosté. Vieme, že jadrom okruhového homomorfizmu je ideál. Ale $K(V^*)$ je pole, teda obsahuje len dva ideály a to nulový ideál a celé pole $K(V^*)$. Teda máme dve možnosti - buď $\ker(\alpha) = 0_{K(V^*)}$, alebo $\ker(\alpha) = K(V^*)$. Keďže $\alpha(1_{K(V^*)}) = 1_{K(V)} \neq 0$, tak $\ker(\alpha) \neq K(V^*)$. Jadro zobrazenia α musí byť teda nulové a zobrazenie α je prosté.

Takže zobrazenie α je skutočne izomorfizmus polí $K(V^*)$ a $K(V)$. □

Poznámka. Uvažujme zúženie zobrazenia α na lokálny okruh $O_P(V^*)$ pre nejaký bod $P = (p_1 : \cdots : p_{n+1}) \in V^*, p_{n+1} \neq 0$. Označme $P_* = (p_1/p_{n+1}, \ldots, p_n/p_{n+1})$. Nech $f/g \in O_P(V^*)$, teda $f, g \in K_h[V^*]$ sú formy rovnakého stupňa a $g(P) \neq 0$. Potom ani $g(p_1/p_{n+1}, \ldots, p_n/p_{n+1}, 1) \neq 0$ (viď dôkaz lemy 10). Takže $g_*(P_*) \neq 0$ a $\alpha(f/g) \in O_{P_*}(V)$. Z toho vyplýva, že $\alpha(O_P(V^*)) \subseteq O_{P_*}(V)$. Navyše pre ľubovoľné $h \in K[V]$ platí, že pokiaľ $h(p_1/p_{n+1}, \ldots, p_n/p_{n+1}) \neq 0$, tak potom $h^*(p_1/p_{n+1}, \ldots, p_n/p_{n+1}, 1) \neq 0$. Takže zobrazenie $\alpha \restriction O_P(V^*)$ je na $O_{P_*}(V)$. Teda α je izomorfizmus $O_P(V^*)$ a $O_{P_*}(V)$.

3 Rovinné krivky

V tejto kapitole sa pozrieme na afinné a projektívne rovinné krivky a ich vlastnosti. Následne zavedieme pojem divizoru, ktorý budeme neskôr potrebovať k zadefinovaniu grupovej operácie na eliptickej krivke, ktorá je špeciálnym prípadom rovinnej krivky. Opäť bude K značiť algebraicky uzavreté pole.

V celej kapitole vychádzame z práce Fultona [1, Kapitoly 3 a 5.1] a Stichtenotha [3, Kapitola 1.4].

3.1 Afinné a projektívne rovinné krivky

Definícia 24. *Na množine $K[x, y]$ definujeme reláciu ekvivalencie $\sim$. Povieme, že dva polynómy $F, G \in K[x, y]$ sú* ekvivalentné*, pokiaľ existuje nenulové $\lambda \in K$ také, že $F = \lambda G$. Triedy ekvivalencie nekonštantných polynómov z $K[x, y]$ v tejto relácii ekvivalencie $\sim$ nazývame* afinné rovinné krivky*.*

Definícia 25. *Na množine $K[x, y, z]$ definujeme reláciu ekvivalencie $\sim$. Povieme, že dva polynómy $F, G \in K[x, y, z]$ sú* ekvivalentné*, pokiaľ existuje nenulové $\lambda \in K$ také, že $F = \lambda G$. Triedy ekvivalencie nekonštantných homogénnych polynómov z $K[x, y, z]$ v tejto relácii ekvivalencie $\sim$ nazývame* projektívne rovinné krivky*.*

Poznámka. Väčšinou vynechávame triedy ekvivalencie a afinnými rovinnými krivkami rozumieme polynómy, ktoré tieto triedy ekvivalencie určujú. Teda namiesto o afinnej rovinnej krivke $[y^3 - x^2]_\sim$ hovoríme o afinnej rovinnej krivke $y^3 - x^2$ alebo o afinnej rovinnej krivke danej rovnicou $y^3 = x^2$. Podobne pre projektívne rovinné krivky.

Povieme, že rovinná krivka je *ireducibilná*, pokiaľ polynóm, ktorý ju určuje, je ireducibilný. Pojem ireducibility rovinnej krivky $[F]_\sim$ nezávisí na voľbe zástupcu triedy ekvivalencie $[F]_\sim$.

Definícia 26. *Uvažujme afinnú (resp. projektívnu) rovinnú krivku určenú polynómom F. Povieme, že bod $P \in K^2$ (resp. bod $P \in \mathbb{P}^2(K)$)* leží *na krivke F, značíme $P \in F$, pokiaľ $F(P) = 0$.*

Poznámka. Pojem bodu ležiaceho na rovinnej krivke $[F]_\sim$ nezávisí na voľbe zástupcu triedy ekvivalencie $[F]_\sim$ a v prípade projektívnej rovinnej krivky ani na voľbe homogénnych súradníc daného bodu.

Definícia 27. *Nech F je afinná rovinná krivka a $P = (a, b) \in F$. Povieme, že bod P je* singulárny bod *F, pokiaľ*

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = 0.$$

Inak povieme, že bod P je nesingulárny bod *F.*

Afinná rovinná krivka, ktorá obsahuje len nesingulárne body, sa nazýva nesingulárna afinná rovinná krivka*.*

Definícia 28. *Nech F je projektívna rovinná krivka a $P = (p_1 : p_2 : p_3) \in F$. Povieme, že bod P je* singulárny bod *F, pokiaľ*

$$\frac{\partial F}{\partial x}(P) = \frac{\partial F}{\partial y}(P) = \frac{\partial F}{\partial z}(P) = 0.$$

Inak povieme, že bod P je nesingulárny bod *F.*

Projektívna rovinná krivka, ktorá obsahuje len nesingulárne body, sa nazýva nesingulárna projektívna rovinná krivka*.*

Poznámka. Singulárny bod na projektívnej rovinnej krivke je dobre definovaný, teda nezávisí na voľbe projektívnych súradníc bodu P. Je to preto, že polynóm F je homogénny, a teda aj všetky jeho parciálne derivácie sú homogénne polynómy.

Tvrdenie 15. *Nech F je projektívna rovinná krivka a $P = (p_1 : p_2 : p_3) \in F$ je bod ležiaci na krivke F spĺňajúci $p_3 \neq 0$. Potom P je nesingulárny bod F práve vtedy, keď bod $(p_1/p_3, p_2/p_3)$ je nesingulárny bod afinnej rovinnej krivky F_*.*

Dôkaz. Kirwan [5, Kapitola 2.4, Lema 2.31]. □

Tvrdenie 16. *Nech $F \neq z$ je ireducibilná projektívna rovinná krivka. Potom afinná rovinná krivka F_* je ireducibilná.*

Dôkaz. Nech $r \in \mathbb{N}_0$ je najväčšie číslo také, že z^r delí F. Polynóm F je ireducibilný, takže $r \leq 1$. Ak $r = 1$, tak z ireducibility F musí platiť $F = z$, čo je spor s predpokladom. Teda $r = 0$.

Pre spor predpokladajme, že polynóm F_* nie je ireducibilný. Takže existujú polynómy $G, H \in K[x, y]$ také, že $\deg(G), \deg(H) < \deg(F_*)$ a $F_* = GH$. Potom z lem 11 a 12 vyplýva

$$F = z^r(F_*)^* = (F_*)^* = (GH)^* = G^*H^*,$$

čo je spor s ireducibilitou F. Teda afinná rovinná krivka F_* je ireducibilná. □

Tvrdenie 17. *Nech F je ireducibilná afinná rovinná krivka. Potom projektívna rovinná krivka F^* je ireducibilná.*

Dôkaz. Pre spor predpokladajme, že projektívna rovinná krivka F^* nie je ireducibilná. Teda existujú polynómy $G, H \in K[x, y, z]$ také, že $\deg(G), \deg(H) < \deg(F^*)$ a $F^* = GH$. Potom z lem 11 a 12 vyplýva

$$F = (F^*)_* = (GH)_* = G_*H_*.$$

Keďže z nedelí F^*, ani jeden z polynómov G, H nie je rovný $\lambda z^s, s \geq 1$ pre nejaké $0 \neq \lambda \in K$. Takže ani jeden z polynómov G_*, H_* nie je invertibilným prvkom $K[x, y]$. To je spor s ireducibilitou F. □

Poznámka. Pre ireducibilnú afinnú rovinnú krivku F je $V(F)$ afinná varieta podľa tvrdenia 7. Namiesto značenia $K[V(F)], O_P(V(F))$ a $K(V(F))$ budeme používať značenie $K[F], O_P(F)$ a $K(F)$. Rovnako pre ireducibilné projektívne rovinné krivky.

Tvrdenie 18. *Nech F je ireducibilná afinná rovinná krivka a $P \in F$. Potom P je nesingulárny bod krivky F práve vtedy, keď $O_P(F)$ je DVR.*

Dôkaz. Fulton [1, Kapitola 3.2, Veta 1]. □

3.2 Divizory

K zavedeniu pojmu divizoru budeme potrebovať najskôr zadefinovať pojem voľnej abelovskej grupy.

Definícia 29. Voľná abelovská grupa nad množinou (alebo generovaná množinou) X *je ľubovoľná abelovská grupa* G *taká, že* $G = \langle X \rangle$ *a pre každú abelovskú grupu* H *a každé zobrazenie* $f\colon X \to H$ *existuje práve jeden homomorfizmus* $\varphi\colon G \to H$ *spĺňajúci* $\varphi \restriction X = f$. *Množina* X *sa nazýva* voľná báza G.

Definícia 30. *Nech* F *je nesingulárna ireducibilná projektívna rovinná krivka.* Grupu divizorov F, *značíme* $\mathrm{Div}(F)$, *definujeme ako (aditívne značenú) voľnú abelovskú grupu generovanú bodmi krivky* F. *Prvky* $\mathrm{Div}(F)$ *nazývame* divizory F.

Poznámka. Divizor krivky F môžeme vyjadriť ako formálnu sumu

$$\sum_{P \in F} n_P P,$$

kde $n_P \in \mathbb{Z}$ pre každé $P \in F$ a len konečne mnoho n_P je nenulových.

Operácia sčítania v grupe $\mathrm{Div}(F)$ potom prebieha po zložkách, teda pre $D_1 = \sum n_P^1 P, D_2 = \sum n_P^2 P \in \mathrm{Div}(F)$ platí

$$D_1 + D_2 = \sum_{P \in F} (n_P^1 + n_P^2) P.$$

Nulový prvok grupy $\mathrm{Div}(F)$ je divizor

$$0 := \sum_{P \in F} n_P P, \text{ kde } n_P = 0 \text{ pre všetky } P \in F.$$

Definícia 31. *Nech* F *je nesingulárna ireducibilná projektívna rovinná krivka a* $D \in \mathrm{Div}(F)$. Nosič *divizoru* D *definujeme ako množinu*

$$\mathrm{supp}(D) := \{P \in F \mid n_P \neq 0\}.$$

Definícia 32. *Nech* F *je nesingulárna ireducibilná projektívna rovinná krivka a* $Q \in F$. *Definujeme zobrazenie*

$$\begin{aligned} v_Q\colon \mathrm{Div}(F) &\to \mathbb{Z} \\ \sum_{P \in F} n_P P &\mapsto n_Q. \end{aligned}$$

Poznámka. Pre divizor $D = \sum_{P \in F} n_P P \in \mathrm{Div}(F)$ teda máme

$$D = \sum_{P \in \mathrm{supp}(D)} v_P(D) \cdot P.$$

Definícia 33. *Nech* F *je nesingulárna ireducibilná projektívna rovinná krivka. Na množine* $\mathrm{Div}(F)$ *zadefinujeme čiastočné usporiadanie* $\leq$. *Pre* $D_1, D_2 \in \mathrm{Div}(F)$ *položíme* $D_1 \leq D_2$, *pokiaľ pre všetky* $P \in F$ *platí* $v_P(D_1) \leq v_P(D_2)$. *Pokiaľ platí* $D_1 \leq D_2$ *a* $D_1 \neq D_2$, *píšeme* $D_1 < D_2$.

Definícia 34. *Nech F je nesingulárna ireducibilná projektívna rovinná krivka a $D \in \mathrm{Div}(F)$.* Stupeň *divizoru D definujeme ako*

$$\deg D := \sum_{P \in F} v_P(D).$$

Poznámka. Stupeň divizoru nám dáva grupový homomorfizmus $\deg\colon \mathrm{Div}(F) \to \mathbb{Z}$. Jadro tohto homomorfizmu budeme značiť $\mathrm{Div}_0(F)$, teda

$$\mathrm{Div}_0(F) = \{D \in \mathrm{Div}(F) \mid \sum_{P \in F} v_P(D) = 0\}.$$

Keďže množina $\mathrm{Div}_0(F)$ je jadrom grupového homomorfizmu, je to podgrupa grupy $\mathrm{Div}(F)$.

Poznámka. Nech F je nesingulárna ireducibilná projektívna rovinná krivka nad K. Najskôr nech $F \notin \{x, y, z\}$. Z dôkazu tvrdenia 16 platí, že $(F_*)^* = F$, a rovnaký výsledok dostaneme aj pri dehomogenizácii a následnej homogenizácii podľa zvyšných dvoch premenných. V prípade, že $F = z$ uvažujeme (de)homogenizáciu len podľa premenných x, y. Analogicky pre $F \in \{x, y\}$.

Nech $P = (p_1 : p_2 : p_3) \in F$. Potom existuje $i \in \{1, 2, 3\}$ také, že $p_i \neq 0$; bez ujmy na všeobecnosti nech $i = 3$. Z tvrdenia 15 je bod $P_* = (p_1/p_3, p_2/p_3)$ nesingulárny bod F_*. Takže $O_{P_*}(F_*)$ je DVR podľa tvrdenia 18. Keďže $(F_*)^* = F$, podľa poznámky za tvrdením 14 platí $O_{P_*}(F_*) \simeq O_P(F)$ (to, že $V((F_*)^*)$ je projektívny uzáver $V(F_*)$ sa ukáže analogicky ako v prípade eliptickej krivky v kapitole 4). Takže aj $O_P(F)$ je DVR a následujúce pojmy sú dobre definované.

Definícia 35. *Nech F je nesingulárna ireducibilná projektívna rovinná krivka nad K a $g \in K(F)$ je nenulová racionálna funkcia na F. Označme Z množinu všetkých núl funkcie g a N množinu všetkých pólov funkcie g. Potom definujeme:*

- nulový divizor g *ako* $(g)_0 := \sum_{P \in Z} v_P(g)P$,
- pólový divizor g *ako* $(g)_\infty := \sum_{P \in N}(-v_P(g))P$ *a*
- hlavný divizor g *ako* $(g) := (g)_0 - (g)_\infty$.

Množinu všetkých hlavných divizorov značíme $\mathrm{PDiv}(F)$.

Overíme, že nulový, pólový a hlavný divizor sú naozaj divizory, teda, že množiny Z a N sú konečné.

Tvrdenie 19. *Nech F je nesingulárna ireducibilná projektívna rovinná krivka nad K a $g \in K(F)$ je nenulová racionálna funkcia na F. Označme Z množinu všetkých núl funkcie g a N množinu všetkých pólov funkcie g. Potom množiny Z a N sú konečné.*

Dôkaz. Najskôr tvrdenie rozoberieme v afinnom prípade pre polynomiálne funkcie. Bez ujmy na všeobecnosti môžeme predpokladať, že $F \neq z$, a uvažovať afinnú rovinnú krivku určenú polynómom F_*. V prípade, že $F = z$, budeme uvažovať dehomogenizáciu podľa inej premennej než z a inak budeme postupovať analogicky ako v prípade $F \neq z$. Z tvrdenia 15 vyplýva, že krivka F_* je nesingulárna, a z tvrdenia 16 vyplýva, že krivka F_* je ireducibilná. Nech $h \in K[F_*]$ je nenulová polynomiálna funkcia na $V(F_*)$ a $H \in K[x,y]$ je zástupca triedy ekvivalencie h

vo faktorokruhu $K[F_*]$. Bod $P \in F_*$ je nula funkcie h práve vtedy, keď $v_P(h) > 0$. To nastáva práve vtedy, keď $h \in M_P(F_*)$, teda $h(P) = 0$. Chceme teda ukázať, že množina všetkých bodov krivky F_*, ktoré sú nulami polynómu H, je konečná; inými slovami $|V(F_*) \cap V(H)| < \infty$.

Vieme, že polynóm F_* je ireducibilný, teda buď $\mathrm{NSD}_{K[x,y]}(F_*, H) = 1$, alebo $\mathrm{NSD}_{K[x,y]}(F_*, H) = F_*$. Navyše h je nenulová polynomiálna funkcia, teda existuje nejaký bod P na krivke F_* (to znamená bod P spĺňajúci $F_*(P) = 0$) taký, že $H(P) \neq 0$. Preto polynóm F_* nedelí polynóm H a $\mathrm{NSD}_{K[x,y]}(F_*, H) = 1$. Pozrieme sa na polynómy F_*, H v obore $K(x)[y]$. Keďže K je pole, $K[x]$ je euklidovský, teda aj gaussovský obor. Ďalej $K(x)$ je podielové pole oboru $K[x]$. Môžeme teda použiť Gaussovu lemu o ireducibilite, z ktorej vyplýva, že polynóm F_* je ireducibilný aj v obore $K(x)[y]$. Z ireducibility F_* v $K[x][y]$ tiež vyplýva, že polynóm F_* je primitívny v $K[x][y]$. Podľa tvrdenia [4, Tvrdenie 1.16] teda máme, že polynóm F_* nedelí polynóm H ani v obore $K(x)[y]$. Takže $\mathrm{NSD}_{K(x)[y]}(F_*, H) = 1$.

Keďže $K(x)$ je pole, $K(x)[y]$ je euklidovský obor. Takže existujú Bézoutove koeficienty $U, V \in K(x)[y]$ spĺňajúce $1 = UF_* + VH$. Nech $U_0, V_0 \in K[x, y]$ a $0 \neq U_1, V_1 \in K[x]$ také, že $U = U_0/U_1$ a $V = V_0/V_1$. Potom máme

$$\begin{aligned} 1 &= \frac{U_0}{U_1} F_* + \frac{V_0}{V_1} H, \\ U_1 V_1 &= U_0 F_* + V_0 H. \end{aligned}$$

Nenulový polynóm U_1V_1 jednej premennej x má konečne mnoho koreňov a pre každý bod $P = (x_0, y_0) \in V(F_*) \cap V(H)$ platí

$$\begin{aligned} (U_1V_1)(x_0) &= U_0(x_0, y_0)F_*(x_0, y_0) + V_0(x_0, y_0)H(x_0, y_0) = \\ &= U_0(x_0, y_0) \cdot 0 + V_0(x_0, y_0) \cdot 0 = 0. \end{aligned}$$

Takže máme len konečne mnoho možností pre x-ovú súradnicu x_0 bodu $P \in V(F_*) \cap V(H)$. Analogicky ukážeme, že máme len konečne mnoho možností aj pre y-ovú súradnicu y_0 bodu P. Z toho vyplýva, že $|V(F_*) \cap V(H)| < \infty$.

Uvažujme teraz formy z okruhu $K_h[F]$. Nech bod $P = (p_1 : \cdots : p_{n+1}) \in F$ je nulou formy $0 \neq g \in K_h[F]$. Potom bod $P_* = (p_1/p_{n+1}, \ldots, p_n/p_{n+1})$ je nulou polynomiálnej funkcie g_*. Z predchádzajúceho vieme, že množina núl polynomiálnej funkcie $g_* \in K[F_*]$ je konečná, takže aj množina núl formy g je konečná.

Teraz už môžeme dokázať tvrdenie v projektívnom prípade pre racionálne funkcie. Nech $g \in K(F)$ je nenulová racionálna funkcia na $V(F)$. Zafixujme bod $P \in F$, v ktorom je funkcia g definovaná. Teda existujú formy $a, b \in K_h[F]$ rovnakého stupňa také, že $g = a/b$ a $b(P) \neq 0$. Označme Z_b množinu núl formy b; už vieme, že táto množina je konečná. Navyše v každom bode množiny $V(F) \setminus Z_b$ je funkcia g definovaná. Pokiaľ bod $Q \in V(F) \setminus Z_b$ je nulou funkcie g, tak $v_Q(g) > 0$. Teda $g \in M_Q(F)$, čo nastáva práve vtedy, keď $g(Q) = 0$. Z toho vyplýva, že $a(Q) = 0$. Množina núl formy a je ale konečná, teda len konečne mnoho prvkov množiny $V(F) \setminus Z_b$ je nulou funkcie g. Nejaké prvky z množiny Z_b môžu byť tiež nulami funkcie g. Keďže je ale množina Z_b konečná, môže nám pribudnúť len konečne mnoho núl. Množina Z všetkých núl funkcie g je teda konečná. To, že množina N všetkých pólov funkcie g je konečná, vyplýva z faktu, že množina pólov funkcie g je rovná množine núl funkcie $1/g$. □

Poznámka. Zjavne $(g) = \sum_{P \in F} v_P(g)P$ pre každé $0 \neq g \in K(F)$. Uvažujme racionálne funkcie $0 \neq g, h \in K(F)$. Potom platí

$$(g) + (h) = \sum_{P \in F} (v_P(g) + v_P(h))P = \sum_{P \in F} v_P(gh)P = (gh) \; a \tag{3.1}$$

$$-(g) = (g^{-1}), \tag{3.2}$$

kde v druhej rovnosti v (3.1) sme využili tvrdenie 1. Takže množina $\mathrm{PDiv}(F)$ je uzavretá na sčítanie a na opačný prvok. Navyše $0 \in \mathrm{PDiv}(F)$, pretože hlavný divizor nenulovej konštantnej polynomiálnej funkcie je nulový divizor. Z toho dostávame, že $\mathrm{PDiv}(F)$ tvorí podgrupu grupy $\mathrm{Div}(F)$.

Tvrdenie 20. *Nech F je nesingulárna ireducibilná projektívna rovinná krivka nad K a uvažujme nekonštantnú racionálnu funkciu $g \in K(F)$. Potom platí*

$$\deg (g)_0 = \deg (g)_\infty. \tag{3.3}$$

Dôkaz. Stichtenoth [3, Veta 1.4.11]. □

Poznámka. Pre nenulovú konštantnú racionálnu funkciu $g \in K(F)$ platí rovnosť (3.3) triviálne:

$$\deg (g)_0 = 0 = \deg (g)_\infty.$$

Takže pre každú nenulovú racionálnu funkciu $g \in K(F)$ platí:

$$\sum_{P \in Z} v_P(g) = \sum_{P \in N} (-v_P(g))$$

Z toho vyplýva, že každá nenulová racionálna funkcia na $V(F)$ má až na násobnosť rovnako veľa núl a pólov.

Navyše pre každú racionálnu funkciu $0 \neq g \in K(F)$ platí

$$\deg (g) = \deg ((g)_0 - (g)_\infty) = \deg (g)_0 - \deg (g)_\infty = 0.$$

Takže $(g) \in \mathrm{Div}_0(F)$ a $\mathrm{PDiv}(F)$ je podgrupou grupy $\mathrm{Div}_0(F)$.

Nakoniec ešte uvedieme definíciu Riemann-Rochového priestoru, ktorý budeme potrebovať v dôkaze Cayleyho vety.

Definícia 36. *Nech F je nesingulárna ireducibilná projektívna rovinná krivka nad K a $A \in \mathrm{Div}(F)$.* Riemann-Rochov priestor pridružený *A definujeme ako množinu*

$$\mathscr{L}(A) := \{0\} \cup \{0 \neq g \in K(F) \mid (g) \geq -A\}.$$

Poznámka. Pokiaľ

$$A = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j,$$

kde $n_i > 0$ pre všetky $i \in \{1, \ldots, r\}$ a $m_j > 0$ pre všetky $j \in \{1, \ldots, s\}$, tak pre nenulové prvky množiny $\mathscr{L}(A)$ platí:

- v bode Q_j musia mať nulu násobnosti aspoň m_j pre každé $j \in \{1, \ldots, s\}$ a

- póly môžu mať len v bodoch $P_1, \ldots, P_r$, pričom v bode P_i môžu mať pól násobnosti najviac n_i pre každé $i \in \{1, \ldots, r\}$.

Vo všetkých ostatných bodoch sú prvky $\mathscr{L}(A)$ definované.

Lema 21. *Nech F je nesingulárna ireducibilná projektívna rovinná krivka nad K a $A \in \mathrm{Div}(F)$. Potom $\mathscr{L}(A)$ je vektorový priestor nad K.*

Dôkaz. Stichtenoth [3, Lema 1.4.6]. □

4 Eliptické krivky nad $\mathbb{C}$

Špeciálnym prípadom afinnej rovinnej krivky je eliptická krivka. Najskôr sa pozrieme na základné vlastnosti eliptických kriviek, a potom si zavedieme grupovú operáciu na eliptickej krivke.

V celej kapitole vychádzame z práce Washingtona [6, Kapitola 2] a z práce Stichtenotha [3, Kapitola 1].

4.1 Definícia a základné vlastnosti

Definícia 37. Eliptickou krivkou nad $\mathbb{C}$ *rozumieme afinnú rovinnú krivku danú rovnicou*

$$y^2 = x^3 + ax + b, \tag{4.1}$$

kde $a, b \in \mathbb{C}$ *a* $4a^3 + 27b^2 \neq 0$. *Rovnicu* (4.1) *nazývame* Weierstrassova rovnica *eliptickej krivky.*

Poznámka. Pozrieme sa bližšie na to, čo hovorí podmienka $4a^3 + 27b^2 \neq 0$. Uvažujme obecný polynóm nad $\mathbb{C}$ stupňa n

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \tag{4.2}$$

s koreňmi $x_1, \ldots, x_n$. Diskriminant polynómu (4.2) definujeme ako

$$D = a_n^{2n-2} \prod_{i<j}^{n} (x_i - x_j)^2.$$

Môžeme vidieť, že diskriminant D je rovný nule práve vtedy, keď aspoň jeden koreň polynómu (4.2) je násobnosti aspoň 2. Navyše diskriminant D je symetrický polynóm v premenných $x_1, \ldots, x_n$. Takže podľa základnej vety o symetrických polynómoch ([7, Veta 11.2]) a Viètových vzťahov môžeme diskriminant D vyjadriť len pomocou koeficientov $a_0, \ldots, a_n$. V prípade obecného kubického polynómu $a_3x^3 + a_2x^2 + a_1x + a_0$ dostaneme vyjadrenie diskriminantu v tvare

$$D = 18a_3a_2a_1a_0 - 4a_2^3a_0 + a_2^2a_1^2 - 4a_3a_1^3 - 27a_3^2a_0^2.$$

V našom prípade je $a_3 = 1, a_2 = 0, a_1 = a, a_0 = b$, teda $D = -4a^3 - 27b^2$. Podmienka $4a^3 + 27b^2 \neq 0$ nám teda hovorí, že kubický polynóm $x^3 + ax + b$ má tri po dvoch rôzne korene.

Pokiaľ $r_1, r_2, r_3 \in \mathbb{C}$ sú tri po dvoch rôzne korene polynómu $x^3 + ax + b$, potom Weierstrassovu rovnicu $y^2 = x^3 + ax + b$ eliptickej krivky môžeme vyjadriť v tvare

$$y^2 = (x - r_1)(x - r_2)(x - r_3).$$

Tvrdenie 22. *Množina všetkých bodov ležiacich na eliptickej krivke E je afinná varieta v $\mathbb{C}^2$.*

Dôkaz. Nech E je eliptická krivka nad $\mathbb{C}$ daná rovnicou $y^2 = (x-r_1)(x-r_2)(x-r_3)$. Množina všetkých bodov ležiacich na eliptickej krivke E je afinná algebraická množina $V(E) = V(y^2 - (x - r_1)(x - r_2)(x - r_3)) \subseteq \mathbb{C}^2$. Ukážeme, že je to

ireducibilná afinná algebraická množina. Položme obor $R = \mathbb{C}[x]$ a jeho podielové pole $Q = \mathbb{C}(x)$. Keďže $\mathbb{C}$ je pole, obor $\mathbb{C}[x]$ je euklidovský, a teda aj gaussovský. Uvažujme polynóm $F = y^2 - (x - r_1)(x - r_2)(x - r_3) \in \mathbb{C}[x, y]$ ako polynóm premennej y s koeficientami v R. Polynóm F je primitívny a z Gaussovej vety o ireducibilite vyplýva, že polynóm F je ireducibilný v $R[y]$ práve vtedy, keď je ireducibilný v $Q[y]$. Pre spor predpokladajme, že polynóm F nie je ireducibilný nad Q. Keďže je to polynóm druhého stupňa, musí mať v Q koreň, teda existuje $G \in Q = \mathbb{C}(x)$ spĺňajúce $G^2 = (x - r_1)(x - r_2)(x - r_3)$. Také G však neexistuje, teda máme spor. Z toho dostávame, že polynóm F je ireducibilný nad R. Teda aj algebraická množina $V(E)$ je ireducibilná podľa tvrdenia 7. □

Poznámka. Jednoduchým dôsledkom dôkazu tvrdenia 22 je, že eliptická krivka je ireducibilná afinná rovinná krivka.

Poznámka. Nech E je eliptická krivka nad $\mathbb{C}$ daná rovnicou

$$y^2 = (x - r_1)(x - r_2)(x - r_3).$$

Z tvrdenia 7 vieme, že ideál afinnej variety $V(E) = V(y^2 - (x - r_1)(x - r_2)(x - r_3))$ je rovný $I(E) = (y^2 - (x - r_1)(x - r_2)(x - r_3)) \leqslant \mathbb{C}[x, y]$. Uvažujme ideál I^* v okruhu $\mathbb{C}[x, y, z]$ generovaný množinou $\{F^* \mid F \in I(E)\}$. Platí

$$(y^2 - (x - r_1)(x - r_2)(x - r_3))^* = y^2 z - (x - r_1 z)(x - r_2 z)(x - r_3 z).$$

Ďalej pre každé $F \in I(E)$ existuje $G \in \mathbb{C}[x, y]$ také, že

$$F = G(y^2 - (x - r_1)(x - r_2)(x - r_3)).$$

Potom

$$\begin{aligned} F^* &= (G(y^2 - (x - r_1)(x - r_2)(x - r_3)))^* = G^*(y^2 - (x - r_1)(x - r_2)(x - r_3))^* = \\ &= G^*(y^2 z - (x - r_1 z)(x - r_2 z)(x - r_3 z)) \\ &\in (y^2 z - (x - r_1 z)(x - r_2 z)(x - r_3 z))\mathbb{C}[x, y, z]. \end{aligned}$$

Takže

$$I^* \subseteq (y^2 z - (x - r_1 z)(x - r_2 z)(x - r_3 z))\mathbb{C}[x, y, z].$$

Naopak $y^2 - (x - r_1)(x - r_2)(x - r_3) \in I(E)$, teda $y^2 z - (x - r_1 z)(x - r_2 z)(x - r_3 z) \in I^*$. Takže

$$(y^2 z - (x - r_1 z)(x - r_2 z)(x - r_3 z))\mathbb{C}[x, y, z] \subseteq I^*.$$

Dokopy $I^* = (y^2 z - (x - r_1 z)(x - r_2 z)(x - r_3 z))\mathbb{C}[x, y, z]$ a projektívny uzáver $V(E^*)$ afinnej variety $V(E)$ je rovný

$$V(E^*) = V(I^*) = V(y^2 z - (x - r_1 z)(x - r_2 z)(x - r_3 z)) \subseteq \mathbb{P}^2(\mathbb{C}).$$

Projektívnu rovinnú krivku danú polynómom $y^2 z - (x - r_1 z)(x - r_2 z)(x - r_3 z)$ budeme nazývať projektívny uzáver eliptickej krivky E a budeme ju značiť E^*. Podľa tvrdenia 17 je E^* ireducibilná projektívna rovinná krivka. Množina všetkých bodov ležiacich na krivke E^* je práve projektívna algebraická množina $V(E^*)$ a podľa tvrdenia 13 to je projektívna varieta.

Poznámka. Uvažujme eliptickú krivku E nad $\mathbb{C}$ danú rovnicou

$$y^2 = (x - r_1)(x - r_2)(x - r_3)$$

a jej projektívny uzáver E^*. Pozrieme sa na body v nekonečne ležiace na E^*, teda na body $(x_0 : y_0 : 0) \in E^*$. Po dosadení bodu $(x_0 : y_0 : 0)$ do polynómu $y^2z - (x - r_1z)(x - r_2z)(x - r_3z)$ určujúceho projektívny uzáver E^*, dostaneme $0 = -x_0^3$. Takže x_0 musí byť rovné 0, a teda y_0 musí byť nenulové. Teda E^* má práve jeden bod v nekonečne a to bod $(0 : 1 : 0)$. Eliptickú krivku E budeme teda vždy uvažovať aj spolu s bodom v nekonečne, značíme ho O, ktorý odpovedá bodu $(0 : 1 : 0)$ na jej projektívnom uzávere E^*. Bod $(0 : 1 : 0)$ budeme značiť O^*.

Tvrdenie 23. *Eliptická krivka nad $\mathbb{C}$ je nesingulárna afinná rovinná krivka.*

Dôkaz. Uvažujme eliptickú krivku E danú polynómom $y^2 - x^3 - ax - b$. Pre spor predpokladajme, že na eliptickej krivke E existuje singulárny bod $P = (x_0, y_0)$. Pre bod P potom platí

$$0 = \frac{\partial E}{\partial x}(x_0, y_0) = -3x_0^2 - a, \tag{4.3}$$

$$0 = \frac{\partial E}{\partial y}(x_0, y_0) = 2y_0. \tag{4.4}$$

Z rovnice (4.4) vyplýva, že $y_0 = 0$, a z rovnice (4.3) vyplýva, že $x_0 = \pm\sqrt{-a/3}$. Aby bod $P = \left(0, \pm\sqrt{-a/3}\right)$ ležal na krivke E, musí splňovať

$$0^2 = \left(\pm\sqrt{-a/3}\right)^3 + a\left(\pm\sqrt{-a/3}\right) + b.$$

Úpravou tejto rovnice dostaneme $b = \mp 2/3a\sqrt{-a/3}$. Takže

$$0 \neq 4a^3 + 27b^2 = 4a^3 + 27\left(\mp 2/3a\sqrt{-a/3}\right)^2 = 4a^3 - 4a^3 = 0,$$

čo je spor. □

Lema 24. *Nech E je eliptická krivka nad $\mathbb{C}$ daná rovnicou $s^2 = (t-t_1)(t-t_2)(t-t_3)$ a nech O je jej bod v nekonečne. Potom $O_O(E)$ je DVR a platí*

$$v_O([s]_{\mathbb{C}[E]}) = -3,$$
$$v_O([t]_{\mathbb{C}[E]}) = -2.$$

Dôkaz. Množina všetkých bodov ležiacich na eliptickej krivke E je afinná algebraická množina $V(E) = V(s^2 - (t - t_1)(t - t_2)(t - t_3)) \subseteq \mathbb{C}^2$. Z tvrdenia 22 vieme, že $V(E)$ je afinná varieta, a z tvrdenia 7 máme, že ideál množiny $V(E)$ je rovný $I(E) = (s^2 - (t - t_1)(t - t_2)(t - t_3)) \leqslant \mathbb{C}[t, s]$. Teda súradnicový okruh $\mathbb{C}[E]$ neprázdnej afinnej variety $V(E)$ je rovný

$$\mathbb{C}[E] = \mathbb{C}[t, s]/(s^2 - (t - t_1)(t - t_2)(t - t_3)).$$

Odteraz budeme stotožňovať prvky $\mathbb{C}[t, s]$ s polynomiálnymi funkciami, ktoré určujú triedy ekvivalencie daných prvkov v $\mathbb{C}[E]$.

Uvažujme afinnú rovinnú krivku $\overline{E}$ danú polynómom $u-(t-t_1u)(t-t_2u)(t-t_3u)$. Ukážeme, že afinná algebraická množina

$$V(\overline{E}) = V(u-(t-t_1u)(t-t_2u)(t-t_3u)) \subseteq \mathbb{C}^2$$

je ireducibilná. Projektívna rovinná krivka $\overline{E}^*$ je krivka daná polynómom

$$s^2u-(t-t_1u)(t-t_2u)(t-t_3u).$$

Teda $\overline{E}^* = E^*$ a podľa druhej poznámky za tvrdením 22 je E^*, teda aj $\overline{E}^*$, ireducibilná projektívna rovinná krivka. Z tvrdenia 16 potom vyplýva, že afinná rovinná krivka $\overline{E}$ je ireducibilná. Teda z tvrdenia 7 je $V(\overline{E})$ afinná varieta.

Ďalej z tvrdenia 7 máme, že ideál množiny $V(\overline{E})$ je rovný

$$I(\overline{E}) = (u-(t-t_1u)(t-t_2u)(t-t_3u)) \leqslant \mathbb{C}[t,u].$$

Takže súradnicový okruh neprázdnej afinnej variety $V(\overline{E})$ je rovný

$$\mathbb{C}[\overline{E}] = \mathbb{C}[t,u]/(u-(t-t_1u)(t-t_2u)(t-t_3u)).$$

Rovnako aj tu budeme stotožňovať prvky $\mathbb{C}[t,u]$ s polynomiálnymi funkciami, ktoré určujú triedy ekvivalencie daných prvkov v $\mathbb{C}[\overline{E}]$.

Rovnako ako v druhej poznámke za tvrdením 22 vieme ukázať, že projektívny uzáver $V(\overline{E}^*)$ afinnej variety $V(\overline{E})$ je rovný

$$V(\overline{E}^*) = V(s^2u-(t-t_1u)(t-t_2u)(t-t_3u)) = V(E^*).$$

Z tvrdenia 14 dostávame $\mathbb{C}(E) \simeq \mathbb{C}(E^*) \simeq \mathbb{C}(\overline{E})$. Označme α_1, resp. α_2, izomorfizmus $\mathbb{C}(E^*) \simeq \mathbb{C}(E)$, resp. izomorfizmus $\mathbb{C}(E^*) \simeq \mathbb{C}(\overline{E})$, z tvrdenia 14. Potom funkcia $s/1 \in \mathbb{C}(E)$ odpovedá pri zobrazení α_1 funkcii $s/u \in \mathbb{C}(E^*)$, ktorá odpovedá pri zobrazení α_2 funkcii $1/u \in \mathbb{C}(\overline{E})$. Analogicky, funkcia $t/1 \in \mathbb{C}(E)$ odpovedá funkcii $t/u \in \mathbb{C}(E^*)$, ktorá odpovedá funkcii $t/u \in \mathbb{C}(\overline{E})$. Navyše bod O eliptickej krivky E odpovedá bodu $(0:1:0)$ jej projektívneho uzáveru E^*, a ten odpovedá bodu $(0,0)$ afinnej rovinnej krivky $\overline{E}$. Takže namiesto hľadania násobnosti pólov funkcií $s,t \in \mathbb{C}(E)$ v bode O, môžeme hľadať násobnosti pólov funkcií $1/u, t/u \in \mathbb{C}(\overline{E})$ v bode $(0,0)$.

Ukážeme, že lokálny okruh $O_{(0,0)}(\overline{E})$ afinnej variety $V(\overline{E})$ v bode $(0,0)$ je DVR. Z tvrdenia 9 a z poznámky pred ním vieme, že $O_{(0,0)}(\overline{E})$ je lokálny noetherovský obor, ktorý nie je poľom; stačí teda ukázať, že jeho jednoznačne určený maximálny ideál $M_{(0,0)}(\overline{E})$ je hlavný. Vieme, že racionálna funkcia $z = f/g \in O_{(0,0)}(\overline{E})$, kde $f,g \in \mathbb{C}[\overline{E}]$ a $g(0,0) \neq 0$, patrí do $M_{(0,0)}(\overline{E})$ práve vtedy, keď $z(0,0) = 0$, čo nastáva práve vtedy, keď $f(0,0) = 0$. Nech $F \in \mathbb{C}[t,u]$ je zástupca triedy ekvivalencie určenej polynomiálnou funkciou f vo faktorokruhu $\mathbb{C}[\overline{E}]$. Potom $F(0,0) = 0$ práve vtedy, keď $F \in I((0,0)) = (t,u) \leqslant \mathbb{C}[t,u]$. Teda $f(0,0) = 0$ práve vtedy, keď $f \in (t,u)/I(\overline{E})$. Označme $[F]_{\mathbb{C}[\overline{E}]}$ triedu ekvivalencie prvku F v $\mathbb{C}[\overline{E}]$. Potom $(t,u)/I(\overline{E}) = ([t]_{\mathbb{C}[\overline{E}]}, [u]_{\mathbb{C}[\overline{E}]})$. Takže $M_{(0,0)}(\overline{E}) = ([t]_{\mathbb{C}[\overline{E}]}, [u]_{\mathbb{C}[\overline{E}]})$. Teda pri stotožňovaní prvkov $\mathbb{C}[t,u]$ s polynomiálnymi funkciami, ktoré určujú ich triedy ekvivalencie v $\mathbb{C}[\overline{E}]$ platí $M_{(0,0)}(\overline{E}) = (t,u)$.

Ďalej v $O_{(0,0)}(\overline{E})$ platí

$$\begin{aligned}
u &= (t-t_1u)(t-t_2u)(t-t_3u),\\
u &= t^3 - t^2u(t_1+t_2+t_3) + tu^2(t_1t_2+t_1t_3+t_2t_3) - t_1t_2t_3u^3,\\
u + t_1t_2t_3u^3 &= t^3 - t^2u(t_1+t_2+t_3) + tu^2(t_1t_2+t_1t_3+t_2t_3),\\
u(1+t_1t_2t_3u^2) &= t(t^2 - tu(t_1+t_2+t_3) + u^2(t_1t_2+t_1t_3+t_2t_3)).
\end{aligned}$$

Keďže polynomiálna funkcia $(1 + t_1t_2t_3u^2)$ nie je rovná nule v bode $(0, 0)$, má v $O_{(0,0)}(\overline{E})$ inverz a platí

$$u = t\frac{(t^2 - tu(t_1 + t_2 + t_3) + u^2(t_1t_2 + t_1t_3 + t_2t_3))}{(1 + t_1t_2t_3u^2)} \in tO_{(0,0)}(\overline{E}).$$

Takže $M_{(0,0)}(\overline{E}) = (t, u) = (t)$. Teda ideál $M_{(0,0)}(\overline{E})$ je hlavný a $O_{(0,0)}(\overline{E})$ je DVR s uniformizačným parametrom t. Z poznámky za tvrdením 14 vyplýva, že $O_{(0,0)}(\overline{E}) \simeq O_{(0:1:0)}(E^*) \simeq O_O(E)$. Teda aj $O_O(E)$ je DVR.

Skúsime teraz vyjadriť funkcie $1/u, t/u$ pomocou uniformizačného parametru t. Platí

$$u + t^2u(t_1 + t_2 + t_3) - tu^2(t_1t_2 + t_1t_3 + t_2t_3) + t_1t_2t_3u^3 = t^3,$$
$$u(1 + t^2(t_1 + t_2 + t_3) - tu(t_1t_2 + t_1t_3 + t_2t_3) + t_1t_2t_3u^2) = t^3.$$

Keďže polynomiálna funkcia $(1 + t^2(t_1 + t_2 + t_3) - tu(t_1t_2 + t_1t_3 + t_2t_3) + t_1t_2t_3u^2)$ nie je rovná nule v bode $(0, 0)$, je to invertibilný prvok $O_{(0,0)}(\overline{E})$ a platí

$$1/u = t^{-3}(1 + t^2(t_1 + t_2 + t_3) - tu(t_1t_2 + t_1t_3 + t_2t_3) + t_1t_2t_3u^2),$$
$$t/u = t^{-2}(1 + t^2(t_1 + t_2 + t_3) - tu(t_1t_2 + t_1t_3 + t_2t_3) + t_1t_2t_3u^2).$$

Z toho dostávame, že $v_O^E(s) = v_{(0,0)}^{\overline{E}}(1/u) = -3$ a $v_O^E(t) = v_{(0,0)}^{\overline{E}}(t/u) = -2$. □

Tvrdenie 25. *Nech E je eliptická krivka nad $\mathbb{C}$ a E^* je jej projektívny uzáver. Potom E^* je nesingulárna projektívna rovinná krivka.*

Dôkaz. Najskôr uvažujme bod $P = (p_1 : p_2 : p_3) \in E^*$ taký, že $p_3 \neq 0$. Z tvrdenia 23 vieme, že bod $(p_1/p_3, p_2/p_3) \in E$ je nesingulárny bod E. Potom z tvrdenia 15 máme, že bod P je nesingulárny bod E^*.

Teraz uvažujme bod $O^* = (0 : 1 : 0) \in E^*$. Nech $\overline{E}$ je afinná rovinná krivka definovaná v dôkaze lemy 24. Z dôkazu lemy 24 vieme, že $\overline{E}$ je ireducibilná afinná rovinná krivka a $O_{(0,0)}(\overline{E})$ je DVR. Takže podľa tvrdenia 18 je bod (0,0) nesingulárny bod $\overline{E}$. Potom z tvrdenia 15 máme, že bod O^* je nesingulárny bod E^* (musíme uvažovať dehomogenizáciu podľa premennej s). □

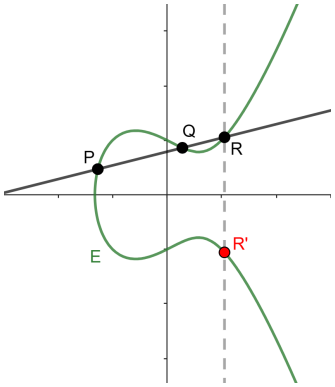
4.2 Grupová štruktúra eliptickej krivky

Teraz zavedieme operáciu sčítania na množine bodov projektívneho uzáveru eliptickej krivky a ukážeme, že body tohto projektívneho uzáveru spolu s touto operáciou sčítania tvoria grupu. Na všetkých obrázkoch súvisiacich s eliptickými krivkami sa pre lepšiu ilustráciu nachádzajú priamo eliptické krivky a nie ich projektívne uzávery. Všetky tieto obrázky sú nad $\mathbb{R}$.

Nech E je eliptická krivka nad $\mathbb{C}$ a E^* je jej projektívny uzáver. Nech

$$P = (p_1 : p_2 : 1),\ Q = (q_1 : q_2 : 1) \in V(E^*) \setminus \{O^*\}$$

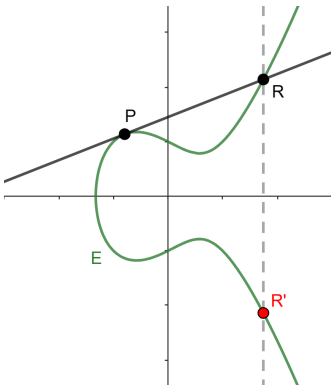
sú body na krivke E^*. Najskôr predpokladajme, že $p_1 \neq q_1$, teda máme situáciu ako na obrázku 4.1. Uvažujme projektívnu priamku l prechádzajúcu bodmi P, Q. Ako neskôr ukážeme, každá projektívna priamka v $\mathbb{P}(\mathbb{C}^2)$ sa až na násobnosť pretína s krivkou E^* v troch bodoch. Takže okrem bodov P, Q existuje ešte jeden



Obr. 4.1 Sčítanie bodov na eliptickej krivke v prípade, že $P \neq Q$.

bod v prieniku priamky l a krivky E^*; označme ho $R = (r_1 : r_2 : r_3)$. Bod R zobrazíme v osovej symetrii podľa projektívnej priamky $y = 0$ a dostaneme bod $R' = (r_1 : -r_2 : r_3)$. Súčet bodov P a Q definujeme ako bod $P \oplus Q = R'$.

Teraz predpokladajme, že $p_1 = q_1$ a $p_2 \neq q_2$. Potom položíme $P \oplus Q = O^*$. V prípade, že $P = Q$ a $p_2 \neq 0$, postupujeme rovnako ako v prvom prípade, ale tentokrát bude projektívna priamka l dotyčnica ku krivke E^* v bode P (viď obrázok 4.2). Pokiaľ $P = Q$ a $p_2 = 0$, položíme $P \oplus Q = O^*$.



Obr. 4.2 Sčítanie bodov na eliptickej krivke v prípade, že $P = Q$.

Nakoniec položíme $P \oplus O^* = P$, $O^* \oplus P = P$ a $O^* \oplus O^* = O^*$. Teda bod O^* sa správa ako neutrálny prvok vzhľadom ku sčítaniu.

Môžeme si všimnúť, že pokiaľ v afinnom prípade bod O uvažujeme ako jeden bod na obidvoch koncoch osi y a priamky prechádzajúce bodom O sú práve všetky zvislé priamky, tak všetky uvedené prípady odpovedajú tomu prvému.

Poznámka. Pre takto zadefinovanú operáciu $\oplus$ a pre ľubovoľné tri body P, Q, R na krivke E^*, ktoré ležia na jednej priamke, platí $(P \oplus Q) \oplus R = O^*$.

Zostáva nám ešte ukázať, že každá projektívna priamka a projektívny uzáver každej eliptickej krivky sa pretínajú v troch bodoch.

Lema 26. *Nech E je eliptická krivka nad $\mathbb{C}$ daná polynómom $y^2 - x^3 - ax - b$ a E^* je jej projektívny uzáver. Nech $l\colon ex + fy + gz$ je projektívna priamka v $\mathbb{P}^2(\mathbb{C})$. Potom priamka l a krivka E^* sa až na násobnosť pretínajú v troch bodoch.*

Dôkaz. Projektívna rovinná krivka E^* je určená polynómom $y^2z - x^3 - axz^2 - bz^3$.

Bod $O^* = (0 : 1 : 0) \in E^*$ leží na priamke l práve vtedy, keď

$$0 = e \cdot 0 + f \cdot 1 + g \cdot 0 = f.$$

Najskôr predpokladajme, že bod O^* neleží v prieniku l a E^*, teda $f \neq 0$. Platí, že bod $P = (p_1 : p_2 : p_3) \in \mathbb{P}^2(\mathbb{C})$, $p_3 \neq 0$, leží v prieniku l a E^* práve vtedy, keď bod $P_* = (p_1/p_3, p_2/p_3)$ leží v prieniku $l_*\colon ex + fy + g$ a E. Stačí nám teda zistiť veľkosť prieniku priamky l_* a krivky E. Pre bod (x, y) na priamke l_* platí

$$ex + fy + g = 0, \tag{4.5}$$
$$y = -f^{-1}(ex + g). \tag{4.6}$$

Výraz v (4.6) dosadíme do polynómu určujúceho krivku E a dostaneme kubický polynóm v premennej x

$$\left(-f^{-1}(ex + g)\right)^2 - x^3 - ax - b. \tag{4.7}$$

Zo základnej vety algebry vieme, že polynóm (4.7) má práve tri korene až na násobnosť. Takže v prieniku priamky l_* a krivky E, a teda aj v prieniku priamky l a krivky E^*, ležia práve tri body až na násobnosť.

Teraz predpokladajme, že bod O^* leží v prieniku l a E^*. Potom $f = 0$, teda priamka l je rovná $ex + gz$. Pokiaľ $e \neq 0$, pre bod $(x : y : z)$ na priamke l platí

$$ex + gz = 0, \tag{4.8}$$
$$x = -e^{-1}gz. \tag{4.9}$$

Výraz v (4.9) dosadíme do polynómu určujúceho krivku E^* a dostaneme

$$y^2z - (-e^{-1}g)^3z^3 - a(-e^{-1}g)z^3 - bz^3 = 0,$$
$$z(y^2 - (-e^{-1}g)^3z^2 - a(-e^{-1}g)z^2 - bz^2) = 0.$$

Takže máme dve možnosti. Prvá možnosť je, že $z = 0$. Potom zo (4.9) platí $x = 0$, a teda y už musí byť nenulové. Dostávame bod $(0 : 1 : 0)$. Druhá možnosť je, že

$$y = \pm\sqrt{(-e^{-1}g)^3z^2 + a(-e^{-1}g)z^2 + bz^2} = \pm z\sqrt{(-e^{-1}g)^3 + a(-e^{-1}g) + b},$$

teda dostávame body $(-e^{-1}g : \pm\sqrt{(-e^{-1}g)^3 + a(-e^{-1}g) + b} : 1)$. Dokopy v prieniku l a E^* teda ležia tri body.

Nakoniec vyriešime prípad, keď $f = 0$ a $e = 0$. Potom $g \neq 0$ a pre bod $(x : y : z)$ na priamke l platí $gz = 0$, teda $z = 0$. Dosadením do polynómu určujúceho krivku E^* dostávame $0 = -x^3$. Kubický polynóm x^3 má trojnásobnú nulu v bode 0, teda y už musí byť nenulové. Priamka l a krivka E^* majú teda trojnásobný prienik v bode O^*. □

Poznámka. Lema 26 je špeciálnym prípadom Bézoutovej vety (Fulton [1, Kapitola 5.3]).

Overenie toho, že takto zadefinovaná operácia sčítania $\oplus$ na množine bodov projektívneho uzáveru eliptickej krivky má naozaj vlastnosti grupovej operácie, nie je jednoduché. Najväčším problémom je overenie asociativity. V tejto práci nebudeme z definície overovať, že operácia $\oplus$ je grupovou operáciou. Namiesto toho uvedieme inú definíciu grupovej štruktúry na projektívnom uzávere eliptickej krivky a ukážeme, že tieto dve grupové štruktúry si odpovedajú.

Poznámka. Projektívny uzáver E^* eliptickej krivky E je nesingulárna ireducibilná projektívna rovinná krivka, takže následujúca definícia má zmysel.

Definícia 38. *Nech E je eliptická krivka nad $\mathbb{C}$ a E^* je jej projektívny uzáver.* Grupu projektívneho uzáveru eliptickej krivky E *definujeme ako faktorgrupu*

$$\mathrm{Cl}_0(E^*) := \frac{\mathrm{Div}_0(E^*)}{\mathrm{PDiv}(E^*)}.$$

Tvrdenie 27. *Nech E je eliptická krivka nad $\mathbb{C}$ a E^* je jej projektívny uzáver. Označme O^* bod $(0:1:0) \in E^*$. Potom zobrazenie*

$$\begin{aligned} \varphi\colon E^* &\to \mathrm{Cl}_0(E^*) \\ P &\mapsto [P - O^*]_{\mathrm{Cl}_0(E^*)} \end{aligned}$$

je bijekcia.

Dôkaz. Nech E je eliptická krivka daná polynómom $s^2 - (t-t_1)(t-t_2)(t-t_3)$. Kvôli jednoduchšiemu zápisu budeme triedu ekvivalencie prvku $D \in \mathrm{Div}_0(E^*)$ vo faktorgrupe $\mathrm{Cl}_0(E^*)$ značiť $[D]$ namiesto $[D]_{\mathrm{Cl}_0(E^*)}$.

Uvažujme projektívnu priamku $l\colon et + fs + gu$ a označme P, Q, R tri body, ktoré ležia v prieniku priamky l a krivky E^*. Z lemy 26 vieme, že prienik l a E^* obsahuje práve tri body až na násobnosť. Platí $l(P) = l(Q) = l(R) = 0$. Priamku l budeme uvažovať ako prvok $\mathbb{C}_h[E^*]$. Potom l/u je racionálna funkcia na $V(E^*)$. Vieme, že racionálna funkcia $f \in \mathbb{C}(E^*)$ má v bode $A \in E^*$ nulu práve vtedy, keď $v_A(f) > 0$. Čo nastáva práve vtedy, keď $f \in M_A(E^*)$, teda práve vtedy, keď funkcia f je definovaná v bode A a platí $f(A) = 0$. Vidíme, že racionálna funkcia l/u je definovaná na množine $V(E^*) \setminus \{O^*\}$. Postupne rozoberieme všetky tri možnosti pre body P, Q, R v prieniku l a E^* z dôkazu lemy 26:

(1) Predpokladajme, že $P, Q, R \in V(E^*) \setminus \{O^*\}$. Potom je funkcia l/u definovaná vo všetkých troch bodoch P, Q, R a platí

$$(l/u)(P) = (l/u)(Q) = (l/u)(R) = 0.$$

Zároveň z lemy 26 vieme, že v prieniku l a E^* ležia práve tri body (až na násobnosť), teda funkcia l/u žiadne iné nuly nemá. Z tvrdenia 20 vieme, že funkcia l/u musí mať až na násobnosť rovnaký počet núl a pólov. Keďže je funkcia l/u definovaná vo všetkých bodoch množiny $V(E^*) \setminus \{O^*\}$, pól môže mať jedine v bode O^*. Z tvrdenia 20 teda vyplýva, že funkcia l/u má v bode O^* pól násobnosti 3. Takže hlavný divizor funkcie l/u je rovný $(l/u) = P + Q + R - 3O^*$.

(2) Predpokladajme, že jeden z bodov P, Q, R je bod O^*; bez ujmy na všeobecnosti nech je to bod R. Potom z dôkazu lemy 26 vieme, že priamka l je rovná $et + gu$, kde $e \neq 0$. Takže racionálna funkcia l/u je rovná $e(t/u) + g$. Z dôkazu lemy 24 a z poznámky za tvrdením 14 platí, že valuácia funkcie t/u v bode O^* je -2. Takže z tvrdenia 1 a 2 platí $v_{O^*}(l/u) = v_{O^*}(e(t/u)+g) = -2$. V bodoch P, Q je funkcia l/u definovaná a platí $(l/u)(P) = (l/u)(Q) = 0$. Z lemy 26 vieme, že žiadne iné nuly funkcia l/u nemá. Takže hlavný divizor funkcie l/u je rovný $(l/u) = P + Q - 2O^*$.

(3) Predpokladajme, že $P = Q = R = O^*$. Potom z dôkazu lemy 26 vieme, že priamka l je rovná gu, kde $g \neq 0$. Teda racionálna funkcia l/u je rovná nenulovej konštante g a platí, že hlavný divizor funkcie l/u je nulový divizor.

Uvažujme bod $O^* \neq A = (a_1 : a_2 : a_3) \in E^*$ a projektívnu priamku m prechádzajúcu bodmi A a O^*. Z dôkazu lemy 26 vieme, že tretí bod v prieniku m a E^* je bod $A' = (a_1 : -a_2 : a_3)$. Pre ľubovoľný bod $A = (a_1 : a_2 : a_3) \in E^*$ teda platí, že body $A, A' = (a_1 : -a_2 : a_3)$ a O^* ležia na jednej projektívnej priamke.

Teraz už vieme ukázať, že zobrazenie φ je na. Nech

$$O^* \neq P = (p_1 : p_2 : 1), Q = (q_1 : q_2 : 1) \in E^*,$$

l je projektívna priamka prechádzajúca bodmi P, Q a R je tretí bod v prieniku priamky l a krivky E^*. Pokiaľ $R = O^*$, platí $Q = (p_1 : -p_2 : 1) =: P'$ a máme hlavný divizor $P + P' - 2O^*$. Vo faktorgrupe $\mathrm{Cl}(E^*) = \mathrm{Div}(E^*)/\mathrm{PDiv}(E^*)$ potom platí

$$\begin{aligned} [P + P' - 2O^*] &= 0_{\mathrm{Cl}(E^*)}, \\ [-P] &= [P'] - [2O^*]. \end{aligned} \tag{4.10}$$

Pokiaľ $O^* \neq R = (r_1 : r_2 : 1) \in E^*$, máme hlavný divizor $P + Q + R - 3O^*$. Označme R' bod $(r_1 : -r_2 : 1)$. Vo faktorgrupe $\mathrm{Cl}(E^*) = \mathrm{Div}(E^*)/\mathrm{PDiv}(E^*)$ potom platí

$$\begin{aligned} [P + Q + R - 3O^*] &= 0_{\mathrm{Cl}(E^*)}, \\ [P + Q] &= [-R] + [3O^*] = [R'] - [2O^*] + [3O^*] = [R'] + [O^*], \end{aligned} \tag{4.11}$$

kde v druhej rovnosti sme využili (4.10).

Zo (4.10) a (4.11) vyplýva, že každý prvok $\sum_{P_i \in E^*} n_i[P_i] \in \mathrm{Cl}_0(E^*) \subseteq \mathrm{Cl}(E^*)$ sa dá vyjadriť v tvare $[R'] + k[O^*]$ pre vhodné $R' \in E^*$ a $k \in \mathbb{Z}$. Pre prvky z $\mathrm{Cl}_0(E^*)$ musí byť ale $k = -1$. Takže každý prvok z $\mathrm{Cl}_0(E^*)$ sa dá vyjadriť v tvare $[R'] - [O^*]$, a teda zobrazenie φ je na.

Teraz ukážeme, že zobrazenie φ je prosté. Pre spor predpokladajme, že existujú dva rôzne body $P, Q \in E^*$ také, že $[P - O^*] = [Q - O^*]$. Potom platí $[P - Q] = 0_{\mathrm{Cl}_0(E^*)}$. Navyše vieme, že $[P - Q] = [R' - O^*]$ pre vhodné $R' \in E^*$, takže máme

$$[R' - O^*] = [P - Q] = 0_{\mathrm{Cl}_0(E^*)}.$$

Z toho vyplýva, že $(R' - O^*) \in \mathrm{PDiv}(E^*)$, teda existuje racionálna funkcia $f \in \mathbb{C}(E^*)$ spĺňajúca $(f) = R' - O^*$. Ukážeme, že takáto funkcia existovať nemôže.

Uvažujme divizor $A = O^* \in \mathrm{Div}(E^*)$ a Riemann-Rochov priestor $\mathscr{L}(A)$. Z tvrdenia 14 vieme, že $\mathbb{C}(E) \simeq \mathbb{C}(E^*)$. Môžeme teda pomocou izomorfizmu α z tvrdenia 14 stotožniť množinu $\mathscr{L}(A)$ s množinou

$$L := \{0\} \cup \{0 \neq g \in \mathbb{C}(E) \mid v_O(g) \geq -1 \text{ a } v_P(g) \geq 0 \; \forall P \in E\}.$$

Keďže všetky prvky L sú definované v každom bode eliptickej krivky E (okrem bodu O), podľa tvrdenia 8 sú prvky L polynomiálne funkcie na $V(E)$. Už vieme, že súradnicový okruh neprázdnej afinnej variety $V(E)$ je rovný

$$\mathbb{C}[E] = \mathbb{C}[t, s]/(s^2 - (t - t_1)(t - t_2)(t - t_3)).$$

Opäť budeme stotožňovať prvky $\mathbb{C}[t,s]$ s polynomiálnymi funkciami, ktoré určujú triedy ekvivalencie daných prvkov v $\mathbb{C}[E]$. V $\mathbb{C}[E]$ platí $s^2=(t-t_1)(t-t_2)(t-t_3)$, a preto je každá polynomiálna funkcia na $V(E)$ konečnou lineárnou kombináciou polynomiálnych funkcií $\{t^i, st^i \mid i \geq 0\}$ s koeficientami v $\mathbb{C}$. Navyše z lemy 24 vieme, že $v_O(s)=-3$ a $v_O(t)=-2$, teda podľa tvrdenia 1 platí $v_O(t^i)=-2i$ a $v_O(st^i)=-3-2i$. Z toho môžeme vidieť, že funkcie $t^i, st^i, i\geq 0$ majú po dvoch rôzne valuácie v bode O. Uvažujme nenulovú polynomiálnu funkciu

$$g=c_0+c_1t+c_2s+c_3t^2+c_4st+\cdots+c_{2i+1}t^{i+1}+c_{2i+2}st^i+\ldots$$

Keďže všetky nenulové členy v tejto lineárnej kombinácii majú po dvoch rôzne nekladné valuácie v bode O, valuácia funkcie g v bode O je podľa tvrdenia 2 rovná valuácii členu s koeficientom c_k, kde $k=\max(j \mid c_j \neq 0)$. Tento člen ma totižto najmenšiu valuáciu v bode O. Pokiaľ $g\in L$, tak $v_O(g)\geq -1$. Takže valuácia členu s koeficientom c_k musí byť ≥ -1. Musí teda platiť $k=0$, lebo všetky ďalšie členy majú v bode O valuáciu ostro menšiu ako -1. To znamená, že L obsahuje len konštantné polynomiálne funkcie. Teda aj $\mathscr{L}(A)$ obsahuje len konštantné funkcie, a tie majú v bode O^* valuáciu rovnú 0. Teda neexistuje racionálna funkcia na $V(E^*)$, ktorá by mala jediný pól v bode O^* násobnosti 1. Takže $(R'-O^*)$ nemôže byť hlavný divizor, čo je spor. Z toho vyplýva, že zobrazenie φ je prosté. □

Pomocou bijekcie φ z tvrdenia 27 môžeme preniesť grupovú štruktúru faktorgrupy $\mathrm{Cl}_0(E^*)$ na množinu $V(E^*)$ všetkých bodov ležiacich na projektívnom uzávere E^* eliptickej krivky E. Pre body $P,Q\in V(E^*)$ definujeme

$$\begin{aligned} P+Q &:= \varphi^{-1}(\varphi(P)+\varphi(Q)),\\ -P &:= \varphi^{-1}(-\varphi(P)),\\ 0 &:= \varphi^{-1}(0_{\mathrm{Cl}_0(E^*)})=O^*. \end{aligned}$$

Rozmyslíme si, že táto prenesená operácia sčítania odpovedá operácii $\oplus$ zavedenej na začiatku tejto podkapitoly.

Nech

$$P=(p_1:p_2:1),\ Q=(q_1:q_2:1)\in V(E^*)\setminus\{O^*\},$$

kde $p_1\neq q_1$, a l je projektívna priamka prechádzajúca bodmi P,Q. Nech R je tretí bod v prieniku priamky l a krivky E^*. Keďže $Q\neq(p_1:-p_2:1)$, z dôkazu lemy 26 vieme, že $R\neq O^*$, teda $R=(r_1:r_2:1)$. Označme R' bod $(r_1:-r_2:1)$. Potom platí

$$\begin{aligned} P+Q &= \varphi^{-1}(\varphi(P)+\varphi(Q))=\varphi^{-1}([P-O^*]+[Q-O^*])=\\ &= \varphi^{-1}([P+Q-2O^*])=\varphi^{-1}([R'+O^*-2O^*])=\\ &= \varphi^{-1}([R'-O^*])=R'=P\oplus Q, \end{aligned}$$

kde vo štvrtej rovnosti sme použili (4.11). Pokiaľ $Q=P=(p_1:p_2:1)$ a $p_2\neq 0$, postupujeme rovnako.

V prípade, že $p_1=q_1$ a $p_2\neq q_2$, už musí z definície eliptickej krivky nutne platiť $p_2=-q_2$. Teda $Q=(p_1:-p_2:1)=:P'$ a $R=O^*$. Potom platí

$$\begin{aligned} P+Q=P+P' &= \varphi^{-1}(\varphi(P)+\varphi(P'))=\varphi^{-1}([P-O^*]+[P'-O^*])=\\ &= \varphi^{-1}([P+P'-2O^*])=\varphi^{-1}([P-P])=\varphi^{-1}(0_{\mathrm{Cl}_0(E^*)})=O^*=P\oplus Q, \end{aligned}$$

kde v piatej rovnosti sme použili (4.10). Pokiaľ $Q = P = (p_1 : p_2 : 1)$ a $p_2 = 0$, postupujeme rovnako. V prípade prenesenej operácie sčítania aj operácie $\oplus$ sa bod O^* správa ako neutrálny prvok.

Takže prenesená operácia sčítania naozaj odpovedá operácii $\oplus$. Tým sme ukázali, že operácia $\oplus$ je skutočne grupová operácia a množina všetkých bodov projektívneho uzáveru eliptickej krivky spolu s operáciou $\oplus$ tvorí grupu.

5 Cayleyovo kritérium

V tejto kapitole formulujeme a dokážeme Cayleyovo kritérium pre rád bodu na eliptickej krivke. Pre eliptickú krivku E danú rovnicou $s^2 = (t - t_1)(t - t_2)(t - t_3)$ budeme opäť stotožňovať prvky $\mathbb{C}[t, s]$ s polynomiálnymi funkciami na $V(E)$, ktoré určujú triedy ekvivalencie daných prvkov v $\mathbb{C}[E]$. Táto kapitola vychádza z článku O. Nasha [2].

Cayleyovo kritérium je dôsledkom následujúceho tvrdenia.

Tvrdenie 28. *Nech E je eliptická krivka nad $\mathbb{C}$ daná rovnicou*

$$s^2 = (t - t_1)(t - t_2)(t - t_3),$$

kde $t_1, t_2, t_3 \neq 0$, a označme O jej bod v nekonečne. Nech $(t, s) = (0, a_0) \in \mathbb{C}^2$ je bod ležiaci na eliptickej krivke E a $n \in \mathbb{N}, n \geq 3$. Uvažujme rozvoj prvku s do mocninového radu

$$s = \sum_{i=0}^{\infty} \lambda_i t^i.$$

Potom racionálna funkcia $f \in \mathbb{C}(E)$, ktorá má v bode $(0, a_0)$ nulu násobnosti n, v bode O pól násobnosti n a nemá žiadne iné nuly ani póly, existuje práve vtedy, keď platí

$$\begin{vmatrix} \lambda_2 & \dots & \lambda_{p+1} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \lambda_{p+1} & \dots & \lambda_{2p} \end{vmatrix} = 0, \text{ pokiaľ } n = 2p + 1, \text{ kde } p \in \mathbb{N}, \text{ alebo}$$

$$\begin{vmatrix} \lambda_3 & \dots & \lambda_{p+1} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \lambda_{p+1} & \dots & \lambda_{2p-1} \end{vmatrix} = 0, \text{ pokiaľ } n = 2p, \text{kde } p \in \mathbb{N}, p \geq 2.$$

Najskôr však potrebujeme ukázať existenciu rozvoja prvku s do mocninového radu.

Lema 29. *Nech E je eliptická krivka nad $\mathbb{C}$ daná rovnicou $s^2 = (t-t_1)(t-t_2)(t-t_3)$, kde $t_1, t_2, t_3 \neq 0$. Nech $(t, s) = (0, a_0) \in \mathbb{C}^2$ je bod ležiaci na eliptickej krivke E. Potom $O_{(0,a_0)}(E)$ je diskrétny valuačný okruh s uniformizačným parametrom t a existujú $\lambda_0, \lambda_1, \ldots \in \mathbb{C}$ také, že*

$$s = \sum_{i=0}^{\infty} \lambda_i t^i.$$

Dôkaz. Množina všetkých bodov ležiacich na eliptickej krivke E je množina $V(E) = V(s^2 - (t - t_1)(t - t_2)(t - t_3)) \subseteq \mathbb{C}^2$. Z tvrdenia 22 vieme, že $V(E)$ je afinná varieta, a z tvrdenia 7 máme, že ideál množiny $V(E)$ je rovný

$$I(E) = (s^2 - (t - t_1)(t - t_2)(t - t_3)) \leqslant \mathbb{C}[t, s].$$

Teda súradnicový okruh $\mathbb{C}[E]$ neprázdnej afinnej variety $V(E)$ je rovný

$$\mathbb{C}[E] = \mathbb{C}[t, s]/(s^2 - (t - t_1)(t - t_2)(t - t_3)).$$

Pozrime sa na bod $(t,s) = (0,a_0) \in E$. Po dosadení 0 za t v rovnici určujúcej eliptickú krivku E dostaneme $s^2 = -t_1t_2t_3$, takže $s = \pm\sqrt{-t_1t_2t_3}$. Bez ujmy na všeobecnosti môžeme položiť $a_0 = +\sqrt{-t_1t_2t_3}$. Zjavne $a_0 \neq 0$.

Z tvrdenia 9 a z poznámky pred ním vieme, že $O_{(0,a_0)}(E)$ je lokálny noetherovský obor, ktorý nie je poľom. Stačí teda ukázať, že jeho jednoznačne určený maximálny ideál $M_{(0,a_0)}(E)$ je hlavný. Rovnako ako v dôkaze lemy 24 ukážeme, že $M_{(0,a_0)}(E) = (t, s-a_0)$. V okruhu $\mathbb{C}[E]$ ďalej platí

$$\begin{aligned} 0 &= s^2 - (t-t_1)(t-t_2)(t-t_3) = \\ &= s^2 - t^3 + t^2(t_1+t_2+t_3) - t(t_1t_2+t_1t_3+t_2t_3) + t_1t_2t_3 \end{aligned}$$

a $(s-a_0)(s+a_0) = s^2 + t_1t_2t_3$. Takže

$$\begin{aligned} (s-a_0)(s+a_0) &= t^3 - t^2(t_1+t_2+t_3) + t(t_1t_2+t_1t_3+t_2t_3) = \\ &= t(t^2 - t(t_1+t_2+t_3) + (t_1t_2+t_1t_3+t_2t_3)). \end{aligned}$$

Keďže $a_0 \neq 0$, je polynóm $s+a_0$ nenulový v bode $(0,a_0)$. Teda polynóm $s+a_0$ je invertibilný prvok $O_{(0,a_0)}(E)$ a platí

$$s - a_0 = t\frac{t^2 - t(t_1+t_2+t_3) + (t_1t_2+t_1t_3+t_2t_3)}{s+a_0} \in tO_{(0,a_0)}(E).$$

Teda $M_{(0,a_0)}(E) = (t, s-a_0) = (t)$ a ideál $M_{(0,a_0)}(E)$ je hlavný. Ukázali sme, že $O_{(0,a_0)}(E)$ je DVR s uniformizačným parametrom t.

Uvažujme vnorenie $\mathbb{C} \hookrightarrow O_{(0,a_0)}(E)$ a kanonickú projekciu

$$O_{(0,a_0)}(E) \twoheadrightarrow O_{(0,a_0)}(E)/M_{(0,a_0)}(E).$$

Z poznámky nad tvrdením 9 máme, že

$$\mathbb{C} \simeq O_{(0,a_0)}(E)/M_{(0,a_0)}(E).$$

Takže zobrazenie $\mathbb{C} \hookrightarrow O_{(0,a_0)}(E) \twoheadrightarrow O_{(0,a_0)}(E)/M_{(0,a_0)}(E)$ je izomorfizmus a sú splnené predpoklady tvrdenia 3. Z toho vyplýva, že každý prvok $O_{(0,a_0)}(E)$ vieme rozvinúť do mocninového radu. Špeciálne, vieme rozviesť prvok s do mocninového radu $s = \sum_{i=0}^{\infty} \lambda_i t^i$. □

Teraz už môžeme dokázať tvrdenie 28.

Dôkaz. Rovnako ako v predchádzajúcej leme 29 máme neprázdnú afinnú varietu $V(E) = V(s^2 - (t-t_1)(t-t_2)(t-t_3)) \subseteq \mathbb{C}^2$ a jej súradnicový okruh

$$\mathbb{C}[E] = \mathbb{C}[t,s]/(s^2 - (t-t_1)(t-t_2)(t-t_3)).$$

Opäť bez ujmy na všeobecnosti môžeme položiť $a_0 = +\sqrt{-t_1t_2t_3}$. Postupne dokážeme obidve implikácie.

$\Longleftarrow$ Predpokladajme najskôr, že $n = 2p+1$, kde $p \in \mathbb{N}$. Pre každé $i \in \{1,\ldots,p\}$ položíme polynomiálnu funkciu

$$f_i = t^{p-i}(s - \lambda_0 - \lambda_1 t - \ldots - \lambda_i t^i).$$

Dostaneme

$$\begin{aligned}
f_1 &= t^{p-1}(s-\lambda_0-\lambda_1 t) = t^{p-1}(\lambda_2 t^2+\lambda_3 t^3+\dots) = \lambda_2 t^{p+1}+\lambda_3 t^{p+2}+\dots,\\
f_2 &= t^{p-2}(s-\lambda_0-\lambda_1 t-\lambda_2 t^2) = t^{p-2}(\lambda_3 t^3+\lambda_4 t^4+\dots) = \lambda_3 t^{p+1}+\lambda_4 t^{p+2}+\dots,\\
&\vdots\\
f_p &= t^{p-p}(s-\lambda_0-\lambda_1 t-\dots-\lambda_p t^p) = \lambda_{p+1} t^{p+1}+\lambda_{p+2} t^{p+2}+\dots,
\end{aligned}$$

teda

$$\begin{aligned}
f_1 &= \lambda_2 t^{p+1}+\lambda_3 t^{p+2}+\dots+\lambda_{p+1} t^{2p}+\dots,\\
f_2 &= \lambda_3 t^{p+1}+\lambda_4 t^{p+2}+\dots+\lambda_{p+2} t^{2p}+\dots,\\
&\vdots\\
f_p &= \lambda_{p+1} t^{p+1}+\lambda_{p+2} t^{p+2}+\dots+\lambda_{2p} t^{2p}+\dots.
\end{aligned} \tag{5.1}$$

Predpokladáme, že

$$\begin{vmatrix} \lambda_2 & \dots & \lambda_{p+1} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \lambda_{p+1} & \dots & \lambda_{2p} \end{vmatrix} = 0.$$

Teda táto matica je singulárna a jej riadky sú lineárne závislé vektory. Takže existujú skaláry $c_1,\dots,c_p \in \mathbb{C}$, aspoň jeden z nich nenulový, také, že

$$0 = c_1(\lambda_2,\dots,\lambda_{p+1}) + c_2(\lambda_3,\dots,\lambda_{p+2}) + \dots + c_p(\lambda_{p+1},\dots,\lambda_{2p}).$$

Položíme polynomiálnu funkciu $f = c_1 f_1 + c_2 f_2 + \dots + c_p f_p \in \mathbb{C}[E]$. Platí

$$\begin{aligned}
f &= (c_1\lambda_{p+2}+c_2\lambda_{p+3}+\dots+c_p\lambda_{2p+1})t^{2p+1}+\\
&\qquad +(c_1\lambda_{p+3}+c_2\lambda_{p+4}+\dots+c_p\lambda_{2p+2})t^{2p+2}+\dots =\\
&= t^{2p+1}(c_1\lambda_{p+2}+c_2\lambda_{p+3}+\dots+c_p\lambda_{2p+1}+\\
&\qquad +(c_1\lambda_{p+3}+c_2\lambda_{p+4}+\dots+c_p\lambda_{2p+2})t+\dots).
\end{aligned}$$

Keďže $O_{(0,a_0)}(E)$ je DVR s uniformizačným parametrom t, tak $v_{(0,a_0)}(f) \geq 2p+1$. Vieme teda, že funkcia f má v bode $(0,a_0)$ nulu násobnosti aspoň $2p+1$.

Pozrieme sa teraz na valuáciu funkcie f v bode O. K tomu budeme potrebovať zistiť valuácie jednotlivých funkcií $f_i, i \in \{1,\dots,p\}$ v bode O. Z lemy 24 vieme, že $v_O(s) = -3$ a $v_O(t) = -2$. Navyše polynomiálne funkcie $t, s \in \mathbb{C}[E] = \cap_{P\in E} O_P(E)$ sú definované v každom bode $P \in E$, teda v žiadnom z týchto bodov nemôžu mať pól. Takže funkcia t má jediný pól v bode O násobnosti 2 a funkcia s má jediný pól v bode O násobnosti 3. S týmito informáciami už vieme spočítať valuácie jednotlivých funkcií $f_i, i \in \{1,\dots,p\}$ v bode O.

Pre $i = 1$ máme $f_1 = t^{p-1}(s-\lambda_0-\lambda_1 t)$. Pokiaľ $\lambda_0, \lambda_1 \neq 0$, z tvrdenia 1 platí:

$$\begin{aligned}
v_O(t^{p-1}s) &= v_O(t^{p-1}) + v_O(s) = (p-1)v_O(t) + v_O(s) = -2p-1,\\
v_O(t^{p-1}\lambda_0) &= (p-1)v_O(t) + v_O(\lambda_0) = (p-1)(-2)+0 = -2p+2,\\
v_O(t^p\lambda_1) &= p\cdot v_O(t) + v_O(\lambda_1) = p(-2)+0 = -2p.
\end{aligned}$$

Konštanty λ_0, λ_1 nemusia byť nutne nenulové. Avšak v každom prípade, bude mať člen $t^{p-1}s$ najmenšiu valuáciu v bode O. Takže podľa tvrdenia 2 platí

$$v_O(f_1) = v_O(t^{p-1}s - t^{p-1}\lambda_0 - t^p\lambda_1) = -2p-1.$$

Teda pokiaľ $c_1 \neq 0$, dostávame

$$v_O(c_1 f_1) = v_O(c_1) + v_O(f_1) = -2p - 1.$$

Ďalej pre $i > 1$ máme $f_i = t^{p-i}(s - \lambda_0 - \lambda_1 t - \ldots - \lambda_i t^i)$. Pokiaľ $\lambda_0, \ldots, \lambda_i \neq 0$, platí:

$$\begin{aligned}
&v_O(t^{p-i}s) = v_O(t^{p-i}) + v_O(s) = (p-i)v_O(t) + v_O(s) = -2p + 2i - 3,\\
&v_O(t^{p-i}\lambda_0) = (p-i)v_O(t) + v_O(\lambda_0) = -2p + 2i,\\
&v_O(t^{p-i+1}\lambda_1) = (p-i+1)v_O(t) + v_O(\lambda_1) = -2p + 2i - 2,\\
&\vdots\\
&v_O(t^p\lambda_i) = p \cdot v_O(t) + v_O(\lambda_i) = -2p.
\end{aligned}$$

Avšak konštanty $\lambda_0, \ldots, \lambda_i$ nemusia byť nutne nenulové. Takže platí

$$\begin{aligned}
v_O(f_i) &= v_O(t^{p-i}s - t^{p-i}\lambda_0 - t^{p-i+1}\lambda_1 - \ldots - t^p\lambda_i)\\
&\geq \min(-2p + 2i - 3, -2p + 2i, \ldots, -2p) = -2p.
\end{aligned}$$

Teda pokiaľ $c_i \neq 0$, platí

$$v_O(c_i f_i) = v_O(c_i) + v_O(f_i) \geq -2p.$$

Dokopy dostávame

$$v_O(f) = v_O(c_1 f_1 + c_2 f_2 + \cdots + c_p f_p) \geq \min(-2p - 1, -2p) = -2p - 1,$$

čiže funkcia f môže mať v bode O pól násobnosti najviac $2p+1$. Navyše $f \in \mathbb{C}[E] = \cap_{P \in E} O_P(E)$ je polynomiálna funkcia, teda je definovaná v každom bode $P \in E$ a v žiadnom z týchto bodov nemôže mať pól. Teda funkcia f môže mať len jeden pól, a to v bode O.

Nech E^* je projektívny uzáver eliptickej krivky E. Z tvrdenia 20 vieme, že každá nenulová racionálna funkcia z $\mathbb{C}(E^*)$ má rovnaký počet núl a pólov až na násobnosť. Podľa tvrdenia 14 a poznámky za ním platí, že $\mathbb{C}(E^*) \simeq \mathbb{C}(E)$ a $O_P(E^*) \simeq O_{P_*}(E)$ pre všetky body $P = (p_1 : p_2 : p_3) \in E^*, P_* = (p_1/p_3, p_2/p_3)$, kde $p_3 \neq 0$. Takže pokiaľ eliptickú krivku E uvažujeme aj spolu s bodom O odpovedajúcemu bodu $(0 : 1 : 0) \in E^*$, platí, že každá nenulová racionálna funkcia z $\mathbb{C}(E)$ má rovnaký počet núl a pólov až na násobnosť. Keďže racionálna funkcia f má v bode $(0, a_0)$ nulu násobnosti aspoň $2p + 1$ a nemá žiadny iný pól mimo bodu O, musí mať v bode O pól násobnosti $2p + 1$. Teda v bode $(0, a_0)$ musí mať funkcia f nulu násobnosti $2p + 1$ a žiadnu inú nulu funkcia f nemôže mať.

V prípade $n = 2p$, kde $p \in \mathbb{N}, p \geq 2$, zadefinujeme funkcie $f_i, i \in \{1, \ldots, p-1\}$ nasledovne

$$f_i = t^{p-i-1}(s - \lambda_0 - \lambda_1 t - \ldots - \lambda_{i+1} t^{i+1}).$$

Inak postupujeme analogicky ako v prípade $n = 2p + 1$.

$\Longrightarrow$ Najskôr predpokladajme, že $n = 2p + 1$, kde $p \in \mathbb{N}$. Označme P bod $(0 : a_0 : 1) \in E^*$ a ďalej označme O^* bod $(0 : 1 : 0) \in E^*$. Uvažujme divizor $A = (-(p+1) \cdot P + n \cdot O^*) \in \mathrm{Div}(E^*)$ a Riemann-Rochov priestor

$$\mathscr{L}(A) = \{0\} \cup \{0 \neq g \in \mathbb{C}(E^*) \mid (g) \geq -A\}.$$

Na základe diskusie vyššie môžeme pomocou izomorfizmu α z tvrdenia 14 stotožniť množinu $\mathscr{L}(A)$ s množinou $L := \{0\} \cup \overline{L}$, kde

$$\overline{L} := \{0 \neq g \in \mathbb{C}(E) \mid v_{(0,a_0)}(g) \geq p+1,\ v_O(g) \geq -n \text{ a } v_Q(g) \geq 0\ \forall (0,a_0) \neq Q \in E\}.$$

Podľa lemy 21 je $\mathscr{L}(A)$, a teda aj L, vektorový priestor nad $\mathbb{C}$. Vidíme, že všetky prvky priestoru L sú definované v každom bode eliptickej krivky E. Takže podľa tvrdenia 8 sú všetky prvky priestoru L polynomiálne funkcie na $V(E)$. V okruhu $\mathbb{C}[E]$ platí $s^2 = (t-t_1)(t-t_2)(t-t_3)$, takže každá polynomiálna funkcia na $V(E)$ je konečnou lineárnou kombináciou polynomiálnych funkcií $\{t^i, st^i \mid i \geq 0\}$ s koeficientami v $\mathbb{C}$. Uvažujme nenulovú funkciu $g \in \mathbb{C}[E]$:

$$g = c_0 + c_1 t + c_2 s + c_3 t^2 + c_4 st + \cdots + c_{2i+1} t^{i+1} + c_{2i+2} st^i + \cdots .$$

Keďže $v_O(s) = -3$ a $v_O(t) = -2$, tak pre každé $i \geq 0$ platí $v_O(t^i) = -2i$ a $v_O(st^i) = -3-2i$. Teda funkcie z množiny $\{t^i, st^i \mid i \geq 0\}$ majú v bode O po dvoch rôzne, nekladné, valuácie. Z tvrdenia 2 vyplýva, že valuácia funkcie g v bode O je rovná valuácii členu s koeficientom c_k, kde $k = \max(j \mid c_j \neq 0)$. Valuácie jednotlivých nenulových členov v bode O totiž ostro klesajú s rastúcim j. Pokiaľ $g \in L$, tak $v_O(g) \geq -n = -2p-1$, a teda $k \leq 2(p-1)+2$. Takže

$$g = c_0 + c_1 t + c_2 s + c_3 t^2 + c_4 st + \cdots + c_{2(p-1)+1} t^p + c_{2(p-1)+2} st^{p-1}. \tag{5.2}$$

Všetky prvky priestoru L sú teda tvaru (5.2).

Ukážeme, že funkcie $f_i = t^{p-i}(s - \lambda_0 - \lambda_1 t - \ldots - \lambda_i t^i), i \in \{1, \ldots, p\}$ tvoria bázu vektorového priestoru L. Zjavne polynomiálne funkcie f_i sú definované v každom bode krivky E. Z prvej časti dôkazu vidíme, že funkcie f_i majú v bode O pól násobnosti najviac $2p+1$. Z rozvoja funkcií f_i do mocninových radov (5.1) vidíme, že funkcie f_i majú v bode $(0, a_0)$ nulu násobnosti aspoň $p+1$. Takže funkcie $f_i, i \in \{1, \ldots, p\}$ sú prvkami priestoru L.

Keďže funkcie $\{t^i, st^i \mid i \geq 0\}$ majú po dvoch rôzne valuácie v bode O, z tvrdenia 2 vyplýva, že nevieme jednu funkciu z množiny $\{t^i, st^i \mid i \geq 0\}$ vyjadriť ako lineárnu kombináciu ostatných. V každej funkcii z množiny $\{f_i \mid i \in \{1, \ldots, p\}\}$ sa nachádza práve jeden člen obsahujúci s. Všetky tieto členy obsahujúce s vo funkciách $f_i, i \in \{1, \ldots, p\}$ sú po dvoch rôzne. Pre spor predpokladajme, že existujú koeficienty $d_1, \ldots, d_p \in \mathbb{C}$, aspoň jeden z nich nenulový, spĺňajúce $d_1 f_1 + \cdots + d_p f_p = 0$. Bez ujmy na všeobecnosti nech $d_1 \neq 0$. Potom platí

$$d_1 st^{p-1} = -d_1(-t^{p-1}\lambda_0 - t^p \lambda_1) - d_2 f_2 - \ldots - d_p f_p. \tag{5.3}$$

Na pravej strane (5.3) sa nenachádza žiadny člen obsahujúci funkciu st^{p-1}, takže vieme funkciu st^{p-1} vyjadriť ako lineárnu kombináciu zvyšných funkcií z množiny $\{t^i, st^i \mid i \geq 0\}$, čo je spor. Funkcie $f_i, i \in \{1, \ldots, p\}$ sú teda lineárne nezávislé.

Zostáva nám ukázať, že funkcie $f_i, i \in \{1, \ldots, p\}$ generujú priestor L. Nech $g \in L$. Potom existujú koeficienty $c_0, \ldots, c_{2p} \in \mathbb{C}$ také, že

$$g = c_0 + c_1 t + c_2 s + c_3 t^2 + c_4 st + \cdots + c_{2p-1} t^p + c_{2p} st^{p-1}.$$

Položme polynomiálnu funkciu

$$h := g - c_2 f_p - c_4 f_{p-1} - \ldots - c_{2p} f_1 \in L.$$

Pre spor predpokladajme, že $h \neq 0$. Z definície funkcií $f_i, i \in \{1, \ldots, p\}$ vyplýva, že všetky členy funkcie h obsahujú len funkcie $\{t^i \mid i \in \{0, \ldots, p\}\}$. Takže existujú koeficienty $d_0, \ldots, d_p \in \mathbb{C}$, aspoň jeden z nich nenulový, také, že

$$h = d_0 + d_1 t + \cdots + d_p t^p.$$

Nech $l = \min(j \mid d_j \neq 0)$. Potom z tvrdenia 2 vyplýva, že

$$v_{(0,a_0)}(h) = v_{(0,a_0)}(d_l t^l) = l \leq p.$$

To je spor s tým, že všetky nenulové prvky L majú v bode $(0, a_0)$ nulu násobnosti aspoň $p + 1$. Takže h je nulová funkcia a funkcia g sa dá vyjadriť ako lineárna kombinácia funkcií $f_i, i \in \{1, \ldots, p\}$ s koeficientami v $\mathbb{C}$. Funkcie $f_i, i \in \{1, \ldots, p\}$ teda generujú priestor L.

Predpokladáme, že existuje racionálna funkcia $f \in \mathbb{C}(E)$, ktorá má v bode O pól násobnosti n, v bode $(0, a_0)$ nulu násobnosti n a nemá žiadne iné nuly ani póly. Táto funkcia f je zjavne prvkom priestoru L. Takže ju vieme vyjadriť ako lineárnu kombináciu prvkov báze $\{f_i \mid i \in \{1, \ldots, p\}\}$ priestoru L s koeficientami v $\mathbb{C}$:

$$f = c_1 f_1 + \cdots + c_p f_p.$$

Z rozvoja funkcii f_i do mocninových radov (5.1) dostávame

$$f = (c_1\lambda_2 + c_2\lambda_3 + \cdots + c_p\lambda_{p+1})t^{p+1} + (c_1\lambda_3 + c_2\lambda_4 + \cdots + c_p\lambda_{p+2})t^{p+2} + \ldots.$$

Nech $k = \min(j \geq 1 \mid c_1\lambda_{1+j} + c_2\lambda_{2+j} + \cdots + c_p\lambda_{p+j} \neq 0)$. Potom

$$\begin{aligned} f &= \sum_{j \geq k} (c_1\lambda_{1+j} + c_2\lambda_{2+j} + \cdots + c_p\lambda_{p+j})t^{p+j} = \\ &= t^{p+k} \sum_{j \geq k} (c_1\lambda_{1+j} + c_2\lambda_{2+j} + \cdots + c_p\lambda_{p+j})t^{j-k}. \end{aligned}$$

Keďže

$$\sum_{j \geq k} (c_1\lambda_{1+j} + c_2\lambda_{2+j} + \cdots + c_p\lambda_{p+j})t^{j-k} = \frac{f}{t^{p+k}},$$

je $\sum_{j \geq k}(c_1\lambda_{1+j} + c_2\lambda_{2+j} + \cdots + c_p\lambda_{p+j})t^{j-k}$ racionálna funkcia na $V(E)$. Navyše racionálna funkcia $\sum_{j \geq k}(c_1\lambda_{1+j} + c_2\lambda_{2+j} + \cdots + c_p\lambda_{p+j})t^{j-k}$ je definovaná v bode $(0, a_0)$, teda bod $(0, a_0)$ môžeme do nej dosadiť a dostaneme

$$\sum_{j \geq k} (c_1\lambda_{1+j} + c_2\lambda_{2+j} + \cdots + c_p\lambda_{p+j})0^{j-k} = (c_1\lambda_{1+k} + c_2\lambda_{2+k} + \cdots + c_p\lambda_{p+k}) \neq 0.$$

Takže $\sum_{j \geq k}(c_1\lambda_{1+j} + c_2\lambda_{2+j} + \cdots + c_p\lambda_{p+j})t^{j-k}$ je invertibilný prvok $O_{(0,a_0)}(E)$. Z toho vyplýva, že $v_{(0,a_0)}(f) = p + k$. Keďže funkcia f má v bode $(0, a_0)$ nulu násobnosti $n = 2p + 1$, platí $k = p + 1$. Takže

$$(0, \ldots, 0) = c_1(\lambda_2, \ldots, \lambda_{p+1}) + \cdots + c_p(\lambda_{p+1}, \ldots, \lambda_{2p}).$$

Teda vektory $(\lambda_2, \ldots, \lambda_{p+1}), \ldots, (\lambda_{p+1}, \ldots, \lambda_{2p})$ sú lineárne závislé a matica

$$\begin{pmatrix} \lambda_2 & \ldots & \lambda_{p+1} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \lambda_{p+1} & \ldots & \lambda_{2p} \end{pmatrix}$$

je singulárna. Determinant tejto matice je preto rovný 0.

V prípade, že $n = 2p$, kde $p \in \mathbb{N}, p \geq 2$, postupujeme analogicky ako v prípade $n = 2p + 1, p \in \mathbb{N}$. Tentokrát však budú bázu príslušného vektorového priestoru L tvoriť funkcie $f_i = t^{p-i-1}(s - \lambda_0 - \lambda_1 t - \ldots - \lambda_{i+1} t^{i+1}), i \in \{1, \ldots, p-1\}$. □

Teraz sa už môžeme pozrieť na samotné Cayleyovo kritérium.

Veta 30 (Cayleyovo kritérium)**.** *Nech E je eliptická krivka nad $\mathbb{C}$ daná rovnicou $s^2 = (t - t_1)(t - t_2)(t - t_3)$, kde $t_1, t_2, t_3 \neq 0$, a E^* je projektívny uzáver krivky E. Nech $(t : s : u) = (0 : a_0 : 1) \in \mathbb{P}^2(\mathbb{C})$ je bod ležiaci na krivke E^* a $n \in \mathbb{N}, n \geq 3$. Uvažujme rozvoj prvku s do mocninového radu*

$$s = \sum_{i=0}^{\infty} \lambda_i t^i.$$

Potom rád bodu $(0 : a_0 : 1)$ delí n práve vtedy, keď platí

$$\begin{vmatrix} \lambda_2 & \ldots & \lambda_{p+1} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \lambda_{p+1} & \ldots & \lambda_{2p} \end{vmatrix} = 0, \text{ pokiaľ } n = 2p + 1, \text{ kde } p \in \mathbb{N}, \text{ alebo}$$

$$\begin{vmatrix} \lambda_3 & \ldots & \lambda_{p+1} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \lambda_{p+1} & \ldots & \lambda_{2p-1} \end{vmatrix} = 0, \text{ pokiaľ } n = 2p, \text{kde } p \in \mathbb{N}, p \geq 2.$$

Dôkaz. Označme P bod $(0 : a_0 : 1)$ a O^* bod $(0 : 1 : 0)$. Pomocou zobrazenia φ z tvrdenia 27 prenesieme bod P na prvok $[P - O^*] \in \mathrm{Cl}_0(E^*)$. Nech d je rád bodu P resp. rád prvku $[P - O^*]$ vo faktorgrupe $\mathrm{Cl}_0(E^*)$. Potom $d \,|\, n$ práve vtedy, keď

$$n[P - O^*] = [nP - nO^*] = 0_{\mathrm{Cl}_0(E^*)}.$$

To nastáva práve vtedy, keď $(nP - nO^*) \in \mathrm{PDiv}(E^*)$. A divizor $(nP - nO^*)$ je hlavný práve vtedy, keď existuje nenulová racionálna funkcia $f \in \mathbb{C}(E^*)$, ktorá má v bode P nulu násobnosti n, v bode O^* pól násobnosti n a nemá žiadne iné nuly ani póly. Z tvrdenia 14 a z poznámky za ním vyplýva, že taká funkcia f existuje práve vtedy, keď existuje nenulová racionálna funkcia $g \in \mathbb{C}(E)$, ktorá má v bode $(0, a_0)$ nulu násobnosti n, v bode O pól násobnosti n a nemá žiadne iné nuly ani póly. A nakoniec z tvrdenia 28 vyplýva, že taká funkcia g existuje práve vtedy, keď

$$\begin{vmatrix} \lambda_2 & \ldots & \lambda_{p+1} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \lambda_{p+1} & \ldots & \lambda_{2p} \end{vmatrix} = 0, \text{ pokiaľ } n = 2p + 1, \text{ kde } p \in \mathbb{N}, \text{ alebo}$$

$$\begin{vmatrix} \lambda_3 & \ldots & \lambda_{p+1} \\ \cdot & & \cdot \\ \cdot & & \cdot \\ \lambda_{p+1} & \ldots & \lambda_{2p-1} \end{vmatrix} = 0, \text{ pokiaľ } n = 2p, \text{kde } p \in \mathbb{N}, p \geq 2.$$

□

Záver

Cieľom tejto práce bolo dokázať Cayleyovo kritérium pre rád bodu na eliptickej krivke. Vychádzali sme z článku O. Nasha [2], v ktorom môžeme nájsť hlavné myšlienky dôkazu jednej implikácie. Tieto hlavné myšlienky sme spracovali a doplnili sme všetky chýbajúce časti dôkazu. Doplnili sme taktiež aj dôkaz druhej implikácie. V znení Cayleyovho kritéria a neskôr v jeho dôkaze sme využívali rozvoj prvku do mocninového radu, ktorý sme riadne zadefinovali v kapitole 1. V dôkaze ďalej zohrali dôležitú úlohu polynomiálne a racionálne funkcie na varietách, ktoré sme zaviedli v kapitole 2. V kapitole 4 sme dokázali všetky potrebné vlastnosti eliptických kriviek, mimo iného aj nesingularitu a ireducibilitu, ktorú sme zadefinovali v kapitole 3 obecne pre rovinné krivky. V druhej časti kapitoly 4 sme navyše popísali dve grupové štruktúry na projektívnom uzávere eliptickej krivky a podrobne vysvetlili, prečo si tieto dve grupové štruktúry odpovedajú.

Táto práca by sa dala rozšíriť napríklad nadviazaním na úvod a detailným vysvetlením vzťahu medzi Ponceletovým porismatom a Cayleyovým kritériom.

Literatúra

1. Fulton, William. *Algebraic Curves. An Introduction to Algebraic Geometry.* electronic edition, 2008. https://dept.math.lsa.umich.edu/~wfulton/CurveBook.pdf, [cit. 2024-04-12].
2. Nash, Oliver. Poring over Poncelet. 2018. http://olivernash.org/2018/07/08/poring-over-poncelet/index.html, [cit. 2024-04-12].
3. Stichtenoth, Henning. *Algebraic Function Fields and Codes. Graduate Texts in Mathematics.* Zv. 254. Berlin: Springer Science & Business Media, 2009. 2nd edition.
4. Kala, Vítězslav. *Úvod do komutativní algebry.* 2023. https://karlin.mff.cuni.cz/~kala/files/UKA22.pdf, [cit. 2024-04-12].
5. Kirwan, Frances Clare. *Complex Algebraic Curves.* Cambridge University Press, 1992. Č. 23.
6. Washington, Lawrence C. *Elliptic Curves: Number Theory and Cryptography.* Chapman a Hall/CRC, 2008. 2nd edition.
7. Stanovský, David. *Učební text, Algebra 2021/22.* 2022. https://www.karlin.mff.cuni.cz/~stovicek/dl/22-23-ls/algebra22.pdf, [cit. 2024-05-02].

Zoznam obrázkov