



**MATEMATICKO-FYZIKÁLNÍ
FAKULTA**
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Anna Mlezivová

Ponceletovo porisma

Katedra algebry

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

Studijní program: Matematika

Studijní obor: Obecná matematika

Praha 2021

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

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

Především bych chtěla poděkovat svému vedoucímu doc. RNDr. Janu Štovíčkovi, Ph.D. za vydatnou pomoc, trpělivost a všechnen čas strávený mou prací. Dále bych chtěla poděkovat Radku Olšákovi za podporu, ochotu povídat si o Ponceletově porismatu téměř kdykoliv a pomoc s vymýšlením sekce 2.2. V neposlední řadě děkuji Karlu Balejovi za cenné rady ohledně L^AT_EXu.

Název práce: Ponceletovo porisma

Autor: Anna Mlezivová

Katedra: Katedra algebry

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

Abstrakt: V práci je uveden kompletní důkaz Ponceletova porismatu. To říká, že máme-li dvě kuželosečky a pro dané n existuje n -úhelník, který je jedné z nich opsaný a druhé vepsaný, existuje takovýchto n -úhelníků hned nekonečně mnoho. V první kapitole zavádíme potřebnou teorii z oblasti algebraické geometrie, kapitola druhá se věnuje samotnému důkazu. V ní ukážeme, že porisma stačí dokazovat pro soustřednou kružnici a elipsu. Také v důkazu využíváme řadu izomorfismů projektivních variet, které problém převedou do tvaru eliptické křivky se známou grupovou strukturou.

Klíčová slova: algebraická geometrie, Ponceletovo porisma, eliptická křivka

Title: Poncelet's porism

Author: Anna Mlezivová

Department: Department of Algebra

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

Abstract: The thesis presents a complete proof of Poncelet's porism, which states that if we have two conic sections and for given n exists an n -gon, which is circumscribed by one and inscribed in the other, there are infinitely many such n -gons. In the first chapter we introduce the necessary theory from the field of algebraic geometry. The second chapter deals with the proof. We show that it is enough to prove the porism only for a concentric circle and ellipse. We also use a series of isomorphisms between projective varieties to transform the problem into a form of an elliptic curve with a known group structure.

Keywords: algebraic geometry, Poncelet's porism, elliptic curve

Obsah

Úvod	2
1 Příprava	3
1.1 Topologie	3
1.2 Afinity algebraické množiny	3
1.3 Polynomiální zobrazení	5
1.4 Racionální zobrazení	6
1.5 Projektivní algebraická geometrie	6
2 Ponceletovo porisma	9
2.1 Znění	9
2.2 Převod kuželoseček na soustřednou kružnici a elipsu	10
2.2.1 Jedna kuželosečka	10
2.2.2 Soustředná kuželosečka s kružnicí	11
2.2.3 Diagonalizace	12
2.3 Reformulace problému	13
2.4 Stereografická projekce	14
2.4.1 Zobrazení přímky na elipsu	14
2.4.2 Zobrazení elipsy na přímku	15
2.4.3 Převod N na M	16
2.5 Ireducibilita M	16
2.6 Převod M do projektivní variety	18
2.7 Izomorfismus elipsy a přímky	18
2.8 Zavedení dalších variet	19
2.9 Biracionální ekvivalence M , K a L	20
2.10 Ekvivalentní vyjádření t a d	21
2.11 Izomorfismus M' a L'	22
2.11.1 $M' \rightarrow L'$	22
2.11.2 $L' \rightarrow M'$	23
2.11.3 Celý izomorfismus	24
2.12 Dokončení důkazu	25
2.12.1 Grupová struktura L'	25
2.12.2 Involuce	25
Závěr	27
Seznam použité literatury	28

Úvod

Ponceletovo porisma je asi 200 let starý geometrický problém. Říká, že pokud máme v komplexní projektivní rovině dvě kuželosečky a pro dané $n \geq 3$ existuje nějaký n -úhelník, který je opsaný jedné z nich a vepsaný druhé, tak už takovýchto n -úhelníků existuje nekonečně mnoho. Nejznámější důkazy využívají buď analytického, nebo algebraického pohledu na eliptické křivky. Cílem této práce je jeden z důkazů srozumitelně prezentovat. Jde o algebraický důkaz, jehož myšlenka je podobná známému důkazu Griffitse a Harrise, ovšem k důkazu, že je jistá množina eliptická křivka, přistupujeme elementárnějším způsobem.

Než se k Ponceletovu porismatu dostaneme, zavedeme v kapitole 1 teorii, kterou budeme k důkazu potřebovat. Jedná se o řadu definic a tvrzení z afinní i projektivní algebraické geometrie s využitím několika topologických pojmů.

Znění Ponceletova porismatu formulujeme na začátku kapitoly 2. V sekci 2.2 zdůvodníme, že větu stačí dokázat pro soustřednou kružnici a elipsu. Dále v sekci 2.3 zavedeme N' množinu všech dvojic bodů takových, že první leží na elipse, druhý na kružnici a oba leží na společné tečně ke kružnici. Na této množině najdeme dvě přirozené involuce, jejich složení označíme T . Pak Ponceletovo porisma přeformulujeme tak, aby stačilo dokázat, že T^n má pevný bod právě tehdy, když je to identické zobrazení. Naším cílem bude ukázat, že N' je eliptická křivka a vzhledem k její grupové struktuře je T translace. Translace s pevným bodem je identické zobrazení, tedy tvrzení bude dokázáno.

Že je N' eliptická křivka ukážeme tak, že N' převedeme do známého Jacobiho tvaru eliptické křivky a ukážeme, že převody jsou izomorfismy projektivních variet. To provedeme v kapitolách 2.4–2.11. Obsah těchto kapitol je z velké části vlastní za pomoci vedoucího. Výpočty v nich jsou mé vlastní a k některým jsem z důvodu ulehčení práce použila matematický software *Mathematica*.

Následně v sekci 2.12 díky známé grupové struktuře zjistíme, že zobrazení T je opravdu translace, čímž bude Ponceletovo porisma dokázáno.

1. Příprava

V této kapitole jsou definovány pojmy potřebné pro pochopení hlavní části práce. Jedná se především o stručný úvod do algebraické geometrie s využitím několika topologických pojmů. Podrobnější vysvětlení a širší souvislosti najdeme v knize *Algebraic curves* (Fulton, 2008), která je hlavním zdrojem první kapitoly. Pomocným zdrojem jsou kapitoly 1, 4, 5 a 8 z knihy *Ideals, varieties and algorithms* (Cox, Little a O'Shea, 2007).

1.1 Topologie

Definice 1.1 (Topologie). *Topologie* na množině X je systém $\tau \subseteq \mathcal{P}(X)$ splňující

1. $\emptyset \in \tau$, $X \in \tau$,
2. $U_1, U_2 \in \tau \Rightarrow U_1 \cap U_2 \in \tau$,
3. $\mathcal{A} \subseteq \tau \Rightarrow \bigcup \mathcal{A} \in \tau$.

Dvojici (X, τ) nazýváme *topologický prostor*. Prvky τ se nazývají *otevřené množiny* a jejich doplňky *uzavřené množiny*.

Definice 1.2 (Uzávěr). *Uzávěr* podmnožiny A topologického prostoru je nejmenší uzavřená množina obsahující A . Uzávěr A značíme $\overline{A}$.

Definice 1.3 (Spojité zobrazení). Jsou-li X, Y topologické prostory, pak zobrazení $f: X \rightarrow Y$ je *spojité*, pokud vzory všech uzavřených podmnožin Y jsou uzavřené v X .

Definice 1.4 (Reducibilní a ireducibilní podmnožiny). Podmnožina A topologického prostoru X je *reducibilní*, pokud existují A_1, A_2 uzavřené podmnožiny X takové, že $A = (A_1 \cap A) \cup (A_2 \cap A)$ a A není obsažena ani v jedné z nich. Podmnožina A topologického prostoru X je *ireducibilní*, pokud není reducibilní.

1.2 Afinní algebraické množiny

Afinní algebraické množiny jsou ve Fultonově knize (Fulton, 2008) obsahem kapitoly 1.

Ve zbytku první kapitoly budeme značit K těleso, v kapitole 2 budeme pracovat s $K = \mathbb{C}$ tělesem komplexních čísel. $\mathbb{A}^n(K)$ pro $n \geq 1$ značíme n -rozměrný afinní prostor nad K , neboli kartézský součin $K \times K \times \cdots \times K$.

Množinu polynomů nad K v proměnných $x_1, \dots, x_n$ značíme $K[x_1, \dots, x_n]$ nebo jen zkráceně $K[\bar{x}]$.

Definice 1.5 (Nula polynomu). Pro $f \in K[x_1, \dots, x_n]$ se bod $A = (a_1, \dots, a_n)$ nazývá *nulou polynomu* f , jestliže $f(a_1, \dots, a_n) = 0$. Množina všech nul polynomu f se značí $V(f)$.

Definice 1.6 (Afinní algebraická množina). Pro množinu polynomů $S \subseteq K[\bar{x}]$ definujeme

$$V(S) = \{A \in \mathbb{A}^n(K) \mid f(A) = 0 \ \forall f \in S\}$$

Množina $X \subseteq \mathbb{A}^n(K)$ je *afinní algebraická množina*, pokud $X = V(S)$ pro nějaké $S \subseteq K[\bar{x}]$.

Definice 1.7 (Algebraická nadplocha). Množina $X \subseteq \mathbb{A}^n(K)$ je *afinní algebraická nadplocha*, pokud $X = V(f)$, kde $f \in K[x_1, \dots, x_n]$ je nekonstantní polynom.

Definice 1.8 (Afinní algebraická rovinná křivka). *Afinní algebraická rovinná křivka* je algebraická nadplocha v afinním prostoru dimenze dva.

Definice 1.9 (Ideál množiny). Pro množinu $X \subseteq \mathbb{A}^n(K)$ definujeme *ideál množiny* X jako $I(X) = \{f \in K[\bar{x}] \mid f(A) = 0 \ \forall A \in X\}$.

Pozorování. Necht $X_1, X_2 \subseteq \mathbb{A}^n(K)$ a $S_1, S_2 \subseteq K[\bar{x}]$. Pak platí:

1. Pokud $X_1 \subseteq X_2$, pak $I(X_1) \supseteq I(X_2)$.
2. Pokud $S_1 \subseteq S_2$, pak $V(S_1) \supseteq V(S_2)$.

Lemma 1.10. Necht $S \subseteq K[\bar{x}]$ a $I = (S)$ ideál generovaný S . Pak $V(I) = V(S)$.

Důkaz. Jistě $V(I) \subseteq V(S)$. Na druhou stranu $I = \{\sum g_i f_i \mid g_i \in K[\bar{x}], f_i \in S\}$, tedy pokud $A \in V(S)$, neboli $f(A) = 0 \ \forall f \in S$, pak i $(\sum g_i f_i)(A) = 0$, takže $A \in V(I)$. $\square$

Pozorování.

1. $V(0) = \mathbb{A}^n(K), V(1) = \emptyset$
2. Pro I, J ideály platí $V(I) \cup V(J) = V(\{fg \mid f \in I, g \in J\}) = V(IJ)$
3. Je-li J množina ideálů v $K[\bar{x}]$, pak $\bigcap_{I \in J} V(I) = V(\bigcup_{I \in J} I)$.

Definice 1.11 (Zariského topologie). Topologie na $\mathbb{A}^n(K)$, jejíž uzavřené množiny jsou algebraické, se nazývá *Zariského topologie*.

Zariského topologie splňuje podmínky topologie díky předchozímu pozorování. Z 1. části pozorování jsou $\mathbb{A}^n(K)$ i $\emptyset$ uzavřené množiny a jedna je doplňkem druhé, tudíž jsou i otevřené. Z 2. části plyne, že konečné sjednocení uzavřených množin je uzavřené, takže konečný průnik doplňků uzavřených bude doplněk uzavřený, neboli konečný průnik otevřených množin bude otevřená množina. Z 3. části pozorování máme, že průnik libovolně mnoha uzavřených množin je uzavřený, tedy sjednocení libovolně mnoha otevřených bude otevřené.

Definice 1.12 (Afinní varieta). Neprázdná ireducibilní afinní algebraická množina se nazývá *afinní varieta*.

Ireducibilita je myšlena ve smyslu definice 1.4, ve které bereme prostor $\mathbb{A}^n(K)$ se Zariského topologií.

Tvrzení 1.13. *Neprázdňá algebraická množina X je ireducibilní právě tehdy, když $I(X)$ je prvoideál.*

Důkaz. Předpokládejme, že $I(X)$ není prvoideál. Pak existují $f_1, f_2 \notin I(X)$, ale $f_1 f_2 \in I(X)$. Podíváme se na algebraické množiny $X_i = V(I(X) \cup \{f_i\})$. Jelikož $f_i \notin I(X)$, pak $X_i \subsetneq X$. Pro každé $A \in X$ platí, že $f_1(A) = 0$ nebo $f_2(A) = 0$, neboť $f_1 f_2 \in I(X)$. Tudíž $X = X_1 \cup X_2$ je reducibilní.

Naopak pokud X má rozklad $X = X_1 \cup X_2$, $X_i \subsetneq X$, pak $I(X_i) \supsetneq I(X)$. Tudíž můžeme vzít $f_i \in I(X_i) \setminus I(X)$, pak $f_1 f_2 \in I(X)$, tedy $I(X)$ není prvoideál. $\square$

Tvrzení 1.14. *Pokud f je ireducibilní polynom nad algebraicky uzavřeným tělesem, pak $V(f)$ je afinní varieta.*

Důkaz. Tvrzení plyne z důsledku Hilbertovy věty o nulách, který je uveden v knize W. Fultona (Fulton, 2008, Kapitola 1.7, Corollary 3). V též kapitole je uvedena a dokázána i samotná Hilbertova věta o nulách. $\square$

1.3 Polynomiální zobrazení

Tato sekce je sepsána podle kapitol 2.1 a 2.2 ve zmiňované knize (Fulton, 2008).

Dále bude $V \subseteq \mathbb{A}^n(K)$ značit neprázdňou varietu. Pak je $I(V)$ prvoideál v $K[\bar{x}]$ podle tvrzení 1.13, tudíž $K[\bar{x}]/I(V)$ je obor integrity.

Definice 1.15 (Souřadnicový okruh). Souřadnicový okruh variety V definujeme jako $K[\bar{x}]/I(V)$ a budeme značit $\Gamma(V)$.

Nechť $\mathcal{F}(V, K)$ značí množinu všech funkcí z V do K . Pak $\mathcal{F}(V, K)$ tvoří okruh s operacemi $\cdot$ a $+$ definovaných po bodech. Funkce $\varphi_f \in \mathcal{F}(V, K)$ se nazývá polynomiální funkce, jestliže existuje polynom $f \in K[x_1, \dots, x_n]$ takový, že $\varphi_f(a_1, \dots, a_n) = f(a_1, \dots, a_n)$. Označme $\mathcal{Pol}(V, K) \subseteq \mathcal{F}(V, K)$ okruh polynomiálních funkcí z V do K .

Tvrzení 1.16. $\Gamma(V) \cong \mathcal{Pol}(V, K)$

Důkaz. Definujme zobrazení

$$\begin{aligned} \Psi : K[\bar{x}] &\rightarrow \mathcal{F}(V, K) \\ f &\rightarrow \varphi_f. \end{aligned}$$

Pak Ψ je homomorfismus, obraz Ψ jsou polynomiální funkce $\mathcal{Pol}(V, K)$. V jádru Ψ jsou přesně polynomy, které se nulují na celé množině V , neboli právě polynomy náležící $I(V)$. Podle první věty o izomorfismu máme $\Gamma(V) = K[\bar{x}]/I(V) \cong \mathcal{Pol}(V, K)$. $\square$

Prvky $\Gamma(V)$ tak můžeme vnímat jako polynomiální funkce z V do K nebo jako třídy ekvivalence polynomů.

Definice 1.17 (Polynomiální zobrazení). Nechť $V \subseteq \mathbb{A}^n(K)$, $W \subseteq \mathbb{A}^m(K)$ jsou variety. Zobrazení $\varphi : V \rightarrow W$ je *polynomiální*, pokud existují polynomy $f_1, \dots, f_m \in K[x_1, \dots, x_n]$ takové, že $\varphi(A) = (f_1(A), \dots, f_m(A))$ pro všechna $A \in V$.

Definice 1.18 (Izomorfismus variet). Afinní variety V a W jsou *izomorfní*, pokud existuje bijektivní polynomiální zobrazení $\varphi : V \rightarrow W$ takové, že $\varphi^{-1} : W \rightarrow V$ je také polynomiální zobrazení.

1.4 Racionální zobrazení

V knize W. Fultona (Fulton, 2008) nalezneme racionální zobrazení v kapitolách 2.4, 6.3 a 6.6.

Jak jsme zmínili na začátku minulé sekce, souřadnicový okruh $\Gamma(V)$ je obor integrity. Tudíž můžeme definovat jeho podílové těleso $K(V)$, kterému budeme říkat funkční těleso V . Prvky $K(V)$ nazýváme racionální funkce na V .

Definice 1.19. Necht q je racionální funkce na V a $A \in V$. Pak q je *definovaná* v A , pokud existují nějaké $f, g \in \Gamma(V)$, $q = \frac{f}{g}$ a $g(A) \neq 0$.

Prvky f a g nemusí být určeny jednoznačně. Uvažujme $\frac{f_1}{g_1} = \frac{f_2}{g_2}$ dva různé zlomky představující stejný prvek $K(V)$. Necht pro $A \in V$ platí $g_1(A) \neq 0 \neq g_2(A)$. Díky rovnosti zlomků v $K(V)$ máme rovnost $f_1 g_2 = f_2 g_1$ v $\Gamma(V)$ a tudíž $f_1(A) g_2(A) = f_2(A) g_1(A)$ v K . Takže $\frac{f_1(A)}{g_1(A)} = \frac{f_2(A)}{g_2(A)}$.

Definice 1.20 (Racionální zobrazení). Necht $V \subseteq \mathbb{A}^n(K)$, $W \subseteq \mathbb{A}^n(K)$ jsou variety. *Racionální zobrazení* z V do W je takové zobrazení $r : U \rightarrow W$, že U je neprázdná Zariski otevřená podmnožina V a existují racionální funkce $r_1, \dots, r_m \in K(V)$ takové, že $r(A) = (r_1(A), \dots, r_m(A))$ pro všechna $A \in U$.

Definice 1.21 (Ekvivalence). Necht V, W jsou variety nad K , $r : U_1 \rightarrow W$ a $s : U_2 \rightarrow W$ jsou racionální zobrazení z V do W . Pak r a s jsou *ekvivalentní*, pokud existuje neprázdná Zariski otevřená $U \subseteq U_1 \cap U_2$ taková, že $r|_U = s|_U$. Třidu ekvivalence r budeme značit $r : V \dashrightarrow W$.

Definice 1.22 (Biracionální ekvivalence). Necht V, W jsou variety nad K . Racionální zobrazení $r : V \dashrightarrow W$ se nazývá *biracionální ekvivalence*, pokud existuje racionální zobrazení $s : W \dashrightarrow V$ takové, že složení $s \circ r$ i $r \circ s$ jsou definované a ekvivalentní identickým zobrazením na V a W .

Variety V a W jsou *biracionálně ekvivalentní*, pokud existuje biracionální ekvivalence $r : V \dashrightarrow W$.

Pokud V a W jsou křivky nad nekonečným tělesem, pak jejich biracionální ekvivalence znamená přesně to, že až na konečně bodů na obou stranách máme mezi V a W bijekci. Pro neprázdnou otevřenou podmnožinu U variety V totiž díky klasifikaci variet v rovině (Fulton, 2008, Kapitola 1.6, Corollary 2) platí, že $V \setminus U$ je konečná.

Tvrzení 1.23. *Dvě variety jsou biracionálně ekvivalentní právě tehdy, když jsou jejich funkční tělesa izomorfní.*

Důkaz. Viz Fulton (2008, Kapitola 6.6, Proposition 12). □

1.5 Projektivní algebraická geometrie

V knize W. Fultona (Fulton, 2008) je úvod do projektivní algebraické geometrie obsahem kapitoly 4.

Definice 1.24 (Projektivní prostor). Množinu přímk procházejících $(0, 0, \dots, 0)$ v $\mathbb{A}^{n+1}(K)$ nazveme *projektivní n -rozměrný prostor* a budeme značit $\mathbb{P}^n(K)$.

Každý bod $(x_1, \dots, x_{n+1}) \neq (0, \dots, 0)$ určuje právě jeden prvek $\mathbb{P}^n(K)$, konkrétně $\{(\lambda x_1, \dots, \lambda x_{n+1}) \mid \lambda \in K\}$.

Pokud je prvek $P \in \mathbb{P}^n(K)$ určen bodem $(x_1, \dots, x_{n+1})$, pak $(x_1, \dots, x_{n+1})$ nazýváme homogenní souřadnice P . Budeme psát $P = [x_1 : \dots : x_{n+1}]$, abychom homogenní souřadnice odlišili od afinních. Zápis P v homogenních souřadnicích sice není jednoznačně určen, ale pro libovolné $1 \leq i \leq n+1$ je souřadnice x_i ve všech zápisech nulová nebo ve všech nenulová. Pokud $x_i \neq 0$, pak můžeme všechny souřadnice vydělit x_i a P můžeme jednoznačně zapsat ve tvaru $[x_1 : \dots : x_{i-1} : 1 : x_{i+1} : \dots : x_{n+1}]$.

Standardně budeme za i volit $n+1$. Pro množinu všech prvků $P \in \mathbb{P}^n(K)$, kde $x_{n+1} \neq 0$, existuje přirozená bijekce s $\mathbb{A}^n(K)$, neboť máme bijekci mezi afinními body $(x_1, \dots, x_n)$ a body jednoznačně určenými zápisem v homogenních souřadnicích $[x_1 : \dots : x_n : 1]$. Množině prvků $\mathbb{P}^n(K)$ s nenulovou $n+1$ souřadnicí říkáme afinní část $\mathbb{P}^n(K)$.

Naopak množina všech prvků $P \in \mathbb{P}^n(K)$, kde $x_{n+1} = 0$, má přirozenou bijekci s $\mathbb{P}^{n-1}(K)$. Těmto bodům říkáme body v nekonečnu v $\mathbb{P}^n(K)$ nebo také nevlastní body.

Definice 1.25 (Forma). *Forma stupně i* je polynom, jehož všechny členy jsou stupně i .

Polynom stupně d pak můžeme jednoznačně zapsat ve tvaru $f = f_0 + f_1 + \dots + f_d$, kde f_i je forma stupně i .

Definice 1.26 (Homogenizace). Pro polynom f stupně d , $f = f_0 + f_1 + \dots + f_d$, $f \in K[x_1, \dots, x_n]$ definujeme $f^* \in K[x_1, \dots, x_{n+1}]$, $f^* = \sum_{i=0}^d f_i \cdot x_{n+1}^{d-i}$. Tento proces nazveme *homogenizací* polynomu f .

Definice 1.27 (Dehomogenizace). Pro polynom $f \in K[x_1, \dots, x_{n+1}]$ definujeme $f_* = f(x_1, \dots, x_n, 1)$. Tento proces nazveme *dehomogenizací* polynomu f .

Definice 1.28 (Projektivní nula). $P = [p_1 : \dots : p_{n+1}]$ je *projektivní nula* f , jestliže $f(\lambda p_1, \dots, \lambda p_{n+1}) = 0 \ \forall \lambda \in K$.

Pokud je f forma stupně i , pak $f(\lambda p_1, \dots, \lambda p_{n+1}) = \lambda^i f(p_1, \dots, p_{n+1})$. Tedy bod je projektivní nulou f právě tehdy, když je nulou f ve smyslu definice 1.5.

Definice 1.29 (Projektivní algebraická množina). Pro množinu polynomů $S \subseteq K[\bar{x}]$ definujeme

$$V_p(S) = \{P \in \mathbb{P}^n(K) \mid P \text{ je projektivní nula } f \ \forall f \in S\}.$$

Množina $X \subseteq \mathbb{P}^n(K)$ je *projektivní algebraická množina*, pokud $X = V_p(S)$ pro nějaké $S \subseteq K[\bar{x}]$.

Stejně jako u afinního prostoru můžeme i zde definovat Zariského topologii jako topologii na $\mathbb{P}^n(K)$ takovou, že projektivní algebraické množiny jsou uzavřené.

Definice 1.30 (Projektivní algebraická křivka). Množina $X \subseteq \mathbb{P}^2(K)$ je *projektivní algebraická křivka*, pokud $X = V(f)$, kde $f \in K[x, y, z]$ je forma stupně $d > 0$.

Definice 1.31 (Ideál množiny). Pro množinu $X \subseteq \mathbb{P}^n(K)$ definujeme *ideál* $I_P(X) = \{f \in K[\bar{x}] \mid f(P) = 0 \ \forall P \in X\}$.

Definice 1.32 (Projektivní varieta). Neprázdná ireducibilní projektivní algebraická množina se nazývá *projektivní varieta*.

Definice 1.33 (Homogenizace ideálu). Pro $I \subseteq K[x_1, \dots, x_n]$ ideál definujeme $I^* = (f^* : f \in I)$. Tento proces nazveme *homogenizace ideálu*.

Pokud $I = (f)$ je hlavní ideál, pak jeho homogenizace je generovaná homogenizací jeho generátoru, tedy $I^* = (f^*)$.

Obecně tato vlastnost neplatí. Pokud máme ideál $I = (f_1, \dots, f_k)$, pak I^* se nemusí rovnat $(f_1^*, \dots, f_k^*)$. Obojí najdeme ve Fultonově knize (Fulton, 2008, Kapitola 4.3).

Definice 1.34 (Projektivní uzávěr). Pro algebraickou množinu $X \subseteq \mathbb{A}^n(K)$ definujeme *projektivní uzávěr* X jako $X^* = V_p(I(X)^*)$.

Po ztotožnění $\mathbb{A}^n(K)$ s podmnožinou $\mathbb{P}^n(K)$ je projektivní uzávěr množiny její uzávěr v projektivní Zariského topologii, viz Cox, Little a O'Shea (2007, Kapitola 4, Proposition 7).

Definice 1.35 (Dehomogenizace ideálu). Pro ideál $I \subseteq K[x_1, \dots, x_n]$ definujeme $I_* = (f_* : f \in I)$. Tento proces nazveme *dehomogenizace ideálu*.

Definice 1.36 (Afinní část). Pro algebraickou množinu $X \subseteq \mathbb{P}^n(K)$ definujeme *afinní část* X jako $X_* = V(I_p(X)_*)$.

Definice 1.37 (Projektivní změna souřadnic). Nechť $A = (a_1, \dots, a_{n+1}) \in \mathbb{A}^{n+1}$ a $T : \mathbb{A}^{n+1} \rightarrow \mathbb{A}^{n+1}$ je bijektivní lineární zobrazení, pro které $T(a_1, \dots, a_n) = (T_1(A), \dots, T_n(A))$. Pak zobrazení $T : \mathbb{P}^n \rightarrow \mathbb{P}^n$, které zobrazí $[a_1 : \dots : a_{n+1}]$ na $[T_1(A) : \dots : T_n(A)]$ se nazývá *projektivní změna souřadnic*.

Projektivní změna souřadnic je dobře definovaná, protože T_i jsou formy stejné stupně jedna.

Definice 1.38 (Morfismus). Nechť $V \subseteq \mathbb{P}^n(K)$, $W \subseteq \mathbb{P}^m(K)$ jsou projektivní variety. Zobrazení $\varphi : V \rightarrow W$ je *morfismus* projektivních variet, pokud $\forall A \in V$ existuje Zariski otevřená podmnožina U , $A \in U \subseteq V$, taková, že $\forall B \in U$ platí $\varphi|_U([B]) = [f_1(B) : \dots : f_m(B)]$ pro nějaké $f_1, \dots, f_m$ formy stejného stupně.

Definice 1.39 (Izomorfismus projektivních variet). Projektivní variety V a W jsou *izomorfní*, pokud existuje bijektivní morfismus $\varphi : V \rightarrow W$ takový, že $\varphi^{-1} : W \rightarrow V$ je také morfismus.

2. Ponceletovo porisma

2.1 Znění

Definice 2.1 (Kuželosečka). Projektivní algebraická křivka se nazývá *kuželosečka*, pokud je určena formou stupně dva. Kuželosečka je *nedegenerovaná*, pokud jde o ireducibilní křivku.

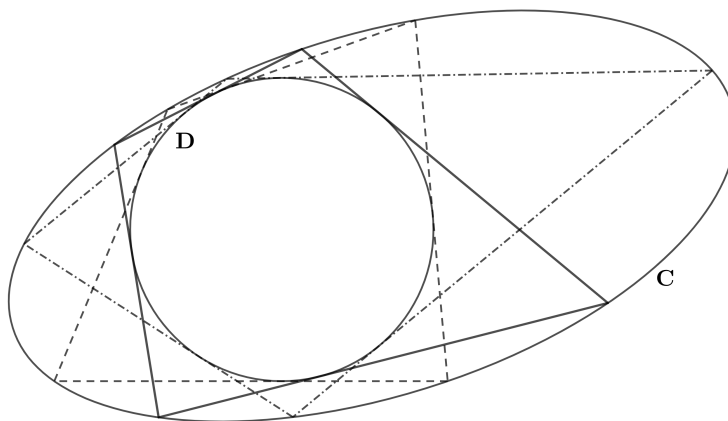
Kuželosečka je tedy množina bodů $[x : y : z]$ splňujících $Ax^2 + Bxy + Cy^2 + Dxz + Eyz + Fz^2 = 0$. Tuto rovnost můžeme zapsat i pomocí symetrické matice

$$\begin{pmatrix} x & y & z \end{pmatrix} \begin{pmatrix} A & B/2 & D/2 \\ B/2 & C & E/2 \\ D/2 & E/2 & F \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0.$$

Tento maticový pohled využijeme v sekci 2.2. Pro jednoduchost budeme o kuželosečce určené maticí M mluvit jako o kuželosečce M .

Znění následující věty je přeloženo z článku *Poring over Poncelet* (Nash, 2018).

Věta 2.2 (Ponceletovo porisma). *Nechť $\mathbf{C}$, $\mathbf{D}$ jsou dvě nedegenerované kuželosečky v komplexní projektivní rovině se čtyřmi různými průniky a $n \geq 3$ přirozené číslo. Pokud existuje n -úhelník takový, že všechny jeho vrcholy leží na $\mathbf{C}$ a všechny jeho strany jsou tečné k $\mathbf{D}$, pak pro libovolný bod $\mathbf{C}$ existuje takový n -úhelník s vrcholem v tomto bodě.*



Obrázek 2.1: Ukázka Ponceletova porismatu

Z Bézoutovy věty (viz Fulton, 2008, Kapitola 5.3) plyne, že dvě kuželosečky v komplexní projektivní rovině mají přesně čtyři průniky včetně násobnosti. V této práci formulujeme a dokazujeme Ponceletovo porisma pro případ, kdy žádný z průníků není násobný. Ve skutečnosti porisma platí i pro nedegenerované kuželosečky s násobnými průniky, ale touto situací se v této práci zabývat nebudeme.

2.2 Převod kuželoseček na soustřednou kružnici a elipsu

Obsah této sekce nebyl odnikud převzat, původní inspirací pro sepsání byla část 2 z Schoenberg (1983).

Cílem této sekce je ukázat, že každé dvě nedegenerované kuželosečky v komplexní projektivní rovině se čtyřmi různými průniky můžeme projektivní změnou souřadnic převést na soustřednou kružnici a elipsu.

2.2.1 Jedna kuželosečka

Nejdřív se vypořádáme s jednou nedegenerovanou kuželosečkou. Ukážeme, že pokud vezmeme libovolný bod projektivní roviny, který na ní neleží, umíme najít projektivní změnu souřadnic, která zobrazí tento bod na střed zobrazené kuželosečky. Středem myslíme bod, podle kterého je kuželosečka středově souměrná, neboli pokud afinní bod X leží na kuželosečce se středem O , pak $2O - X$ leží na kuželosečce také.

Definice 2.3 (Polára a pól). *Polára* bodu $\mathbf{u}$ vzhledem ke kuželosečce dané maticí M je přímka $\{\mathbf{v} \mid \mathbf{u}^T M \mathbf{v} = 0\}$. Naopak $\mathbf{u}$ je *pól* přímky vzhledem k dané kuželosečce, pokud je tato přímka jeho polárou.

Mějme kuželosečku a libovolný bod, který na ní neleží. Vezmeme projektivní změnu souřadnic, která zobrazí tento bod na $[0 : 0 : 1]$ a jeho poláru na přímku v nekonečnu. Taková projektivní změna souřadnic jistě existuje, v další sekci dokážeme dokonce něco silnějšího. Ukážeme, že projektivní změna souřadnic zachovává vztah pólu a poláry a že pól přímky v nekonečnu vzhledem ke kuželosečce, tedy bod $[0 : 0 : 1]$, je střed této kuželosečky. Pak budeme mít zobrazení, které z libovolného bodu udělá střed zobrazené kuželosečky. Zobrazenou kuželosečku budeme nazývat M .

Lemma 2.4. *Projektivní změna souřadnic zachovává vztah pólu a poláry.*

Důkaz. Pro zobrazenou kuželosečku M projektivní změnou souřadnic určenou maticí T je původní zobrazovaná kuželosečka dána maticí $T^T M T$. Bod $\mathbf{u}$ byl bodem původní kuželosečky, tedy $\mathbf{u}^T (T^T M T) \mathbf{u} = 0$, právě tehdy, když $T\mathbf{u}$ je bod kuželosečky M , tedy $(T\mathbf{u})^T M (T\mathbf{u}) = 0$.

Přímka p je polára bodu $\mathbf{u}$ vzhledem ke kuželosečce $T^T M T$, tedy $p = \{\mathbf{v} \mid \mathbf{u}^T (T^T M T) \mathbf{v} = 0\}$, právě tehdy, když je přímka TP polára bodu $T\mathbf{u}$ vzhledem ke kuželosečce M , tedy $\{T\mathbf{v} \mid (T\mathbf{u})^T M (T\mathbf{v}) = 0\}$. $\square$

Lemma 2.5. *Bod $[0 : 0 : 1]$, jehož polára je přímka v nekonečnu, je střed kuželosečky M .*

Důkaz. Nevlastní přímku můžeme zapsat jako množinu $\{\mathbf{v} \mid (0 \ 0 \ 1) \cdot \mathbf{v} = 0\}$. Polára k $[0 : 0 : 1]$ je z definice $\{\mathbf{v} \mid (0 \ 0 \ 1) M \mathbf{v} = 0\}$, což je v našem případě právě nevlastní přímka, tedy tyto dvě množiny se rovnají. Takže $(0 \ 0 \ 1) M$ i $(0 \ 0 \ 1)$ jsou normálové vektory téže roviny v $\mathbb{A}^3$, neboli $(0 \ 0 \ 1) M = (0 \ 0 \ k)$ pro nějaké k nenulové.

Označme $\mathbf{e} = (0 \ 0 \ 1)^T$. Že je $[0 : 0 : 1]$ střed M znamená, že pokud $\mathbf{e} + \mathbf{v}$ leží na M , tak i $\mathbf{e} - \mathbf{v}$ leží na M pro $\mathbf{v} = (x \ y \ 0)^T$.

Máme $2\mathbf{e}^T M \mathbf{v} = 2(0 \ 0 \ 1)M \cdot (x \ y \ 0)^T = 2(0 \ 0 \ k) \cdot (x \ y \ 0)^T = 0 = -2\mathbf{e}^T M \mathbf{v}$.
Tudíž

$$\begin{aligned} (\mathbf{e} + \mathbf{v})^T M (\mathbf{e} + \mathbf{v}) &= \mathbf{e}^T M \mathbf{e} + 2\mathbf{e}^T M \mathbf{v} + \mathbf{v}^T M \mathbf{v} \\ &= \mathbf{e}^T M \mathbf{e} - 2\mathbf{e}^T M \mathbf{v} + \mathbf{v}^T M \mathbf{v} = (\mathbf{e} - \mathbf{v})^T M (\mathbf{e} - \mathbf{v}). \end{aligned}$$

Takže $\mathbf{e} + \mathbf{v}$ leží na M právě tehdy, když $\mathbf{e} - \mathbf{v}$ leží na M , tedy $[0 : 0 : 1]$ je opravdu střed kuželosečky M . $\square$

2.2.2 Soustředná kuželosečka s kružnicí

Nyní mějme v projektivní rovině dvě kuželosečky, které nemají žádný násobný průnik. Pokud existuje bod, pro který je polára vzhledem k oběma kuželosečkám ta samá přímka, můžeme tento bod projektivní změnou souřadnic zobrazit na $[0 : 0 : 1]$ a přímku na přímku v nekonečnu. Tím získáme dvě soustředné kuželosečky se středem v $[0 : 0 : 1]$.

Takový bod existuje, protože každá spojitá funkce z projektivního prostoru nad $\mathbb{C}$ sudé dimenze do sebe sama má pevný bod, důkaz nalezneme v článku Taghavi (2015). Zobrazení, které bod projektivního prostoru zobrazí na jeho poláru k první kuželosečce a následně na pól této poláry vzhledem k druhé, je jako složení dvou lineárních zobrazení spojitě. Zároveň hledaný bod na kuželosečkách neleží, jinak by jeho polára vzhledem k oběma kuželosečkám byla společná tečna, ale naše kuželosečky nemají násobný průnik. Tedy hledaný bod neleží ani na poláře.

Můžeme to ale udělat ještě lépe a jednu z kuželoseček zobrazit rovnou na jednotkovou kružnici. Zatím jsme vzali bod, řekněme mu P , pro který je polára k oběma kuželosečkám stejná přímka, ten jsme zobrazili na $[0 : 0 : 1]$ a příslušnou přímku na přímku v nekonečnu.

Nyní si vezmeme přísnější podmínky. Stále chceme, aby se bod P zobrazil na $[0 : 0 : 1]$. Dále budeme požadovat, aby se průsečíky první kuželosečky s polárou P zobrazily na $[i : \pm 1 : 0]$, pak se polára zobrazí na přímku v nekonečnu. Bod P a průsečíky poláry s první kuželosečkou neleží na jedné přímce, jak jsme zdůvodnili výše.

K těmto třem bodům najdeme čtvrtý bod ležící na první kuželosečce takový, že žádné tři z nich neleží na přímce. Takový bod jistě existuje, protože tuto podmínku nespĺňuje jen konečně bodů kuželosečky. Tento bod chceme zobrazit na takový bod jednotkové kružnice, aby spolu s body $[0 : 0 : 1]$ a $[i : \pm 1 : 0]$ žádné tři z nich neležely na přímce. Obraz první kuželosečky bude kružnice z následujícího důvodu. Každá kružnice má nevlastní body $[i : \pm 1 : 0]$, zobrazená první kuželosečka má nějaké tři reálné body, kterým můžeme opsat kružnici, takže máme pět bodů, které leží jak na kružnici, tak na zobrazené první kuželosečce, ta tedy musí být z Bézoutovy věty kružnice a díky definici zobrazení čtvrtého bodu dokonce jednotková.

Že existuje projektivní změna souřadnic, která zobrazí zmíněné čtyři body požadovaným způsobem, plyne z následujícího tvrzení.

Tvrzení 2.6. *Mějme v $\mathbb{P}^2(\mathbb{C})$ body A, B, C, D z nichž žádné tři neleží na přímce a body A', B', C', D' z nichž také žádné tři neleží na přímce. Pak existuje projektivní změna souřadnic T taková, že $T(A) = A', T(B) = B', T(C) = C', T(D) = D'$.*

Důkaz. Označme $A = [x_A : y_A : z_A]$, $B = [x_B : y_B : z_B]$, $C = [x_C : y_C : z_C]$, $D = [x_D : y_D : z_D]$. Vyřešíme lineární soustavu rovnic

$$\begin{pmatrix} x_A & x_B & x_C \\ y_A & y_B & y_C \\ z_A & z_B & z_C \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ \gamma \end{pmatrix} = \begin{pmatrix} x_D \\ y_D \\ z_D \end{pmatrix}.$$

Protože A, B, C neleží na přímce, řešení existuje. Zároveň α, β, γ vyjdou nenulové, protože žádné tři z bodů A, B, C, D neleží na přímce. Označme S matici projektivní změny souřadnic

$$S = \begin{pmatrix} \alpha x_A & \beta x_B & \gamma x_C \\ \alpha y_A & \beta y_B & \gamma y_C \\ \alpha z_A & \beta z_B & \gamma z_C \end{pmatrix}.$$

Zobrazení S zobrazí $[1 : 0 : 0]$, $[0 : 1 : 0]$, $[0 : 0 : 1]$, $[1 : 1 : 1]$ postupně na A, B, C, D . Analogicky získáme matici zobrazení R , které zobrazí $[1 : 0 : 0]$, $[0 : 1 : 0]$, $[0 : 0 : 1]$, $[1 : 1 : 1]$ postupně na A', B', C', D' . Matice výsledného zobrazení T tedy bude $T = RS^{-1}$. $\square$

2.2.3 Diagonalizace

Nyní máme dvě kuželosečky se společným středem v $[0 : 0 : 1]$, první je jednotková kružnice, druhá je určena maticí 3×3 s nulovým třetím řádkem i třetím sloupcem kromě prvku na diagonále. Zbývá říct, že existuje projektivní změna souřadnic, která z druhé matice udělá matici diagonální a přitom se druhá kuželosečka i soustřednost zachová. K tomu použijeme následující tvrzení.

Tvrzení 2.7. *Mějme nedegenerované kuželosečky určené maticemi A, B se čtyřmi různými průniky, pak $B^{-1}A$ má tři různá vlastní čísla.*

Důkaz. Mějme čtyři různé body průniků A a B . Pak žádné tři z těchto bodů neleží na přímce, protože přímka se s kuželosečkou protíná maximálně ve dvou bodech. To znamená, že existují právě tři různé dvojice přímk takové, že všechny čtyři body leží na některé z přímk z této dvojice.

Teď ukážeme, že pro každou možnou dvojici existuje odpovídající vlastní číslo matice $B^{-1}A$ a protože máme tři různé dvojice, má $B^{-1}A$ tři různá vlastní čísla.

Vezmeme si libovolnou z našich tří dvojic přímk. Ta patří do množiny afinních kombinací $\mu A + \xi B$, kde alespoň jedno z $\mu, \xi \in \mathbb{C}$ je nenulové, z následujícího důvodu. Označme průsečík vybrané dvojice přímk X , hodnotu A v X a a hodnotu B v X b , pak $bA - aB$ bude mít v X hodnotu nula a ve čtyřech průsečících A a B také. Čili se kuželosečka $bA - aB$ protíná s každou z přímk z vybrané dvojice ve třech bodech, a proto je musí podle Bézoutovy věty mít za komponentu. To znamená, že vybraná dvojice přímk je určena maticí $bA - aB$.

Jelikož A, B jsou nedegenerované, platí $a, b \neq 0$, a tak pro nějaké λ můžeme tuto dvojici přímk zapsat maticí $A - \lambda B$ a jelikož dvojice přímk je degenerovaná kuželosečka, $A - \lambda B$ musí být singulární.

Protože B je regulární matice, tak $\det(A - \lambda B) = 0$ právě tehdy, když $0 = \det(B^{-1}(A - \lambda B)) = \det(B^{-1}A - \lambda I)$. Neboli λ je vlastní číslo $B^{-1}A$ právě tehdy, když $(A - \lambda B)$ je singulární.

To znamená, že λ je vlastní číslo $B^{-1}A$. Naše tři dvojice přímk jsou různé, tudíž i odpovídající lineární kombinace, kterými je dostaneme, jsou různé, a tak $B^{-1}A$ má tři různá vlastní čísla. $\square$

Nyní tvrzení využijeme na naše dvě kuželosečky. Matice B z tvrzení bude matice určující jednotkovou kružnici, matice A má nulový třetí řádek i třetí sloupec kromě prvku na diagonále a chceme ji diagonalizovat. Z tvrzení víme, že $B^{-1}A$ má tři různá vlastní čísla. Tedy z výpočtu vlastních čísel pomocí charakteristického polynomu plyne, že její horní podmatice 2×2 , kterou označíme C , má dvě různá vlastní čísla, tedy je diagonalizovatelná.

Matice C je dokonce ortogonálně diagonalizovatelná. Pokud $\mathbf{x}, \mathbf{y}$ jsou vlastní vektory C příslušné vlastním číslům λ a μ , pak

$$\mu \mathbf{x}^T \mathbf{y} = \mathbf{x}^T (\mu \mathbf{y}) = \mathbf{x}^T C \mathbf{y} = \mathbf{x}^T C^T \mathbf{y} = (\lambda \mathbf{x}^T) \mathbf{y} = \lambda \mathbf{x}^T \mathbf{y}.$$

Tedy $\mathbf{x}^T \mathbf{y} = 0$, neboli $\mathbf{x}, \mathbf{y}$ tvoří ortogonální bázi.

Tuto bázi rozšíříme přidáním nuly na třetí pozici do $\mathbb{C}^3$ a přidáme vektor $(0 \ 0 \ 1)^T$. Tyto tři vektory budou tvořit ortogonální bázi $\mathbb{C}^3$, ve které jsou matice A, B diagonální. Po projektivní změně souřadnic určené maticí změny báze se hodnota A, B nezmění, neboť násobíme regulární maticí. Proto po vhodném znormování získáme matici jednotkové kružnice a diagonální matici s ní soustředné elipsy.

Ve zbytku práce tak budeme jako kuželosečky $\mathbf{C}, \mathbf{D}$ ze znění Ponceletova porismatu (Věta 2.2) uvažovat jednotkovou kružnici a elipsu s délkami poloos $a, b \in \mathbb{C} \setminus \{0\}$, obojí se středy v počátku souřadnic $\mathbb{A}^2(\mathbb{C})$ (podle sekce 1.5).

$$\begin{aligned} \mathbf{C} &= \left\{ [x_1 : y_1 : z_1] \mid \left(\frac{x_1}{a}\right)^2 + \left(\frac{y_1}{b}\right)^2 = z_1^2 \right\} \\ \mathbf{D} &= \left\{ [x_2 : y_2 : z_2] \mid x_2^2 + y_2^2 = z_2^2 \right\} \end{aligned}$$

2.3 Reformulace problému

Tato sekce je sepsána na základě začátku kapitoly *Griffiths and Harris proof* z článku Nash (2018).

Definujme $N' = \{(p, q) \in \mathbf{C} \times \mathbf{D} \mid p \text{ leží na tečně k } \mathbf{D} \text{ v bodě } q\}$.

Tečna k projektivní algebraické křivce $V(f)$, $f \in \mathbb{C}[x, y, z]$ v nesesingulárním bodě $P \in V(f)$ je $V\left(\frac{\partial f}{\partial x}(P)x + \frac{\partial f}{\partial y}(P)y + \frac{\partial f}{\partial z}(P)z\right)$ (Fulton, 1984, Kapitola 1.2). Takže pro $p = [x_1 : y_1 : z_1]$ a $q = [x_2 : y_2 : z_2]$ můžeme N' algebraicky zapsat jako

$$N' = \left\{ ([x_1 : y_1 : z_1], [x_2 : y_2 : z_2]) \mid \left(\frac{x_1}{a}\right)^2 + \left(\frac{y_1}{b}\right)^2 = z_1^2, x_2^2 + y_2^2 = z_2^2, x_1 x_2 + y_1 y_2 = z_1 z_2 \right\}.$$

Obecným bodem $p \in \mathbf{C}$ prochází dvě tečny k $\mathbf{D}$ (např. opět podle knihy Fulton, 1984, Kapitola 1.2). Tudíž máme na N' přirozenou involuci $i_D : N' \rightarrow N'$, která zobrazí (p, q) na (p, q') , kde $q' \in \mathbf{D}$ leží na druhé tečně k $\mathbf{D}$ z bodu p než

q . Body (p, q) , $p \in \mathbf{C} \cap \mathbf{D}$, prochází jediná tečna k $\mathbf{D}$. Takové body jsou přesně pevné body involuce i_D .

Také na každé tečně k $\mathbf{D}$ leží právě dva body z $\mathbf{C}$. Tím získáme druhou involuci $i_C : N' \rightarrow N'$ přehazující body p na stejné tečně. Složení involucí označíme $T = i_D \circ i_C : N' \rightarrow N'$.

Ponceletovo porisma říká přesně to, že T^n má pevný bod právě tehdy, když je to identické zobrazení.

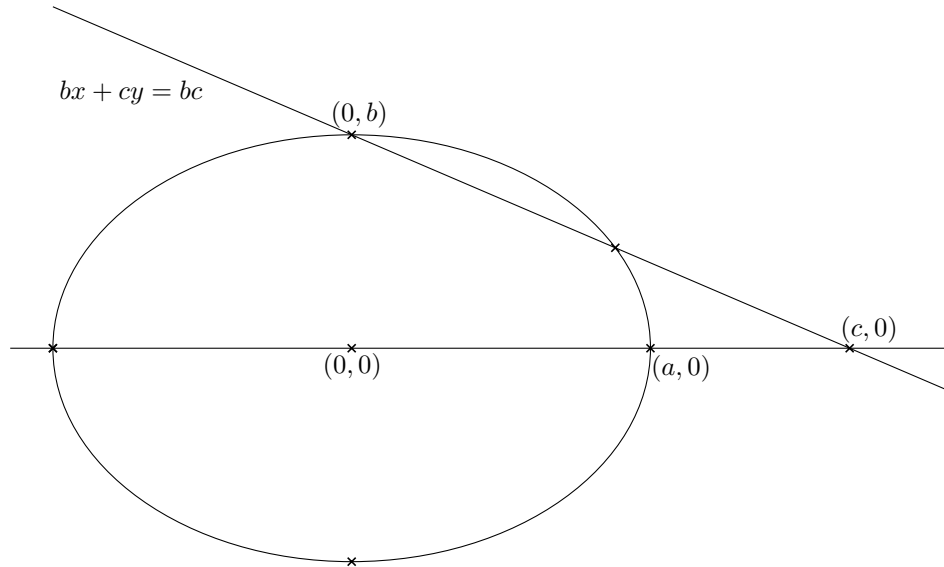
Dále dokážeme, že N' je eliptická křivka, na které máme grupovou strukturu. Stačí tedy ukázat, že T je vzhledem k této grupové struktuře translace, neboli existuje $s \in N'$ takové, že T zobrazí každý prvek $r \in N'$ na $r + s$. Pak i T^n bude translace a jediná translace s pevným bodem je identické zobrazení.

Nejdřív se pustíme do zdůvodnění, proč je N' eliptická křivka a to tak, že pomocí sekcí 2.4–2.11 ukážeme, že N' je izomorfní známému tvaru eliptické křivky. K výše zmíněným involucím se vrátíme v sekci 2.12.

2.4 Stereografická projekce

Mějme v $\mathbb{A}^2(\mathbb{C})$ elipsu s rovnicí $(\frac{x}{a})^2 + (\frac{y}{b})^2 = 1$, neboli afinní část $\mathbf{C}$. Nyní ukážeme zobrazení přímky na tuto elipsu a následně naopak zobrazení elipsy na přímku. Práce s afinní částí kružnice $\mathbf{D}$ je speciálním případem pro $a = b = 1$. Tyto křivky budeme v souladu s definicí 1.36 značit $\mathbf{C}_*$ a $\mathbf{D}_*$. Toto značení využijeme hlavně v sekci 2.7.

2.4.1 Zobrazení přímky na elipsu



Obrázek 2.2: Zobrazení přímky na elipsu v $\mathbb{R}$

Nejdřív zobrazíme přímku $y = 0$ na elipsu. Bod $(0,0)$ zobrazíme na vrchol elipsy $(0, -b)$.

Zvolme bod $(c, 0)$, $c \neq \pm ia$, 0 na přímce $y = 0$. Naše zobrazení přiřadí tomuto bodu takový bod elipsy, který zároveň leží na přímce určené bodem $(c, 0)$

a vrcholem elipsy $(0, b)$, neboli na přímce s rovnicí $bx + cy = bc$. Po dosazení za y z rovnice přímky do rovnice elipsy máme

$$\frac{x^2}{a^2} + \frac{b^2 x^2}{c^2 b^2} - \frac{2b^2 cx}{c^2 b^2} = 0 \Rightarrow \frac{x^2}{a^2} + \frac{x^2}{c^2} - \frac{2x}{c} = 0.$$

A jelikož $x \neq 0$, neboť hledáme druhý průsečík přímky s elipsou než vrchol $(0, b)$, dostáváme

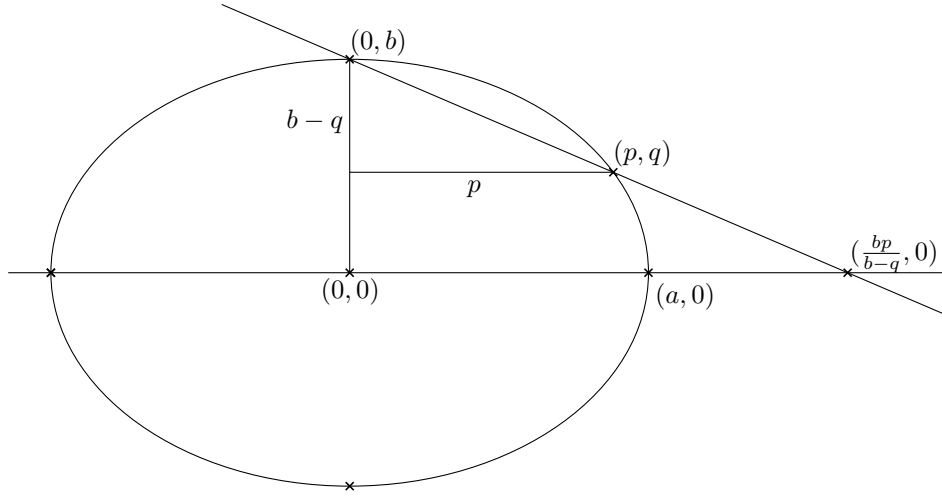
$$x = \frac{2a^2 c}{c^2 + a^2}, y = \frac{b(c^2 - a^2)}{c^2 + a^2}.$$

Všimněme si, že toto vyjádření dává smysl i pro $c = 0$ a obraz $(0, 0)$ vychází opět $(0, -b)$.

Provedeme substituci $s = \frac{c}{a}$, $s \in \mathbb{C} \setminus \{\pm i\}$ a definujeme zobrazení z komplexních čísel na elipsu

$$s \rightarrow \left(\frac{2as}{s^2 + 1}, \frac{b(s^2 - 1)}{s^2 + 1} \right). \quad (2.1)$$

2.4.2 Zobrazení elipsy na přímku



Obrázek 2.3: Stereografická projekce elipsy v $\mathbb{R}$

Nyní naopak elipsu promítneme na přímku $y = 0$. Bod elipsy (p, q) , $q \neq b$, zobrazíme na průsečík přímky $y = 0$ a přímky určené bodem (p, q) a vrcholem elipsy $(0, b)$. Tedy (p, q) se zobrazí na $(\frac{bp}{b-q}, 0)$. Definujme zobrazení z elipsy na komplexní čísla

$$(p, q) \rightarrow \frac{bp}{a(b - q)}.$$

Do vzorce jsme přidali a kvůli zmíněné substituci, takto budou toto zobrazení a zobrazení 2.1 vzájemně inverzní.

2.4.3 Převod N na M

Stereografickou projekci z komplexních čísel na jednotkovou kružnici získáme z předchozího dosazením $a = 1$ a $b = 1$. Pak pro $t \in \mathbb{C} \setminus \{\pm i\}$ máme

$$t \rightarrow \left(\frac{2t}{t^2 + 1}, \frac{t^2 - 1}{t^2 + 1} \right).$$

Uvažujme N afinní verzi N' ,

$$N = \left\{ ((x_1, y_1), (x_2, y_2)) \left| \left(\frac{x_1}{a} \right)^2 + \left(\frac{y_1}{b} \right)^2 = 1, x_2^2 + y_2^2 = 1, x_1 x_2 + y_1 y_2 = 1 \right. \right\}.$$

Pomocí stereografické projekce můžeme N zjednodušit tak, že x_1, y_1, x_2, y_2 nahradíme s, t a zachováme poslední rovnici určující, že bod kružnice a elipsy leží na tečně ke kružnici.

Pro zvolené t má tečna ke kružnici v bodě $\left(\frac{2t}{t^2+1}, \frac{t^2-1}{t^2+1} \right)$ rovnici $\frac{2t}{t^2+1}x + \frac{t^2-1}{t^2+1}y - 1 = 0$. Dosadíme-li vyjádření soustředné elipsy $x = \frac{2as}{s^2+1}$ a $y = \frac{b(s^2-1)}{s^2+1}$, dostaneme

$$\frac{4ast}{(s^2+1)(t^2+1)} + \frac{b(s^2-1)(t^2-1)}{(s^2+1)(t^2+1)} - 1 = 0.$$

Získali jsme

$$M = \left\{ (s, t) \in \mathbb{C}^2 \mid 4ast + b(s^2-1)(t^2-1) - (s^2+1)(t^2+1) = 0 \right\}.$$

Přestože jsme u zobrazení z přímky na elipsu a kružnici uvažovali $s, t \neq \pm i$, v definici M nám tyto body nevadí, k vysvětlení se dostaneme v sekci 2.7.

2.5 Ireducibilita M

Označme

$$\begin{aligned} f &= 4ast + b(s^2-1)(t^2-1) - (s^2+1)(t^2+1) \\ &= \left(-(s^2+1) + b(s^2-1) \right) t^2 + (4as)t + \left(-(s^2+1) - b(s^2-1) \right). \end{aligned}$$

Pokud je f ireducibilní polynom nad $\mathbb{C}$, pak $M = V(f)$ je podle tvrzení 1.14 afinní varieta.

Věta 2.8 (Gaussovo lemma). *Bud' R gaussovský obor a K jeho podílové těleso. Ireducibilní prvky v $R[x]$ jsou právě*

- *prvočinitele $p \in R$ a*
- *primitivní nekonstantní polynomy $g \in R[x]$, které jsou ireducibilní jako prvky $K[x]$.*

Důkaz. Viz Kala (2020). □

Pro $R = \mathbb{C}[s]$ a $K = \mathbb{C}(s)$ máme, že f je ireducibilní v $\mathbb{C}[s][t]$, právě když je primitivní a ireducibilní jako prvek $\mathbb{C}(s)[t]$. Tedy se stačí podívat na primitivitu $f \in \mathbb{C}[s][t]$ a ireducibilitu $f \in \mathbb{C}(s)[t]$.

Lemma 2.9. *Polynom $f \in \mathbb{C}[s][t]$ je primitivní.*

Důkaz. Připomeňme, že $a, b \in \mathbb{C} \setminus \{0\}$. Primitivita znamená, že NSD koeficientů má být jedna. Nám stačí vzít pouze koeficienty konstantního a kvadratického členu.

$$\begin{aligned} & NSD(-(s^2 + 1) - b(s^2 - 1), -(s^2 + 1) + b(s^2 - 1)) \\ &= NSD(-(s^2 + 1) - b(s^2 - 1), 2b(s^2 - 1)) \\ &= NSD(-(s^2 + 1), 2b(s^2 - 1)) = NSD(-(s^2 + 1), -4b) = 1 \end{aligned}$$

Zde využíváme Eukleidův algoritmus a to, že NSD je určen až na asociovanost, takže násobky z $\mathbb{C}$ nemusíme řešit. $\square$

Lemma 2.10. *Jako polynom v t je f ireducibilní nad $\mathbb{C}(s)$ právě tehdy, když jsou splněny podmínky $(\star)$ $a \neq \pm 1$, $b \neq \pm 1$ a $a \neq \pm b$.*

Důkaz.

$$f = \left(-(s^2 + 1) + b(s^2 - 1) \right) t^2 + (4as) t + \left(-(s^2 + 1) - b(s^2 - 1) \right)$$

Jako polynom v proměnné t je f kvadratický, rozkládá se tedy právě tehdy, když jeho diskriminant D je čtverec.

$$D = 4((b^2 - 1)s^4 + (-2 + 4a^2 - 2b^2)s^2 + (b^2 - 1)) \quad (2.2)$$

Předně pokud $b = \pm 1$, pak D je čtverec. Dál předpokládejme, že $b \neq \pm 1$, to znamená, že vedoucí koeficient $D(s)$ je nenulový. D je čtverec právě tehdy, když existují α, β, γ takové, že

$$D = (\alpha s^2 + \beta s + \gamma)^2 = \alpha^2 s^4 + 2\alpha\beta s^3 + (2\alpha\gamma + \beta^2)s^2 + 2\beta\gamma s + \gamma^2.$$

Po porovnání s 2.2 vidíme, že $\alpha = \pm 2\sqrt{b^2 - 1} \neq 0$, $\gamma = \pm 2\sqrt{b^2 - 1}$, a tedy $\beta = 0$. Porovnáním kvadratických členů dostáváme $4(-2 + 4a^2 - 2b^2) = 2\alpha\gamma = \pm 8(b^2 - 1)$.

$$\begin{aligned} -2 + 4a^2 - 2b^2 &= 2(b^2 - 1) & -2 + 4a^2 - 2b^2 &= -2(b^2 - 1) \\ 4a^2 &= 4b^2 & 4a^2 - 4 &= 0 \\ a &= \pm b & a &= \pm 1 \end{aligned}$$

Zjistili jsme, že f je ireducibilní nad $\mathbb{C}(s)$ právě tehdy, když jsou splněny podmínky $(\star)$. $\square$

Podle Gaussova lemmatu je f ireducibilní nad $\mathbb{C}$ právě při splnění podmínek $(\star)$. Pak je tedy ireducibilní i M . Jinak řečeno, při splnění podmínek $(\star)$ je M afinní varieta.

Situace $a = \pm 1$ ani $b = \pm 1$ nemůžou nastat, poněvadž v takovém případě by měla elipsa s jednotkovou kružnicí násobné průniky a my jsme uvažovali případ, kdy mají kuželosečky průniky čtyři různé.

Pokud $a = b \neq \pm 1$, pak máme dvě soustředné kružnice s rovnicemi $x^2 + y^2 = 1$, $x^2 + y^2 = a^2$. Po odečtení druhé rovnice od první dostáváme $0 = 1 - a^2$, ale $a \neq \pm 1$, tudíž tyto kružnice nemají v afinní komplexní rovině žádný průnik. Obě kružnice mají dva body v nekonečnu $[i : \pm 1 : 0]$. Z Bézoutovy věty (Fulton, 2008, Kapitola 5.3) plyne, že aspoň jeden z průníků je násobný. V našem případě tedy dvě soustředné kružnice neuvažujeme, i když není těžké ukázat, že i pro ně Ponceletovo porisma platí.

Ve zbytku práce můžeme předpokládat, že M je afinní varieta.

2.6 Převedení M do projektivní variety

V této sekci budeme pracovat s prostorem $\mathbb{P}^1 \times \mathbb{P}^1$, což je takzvaný multi-projektivní prostor. O těchto prostorech pojednává kapitola 4.4 v knize Fulton (2008).

Afinní varietu M vnoříme do multiprojektivního prostoru $\mathbb{P}^1 \times \mathbb{P}^1$ pomocí zobrazení $(s, t) \rightarrow ([s : 1], [t : 1])$. Uzávěr obrazu v Zariského topologii nazveme M' . Ukážeme, že když byla M afinní varieta, M' je projektivní varieta.

Tvrzení 2.11. *Nechť X, Y jsou topologické prostory, $g : X \rightarrow Y$ je spojitý a $A \subseteq X$ je ireducibilní, pak $\overline{g(A)} \subseteq Y$ je též ireducibilní.*

Důkaz. Předpokládejme, že $\overline{g(A)} = B \cup C$, kde B a C jsou uzavřené. Jelikož g je spojitý, $g^{-1}(B)$ a $g^{-1}(C)$ jsou uzavřené množiny pokrývající A . A je ireducibilní, tudíž buď $g^{-1}(B) = A$ nebo $g^{-1}(C) = A$. Bez újmy na obecnosti předpokládejme, že $g^{-1}(B) = A$.

$$B \subseteq \overline{g(A)} = \overline{g(g^{-1}(B))} \subseteq B$$

Tedy $B = \overline{g(A)}$ a tudíž $\overline{g(A)}$ je ireducibilní. $\square$

Vnoření je spojitý zobrazení, tudíž M' je projektivní varieta. Ideál $I(M)$ je hlavní, díky analogii k definici 1.34 a poznámce nad ní získáme M' z M homogenizací f v obou souřadnicích. Varieta M' je tvaru

$$M' = \left\{ ([s : r], [t : u]) \mid 4asrtu + b(s^2 - r^2)(t^2 - u^2) = (s^2 + r^2)(t^2 + u^2) \right\}.$$

2.7 Izomorfismus elipsy a přímky

Ze sekce 2.4 plyne, že elipsa $\mathbf{C}_* = V\left(\left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 - 1\right)$ je pomocí stereografické projekce biracionálně ekvivalentní přímkě, stereografická projekce totiž dává bijekci elipsy a přímky až na konečné body na každé straně. Tato biracionální ekvivalence je dána pomocí zobrazení:

$$\begin{aligned} \mathbf{C}_* &\rightarrow \mathbb{A}^1(\mathbb{C}) & \mathbb{A}^1(\mathbb{C}) &\rightarrow \mathbf{C}_* \\ (x, y) &\rightarrow \frac{bx}{a(b-y)} & s &\rightarrow \left(\frac{2as}{s^2+1}, \frac{b(s^2-1)}{s^2+1} \right). \end{aligned} \quad (2.3)$$

Mezi projektivními uzávěry těchto variet, tedy mezi $V\left(\left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 - z^2\right) = \mathbf{C}$ v $\mathbb{P}^2(\mathbb{C})$ a $\mathbb{P}^1(\mathbb{C})$, bude dokonce izomorfismus, jak ukážeme ve zbytku této sekce.

Nejdřív rozšíříme výše uvedené zobrazení 2.3 z $\mathbf{C}_*$ do $\mathbb{A}^1(\mathbb{C})$.

$$\begin{aligned} \mathbf{C} &\rightarrow \mathbb{P}^1(\mathbb{C}) \\ [x : y : z] &\rightarrow [bx : a(bz - y)] \end{aligned}$$

Toto zobrazení nedává smysl pro $[0 : b : 1]$, jelikož takový bod by se zobrazil na $[0 : 0]$. Pro tento bod zvolíme alternativní předpis $[x : y : z] \rightarrow [a(bz + y) : bx]$, to je pro $[0 : b : 1]$ dobře definované.

Ověříme, že $[bx : a(bz - y)] = [a(bz + y) : bx]$, pokud mají obě strany smysl.

$$\begin{aligned} (bx)(bx) &= (a(bz - y))(a(bz + y)) \\ &\Downarrow \\ b^2x^2 &= a^2b^2z^2 - a^2y^2 \\ &\Downarrow \\ \left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 &= z^2 \end{aligned}$$

Rovnost je ověřena, jelikož jsme se dostali do ekvivalentního tvaru, který na $\mathbf{C}$ platí.

V opačném směru rozšíříme 2.3 následovně:

$$\begin{aligned} \mathbb{P}^1(\mathbf{C}) &\rightarrow \mathbf{C} \\ [s : r] &\rightarrow [2asr : b(s^2 - r^2) : s^2 + r^2] \end{aligned}$$

Toto zobrazení je dobře definované na celém $\mathbb{P}^1$, neboť žádný bod se nezobrazí na samé nuly.

Dohromady máme izomorfismus daný vzorci

$$\begin{aligned} \mathbf{C} &\longleftrightarrow \mathbb{P}^1(\mathbf{C}) \\ \varphi : [x : y : z] &\longrightarrow \begin{cases} [bx : a(bz - y)] & \text{pro } bz \neq y \\ [a(bz + y) : bx] & \text{pro } bz \neq -y \end{cases} \\ [2asr : b(s^2 - r^2) : s^2 + r^2] &\longleftarrow [s : r] : \psi \end{aligned}$$

Zobrazení jsou opravdu bijektivní, což pro většinu bodů plyne přímočaře z biracionální ekvivalence 2.3.

Ověřit tuto vlastnost izomorfismu tak stačí pro body $\mathbf{C}$ v nekonečnu, tedy pro $[\pm ia : b : 0]$ a pro $[0 : b : 1]$, jelikož $(0, b)$ je jediný bod $\mathbf{C}_*$, pro který zobrazení 2.3 nedává dobrý smysl.

Na druhé straně máme v $\mathbb{P}^1(\mathbf{C})$ bod v nekonečnu $[1 : 0]$ a jediné problematické body pro biracionální ekvivalenci $[\pm i : 1]$.

Ukážeme, že naše zobrazení tyto body spáruje.

$$\begin{aligned} \varphi([\pm ia : b : 0]) &= [\pm iab : ab] = [\pm i : 1] & \psi([\pm i : 1]) &= [\pm ai : b : 0] \\ \varphi([0 : b : 1]) &= [2ab : 0] = [1 : 0] & \psi([1 : 0]) &= [0 : b : 1] \end{aligned}$$

Máme tedy $\mathbf{C} \cong \mathbb{P}^1(\mathbf{C})$ a po dosazení $a = b = 1$ i $\mathbf{D} \cong \mathbb{P}^1(\mathbf{C})$, tudíž $\mathbf{C} \times \mathbf{D} \cong \mathbb{P}^1(\mathbf{C}) \times \mathbb{P}^1(\mathbf{C})$. Pak $N' \cong M'$, neboť přepočítání rovnice tečny obdobně tomu v sekci 2.4.3 nyní funguje i pro původně problematické body.

2.8 Zavedení dalších variet

Nášim cílem je dostat se izomorfismy od N' až do tvaru se známou grupovou strukturou. Zatím jsme zavedli varietu M' , o které jsme ukázali, že je s N' izomorfní.

Stejně jako u prvního izomorfismu nejdřív budeme pracovat v afinním prostoru. V této sekci se dostaneme ke K a L , v další sekci spočítáme jejich biracionální ekvivalenci s afinní varietou M . Následně biracionální ekvivalenci rozšíříme na izomorfismus mezi M' a L' , což bude právě varieta se známou grupovou strukturou.

Budeme pracovat s $\mathbb{C}(M)$ podílovým tělesem souřadnicového okruhu $\Gamma(M)$. Funkční těleso $\mathbb{C}(M)$ je jakožto tělesové rozšíření $\mathbb{C}$ generováno s a t , které musí splňovat rovnici $f = 0$.

Prvek s je transcendentní nad $\mathbb{C}$, neboť pokud by bylo algebraické, existovalo by $n \in \mathbb{N}$ a $a_i \in \mathbb{C}$ takové, že $\sum_{i=1}^n a_i s^i = 0$. Jenže to by znamenalo, že s nabývá v M maximálně n hodnot, což není pravda.

Lemma 2.10 nám říká, že pokud jsou splněny podmínky $(\star)$, f je jako polynom v t ireducibilní nad $\mathbb{C}(s)$. Tedy $\mathbb{C}(M)$ je kvadratické rozšíření $\mathbb{C}(s)$ o kořen $f \in \mathbb{C}(s)[t]$. U kvadratických rozšíření můžeme místo kořene ekvivalentně přidat odmocninu z diskriminantu. Také $\sqrt{4(b^2 - 1)} \in \mathbb{C}$, takže my pro jednoduchost můžeme přidat rovnou odmocninu z $\frac{D}{4(b^2 - 1)}$, kde D značí diskriminant $f \in \mathbb{C}(s)[t]$ (viz 2.2).

$$\frac{D}{4(b^2 - 1)} = s^4 + \left(\frac{-2 + 4a^2 - 2b^2}{b^2 - 1} \right) s^2 + 1$$

Označme

$$c = \frac{-2 + 4a^2 - 2b^2}{b^2 - 1}.$$

Funkční těleso $\mathbb{C}(M)$ je generováno nad $\mathbb{C}$ prvky s a $d = \sqrt{\frac{D}{4(b^2 - 1)}}$. Z variety M jsme se dostali ke

$$K = \{(s, d) \mid d^2 = s^4 + cs^2 + 1\}.$$

Nyní zavedeme ještě $L \cong K$ přidáním $w = s^2$,

$$L = \{(s, d, w) \mid d^2 = w^2 + cw + 1, w = s^2\}.$$

2.9 Biracionální ekvivalence M , K a L

Ukážeme, že M a K jsou biracionálně ekvivalentní pomocí vzorců pro výpočet kvadratické rovnice.

Mějme kvadratickou rovnici $\alpha t^2 + \beta t + \gamma = 0$. Pro nás platí

$$\alpha = \left(-(s^2 + 1) + b(s^2 - 1) \right) \quad \beta = 4as \quad \gamma = \left(-(s^2 + 1) - b(s^2 - 1) \right).$$

Vezmeme diskriminant $D = \beta^2 - 4\alpha\gamma$, pak víme, že jedno řešení je

$$t = \frac{-\beta + \sqrt{D}}{2\alpha} = \frac{-\beta + 2d\sqrt{b^2 - 1}}{2\alpha}.$$

Tedy d můžeme vyjádřit jako

$$d = \frac{2\alpha t + \beta}{2\sqrt{b^2 - 1}}.$$

To nám dohromady dává biracionální ekvivalenci mezi M a K .

$$\begin{aligned} M &\longleftrightarrow K \\ (s, t) &\longrightarrow \left(s, \frac{2\alpha t + \beta}{2\sqrt{b^2 - 1}}\right) \\ \left(s, \frac{-\beta + 2d\sqrt{b^2 - 1}}{2\alpha}\right) &\longleftarrow (s, d) \end{aligned}$$

Pak jistě máme i biracionální ekvivalenci mezi M a L .

$$\begin{aligned} M &\longleftrightarrow L \\ (s, t) &\longrightarrow \left(s, \frac{2\alpha t + \beta}{2\sqrt{b^2 - 1}}, s^2\right) \\ &= \left(s, \left(\sqrt{\frac{b-1}{b+1}}s^2 - \sqrt{\frac{b+1}{b-1}}\right)t + \frac{2a}{\sqrt{b^2 - 1}}s, s^2\right) \\ \left(s, \frac{-\beta + 2d\sqrt{b^2 - 1}}{2\alpha}\right) &\longleftarrow (s, d, w) \\ &= \left(s, \frac{-2as + d\sqrt{b^2 - 1}}{(b-1)w - (b+1)}\right) \end{aligned} \tag{2.4}$$

2.10 Ekvivalentní vyjádření t a d

Nyní se vrátíme ke kvadratické rovnici $\alpha t^2 + \beta t + \gamma = 0$. Její řešení můžeme vyjádřit ve tvaru $t_{1,2} = \frac{-\beta \pm \sqrt{D}}{2\alpha}$. Pokud $t \neq 0$, můžeme rovnici přenásobit t^{-2} a ekvivalentně řešit rovnici $\gamma t^{-2} + \beta t^{-1} + \alpha = 0$. Diskriminant této rovnice je stejný a řešení jsou ve tvaru $t_{1,2}^{-1} = \frac{-\beta \pm \sqrt{D}}{2\gamma}$, tedy $t_{1,2} = \frac{2\gamma}{-\beta \mp \sqrt{D}}$.

Ukážeme, že pokud mají obě vyjádření t_1 a t_2 smysl, dávají stejný výsledek a pořadí znamének před $\sqrt{D}$ je správné ve výše zmíněném pořadí.

$$\begin{aligned} t_1 = \frac{-\beta + \sqrt{D}}{2\alpha} = \frac{2\gamma}{-\beta - \sqrt{D}} & \quad t_2 = \frac{-\beta - \sqrt{D}}{2\alpha} = \frac{2\gamma}{-\beta + \sqrt{D}} & (2.5) \\ \Updownarrow & \quad \Updownarrow \\ (-\beta)^2 - D = 4\alpha\gamma & \quad (-\beta)^2 - D = 4\alpha\gamma \\ \Updownarrow & \quad \Updownarrow \\ \beta^2 - (\beta^2 - 4\alpha\gamma) = 4\alpha\gamma & \quad \beta^2 - (\beta^2 - 4\alpha\gamma) = 4\alpha\gamma \end{aligned}$$

Oba případy jsme přepsali na ekvivalentní rovnosti, které platí. Tedy pro $d = \sqrt{\frac{D}{4(-1+b^2)}}$ a $t = t_1$ můžeme d vyjádřit dvěma způsoby:

$$d = \frac{2\alpha t + \beta}{2\sqrt{b^2 - 1}} = \frac{-\beta t - 2\gamma}{t(2\sqrt{b^2 - 1})}. \tag{2.6}$$

2.11 Izomorfismus M' a L'

V této sekci dokážeme, že mezi projektivními varietami

$$M' = \{([s : r], [t : u]) \mid 4asrtu + b(s^2 - r^2)(t^2 - u^2) = (s^2 + r^2)(t^2 + u^2)\} \\ \text{a } L' = \{[s : d : w : z] \mid d^2 = w^2 + cwz + z^2, wz = s^2\} \quad (2.7)$$

je dokonce izomorfismus.

2.11.1 $M' \rightarrow L'$

Nejdřív se podíváme na zobrazení z M' do L' .

Jelikož $([x_1 : y_1], [x_2 : y_2])$ a $([\lambda x_1 : \lambda y_1], [\mu x_2 : \mu y_2])$, $\lambda, \mu \in \mathbb{C} \setminus \{0\}$, určují stejný prvek M' , nesmí se zobrazit na dva různé prvky L' . Pro afinní body M' , pro které už máme definovanou biracionální ekvivalenci 2.4, budeme chtít, aby obě zobrazení souhlasila.

Zobrazení z M' do L' tak získáme z 2.4 homogenizací v obou dvojicích souřadnic:

$$([s : r], [t : u]) \longrightarrow \left[sru : \left(\sqrt{\frac{b-1}{b+1}}s^2 - \sqrt{\frac{b+1}{b-1}}r^2 \right) t + \frac{2a}{\sqrt{b^2-1}}sru : s^2u : r^2u \right]. \quad (2.8)$$

Je potřeba ověřit, jestli se některý bod nezobrazí na samé nuly, pro takové body bude třeba najít alternativní vzorec.

Pro $u \neq 0$ bude třetí nebo čtvrtá souřadnice obrazu nenulová, jelikož nemůže nastat $s = r = 0$. Pro $u = 0$ bude nulová první, druhá i třetí souřadnice a druhá se zjednoduší na $\left(\sqrt{\frac{b-1}{b+1}}s^2 - \sqrt{\frac{b+1}{b-1}}r^2 \right) t$, což se rovná nule právě tehdy, když $[s : r] = [\sqrt{b+1} : \pm\sqrt{b-1}]$.

K nalezení alternativního vzorce použijeme druhé vyjádření d z 2.6. Po dosazení za α, β, γ máme

$$d = \left(-\sqrt{\frac{b-1}{b+1}} + \sqrt{\frac{b+1}{b-1}}s^2 \right) \frac{1}{t} - \frac{2a}{\sqrt{b^2-1}}s.$$

Obdobným způsobem jako jsme získali 2.8 dostaneme

$$([s : r], [t : u]) \longrightarrow \left[srt : \left(-\sqrt{\frac{b-1}{b+1}}r^2 + \sqrt{\frac{b+1}{b-1}}s^2 \right) u - \frac{2a}{\sqrt{b^2-1}}srt : s^2t : r^2t \right]. \quad (2.9)$$

To zobrazí body $([\sqrt{b+1} : \pm\sqrt{b-1}], [1 : 0])$ na $[\pm\sqrt{b^2-1} : \pm 2a : b-1 : b+1]$.

Body M' , které dává smysl zobrazit pomocí 2.8 i 2.9, se v obou případech zobrazí na stejný prvek L' .

Tyto body mají souřadnici u i t nenulovou. Jediné body M' s $u = 0$ jsou $([\sqrt{b+1} : \pm\sqrt{b-1}], [1 : 0])$, pro které nedává smysl první zobrazení. Body M' s $t = 0$ jsou $([\sqrt{b-1} : \pm\sqrt{b+1}], [0 : 1])$, pro které zase nedává smysl druhé zobrazení. Pokud $u \neq 0 \neq t$, pak se obrazy obou zobrazení rovnají až na $\frac{t}{u}$ násobek, druhá souřadnice se shoduje díky rovnosti 2.6, zbylé se shodují triviálně.

2.11.2 $L' \rightarrow M'$

Teď se podíváme na zobrazení z L' do M' . Opět se budeme snažit rozšířit biracionální ekvivalenci 2.4.

$$[s : d : w : z] \longrightarrow ([s : z], [-2as + d\sqrt{b^2 - 1} : (b - 1)w - (b + 1)z]) \quad (2.10)$$

Zobrazení není dobře definované pro body L' , jejichž obraz by měl v první nebo druhé dvojici souřadnic obě souřadnice nulové. Pro takové body nalezneme jiné zobrazení.

První dvojice souřadnic je nulová právě tehdy, když $s = 0 = z$. Pak jistě $w \neq 0$, protože v opačném případě by z rovnosti $d^2 = w^2 + cwz + z^2$, která platí na L' , plynulo, že jsou nulové všechny čtyři souřadnice, což není možné.

Díky rovnosti $wz = s^2$ z definice L' platí $[s : z] = [w : s]$, mají-li obě strany smysl. Tedy pro body $s = 0 = z$ nahradíme v 2.10 $[s : z]$ za $[w : s]$.

Alternativní vzorec pro body, ve kterých je druhá dvojice souřadnic nulová, najdeme pomocí rovnosti 2.5. Po dosazení do druhého vyjádření t_1 dostaneme

$$t = \frac{(b - 1) - (b + 1)w}{-2as - d\sqrt{b^2 - 1}}.$$

Tudíž jako náhradní vyjádření druhé dvojice souřadnic zvolíme $[(b - 1)z - (b + 1)w : -2as - d\sqrt{b^2 - 1}]$.

Nemůže se stát, že by v obou vyjádřeních druhé dvojice souřadnic vycházely dvě nuly. Jinak by se i součet první souřadnice v prvním vyjádření a druhé v druhém rovnal nule, neboli $-4as = 0$. Pak $s = 0$, neboť $a \neq 0$. Jenže pak by z rovnic z definice L' a rovnosti $(b - 1)z - (b + 1)w = 0$ vycházely nulové i w, z, d .

Ještě ověříme rovnost obou vyjádření pro body, kde obě dávají smysl.

$$\begin{aligned} (-2as + d\sqrt{b^2 - 1})(-2as - d\sqrt{b^2 - 1}) &= \\ &= ((b - 1)z - (b + 1)w)((b - 1)w - (b + 1)z) \\ &\Downarrow \\ 4as^2 - d^2(b^2 - 1) &= (2b^2 + 2)wz - (b^2 - 1)(w^2 + z^2) \\ &\Downarrow wz = s^2 \\ 4awz - d^2(b^2 - 1) &= (2b^2 + 2)wz - (b^2 - 1)(w^2 + z^2) \\ &\Downarrow c = \frac{-2 + 4a^2 - 2b^2}{-1 + b^2} \\ -d^2(b^2 - 1) &= -(b^2 - 1)cwz - (b^2 - 1)(w^2 + z^2) \\ &\Downarrow d^2 = w^2 + cwz + z^2 \\ -d^2(b^2 - 1) &= -d^2(b^2 - 1) \end{aligned}$$

Původní rovnost jsme ekvivalentně upravili do tvaru, ve kterém bezpochyby platí.

2.11.3 Celý izomorfismus

Nyní dáme dohromady všechny výše zmíněné zobrazení mezi M' a L' .

$$\begin{aligned}
 & M' \longleftrightarrow L' \\
 & \varphi : ([s : r], [t : u]) \longrightarrow \left\{ \begin{aligned} & [sru : \left(\sqrt{\frac{b-1}{b+1}} s^2 - \sqrt{\frac{b+1}{b-1}} r^2 \right) t + \frac{2a}{\sqrt{b^2-1}} sru : s^2 u : r^2 u] \\ & [srt : \left(-\sqrt{\frac{b-1}{b+1}} r^2 + \sqrt{\frac{b+1}{b-1}} s^2 \right) u - \frac{2a}{\sqrt{b^2-1}} srt : s^2 t : r^2 t] \end{aligned} \right. \\
 & \quad \left. \begin{aligned} & ([s : z], [-2as + d\sqrt{b^2-1} : (b-1)w - (b+1)z]) \\ & ([w : s], [-2as + d\sqrt{b^2-1} : (b-1)w - (b+1)z]) \\ & ([s : z], [(b-1)z - (b+1)w : -2as - d\sqrt{b^2-1}]) \end{aligned} \right\} \longleftarrow [s : d : w : z] : \psi
 \end{aligned} \tag{2.11}$$

Čtvrtá kombinace vzorců u ψ není potřeba, neboť pokud $s = 0 = z$, pak $w, d \neq 0$ a protože $b \neq \pm 1$, je možné použít třetí kombinaci.

Aby zobrazení 2.11 dávala izomorfismus, zbývá zdůvodnit, že dávají bijekci bodů M' a L' . Většinu afinních bodů už máme spárovanou pomocí biracionální ekvivalence 2.4, tuto vlastnost tedy stačí ověřit pro konečné body, které biracionální ekvivalence vynechává a pro body v nekonečnu.

Zobrazení zmíněné v 2.4 z M do L je dobře definované na celém M . V M' máme oproti M navíc čtyři body v nekonečnu $([\sqrt{b+1} : \pm\sqrt{b-1}], [1 : 0])$ a $([1 : 0], [\sqrt{b+1} : \pm\sqrt{b-1}])$.

V L' jsou dva body v nekonečnu $[0 : 1 : \pm 1 : 0]$. Navíc zobrazení z L do M z 2.4 není definované pro $w = \frac{b+1}{b-1}$, což splňují hned čtyři body L . V L' je můžeme zapsat jako $[\pm\sqrt{b^2-1} : \pm 2a : b+1 : b-1]$ a $[\pm\sqrt{b^2-1} : \mp 2a : b+1 : b-1]$.

Čtyři nedorěšené body z M' a čtyři nedorěšené body z L' naše zobrazení 2.11 páruje následovně.

$$\begin{aligned}
 \varphi \left(([1 : 0], [\sqrt{b+1} : \pm\sqrt{b-1}]) \right) &= [0 : \sqrt{b-1} : \pm\sqrt{b-1} : 0] = [0 : 1 : \pm 1 : 0] \\
 \psi \left(([0 : 1 : \pm 1 : 0]) \right) &= ([1 : 0], [\sqrt{b^2-1} : \pm(b-1)]) \\
 &= ([1 : 0], [\sqrt{b+1} : \pm\sqrt{b-1}]) \\
 \varphi \left(([\sqrt{b+1} : \pm\sqrt{b-1}], [1 : 0]) \right) &= [\pm\sqrt{b^2-1} : \mp 2a : b+1 : b-1] \\
 \psi \left([\pm\sqrt{b^2-1} : \mp 2a : b+1 : b-1] \right) &= \\
 &= ([\pm\sqrt{b^2-1} : b-1], [-4b : \mp 2a\sqrt{b^2-1} \pm 2a\sqrt{b^2-1}]) \\
 &= ([\sqrt{b+1} : \pm\sqrt{b-1}], [1 : 0])
 \end{aligned}$$

Zbývá se podívat, kam se zobrazí body $[\pm\sqrt{b^2-1} : \pm 2a : b+1 : b-1]$.

$$\psi \left([\pm\sqrt{b^2-1} : \pm 2a : b+1 : b-1] \right) = ([\sqrt{b+1} : \pm\sqrt{b-1}], [\pm b : a\sqrt{b^2-1}])$$

Zobrazí se tedy na body L' , ukážeme, že φ tyto obrazy zobrazí zase zpět na původní body M' .

$$\begin{aligned}
 \varphi \left(([\sqrt{b+1} : -\sqrt{b-1}], [-b : a\sqrt{b^2-1}]) \right) &= \\
 &= [\sqrt{b^2-1}b : 2ab : (b+1)(-b) : (b-1)(-b)] = [\sqrt{b^2-1} : 2a : b+1 : b-1]
 \end{aligned}$$

To znamená, že jsme opravdu našli izomorfismus projektivních variet M' a L' .

2.12 Dokončení důkazu

V sekci 2.3 jsme zavedli N' a zdůvodnili, že pro důkaz Poncletova porismatu nám stačí ukázat, že $T = i_D \circ i_C : N' \rightarrow N'$ je translace. V dalších sekcích jsme se z N' dostali přes M' až k L' a dokázali, že $N' \cong M' \cong L'$. Nyní se podíváme na to, jak budou naše involuce vypadat v těchto izomorfních varietách. K práci s involucí v L' se nám bude hodit znát její grupovou strukturu.

2.12.1 Grupová struktura L'

Projektivní varieta L' (2.11) je jakožto průnik dvou kvadrik eliptická křivka, tomuto tvaru se také říká Jacobiho tvar eliptické křivky. Na L' máme podle kapitoly 4, především 4.1 a 4.2, článku Hisil a kol. (2009) následující grupovou strukturu.

- Jednotkový prvek grupy je $[0 : 1 : 0 : 1]$.
- Inverzní prvek k $[s : d : w : z]$ je $[-s : d : w : z]$.
- Pro body $[s_1 : d_1 : w_1 : z_1] \neq [s_2 : d_2 : w_2 : z_2]$, pro které se alespoň jedno ze z_1, z_2 nerovná nule, máme grupové sčítání $[s_1 : d_1 : w_1 : z_1] + [s_2 : d_2 : w_2 : z_2] = [s_3 : d_3 : w_3 : z_3]$, kde

$$\begin{aligned} s_3 &= (s_1 d_2 - d_1 s_2)(w_1 z_2 - z_1 w_2), \\ d_3 &= (d_1 d_2 - c s_1 s_2)(w_1 z_2 + z_1 w_2) - 2 s_1 s_2 (z_1 z_2 + w_1 w_2), \\ w_3 &= (w_1 z_2 - z_1 w_2)^2, \\ z_3 &= (s_1 d_2 - d_1 s_2)^2. \end{aligned}$$

- Pro bod $[s : d : w : z]$, máme sečtení bodu se sebou samým jako $2[s : d : w : z] = [s_3 : d_3 : w_3 : z_3]$, kde

$$\begin{aligned} s_3 &= 2sd(2z^2 + cs^2 - d^2), \\ d_3 &= 2d^2(d^2 - cs^2) - (2z^2 + cs^2 - d^2)^2, \\ w_3 &= (2sd)^2, \\ z_3 &= (2z^2 + cs^2 - d^2)^2. \end{aligned}$$

Zbývá součet různých bodů, které mají oba nulovou poslední souřadnici. V L' jsou takové body jen $[0 : \pm 1 : 1 : 0]$. Jelikož $[0 : -1 : 0 : 1] - [0 : 1 : 1 : 0] = [0 : -1 : 0 : 1] + [0 : 1 : 1 : 0] = [0 : -1 : 1 : 0]$, vychází $[0 : 1 : 1 : 0] + [0 : 1 : -1 : 0] = [0 : -1 : 0 : 1]$.

2.12.2 Involuce

Nyní už se dostáváme k involucím i_D a i_C . Nejdřív se zaměříme na involuci i_D . Ta dvojici $(p, q) \in \mathbf{C} \times \mathbf{D}$ zobrazí na (p, q') , kde q' leží na druhé tečně k $\mathbf{D}$ z bodu p než q .

V M' bude tato involuce zobrazovat bod $([s : r], [t : u])$ na jediný další bod M' s první dvojicí souřadnic stejnou, tedy na $([s : r], [t' : u'])$, protože souřadnice určující bod na $\mathbf{C}$ musí zůstat stejné.

Teď ji převedeme do L' pomocí zobrazení 2.11. Pokud $u \neq 0$, respektive $u' \neq 0$, nechť u , respektive u' , je rovno 1, v opačném případě nechť t , respektive $t' = 1$. Pak vidíme, že obrazy $([s : r], [t : u])$ a $([s : r], [t' : u'])$ v L' se mohou lišit pouze v druhé souřadnici. Z definice L' (2.7) plyne, že naše involuce zobrazuje $[s : d : w : z]$ na $[s : -d : w : z]$.

Z výše uvedených grupových struktur vychází pro všechny $[s : d : w : z] \in L'$ $[s : d : w : z] + [s : -d : w : z] = [0 : -1 : 0 : 1]$. (Jde pouze o dosazení do uvedených vzorců, které jsem pro jednoduchost provedla v *Mathematice*.)

Izomorfismus eliptických křivek coby projektivních variet ještě nemusí být grupový izomorfismus, protože jednotkový prvek může být zvolen na každé jinak. Ovšem podle příkladu 4.7 na straně 71 v knize Silverman (2009) je každý morfismus eliptických křivek složením grupového homomorfismu a translace. Proto k vyjádření výše přidáme na pravou stranu jednotkový prvek grupy. Máme $[s : d : w : z] + [s : -d : w : z] = [0 : -1 : 0 : 1] + [0 : 1 : 0 : 1]$, tedy na obou stranách součet dvou prvků, takže libovolná translace tuto rovnost zachová. Po převedení zpět do variety M' pomocí 2.11 dostaneme $([s : r], [t : u]) + ([s : r], [t' : u']) = ([0 : 1], [\sqrt{b-1} : -\sqrt{b+1}]) + ([0 : 1], [\sqrt{b-1} : \sqrt{b+1}])$. Naše involuce má v M' tvar

$$([s : r], [t : u]) \longrightarrow k_D - ([s : r], [t : u]),$$

kde $k_D = ([0 : 1], [\sqrt{b-1} : -\sqrt{b+1}]) + ([0 : 1], [\sqrt{b-1} : \sqrt{b+1}])$.

Obdobně můžeme rozebrat i druhou involuci i_C , která přehazuje body $\mathbf{C}$ ležící na stejné tečně k $\mathbf{D}$. Stačí brát polynom f v sekci 2.8 jako polynom v s nad $\mathbb{C}(t)$ a následně pokračovat totožným způsobem jako v kapitolách 2.8–2.11. Pak budeme mít v M' vyjádření

$$([s : r], [t : u]) \longrightarrow k_C - ([s : r], [t : u]),$$

kde k_C je opět pevný bod v M' .

Složením obou involucí v M' získáme

$$\begin{aligned} T([s : r], [t : u]) &= (i_D \circ i_C)([s : r], [t : u]) = \\ &= i_D(k_C - ([s : r], [t : u])) = ([s : r], [t : u]) + k_D - k_C, \end{aligned}$$

kde T , i_D i i_C jsou izomorfní obrazy v M' stejně pojmenovaných zobrazení v N' .

To znamená, že T je vzhledem ke grupové struktuře translace, tedy T^n je také translace a jediná translace s pevným bodem je identita, což jsme chtěli dokázat.

Závěr

V této práci jsme uvedli kompletní důkaz Ponceletova porismatu. V první kapitole jsme zavedli teorii potřebnou pro hlavní část práce. V kapitole druhé jsme se věnovali důkazu. Na rozdíl od jiných dohledatelných zdrojů jsme uvedli řádné zdůvodnění, proč stačí větu dokazovat pouze pro soustřednou kružnici a elipsu. V další části důkazu jsme ukázali, že varieta N' je eliptická křivka, a to tak, že jsme spočítali izomorfismus s Jacobiho tvarem eliptické křivky. Známou grupovou strukturu Jacobiho tvaru jsme využili k dokončení důkazu.

Existuje i několik dalších důkazů Ponceletova porismatu. Známým algebraickým důkazem je důkaz Griffitse a Harrise, ve kterém se stejně jako v našem důkazu využívá, že N' je eliptická křivka, ovšem místo převodu na známý tvar eliptické křivky se zde dokazuje, že N' je projektivní nesingulární křivka rodu jedna. Naopak příkladem analytického důkazu je důkaz vzniklý spojením myšlenek Bertranda, Jacobiho a Schoenberga. V něm se pracuje se soustřednou kružnicí a elipsou nad $\mathbb{R}$. Využívá se vhodně zvolené míry na vnější kružnici takové, že oblouky příslušící libovolné tečně k vnitřní elipse mají stejnou hodnotu. Podrobnější nástin důkazů lze nalézt na stránce Nash (2018).

Seznam použité literatury

- COX, D., LITTLE, J. a O'SHEA, D. (2007). *Ideals, varieties, and algorithms: an introduction to computational algebraic geometry and commutative algebra*. Springer Science & Business Media.
- FULTON, W. (1984). *Introduction to intersection theory in algebraic geometry*. Number 54. American Mathematical Soc.
- FULTON, W. (2008). Algebraic curves. URL <http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf>.
- HISIL, H., WONG, K. K.-H., CARTER, G. a DAWSON, E. (2009). Jacobi quartic curves revisited. In *Australasian Conference on Information Security and Privacy*, pages 452–468. Springer.
- KALA, V. (2020). Komutativní okruhy. URL <https://www2.karlin.mff.cuni.cz/~kala/1920%20ko/K0%20skripta.pdf>.
- NASH, O. (2018). Poring over poncelet. URL olivernash.org/2018/07/08/poring-over-poncelet/index.html.
- SCHOENBERG, I. (1983). On Jacobi–Bertrand’s proof of a Theorem of Poncelet. In *Studies in pure mathematics*, pages 623–627. Springer.
- SILVERMAN, J. H. (2009). *The arithmetic of elliptic curves*, volume 106. Springer.
- TAGHAVI, A. (2015). An alternative proof for the fixed point property of $\mathbb{CP}^{2n}$. *Expositiones Mathematicae*, **33**(1), 105–107.