



**MATEMATICKO-FYZIKÁLNÍ  
FAKULTA**  
Univerzita Karlova

## **BAKALÁŘSKÁ PRÁCE**

Ivana Trummová

### **Planimetrické problémy řešené algebraickou geometrií**

Katedra algebry

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

Studijní program: Matematika (B1101)

Studijní obor: MMIB (1801R013)

Praha 2018

UNIVERZITA KARLOVA  
Matematicko-fyzikální fakulta

Katedra algebry

Akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jméno a příjmení: **Ivana Trummová**

Studijní program: **Matematika**

Studijní obor: **Matematické metody informační bezpečnosti**

Děkan fakulty Vám podle zákona č. 111/1998 Sb. určuje tuto bakalářskou práci:

Téma práce v českém jazyce: **Planimetrické problémy řešené algebraickou geometrií**

Téma práce v anglickém jazyce: **Plane geometry problems solved by algebraic geometry**

Zásady pro vypracování:

Student se seznámí se základy algebraické geometrie a především s Bézoutovou větou o počtu průniků rovinných křivek. Poté zpracuje různé zajímavé důsledky Bézoutovy věty: Pascalovu větu o šestiúhelníku vepsaném kuželosečce, Pappovu větu, Cayley-Bacharachovu větu o průnicích kubických rovinných křivek, asociativní zákon grupy na eliptických křivkách. Jelikož jde z velké části o velmi geometricky názorné problémy, bylo by vhodné práci doplnit i grafickými ilustracemi.

Seznam odborné literatury:

- [1] W. Fulton, Algebraic Curves (An Introduction to Algebraic Geometry), 2008.
- [2] J. Richter-Gebert, Perspectives on Projective Geometry, A Guided Tour Through Real and Complex Geometry, Springer, 2011.
- [3] Q. Ren, J. Richter-Gebert, B. Sturmfels, Cayley-Bacharach Formulas, preprint, arXiv:1405.6438v2.

Vedoucí bakalářské práce: **doc. RNDr. Šťoviček Jan, Ph.D.**

Navrhování oponenti:

Konzultanti:

Datum zadání bakalářské práce: 9.4.2018

Termín odevzdání bakalářské práce: dle harmonogramu příslušného akademického roku

*Téma*

Vedoucí katedry

V Praze dne 9.4.2018

**Univerzita Karlova**  
**Matematicko-fyzikální fakulta**  
Studijní oddělení  
121 16 Praha 2, Ke Karlovu 3  
IČ: 00216208, DIČ: CZ00216208  
Tel.: 951 551 412, 951 551 111

*M. F. Čmelík*

Děkan

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

Ráda bych poděkovala především doc. RNDr. Janu Šťovíčkovi, Ph.D., za všechny čas strávený konzultováním a odpovídáním na otázky, a hlavně za přístup, který mě motivoval a podporoval. Za cenné rady děkuji Tomáši Lysoňkovi a Báře Hudcové, kteří mi často pomohli formulovat moje myšlenky.

Název práce: Planimetrické problémy řešené algebraickou geometrií

Autor: Ivana Trummová

Katedra: Katedra algebry

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

Abstrakt: Práce je zaměřena na oblast algebraické geometrie, která se zabývá rovinnými křivkami a jejich křížícími body. Hlavní částí je důkaz Bézoutovy věty a přehled jejích důsledků, které mají zajímavé geometrické znázornění. Mezi důsledky je pro praxi nejdůležitější důkaz asociativity sčítání na eliptických křivkách – sčítání je hojně využíváno v moderní kryptografii.

Klíčová slova: algebraická geometrie, rovinné křivky, Bézoutova věta

Title: Plane geometry problems solved by algebraic geometry

Author: Ivana Trummová

Department: Department of Algebra

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

Abstract: In this thesis I focus on a certain part of algebraic geometry which studies plane curves and their intersection points. The main part is a proof of Bézout's theorem and an overview of its corollaries, which have an interesting geometric visualization. The most important corollary is the proof of associativity of adding points on elliptic curves. This fact is widely used in modern cryptography.

Keywords: algebraic geometry, plane curves, Bézout's theorem

# Obsah

|                                                            |           |
|------------------------------------------------------------|-----------|
| <b>Úvod</b>                                                | <b>2</b>  |
| <b>1 Teorie a příprava</b>                                 | <b>3</b>  |
| 1.1 Úplný úvod do algebraické geometrie . . . . .          | 3         |
| 1.1.1 Značení . . . . .                                    | 3         |
| 1.1.2 Několik definic . . . . .                            | 3         |
| 1.1.3 Několik příkladů rovinných křivek . . . . .          | 4         |
| 1.2 Lokální vlastnosti rovinných křivek, křížení . . . . . | 5         |
| 1.3 Projektivní geometrie . . . . .                        | 6         |
| 1.3.1 Úvod do projektivní geometrie . . . . .              | 6         |
| 1.3.2 Formy . . . . .                                      | 8         |
| 1.4 Exaktní posloupnosti . . . . .                         | 9         |
| <b>2 Důkaz Bézoutovy věty</b>                              | <b>10</b> |
| <b>3 Důsledky Bézoutovy věty</b>                           | <b>13</b> |
| 3.1 Cayley-Bacharachova věta . . . . .                     | 13        |
| 3.2 Pappova věta . . . . .                                 | 16        |
| 3.3 Pascalův šestiúhelník . . . . .                        | 17        |
| 3.4 Eliptické křivky . . . . .                             | 17        |
| <b>Závěr</b>                                               | <b>21</b> |
| <b>Seznam použité literatury</b>                           | <b>22</b> |

# Úvod

Ačkoli je moderní algebraická geometrie záležitostí posledních staletí, obsah této práce sahá daleko více do historie. Pappus z Alexandrie žil zhruba v letech 290–350 našeho letopočtu a byl jedním z velkých geometrů antického Řecka (viz [Richter-Gebert, 2010](#), Kapitola 1). Byl autorem několika knih, a známou částí jeho práce je věta o devíti přímkách a devíti bodech, nyní známá jako Pappova věta.

Další variantu (či v jistém smyslu zobecnění) Pappovy věty objevil v sedmáctém století Blaise Pascal. Vzhledem k tomu, že se Pascal věnoval nejen různým odvětvím matematiky, ale i fyziky, teologie a filozofie, jeho objev věty o vztazích bodů na kuželosečkách není tak široce známý jako jeho jiné práce, konkrétně tento výsledek ale byl pro Pascala důležitý, protože byl „důkazem“ toho, že jeho současníci překonali staré Řeky.

V devatenáctém století byla dokázána Cayley-Bacharachova věta, která je nejsložitějším důsledkem Bézoutovy věty, kterým se tato práce zabývá, zároveň ale nejsilnějším – dává nám silný nástroj na důkaz dvou starších vět a obecného případu asociativity sčítání na eliptických křivkách.

Úloha eliptických křivek v kryptografii nás vede až do roku 1985, kdy nezávisle na sobě Neal Koblitz a Victor S. Miller navrhli jejich použití. Bezpečnost kryptosystému, který používá aditivní grupu na eliptické křivce, stojí na obtížnosti nalezení diskrétního logaritmu náhodného bodu eliptické křivky s ohledem na známý základní bod. Pro použití grupové struktury je nezbytné dokázat existenci inverzů, jednotky, komutativity a hlavně asociativity sčítání, čímž se alespoň v omezené míře zabývá závěr této práce.



# 1. Teorie a příprava

Pro formulaci a důkaz Bézoutovy věty bude nutné se nejdříve věnovat přípravě. V této kapitole je zadefinováno a vysvětleno nutné minimum pojmů potřebných k tomu, aby čtenář mohl s pochopením číst další kapitoly a dostat se k samotnému jádru práce. V této práci jsou nově definovány jen pojmy, které přesahují znalosti z kurzů Algebra 1 a Algebra 2, tedy učiva druhého ročníku matematiky na MFF UK.

## 1.1 Úplný úvod do algebraické geometrie

### 1.1.1 Značení

V celé práci budeme používat značení  $\mathbf{K}$  pro těleso,  $\mathbb{A}^n(\mathbf{K})$ , nebo jen  $\mathbb{A}^n$  pro  $n$ -rozměrný afinní prostor nad  $\mathbf{K}$  (tím rozumíme  $\mathbf{K}^n$ ),  $\bar{a} = (a_1, a_2, \dots, a_n)$  pro prvek prostoru  $\mathbb{A}^n(\mathbf{K})$ ,  $\mathbf{K}[\bar{x}] = \mathbf{K}[x_1, \dots, x_m]$  pro obor polynomů  $m$  proměnných nad  $\mathbf{K}$ ,  $n, m \in \mathbb{N}$ . Jako  $S$  budeme značit soustavu polynomiálních rovnic,  $S \subseteq \mathbf{K}[\bar{x}]$  (přesnější by bylo pojmenování  $S$  jako množiny polynomů z  $\mathbf{K}[\bar{x}]$ , které vytvoří při porovnání s nulou rovnice, pro jednoduchost se budeme držet zkráceného pojmu soustavy rovnic).

Uvažujme polynom  $f \in \mathbf{K}[\bar{x}]$ ,  $\bar{a} \in \mathbb{A}^n(\mathbf{K})$ . Pokud po dosazení  $f(\bar{a}) = 0$ , pak  $\bar{a}$  je kořenem polynomu  $f$ , neboli  $\bar{a}$  je nulou  $f$ .

V celé práci budeme předpokládat, že  $\mathbf{K}$  je algebraicky uzavřené a komutativní těleso.

Veškeré definice použité v této kapitole jsou v souladu s knihou Algebraic Geometry (Fulton, 2008).

### 1.1.2 Několik definic

**Definice 1** (Řešení soustavy). *Nechť  $S \subseteq \mathbf{K}[\bar{x}]$  je soustava polynomiálních rovnic. Pak  $V(S) = \{\bar{a} \in \mathbb{A}^n(\mathbf{K}) : f(\bar{a}) = 0 \ \forall f \in S\}$  je řešením soustavy  $S$ .*

**Definice 2** (Algebraická množina). *Nechť  $X$  je množina bodů z  $\mathbb{A}^n(\mathbf{K})$  a existuje  $S$  tak, že  $X = V(S)$ , tedy  $X$  je řešením nějaké soustavy rovnic. Pak  $X$  je algebraická množina.*

**Definice 3** (Algebraická nadplocha). *Nechť  $X$  je množina bodů z  $\mathbb{A}^n(\mathbf{K})$  a existuje nekonzantní polynom  $f$  tak, že  $X = V(f)$ , tedy  $X$  je řešením nějaké polynomiální rovnice. Pak  $X$  je algebraická nadplocha.*

**Definice 4** (Ideál množiny). *Ať  $X$  je množina bodů z  $\mathbb{A}^n(\mathbf{K})$ , pak vyjádřením  $I(X)$  rozumíme  $I(X) = \{f \in \mathbf{K}[\bar{x}] : f(\bar{a}) = 0 \ \forall \bar{a} \in X\}$ . O množině  $I(X)$  mluvíme jako o ideálu množiny  $X$ .*

**Věta 1** (Hilbertova věta o nulách). *Je-li  $\mathbf{K}$  algebraicky uzavřené, pak*

$$I(V(f)) = \sqrt{(f)}.$$

*Poznámka.* Odmocnina na pravé straně rovnosti označuje radikál hlavního ideálu generovaného  $f$ ,  $\sqrt{(f)} = \{g \in \mathbf{K}[\bar{x}] : \exists n \in \mathbb{N} \text{ tak, že } g^n \in (f)\}$ .

Důkaz. Viz [Fulton \(2008\)](#), Kapitola 1.7). □

**Definice 5** (Afinní rovinná křivka). Afinní rovinná křivka je algebraická nadplocha v afinním prostoru dimenze 2.

*Poznámka.* Křivka je jednoznačně určena polynomem  $f$ , jehož je řešením. Každá křivka naopak jednoznačně (až na násobení skalárem) určuje bezčtvercový polynom  $f$ . Je-li totiž  $f$  bezčtvercový (jeho rozklad na ireducibilní polynomy je bez druhých a vyšších mocnin), pak nám Hilbertova věta o nulách dává  $I(V(f)) = \sqrt{(f)} = (f)$ , umožní nám ho tedy zkonstruovat ze znalosti křivky. Odteď budeme křivky a jejich určující polynomy ztotožňovat. Stupněm křivky rozumíme stupeň polynomu  $f$ .

**Definice 6** (Společná komponenta). Řekneme, že dvě křivky určené polynomy  $f, g$  mají společnou komponentu, pokud mají  $f, g$  netriviálního společného dělitele.

**Definice 7** (Reducibilní a ireducibilní algebraická množina). Neprázdná algebraická množina  $V \subseteq \mathbb{A}^n$  je reducibilní, pokud  $V = V_1 \cup V_2$ , kde  $V_1, V_2$  jsou algebraické množiny v  $\mathbb{A}^n$ ,  $V_i \neq V$ ,  $i = 1, 2$ . Jinak je  $V$  ireducibilní.

*Poznámka.* Neprázdná algebraická množina  $V$  je ireducibilní, právě když  $I(V)$  je proudeál (viz [Fulton, 2008](#), Kapitola 1.5). Ireducibilní afinní rovinné křivky tedy odpovídají ireducibilním polynomům.

### 1.1.3 Několik příkladů rovinných křivek

Rovinnou křivku jsme si definovali jako algebraickou nadplochu, tedy množinu řešení nějaké rovnice zadané polynomem dvou proměnných, což je

$$V(f) = \{(x, y) \in \mathbb{A}^2(\mathbf{K}) : f(x, y) = 0\}.$$

Ukážeme si příklady křivek nízkého stupně.

*Příklad.* Křivky stupně 1 (přímky) se dají zapsat jako

$$\{(x, y) \in \mathbb{A}^2(\mathbf{K}) : ax + by = c\},$$

např. tyrkysová přímka na Obr. 1.1.

*Příklad.* Křivky stupně 2 (kvadriky) jsou množiny

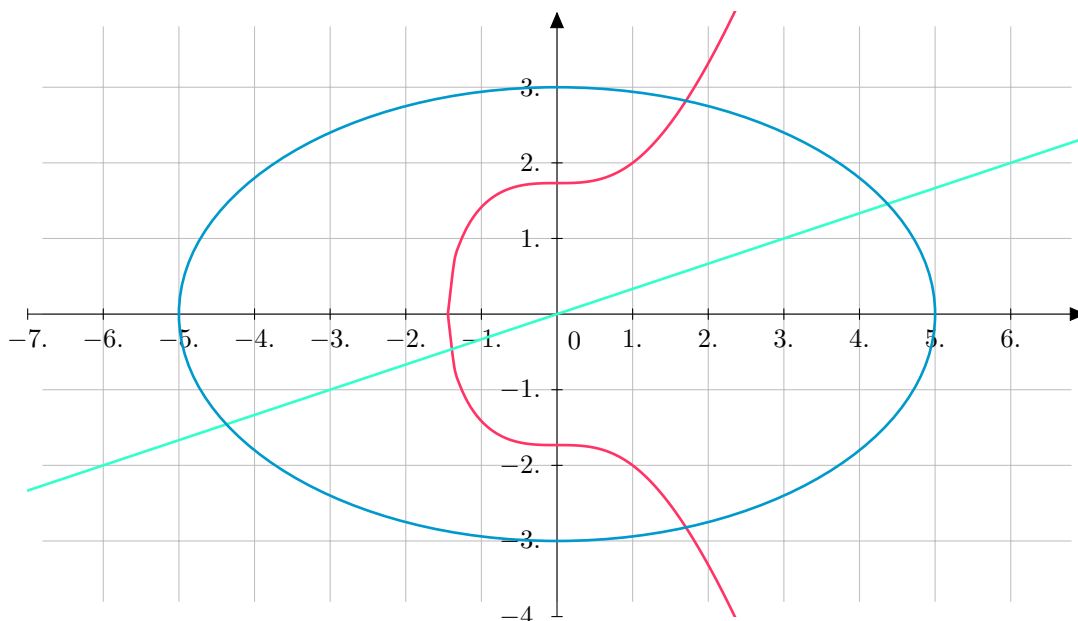
$$\{(x, y) \in \mathbb{A}^2(\mathbf{K}) : ax^2 + bxy + cy^2 + dx + ey + f = 0\},$$

nad reálnými čísly jsou to kuželosečky (např. modrá elipsa na Obr. 1.1), ale patří tam také sjednocení dvou přímek, pokud polynom není ireducibilní.

*Příklad.* Křivky stupně 3 (kubiky) jsou tvaru

$$\{(x, y) \in \mathbb{A}^2(\mathbf{K}) : ax^3 + bx^2y + cxy^2 + dy^3 + ex^2 + fxy + gy^2 + hx + iy + j = 0\},$$

patří tam např. eliptické křivky (např. červená křivka na Obr. 1.1), ale v reducibilním případě i sjednocení kuželosečky a přímky, nebo tří přímek.



Obrázek 1.1: Příklady rovinných křivek

## 1.2 Lokální vlastnosti rovinných křivek, křížení

**Definice 8** (Jednoduchý a násobný bod). *Bod  $a$  na křivce  $f$  se nazývá jednoduchý, pokud*

$$\frac{\partial f}{\partial x}(\bar{a}) \neq 0$$

*nebo*

$$\frac{\partial f}{\partial y}(\bar{a}) \neq 0.$$

*V opačném případě je bod násobný (singulární).*

Derivací zde myslíme formální derivaci definovanou vzorcem

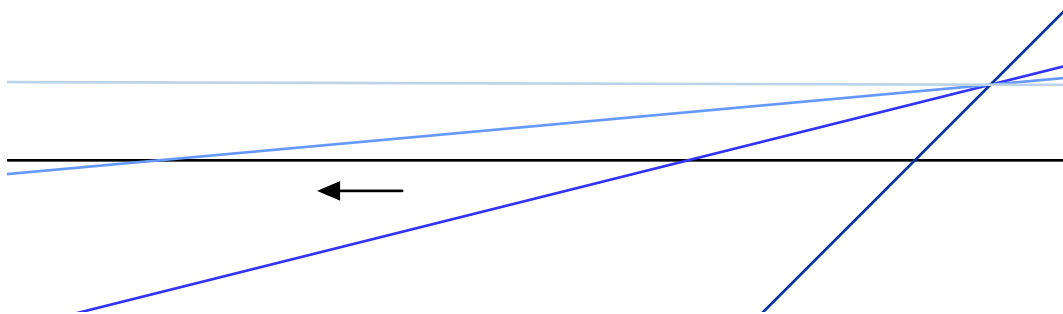
$$\left( \sum_{i=0}^n a_i x^i \right)' = \sum_{i=0}^n i a_i x^{i-1}.$$

**Lemma 2.** *At  $f, g$  jsou polynomy v  $\mathbf{K}[x, y]$ , které nemají společné dělitele. Pak  $V(f, g) = V(f) \cap V(g)$  je konečná množina bodů.*

*Důkaz.* Polynomy  $f, g$  nemají z Gaussova lemmatu společné dělitele ani v  $\mathbf{K}(x)[y]$ . Víme, že  $\mathbf{K}(x)[y]$  je obor hlavních ideálů a můžeme tedy psát  $(f, g) = (1)$ . Máme tedy  $1 = rf + gs$  pro nějaké  $r, s \in \mathbf{K}(x)[y]$ .

Dále existuje nějaký polynom  $d \in \mathbf{K}[x]$ , pro který platí  $dr = a, ds = b, a, b \in \mathbf{K}[x, y]$ . Rovnost  $1 = rf + gs$  vynásobíme polynomem  $d$  a dostaneme  $d = af + bg \in \mathbf{K}[x, y]$ . Nyní pokud nějaký bod  $(A, B)$  patří do  $V(f, g)$ , pak se nuluje v  $d$ . Polynom  $d$  je ale nenulový, takže může mít pouze konečně mnoho nul. Když tento argument použijeme na souřadnici  $y$ , je důkaz dokončen.

□



Obrázek 1.2: Posouvání průsečíku

*Důsledek.* Průnik dvou křivek zadaných polynomy  $f, g$ , které nemají společnou komponentu, je konečná množina.

**Definice 9** (Křížící číslo). Křížící číslo dvou rovinných křivek zadaných polynomy  $f, g$ , značíme  $I(\bar{a}, f \cap g)$ , definujeme jako  $I(\bar{a}, f \cap g) = \dim_{\mathbf{K}}(\mathcal{O}_{\bar{a}}(\mathbb{A}^2)/(f, g))$ , kde  $\mathcal{O}_{\bar{a}}(\mathbb{A}^2)$  značí lokální okruh  $\mathbb{A}^n$  v bodě  $\bar{a}$ .

*Poznámka.* Definice lokálního okruhu je nad rámec této práce (viz [Fulton, 2008](#), Kapitola 2.4).

**Lemma 3** (Několik vlastností křížících čísel). Mějme dvě různé křivky určené polynomy  $f, g$ .

1. Pokud křivky mají společnou komponentu  $k$  a křížící bod  $\bar{a} \in k$ , pak  $I(\bar{a}, f \cap g) = \infty$ , jinak  $I(\bar{a}, f \cap g) < \infty$ .
2. Bod  $\bar{a} \notin f \cap g$  právě když  $I(\bar{a}, f \cap g) = 0$ .
3. Pokud křivky nemají společnou komponentu, platí, že  $\sum_{\bar{a} \in (f \cap g)} I(\bar{a}, f \cap g) = \dim_{\mathbf{K}} \mathbf{K}[x, y]/(f, g)$ .

*Důkaz.* Viz [Fulton \(2008, Kapitola 3.3\)](#).

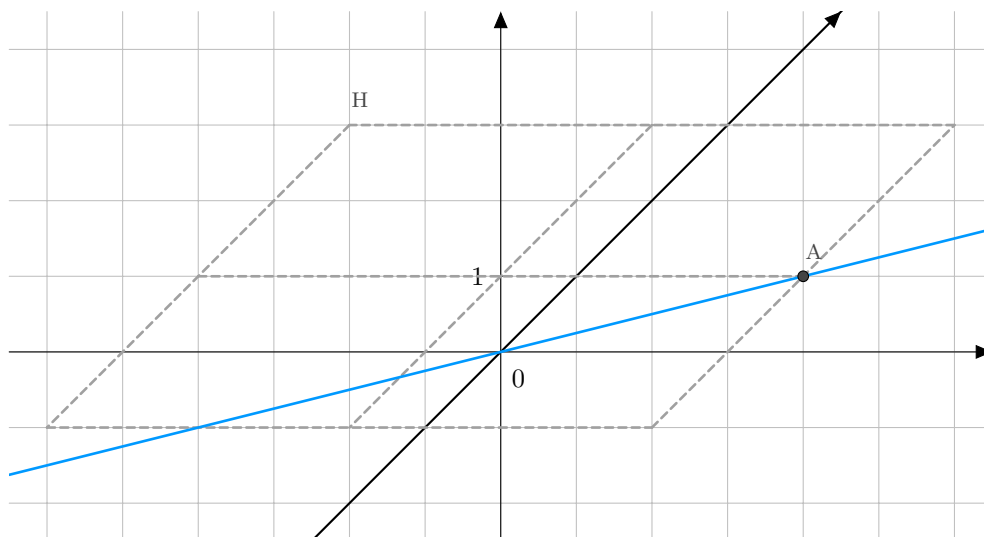
□

## 1.3 Projektivní geometrie

### 1.3.1 Úvod do projektivní geometrie

Všechny definice i věty v této kapitole jsou opět v souladu s knihou W. Fultona ([Fulton, 2008](#)).

Při studiu algebraických křivek a jejich křížení budeme chtít zkoumat všechny křížící body, i ty „v nekonečnu“. Pro příklad mějme dvě přímky v afinní rovině, které se kříží v bodě  $P$ . Zafixujeme jednu z nich (černá na Obr. 1.1), a druhou otáčíme tak, že bod  $P$  se bude vzdalovat doleva (modré přímky a šipka na Obr. 1.2 označují posouvání přímky). Čím víc budeme přímku „narovnávat“, tím dál bude průsečík. Až budou přímky rovnoběžné, průsečík zmizí. Když budeme otáčet přímku dál stejným směrem, průsečík se objeví na druhé straně. Nyní bychom tedy potřebovali rozšířit afinní rovinu tak, aby se dalo mluvit o průsečíku v nekonečnu.



Obrázek 1.3: Ukotvení roviny  $H$  do prostoru

**Definice 10** (Homogenní souřadnice). Každý bod  $(x, y)$  v  $\mathbb{A}^2(\mathbf{K})$  ztotožníme s bodem  $(x : y : 1)$  v  $\mathbb{A}^3(\mathbf{K})$ . Označení  $(x : y : z)$  budeme říkat homogenní souřadnice.

Nyní máme přirozené vnoření roviny do prostoru, kde afinní rovinu (označme ji  $H$ ) ukotvíme na místo, kde  $z = 1$  (viz Obr. 1.2 – rovina  $H$  je šedá). Každý bod  $(x : y : 1)$  jednoznačně určuje přímku v prostoru  $\mathbb{A}^3(\mathbf{K})$ , která prochází počátkem a protíná rovinu  $H$  v bodě  $(x : y : 1)$  (např. bod  $A$  a modrá přímka na Obr. 1.2). Takto lze popsat všechny přímky procházející počátkem kromě těch, co jsou s rovinou  $H$  rovnoběžné (a tedy mají třetí souřadnici  $z = 0$ ). Tyto přímky budou charakterizovat body v nekonečnu.

**Definice 11** (Projektivní prostor). Projektivní prostor nad  $\mathbf{K}$  dimenze  $n$ , píšeme  $\mathbb{P}^n(\mathbf{K})$ , nebo jen  $\mathbb{P}^n$ , je množina všech přímek procházejících počátkem v  $\mathbb{A}^{n+1}(\mathbf{K})$ .

Každý bod v tomto prostoru (kromě nuly) určuje jednoznačně přímku procházející počátkem. Dva body  $(x_1 : y_1 : z_1)$ ,  $(x_2 : y_2 : z_2)$  označíme za ekvivalentní, pokud existuje  $\lambda \neq 0$  tak, že  $(x_1 : y_1 : z_1) = \lambda(x_2 : y_2 : z_2)$ , tedy leží na stejné přímce procházející počátkem. Na projektivní prostor  $\mathbb{P}^n(\mathbf{K})$  se tedy můžeme dívat i jako na množinu tříd ekvivalence bodů v  $\mathbb{A}^{n+1}(\mathbf{K})$  takových, že alespoň jedno z  $x, y, z$  je nenulové (v našem případě jde o nenulové  $z$ , v případě ostatních souřadnic bychom museli rovinu  $H$  ukotvit jinak).

**Definice 12** (Afinní změna souřadnic). Afinní změna souřadnic v  $\mathbb{A}^n(\mathbf{K})$  je polynomiální zobrazení  $T = (T_1, \dots, T_n) : \mathbb{A}^n(\mathbf{K}) \rightarrow \mathbb{A}^n(\mathbf{K})$  takové, že každé  $T_i$  je polynom stupně 1, a  $T$  je bijekce.

*Poznámka.* Pokud  $T_i = \sum a_{ij}x_j + a_{i0}$ , pak  $T = T' \circ T''$ , kde  $T'$  je lineární změna souřadnic (zobrazení) ( $T'_i = \sum a_{ij}x_j$ ) a  $T''$  je posunutí ( $T'' = x_i + a_{i0}$ ). Protože posunutí je invertibilní (inverz je také posunutí),  $T$  je bijekce právě tehdy, když je  $T'$  invertibilní.

Pokud  $T$  a  $U$  jsou afinní změny souřadnic na  $\mathbb{A}^n(\mathbf{K})$ , pak také  $T \circ U$  a  $T^{-1}$  jsou afinní změny souřadnic, a navíc  $T$  je izomorfismus na  $\mathbb{A}^n(\mathbf{K})$ .

**Definice 13** (Projektivní změna souřadnic).  $T : \mathbb{A}^{n+1}(\mathbf{K}) \longrightarrow \mathbb{A}^{n+1}(\mathbf{K})$  je lineární změna souřadnic, pak  $T$  zobrazuje přímky procházející počátkem znovu na nějaké přímky procházející počátkem (neposunuje).  $T$  určuje zobrazení  $z \mathbb{P}^n \longrightarrow \mathbb{P}^n$ , které se nazývá projektivní změnou souřadnic.

### 1.3.2 Formy

**Definice 14** (Stupeň polynomu m proměnných). Mějme polynom  $f \in \mathbf{K}[\bar{x}]$ ,  $f = A_1 + A_2 + \dots + A_n$ ,  $n \in \mathbb{N}$ , kde  $A_i = a_i x_1^{l_1} x_2^{l_2} \dots x_m^{l_m}$ . Stupněm členu  $x_1^{l_1} x_2^{l_2} \dots x_m^{l_m}$  rozumíme součet  $l_1 + \dots + l_m$ . Stupněm polynomu  $f$  je nejvyšší hodnota ze stupňů jeho členů.

**Definice 15** (Forma). Forma stupně  $i$  je polynom, jehož všechny členy mají stejný stupeň  $i$ .

**Definice 16** (Homogenizace). Pro libovolný polynom  $f \in \mathbf{K}[x_1, \dots, x_n]$  stupně  $d$ , pišme  $f = f_0 + f_1 + \dots + f_d$ , kde  $f_i$  je forma stupně  $i$ , definujeme  $f^* \in \mathbf{K}[x_1, \dots, x_{n+1}]$  jako  $f^* = x_{n+1}^d f_0 + x_{n+1}^{d-1} f_1 + \dots + f_d = x_{n+1}^d f(\frac{x_1}{x_{n+1}}, \dots, \frac{x_n}{x_{n+1}})$ , a  $f^*$  je forma stupně  $d$ . Řekneme, že  $f^*$  vznikne z  $f$  homogenizací.

**Definice 17** (Dehomogenizace). Ať  $f \in \mathbf{K}[x_1, \dots, x_{n+1}]$  je forma. Definujeme  $f_* \in \mathbf{K}[x_1, \dots, x_n]$  tak, že  $f_* = f(x_1, \dots, x_n, 1)$ . Proces vytváření polynomu  $f_*$  nazveme dehomogenizací formy  $f$ .

*Poznámka.* Bod  $\bar{a} \in \mathbb{P}^n(\mathbf{K})$  je kořenem polynomu  $f \in \mathbf{K}[x_1, \dots, x_{n+1}]$ , pokud  $f(x_1, \dots, x_{n+1}) = 0$  pro každou volbu homogenních souřadnic pro  $\bar{a}$ .

**Definice 18** (Řešení soustavy v  $\mathbb{P}^n(\mathbf{K})$ ). Necht  $S \subseteq \mathbf{K}[x_1, \dots, x_{n+1}]$  je soustava polynomiálních rovnic. Pak  $V(S) = \{\bar{a} \in \mathbb{P}^n(\mathbf{K}) : f(\bar{a}) = 0 \ \forall f \in S\}$  je řešením soustavy  $S$ .

**Definice 19** (Projektivní rovinná křivka). Projektivní rovinná křivka je nadplocha v  $\mathbb{P}^2(\mathbf{K})$ . Je jednoznačně určena formou  $f$ , jíž je řešením.

*Poznámka.* Afinní rovinnou křivku můžeme rozšířit do projektivní roviny tím, že místo polynomu  $f$ , jehož je řešením, budeme uvažovat homogenizovaný polynom  $f^*$ , který má o jednu proměnnou víc. Tím vytvoříme projektivní rovinnou křivku.

**Definice 20** (Homogenní ideál). O ideálu  $I \subseteq \mathbf{K}[x_1, \dots, x_{n+1}]$  řekneme, že je homogenní, pokud pro každé  $f = \sum_{i=0}^m f_i \in I$ ,  $f_i$  je forma stupně  $i$ , je také  $f_i \in I$ .

**Věta 4** (Projektivní Hilbertova věta o nulách). Mějme  $I$  je homogenní ideál v  $\mathbf{K}[x_1, \dots, x_{n+1}]$ . Potom

- $V(I) = \emptyset$  právě když existuje celé číslo  $n$  tak, že  $I$  obsahuje všechny formy stupně  $\geq n$ .
- Pokud  $V(I) \neq \emptyset$ , pak  $I(V(I)) = \sqrt{I}$ .

*Poznámka.* Stejně jako v afinním případě nám Hilbertova věta o nulách dává korespondenci projektivních rovinných nadploch (spec. křivek) a bezčtvercových forem.

**Definice 21** (Křížící číslo v projektivním smyslu). Mějme projektivní křivky určené formami  $f, g$ . Definujeme křížící číslo  $I(\bar{a}, f \cap g)$  jako  $\dim_{\mathbf{K}}(\mathcal{O}_{\bar{a}}(\mathbb{P}^2)/(f_*, g_*))$ .

## 1.4 Exaktní posloupnosti

**Definice 22** (R-modul). *Mějme  $R$  komutativní okruh, pak  $R$ -modul je komutativní grupa  $M$  spolu s násobením skalárem z  $R$  (tedy se zobrazením z  $R \times M$  do  $M$ ), která splňuje:*

1.  $(a + b)m = am + bm$  pro  $a, b \in R, m \in M$ ,
2.  $a(m + n) = am + an$  pro  $a \in R, m, n \in M$ ,
3.  $(ab)m = a(bm)$  pro  $a, b \in R, m \in M$ ,
4.  $1_R m = m$  pro  $m \in M$ , kde  $1_R$  je okruhová jednotka vzhledem k násobení v  $R$ .

**Definice 23** (Homomorfismus R-modulů). *Mějme  $R$  okruh,  $M, N$   $R$ -moduly. Zobrazení  $f$  z  $M$  do  $N$  je homomorfismus  $R$ -modulů právě tehdy, když splňuje:*

1.  $f(a + b) = f(a) + f(b)$  pro  $a, b \in M$ ,
2.  $f(ra) = rf(a)$  pro  $r \in R, a \in M$ .

*Poznámka.* V důkazu Bézoutovy věty budeme pracovat pouze s exaktními posloupnostmi vektorových prostorů (definice byla obecnější – vektorové prostory jsou moduly nad tělesem).

**Definice 24** (Exaktní posloupnost). *Mějme  $R$  okruh,  $M_i, i \in \mathbb{N}$   $R$ -moduly,  $\varphi_i : M_i \rightarrow M_{i+1}$  homomorfismy  $R$ -modulů. Řekneme, že posloupnost modulů a zobrazení*

$$M_1 \xrightarrow{\varphi_1} M_2 \xrightarrow{\varphi_2} \dots \xrightarrow{\varphi_n} M_{n+1}$$

*je exaktní, pokud  $\text{Im } \varphi_i = \text{Ker } \varphi_{i+1}$  pro každé  $i \in 1, \dots, n-1$ .*

**Lemma 5.** *Ať  $0 \rightarrow V_1 \xrightarrow{\varphi_1} V_2 \xrightarrow{\varphi_2} V_3 \xrightarrow{\varphi_3} V_4 \rightarrow 0$  je exaktní posloupnost konečně generovaných vektorových prostorů nad tělesem  $\mathbf{K}$ . Pak  $\dim V_4 = \dim V_3 - \dim V_2 + \dim V_1$ .*

*Důkaz.* Pro posloupnost  $0 \rightarrow V_1 \xrightarrow{\psi} V_2 \xrightarrow{\varphi} V_3 \rightarrow 0$  je  $\dim V_2 = \dim V_1 + \dim V_3$  zobecněním věty o dimenzi jádra a obrazu z lineární algebry.

Dále buď  $W = \text{Im } \varphi_2 = \text{Ker } \varphi_3$ . Posloupnosti  $0 \rightarrow V_1 \xrightarrow{\varphi_1} V_2 \xrightarrow{\varphi_2} W \rightarrow 0$  a  $0 \rightarrow W \xrightarrow{\psi} V_3 \xrightarrow{\varphi_3} V_4 \rightarrow 0$  jsou exaktní, tedy  $\dim V_2 = \dim V_1 + \dim W$  a  $\dim V_3 = \dim V_4 + \dim W$ . Z toho dostáváme výsledek  $\dim V_4 = \dim V_3 - (\dim V_2 - \dim V_1)$ .

□

*Poznámka.* Znění a důkaz Věty o dimenzi jádra a obrazu je např. ve skriptech J. Pytlíčka, viz [Pytlíček \(2008\)](#), Věta 33).

## 2. Důkaz Bézoutovy věty

Projektivní rovinu  $\mathbb{P}^2$  jsme konstruovali především proto, abychom mohli zkoumat všechny křížící body libovolných dvou křivek, a abychom se neomezovali na ty afinní. Bézoutova věta nám k tomu dává užitečný nástroj: Že křížící číslo dvou projektivních křivek je přesně dáno a závisí pouze na jejich stupních a na tom, zda mají společnou komponentu, tedy zda jejich určující polynomy jsou soudělné.

V důsledcích Bézoutovy věty budeme používat hlavně fakt, že pokud dvě křivky mají více průsečíků, než je součin jejich stupňů, pak obsahují společnou komponentu, a pokud jsou navíc ireducibilní a jejich stupně se shodují, jedná se o totožné křivky.

Důkaz Bézoutovy věty je přeložen z knihy Williama Fultona ([Fulton, 2008](#)).

**Věta 6** (Bézout). *Mějme dvě různé projektivní rovinné křivky stupňů  $m, n$  určené formami  $f, g$ . Předpokládejme, že nemají společnou komponentu. Potom*

$$\sum_{\bar{a}} I(\bar{a}, f \cap g) = mn.$$

*Důkaz.* Protože  $f \cap g$  je konečná množina (Lemma 1), můžeme předpokládat, že žádný z bodů v průniku  $f \cap g$  neleží v nekonečnu, tedy nemá souřadnici  $z = 0$  (použijeme vhodnou projektivní změnu souřadnic, viz poznámku za důkazem).

Pak

$$\sum_p I(p, f \cap g) = \sum_p I(p, f_* \cap g_*) = \dim_{\mathbf{K}} \mathbf{K}[x, y] / (f_*, g_*),$$

kde první rovnost vyplývá z toho, že  $z = 1$  (křivky  $f, g$  nemají žádný bod průniku v nekonečnu, obě sumy tedy označují stejný součet) a druhá vyplývá z vlastností křížících čísel (Lemma 3).

Označme

$$\Gamma_* = \mathbf{K}[x, y] / (f_*, g_*);$$

$$\Gamma = \mathbf{K}[x, y, z] / (f, g);$$

$$R = \mathbf{K}[x, y, z];$$

$\Gamma_d$  = vektorový prostor forem stupně  $d$  v  $\Gamma$  (prvky  $\Gamma_d$  jsou rozkladové třídy z  $\mathbf{K}[x, y, z] / (f, g)$  reprezentované homogenními polynomy stupně  $d$ );

$R_d$  = vektorový prostor forem stupně  $d$  v  $R$ .

Když ukážeme, že platí rovnosti  $\dim \Gamma_* = \dim \Gamma_d$  a  $\dim \Gamma_d = mn$  pro nějaké velké  $d$  ( $d \geq m + n$ ), věta bude dokázána.

**Část 1:** Dokážeme, že  $\dim \Gamma_d = mn$  pro libovolné  $d \geq m + n$ .

Zdefinujeme si zobrazení:

$$\psi : R \longrightarrow R \times R, \psi(c) = (gc, -fc);$$

$$\varphi : R \times R \longrightarrow R, \varphi(a, b) = (af + bg);$$



$\pi : R \longrightarrow \Gamma$ , přirozená projekce.

Ověříme exaktnost této posloupnosti vektorových prostorů:

$$0 \rightarrow R \xrightarrow{\psi} R \times R \xrightarrow{\varphi} R \xrightarrow{\pi} \Gamma \rightarrow 0$$

Z nulového vektorového prostoru existuje jen jediný homomorfismus, který zobrazí 0 na  $0 \in R$ . Jeho obraz je 0, chceme tedy, aby  $\psi$  bylo prosté.  $\psi$  je prosté, protože  $(0, 0) = (gc, -fc)$  implikuje  $c = 0$  (jsme v oboru integrity a  $f, g$  jsou nenulové formy).

$\text{Im } \psi = \{(u, v) \in R \times R, u = gc, v = -fc\}$ ,  $\text{Ker } \varphi = \{(u, v) \in R \times R, uf + vg = 0\}$ . Ověříme, že jsou podmínky ekvivalentní a obě množiny stejné:

$\text{Im } \psi \subseteq \text{Ker } \varphi$ : Máme  $(u, v) \in \text{Im } \psi$ . Tedy  $u = gc, v = -fc$  pro nějaké  $c \in R$ . Pak  $uf = gcf, vg = -fcg$  a  $gcf - fcg = 0$ .

$\text{Ker } \varphi \subseteq \text{Im } \psi$ : Máme  $(u, v) \in \text{Ker } \varphi$ . Tedy  $uf + vg = 0$ . Víme, že  $f, g$  jsou nesoudělné polynomy a  $u, v$  jsou nějaké polynomy z  $R$ . Napišme  $u$  jako  $u = -\frac{vg}{f}$ , a protože  $f$  nedělí  $g$ , dělí  $v$  a  $-\frac{v}{f}$  je nějaký polynom, označme ho jako  $c$ . Podobně  $v = -\frac{uf}{g}$ , a  $\frac{u}{g}$  je nějaký polynom. Z rovnosti  $uf + vg = 0$  dostaneme, že  $c = \frac{-v}{f} = \frac{u}{g}$ , tedy  $u = gc, v = -fc$ .

$\varphi$  z definice vše zobrazuje na prvky ideálu  $(f, g)$ , a projekce  $\pi$  je zobrazení do okruhu faktorizovaného podle stejného ideálu. Takže  $\text{Im } \varphi = \text{Ker } \pi$ . Přirozená projekce je zobrazení na (každý prvek spadne do již existující třídy ekvivalence, nebo vytvoří novou), tím je ověřena exaktnost posloupnosti, která platí i po restrikci zobrazení na formy určitého stupně:

$$0 \rightarrow R_{d-m-n} \xrightarrow{\psi} R_{d-m} \times R_{d-n} \xrightarrow{\varphi} R_d \xrightarrow{\pi} \Gamma_d \rightarrow 0.$$

Spočítáme  $\dim R_d$ . Generátory  $R_d$  jsou tvaru  $x^i y^j z^{d-i-j}$ . Jejich počet vyjadřuje suma  $\sum_{i=0}^d (d-i+1)$ , kde  $(d-i-1)$  označuje počet přípustných  $j$  u při příslušném  $i$ .

$$\sum_{i=0}^d (d-i+1) = 1 + 2 + \dots + (d+1) = \frac{(d+1)(d+2)}{2}$$

Podle Lemmatu 5 máme vztah

$$\begin{aligned} \dim \Gamma_d &= \dim R_d - \dim R_{d-n} \times R_{d-m} + \dim R_{d-m-n} \\ &= \frac{(d+1)(d+2)}{2} - \left( \frac{(d-n+1)(d-n+2)}{2} + \frac{(d-m+1)(d-m+2)}{2} \right) \\ &\quad + \frac{(d-n-m+1)(d-n-m+2)}{2} \\ &= mn. \end{aligned}$$

**Část 2:** Dokážeme, že zobrazení  $\alpha : \Gamma \longrightarrow \Gamma$  definované jako  $\alpha(\bar{h}) = \overline{zh}$  (kde pruh nad prvkem značí, že prvek patří do rozkladové třídy ideálu  $(f, g)$ ) je prosté.

Musíme ukázat, že pokud  $zh = af + bg$ , pak  $h = a'f + b'g$  pro nějaké  $a', b'$ . Pro  $j \in K[x, y, z]$  označíme  $j_0 = j(x, y, 0)$  (dosazením 0 za třetí souřadnici dostaneme projektivní – nekonečnou část křivky). Vzhledem k tomu, že formy  $f, g$  nemají společné kořeny v nekonečnu,  $f_0, g_0$  jsou nesoudělné formy v  $\mathbf{K}[x, y]$  (jsou to opět formy, dosazením zmizí členy obsahující  $z$  a ostatní zůstanou nezměněny). Pokud

$zh = af + bg$ , pak  $a_0f_0 = -b_0g_0$ , takže  $b_0 = f_0c$  a  $a_0 = -g_0c$  pro nějaké  $c \in K[x, y]$ . Ať  $a_1 = a + cg, b_1 = b - cf$ . Protože  $(a_1)_0 = (b_1)_0 = 0$ , máme  $a_1 = za', b_1 = zb'$  pro nějaké  $a', b'$ . A protože  $zh = a_1f + b_1g$ , dostáváme  $h = a'f + b'g$ .

Z toho, že  $zh = af + bg$  implikuje  $h = a'f + b'g$ , vidíme, že když je  $\overline{zh} = 0$ , tak i  $\overline{h} = 0$ . Ker  $\alpha$  je tedy rovné nule a zobrazení je prosté.

**Část 3:** Ať  $d \geq m + n$ , vybereme formy  $a_1, \dots, a_{mn} \in R_d$ , jejichž zbytky modulo  $(f, g)$  jsou v  $\Gamma_d$  a tvoří v  $\Gamma_d$  bázi (z Části 1 víme, že jich je potřeba právě  $mn$ ). Označme  $a_{i*} = a_i(x, y, 1) \in \mathbf{K}[x, y]$  a  $a'_i$  buď residuum prvku  $a_{i*}$  v  $\Gamma_*$ . Dokážeme, že prvky  $a'_1, \dots, a'_{mn}$  tvoří bázi pro  $\Gamma_*$ .

Použijeme zobrazení  $\alpha$  definované v části 2. Dokázali jsme, že je prosté, a použijeme restrikci  $\alpha$  na  $\Gamma_d \rightarrow \Gamma_{d+1}$ . Tato restrikce už je bijektivní, protože je to injektivní homomorfismus vektorových prostorů stejné dimenze (viz část 1).

Tedy všechny  $\Gamma_d$  jsou navzájem izomorfní a použitím zobrazení  $\alpha$  máme univerzální předpis báze pro  $\Gamma_{d+r}$  pro všechna  $r \geq 0$ .

Nyní chceme dokázat, že  $a'_i$  tvoří bázi  $\Gamma_*$ .

**Generování:** Když  $h' = \overline{h} \in \Gamma_*$ ,  $h \in \mathbf{K}[x, y]$ , pro vhodné  $n$  je  $z^n h^*$  forma stupně  $d + r$ , tedy  $z^n h^* = \sum_{i=1}^{mn} \lambda_i z^r a_i + (bf + cg)$  pro nějaká  $\lambda_i \in \mathbf{K}, b, c \in \mathbf{K}[x, y, z]$ . Po dehomogenizaci máme  $h = (z^n h^*)_* = \sum_{i=1}^{mn} \lambda_i a_{i*} + (b_*f_* + c_*g_*)$ , a  $h' = \sum_{i=1}^{mn} \lambda_i a'_i$ .

**Nezávislost:** Když  $\sum \lambda_i a'_i = 0$ , tak  $\sum \lambda_i a_{i*} = (bf_* + cg_*)$ . Proto (podle vlastností homogenizace) pro nějaká  $r, s, t$  platí  $z^r \sum \lambda_i a_i = (z^s b^* f + z^t c^* g)$ . Potom je ale  $\sum \lambda_i \overline{z^r a_i} = 0$  v  $\Gamma_{d+r}$ , a prvky  $\overline{z^r a_i}$  tam tvoří bázi, tedy každé  $\lambda_i = 0$ .

□

*Poznámka.* V důkazu Bézoutovy věty mluvíme o projektivní změně souřadnic. Můžeme použít například tuto: Předpokládejme, že křivky mají konečný počet průsečíků na přímce v nekonečnu a konečný počet průsečíků v afinní rovině. Protože máme prostor nad nekonečným tělesem ( $\mathbf{K}$  je algebraicky uzavřené, tedy nekonečné), můžeme vybrat afinní přímku  $L$  tak, aby neprocházela žádným bodem v nekonečnu (vybereme jiný směr) ani žádným afinním bodem (protože je jich konečně mnoho, takovou přímku najdeme). Nyní použijeme afinní transformaci celého prostoru - otočíme s ním tak, aby přímka  $L$  byla na místě osy  $x$  (tedy budeme mít nově přímku  $y = 0$ ). Nakonec vyměníme proměnnou  $y$  za  $z$  a budeme se moci na  $L$  dívat jako na přímku v nekonečnu. Všechny body, které přímka  $L$  neobsahuje, tedy i všechny průsečíky, budou ležet v afinní rovině.

## 3. Důsledky Bézoutovy věty

### 3.1 Cayley-Bacharachova věta

Mezi nejsilnější důsledky Bézoutovy věty patří Cayley-Bacharachova věta, která nám pomůže dokázat větu Pappovu i Pascalovu a skoro přímočaře z ní plyne i asociativita sčítání na eliptických křivkách. Cayley-Bacharachova věta, v literatuře uváděná i jako Chaslesova věta (podle Michela Chaslese) mluví o kubikách: konkrétně o případě, kdy dvě kubiky s devíti společnými průsečíky určují podmínku pro libovolnou další kubiku, která s nimi sdílí libovolných osm z nich. Speciálními případy, kdy nejsou některé z těchto kubik ireducibilní a rozpadají se na přímky a kuželosečky, se zabývá Pappus a Pascal; jejich věty byly vysloveny dříve než obecnější a silnější věta Cayley-Bacharachova mluvící o kubikách.

Podkapitola 3.1 čerpá z článku Eisenbuda, Greena a Harrise (Eisenbud a kol., 1996). Důkazy 3.2, 3.3 a 3.4 jsou napsány na základě stránky Terence Taa (Tao, 2011) a knihy Williama Fultona (Fulton, 2008). Speciálně definice sčítání v podkapitole 3.4 je v souladu s knihou L. Washingtona (Washington, 2008).

V celé kapitole budeme pracovat s projektivní rovinou nad algebraicky uzavřeným tělesem  $\mathbf{K}$ .

**Definice 25** (Kodimenze). *Ať  $W$  je vektorový podprostor prostoru  $V$ . Kodimenze  $W$  ve  $V$  je definována jako  $\dim V - \dim W$  (neboli dimenze faktoru  $V/W$ ).*

**Definice 26.** *Ať  $M = \{p_1, \dots, p_n\}$  je množina  $n$  různých bodů. Řekneme, že množina  $M$  ukládá (klade, dává)  $l$  podmínek na formy (z  $\mathbf{K}[x, y, z]$ ) stupně  $d$ , pokud má podprostor forem stupně  $d$  nulujících ve všech bodech z  $M$  kodimenzi vzhledem k prostoru všech forem stupně  $d$  rovnou  $l$ .*

*Poznámka.* Obdobně řekneme, že množina  $M$  klade  $l$  podmínek na křivky stupně  $d$  (uvažujeme kodimenzi podprostoru forem stupně  $d$ , které křivky určují).

*Poznámka.* Přidávání podmínek na křivky si můžeme představit jako přidávání lineárních rovnic a hledání prostoru řešení. S každým novým bodem v množině přidáváme jednu další podmínku (ne víc), a každý typ křivek má svůj maximální počet nezávislých podmínek, které na ně můžeme klást, a stále být schopni najít netriviální řešení.

*Příklad.* Vezměme si křivky stupně 1 – přímky v rovině. Pokud máme množinu o jednom bodu, dimenze prostoru forem stupně 1 nulujících se v tomto bodě je 2, tedy kodimenze (dimenze prostoru všech forem stupně 1 faktorizovaného podle podprostoru forem stupně 1 nulujících se v určeném bodě) je 1. Máme tedy jednu podmínku. Přidáme-li další bod (různý od prvního), tyto dva body už přímku určí jednoznačně, dimenze prostoru řešení se zmenší na 0, dimenze faktoru vzroste na 2, máme tedy 2 nezávislé podmínky. Každý další bod přidáný do množiny tak, že nalezneme přímku obsahující všechny body z množiny ( netriviální řešení soustavy), už bude kolineární s původními dvěma a stejně jako u přidávání další lineární rovnice (která pro nalezení netriviálního řešení musí být lineárně závislá na původních dvou) přidáme jen další závislou podmínku. V případě přidání další nezávislé podmínky (bodu, který není kolineární s předchozími) dostáváme pouze nulové řešení.

K důkazu tvrzení se nám bude hodit následující lemma:

**Lemma 7.** *Dimenze prostoru forem stupně  $d$  v  $\mathbf{K}[x, y, z]$  je rovna  $\binom{d+2}{2}$ .*

*Důkaz.* Generátory prostoru jsou tvaru  $x^i y^j z^{d-i-j}$ . Jejich počet vyjadřuje suma  $\sum_{i=0}^d (d-i+1)$ , kde  $(d-i-1)$  označuje počet přípustných  $j$  při příslušném  $i$ .

$$\sum_{i=0}^d (d-i+1) = 1 + 2 + \cdots + (d+1) = \frac{(d+1)(d+2)}{2} = \binom{d+2}{2}.$$

□

*Poznámka.* Stejně vyjde i dimenze prostoru polynomů stupně maximálně  $d$  v  $\mathbf{K}[x, y]$ .

**Tvrzení 8.** *Ať  $\Omega = \{p_1, \dots, p_n\} \subseteq \mathbb{P}^2(\mathbf{K})$  je libovolná množina  $n \leq 2d+2$  různých bodů. Pak body z  $\Omega$  nekladou nezávislé podmínky na křivky stupně  $d$  právě tehdy, když nastane některá z možností: Buď  $d+2$  z bodů v  $\Omega$  leží na jedné přímce, nebo  $n = 2d+2$  a  $\Omega$  je obsažena v kvadrice.*

*Poznámka.* Body z množiny  $M$  nekladou nezávislé podmínky na křivky stupně  $d$  právě tehdy, když je kodimenze (ve smyslu jako výše) menší než počet bodů v množině  $M$ . Pro zpětnou implikaci budeme tedy dokazovat, že na základě předpokladů na pravé straně ekvivalence vypočítáme, jaký je maximální počet nezávislých podmínek kladených množinou  $\Omega$  a dojdeme k tomu, že je menší než počet bodů v množině  $\Omega$ .

*Důkaz.*

**Implikace zprava doleva:**

Ať  $d+2$  z bodů v  $\Omega$  leží na jedné přímce, označme ji  $l$ . Pak z Bézoutovy věty libovolná křivka stupně  $d$  obsahující  $\Omega$  už musí obsahovat i přímku  $l$  (pokud  $d = 1$ , pak je to sama přímka  $l$ , a pro křivky vyššího stupně máme z Bézoutovy věty maximální možný počet průsečíků s přímkou rovný  $d \cdot 1$ , jinak mají společnou komponentu, a tou je přímka, která je ireducibilní).

Nyní chceme spočítat, kolik podmínek ukládají body v  $\Omega$ . Spočteme proto kodimenzi podprostoru forem určujících křivky obsahující  $l$  – tu dostaneme jako rozdíl dimenze prostoru všech forem stupně  $d$  a dimenze podprostoru těch, které určují křivky obsahující  $l$ , tedy  $\binom{d+2}{2} - \binom{d+1}{2} = d+1$ . Těchto  $d+2$  bodů ležících na jedné přímce tedy dává jen  $d+1$  podmínek, a dohromady se zbylými body v  $\Omega$  dávají pouze  $n-1$  nezávislých podmínek. Obdobně budeme postupovat i v případě, kdy předpokládáme, že  $n = 2d+2$  a  $\Omega$  je obsažena v kvadrice. Prostor forem stupně  $d$ , které určují křivky obsahující kvadriku, mají dimenzi stejnou jako prostor všech forem stupně  $d-2$ . Máme tedy maximálně  $\binom{d+2}{2} - \binom{d}{2} = 2d+1$  nezávislých podmínek kladených množinou  $\Omega$  na křivky stupně  $d$ .

**Implikace zleva doprava:**

Důkaz této implikace si rozdělíme na několik případů podle velikosti parametrů  $d$  a  $n$ . Postupně budeme dokazovat případy:

1.  $d = 1$ ;

2.  $d > 1; n \leq d + 1$ ;
3.  $d > 1; d + 1 < n \leq 2d + 2$ ;
  - (a)  $d + 2$  a více bodů z  $\Omega$  leží na přímce;
  - (b) právě  $d + 1$  bodů z  $\Omega$  leží na přímce;
  - (c) alespoň 3 body z  $\Omega$  leží na přímce;
  - (d) žádné tři body z  $\Omega$  neleží na přímce.

Pro  $d = 1$  stačí dokazovat větu pro  $n = 3, 4$  (pro menší  $n$  máme nezávislost podmínek z příkladu výše). Je zřejmé, že pokud klade množina o 3 bodech závislé podmínky, tak jsou  $3 = d + 2$  body kolineární, a pokud má množina 4 body, pak  $n = 2d + 2$  a všechny body jsou obsažené v nějaké kvadrice (v případě, že jsou 3 nebo 4 body kolineární, bude se jednat o sjednocení dvou přímek).

Pro zbytek důkazu budeme bez újmy na obecnosti předpokládat, že libovolná vlastní podmnožina  $\Omega$  dává nezávislé podmínky na křivky stupně  $d$ . Z tohoto předpokladu a z levé části implikace plyne výrok, který označíme jako (\*):

*Libovolná rovinná křivka stupně  $d$  obsahující všechny body z  $\Omega$  kromě jednoho obsahuje celou množinu bodů  $\Omega$ .*

Když tedy dokážeme pro jednotlivé skupiny bodů a křivek, že z (\*) plyne jedna z podmínek napravo, bude důkaz dokončen.

Pro  $d > 1; n \leq d + 1$  sestojíme křivku stupně  $d$ , která prochází všemi body kromě jednoho (použijeme například přímky  $L_i$ , které postupně procházejí body  $p_1, \dots, p_{n-1}$ , ale neprocházejí  $p_n$ , a případně ještě přidáme přímky, které neprocházejí žádnými body pro dorovnání stupně). Vyvrátili jsme pro tento případ výrok (\*), tedy není co dokazovat (v tomto případě se nikdy nestane závislost podmínek).

Pro případ, že  $d + 2$  a více bodů z  $\Omega$  leží na přímce, je důkaz triviální.

Ať právě  $d + 1$  bodů z  $\Omega$  leží na přímce  $L$ . Označme  $\Omega'$  množinu bodů ležících mimo přímku  $L$ . Můžeme tvrdit, že  $\Omega'$  nedává nezávislé podmínky na křivky stupně  $d - 1$  (kdyby tomu tak bylo, našli bychom křivku stupně  $d - 1$ , která prochází všemi body z  $\Omega'$  kromě jednoho, a ve sjednocení s přímkou  $L$  bychom měli křivku stupně  $d$ , která prochází všemi body z  $\Omega$  kromě jednoho, a to je ve sporu s předpokladem věty). Z indukčního předpokladu, že implikace platí pro všechny menší  $n$  a  $d$  dostáváme, že  $\Omega'$  obsahuje alespoň  $d + 1$  bodů, a ty jsou všechny kolineární (je jich tam maximálně  $d + 1$ , a to je málo pro druhou podmínku s kvadrikou). Když tedy platí (\*) a  $\Omega$  obsahuje přesně  $d + 1$  bodů na přímce  $L$ , tak zbylých bodů je právě  $d + 1$  a leží na přímce  $M$ . Dostáváme kvadriku  $L \cup M$ , která obsahuje celou  $\Omega$ .

Nyní ať alespoň 3 body z  $\Omega$  leží na přímce  $L$ , označme  $l$  jejich počet,  $\Omega' = \Omega \setminus \{p_1, \dots, p_l\}$ ,  $|\Omega'| \leq 2d - 1$ . Použijeme stejný argument jako v předchozím odstavci –  $\Omega'$  nemůže dát nezávislé podmínky na křivky stupně  $d - 1$ , tedy musí obsahovat alespoň  $d + 1$  kolineárních bodů. Tím pádem jsme důkaz převedli na předchozí případ.

Zbývá větu dokázat pro případ, kdy žádné tři body z  $\Omega$  neleží na přímce. Vybereme libovolné tři body z  $\Omega$ , označme  $\Omega' = \Omega \setminus \{p_1, p_2, p_3\}$ . Kdyby pro libovolné  $i$  dávala množina  $\Omega' \cup \{p_i\}$  nezávislé podmínky na křivky stupně  $d - 1$ , pak jsme hotovi, protože bychom našli křivku  $C$  obsahující všechny body kromě bodu  $p_i$ ,

a sjednocení křivky  $C$  a přímky spojující zbylé dva body v  $\Omega$  by bylo přímkou stupně  $d$  vynechávající poslední bod, tím pádem bychom vyvrátili (\*). Dále tedy můžeme předpokládat, že  $\Omega' \cup \{p_i\}$  nezávislé podmínky na křivky stupně  $d-1$  nedává. Protože naše množina  $\Omega$  nemůže obsahovat  $d+1$  bodů na přímce, z indukce plyne, že  $n = 2d+2$  a každá z množin  $\Omega' \cup \{p_i\}$  leží na kvadrice  $C_i$ ,  $i = 1, 2, 3$ . Pro případ  $d = 2$  důkaz končí – množina o šesti bodech nedává nezávislé podmínky na kvadriky právě tehdy, když celá leží na kvadrice. Ať  $d > 2$ . Žádné tři body nejsou kolineární, a v každé množině  $\Omega' \cup \{p_i\}$  je alespoň 6 bodů, máme tedy  $C_1 = C_2 = C_3$  z Bézoutovy věty a celá  $\Omega$  leží na kvadrice  $C_1 = C_2 = C_3$ .  $\square$

**Věta 9** (Cayley-Bacharach). *Ať  $X_1, X_2 \subset \mathbb{P}^2(\mathbf{K})$  jsou dvě kubické křivky, které nemají společnou komponentu, ale protínají se v devíti různých bodech  $p_1, \dots, p_9$ . Označme  $X \subset \mathbb{P}^2(\mathbf{K})$  kubickou křivku, která obsahuje body  $p_1, \dots, p_8$ . Pak  $X$  obsahuje i bod  $p_9$ .*

*Důkaz.* Pokud  $\Gamma = \{p_1, \dots, p_9\}$  je množina bodů v průniku  $X_1, X_2$ , a  $\Gamma' = \{p_1, \dots, p_8\}$  je libovolná podmnožina vynechávající jeden bod, pak je tvrzení věty ekvivalentní výroku, že  $\Gamma$  a  $\Gamma'$  kladou na kubické křivky stejný počet nezávislých podmínek. V tomto případě je jich právě osm, víc jich být nemůže (máme k dispozici osm bodů v  $\Gamma'$ ), a že jich není méně, ukážeme ve zbytku důkazu.

Na začátek použijeme tuto úvahu: Desetidimenzionální vektorový prostor kubických forem obsahuje alespoň dvoudimenzionální podprostor těch, které se nulují na bodech z  $\Gamma$ , konkrétně ten generovaný dvěma formami určujícími křivky  $X_1, X_2$ . Z toho je zřejmé, že  $\Gamma$  neklade nezávislé podmínky. Na zbytek důkazu použijeme tvrzení dokázané výše.

Vezmeme  $\Omega = \Gamma'$ ,  $n = 8$ ,  $d = 3$ . Z Bézoutovy věty plyne, že pokud by  $\Gamma'$  ležela na kuželosečce  $C$ , pak by ji  $X_1$  i  $X_2$  musely obsahovat, a podobně pokud by 4 a více bodů z  $\Gamma'$  leželo na přímce  $L$ ,  $X_1$  i  $X_2$  by musely obsahovat  $L$ . Protože jsme předpokládali, že křivky  $X_1, X_2$  nemají společnou komponentu, pak  $\Gamma'$  musí klást na kubické křivky osm nezávislých podmínek. Tím je důkaz dokončen.  $\square$

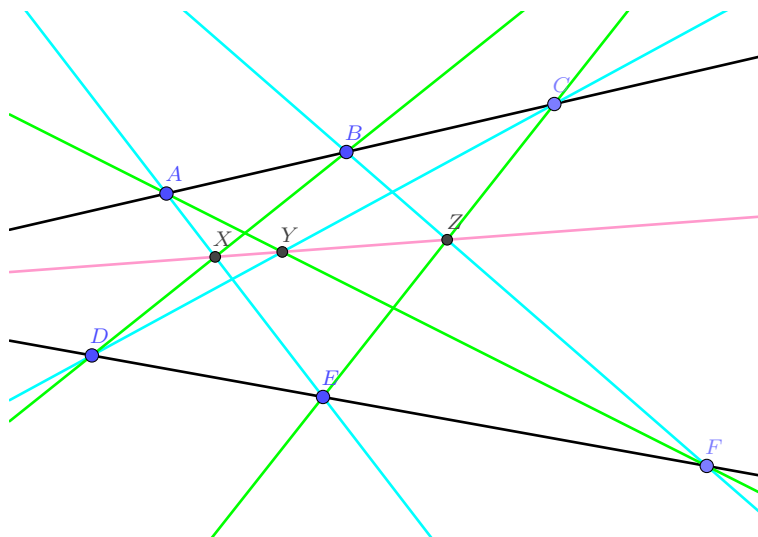
## 3.2 Pappova věta

**Věta 10** (Pappus). *Ať  $l, l'$  jsou dvě různé přímky (křivky definované formami  $f, g$ ), a  $A, B, C$  různé body ležící na  $l$ , které neleží na  $l'$ ,  $D, E, F$  různé body ležící na  $l'$ , které neleží na  $l$ . Předpokládejme, že přímky  $\overline{AE}, \overline{BF}, \overline{CD}$  protínají popořadě přímky  $\overline{BD}, \overline{CE}, \overline{AF}$ . Pak jejich tři průsečíky  $X, Y, Z$  leží na jedné přímce.*

*Důkaz.* Můžeme předpokládat, že  $X, Y, Z$  jsou po dvou různé, jinak by bylo tvrzení triviální.

Označme  $x_1$  sjednocení přímek  $\overline{AE}, \overline{BF}, \overline{CD}$  (modré přímky na Obr. 3.1),  $x_2$  sjednocení  $\overline{BD}, \overline{CE}, \overline{AF}$  (zelené přímky) a  $x_3$  sjednocení  $l, l', \overline{XZ}$  (dvě černé a jedna růžová přímka).

Z definice jsou  $x_1$  a  $x_2$  kubické křivky bez společné komponenty, které se protínají v 9 bodech. Také  $x_3$  je kubická křivka, a navíc se protíná s  $x_1$  a  $x_2$  v osmi



Obrázek 3.1: Pappova věta

bodech. Podle Cayley-Bacharachovy věty tedy také obsahuje bod devátý, čímž je  $Y$ . Protože  $Y$  nemůže ležet na  $l$  ani  $l'$ , musí ležet na poslední přímce, která je částí kubiky  $x_3$ .

□

### 3.3 Pascalův šestiúhelník

Pascalova věta o šestiúhelníku je variantou věty Pappovy, s tím rozdílem, že neuvažujeme šest bodů ležících na dvou přímkách, ale šest bodů ležících na jedné kuželosečce, tedy křivce stupně dva. Tu můžeme chápat i jako křivku určenou součinem polynomů určujících dvě přímky v Pappově větě.

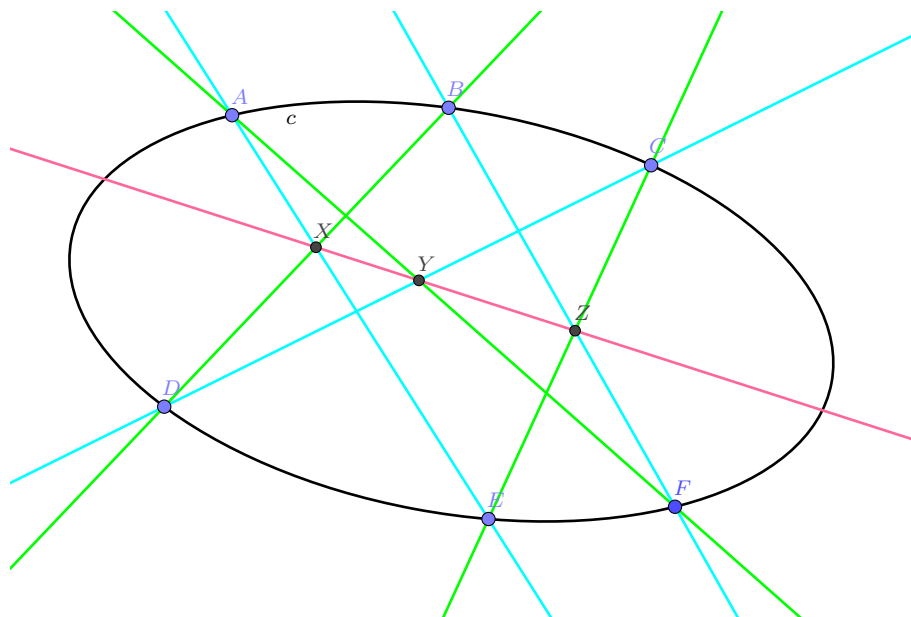
**Věta 11** (Pascal). *Ať  $f$  je forma, která určuje ireducibilní kvadratickou křivku  $c$ .  $A, B, C, D, E, F$  nechť jsou po dvou různé body ležící na  $c$ . Pokud přímky  $\overline{AE}, \overline{BF}, \overline{CD}$  protínají popořadě přímky  $\overline{BD}, \overline{CE}, \overline{AF}$ , pak jejich tři průsečíky  $X, Y, Z$  leží na jedné přímce.*

*Důkaz.* Důkaz je úplně stejný jako důkaz Pappovy věty, jen místo sjednocení přímek  $l \cap l'$  uvažujeme kvadriku  $c$  (Obr. 3.2).

□

### 3.4 Eliptické křivky

Posledním důsledkem Bézoutovy, a hlavně Cayley-Bacharachovy věty, který má navíc obrovské využití v kryptografické praxi, je důkaz, že eliptické křivky spolu se sčítáním, nulou a inverzem tvoří abelovskou grupu. Nejprve zadefinujeme eliptické křivky a vysvětlíme způsob, jak se na nich body dají sčítat, a potom se dostaneme k důkazu asociativity, který využívá výše dokázané věty.



Obrázek 3.2: Pascalův šestiúhelník

**Definice 27** (Eliptická křivka). Eliptická křivka je rovinná křivka (kubika) zadaná rovnicí (polynomem)

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

který má pouze jednoduché kořeny, popřípadě projektivní křivka určená formou vzniklou homogenizací tohoto polynomu.

Nejprve musíme zadefinovat sčítání bodů a upřesnit ho pro všechny možné případy, které mohou nastat. Začneme se dvěma body na křivce,  $P_1 = (x_1, y_1, z_1)$  a  $P_2 = (x_2, y_2, z_2)$ . Uvažujme eliptickou křivku  $e$  v projektivním smyslu – tedy zadanou polynomem

$$y^2 z = x^3 + Axz^2 + Bz^3,$$

Pak definujeme součet bodů  $P_1 + P_2 = P_3 = (x_3, y_3, z_3)$  takto: Uvažujme přímku  $l$  procházející body  $P_1, P_2$ . Součin stupňů přímky a kubiky je 3 a můžeme tedy ještě hledat jeden průsečík.

Může se nám stát několik případů:

**Oba body jsou afinní a mají rozdílnou souřadnici  $x$ .** Pak směrnice přímky  $l$  je  $m = \frac{y_2 - y_1}{x_2 - x_1}$ , tedy její rovnici můžeme napsat jako

$$y = m(x - x_1) + y_1.$$

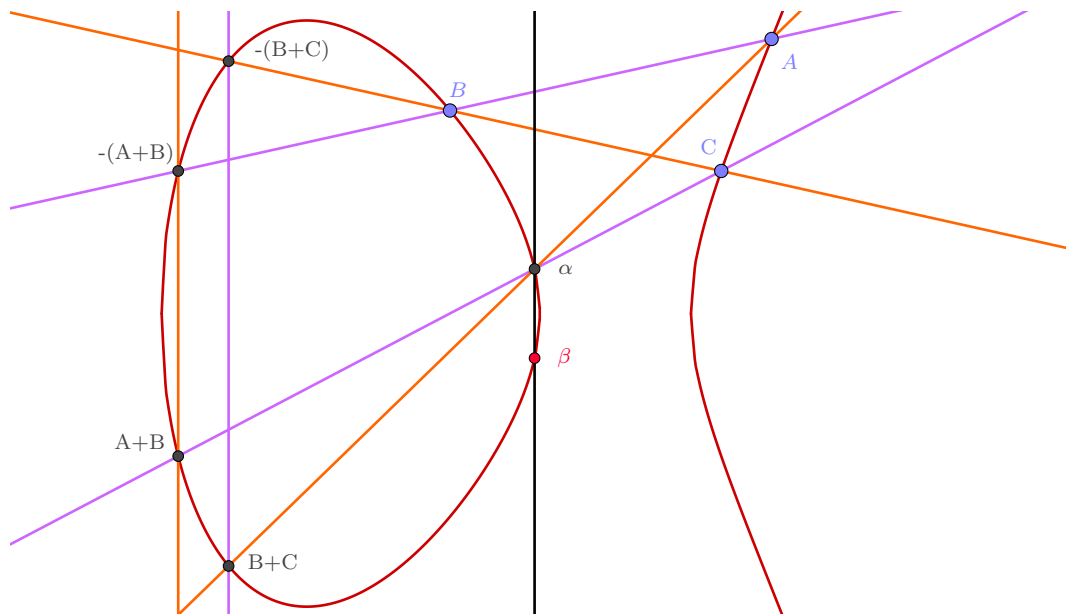
Body průniku s křivkou  $e$  najdeme tak, že rovnici křivky (hledáme afinní bod, za  $z$  si tedy dosadíme 1) a přímky porovnáme, a upravíme-li vzniklý výraz, dostaneme kubický polynom:

$$0 = x^3 - m^2 x^2 + \dots$$

Kubický polynom má v algebraicky uzavřeném tělese tři kořeny, z toho dva už známe (souřadnice bodů, které sčítáme). Můžeme ale polynom upravit:

$$x^3 + ax^2 + bx + c = (x - r)(x - s)(x - t) = x^3 - (r + s + t)x^2 + \dots$$





Obrázek 3.3: Asociativita sčítání na eliptické křivce

Zde známe kořeny  $r, s$ , tedy  $t = -a - r - s$ . V našem případě dostaneme

$$x = -x_1 - x_2 + m^2;$$

$$y = m(x - x_1) + y_1,$$

a po dosazení a reflexi

$$x_3 = -x_1 - x_2 + m^2;$$

$$y_3 = -m(x_2 - x_1) - y_1.$$

Protože jsme zůstali v afinní rovině, třetí souřadnice zůstává rovna jedné.

**Oba body jsou afinní a mají stejnou souřadnici  $x$ .** Jejich spojnice (resp. tečna, pokud  $y_1 = y_2 = 0$ ) je tedy vertikální a protíná se s křivkou v nekonečnu, tedy v bodě  $(0, 1, 0)$ . Při reflexi podle osy  $x$  zůstává bod stejný, protože body v opačném směru v nekonečnu ztotožňujeme.

**Oba body jsou afinní a mají stejnou souřadnici  $x$  i  $y$ ,  $y$  nenulové.** Pak místo spojnice  $l$  uvažujeme tečnu  $l$  v příslušném bodě. Její směrnici určíme pomocí implicitní derivace a je rovna  $m = \frac{3x_1^2 + A}{2y_1}$ .

**Jeden z bodů je  $(0, 1, 0)$ .** Pak zadefinujeme, že součet bodu  $P$  a  $(0, 1, 0)$  je rovný  $P$ . Pokud totiž vedeme vertikální přímkou bodem  $P$ , buď je to dvojnásobný kořen (a jsme u konce, protože není co reflektovat), a nebo najdeme třetí průsečík s křivkou  $-P$ , a ten zreflektujeme zpět na původní bod.

Posledním omezením je charakteristika tělesa, nad kterým počítáme. Pokud má těleso charakteristiku rovnou 2 nebo 3, musíme definici upravit, protože se v ní vyskytují konstanty 2 a 3.

Poznatky shrneme do následující definice:

**Definice 28** (Sčítání bodů na eliptické křivce). *Ať je charakteristika tělesa, nad kterým pracujeme, různá od 2 a 3. Mějme eliptickou křivku  $e$  zadanou formou*

$$y^2z = x^3 + Axz^2 + Bz^3,$$

body  $P_1 = (x_1, y_1, z_1)$  a  $P_2 = (x_2, y_2, z_2)$  ležící na  $e$ . Pak součet  $P_1 + P_2 = P_3 = (x_3, y_3, z_3)$  je definován jako:

1. Pokud  $x_1 \neq x_2$  a  $z_1 = z_2 = 1$ , pak  $x_3 = m^2 - x_1 - x_2$ ,  $y_3 = m(x_1 - x_3) - y_1$ , kde  $m = \frac{y_2 - y_1}{x_2 - x_1}$ .
2. Pokud  $x_1 = x_2$ , ale  $y_1 \neq y_2$ , pak je  $P_1 + P_2 = (0, 1, 0)$ .
3. Pokud  $P_1 = P_2$  a  $y_1 \neq 0$ , pak  $x_3 = m^2 - 2x_1$ ,  $y_3 = m(x_1 - x_3) - y_1$ , kde  $m = \frac{3x_1^2 + A}{2y_1}$ .
4. Pokud  $P_1 = P_2$  a  $y_1 = 0$ , pak  $P_1 + P_2 = (0, 1, 0)$ .
5. Pokud  $P_2 = (0, 1, 0)$ , pak  $P_1 + P_2 = P_1$ .

**Tvrzení 12.** *Elipsoidická křivka  $e$  spolu se sčítáním + zadaným výše, identitou  $\mathcal{O} = (0, 1, 0)$  a inverzem  $-$  (reflexí podle osy  $x$ ) tvoří abelovskou grupu.*

*Důkaz.* Nejprve dokážeme jednodušší části: Komutativita je zřejmá, protože přímka propojující body  $P_1, P_2$  je stejná jako ta, která propojuje body  $P_2, P_1$ . Existence identity  $\mathcal{O}$  vychází z bodu 5 v definici sčítání. Pokud položíme  $-P$  rovné reflexi bodu  $P$  podle osy  $x$ , máme  $P + (-P) = \mathcal{O}$ , máme tedy existenci inverzů.

Nejsložitější je dokázat asociativitu, tedy že pro každé body  $A, B, C \in e$  platí

$$(A + B) + C = A + (B + C).$$

Dokážeme obecnou verzi, tedy případ, kdy  $\mathcal{O}, A, B, C, A + B, B + C, -(A + B), -(B + C)$  jsou po dvou různé body na křivce  $e$  a všechny jsou různé od  $-((A + B) + C), -(A + (B + C))$ .

Ať  $\gamma$  je sjednocení třech přímek  $\overline{AB}, \overline{C(A + B)}, \overline{\mathcal{O}(B + C)}$  (fialové přímky na Obr. 3.3),  $\gamma'$  je sjednocení třech přímek  $\overline{BC}, \overline{A(B + C)}, \overline{\mathcal{O}(A + B)}$  (oranžové přímky na Obr. 3.3). Vidíme, že  $\gamma$  a elipsoidická křivka  $e$  jsou kubické křivky, které nemají žádnou společnou komponentu, a mají devět společných bodů:  $\mathcal{O}, A, B, C, A + B, -(A + B), B + C, -(B + C), -((A + B) + C)$ . Kubická křivka  $\gamma'$  prochází prvními osmi z těchto bodů, tedy z Věty 9 plyne, že prochází i bodem  $-((A + B) + C)$ . To implikuje, že přímka spojující body  $A$  a  $B + C$  protíná křivku  $e$  v bodech  $-(A + (B + C))$  i  $-((A + B) + C)$ , které se tedy musí shodovat (bod  $\alpha$  na Obr. 3.3). Po reflexi podle osy  $x$  dostáváme  $(A + B) + C = A + (B + C)$  (bod  $\beta$  na Obr. 3.3).

□

*Poznámka.* Důkaz Tvrzení 12 je neúplný, platí jen pro případy, kdy jsou všechny body po dvou různé a přímky mezi nimi nesplývají. Kompletní důkaz je nad rámec této práce a je napsán např. v knize L. Washingtona (Washington, 2008).

# Závěr

Po dočtení této práce by měl čtenář mít jasno v základních pojmech algebraické geometrie a měl by chápat nutnost v určité chvíli eukleidovskou rovinu rozšířit a vybudovat si aparát, jak pracovat s abstrakcí v nekonečnu. Čtenářovi by měl mít možnost přecházet si srozumitelně rozepsaný důkaz Bézoutovy i Cayley-Bacharachovy věty, které jsou pomyslnými vrcholy práce, a měl by mít povědomí o tom, že poté již není obtížné (i když technicky celkem náročné) si rozmyslet důkaz asociativity sčítání na eliptických křivkách.

Dílčím cílem práce bylo ukázat, že dlouhá cesta od Pappuse z Alexandrie do moderních dob byla potřeba k tomu, aby fungovaly některé kryptosystémy, bez kterých by se dnešní civilizace neobešla.

# Seznam použité literatury

- EISENBUD, D., GREEN, M. a HARRIS, J. (1996). Cayley-Bacharach Theorems and Conjectures. *Bulletin (New Series) of the American Mathematical Society*, **33**, 298–303.
- FULTON, W. (2008). *Algebraic Curves*. Elektronické vydání. Dostupné z [www.math.lsa.umich.edu/~wfulton/CurveBook.pdf](http://www.math.lsa.umich.edu/~wfulton/CurveBook.pdf).
- PYTLÍČEK, J. (2008). *Lineární algebra a geometrie*. Třetí vydání. Česká technika – nakladatelství ČVUT, Praha. ISBN 978-80-01-04063-8.
- RICHTER-GEBERT, J. (2010). *Prospectives of Projective Geometry*. Springer.
- TAO, T. (2011). *Pappus's theorem and elliptic curves*. [online]. Dostupné z [terrytao.wordpress.com/2011/07/15/pappuss-theorem-and-elliptic-curves/](http://terrytao.wordpress.com/2011/07/15/pappuss-theorem-and-elliptic-curves/).
- WASHINGTON, L. C. (2008). *Elliptic Curves: Number Theory and Cryptography*. Second Edition. Taylor Francis Group, LLC, University of Maryland, College Park, Maryland. ISBN 978-1-4200-7146-7.