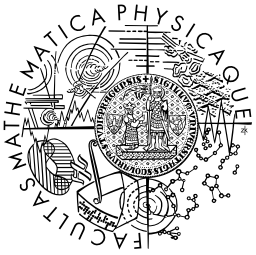


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Marie Skalová

Aplikace Groebnerových bází

Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Pavel Příhoda, Ph.D.

Studijní program: Matematika

Studijní obor: Matematika pro informační technologie

Praha 2020

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

Děkuji svému vedoucímu bakalářské práce doc. Mgr. Pavlu Příhodovi, Ph.D. za odborné vedení. Nejvíce si vážím trpělivosti, vstřícnosti a věcnosti během komunikace i samotných konzultací. Jeho cenné rady a připomínky mi velice pomáhaly během vypracovávání mé práce.

Název práce: Aplikace Groebnerových bází

Autor: Marie Skalová

Katedra: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. Pavel Příhoda, Ph.D., Katedra algebry

Abstrakt: Groebnerovy báze lze využít jako nástroj algebraické geometrie s aplikací v dokazování geometrických tvrzení. V této práci představujeme metodu automatického dokazování geometrických tvrzení ve dvou variantách, nejprve podle učebnice D. Cox, J. Little, D. O'Shea Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra, následně podle učebnice D. Stanovský, L. Barto, Počítačová algebra. Nejprve zde shrneme potřebnou teorii k odvození metody automatického dokazování. Dále teorii potřebnou k definici Groebnerovy báze a k vyslovení vět popisující její základní vlastnosti. Součástí práce jsou řešené příklady, na kterých jednotlivé kroky metody motivujeme, a také řešené příklady z již zmíněné učebnice autorů D. Cox, J. Little, D. O'Shea, některé z nich oběma variantami. V druhé kapitole se nachází vlastní důkaz rozkladu konkrétní algebraické množiny.

Klíčová slova: Groebnerova báze, algebraická geometrie, geometrie

Title: Applications of Groebner bases

Author: Marie Skalová

Department: Department of algebra

Supervisor: doc. Mgr. Pavel Příhoda, Ph.D., Department of algebra

Abstract: Groebner bases are useful tool from algebraic geometry for geometry proving. In the thesis we are presenting an automatic geometric theorem proving method in two variants. First the variant from the book D. Cox, J. Little, D. O'Shea Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra and then the variant from the book D. Stanovský, L. Barto, Počítačová algebra. We summarize theory necessary for deduction of the method, then theory necessary for definition of Groebner base and theorem about her properties. The thesis is including solved exercises used for motivate several steps in method and solved exercises from already mentioned book by D. Cox, J. Little, D. O'Shea, some of them are solved by both variants. There is also own proof of decomposition of an affine variety in chapter 2.

Keywords: Groebner base, algebraic geometry, geometry

Obsah

Úvod

Už od starověkého Řecka se matematici zabývali důkazy geometrických tvrzení. V polovině 20. století však přichází matematici tehdejší doby s myšlenkou automatického dokazování. V souvislosti se vznikem této myšlenky jsou zmiňováni matematici A. Tarski [1], H. Gelertner [2] nebo Wu Wenjun [3]. V této práci se budeme zabývat aplikací Groebnerových bází ve spojení právě s metodou automatického dokazování geometrických tvrzení.

Metoda využívá propojení eukleidovské geometrie a soustav polynomiálních rovnic. Konkrétně geometrických vlastností útvarů v eukleidovské geometrii a algebraických vlastností rovnic popisujících tyto útvary skrze souřadnice bodů. Jistě umíme každému bodu v rovině přiřadit dvě souřadnice. Pokud jsou dva body v nějakém vztahu, pravděpodobně budeme umět tento vztah popsat jako rovnici, kde jsou neznámými souřadnice zkoumaných bodů. Stejným způsobem můžeme popsat vztah mezi více body.

Ve chvíli, kdy umíme geometrické útvary a pojmy popsat pomocí polynomiálních rovnic, proč bychom nemohli zkoumat algebraické vlastnosti polynomů vycházejících z těchto rovnic? Dostali bychom tak způsob, jak můžeme zkoumat geometrické vlastnosti útvarů tak, že budeme zkoumat algebraické vlastnosti polynomů. To může být více algoritmické a automatizovatelné. Kdykoliv také přidáme polynomiální rovnici, která nezmění množinu řešení, a podíváme se na to, co tato rovnice vyjadřuje z hlediska vztahu mezi body, jejichž souřadnice rovnice obsahuje, lze z ní odvodit nějaké vlastnosti útvaru nebo závěry tvrzení, které chceme dokázat. Díky vlastnostem Groebnerovy báze, která je za určitých podmínek jednoznačná, můžeme snadno porovnávat ideály a tím pádem i jejich množiny nul.

První kapitola shrnuje základní teorii nezbytnou pro odvození metody automatického dokazování. Obsahuje pojmy týkající se algebraické geometrie od základních definic až po věty používané v druhé kapitole. Nezbytnou součástí jsou také pojmy potřebné k definici a výpočtu Groebnerovy báze, Buchbergerův algoritmus a nakonec krátká sekce shrnující používané značení při práci s geometrickými objekty.

Druhá kapitola se zabývá samotnou metodou automatického dokazování geometrických tvrzení, nejprve variantou metody popisovanou v [4] kapitola 6 §4 a krátce také variantou z [5] kapitola 22.5. Součástí druhé kapitoly je motivační příklad, na kterém jsou jednotlivé kroky metody popisovány a motivovány, včetně vlastního důkazu rozkladu konkrétní algebraické množiny.

Ve třetí kapitole se nachází vlastní řešené příklady, nejprve důkaz tvrzení o středových a obvodových úhlech a následně vyřešené příklady z [4] kapitola 6 §4, příklady 5, 6, 7, přičemž příklady 5 a 6 jsou řešeny oběma metodami.

1. Základní teorie

1.1 Algebraická geometrie

Metoda automatického dokazování geometrických tvrzení je založená na převedení dokazovaného problému na problém řešitelný v algebraické geometrii. Je proto potřeba zavést si základní pojmy, které budeme používat. Na úvod zavedeme značení, které budeme používat v celé této práci. Definice a tvrzení v této kapitole (až na vyjímky) odpovídají pojmům ve skriptech k předmětu Komutativní okruhy vyučovaném v akademickém roce 2019/2020 [6].

Značení 1.

- $K \ldots$ *komutativní těleso*
- $\mathbb{A}^n_K \ldots$ *afinní prostor dimenze n nad tělesem K*

Následující definice formálně zavádějí pojmy množina nul a ideál množiny. Množinu nul si lze představit jako množinu všech řešení soustavy polynomiálních rovnic (ptáme se, kdy se všechny polynomy nulují zároveň) a ideál množiny jako množinu polynomů, které se nulují na nějaké množině řešení.

Definice 1 (Množina nul)**.**
Buď $S \subseteq K[x_1, \ldots, x_n]$ *množina polynomů.* $\mathbf{V}(S) := \{A \in \mathbb{A}^n_K : \forall f \in S \; f(A) = 0\}$ *nazveme množinou nul množiny S.*

Definice 2 (Algebraická množina)**.**
Buď $X \subseteq \mathbb{A}^n_K$*. Řekneme, že X je algebraická množina, pokud* $X = \mathbf{V}(S)$*, pro nějaké* $S \subseteq K[x_1, \ldots, x_n]$*.*

Definice 3 (Ideál množiny)**.**
Buď $X \subseteq \mathbf{A}^n_K$*.* $\mathbf{I}(X) := \{f \in K[x_1, \ldots, x_n] : \forall A \in X \; f(A) = 0\}$ *nazveme ideálem množiny X.*

Pochopení těchto definic je stěžejní pro kroky, které budeme rozebírat v sekcích 2.2 až 2.4. Navíc budeme volně přecházet mezi soustavou polynomiálních rovnic a mezi polynomy, které vzniknou z této soustavy tak, že v každé rovnici všechny nenulové členy převedeme na jednu stranu rovnice a tu nenulovou stranu rovnice vezmeme jako náš polynom. Další definice nám pomůže porozumět tomu, co říká silná Hilbertova věta o nulách.

Definice 4 (Radikál)**.**
Buď I ideál v R komutativním okruhu. $Rad(I) := \{r \in R : \exists s \in \mathbb{N} \text{ tž. } r^s \in I\}$*. Pokud Rad(I)=I, řekneme, že I je radikálový ideál.*

Věta 1 (Silná Hilbertova věta o nulách)**.**
Buď I *ideál v* $K[x_1, \ldots, x_n]$*. K algebraicky uzavřené. Potom* $\mathbf{I}(\mathbf{V}(I)) = Rad(I)$

Silnou Hilbertovu větu o nulách využijeme v sekci 2.4 pro důkaz věty 11. Další Hilbertova věta (o bázi) vysvětluje, proč se vůbec můžeme v sekci 2.3 ptát na konečnou bázi (konkrétně Groebnerovu bázi). V obecném znění Hilbertova věta o bázi říká, že $R[x]$ je notherovský právě, když R je noetherovský. Pro připomenutí uvedeme definici noetherovského okruhu.

Definice 5 (Noetherovský okruh)**.**
Buď R komutativní okruh, řekneme, že je noetherovský pokud každý jeho ideál je konečně generovaný.

K těleso je triviálně noetherovský okruh, z toho plyne, že $K[x_1]$ je také noetherovský. Iterativně získáme následující důsledek.

Věta 2 (Důsledek Hilbertovy věty o bázi, [4] str. 76)**.**
Každý I ideál v $K[x_1, \ldots, x_n]$ je konečně generovaný.

Dále zde uvedeme také pomocná tvrzení, které budeme využívat v důkazu věty v sekci 2.2. Tvrzení se týkají rozkladu algebraické množiny na ireducibilní komponenty, které odpovídají prvoideálům.

Definice 6 (Ireducibilní algebraická množina)**.**
Buď $X \subseteq \mathbb{A}^n_K$ algebraická množina. Řekneme, že je ireducibilní pokud $\forall Y,Z \subseteq \mathbb{A}^n_K$ algebraické množiny tž. $X = Y \cup Z$ platí $X = Y$ nebo $X = Z$.

Věta 3 (Ireducibilní množiny a prvoideály)**.**
Neprázdná algebraická množina je ireducibilní právě, když $\mathbf{I}(V)$ je prvoideál.

Nyní, když umíme o algebraických množinách rozhodovat, jestli jsou ireducibilní nebo ne, podle toho, jestli jejich ideály jsou prvoideály nebo ne, hodilo by se umět rozhodnout i to jestli nějaký ideál je prvoideál jinak než z definice.

Tvrzení 4 (Charakterizace prvoideálu)**.**
Buď I vlastní ideál v R okruhu, potom I je prvoideál právě, když R/I je obor integrity.

1.2 Groebnerova báze

V této sekci definujeme Groebnerovu bázi a ukážeme si věty, které dokazují její existenci a zároveň, že Groebnerova báze je báze ideálu. Nejprve si zavedeme několik definic, které budeme potřebovat k samotné definici Groebnerovy báze. Jako první budeme definovat monomiální uspořádání, vůči kterému budeme chápat vedoucí členy polynomů. Monomiální uspořádání je alternativou uspořádání členů v polynomu podle mocniny proměnné pro polynomy více proměnných. V další definici formálně zavedeme, čemu budeme říkat vedoucí člen.

Všechny definice a věty v této sekci pochází z učebnice Ideals, varieties and algoritms [4]. V textu, ze kterého jsou tyto definice čerpány, není kladen důraz na to, že je potřeba pojmy z definice 9 vztahovat k nějakému fixnímu monomiálnímu uspořádání, tudíž pro lepší přehlednost přidáme do definice značení dolního indexu, které má vyjadřovat to monomiální uspořádání, vůči kterému jsou pojmy brány.

Značení 2.
Buď $K[x_1, \ldots, x_n]$ okruh polynomů nad tělesem v $n \in \mathbb{N}$ proměnných. Monočlen $x_1^{\alpha_1} \cdot \cdots \cdot x_n^{\alpha_n}$ budeme značit x^α, pro $\alpha = (\alpha_1, \ldots, \alpha_n)$.

Definice 7 (Monomiální uspořádání, [4] str. 55)**.**
Buď $>$ relace na M množině všech monočlenů z $K[x_1, \ldots, x_n]$ pro $n \in \mathbb{N}$. Řekneme, že $>$ je monomiální uspořádání, pokud splňuje následující:

- $>$ *je úplné (nebo také lineární) uspořádání na* M
- $\forall x^\alpha, x^\beta, x^\gamma \in M$, *tž.* $x^\alpha > x^\beta$ *platí* $x^{\alpha+\gamma} > x^{\beta+\gamma}$
- *každá neprázdná podmnožina* M *má nejmenší prvek*

Definice 8 (Lexikografické uspořádání, [4] str. 56)**.**
Lexikografické uspořádání definujeme jako relaci $>$ *na* M *množině všech monočlenů z* $K[x_1, \ldots, x_n]$, *pro kterou platí* $x^\alpha > x^\beta$, *pro* $\alpha = (\alpha_1, \ldots, \alpha_n)$, $\beta = (\beta_1, \ldots, \beta_n)$, *pokud vektorový rozdíl* $\alpha - \beta$ *nad* $\mathbb{Z}^n$ *má na první nenulové pozici kladnou hodnotu.*

Příklad.
Lexikografické uspořádání je monomiální uspořádání, jelikož splňuje všechny tři podmínky z definice 7:

- Je to úplné uspořádání z definice. Vektorový rozdíl nad $\mathbb{Z}^n$ existuje vždy a je určen jednoznačně. Pokud neexistuje nenulová pozice, tak je to právě když $\alpha = \beta$.
- $\alpha > \beta \Rightarrow \alpha - \beta$ má na první nenulové pozici kladnou hodnotu $\Rightarrow \alpha + \gamma - \beta - \gamma$ má na první nenulové pozici kladnou hodnotu $\Rightarrow \alpha + \gamma > \beta + \gamma$.
- Jelikož jde o lineární uspořádání, lze prvky seřadit do jednoho ostře klesajícího řetězce. Pokud je A konečná, potom máme vyhráno, jelikož vezmeme ten poslední. Pokud je A nekonečná, podíváme se na exponenty monočnů u proměnné x_1. Ty budou tvořit nerostoucí posloupnost, od nějakého členu konstantní. Nyní se podíváme na exponenty monočlenů patřících do této konstantní části u proměnné x_2. Ty budou tvořit také nerostoucí posloupnost, od nějakého členu konstantní. Kdybychom postupovali takto dál až k proměnné x_n dostaneme, že i zde po nějaké době budou konstantní exponenty a, jelikož všechny předchozí jsou také konstantní, dostáváme, že celý exponent jakožto n-tice exponentů u jednotlivých proměnných bude také konstantní. Navíc ale máme, že celá posloupnost je klesající a proto tam musí existovat nejmenší prvek.

Definice 9 (Vedoucí člen [4] str. 59)**.**
Buď $f = \sum_{\alpha \in A} a_\alpha x^\alpha$ *nenulový polynom z* $K[x_1, \ldots, x_n]$, M *množina všech monočlenů z* $K[x_1, \ldots, x_n]$ *pro* $n \in \mathbb{N}$ *a buď* $>$ *monomiální uspořádaní na* M. *Potom definujeme:*

- *Multistupeň* f *jako* $multideg(f) := argmax_>(x^\alpha)_{\alpha \in A, a_\alpha \neq 0}$
  neboli takové $0 \neq \alpha \in A$, *pro které platí* $x^\alpha = max_>(x^\alpha : \alpha \in A)$
- *Vedoucí koeficient* f *jako* $LC_>(f) := a_{multideg_>(f)}$
- *Vedoucí monom* f *jako* $LM_>(f) := x^{multideg_>(f)}$
- *Vedoucí člen* f *jako* $LT_>(f) := LC_>(f) \cdot LM_>(f)$
- *Množinu vedoucích členů ideálu* $I \subseteq K[x_1, \ldots, x_n]$ *jako* $LT_>(I) := \{LT_>(f) : f \in I\}$

Existenci Groebnerovy báze, jak si ji definujeme za chvíli, dokazuje následující věta.

Věta 5 (Ideál generovaný $LT_>(I)$, [4] str. 76)**.**
Buď I ideál v $K[x_1,\dots,x_n]$. Potom $\exists g_1,\dots,g_s \in I$, $s \in \mathbb{N}$ takové, že $\langle LT_>(g_1),\dots,LT_>(g_s)\rangle = \langle LT_>(I)\rangle$

Definice 10 (Groebnerova báze, [4] str. 77)**.**
Buď $>$ fixní monomiální uspořádání. Konečnou podmnožinu $G = \{g_1,\dots,g_s\}$ ideálu I nazveme Groebnerovou bází, pokud $\langle LT_>(g_1),\dots,LT_>(g_s)\rangle = \langle LT_>(I)\rangle$

Definice 11 (Redukovaná Groebnerova báze, [4] str. 92)**.**
Buď G Groebnerova báze ideálu I s monomiálním uspořádáním $>$, potom řekneme, že G je redukovaná Groebnerova báze, pokud:

- *$\forall f \in G$ platí $LC_>(f) = 1$*
- *$\forall f \in G$ žádný monočlen f neleží v $\langle LT(G \setminus \{f\})\rangle$*

Redukovaná Groebnerova báze je speciální případ Groebnerovy báze a podle věty 6 je určena jednoznačně pro fixní monomiální uspořádání.

Z věty 5 jsme dostali, že Groebnerova báze existuje pro každý ideál v $K[x_1,\dots,x_n]$. Věta 6 ukazuje navíc, že každá Groebnerova báze je báze I.

Věta 6 (spojení [4] str. 77 a [4], str. 92)**.**
Buď I ideál v $K[x_1,\dots,x_n]$. Potom pro každé monomiální uspořádání existuje jeho Groebnerova báze $G = \{g_1,\dots,g_s\}$ pro nějaké $s \in \mathbb{N}$. Platí také, že G je báze I, tedy $I = \langle g_1,\dots,g_s\rangle$. Navíc pro každé monomiální uspořádání existuje redukovaná Groebnerova báze a je určena jednoznačně.

Dále budeme k samotnému výpočtu Groebnerovy báze podle Buchbergerova algoritmu potřebovat definici S-polynomu a zbytku po dělení polynomů více proměnných. Přikládáme i větu, která dokazuje jeho existenci.

Definice 12 (S-polynom, [4] str. 83)**.**
Buďte $f,g \in K[x_1,\dots,x_n]$ nenulové polynomy. Buď $>$ fixní monomiální uspořádání. Označme $\alpha := multideg_>(f)$, $\beta := multideg_>(g)$ a $\gamma := (\gamma_1,\dots,\gamma_n)$, kde $\gamma_i := max(\alpha_i,\beta_i)$. S-polynom vzhledem k uspořádání $>$ pro polynomy f a g definujeme jako $S_>(f,g) := \frac{x^\gamma}{LT_>(f)} \cdot f - \frac{x^\gamma}{LT_>(g)} \cdot g$.

Věta 7 (Dělení se zbytkem polynomů více proměnných, [4] str. 64)**.**
Buď f, $f_1,\dots,f_s \in K[x_1,\dots,x_n]$ a $>$ fixní monomiální uspořádání. Potom existují $a_1,\dots,a_s,r \in K[x_1,\dots,x_n]$ tž. $f = a_1f_1 + \cdots + a_sf_s + r$, kde navíc $r = 0$ nebo žádný monočlen r není násobkem $LT_>(f_i)$ pro žádné i.

Definice 13 (Zbytek po dělení polynomů více proměnných, [4] str. 64)**.**
Buď f $f_1,\dots,f_s \in K[x_1,\dots,x_n]$. Označ $F = \{f_1,\dots,f_s\}$. Prvek r z výstupu následujícího algoritmu nazveme zbytkem polynomu f po dělení $f_1,\dots,f_s$. Budeme značit $\overline{f}^F$.

Zbytek po dělení lze vypočítat např. podle algoritmu z [4], str. 64. Bližší vysvětlení algoritmu a důkaz jeho správnosti lze nahlédnout v literatuře na str. 64 a dál.

Algoritmus dělení se zbytkem v okruhu polynomů více proměnných nad tělesem:
Vstup: $f,f_1,\dots,f_s \in K[x_1,\dots,x_n]$, $>$ fixní uspořádání
Výstup: $a_1,\dots,a_s$, r, kde $f = a_1f_1 + \cdots + a_sf_s + r$, r zbytek f po dělení $f_1,\dots,f_s$

0. $a_1, \ldots, a_s$, $r := 0$, $p := f$
1. **while** $p \neq 0$ **do**:
   a. $i := 1$
   b. $d := false$
   c. **while** $i \leq s$ **and** $d = false$ **do**:
      i. **if** $LT_>(f_i) | p$ **then**:
      $a_i += \frac{LT_>(p)}{LT_>(f_i)}$
      $p- = \frac{LT_>(p)}{LT_>(f_i)} \cdot f_i$
      $d = true$
      else:
      $i += 1$
   d. **if** $d = false$ **then**:
   $r += LT_>(p)$
   $p- = LT_>(p)$
2. **return** $a_i, \ldots, a_S$, r

1.3 Výpočet Groebnerovy báze

V celé sekci se budeme opírat o definice a tvrzení z předchozí sekce. Ukážeme si jak obecně nalézt Groebnerovu bázi, která podle věty 5 existuje pro každý nenulový ideál. Postupovat budeme podle Buchbergerova algoritmu.

Buchbergerův algoritmus: ([4] str. 90])
Vstup: F=$(f_1, \ldots, f_n)$ neprázdná uspořádaná generující množina ideálu I, $>$ fixní uspořádání
Výstup: Groebnerova báze G=$(g_1, \ldots, g_n)$ ideálu I, kde $F \subseteq G$

0. $G := F$
1. **repeat**:
   a. $G' := G$
   b. **for** $\{p,q\} \subseteq G^2$, $p \neq q$ **do**:
      i. $S := \overline{S(p,q)}^{G'}$
      ii. **if** $S \neq 0$ **then** $G := G \cup \{S\}$
   until $G = G'$
2. **return** G

Podívejme se blíže na to, co se vlastně uvnitř algoritmu děje: vezmeme si generující množinu, kterou jsme dostali jako vstup, a postupně do ní přidáváme další členy, které získáme následujícím způsobem. Ze stávající množiny vezmeme všechny dvojice p, q (vždy dva různé prvky) a podíváme se na to, jak vypadají $S := \overline{S(p,q)}^{G'}$ pro všechny tyto dvojice. Podle značení 13 to je zbytek po dělení

$S(p,q)$ polynomy $g_i \in G'$ (bráno postupně $g_1, \ldots, g_n \in G'$), kde $S(p,q)$ vypočteme z definice 11.

Pokud $S = 0$ pro nějakou dvojici, potom ho do generující množiny nepřidáváme, ale pokud $S \neq 0$, přidáme ho do generující množiny. Až přidáme taková S pro všechny dvojice, znovu se podíváme na každou dvojici v generující množině (která nyní obsahuje navíc nějaké prvky S) a zopakujeme předchozí postup, tedy výpočet $S := \overline{S(p,q)}^{G'}$ pro každou dvojici a přidání nenulových prvků. Pokud se v nějakém kroku stane, že $S = 0$ pro všechny dvojice, končíme a generující množinu (do které jsme postupně přidávali prvky S) prohlásíme za Groebnerovu bázi ideálu I.

Pro ukázku zde uvedeme jednoduchý příklad, na kterém si výpočet Groebnerovy báze ukážeme s konkrétními polynomy.

Příklad (viz [4] str. 89).

Mějme ideál $I = \langle x^3 - 2xy, x^2y - 2y^2 + x \rangle \subseteq K[x,y]$ s odstupňovaným lexikografickým uspořádáním $x > y$. Odstupňované lexikografické uspořádání nejprve porovná celkový stupeň monočlenů (součet všech exponentů) a pokud jsou tyto součty stejné, porovná je lexikogra fickým uspořádáním.

Označme $f_1 := x^3 - 2xy$, $f_2 := x^2y - 2y^2 + x$. $F = (f_1, f_2)$ není Groebnerova báze, protože $S(f_1,f_2) = -x^2 \in I$ a tedy $S(f_1,f_2) = -x^2 \in \langle LT(I) \rangle$. Na druhé straně ale máme $S(f_1,f_2) = -x^2 \notin \langle LT(f_1), LT(f_2) \rangle$. Celkem tedy dostáváme, že $\langle LT(f_1), LT(f_2) \rangle \subsetneq \langle LT(I) \rangle$.

K výpočtu Groebnerovy báze použijeme Buchbergerův algoritmus následujícím způsobem. Pomocí definice 12 vypočteme:

$$\begin{aligned} S(f_1,f_2) &= \frac{x^3y}{x^3} \cdot f_1 - \frac{x^3y}{x^2y} \cdot f_2 = y \cdot f_1 - x \cdot f_2 = \\ &= y \cdot (x^3 - 2xy) - x \cdot (x^2y - 2y^2 + x) = x^3y - 2xy^2 - x^3y + 2y^2x - x^2 = -x^2 \\ S &= \overline{S(f_1,f_2)}^F = \overline{(\overline{-x^2}^{x^3-2xy})}^{x^2y-2y^2+x} = -x^2 \end{aligned}$$

Přidáme tedy $-x^2$ do generující množiny a označíme $f_3 := -x^2$, dostaneme $G = F \cup \{f_3\}$. Nyní se znovu díváme na všechny dvojice.

$$\begin{aligned} S(f_1,f_2) &= f_3 \Rightarrow S = 0 \\ S(f_1,f_3) &= \frac{x^3}{x^3} \cdot f_1 - \frac{x^3}{-x^2} \cdot f_3 = f_1 - (-x) \cdot f_3 = \\ &= x^3 - 2xy - x^3 = -2xy \\ S &= \overline{S(f_1,f_3)}^G = \overline{-2xy}^G = \\ &= -2xy \\ S(f_2,f_3) &= \frac{x^2y}{x^2y} \cdot f_2 - \frac{x^2y}{-x^2} \cdot f_3 = f_2 - (-y) \cdot f_3 = \\ &= x^2y - 2y^2 + x - yx^2 = -2y^2 + x \\ S &= = \overline{S(f_2,f_3)}^G = \overline{-2y^2 + x}^G = \\ &= -2y^2 + x \end{aligned}$$

Přidáme $f_4 := -2xy$ a $f_5 := -2y^2 + x$ do generující množiny. Pokud bychom se nyní znovu dívali na všechny dvojice, zjistili bychom, že všechna S jsou rovna 0 a tím jsme hotovi. Groebnerovou bází ideálu I je tedy množina $(f_1,f_2,f_3,f_4,f_5) = (x^3 - 2xy,x^2y - 2y^2 + x, -x^2, -2xy, -2y^2 + x)$.

Příklad (výpočet redukované Groebnerovy báze, [4] str. 91,92).

Mějme množinu, kterou jsme v předchozím příkladu získali jako Groebnerovu bázi ideálu $I := \langle f_1,f_2\rangle$. Podívejme se, jestli jde o redukovanou Groebnerovu bázi a pokud ne, pokusme se ji upravit tak, aby byla. Nejprve si můžeme všimnout, že vedoucí koeficienty polynomů f_3, f_4, f_5 nejsou 1, vynásobíme tedy f_3 ,f_4, f_5 příslušnou konstantou, aby tomu tak bylo. Dostaneme:

$$G = \{x^3 - 2xy,x^2y - 2y^2 + x,x^2,xy,y^2 - \tfrac{1}{2}x\}$$

Dále si můžeme všimnout, že platí $LT_>(f_1) = x \cdot f_3$ a $LT_>(f_2) = x \cdot f_4$. Z toho plyne, že $LT_>(f_1,f_2,f_3,f_4,f_5) = \acute{L}T_>(f_3,f_4,f_5)$. f_1, f_2 můžeme odstranit z množiny a stále to bude Groebnerova báze I. Dostaneme tedy:

$$G = \{x^2,xy,y^2 - \tfrac{1}{2}x\}$$

Nyní vidíme, že vedoucí člen f_i neleží v $\langle LT_>(G \setminus f_i)\rangle$ pro žádné i. Jediný f_5 má také další monočleny, stačí tedy už jen ověřit, že $-\frac{1}{2}x$ neleží v $\langle LT_>(G \setminus f_5)\rangle = \langle x^2,xy\rangle$. Snadno lze nahlédnout, že neleží, a tím jsme hotovi. Redukovaná Groebnerova báze I je tedy $G = \{x^2,xy,y^2 - \frac{1}{2}x\}$.

Pro samotný výpočet Grobnerovy báze nebo redukované Groebnerovy báze lze využít různých technologií. Nejsložitější by nejspíše bylo vše si naprogramovat v libovolném jazyku bez využití knihoven. Existuje ale také několik nástrojů jako je Mathematica, SageMath, Singular a další, které v sobě na práci s polynomy a algebraickými pojmy již mají implementované metody. Většinu výpočtů zmiňovaných v této práci probíhaly v technologii SageMath, protože má jednoduchou syntaxi Pythonu. V Sage jsme využívali knihovny sage.rings.polynomial.toy_buchberger, která využívá technologie Singular.

1.4 Geometrie

V této sekci si zavedeme značení pro základní geometrické pojmy a vyslovíme větu, která nám umožní vyjádřit některé geometrické vztahy pomocí polynomiálních rovnic.

Značení 3.

- $A = (a_1, \ldots ,a_n)$... *bod v (afinním) prostoru dimenze* $n \in \mathbb{N}$
- $\overline{AB}$... *přímka procházející dvěma různými body A,B*
- $\angle ABC$ ... *úhel ABC s vrcholem v B, pro A,B,C body*
- $|AB|$... *vzdálenost mezi body A,B*

Věta 8 ([4] str. 294)**.**

Buďte A,B,C,D,E,F body v rovině. Všechny následující tvrzení lze vyjádřit jako soustavu polynomiálních rovnic o jedné nebo více rovnicích:

(i) $\overline{AB}$ *je rovnoběžná s* $\overline{CD}$

(ii) $\overline{AB}$ *je kolmá k* $\overline{CD}$

(iii) A,B,C *leží na jedné přímce*

(iv) Vzdálenost mezi A *a* B *je rovna vzdálenosti mezi* C *a* D *neboli* $|AB| = |CD|$

(v) C *leží na kružnici se středem v* A *a poloměrem* $|AB|$

(vi) C *leží ve středu úsečky* $\overline{AB}$

(vii) Ostrý úhel $\angle ABC$ *je roven ostrému úhlu* $\angle DEF$

(viii) $\overline{BD}$ *půlí úhel* $\angle ABC$

Následující tabulka přímo popisuje převod geometrického pojmu do polynomiálních rovnic v obecné variantě (bez konkrétní volby souřadnicového systému).

Tabulka 1.1: Vyjádření výrazů v rovnicích

$\overline{AB} \parallel \overline{CD}$	$(b_1 - a_1) \cdot (d_2 - c_2) - (b_2 - a_2) \cdot (d_1 - c_1) = 0$
$\overline{AB} \perp \overline{CD}$	$(b_1 - a_1) \cdot (d_1 - c_1) + (b_2 - a_2) \cdot (d_2 - c_2) = 0$
|AB|=|CD|	$(b_1 - a_1)^2 + (b_2 - a_2)^2 - (d_1 - c_1)^2 - (d_2 - c_2)^2 = 0$
$\angle ABC = \angle DEF$ (ostré úhly)	$((b_1 - a_1)(c_1 - b_1) + (b_2 - a_2)(c_2 - b_2))^2 \cdot$ $((e_1 - d_1)^2 + (e_2 - d_2)^2)((f_1 - e_1)^2 + (f_2 - e_2)^2) -$ $((b_1 - a_1)^2 + (b_2 - a_2)^2)((c_1 - b_1)^2 + (c_2 - b_2)^2) \cdot$ $((e_1 - d_1)(f_1 - e_1) + (e_2 - d_2)(f_2 - e_2))^2 = 0$

2. Postup řešení

2.1 Interpretace geometrického problému

V syntetické geometrii existují pojmy, které lze vyjádřit jednak slovy ale také polynomiálními rovnicemi. Vyjádření problému v rovnicích nám umožňuje uvažovat o problému z jiného pohledu a využívat u toho např. nástroje, které nabízí algebraická geometrie.

Vyjádření geometrického problému v rovnicích vyžaduje v první řadě zvolení souřadnicového systému. Souřadnicový systém nám zaručí jasně popsatelný vztah mezi geometrickými objekty, jako je např. vzdálenost mezi body nebo úhel mezi přímkami. Vztahy lze popsat rovnicemi, kde neznámými a parametry jsou souřadnice bodů.

Souřadnicový systém volíme zpravidla ortonormální s počátkem ve významném bodě geometrického útvaru, který studujeme. Osy pak volíme tak, aby alespoň jedna z nich procházela dalším významným bodem útvaru. Translace, rotace ani osová souměrnost nemění zkoumané vlastnosti, a proto je kterákoliv volba ortonormálního souřadnicového systému přípustná.

Geometrický problém se skládá z předpokladu (inicializace objektů a jejich vztahů) a ze závěru tvrzení (existence dalšího objektu, existence dalšího vztahu atp.). Obě tyto části je potřeba převést do řeči rovnic. Věta 8 v první kapitole ukazuje, že některé základní vztahy lze převést do řeči rovnic. Zavedeme jednotné značení:

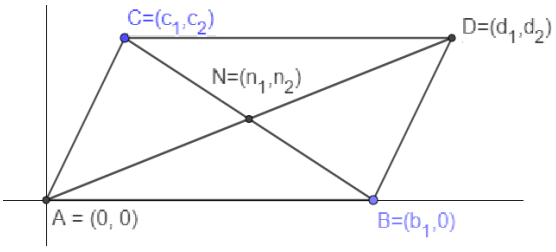
Značení 4.

- *Rovnice popisující předpoklady tvrzení budeme značit* h_i*, kde* $i \in \mathbb{N}$*.*
- *Rovnice popisující závěry tvrzení budeme značit* g_i*, kde* $i \in \mathbb{N}$

Tabulka 1.1 přímo popisuje jak vyjádřit některé geometrické pojmy jako rovnost. V příkladu níže si ukážeme jak převést konkrétní pojmy do vyjádření pomocí polynomiálních rovnic. Zároveň si ukážeme jak volit souřadný systém tak, abychom si soustavu rovnic co nejvíce zjednodušili.

Příklad (hlavní myšlenka viz [4] str. 291-300).

Mějme *předpoklad*: buď $ABDC$ netriviální rovnoběžník v rovině $\mathbb{R}^2$. Ekvivalentně bychom řekli: buďte A,B,C,D různé body v rovině $\mathbb{R}^2$ takové, že neleží na přímce a $\overline{AB} \parallel \overline{CD}$ a zároveň $\overline{AC} \parallel \overline{BD}$.



Obrázek 2.1: Rovnoběžník

V tabulce níže vidíme vlevo zápis (pro nezdegenerovaný případ) pro obecný Kartézský souřadnicový systém (bez konkrétní volby počátku a os), vpravo potom zápis pro souřadnicový systém takový, že počátek je v bodě A, tedy $A = (a_1,a_2) = (0,0)$, a že první osa prochází bodem B, tedy $B = (b_1,b_2) = (b_1,0)$. První osa má tedy směrový vektor $\overrightarrow{AB}$. Druhá osa je na ni kolmá a souřadnicový systém je tedy ortogonální.

$$\begin{array}{l|c} (b_1 - a_1) \cdot (d_2 - c_2) - (b_2 - a_2) \cdot (d_1 - c_1) = 0 & b_1 \cdot (d_2 - c_2) = 0 \\ (c_1 - a_1) \cdot (d_2 - b_2) - (c_2 - a_2) \cdot (d_1 - b_1) = 0 & c_1 \cdot d_2 - c_2 \cdot (d_1 - b_1) = 0 \end{array}$$

První rovnice je splněna pokud $b_1 = 0$, nebo pokud $d_2 - c_2 = 0$. Situace $b_1 = 0$ nastat nemůže, jelikož v předpokladech máme, že body mají být různé. Získáváme tedy $d_2 - c_2 = 0$. Dosazením do druhé rovnice $d_2 = c_2$ získáváme $c_2 \cdot (c_1 - d_1 + b_1) = 0$. Toto je splněno pokud $c_2 = 0$, nebo $c_1 - d_1 + b_1 = 0$. Podmínka $c_2 = 0$ nastat nemůže, jelikož z předpokladů víme, že $\overline{AB} \parallel \overline{CD}$ a body A,B,C,D neleží na jedné přímce. Získáváme tedy $c_1 - d_1 + b_1 = 0$.

Příklad (použití značení 3).

Získali jsme vyjádření *předpokladů* ve dvou polynomiálních rovnicích:

$$h_1 := d_2 - c_2 = 0$$
$$h_2 := d_1 - b_1 - c_1 = 0$$

Zpravidla nám vznikne soustava rovnic, kde počet proměnných převyšuje počet rovnic. Nabízí se tedy některé zvolit jako parametry a některé jako neznámé. Pro naše účely budeme rozlišovat proměnné na *libovolné* a *určené*. Pokus o formalizaci těchto pojmů by vyžadovalo prostor, který v této práci nemáme, a proto je jen stručně okomentujeme. Libovolné proměnné by mohly být ty, které lze volit jakkoliv, až na hodnoty, které by vedly na degenerované případy, v našem příkladě to je např. hodnota $b_1 = 0$. Určené proměnné by naopak mohly být ty, které jsou do značné míry určené těmi libovolnými, ve smyslu, že mohou nabývat maximálně konečně hodnot, ale typicky bychom chtěli, aby měly jednoznačně určenou hodnotu v závislosti na volbě libovolných proměnných.

Značení 5 (viz [4] první odstavec na str. 293)**.**

Libovolné proměnné budeme značit u_i pro vhodné $i \in \mathbb{N}$. Určené proměnné budeme značit x_i pro vhodné $i \in \mathbb{N}$

Příklad (použití značení 5).

Pro soustavu rovnic v příkladu výše jsou b_1,c_1,c_2 *libovolné* proměnné a d_1,d_2 *určené* proměnné.

V následujícím příkladě lze nahlédnout jak převést celé geometrické tvrzení do rovnic.

Příklad (hlavní myšlenka viz [4] str. 291-300).

Mějme rovnoběžník $ABDC$ v rovině s vrcholy A,B,C,D (4 různé a nekolineární body). Potom se jeho úhlopříčky půlí. *Předpoklady* tohoto tvrzení (jak jsme si ukázali v předchozím příkladě) lze vyjádřit v rovnicích jako následující (vlevo podle značení 3, vpravo podle značení 5):

$$\begin{array}{c|c} h_1 := d_2 - c_2 = 0 & h_1 := x_2 - u_3 = 0 \\ h_2 := d_1 - b_1 - c_1 = 0 & h_2 := x_1 - u_1 - u_2 = 0 \end{array}$$

Tímto jsme vyjádřili *předpoklady* a nyní vyjádříme *závěr*. Úhlopříčky se půlí, právě když pro průsečík, označme ho N, platí, že $|AN| = |ND|$ a zároveň $|BN| = |NC|$. Navíc k tomu, aby N byl průsečík úhlopříček, potřebujeme, že N leží na přímce $\overline{AD}$ a zároveň na přímce $\overline{BC}$. Je tedy potřeba přidat do *předpokladů* rovnice popisující kolinearitu trojic bodů. Podle věty 8 lze tento *předpoklad* převést na soustavu rovnic a se stejnou volbou souřadnicového systému jako výše dostáváme následující:

$$\begin{array}{c|c} (d_1 - a_1)(a_2 - n_2) - (d_2 - a_2)(a_1 - n_1) = 0 & d_1 \cdot n_2 - d_2 \cdot n_1 = 0 \\ (c_1 - b_1)(b_2 - n_2) - (c_2 - b_2)(b_1 - n_1) = 0 & n_2(c_1 - b_1) + c_2(b_1 - n_1) = 0 \end{array}$$

Podle značení 3 dostáváme:

$$\begin{aligned} h_3 &:= x_1x_4 - x_2x_3 \\ h_4 &:= x_4u_2 - x_4u_1 - u_3x_3 + u_3u_1 \end{aligned}$$

Závěr (rovnost vzdáleností) lze podle věty 8 vyjádřit jako soustavu polynomiálních rovnic. Podle tabulky za větou dostáváme:

$$\begin{aligned} g_1 &:= (n_1 - a_1)^2 + (n_2 - a_2)^2 - (d_1 - n_1)^2 - (d_2 - n_2)^2 = 0 \\ g_2 &:= (n_1 - b_1)^2 + (n_2 - b_2)^2 - (c_1 - n_1)^2 - (c_2 - n_2)^2 = 0 \end{aligned}$$

n_1,n_2 jsou *určené* proměnné, jelikož máme dvě různoběžné přímky (a tedy se protínají v právě jednom bodě), označíme je tedy x_3,x_4. Dále a_1,a_2,$b_2 = 0$ a b_1,c_1,c_2 jsme po řadě označili jako u_1,u_2,u_3. Po tomto přeznačení, roznásobení a zjednodušení dostaneme:

$$\begin{aligned} g_1 &:= -x_1^2 - x_2^2 + 2x_1x_3 + 2x_2x_4 = 0 \\ g_2 &:= u_1^2 - u_2^2 - u_3^2 - 2u_1x_3 + 2u_2x_3 + 2u_3x_4 = 0 \end{aligned}$$

Celkem dostáváme soustavu *předpokladů* h_1, h_2, h_3, h_4 a *závěry* g_1, g_2.

2.2 Rozklad množiny řešení

V předchozí sekci jsme si ukázali jak převést geometrický problém do soustavy polynomiálních rovnic. V této sekci se budeme zabývat tím, co znamená, že *závěry* plynou z *předpokladů* v řeči rovnic.

Máme soustavu k polynomiálních rovnic o n určených proměnných a m libovolných proměnných popisující *předpoklady* (použité značení viz Definice 3):

$$\begin{aligned} h_1(u_1, \ldots, u_m, x_1, \ldots, x_n) &= 0 \\ &\vdots \\ h_k(u_1, \ldots, u_m, x_1, \ldots, x_n) &= 0 \end{aligned}$$

Dále máme také soustavu r polynomiálních rovnic o n určených proměnných a m libovolných proměnných popisující *závěr*:

$$g_1(u_1,\ldots,u_m,x_1,\ldots,x_n) = 0$$
$$\vdots$$
$$g_r(u_1,\ldots,u_m,x_1,\ldots,x_n) = 0$$

Pro jednoduchost budeme předpokládat, že $r = 1$, neboť, pokud $r > 1$, lze brát tyto rovnice jednu po druhé. Rovnici, kterou se právě budeme chtít zabývat, budeme značit g. Chceme, aby z *předpokladů* plynul *závěr*, neboli aby rovnost popisující *závěr* plynula z rovností popisující *předpoklady*. Jinak řečeno, aby se polynom g nuloval pro všechny $m + n$-tice, které nulují všechny $h_1, \ldots, h_k$. Zde se dostáváme k důležitému kroku, přechodu od soustav rovnic k algebraické geometrii. Znamená to totiž, že, aby z *předpokladů* plynul *závěr*, musí platit $g \in \mathbf{I}(\mathbf{V}(h_1,\ldots,h_n))$. Zavedeme následující definici.

Definice 14 (viz[4] str. 297)**.**
Řekneme, že závěr g ***plyne čistě*** *z předpokladů $h_1,\ldots,h_n$, pokud pro $V = \mathbf{V}(h_1,\ldots,h_n)$ platí $g \in \mathbf{I}(V) \subset \mathbb{R}[u_1,\ldots,u_m,x_1,\ldots,x_n]$.*

V následujícím příkladě si ukážeme, že tato definice je ve skutečnosti příliš náročná a že vyžaduje platnost tvrzení i pro všechny degenerované případy, které však chceme vyloučit.

Příklad (pokračování předchozího příkladu).
Mějme stejné tvrzení jako v příkladech v sekci 2.1. Máme již připravené polynomy, na které bychom chtěli aplikovat definici 14.

$$h_1 = x_2 - u_3$$
$$h_2 = x_1 - u_1 - u_2$$
$$h_3 = x_1x_4 - x_2x_3$$
$$h_4 = x_4u_2 - x_4u_1 - u_3x_3 + u_3u_1$$

Nyní nás bude zajímat výsledek výpočtu Groebnerovy báze ideálu generovaného h_1, h_2, h_3, h_4, $1 - yg$. V kapitole 2.4 si ukážeme větu, která říká, že *závěr g plyne čistě* z *předpokladů* právě, když Groebnerova báze tohoto ideálu je $\{1\}$. Pro náš příklad tomu tak bohužel není a je tedy na místě se zamyslet, kde děláme chybu. Groebnerova báze ideálu $\langle h_1,h_2,h_3,h_4\rangle$ vzhledem k lexikografickému uspořádání vyjde:

$$f_1 = u_1 + u_2 - x_1$$
$$f_2 = u_2x_2 - 2u_2x_4 - x_1x_2 + 2x_2x_3$$
$$f_3 = u_3 - x_2$$
$$f_4 = x_1x_4 - x_2x_3$$

Podívejme se na rozklad množiny $V := \mathbf{V}(h_1,h_2,h_3,h_4)$, podle technologie Sage vychází $V = W_1 \cup W_2 \cup W_3$, kde:

$$W_1 = \mathbf{V}(u_3,x_4,u_3 - x_2,u_2 - u_1 - x_1)$$
$$W_2 = \mathbf{V}(2x_4 - x_2,2x_3 - u_1 - x_1,u_3 - x_2,u_2 - u_1 - x_1)$$
$$W_3 = \mathbf{V}(x_3x_2 - x_4x_1, u_1,u_3 - x_2,u_2 - u_1 - x_1)$$

Podíváme-li se na W_1 a W_3, zjistíme, že řešení v nich obsažená nechceme do našich předpokladů počítat, jelikož jsme chtěli, aby $u_1,\ u_3$ byly nenulové a zde je povolujeme rovné 0. Dále nás zajímá pouze W_2. Tím, že z rozkladu odebereme W_1 a W_3, nepovolíme případ, kdy $u_1,\ u_3 = 0$, tedy případ, kdy $A = B$ a případ, kdy jsou body kolineární.

V následující sekci se přesvědčíme o tom, že odebrání W_1, W_3 stačí k úspěšnému dokončení důkazu. Pokud bychom pro platnost dokazovaného tvrzení vyžadovali, aby g splňoval definici 14, vyžadovali bychom platnost tvrzení i v degenerovaných případech, které jsme právě odebrali. Často tvrzení v degenerovaných případech platit nebude a proto budeme na konci kapitoly zavádět definici 16.

Nyní okážeme, že rozklad množiny V, který jsme dostali ze Sage je opravdu rozkladem V v okruhu polynomů nad $\mathbb{R}$.

Věta 9.
Označ W_1, W_2, W_3 jako výše. Potom $V = W_1 \cup W_2 \cup W_3$.

Než si větu 9 dokážeme, vyslovíme a dokážeme lemma, které budeme v důkazu potřebovat.

Lemma 10.
Buď K komutativní těleso, I ideál v $K[x_1,\dots,x_n]$, $n \in \mathbb{N}$. Pokud I obsahuje polynom $g = x_1 - f(x_2,\dots,x_n)$, pro nějaký polynom $f \in K[x_2,\dots,x_n]$, potom platí $K[x_1,\dots,x_n]/I \cong K[x_2,\dots,x_n]/\phi(I)$, kde ϕ je dosazovací homomorfismus $\phi : K[x_1,\dots,x_n] \to K[x_2,\dots,x_n]$ tž. $g(x_1,\dots,x_n) \mapsto g(f,x_2,\dots,x_n)$.

Důkaz. [lemma 10
$\underline{Im(\phi) = K[x_2,\dots,x_n]}$: $\subseteq$ z definice zobrazení ϕ. $\supseteq$ z toho, že pro každý polynom $h \in K[x_2,\dots,x_n]$ platí $h = \phi(h)$. Celkem je tedy ϕ na $K[x_2,\dots,x_n]$.
$\underline{Ker(\phi) = \langle x_1 - f\rangle}$: $\phi(h(x_1,\dots,x_n)) = 0 \iff h(f,x_2,\dots,x_n) = 0 \iff h(x_1,\dots,x_n) = 0$ nebo $h(x_1,\dots,x_n) = \tilde{h}\cdot x_1 - \tilde{h}\cdot f = \tilde{h}\cdot(x_1 - f)$ pro nějaké $0 \neq \tilde{h} \in K[x_1,\dots,x_n] \iff h \in \langle x_1 - f\rangle$.
Dále uvažme projekci $\Pi : K[x_2,\dots,x_n] \to K[x_2,\dots,x_n]/\phi(I)$ tž. $g \mapsto [g]_{\phi(I)}$ (rozkladová třída). Složení homomorfismů $\Pi \circ \phi$ je homomorfismus s jádrem I a obrazem $K[x_2,\dots,x_n]/\phi(I)$ jelikož ϕ i Π jsou na. Nyní použijeme první větu o isomorfismu na zobrazení $\Pi\circ\phi : K[x_1,\dots,x_n] \to K[x_2,\dots,x_n]/\phi(I)$ a dostaneme, že $K[x_1,\dots,x_n]/I \cong K[x_2,\dots,x_n]/\phi(I)$.

□

Důkaz. [věta 9]
Označ:
$I_1 := \langle u_3,x_4,u_3 - x_2,u_2 - u_1 - x_1\rangle$
$I_2 := \langle 2x_4 - x_2,2x_3 - u_1 - x_1,u_3 - x_2,u_2 - u_1 - x_1\rangle$
$I_3 := \langle x_3x_2 - x_4x_1, u_1,u_3 - x_2,u_2 - u_1 - x_1\rangle$
$I = \langle x_2 - u_3,x_1 - u_1 - u_2,x_1x_4 - x_2x_3,x_4u_2 - x_4u_1 - u_3x_3 + u_3u_1\rangle$
ideály v okruhu polynomů s racionálními koeficienty

a dále označ:
$J_1 := \langle u_3,x_4,u_3 - x_2,u_2 - u_1 - x_1\rangle$
$J_2 := \langle 2x_4 - x_2,2x_3 - u_1 - x_1,u_3 - x_2,u_2 - u_1 - x_1\rangle$

$J_3 := \langle x_3x_2 - x_4x_1, u_1,u_3 - x_2,u_2 - u_1 - x_1\rangle$
$J = \langle x_2 - u_3,x_1 - u_1 - u_2,x_1x_4 - x_2x_3,x_4u_2 - x_4u_1 - u_3x_3 + u_3u_1\rangle$
ideály v okruhu polynomů s reálnými koeficienty

Budeme postupovat podle následující struktury:

1. $I_1 \cap I_2 \cap I_3 = Rad(I) \Rightarrow V = W_1 \cup W_2 \cup W_3$
2. $I_1 \cap I_2 \cap I_3 = Rad(I)$
3. J_1, J_2, J_3 jsou prvoideály

1. Nejprve ukážeme, že W_1, W_2, W_3 tvoří rozklad V, pokud $I_1 \cap I_2 \cap I_3 = Rad(I)$.

Podle věty z komutativní algebry platí pro I ideál v R komutativním okruhu, že $Rad(I) = \bigcap_{I \subseteq P \ prvoideál \ R} P$. To znamená, že každý prvoideál obsahující I v sobě obsahuje $Rad(I)$. Dále také víme, že $I_1 \cdot I_2 \cdot I_3 \subseteq I_1 \cap I_2 \cap I_3$. Z toho, že $I_1 \cap I_2 \cap I_3 = Rad(I)$, víme, že každý prvoideál obsahující I v sobě obsahuje také $I_1 \cdot I_2 \cdot I_3$ a musí z definice obsahovat také I_1 nebo I_2 nebo I_3, jelikož je to prvoideál.

Mějme prvek $a \in V$. Nechť není obsažen v W_1, W_2,W_3. Je to jednoprvková množina, je tedy ireducibilní a $\mathbf{I}(\{a\})$ je prvoideál. Z toho, že $\{a\} \subset V$, dostaneme, že $\mathbf{I}(\{a\}) \supset \mathbf{I}(V)$. Je to tedy prvoideál obsahující I a podle předchozího obsahuje i I_1, I_2 nebo I_3. Celkem dostáváme, že $a \in W_1$, W_2 nebo W_3.

2. Nyní ukážeme, že $J_1 \cap J_2 \cap J_3 = Rad(J)$. Podle technologie Sage je nad racionálními čísly redukovaná Groebnerova báze průniku $I_1 \cap I_2 \cap I_3$ následující:

$$G_{I_1 \cap I_2 \cap I_3} = \{u_1 + u_2 - x_1, u_2x_2 - 2u_2x_4 - x_1x_2 + 2x_2x_3, u_3 - x_2, x_1x_4 - x_2x_3\}$$

Stejnou redukovanou Groebnerovu bázi nám dá Sage i pro $Rad(I)$. Obě báze musí generovat stejnou množinu a z toho plyne, že $I_1 \cap I_2 \cap I_3 = Rad(I)$ v okruhu polynomů s racionálními koeficienty.

Buchbergerův algoritmus bude pracovat stejně nad $\mathbb{R}[u_1,u_2,u_3,x_1,x_2,x_3,x_4]$ jako nad $\mathbb{Q}[u_1,u_2,u_3,x_1,x_2,x_3,x_4]$. Z toho dostaneme, že pro Groebnerovu bázi průniku $J_1 \cap J_2 \cap J_3$ platí $G_{J_1 \cap J_2 \cap J_3} = G_{I_1 \cap I_2 \cap I_3}$. Z toho, že máme $G_{J_1 \cap J_2 \cap J_3} = G_{I_1 \cap I_2 \cap I_3} \subseteq Rad(I)$, dostaneme, že $G_{J_1 \cap J_2 \cap J_3} \subseteq Rad(J)$ a tedy i $J_1 \cap J_2 \cap J_3 \subseteq Rad(J)$.

V kroku 3 tohoto důkazu ukážeme, že J_1, J_2, J_3 jsou prvoideály a my navíc víme, že $I \subseteq I_1 \cap I_2 \cap I_3$, obsahuje tedy generující množinu I, z toho plyne, že $J_1 \cap J_2 \cap J_3$ obsahuje generující množinu J a tedy i celý ideál J. Z toho podle již zmiňované věty z komutativní algebry plyne, že $Rad(J) \subseteq J_1 \cap J_2 \cap J_3$. Dohromady dostáváme obě inkluse a tedy rovnost.

3. Nakonec ukážeme, že J_1, J_2, J_3 jsou prvoideály v $\mathbb{R}[u_1,u_2,u_3,x_1,x_2,x_3,x_4]$. K tomu nám podle věty 4 bude stačit dokázat, že $\mathbb{R}[u_1,u_2,u_3,x_1,x_2,x_3,x_4]/J_i$, $i = 1, +2, 3$ jsou obory integrity. Bude k tomu využívat lemma 10:

$\mathbb{R}[\mathbf{u_1},\mathbf{u_2},\mathbf{u_3},\mathbf{x_1},\mathbf{x_2},\mathbf{x_3},\mathbf{x_4}]/\mathbf{J_1}$ **je obor integrity**:
$\mathbb{R}[u_1,u_2,u_3,x_1,x_2,x_3,x_4]/(u_3,x_4,u_3 - x_2,u_2 - u_1 - x_1) \cong$
$\cong \mathbb{R}[u_1,u_3,x_1,x_2,x_3]/(u_3,u_3 - x_2) \cong \mathbb{R}[u_1,u_3,x_1,x_3]/(u_3) \cong$
$\cong \mathbb{R}[u_1,x_1,x_3]$ a to je obor integrity

$\mathbb{R}[\mathbf{u_1},\mathbf{u_2},\mathbf{u_3},\mathbf{x_1},\mathbf{x_2},\mathbf{x_3},\mathbf{x_4}]/\mathbf{J_2}$ **je obor integrity**:
$\mathbb{R}[u_1,u_2,u_3,x_1,x_2,x_3,x_4]/(2x_4 - x_2, 2x_3 - u_1 - x_1, u_3 - x_2, u_2 - u_1 - x_1) \cong$
$\cong \mathbb{R}[u_1,x_1,x_2,x_3,x_4]/(2x_4 - x_2, 2x_3 - u_1 - x_1) \cong \mathbb{R}[u_1,x_3,x_4]$ a to je obor integrity.

$\mathbb{R}[\mathbf{u_1},\mathbf{u_2},\mathbf{u_3},\mathbf{x_1},\mathbf{x_2},\mathbf{x_3},\mathbf{x_4}]/\mathbf{J_3}$ **je obor integrity**:
$\mathbb{R}[u_1,u_2,u_3,x_1,x_2,x_3,x_4]/(x_2x_3 - x_4x_1, u_1, u_3 - x_2, u_2 - u_1 - x_1) \cong$
$\cong \mathbb{R}[u_1,x_2,x_1,x_2,x_3,x_4]/(x_2x_3 - x_4x_1, u_1) \cong \mathbb{R}[x_1,x_2,x_3,x_4]/(x_2x_3 - x_4x_1)$, polynom $x_2x_3 - x_4x_1$ je ireducibilní a proto je ideál jím generovaný prvoideál a nám podle věty 4 vyšel obor integrity.

□

Poznámka. Pokud bychom pracovali nad algebraicky uzavřeným tělesem a uměli bychom nad ním efektivně počítat Groebnerovy báze, dalo by se dokázat silnější tvrzení, že jde skutečně o ireducibilní rozklad.

V příkladu výše, jsme odebrali komponenty, které povolovaly degenerované případy. Tyto degenerované případy jsme chtěli vyloučit. V literatuře [4] v kapitole 6 §4 si autoři definují algebraickou nezávislost následovně:

Definice 15 (viz[4] str. 299)**.**
Buď $K[u_1,\ldots,u_n,x_1,\ldots,x_m]$ okruh polynomů nad tělesem a $V \subseteq \mathbf{A}_K^{n+m}$ ireducibilní algebraická množina. Řekneme, že $u_1,\ldots,u_n$ jsou ***algebraicky nezávislé*** *na V, pokud žádný nenulový polynom z $K[u_1,\ldots,u_n]$ se nenuluje na V.*

Ekvivalentně bychom mohli říct, že $u_1,\ldots,u_n$ jsou **algebraicky nezávislé** na V, pokud $\mathbf{I}(V) \cap K[u_1,\ldots,u_n] = \{0\}$

Z předchozího příkladu plyne, že k tomu, abychom ukázali splnitelnost rovnice $g = 0$, je potřeba se dívat pouze na ty množiny, na kterých jsou u_i $\forall i$ algebraicky nezávislé. Dále v literatuře [4] v kapitole 6 §4 je uvedena následující definici, kterou autoři prohlašují za dostatečnou k tomu, abychom geometrické tvrzení dokázali.

Definice 16 (viz [4] str. 300)**.**
Řekneme, že závěr g ***plyne*** *z předpokladů $h_1,\ldots,h_n$, pokud pro $V' = W_1 \cup \cdots \cup W_p \subseteq \mathbf{V}(h_1,\ldots,h_n)$, kde $u_1,\ldots,u_n$ jsou algebraicky nezávislé na $W_1,\ldots,W_p$, platí $g \in \mathbf{I}(V') \subset K[u_1,\ldots,u_m,x_1,\ldots,x_n]$.*

Podívejme se znovu na náš příklad. Vylučujeme komponenty, které by povolovali degenerované případy, které chceme zakázat. Chceme ale zakázat všechny degenerované případy? Vadilo by např., kdyby nějaká komponenta povolovala, aby zkoumaný rovnoběžník byl čtverec? V takovém případě by platilo $u_1 - u_3 = 0$ a $u_2 = 0$. V obecném případě nejsme schopni zde dokázat, že každou komponentu obsahující nenulový polynom z $K[u_1,\ldots,u_n]$ je potřeba vyloučit a dále pokračovat bez ní. Můžeme však sledovat myšlenku autorů [4] a hledat komponenty, které by obsahovaly nevyžádané degenerované případy.

2.3 Vyhodnocení

Nyní tedy už víme, že je nejprve potřeba převést geometrický problém do rovnic. Z těchto rovnic si vytáhneme polynomy, které nás zajímají, a najdeme

ireducibilní rozklad algebraické množiny jimi určené. Z těchto ireducibilních komponent vybereme ty, na kterých jsou $u_i \forall i$ algebraicky nezávislé. Jako další krok by následoval výpočet Groebnerovy báze jakéhosi ideálu $\langle h'_1,\ldots,h'_{n'},1-gy\rangle \subseteq K[u_1,\ldots,u_n,x_1,\ldots,x_m,y]$, kde $V' = \langle h'_1,\ldots,h'_{n'}\rangle$ je sjednocení těch 'správných' komponent V. V této sekci se podíváme na to, proč nás zajímá právě tento ideál a jak z toho plyne splnitelnost rovnice $g = 0$.

Spojením následujících dvou vět dostaneme, že pokud $\{1\}$ je Groebnerova báze ideálu $\langle h_1,\ldots,h_n,1-g\cdot y\rangle$, potom g plyne čistě z $h_1,\ldots,h_n$.

Věta 11 (viz [4] str. 297)**.**
Pokud $g \in Rad(\langle h_1,\ldots,h_n\rangle)$, potom g plyne čistě z předpokladů $h_1,\ldots,h_n$.

Věta 12 (viz[4] str. 178)**.**
Buď K těleso a $I = \langle h_1,\ldots,h_n\rangle \subset K[x_1,\ldots,x_n]$ ideál. Potom $g \in Rad(I)$ právě když $1 \in \langle h_1,\ldots,h_n,1-g\cdot y\rangle \subset K[x_1,\ldots,x_n,y]$.
(tedy $\langle h_1,\ldots,h_n,1-g\cdot y\rangle = K[x_1,\ldots,x_n,y]$)

Nyní se pokusíme aplikovat tyto věty na příklad geometrického problému čtyřúhelníku a tím dokončit důkaz platnosti tvrzení rozebíraného v sekcích 2.1 a 2.2.

Příklad.
Pomocí technologie Sage lze rozložit algebraickou množinu $\mathbf{V}(\langle h_1,h_2,h_3,h_4\rangle)$ na komponenty:

$$W_1 = \mathbf{V}(u_3,x_4,u_3-x_2,u_2-u_1-x_1)$$
$$W_2 = \mathbf{V}(2x_4-x_2,2x_3-u_1-x_1,u_3-x_2,u_2-u_1-x_1)$$
$$W_3 = \mathbf{V}(x_3x_2-x_4x_1,u_1,u_3-x_2,u_2-u_1-x_1)$$

Dále označme

$$h'_1 := 2x_4-x_2 \qquad h'_3 := u_3-x_2$$
$$h'_2 := 2x_3-u_1-x_1 \quad h'_4 := u_2-u_1-x_1$$

Podle definice 15 jsou u_1, u_3 algebraicky závislé na W_1, W_2, a proto budeme dále pracovat pouze s W_2. Pomocí technologie Sage lze spočíst Groebnerovu bázi ideálu $\langle h'_1,h'_2,h'_3,h'_4,g_1y-1\rangle$ a ideálu $\langle h'_1,h'_2,h'_3,h'_4,g_2y-1\rangle$. Pro oba ideály tato báze vychází $\{1\}$. Podle věty 12 dostáváme, že $g_1,g_2 \in Rad(h'_1,h'_2,h'_3,h'_4)$. Nyní použijeme větu 11 a dostaneme, že g_1,g_2 plynou čistě z h'_1,h'_2,h'_3,h'_4. To z definice nastane, právě když g_1,g_2 plynou z h_1,h_2,h_3,h_4 Tímto jsme dokázali původní tvrzení, že v každém (netriviálním) rovnoběžníku v rovině se jeho úhlopříčky půlí.

2.4 Alternativní metoda

V příkladě v sekci 2.1 jsme pro vyloučení některých možností použili předpoklady, které by se daly vyjádřit jako nerovnosti. V našem případě to bylo $b_2 \neq 0$ a $c_2 \neq 0$. Navíc jsme museli rozložit $\mathbf{V}(h_1,h_2,h_3,h_4)$ a vybrat pouze tu, která tyto speciální případy nepovoluje. Zde si ukážeme, že se tomu dá vyhnout, pokud bychom uměli do naší metody zahrnout i nerovnosti pro případ, že rozklad algebraické množiny nebude tak snadné použít jako v našem příkladě.

Metoda automatického dokazování pracuje pouze s rovnostmi a je tedy potřeba umět nerovnosti vyjádřit jako rovnosti. Hlavní myšlenka této metody pochází z učebnice Počítačové algebry [5], kde autor nabízí postup, podle kterého přidáme polynom $f \cdot x_{n+1} - 1$ pro vyjádření $f \neq 0$. Podívejme se na odvození tohoto postupu.

Mějme *předpoklady* $h_1, \ldots, h_m$ vycházející z rovností $h_i = 0$, dále mějme *předpoklad* ve tvaru $h_{m+1} \neq 0$. Hledáme tedy množinu řešení ve tvaru $\mathbf{V}(h_1, \ldots, h_m) \cap \mathbf{V}(h_{m+1})^c$ (^{c} značí množinový doplněk). Všimněme si, že tato množina je rovna $\mathbf{V}(I \cup \{h_{m+1} \cdot x_{n+1} - 1\}) \subseteq \mathbb{A}^n_K$. Pokud pro nějaký bod $A = (a_1, \ldots, a_n) \in \mathbb{A}^n_K$ platí $A \in \mathbf{V}(h_1, \ldots, h_m)$ a zároveň $f(A) \neq 0$, potom to je, právě když existuje $A' = (a_1, \ldots, a_n, a_{n+1}) \in \mathbb{A}^{n+1}_K$ takový, že $f(A') \cdot a_{n+1} - 1 = 0$, to je, právě když $A' \in \mathbf{V}(I \cup \{h_{m+1} \cdot x_{n+1} - 1\})$. Celkem tedy pokud chceme přidat nerovnici $h_{m+1} \neq 0$, je potřeba přidat polynom $h_{m+1} \cdot x_{n+1} - 1$. Podobným způsobem lze odvodit polynom pro nerovnici $h_{m+1} \geq 0$, výsledný polynom bude $h_{m+1} - x^2_{n+1} = 0$ (Pokud pracujeme nad $\mathbb{R}$).

Podíváme-li se na větu 12, zjistíme, že tato věta dokazuje sporem, že $g \in Rad(I)$, jelikož, pokud bychom si polynom $1 - gy$ převedli podle výše zmíněné metody zpět na nerovnost, ptáme se na množinu řešení, která splňuje rovnice popisující předpoklady a zároveň nesplňuje rovnici popisující závěr tvrzení. Pokud by taková množina řešení, ale byla prázdná, například pokud $\mathbf{I}(V)$ byl celý prostor $K[u_1, \ldots, u_n, x_1, \ldots, x_m]$, víme, že taková situace nastat nemůže, a proto rovnice popisující závěr tvrzení musí platit.

Příklad (Alternativní výpočet příkladu z 2.1).

Předpoklady h_1,h_2,h_3,h_4 si necháme a podíváme se na předpoklady o netrivialitě a nekolinearitě bodů A,B,C,D Chceme tedy, aby všechny 4 body byly po dvou různé a neležely na jedné přímce. K tomu nám bude stačit, že alespoň jeden z bodů C,D (BÚNO budeme uvažovat C) neleží na přímce $\overline{AB}$, jelikož k tomu máme podmínku na rovnoběžnost $\overline{AB} \parallel \overline{CD}$. Nerovnost, kterou chceme vyjádřit jako rovnici, je tedy:

$$0 \neq (b_1 - a_1) \cdot (a_2 - c_2) - (b_2 - a_2)(a_1 - c_1).$$

Po dosazení hodnot vycházejících z volby souřadnicového systému dostaneme $0 \neq b_1 \cdot c_2$. Převedením na rovnici podle výše popsaného postupu dostaneme $0 = b_1 \cdot c_2 \cdot w - 1$. Celkově jsme dostali následující (*závěry* tvrzení zůstávají také stejné):

$$\begin{aligned} h_1 &= x_2 - u_3 \\ h_2 &= x_1 - u_1 - u_2 \\ h_3 &:= x_1 x_4 - x_2 x_3 \\ h_4 &:= x_4 u_2 - x_4 u_1 - u_3 x_3 + u_3 u_1 \\ h_5 &:= u_1 u_3 w - 1 \end{aligned}$$

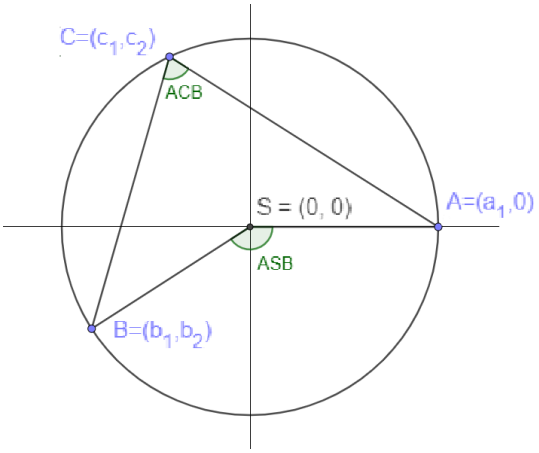
$$\begin{aligned} g_1 &:= -x_1^2 - x_2^2 + 2x_1 x_3 + 2x_2 x_4 \\ g_2 &:= u_1^2 - u_2^2 - u_3^2 - 2u_1 x_3 + 2u_2 x_3 + 2u_3 x_4 \end{aligned}$$

Pomocí technologie Sage vypočteme redukovanou Grobnerovu bázi ideálu $\langle h_1,h_2,h_3,h_4,h_5,g_1 y - 1\rangle$ a ideálu $\langle h_1,h_2,h_3,h_4,h_5,g_2 y - 1\rangle$, pro oba vychází rovna $\{1\}$ a podle věty 11 a 12 dostaneme, že *závěry* g_1,g_2 plynou čistě z *předpokladů* h_1,h_2,h_3,h_4,h_5.

3. Řešené úlohy

3.1 Středový a obvodový úhel

Věta 13.
Buďte A, B, C různé body v $\mathbb{R}^2$ ležící na kružnici k se středem S, potom čtverec cosinu velikosti úhlu $\angle ACB$ je čtverec cosinu poloviny velikosti úhlu $\angle ASB$.



Obrázek 3.1: Středový a obvodový úhel

Důkaz.
V důkazu budeme používat značení 3.
Volme ortonormální souřadnicový systém s počátkem v S a osou x se směrovým vektorem AS, tedy $S = (s_1,s_2) = (0,0)$ a $A = (a_1,0)$. Dále z toho, že body A, B, C leží na kružnici k se středem v S a poloměrem BÚNO $r = 1$, celkem dostaneme:

$$\begin{aligned} h_1 &:= a_1 - 1 \\ h_2 &:= b_1^2 + b_2^2 - 1 \\ h_3 &:= c_1^2 + c_2^2 - 1 \end{aligned}$$

Z toho, že A, B, C jsou různé, dostaneme:

$$h_4 := ((a_1 - b_1)^2 + (a_2 - b_2)^2)((a_1 - c_1)^2 + (a_2 - c_2)^2)((b_1 - c_1)^2 + (b_2 - c_2)^2)w - 1$$

Tvrzení, že čtverec cosinu velikosti úhlu $\angle ACB$ rovná se čtverci cosinu poloviny velikosti úhlu $\angle ASB$ zapíšeme v rovnici takto:

$$\begin{gathered} cos^2(2 \cdot \angle ACB) = cos^2(\angle ASB) \\ (cos^2(\angle ACB) - sin^2(\angle ACB))^2 = \frac{\langle \vec{SA},\vec{SB}\rangle^2}{(|SA| \cdot |SB|)^2} \\ (2cos^2(\angle ACB) - 1)^2 = \frac{\langle \vec{SA},\vec{SB}\rangle^2}{(|SA| \cdot |SB|)^2} \\ (2 \cdot \frac{\langle \vec{CA},\vec{CB}\rangle^2}{(|CA| \cdot |CB|)^2} - 1)^2 = \frac{\langle \vec{SA},\vec{SB}\rangle^2}{(|SA| \cdot |SB|)^2} \\ \frac{(2 \cdot \langle \vec{CA},\vec{CB}\rangle^2 - (|CA| \cdot |CB|)^2)^2}{(|CA| \cdot |CB|)^4} = \frac{\langle \vec{SA},\vec{SB}\rangle^2}{(|SA| \cdot |SB|)^2} \\ (2 \cdot \langle \vec{CA},\vec{CB}\rangle^2 - (|CA| \cdot |CB|)^2)^2 \cdot (|SA| \cdot |SB|)^2 - \langle \vec{SA},\vec{SB}\rangle \cdot (|CA| \cdot |CB|)^4 = 0 \end{gathered}$$

Polynom popisující *závěr* tvrzení tedy bude:

$$g := (2((c_1 - a_1)(b_1 - c_1) + (c_2 - a_2)(b_2 - c_2))^2 - ((c_1 - a_1)^2 + (c_2 - a_2)^2)((b_1 - c_1)^2 + (b_2 - c_2)^2))^2 \cdot ((s_1 - a_1)^2 + (s_2 - a_2)^2)((c_1 - s_1)^2 + (c_2 - s_2)^2) - ((s_1 - a_1)(b_1 - s_1) + (s_2 - a_2)(b_2 - s_2))^2 \cdot (((c_1 - a_1)^2 + (c_2 - a_2)^2)((b_1 - c_1)^2 + (b_2 - c_2)^2))^2$$

Po dosazení hodnot s_1, s_2, $a_1 = 0$ (kvůli volbě souřadnicového systému) dostáváme:

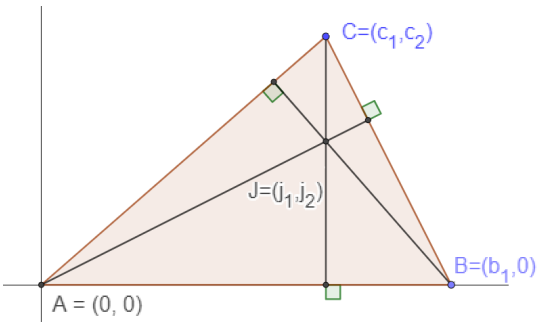
$$\begin{gathered} h_1 := a_1 - 1 \\ h_2 := b_1^2 + b_2^2 - r^2 \\ h_3 := c_1^2 + c_2^2 - r^2 \\ h_4 := ((a_1 - b_1)^2 + b_2^2)((a_1 - c_1)^2 + c_2^2)((b_1 - c_1)^2 + (b_2 - c_2)^2)w - 1 \\ g := (2((c_1 - a_1)(b_1 - c_1) + c_2(b_2 - c_2))^2 - ((c_1 - a_1)^2 + c_2^2)((b_1 - c_1)^2 + (b_2 - c_2)^2))^2 \cdot a_1^2(c_1^2 + c_2^2) - (a_1 b_1)^2 \cdot (((c_1 - a_1)^2 + c_2^2)((b_1 - c_1)^2 + (b_2 - c_2)^2))^2 \end{gathered}$$

Po výpočtu redukované Groebnerovy báze pomocí technologie Sage získáváme $G = \{1\}$ a podle věty 12 tvrzení, které dokazujeme, platí.

□

3.2 Příklady z učebnice

Věta 14 (cvičení 5 [4] str. 304)**.**
Buď ABC trojúhelník v $\mathbb{R}^2$. Všechny jeho tři výšky se protnou v jednom bodě.



Obrázek 3.2: Průsečík výšek

Důkaz. (metoda podle [5])
V důkazu budeme používat značení 3.
Volme ortonormální souřadnicový systém s počátkem v bodě A a osou x procházející bodem B, máme tedy $A = (0,0)$, $B = (b_1,0)$. Z toho, že body A, B, C tvoří trojúhelník plyne, že nejsou kolineární. Dostaneme:

$$h_1 := ((b_1 - a_1)(c_2 - a_2) - (c_1 - a_1)(b_2 - a_2))w - 1$$

Označme J bod, kde se protnou výška spuštěná z vrcholu B na stranu AC a výška spuštěná z vrcholu C na stranu AB. Dostaneme následující:

$$h_2 := (b_1 - j_1)(a_1 - c_1) + (b_2 - j_2)(a_2 - c_2)$$
$$h_3 := (c_1 - j_1)(a_1 - b_1) + (c_2 - j_2)(a_2 - b_2)$$

Nyní, pokud bude přímka procházející body A, J kolmá na stranu BC, potom to musí být výška spuštěná z vrcholu A na stranu BC a jsme hotovi. Pro případ pravoúhlého trojúhelníku s pravým úhlem u vrcholu A bychom dostali $A = J$ a určitě bude existovat přímka kolmá na stranu BC, procházející bodem A. Tento případ bude obsažen v obecném případě:

$$g := (a_1 - j_1)(b_1 - c_1) + (a_2 - j_2)(b_2 - c_2)$$

Po dosazení hodnot z volby souřadnicového systému dostaenme:

$$h_1 := b_1c_2w - 1$$
$$h_2 := (b_1 - j_1)c_1 - j_2c_2$$
$$h_3 := (c_1 - h_1)b_1$$
$$g := j_1(b_1 - c_1) + j_2c_2$$

Po výpočtu redukované Groebnerovy báze pomocí technologie Sage získáváme $G = \{1\}$ a podle věty 12 tvrzení, které dokazujeme, platí. Počet iterací během výpočtu byl...

□

Důkaz. (metoda podle [4])

Množina *předpokladů* bude $\{h_2, h_3\}$, jelikož h_1 je vyjádření nerovnice, se kterým tato varianta metody nepracuje. Podíváme se na $\mathbf{V}(h_2, h_3)$. Podle technologie Sage se tato algebraická množina rozkládá na komponenty:

$$W_1 = \mathbf{V}(b_1,j_1c_1 + j_2c_2)$$
$$W_2 = \mathbf{V}(b_1j_1 - j_2c_2 - j_1^2,j_1 - c_1)$$

Podobně jako v důkazu věty 9 bychom ověřili, že jde opravdu o ireducibilní rozklad množiny $\mathbf{V}(h_2,h_3)$. W_1 obsahuje polynom b_1, který nám povoluje případ $b_1 = 0$. Tím bychom povolovali degenerovaný případ, kde nejde o trojúhelník. Dále tedy budeme pracovat pouze s W_2.

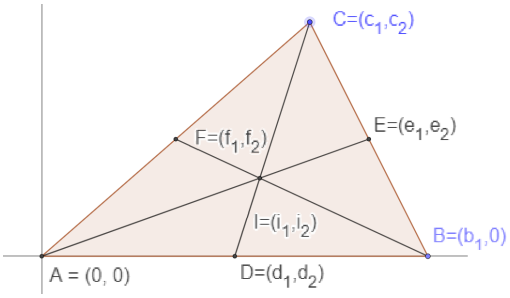
$I_2 := \langle b_1j_1-j_2c_2-j_1^2,j_1-c_1\rangle$ je prvoideál podle věty 3, jelikož W_2 je ireducibilní. Stačí nám tedy dokázat, že $g \in I_2$. Zde máme dvě možnosti jak to dokázat. Můžeme spočíst Groebnerovu bázi ideálu $\langle b_1j_1-j_2c_2-j_1^2,j_1-c_1,g\cdot y-1\rangle$ a tím podle věty 12 budeme hotovi. Další možností je porovnat redukované Groebnerovy báze I_2 a ideálu $\langle b_1j_1 - j_2c_2 - j_1^2,j_1 - c_1,g\rangle$ Budou stejné, právě když $g \in I_2$, jelikož podle věty 6 je s fixním monomiálním uspořádáním redukovaná Groebnerova báze jednoznačně určená.

Groebnerova báze ideálu $\langle b_1j_1 - j_2c_2 - j_1^2,j_1 - c_1,g \cdot y - 1\rangle$ podle technologie Sage vychází $\{1\}$ a Groebnerova báze ideálu $\langle b_1j_1 - j_2c_2 - j_1^2,j_1 - c_1,g\rangle$ vychází $\{b_1j_1 - j_2c_2 - j_1^2,j_1 - c_1\}$. Oběma postupy jsme tedy tvrzení dokázali. Počet iterací během výpočtu prvním způsobem byl... a druhým způsobem byl... Celkem se nám podařilo dokázat tvrzení i metodou podle [4].

□

Věta 15. *([cvičení 6 [4] str. 304]*

Buď ABC trojúhelník v $\mathbb{R}^2$. Všechny jeho tři těžnice se protnou v jednom bodě.



Obrázek 3.3: Průsečík těžnic

Důkaz. (metoda podle [5])

V důkazu budeme používat značení 3.

Volme ortonormální souřadnicový systém s počátkem v bodě A a osou x procházející bodem B, máme tedy $A = (0,0)$, $B = (b_1,0)$. Z toho, že body A, B, C tvoří trojúhelník, plyne, že nejsou kolineární. Dostaneme:

$$h_1 := ((b_1 - a_1)(c_2 - a_2) - (c_1 - a_1)(b_2 - a_2))w - 1$$

Označme D střed úsečky AB, E střed úsečky BC, F střed úsečky AC. Chceme vyjádřit rovnicí, že $|AD| = |BD|$. V tabulce za větou 8 máme vyjádření, které bychom mohli použít, ale jelikož máme navíc předpoklad, že A, D, B jsou kolineární, chceme vlastně vyjádřit to, že $\vec{AD} = \vec{DB}$. Analogicky pro body E, F. Pro tyto body získáváme následující *předpoklady*:

$$\begin{aligned} h_2 &:= (a_1 - d_1) - (d_1 - b_1) \\ h_3 &:= (a_2 - d_2) - (d_2 - b_2) \\ h_4 &:= (b_1 - e_1) - (e_1 - c_1) \\ h_5 &:= (b_2 - e_2) - (e_2 - c_2) \\ h_6 &:= (c_1 - f_1) - (f_1 - c_1) \\ h_7 &:= (c_2 - f_2) - (f_2 - c_2) \end{aligned}$$

Nyní označme I průsečík přímek $\overline{CD}$ a $\overline{BF}$. Z toho nám vzniknou následující *předpoklady*:

$$\begin{aligned} h_8 &:= (c_1 - i_1)(c_2 - d_2) - (c_1 - d_1)(c_2 - i_2) \\ h_9 &:= (b_1 - i_1)(b_2 - f_2) - (b_1 - f_1)(b_2 - i_2) \end{aligned}$$

Pokud nyní budou body A, I, E kolineární, víme, že jimi prochází přímka a je to poslední těžnice. Tím jsme hotovi. *Závěr* tvrzení vyjádříme následovně:

$$g := (a_1 - i_1)(a_2 - e_2) - (a_1 - e_1)(a_2 - i_2)$$

Celkem po dosazení hodnot z volby souřadnicového systému a menšími úpravami dostaneme:

$h_1 := b_1c_2w - 1$	$h_6 := c_1 - 2f_1$
$h_2 := 2d_1 - b_1$	$h_7 := c_2 - 2f_2$
$h_3 := d_2$	$h_8 := (c_1 - i_1)(c_2 - d_2) - (c_1 - d_1)(c_2 - i_2)$
$h_4 := b_1 - 2e_1 + c_1$	$h_9 := f_2(b_1 - i_1) - i_2(b_1 - f_1)$
$h_5 := -2e_2 + c_2$	$g := i_1e_2 - e_1i_2$

Po výpočtu redukované Groebnerovy báze pomocí technologie Sage získáváme $G = \{1\}$ a podle věty 12 tvrzení, které dokazujeme, platí.

□

Důkaz. (metoda podle [4])

Podobně jako v důkazu 14 podle [4] rozložíme algebraickou množinu $V := \mathbf{V}(h_2,h_3,h_4,h_5,h_6,h_7,h_8,h_9)$ na ireducibilní komponenty. Dostaneme

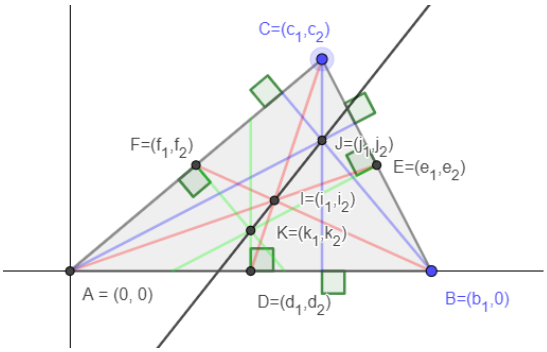
$$W_1 = \mathbf{V}(i_2,f_2,e_2 - f_2,d_2,d_1 - e_1 + f_1,c_2 - 2e_2,c_1 - 2f_1,b_1 - 2d_1)$$
$$W_2 = \mathbf{V}(2f_2 - 3i_2,e_2 - f_2,2e_1 - 3i_1,d_2,d_1 - e_1 + f_1,c_2 - 2e_2,c_1 - 2f_1,b_1 - 2d_1)$$
$$W_3 = \mathbf{V}(f_1i_2 - f_2i_1,e_2 - f_2,e_1 - f_1,d_2,d_1 - e_1 + f_1,c_2 - 2e_2,c_1 - 2f_1,b_1 - 2d_1)$$

Množiny W_1, W_3 povolují degenerované případy $c_2 = 0$ a $b_1 = 0$, dále tedy budeme pracovat pouze s W_2. Groebnerova báze ideálu $\langle 2f_2 - 3i_2,e_2 - f_2,2e_1 - 3i_1,d_2,d_1 - e_1 + f_1,c_2 - 2e_2,c_1 - 2f_1,b_1 - 2d_1,g \cdot y - 1\rangle$ vychází $\{1\}$ na počet iterací... a pokud bychom porovnávali Groebnerovy báze ideálů $\langle 2f_2 - 3i_2,e_2 - f_2,2e_1 - 3i_1,d_2,d_1 - e_1 + f_1,c_2 - 2e_2,c_1 - 2f_1,b_1 - 2d_1\rangle$ a $\langle 2f_2 - 3i_2,e_2 - f_2,2e_1 - 3i_1,d_2,d_1 - e_1 + f_1,c_2 - 2e_2,c_1 - 2f_1,b_1 - 2d_1,g\rangle$, vychází obě stejně a to $\langle b_1 + 2f_1 - 3i_1, c_1 - 2f_1, c_2 - 3i_2, d_1 + f_1 - \frac{3}{2}i_1, d_2, e_1 - \frac{3}{2}i_1, e_2 - \frac{3}{2}i_2, f_2 - \frac{3}{2}i_2\rangle$ na počet iteraci... Celkem se nám podařilo dokázat tvrzení i metodou podle [4].

□

Věta 16 (cvičení 6 [4] str. 304)**.**

Buď ABC trojúhelník v $\mathbb{R}^2$. Ortocentrum (průsečík výšek trojúhelníku), těžiště a střed kružnice opsané jsou kolineární.



Obrázek 3.4: Kolinearita ortocentra, těžiště a středu kružnice opsané

Důkaz.

V důkazu budeme používat značení 3.

Volme ortonormální souřadnicový systém s počátkem v bodě A a osou x procházející bodem B, máme tedy $A = (0,0)$, $B = (b_1,0)$. Z toho, že body A, B, C tvoří trojúhelník, plyne, že nejsou kolineární. Dostaneme:

$$h_1 := ((b_1 - a_1)(c_2 - a_2) - (c_1 - a_1)(b_2 - a_2))w - 1$$

Z důkazu věty 14 a věty 15 získáme několik rovnic, které nám dávají podmínky pro bod J označující ortocentrum, bod I označující těžiště trojúhelníku

a body spojené s definicí těchto dvou bodů. Nyní se podíváme na rovnice, které potřebujeme k označení středu kružnice opsané.

Střed kružnice opsané lze zkonstruovat jako průsečík všech 3 os stran. Nejprve dokážeme, že se všechny protnou v jednom bodě. Budeme postupovat podobným způsobem jako v předchozích důkazech, podíváme se na průsečík dvou z nich a pokud přímka procházející středem poslední strany a tímto průsečíkem bude kolmá na poslední stranu, musí to být osa strany a máme vyhráno. Označme K průsečík os stran BC a CA. Musí platit, že $\overline{EK} \perp \overline{BC}$ a $\overline{FK} \perp \overline{CA}$. Vyjádřením těchto dvou podmínek dostaneme:

$$h'_2 := (k_1 - e_1)(c_1 - b_1) + (c_2 - b_2)(k_2 - e_2)$$
$$h'_3 := (k_1 - f_1)(a_1 - c_1) + (a_2 - c_2)(k_2 - f_2)$$

Závěr tvrzení bude plynout z rovnice popisující $\overline{DK} \perp \overline{AB}$, tedy:

$$g' := (k_1 - d_1)(b_1 - a_1) + (k_2 - d_2)(b_2 - a_2)$$

Po úpravě na hodnoty z souřadnicového systému dostáváme následující množinu polynomů:

$$h_1 := b_1 c_2 w - 1$$
$$h'_2 := (k_1 - e_1)(c_1 - b_1) + c_2(k_2 - e_2)$$
$$h'_3 := (k_1 - f_1)c_1 + c_2(k_2 - f_2)$$
$$g' := (k_1 - d_1)b_1$$

Po výpočtu redukované Groebnerovy báze pomocí technologie Sage získáváme $G = \{1\}$ a podle věty 12 tvrzení (o průsečíku os stran) platí.

Nyní vyřešíme původní úlohu. Máme podmínku pro nekolinearitu bodů A, B, C označenou h_1. Dále potřebujeme podmínky pro určení ortocentra, označme ho J.

$$h_2 := (b_1 - j_1)c_1 + j_2 c_2$$
$$h_3 := (c_1 - j_1)b_1$$

Dále podmínky pro určení těžiště I:

$$h_4 := 2d_1 - b_1$$
$$h_5 := d_2$$
$$h_6 := b_1 - 2e_1 + c_1$$
$$h_7 := -2e_2 + c_2$$
$$h_8 := (c_1 - i_1)(c_2 - d_2) - (c_1 - d_1)(c_2 - i_2)$$
$$h_9 := f_2(b_1 - i_1) - i_2(b_1 - f_1)$$

A podmínky pro určení středu kružnice opsané K:

$$h_{10} := (k_1 - e_1)(c_1 - b_1) + c_2(k_2 - e_2)$$
$$h_{11} := (k_1 - f_1)c_1 + c_2(k_2 - f_2)$$

Konečně se dostáváme k *závěru* tvrzení. Chceme, aby body J, I, K byly kolineární, tedy $\overline{JI} \parallel \overline{JK}$. Z toho nám vznikne následující polynom:

$$g := (i_1 - j_1)(k_2 - j_2) - (k_1 - j_1)(i_2 - j_2)$$

Po výpočtu redukované Groebnerovy báze pomocí technologie Sage získáváme $G = \{1\}$ a podle věty 12 tvrzení platí.

□

Závěr

Cílem této práce bylo představení metody automatického dokazování geometrických tvrzení. Hlavním zdrojem byla učebnice [4], kapitola 6 §4, kde popisují variantu metody pracující s rozklady algebraických množin. Navíc po dohodě s vedoucím práce jsme zde místo metody v [4] kapitola 6 §5, představili druhou variantu podle učebnice [5], která předchází potřebě rozkládat algebraickou množinu a nahrazuje tuto komplikaci vlastním řešením přidáním předpokladů navíc.

V rámci práce jsem se seznámila s oběma těmito metodami a jejich pomocí jsem vyřešila vybrané příklady z [4], kapitola 6 §4. Navíc jsem druhou variantou metody dokázala větu o vztahu středového a obvodového úhlu. Pokusila jsem se také ukázat touto metodou i důkaz asociativity operace "+"v grupě bodů na eliptické křivce, avšak neúspěšně. Problémem by mohla být časová náročnost této metody nebo příliš složité předpoklady.

Jako výpočetní technologii jsem používala SageMath s knihovnou obsahující metodu na výpočet redukované Groebnerovy báze v oboru polynomů více proměnných s racionálními koeficienty. Dalším úskalím metody by mohla být právě tato technologie, která umí počítat pouze nad racionálními čísly, pokud bychom chtěli počítat Groebnerovy báze ideálů polynomů s jinými než racionálními koeficienty.

Námětem na další zkoumání by mohla být formalizace pojmů týkajících se varianty metody podle [4], pokus o její obecnou implementaci a analýzu výpočetní složiosti obou variant.

Seznam použité literatury

[1] A. Tarski. A decision method for elementary algebra and geometry. *Univ. of Calif. Press.*, 1948.

[2] H. Gelertner. Realization of geometry - theorem proving machine. *IFP Congres*, 1959.

[3] Joran Elias. Automated geometric theorem proving: Wu's method. *The Montana Mathematics Enthusiast*, 1998.

[4] D. Cox; J. Little; D. O'Shea. *Ideals, varieties, and algorithms. An introduction to computational algebraic geometry and commutative algebra.* Third edition. Springer, New York, 2007.

[5] Stanovský David; Barto Libor. *Počítačová algebra.* druhé vydání. Matfyzpress, Praha, 2017.

[6] Vítězslav Kala. Komutativní okruhy, `http://karlin.mff.cuni.cz/~kala/1920%20ko/KO%20skripta.pdf`, May 2020.

Seznam obrázků

A. Přílohy

A.1 Používaný kód v SageMath

```
In [1]: from sage.rings.polynomial.toy_buchberger import *
```

```
In [2]: #rovnobeznik
        P.<u_1,u_2,u_3,x_1,x_2,x_3,x_4,z,y>=PolynomialRing(QQ,9,order='lex')
        h1=x_2-u_3
        h2=x_1-u_1-u_2
        h3=x_1*x_4-x_2*x_3
        h4=x_4*u_2-x_4*u_1-u_3*x_3+u_3*u_1
        h5=u_1*u_3*z-1
        g1=-x_1**2-x_2**2+2*x_1*x_3+2*x_2*x_4
        I=P.ideal([h1,h2,h3,h4,h5,g1*y-1])

        print I.groebner_basis()
```

```
[1]
```

```
In [3]: #rovnobeznik rozklad
        print singular.minAssGTZ(P.ideal([x_2-u_3,
        x_1-u_1-u_2,x_1*x_4-x_2*x_3,x_4*u_2-x_4*u_1-u_3*x_3+u_3*u_1]))
```

```
[1]:
   _[1]=x_4
   _[2]=x_2
   _[3]=u_3-x_2
   _[4]=u_1+u_2-x_1
[2]:
   _[1]=x_2-2*x_4
   _[2]=x_1-2*x_3
   _[3]=u_3-x_2
   _[4]=u_1+u_2-x_1
[3]:
   _[1]=x_1*x_4-x_2*x_3
   _[2]=u_3-x_2
   _[3]=u_2-x_1
   _[4]=u_1+u_2-x_1
```

```
In [4]: #Groebnerova baze Rad(h1,h2,h3,h4)
        P.<u_1,u_2,u_3,x_1,x_2,x_3,x_4>=PolynomialRing(QQ,7,order='lex')
        h1=x_2-u_3
        h2=x_1-u_1-u_2
        h3=x_1*x_4-x_2*x_3
        h4=x_4*u_2-x_4*u_1-u_3*x_3+u_3*u_1
        mujideal=P.ideal([h1,h2,h3,h4]).radical()
        print mujideal.groebner_basis()
```

```
[u_1 + u_2 - x_1, u_2*x_2 - 2*u_2*x_4 - x_1*x_2 + 2*x_2*x_3,
u_3 - x_2, x_1*x_4 - x_2*x_3]
```

```
In [5]: #Groebnerova baze pruniku I_1,I_2,I_3
        P.<u_1,u_2,u_3,x_1,x_2,x_3,x_4>=PolynomialRing(QQ,7,order='lex')
        I_1=P.ideal([x_4,x_2,u_3-x_2,u_1+u_2-x_1])
        I_2=P.ideal([x_2-2*x_4,x_1 - 2*x_3, u_3 - x_2, u_1 + u_2 - x_1])
        I_3=P.ideal([x_1*x_4 -x_2*x_3, u_3 -x_2, u_2-x_1, u_1+u_2 - x_1])
        I_123=I_3.intersection(I_2).intersection(I_1)
        print I_123.groebner_basis()
        print I_123.groebner_basis()==mujideal.groebner_basis()
```

```
[u_1 + u_2 - x_1, u_2*x_2 - 2*u_2*x_4 - x_1*x_2 + 2*x_2*x_3, u_3 - x_2,
x_1*x_4 - x_2*x_3]
True
```

```
In [6]: #vztah stredoveho a obvodoveho uhlu
        P.<a_1,b_1,b_2,c_1,c_2,w_1,w_2,w_3,y>=PolynomialRing(QQ,9,order='lex')
        h_1=a_1-1
        h_2=b_1^2+b_2^2-1
        h_3=c_1^2+c_2^2-1
        h_41=((a_1-b_1)^2+b_2^2)*w_1-1
        h_42=((b_1-c_1)^2+(b_2-c_2)^2)*w_2-1
        h_43=((a_1-c_1)^2+c_2^2)*w_3-1
        g=(2*((c_1-a_1)*(b_1-c_1)+c_2*(b_2-c_2))^2-((c_1-a_1)^2+c_2^2)*
        ((b_1-c_1)^2+(b_2-c_2)^2))^2*a_1^2*(c_1^2+c_2^2)-
        (((c_1-a_1)^2+c_2^2)*((b_1-c_1)^2+(b_2-c_2)^2))^2*(a_1*b_1)^2
        I=P.ideal([h_1,h_2,h_3,h_41,h_42,h_43,g*y-1])
        print I.groebner_basis()
```

```
[1]
```

```
In [7]: #priklad 5 z ucebnice
        P.<b_1,c_1,c_2,j_1,j_2,w,y>=PolynomialRing(QQ,7,order='lex')
        h1=b_1*c_2*w-1
        h2=(b_1-j_1)*c_1+j_2*c_2
        h3=(c_1-j_1)*b_1
        g=j_1*(b_1-c_1)+j_2*c_2
        I=P.ideal([h1,h2,h3,g*y-1])
        print I.groebner_basis()
```

```
[1]
```

```
In [8]: #priklad 5 druhou metodou
        P.<b_1,c_1,c_2,j_1,j_2,w,y>=PolynomialRing(QQ,7,order='lex')
        h2=(b_1-j_1)*c_1+j_2*c_2
```

```
        h3=(c_1-j_1)*b_1
        g=j_1*(b_1-c_1)+j_2*c_2
        I=P.ideal([h2,h3])
        print singular.minAssGTZ(I)
        print P.ideal([b_1*j_1+c_2*j_2-j_1^2,c_1-j_1,g*y-1]).groebner_basis()
        print P.ideal([b_1*j_1+c_2*j_2-j_1^2,c_1-j_1]).groebner_basis()
        print P.ideal([b_1*j_1+c_2*j_2-j_1^2,c_1-j_1]).groebner_basis()
        ==P.ideal([b_1*j_1+c_2*j_2-j_1^2,c_1-j_1,g]).groebner_basis()
```

```
[1]:
   _[1]=c_1*j_1-c_2*j_2
   _[2]=b_1
[2]:
   _[1]=b_1*j_1+c_2*j_2-j_1^2
   _[2]=c_1-j_1
[1]
[b_1*j_1 + c_2*j_2 - j_1^2, c_1 - j_1]
True
```

```
In [9]: #priklad 6 z ucebnice
        P.<b_1,c_1,c_2,d_1,d_2,e_1,e_2,f_1,f_2,i_1,i_2,w,y
        =PolynomialRing(QQ,13,order='lex')
        h_1=b_1*c_2*w-1
        h_2=2*d_1-b_1
        h_3=d_2
        h_4=b_1-2*e_1+c_1
        h_5=-2*e_2+c_2
        h_6=c_1-2*f_1
        h_7=c_2-2*f_2
        h_8=(c_1-i_1)*(c_2-d_2)-(c_1-d_1)*(c_2-i_2)
        h_9=f_2*(b_1-i_1)-i_2*(b_1-f_1)
        g=i_1*e_2-e_1*i_2

        I=P.ideal([h_1,h_2,h_3,h_4,h_5,h_6,h_7,h_8,h_9,g*y-1])
        print I.groebner_basis()
```

```
[1]
```

```
In [10]: #priklad 6 druhou metodou
         P.<b_1,c_1,c_2,d_1,d_2,e_1,e_2,f_1,f_2,i_1,i_2,w,y>
         =PolynomialRing(QQ,13,order='lex')
         h_2=2*d_1-b_1
         h_3=d_2
         h_4=b_1-2*e_1+c_1
         h_5=-2*e_2+c_2
         h_6=c_1-2*f_1
         h_7=c_2-2*f_2
```

```
        h_8=(c_1-i_1)*(c_2-d_2)-(c_1-d_1)*(c_2-i_2)
        h_9=f_2*(b_1-i_1)-i_2*(b_1-f_1)
        g=i_1*e_2-e_1*i_2

        I=P.ideal([h_2,h_3,h_4,h_5,h_6,h_7,h_8,h_9])
        print singular.minAssGTZ(I)
        print P.ideal([2*f_2-3*i_2,e_2-f_2,2*e_1-3*i_1,d_2,
        d_1-e_1+f_1,c_2-2*e_2,c_1-2*f_1,b_1-2*d_1,g*y-1]).groebner_basis()
        print P.ideal([2*f_2-3*i_2,e_2-f_2,2*e_1-3*i_1,d_2,
        d_1-e_1+f_1,c_2-2*e_2,c_1-2*f_1,b_1-2*d_1]).groebner_basis()
        print P.ideal([2*f_2-3*i_2,e_2-f_2,2*e_1-3*i_1,d_2,
        d_1-e_1+f_1,c_2-2*e_2,c_1-2*f_1,b_1-2*d_1]).groebner_basis()
        ==P.ideal([2*f_2-3*i_2,e_2-f_2,2*e_1-3*i_1,d_2,
        d_1-e_1+f_1,c_2-2*e_2,c_1-2*f_1,b_1-2*d_1,g]).groebner_basis()
```

```
[1]:
   _[1]=i_2
   _[2]=f_2
   _[3]=e_2-f_2
   _[4]=d_2
   _[5]=d_1-e_1+f_1
   _[6]=c_2-2*e_2
   _[7]=c_1-2*f_1
   _[8]=b_1-2*d_1
[2]:
   _[1]=2*f_2-3*i_2
   _[2]=e_2-f_2
   _[3]=2*e_1-3*i_1
   _[4]=d_2
   _[5]=d_1-e_1+f_1
   _[6]=c_2-2*e_2
   _[7]=c_1-2*f_1
   _[8]=b_1-2*d_1
[3]:
   _[1]=f_1*i_2-f_2*i_1
   _[2]=e_2-f_2
   _[3]=e_1-f_1
   _[4]=d_2
   _[5]=d_1-e_1+f_1
   _[6]=c_2-2*e_2
   _[7]=c_1-2*f_1
   _[8]=b_1-2*d_1
[1]
[b_1 + 2*f_1 - 3*i_1, c_1 - 2*f_1, c_2 - 3*i_2, d_1 + f_1 - 3/2*i_1,
d_2, e_1 - 3/2*i_1, e_2 - 3/2*i_2, f_2 - 3/2*i_2]
True
```

```
In [11]: #stred kruznice opsane
```

```
P.<b_1,c_1,c_2,d_1,d_2,e_1,e_2,f_1,f_2,k_1,k_2,w,y>
=PolynomialRing(QQ,13,order='lex')
h_1=b_1*c_2*w-1
h_2=2*d_1-b_1
h_3=d_2
h_4=b_1-2*e_1+c_1
h_5=-2*e_2+c_2
h_6=c_1-2*f_1
h_7=c_2-2*f_2
h_8=(k_1-e_1)*(c_1-b_1)+c_2*(k_2-e_2)
h_9=(k_1-f_1)*c_1+c_2*(k_2-f_2)
g=(k_1-d_1)*b_1
I=P.ideal([h_1,h_2,h_3,h_4,h_5,h_6,h_7,h_8,h_9,g*y-1])
print I.groebner_basis()
```

```
[1]
```

In [12]:
```
#vsechno dohromady
P.<b_1,c_1,c_2,d_1,d_2,e_1,e_2,f_1,f_2,i_1,i_2,j_1,j_2,
k_1,k_2,w,y>=PolynomialRing(QQ,17,order='lex')
h_1=b_1*c_2*w-1
h_2=2*d_1-b_1
h_3=d_2
h_4=b_1-2*e_1+c_1
h_5=-2*e_2+c_2
h_6=c_1-2*f_1
h_7=c_2-2*f_2
g_2=i_1*e_2-e_1*i_2
h_8=(b_1-j_1)*c_1+j_2*c_2
h_9=(c_1-j_1)*b_1
g_1=j_1*(b_1-c_1)-j_2*c_2
h_10=(c_1-i_1)*(c_2-d_2)-(c_1-d_1)*(c_2-i_2)
h_11=f_2*(b_1-i_1)-i_2*(b_1-f_1)
h_12=(k_1-e_1)*(c_1-b_1)+c_2*(k_2-e_2)
h_13=(k_1-f_1)*c_1+c_2*(k_2-f_2)
g_3=(k_1-d_1)*b_1
g=(i_1-j_1)*(k_2-j_2)-(k_1-j_1)*(i_2-j_2)
I=P.ideal([h_1,h_2,h_3,h_4,h_5,h_6,h_7,h_8,h_9,h_10,h_11,
h_12,h_13,g_1,g_2,g_3,g*y-1])
print I.groebner_basis()
```

```
[1]
```