ZÁPADOČESKÁ UNIVERZITA V PLZNI
FAKULTA PEDAGOGICKÁ
KATEDRA MATEMATIKY, FYZIKY A TECHNICKÉ VÝCHOVY

POLYNOMIÁLNÍ SUBSTITUCE A ROZKLADY

BAKALÁŘSKÁ PRÁCE

Tereza Horová
Učitelství pro 2. stupeň ZŠ, obor Ma-Ge

Vedoucí práce: Mgr. Martina Kašparová, Ph.D.

Plzeň 2020

ZÁPADOČESKÁ UNIVERZITA V PLZNI

Fakulta pedagogická

Akademický rok: 2018/2019

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení:	**Tereza HOROVÁ**
Osobní číslo:	**P17B0005P**
Studijní program:	**B1001 Přírodovědná studia**
Studijní obor:	**Matematická studia**
Téma práce:	**Polynomiální substituce a rozklady**
Zadávající katedra:	**Katedra matematiky, fyziky a technické výchovy**

Zásady pro vypracování

1. Složené funkce
2. Rozložitelnost polynomu na polynomy stupně většího než 1
3. Rittova věta o polynomiálním rozkladu
4. Algoritmus pro výpočet polynomiálního rozkladu
5. Užití rozkladů polynomů

Rozsah bakalářské práce: **30 – 50**
Rozsah grafických prací:
Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam doporučené literatury:

BARTON, D., R., ZIPPEL, R. Polynomial Decomposition Algorithms. Journal of Symbolic Computation. 1985, 1(2), 159-168.
COHEN, J., S. Computer algebra and symbolic computation: mathematical methods. Natick, Mass.: AK Peters, 2003. ISBN 1568811594.
CORRALES-RODRIGÁNEZ, C. A note on Ritt's theorem on decomposition of polynomials. Journal of Pure and Applied Algebra. 1990, 68(3), 293-296. ISSN 00224049.
RITT, J., F. Prime and Composite Polynomials. Transactions of the American Mathematical Society. 1922, 23(1), 51-66.
WYMAN, B., K., ZIEVE, M., E. Two questions on polynomial decomposition. The Quarterly Journal of Mathematics. 2012, 63(2), 507-511.

Vedoucí bakalářské práce: **Mgr. Martina Kašparová, Ph.D.**
Katedra matematiky, fyziky a technické výchovy

Datum zadání bakalářské práce: **3. června 2019**
Termín odevzdání bakalářské práce: **30. června 2020**

RNDr. Miroslav Randa, Ph.D.
děkan

Doc. PaedDr. Jarmila Honzíková, Ph.D.
vedoucí katedry

V Plzni dne 20. června 2019

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně s použitím uvedené literatury a zdrojů informací.

Plzeň, 19. ledna 2020

.....

vlastnoruční podpis

Poděkování

Ráda bych poděkovala především mé vedoucí bakalářské práce
Mgr. Martině Kašparové, Ph.D. za její ochotu, pomoc a spolupráci při tvorbě této práce. Dále chci poděkovat mým blízkým, kteří mě po celou dobu studia podporovali.

Obsah

Abstrakt

Tato práce se zabývá rozkladem polynomů. Čtenář se zde může dozvědět, jaké způsoby rozkladů se v matematice využívají. Kromě lehčích polynomů v podobě základních vzorců pro rozklad na součin, se kterými se setkáváme již na základních školách, se tato práce zaměřuje na rozklad polynomů složitějších. Hlavním cílem je seznámit čtenáře s algoritmem, díky němuž lze rozložit složitější polynomy.

Úvod

Tato bakalářská práce se zabývá rozkladem polynomů. Jejím cílem je čtenáři přiblížit, jaké druhy rozkladů můžeme při práci s polynomy využít. Jedná se především o práci se složitými polynomy, kde na první pohled není jejich rozklad jasný. Podrobně se budu věnovat rozkladu podle Ritterovy věty o polynomiálním rozkladu. Tento způsob rozkladu není v praxi běžný. Ačkoliv se jedná o složitý algoritmus, je pro matematiky velice užitečný. Proto také uvedu i příklady, kdy je jeho využití vhodné.

Práce je rozdělena do pěti kapitol. První kapitolu využiji k popisu běžně používaných rozkladů funkcí a čtenáři připomenu problematiku rozkladu mnohočlenů na součin. Je důležité si tyto typy rozkladů zde uvést, aby si čtenář uvědomil, v jakém významu budeme v této bakalářské práci chápat úkol „rozložit polynom“. V druhé kapitole vysvětlím jednotlivé pojmy týkající se polynomů, s kterými budu nadále pracovat, připravím pole pro objasnění následující problematiky. V třetí kapitole se již dostanu k hlavní části této práce, čímž je uvedení a vysvětlení Ritterovy věty o polynomiálním rozkladu. Následující čtvrtá kapitola bude obsahovat algoritmus pro výpočet polynomiálního rozkladu. Poslední kapitola bude věnována příkladům, kde budu porovnávat různé metody výpočtu hodnot polynomů a v tomto ohledu poukážu na využití rozkladu polynomů. Čtenáři představím program, ve kterém lze provést rozklad polynomu. V úplném závěru této kapitoly zmíním problematiku vyjádření řešení rovnic v radikálech a uvedu příklad, který bude ukazovat výhodu rozkladu polynomů.

1 Operace s funkcemi a mnohočleny

Existuje mnoho operací, které lze s funkcemi i mnohočleny aplikovat. Pro potřeby této práce se zaměříme pouze na dvě konkrétní operace, jimiž jsou rozklad mnohočlenů na součin a skládání funkcí.

1.1 Rozklad mnohočlenů na součin

V následujících kapitolách budeme hovořit především o mnohočlenech. Existují různé typy rozkladů, kterými lze mnohočlen rozložit. Jedním z nich je rozklad na součin. V této podkapitole tedy budeme rozkladem mít na mysli rozklad na součin mnohočlenů. „Rozkladem mnohočlenu rozumíme vyjádření daného mnohočlenu jako součinu jednodušších, většinou již dále nerozložitelných, mnohočlenů.“ (Pavlicová 2010) Vždy musíme předem vědět, v jakém oboru čísel se pohybujeme, aby nedošlo k nesrovnalostem ve výsledcích.

Pro dosáhnutí rozkladu mnohočlenu můžeme využít následující metody:

1. **Vytýkání před závorku**

V tomto případě musíme nalézt společný mnohočlen pro jednotlivé prvky původního mnohočlenu a vytknout jej před závorku. Pokud vytkneme ten nejvyšší možný, proces je již u konce. Jestliže je stále možnost nějaký mnohočlen vytknout musíme tento proces opakovat až do té doby, kdy tomu již nepůjde dál.

Příklad 1.1

V tomto příkladě si názorně ukážeme, jak by vypadal mnohočlen, který upravíme pomocí vytýkání před závorku. Mějme tedy zadaný mnohočlen

$$\boldsymbol{9x^6 + 18x^4 - 36x^2}.$$

Pokud bychom chtěli postupovat opatrněji a vytýkat z jednotlivých členů postupně, mohl by náš výpočet vypadat takto:

$$9x^6 + 18x^4 - 36x^2 = 3x^2(3x^4 + 6x^2 - 12) = 3 \cdot 3x^2(x^4 + 2x^2 - 4) =$$
$$= 9x^2(x^4 + 2x^2 - 4).$$

Pokud bychom chtěli vytknout nejvyšší možný mnohočlen a získat výsledek hned v prvním kroku, náš postup bychom zapsali jako

$$9x^6 + 18x^4 - 36x^2 = 9x^2(x^4 + 2x^2 - 4).$$

2. Vzorce

Dalším způsobem, jak rozložit mnohočlen na součin, je využití vzorců, které nám k tomu napomáhají. Tento typ rozkladu ovšem vyžaduje znalost jednotlivých vzorců. Mezi základní vzorce řadíme

$$(A + B)^2 = A^2 + 2AB + B^2$$
$$(A - B)^2 = A^2 - 2AB + B^2$$
$$A^2 - B^2 = (A + B)(A - B).$$

Dalšími méně využívanými, ale přesto velice zásadními vzorci jsou

$$(A + B)^3 = A^3 + 3A^2B + 3AB^2 + B^3$$
$$(A - B)^3 = A^3 - 3A^2B + 3AB^2 - B^3$$
$$A^3 + B^3 = (A + B)(A^2 - AB + B^2)$$
$$A^3 - B^3 = (A - B)(A^2 + AB + B^2).$$

Příklad 1.2

Na příkladu 1.2 si ukážeme, jak využijeme jeden ze základních vzorců. Mějme zadaný mnohočlen

$$25x^4 + 40x^2 + 16.$$

Podle vzorce $(A + B)^2 = A^2 + 2AB + B^2$ můžeme tento mnohočlen zapsat jako součin dvou stejných mnohočlenů a výsledek bude vypadat takto:

$$25x^4 + 40x^2 + 16 = (5x^2 + 4)^2$$

3. Kvadratický trojčlen

Kvadratický trojčlen $ax^2 + bx + c$ lze rozložit dvěma způsoby. Prvním z nich je řešení kvadratické rovnice

$$ax^2 + bx + c = 0.$$

Důležité je na začátku počítání vědět, v jakém oboru čísel danou rovnici řešíme. Obor čísel nám zásadně ovlivní průběh výpočtu.

Můžeme nejprve zjistit diskriminant D pomocí vzorce

$$D = b^2 - 4ac$$

Následně pak vypočítáme jednotlivé kořeny díky dosazení do vzorečku

$$x_{1,2} = \frac{-b \mp \sqrt{D}}{2a}.$$

V případě, že by se jednalo o obor reálných čísel, je nutné nezapomenout, že $D \geq 0$. Pokud bychom počítali příklad nad tělesem komplexních čísel, diskriminant by mohl nabývat i záporných čísel. Rozklad trojčlenu pak zapíšeme ve tvaru

$$(x - x_1)(x - x_2) = 0.$$

Příklad 1.3.1

Uveďme si konkrétní příklad, kde využijeme postup řešení kvadratické rovnice. Příklad budeme řešit nad tělesem reálných čísel. Uvažujme rovnici

$$x^2 + 2x - 63 = 0.$$

Diskriminant této rovnice vypočítáme jako

$$D = 2^2 - 4 \cdot 1 \cdot (-63) = 4 + 252 = 256.$$

Jelikož je splněna podmínka $D \geq 0$, mohu pokračovat v počítání a dosadit do vzorečku pro výpočet jednotlivých kořenů.

$$x_{1,2} = \frac{-2 \mp \sqrt{256}}{2 \cdot 1}$$

Následně rozdělím rovnost na dvě části, které mě dovedou výsledkům x_1 a x_2.

$$x_1 = \frac{-2 + 16}{2} = 7$$

$$x_2 = \frac{-2 - 16}{2} = -9$$

Nalezla jsem kořeny námi zadané rovnice, kterými jsou čísla -9 a 7. Výsledný rozklad kvadratické trojčlenu zapíšeme následovně:

$$(x + 9)(x - 7) = 0.$$

Druhý způsob, jak kvadratický trojčlen rozložit se zdá být na první pohled složitější, ale často nám usnadní práci. Nejprve si ujasníme podmínky, za kterých tento postup lze využít. Opět řešíme kvadratickou rovnici ve tvaru

$$ax^2 + bx + c = 0.$$

V tomto případě budeme předpokládat, že koeficient a bude roven 1. Následně si rovnici přepíšu do tvaru

$$x^2 - (x_1 + x_2)x + (x_1 \cdot x_2) = 0,$$

kde

$$b = x_1 + x_2 \text{ a } c = x_1 \cdot x_2.$$

Výsledkem našeho snažení je opět zpětné dosazení do mnohočlenu ve tvaru

$$(x - x_1)(x - x_2) = 0.$$

Příklad 1.3.2

V tomto příkladu uvidíme aplikaci druhého postupu při rozkládání kvadratického trojčlenu. Mějme zadanou kvadratickou rovnici

$$x^2 + 2x - 63 = 0$$

Naším úkolem je získat rozklad kvadratického trojčlenu na součin.

$$x^2 - (-9 + 7)x + (-9 \cdot 7) = 0$$
$$(x + 9)(x - 7) = 0$$

Výsledný součinový tvar je u obou postupů totožný, tudíž je na nás, který postup zvolíme.

4. Hornerovo schéma

Hlavním významem vytvoření Hornerova schématu je snadný výpočet hodnoty polynomu v daném bodě, což si ukážeme v páté kapitole této práce. Ovšem díky němu můžeme i nalézt kořeny rovnic, a to v případě, že hodnota v daném bodě bude rovna nule. Většinou tento způsob rozkladu mnohočlenu na součin využíváme ve složitějších případech, než jsou pouze kvadratické mnohočleny. V následujícím příkladu si názorně ukážeme, jakým způsobem dosáhneme kořenu.

Příklad 1.4

Mějme zadanou rovnici

$$x^4 - 4x^3 - 10x^2 + 28x - 15 = 0.$$[1]

[1] MAŘÍK, R. [nedatováno]. Hornerovo schéma. *Mendelova univerzita v Brně: Home Page of Robert Mařík*. (http://user.mendelu.cz/marik/wiki/pdf/algrce.pdf , 14. 6. 2020).

Naším úkolem bude pomocí Hornerova schématu nalézt nulové body této rovnice, díky kterým pak budeme schopni napsat rozklad polynomu na součin.

Na první pohled není zcela jasné, jak tento mnohočlen, který je normovaný (koeficient členu s nejvyšší mocninou je 1) a jeho koeficienty jsou celá čísla, rozložit na součin. Proto budeme zkoušet některá celá čísla z množiny dělitelů čísla -15, tj. $D = \{\pm 1, \pm 3, \pm 5, \pm 15\}$. Pokud má daná rovnice celočíselná řešení, mohou to být jedině prvky množiny D. Schéma vytvoříme tak, že do vrchního řádku napíšeme koeficienty jednotlivých členů mnohočlenu. V našem případě tedy čísla 1, -4, -10, 25, -15. Do levého sloupce budeme psát prvky množiny D. Naše schéma bude vypadat následovně:

	1	− 4	− 10	28	− 15
-1		1	− 5	− 15	33
	1	− 5	− 15	33	**− 48**

násobení

sčítání

přepsání

Hodnotu koeficientu u komponentu s nejvyšším stupněm přepíši do třetího řádku (1). Zároveň jej přepíši i pod hodnotu druhého koeficientu (-4). Číslo zvolené z množiny D (-1) vždy vynásobíme s hodnotou v druhém řádku (1). Tento výsledek sečteme s hodnotou koeficientu, který je nad ním (-4) a získané číslo zaznamenáme do třetího řádku. Toto číslo přepíšeme pod další koeficient a postupujeme stejným způsobem jako u toho prvního. Takto pokračujeme až do konce našeho schématu. Pokud výsledný součet je roven 0, jedná se o vhodně zvolené číslo a můžeme ho nazvat kořenem rovnice. V případě, že jsme zvolili číslo -1, musíme říci, že se o kořen nejedná, jelikož výsledný součet je roven -48. Volme tedy jiného kandidáta z množiny D, číslo 1.

	1	− 4	− 10	28	− 15
1		1	− 3	− 13	15
	1	− 3	− 13	15	**0**

Vidíme, že hodnota, kterou jsme získali na konci Hornerova schématu je rovna 0 a tedy můžeme hovořit o kořenu našeho mnohočlenu $x^4 - 4x^3 - 10x^2 + 28x - 15$. Nalezení kořenu se nám promítne v úpravě naší rovnice a můžeme ji zapsat jako

$$(x^3 - 3x^2 - 13x + 15)(x - 1) = 0.$$

Výraz v levé části rovnice se skládá ze součinu dvou mnohočlenů, z čehož jeden jsme získali právě díky nalezení kořenu. Mluvíme o mnohočlenu $(x - 1)$. Druhý mnohočlen vytvoříme tak, že snížíme jeho stupeň o 1 a koeficienty u jednotlivých členů se rovnají hodnotám třetího řádku v našem schématu. Tato fáze našeho postupu je u konce a my budeme postupovat s rozkladem mnohočlenu $(x^3 - 3x^2 - 13x + 15)$ pomocí stejného algoritmu. Opět zvolím číslo z množiny D, které by mohlo být vhodným kandidátem. Vyzkoušíme tedy opět číslo 1. Do horního řádku zapíšeme nové koeficienty.

	1	− 3	− 13	15
1		1	− 2	− 15
	1	− 2	− 15	**0**

Opět vidíme, že výsledná hodnota je rovna 0 a 1 je tedy dalším kořenem rovnice a rozklad levé strany rovnice na součin bude vypadat takto:

$$(x^2 - 2x - 15)(x - 1)(x - 1) = 0.$$

Jelikož poslední nerozložený mnohočlen je kvadratický, tak ho rozložíme pomocí předchozích metod, čímž dojdeme k výsledku

$$(x + 3)(x - 5)(x - 1)^2 = 0.$$

Kořeny rovnice jsou

$$x_1 = -3,$$

$$x_2 = 5,$$

$$x_3 = 1,$$

kde kořen 1 je dvojnásobným kořenem.

Tyto způsoby rozkladu mnohočlenů jsou v matematice běžné a automaticky používané. Existuje také mnoho dalších typů rozkladů. Nás ovšem bude zajímat pouze jeden z nich. K tomu, abychom se do dané problematiky ponořili, si musíme ještě ujasnit jednu ze základních matematických operací, kterou je skládání funkcí.

1.2 Složené funkce

Než si vyřkneme přímou definici složené funkce, pojďme se podívat na jednoduchý příklad, který nám připomene, jak vypočítáme funkční hodnotu v daném bodě. Díky tomu pak můžeme snadněji porozumět principu skládání funkcí.

Příklad 1.5

Mějme zadanou funkci $cos^2 x$. Naším úkolem bude nalézt funkční hodnotu v bodě 3.

Naším prvním krokem bude dosazení čísla 3 do předpisu funkce, čímž dostáváme výraz $cos^2 3$. V druhé fázi výpočtu se snažíme získat výslednou funkční hodnotu. Tento proces si rozdělíme na dvě části. V první části nejprve vypočteme hodnotu výrazu $cos 3$.

$$cos 3 = 0{,}9986295348$$

V druhé části postupu budeme hodnotu $0{,}9986295348$ umocňovat na druhou. Čímž dostaneme

$$0{,}9986295348^2 = 0{,}9972609478.$$

Můžeme tedy říci, že funkční hodnota funkce $cos^2 x$ v bodě 3 je rovna $0{,}9972609478$.

Pojďme si tedy definovat, co je to složená funkce a následně si ukážeme, jak tento pojem souvisí s příkladem 1.2.

Definice 1.2

Mějme funkce f a g, kde

$$f: B \to R,$$
$$g: A \to R.$$

a H je oborem hodnot funkce. Je-li $H(g)$ podmnožinou B, pak funkci F ve tvaru

$$F = f \circ g: A \to R$$

nebo také

$$F(x) = f\big(g(x)\big)$$

nazýváme složenou funkcí. Tato funkce se skládá z 2 základních složek, jimiž jsou původní funkce f a g. Funkce f označujeme jako vnější složku (vnější funkci) a funkci g pak jako složku vnitřní (vnitřní funkci). (Brabec – Martan – Rozenský 1989: 92)

Vraťme se k příkladu 1.5 a ukažme si, jak v tomto případě lze chápat funkci jako složenou. Měli jsme zadanou funkci $cos^2 x$. Jako vnitřní funkci g označíme funkci $cosx$ a jako funkci f vnější funkci x^2. Složení těchto dvou funkcí zapíšeme jako $F = f \circ g$, nebo také jako $F(x) = f\big(g(x)\big)$. Čili dostáváme

$$F(x) = x^2 \circ cosx = cos^2 x.$$

Abychom problematiku skládání funkcí lépe pochopili, uvedeme si zde ještě jeden příklad.

Příklad 1.6

Mějme zadané funkce

$$f(g) = \sqrt{x+5}$$
$$g(x) = lnx - x^5.$$

Naším úkolem je aplikovat operaci skládání funkcí.

a) $F(x) = f\big(g(x)\big)$

$$F(x) = f\big(g(x)\big) = \sqrt{lnx - x^5 + 5}$$

b) $G(x) = g\big(f(x)\big)$

$$G(x) = g\big(f(x)\big) = ln\sqrt{x+5} - \sqrt{x+5}^5$$

Díky tomuto příkladu můžeme vidět, že je velice důležité, v jakém pořadí funkce skládáme. Ačkoliv v obou případech funkce f i g měly stejnou podobu, tak po jejich složení v rozdílném pořadí se zápis výsledné složené funkce zásadně liší. Můžeme tedy říci, že operace skládání funkcí není komutativní.

Operaci skládání funkcí můžeme aplikovat postupně na více funkcí. Nás bude ovšem zajímat proces opačný a to postupné rozkládání funkcí na jednotlivé složky čili základní elementární funkce.

Příklad 1.7

Mějme zadaný předpis funkce $F(x) = sin^2\big(\sqrt{x+3}\big)$. Rozložme tuto funkci na jednotlivé elementární funkce. V tomto případě je vnější funkcí funkce $f(x) = x^2$ a vnitřní funkcí $g(x) = sin\sqrt{x+3}$. Můžeme si všimnout, že se funkce $g(x)$ je složena ještě z jedné funkce, kterou je odmocnina. Tuto funkci značíme h a její předpis bude $h(x) = \sqrt{x+3}$. Funkce $F(x)$ je tedy složena z třech různých funkcí a zapíšeme to následovně:

$$F(x) = f\Big(g\big(h(x)\big)\Big) = x^2 \circ sinx \circ \sqrt{x+3}.$$

2 Pojmy

V této kapitole si připomeneme některé základní pojmy, které budeme potřebovat v následujících kapitolách. Také je důležité ujasnit si, jaké značení budeme v následujících kapitolách využívat, aby nedošlo ke špatnému pochopení zápisů. Bude nás zajímat problematika týkající se polynomů. Pojďme si tedy nejprve definovat, co to vlastně polynom je a následně si definujeme pojmy složený polynom a rozložitelný polynom.

2.1 Polynom

Hned na úvod této podkapitoly si pojďme uvést definici polynomu

Definice 2.1

„Polynomem je vzorec ve tvaru

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

Kde $a_0, a_1, \ldots, a_n$ jsou komplexní čísla a x je proměnná. Čísla $a_0, a_1, \ldots, a_n$ nazýváme koeficienty polynomu.

Hodnota polynomu $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ v bodě $\alpha \in C$je komplexní číslo, které získáme dosazením čísla α za proměnnou x do uvedného vzorce. “[2]

2.2 Složený polynom

Na začátku této kapitoly je důležité definovat, jaké označení budeme využívat. Polynomy $u(x)$ budeme chápat jako funkce, a tudíž jejich skládání jako skládání funkcí. Ačkoliv jsme v definici 2.1 polynomy nadefinovali v oboru komplexních čísel, budeme se v následujících kapitolách zabývat polynomy definovanými pouze v $Q[x]$.

Definice 2.2

Nechť $u(x), v(x)$ a $w(x)$ jsou polynomy, jejichž stupeň je větší nebo roven nule, definované v $Q[x]$. Polynom $u(x)$ definovaný výrazem

[2] OLŠÁK P. (2012). *BI- Lineární algebra* [přednáška] (Praha: České vysoké učení technické). (http://petr.olsak.net/bilin/polynomy4.pdf, 13. 4. 2020)

$$u(x) = v\big(w(x)\big)$$

Nebo také

$$u(x) = (v \circ w)(x)$$

nazveme složeným polynomem.

Příklad 2.1

V tomto příkladu si uvedeme konkrétní polynom, abychom názorně viděli, jak jeho skládání funguje. Nechť máme zadaný polynom $u(x)$.

$$u(x) = (x^2 + 5x + 2)^2 - 12(x^2 + 5x + 2) - 7.$$

Tento polynom lze prezentovat jako složení dvou polynomů $v(x)$ a $w(x)$. Tento fakt vyjádříme pomocí matematického zápisu skládání.

$$v(x) = x^2 - 12x - 7,$$
$$w(x) = x^2 - 5x + 2,$$
$$u(x) = (v \circ w)(x) = (x^2 - 5x + 2)^2 - 12((x^2 - 5x + 2) - 7.$$

V případě skládání více polynomů je zápis složitější, ale jeho princip je stále stejný. Mějme tedy polynomy $v(x), w(x), y(x), z(x)$. Složený polynom $u(x)$ tedy zapíšeme jako

$$u(x) = (v \circ w \circ y \circ z)(x),$$

neboli

$$u(x) = v\Big(w\Big(y\big(z(x)\big)\Big)\Big).$$

Matematická operace skládání polynomů má několik důležitých vlastností. Jednou z nich je kupříkladu asociativita. Druhou takovou vlastností je fakt, že pokud

při skládání dvou polynomů $u(x)$ a $v(x)$, kde $v(x) = x$, je skládání těchto polynomů komutativní a je rovno polynomu $u(x)$. Třetí vlastnost nám říká, že stupeň složeného polynomu $w = (u \circ v)$ je roven stupni součinu polynomů u, v pro $u \neq 0$ a $v \neq 0$. Všechny tyto vlastnosti včetně konkrétních příkladů si pojďme ukázat v následující větě 2.1.

Věta 2.1

Nechť jsou dány polynomy u, v, w a jsou definovány v $Q[x]$. Potom platí

a) Asociativita: $u \circ (v \circ w) = (u \circ v) \circ w$

Příklad 2.1:

Nechť jsou zadány polynomy $u(x)$, $v(x)$ a $w(x)$.

$$u(x) = x^2 + 3$$
$$v(x) = x^2 - 3x - 2$$
$$w(x) = x^3 + 7$$

Nejprve si ukážeme, jak bude vypadat složený polynom, pokud nejprve složíme polynomy $v(x)$ a $w(x)$ a následně až s polynomem $u(x)$. Náš výpočet bude vypadat takto:

$$y_1(x) = \big(u \circ (v \circ w)\big)(x) = (x^2 + 3) \circ ((x^3 + 7)^2 - 3(x^3 + 7) - 2) =$$
$$= ((x^3 + 7)^2 - 3(x^3 + 7) - 2)^2 + 3 = (x^6 + 14x^3 + 49 - 3x^3 - 21 - 2)^2 + 3 =$$
$$= (x^6 + 11x^3 + 26)^2 + 3 = x^{12} + 22x^9 + 173x^6 + 572x^3 + 679.$$

V druhé části příkladu si ukažme, jak by výsledný polynom vypadal, pokud bychom nejprve složily polynomy $u(x)$ a $v(x)$ a následně až s polynomem $w(x)$. V tomto případě by výpočet vypadal následovně:

$$y_2(x) = \big((u \circ v) \circ w\big)(x) = ((x^2 - 3x - 2)^2 + 3) \circ (x^3 + 7) =$$
$$= ((x^3 + 7)^2 - 3(x^3 + 7) - 2)^2 + 3 = +3 = (x^6 + 11x^3 + 26)^2 + 3 =$$

$$= x^{12} + 22x^9 + 173x^6 + 572x^3 + 679.$$

Všimněme si, že oba výsledné polynomy $y_1(x)$ a $y_2(x)$ jsou totožné. Píšeme tedy

$$y_1(x) = y_2(x)$$

b) $\underline{u \circ x = x \circ u = u}$

Tato vlastnost nám říká, že skládání dvou polynomů $u(x)$ a $v(x)$, kde $v(x) = x$, je v tomto případě komutativní a výsledný polynom je roven polynomu $u(x)$

Příklad 2.2:

Zadejme si polynomy $u(x)$ a $v(x)$, přičemž jeden z nich bude roven x.

$$u(x) = x^2 + 3$$
$$v(x) = x$$

Nejprve se pojďme podívat na situaci, kde řešíme skládání polynomu $u(x)$ s polynomem $v(x)$.

$$w_1(x) = (u \circ v)(x) = (x^2 + 3) \circ (x) = x^2 + 3$$

V druhém případě obraťme pořadí polynomů a skládejme polynom $v(x)$ s polynomem $u(x)$.

$$w_2(x) = (v \circ u)(x) = (x) \circ (x^2 + 3) = x^2 + 3$$

Můžeme pozorovat, že polynomy $w_1(x)$ a $w_2(x)$ se sobě rovnají a jsou taktéž rovny původnímu polynom $u(x)$.

c) $\underline{\text{Stupeň složeného polynomu } w = (u \circ v) \text{ je roven stupni součinu polynomů } u, v \text{ pro } u \neq 0 \text{ a } v \neq 0.}$

Tuto vlastnost si pojďme rovnou ilustrovat na příkladu.

Příklad 2.3

V tomto příkladu si ukažme na konkrétních polynomech, jak funguje výše uvedená vlastnost. Zadejme si tedy dva polynomy $u(x)$ a $v(x)$.

$$u(x) = x^2 + 3$$
$$v(x) = x^3 + 7$$

Polynom $w_1(x)$ vypočtěme tak, že využijeme operaci skládání polynomů.

$$w_1(x) = (u \circ v)(x) = (v^2 + 3) \circ (x^3 + 7) = (x^3 + 7)^2 + 3 = x^6 + 14x^3 + 52$$

Výsledný polynom $w_1(x)$ dosahuje stupně 6. Pojďme k druhému úkonu, čímž je získat součin polynomu $u(x)$ a $v(x)$.

$$w_2(x) = (x^2 + 3)(x^3 + 7) = x^6 + 3x^3 + 7x^2 + 21$$

V tomto případě opět pozorujeme, že stupeň polynomu $w_2(x)$ je také 6.

Další důležitou vlastností polynomů je, že jejich skládání není obecně komutativní. Tento fakt zapíšeme jako

$$u \circ v \neq v \circ u.$$

Příklad 2.4

Využijme předešlého příkladu a pracujme se stejnými polynomy $\boldsymbol{u(x)}$ a $\boldsymbol{v(x)}$. Již jsme taky zjistili, jak bude vypadat, který získáme složením $\boldsymbol{u(x)}$ a $\boldsymbol{v(x)}$.

$$w_1(x) = (u \circ v)(x) = x^6 + 14x^3 + 52$$

Polynom $w_2(x)$ získáme složením naopak polynomu $v(x)$ s polynomem $u(x)$.

$$w_2(x) = (u \circ v)(x) = (x^3 + 7) \circ (x^2 + 3) = ((x^2 + 3)^3 + 7)$$
$$= x^6 + 9x^4 + 27x^2 + 34$$

Po porovnání námi vypočítaných výsledků zjistím, že se polynomy $w_1(x)$ a $w_2(x)$ nerovnají a píšeme

$$w_1(x) \neq w_2(x).$$

Existují ovšem nějaké výjimky. Tyto případy jsou zmíněny v příkladu 2.6.

2.3 Rozložitelný polynom

Již dříve jsme si definovali, složený polynom. Víme tedy, že abychom mohli označit polynom $u(x)$ za složený, tak existují polynomy $v(x)$ a $w(x)$ a zároveň $u(x)$ je definováno jako složená funkce ve tvaru

$$u(x) = v(w(x)).$$

Tento proces jsme si ukázali v Příkladu 2.1.

Výraz $v(w(x))$ můžeme také označit jako rozklad polynomu $u(x)$ a polynomům $v(x)$ a $w(x)$ budeme říkat komponenty polynomu $u(x)$. Rozkladem polynomu rozumíme proces hledání $v(x)$ a $w(x)$.

Definice 2.1

Nechť polynomu u je z integrity $Q[x]$. Polynom u nazveme rozložitelným, jestliže existuje konečný počet polynomů $g_1(x), \dots, g_n(x)$, z nichž každý má stupeň větší než jedna, a takových, že

$$u = g_n \circ g_{n-1} \circ \dots \circ g_1, \quad n > 1. \tag{2.1}$$

Tato rovnice se nazývá rozkladem polynomu $u(x)$. Jednotlivé polynomy $g_i(x)$ se nazývají komponenty rozkladu. Jestliže rozklad polynomu u ve tvaru **(2.1)**

neexistuje, pak polynom $u(x)$ nazveme nerozložitelným. Jestliže dosáhneme toho, že jednotlivé polynomy $g_i(x)$ jsou nerozložitelné, představuje tvar **(2.1)** úplný rozklad polynomu $u(x)$. (Cohen 2003: 181)

Je důležité zdůraznit, že komponenty g_i z předchozí definice musí mít stupeň alespoň dva. Například polynom

$$w(x) = 4x^2 + 18x + 22 = (2x + 3)^2 + 3(2x + 3) + 4$$

není rozložitelný, jelikož vnitřní funkce, polynom $2x + 3$, je pouze lineární. Podmínkou na stupeň komponent v rozkladu v definici 2.1 zajišťujeme, že se budeme zabývat jen takovými rozklady, které jsou v jistém smyslu netriviální. (Cohen 2003: 182)

V následujícím příkladu si ukážeme případ, kdy se bude jednat o polynom rozložitelný.

Příklad 2.5:

Tento příklad je pouze ilustrační pro pochopení výše zmíněné problematiky. Cílem je rozložit zadaný polynom $\boldsymbol{u(x)}$. Zatím ještě nebylo řečeno, jakým principem toho dosáhneme, proto zde pouze naznačíme postup, ale podrobněji se mu budeme věnovat v dalších kapitolách této práce.

$$\begin{aligned} u(x) &= x^8 + 4x^7 + 10x^6 + 16x^5 + 29x^4 + 36x^3 + 40x^2 + 24x + 39 = \\ &= \left((x^2 + x)^2 + 2(x^2 + x)\right)^2 + 12\left((x^2 + x)^2 + 2(x^2 + x)\right) + 39 = \\ &= (x^2 + 12x + 39) \circ (x^2 + 2x) \circ (x^2 + x) \end{aligned}$$ (Cohen 2003: 182)

Zde můžeme vidět, že jednotlivé komponenty jsou polynomy stupně dva, a tudíž lze polynom $u(x)$ označit za rozložitelný.

Rozložení polynomu $u(x)$ není vždy jednoznačné. Může nastat případ, kdy jeho rozložení má více variant provedení, a zároveň v obou případech se jedná o jeho správné rozložení.

Příklad 2.6[3]

Na příkladu 2.6 si opět pouze ilustrativně ukážeme, jak mohou vypadat dva odlišné rozklady téhož zadaného polynomu $\boldsymbol{u(x)}$.

$$u(x) = x^6 + 2x^4 + x^2 + 1 = (x^3 + 2x^2 + x + 1) \circ (x^2)$$

Polynom $u(x)$ lze také rozložit takto

$$u(x) = x^6 + 2x^4 + x^2 + 1 = (x^3 - x^2 + 1) \circ (x^2 + 1).$$

Každý rozložitelný polynom u má nekonečně mnoho tvarů **(2.1)**. Tato skutečnost je založena na následující vlastnosti lineárních polynomů. Polynomy $f(x) = mx + b$ a $g(x) = \frac{x}{m} - \frac{b}{m}$, kde $m \neq 0$, v operaci skládání funkcí navzájem inverzními polynomy. Platí totiž

$$(f \circ g)(x) = (g \circ f)(x) = x.$$

Pokud má polynom u rozklad ve tvaru $u = v \circ w$, pak má podle věty 2.1 i jiný rozklad

$$u = (v \circ w) = (v \circ x \circ w) = (v \circ (f \circ g) \circ w) = (v \circ f) \circ (g \circ w). \quad \textbf{(2.2)}$$

Na polynomu $u(x) = x^6 + 2x^4 + x^2 + 1$ z příkladu 2.6 si ukažme, jak se lze od jednoho rozkladu dostat k rozkladu jinému.

$$\begin{aligned} u(x) &= x^6 + 2x^4 + x^2 + 1 = \\ &= (x^3 + 2x^2 + 1) \circ x^2 = \\ &= (x^3 + 2x^2 + 1) \circ x \circ x^2 = \\ &= (x^3 + 2x^2 + 1) \circ \big((x - 1) \circ (x + 1)\big) \circ x^2 = \\ &= \big((x^3 + 2x^2 + 1) \circ (x - 1)\big) \circ \big((x + 1) \circ x^2\big) = \\ &= (x^3 - x^2 + 1) \circ (x^2 + 1) \end{aligned} \quad \textbf{(2.3)}$$

[3] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 182

Pro výpočet rozkladu polynomu jsou důležité takové rozklady, v nichž má některá komponenta, tj. některý polynom v rozkladu číslo 0 jako nulový bod. V příkladu 2.6 je takovým polynomem komponenta x^2.

Věta 2.2[4]

Nechť u je rozložitelný polynom. Pak existuje jeho rozklad

$$u = v \circ w$$

kde polynom $w(o)$ je roven 0.

Důkaz věty 2.2[5]

Předpokládejme, že $u = v \circ w$. V případě, že $w(x) \neq 0$ zavedeme nové polynomy v' a w' tak, aby jejich složením byl opět polynom u a zároveň platilo $w'(0) = 0$.

$$v'(x) = v\big(x + w(0)\big),$$
$$w'(x) = w(x) - w(0).$$

Následně pak může zapsat, že $w'(0) = 0$ a

$$\begin{aligned}(v' \circ w')(x) &= v'\big(w'(x)\big) = \\ &= v'\big(w(x) - w(0)\big) = \\ &= v\big(w(x) - w(0) + w(0)\big) = \\ &= v\big(w(x)\big) = \\ &= u(x)\end{aligned}$$

Důkaz věty 2.2 si ukažme na příkladu.

[4] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 183
[5] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 183

Příklad 2.7

Mějme zadaný polynom $u(x)$

$$x^6 + 4x^4 + 4x^2 + 2x^3 + 4x + 2,$$

který lze rozložit na polynomy $v(x)$ a $w(x)$

$$v(x) = x^2 + 2x + 2$$
$$w(x) = x^3 + 2x.$$

Předpokládejme, že $w(x) \neq 0$ a zaveďme si nové polynomy zmiňované v důkazu věty 2.2 takové, aby platilo $w'(0) = 0$.

$$v'(x) = v\big(x + w(0)\big) = \big(x + w(0)\big)^2 + 2\big(x + w(0)\big) + 2$$
$$w'(x) = w(x) - w(0) = x^3 + 2x + w(0)$$

Vzhledem k tomu, že $w'(0) = 0$, můžeme psát, že

$$(v' \circ w')(x) = ((x+0)^2 + 2(x+0) + 2) \circ (x^3 + 2x + 0) =$$
$$= (x^2 + 2x + 2) \circ (x^3 + 2x) =$$
$$= x^6 + 4x^4 + 4x^2 + 2x^3 + 4x + 2 =$$
$$= u(x).$$

Na tomto příkladu tedy názorně vidíme, jak funguje v praxi důkaz věty 2.2.

3 Ritterova věta o polynomiálním rozkladu

Předpokládejme, že máme dva rozdílné rozklady polynomu u:

$$u = v_n \circ v_{n-1} \circ \ldots \circ v_1 = w_m \circ w_{m-1} \circ \ldots \circ w_1.$$

Ritterova věta o polynomiálním rozkladu popisuje, jaký vztah je mezi těmito dvěma různými podobami rozkladu. (Cohen 2003: 183)

Věta 3.1 (Ritterova věta)[6]

Mějme polynom $u(x)$ definovaný v oboru $Q[x]$.

- **a)** Každé dva úplné rozklady polynomu u se skládají ze stejného počtu jednotlivých komponent.
- **b)** Až na pořadí jsou stupně komponent v rozkladech tejné.

Důkaz Ritterovy věty o polynomiálním rozkladu je velice složitý. Jelikož náročnost tohoto důkazu je nad rámec matematické odbornosti této bakalářské práce, nebudeme jej tedy provádět. Pro čtenáře, který by se chtěl této problematice věnovat hlouběji, je možnost si důkaz nastudovat v literatuře.[7]

Na rozdíl od rozkladu polynomu na součin ireducibilních polynom, mohou dva úplné rozklady polynomu vypadat naprosto odlišně.

Příklad 3.1

1) $x^6 + 2x^4 + x^2 + 1 = (x^3 + 2x^2 + x + 1) \circ (x^2)$

2) $x^6 + 2x^4 + x^2 + 1 = (x^2 + 1) \circ (x^3 + x)$ **(3.1)**

Na tomto příkladu si můžeme všimnout, že ačkoliv je každý úplný rozklad jiný, tak plně splňuje všechny podmínky Ritterovy věty. V obou případech se rozklad skládá ze dvou komponent a zároveň stupeň jednoho je roven třem a druhé dvěma. Můžeme si všimnout, že se stupně jednotlivých komponent liší v jejich pořadí, jak již bylo uvedeno v bodu **b)** Ritterovy věty. (Cohen 2003: 184)

Tímto příkladem jsme ukázali, že způsob rozkladu, je závislý na využití různých lineárních polynomů a polynomů k nim inverzních. S tím jsme se již setkali ve výrazu **(2.2)**. Pokud bychom chtěli přejít z jednoho úplného rozkladu polynomu na druhý, můžeme toho docílit vložením lineárního polynomu a jeho inverzního

[6] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 183

[7] ENGSTROM, H. T. Polynomial Substitutions. *American Journal of Mathematics*. 1941, 63(2), 249-255

polynomu na to správné místo. Tento případ lze vidět ve výrazu **(2.3)**. Rozklady nazýváme ekvivalentními, když bude možné od jeho rozkladu přejít k jinému s využitím skládání s lineárním polynomem. To ovšem není vždy možné. Například rozklady v příkladu 3.1 nemůžeme nazvat ekvivalentními, jelikož nelze změnit pořadí stupňů v rozkladu vložením lineárního polynomu a k němu inverzního polynomu. (Cohen 2003: 184)

Mezi různými úplnými rozklady existují různé vztahy. Nebudeme se jim věnovat, protože to není nezbytně nutné pro vysvětlení a porozumění algoritmu rozkladu polynomů.

3.1 Racionální rozklady

Z rozkladu polynomů na součin ireducibilních polynomů jsme zvyklí, že rozložitelnost závisí na tělese, z něhož vybíráme koeficienty. Například $x^2 - 2$ je nad tělesem racionálních čísel nerozložitelný na součin, ale nad tělesem reálných čísel je rozložitelný, neboť

$$x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right).$$

Pro základy polynomů, jimiž se zabýváme, není rozložitelnost polynomu závislá na oboru koeficientů, jak dokládá následující věta.

Věta 3.2

Mějme polynom u definovaný v $Q[x]$. Rozkladem polynomu u je $u = v \circ w$. Pak polynom u má ekvivalentní rozklad s racionálními koeficienty. (Cohen 2003: 184)

Důkaz věty 3.2

Tento důkaz je složitý a pro účely vysvětlení problematiky rozkladu polynomů není stěžejní. Z těchto důvodů jej zde uvádět nebudu. Důkaz je dostupný v odborné literatuře[8], kde je podrobně popsán a vysvětlen.

[8] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 185

4 Algoritmus pro výpočet polynomiálního rozkladu

V této kapitole bakalářské práce se dostáváme k jejímu samotnému jádru a její hlavní části. Popíšeme si a podrobně vysvětlíme, jakým způsobem algoritmus funguje. Cílem algoritmu je najít kompletní rozklad polynomu $u(x)$, pokud existuje. Pro začátek se pustíme do rozkladu jednoduchého polynomu, jehož rozklad budou tvořit pouze dvě komponenty, $u = v \circ w$. V nějakých případech bude možné rozložit polynom v nebo polynom w.

Přepokládejme tedy, že máme daný rozklad $u = v \circ w$ a mějme

$$u(x) = u_m x^m + u_{m-1} x^{m-1} + \cdots + u_1 x + u_0,$$
$$v(x) = v_n x^n + v_{n-1} x^{n-1} + \cdots + vx + v_0.$$

Algoritmus pro polynomiální rozklad je založen na vlastnostech rozkladu, které jsou popsány v následující větě. (Cohen 2003: 188-189)

Věta 4.1[9]

Nechť polynom u je rozložitelný polynom definovaný v $Q[x]$. Pak existuje polynomiální rozklad $u = v \circ w$ takový, že polynom w splňuje následující vlastnosti.

a) $1 < st.[w_{(x)}] < st.[u_{(x)}]$.
b) $st.[w_{(x)}] \mid st.[u_{(x)}]$.
c) $w(0) = 0$.
d) $w(x) \mid (u(x) - u_0)$.

Důkaz Věty 4.1

Vlastnost a), která vyplývá z bodu c) věty 2.1, pouze ukazuje, že oba polynomy v a w musí být vyššího stupně než 1. Vlastnost b) je taktéž odvozena z bodu c) věty 2.1. Vlastnost c) je pouze upravené znění věty 2.2. Abychom mohli dokázat poslední vlastnost popsanou v bodu d), je nutné k tomu využít vlastnosti c) této věty 4.1,

$$u_0 = u(0) = v\big(w(0)\big) = v(0) = v(0).$$

[9] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 189

Díky tomu můžeme psát, že

$$u(x) - u_0 = u(x) - v_0 = v_n w(x)^n + v_{n-1} w(x)^{n-1} + \cdots + v_1 w(x).$$

A pokud rozdělíme každou část $w(x)$ na součet, můžeme také rozdělit $u(x) - u_0$. Vlastnost $w(0) = 0$ je dostatečnou podmínkou pro to, abychom zaručili, že platí

$$w(x) \mid (u(x) - u_0).$$

Tato vlastnost ovšem není nutnou podmínkou. Mohou existovat i jiní dělitelé $u(x) - u_0$, kteří nesplňují tuto podmínku, ale zároveň se díky nim lze dostat k rozkladu. I přesto, že nevíme, kteří dělitelé $u(x) - u_0$ nás dovedou k rozkladu, víme, že existuje rozklad $v(x) \circ w(x)$, ve kterém jedním z dělitelů je právě $w(x)$. (Cohen 2003: 189)

Věta 4.2, kterou v následujících řádkách uvedeme, pomůže ukázat způsob, jak dostat $v(x)$ a budeme moci vyzkoušet, zda existuje nějaký dělitel $w(x)$ výrazu $u(x) - u_0$, díky němuž získáme rozklad daného polynomu.

Věta 4.2

Předpokládejme, že polynom u definovaný v $Q[x]$ můžeme rozložit a jeho rozklad zapíšeme jako $u = v \circ w$. Pak polynom v je dán polynomiálním rozšířením polynomu u vhledem k polynomu w. Toto polynomiální rozšíření má koeficienty, ve kterých není přítomno x.

Důkaz Věty 4.2

Pokud $u = v \circ w$, pak dostaneme

$$u(x) = v_n w(x)^n + v_{n-1} w(x)^{n-1} + \cdots + v_1 w(x) + w_0,$$

kde koeficienty v_1 jsou racionálními čísly. Tento výraz ale pouze reprezentuje polynomiální rozšíření polynomu u vzhledem k polynomu w. Obecně platí, že koeficienty po polynomiálním rozšíření mohou být závislé na x. Ale jelikož v našem případě máme dáno, že všechny koeficienty v_i jsou racionální čísla. Z tohoto důvodu u nich x přítomno není. (Cohen 2003: 190)

Díky předchozím větám (Větě 4.1 a Větě 4.2) můžeme pokračovat dále v hledání způsobu, jak bezpečně najdeme postup, kterým se dostaneme až k rozkladu polynomu $u(x)$. Nejprve musíme najít skupinu různých polynomiálních dělitelů výrazu $u(x) - u_0$. Abychom určili tyto dělitele, je nutno nalézt všechny možné ireducibilní komponenty výrazu $u(x) - u_0$. Následně pak musíme správně zformulovat naše výsledky hledání všech komponent. Je důležité, aby se komponenty v našem výsledku neopakovaly. Také je nutno zmínit, že v našem případě při vynásobení polynomu w jakýmkoliv racionálním číslem c nezískám nového dělitele. Díky tomu víme, že je dostačující uvažovat pouze normované dělitele. Například si vezměme skupinu různých polynomiálních dělitelů výrazu $3(x-1)(x-2)^2$, kterou je následující množina.

$$S = \{x-1, x-2, (x-1)(x-2), (x-1)(x-2)^2\}.$$

Vzhledem k tomu, že všechny námi nalezení dělitelé splňují vlastnosti a), b) a d) z věty 4.1, se stávají možnými kandidáty na hledaný polynom $w(x)$. V dalším kroku můžeme o každém našem kandidátovi $w(x)$ z množiny S říci, že tvoří polynomiální rozšíření. Jestliže všechny koeficienty v_i neobsahují x, pak polynom v a polynom w dávají dohromady rozklad polynomu u. V opačném případě, kdy neexistuje žádný dělitel z množiny S, který by nás za této podmínky dovedl k rozšíření, označíme polynom u nerozložitelným. (Cohen 2003: 190)

Příklad 4.1[10]

Mějme zadaný polynom $\boldsymbol{u(x)}$ definovaný v $\boldsymbol{Q[x]}$. Cílem počítání bude získat úplný rozklad polynomu $\boldsymbol{u(x)}$.

$$u(x) = x^6 + 6x^4 + 3x^3 + 9x^2 + 9x + 5$$

[10] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 190

Z tohoto polynomu vyplývá, že $u(x) - u(0) = u(x) - 5$. Postupujeme dále a zjišťujeme, že komponenty polynomu $u(x) - 5$ mohou být kupříkladu

$$u(x) - 5 = x(x^2 + 3)(x^3 + 3x + 3).$$

Teď určeme množinu dělitelů tohoto polynomu.

$$S = \{x, x(x^2 + 3),\ x^3 + 3x + 3, x(x^3 + 3x + 3), (x^2 + 3)(x^3 + 3x + 3),$$
$$x(x^2 + 3)(x^3 + 3x + 3)\}.$$

Podařilo se nám určit všechny možné kandidáty na $w(x)$. Přesto pouze jediný dělitel splňuje všechny naše podmínky známé již z věty 4.1. Jedná se o dělitele $w(x) = (x^2 + 3)$. Dále tedy budeme pracovat pouze s tímto dělitelem. Abychom zjistili, zda nám tento výraz pomůže k dosažení výsledného rozkladu, musíme nalézt polynomiální rozšíření polynomu u vzhledem k polynomu w. To se nám povede pomocí počítačové funkce *Polynomial_expansion(u, w, x, t)* kupříkladu v programu Maple či programu Mathematica. Dostáváme výsledek

$$v(t) = t^2 + 3t + 5.$$

Ve chvíli, kdy víme, že všechny koeficienty $v(t)$ neobsahují x, dostáváme rozklad

$$u = v(x) \circ w(x) = (x^3 + 3x + 5) \circ (x^3 + 3x).$$

V naší množině dělitelů ovšem nalezneme dva jiné dělitele, kteří sice nesplňují všechny vlastnosti z Věty 4.1, ale splňují pouze tři z nich, a to vlastnosti a), b) a d). Jedná se o tyto dělitele:

$$x^2 + 3,\ x^3 + 3x + 3.$$

V případě, že je využijeme k hledání rozkladu, jejich polynomiální rozšíření bude vypadat následovně.

a) $w(x) = x^3 + 3x + 3, v(t) = t^2 - 3t + 5$

b) $w(x) = x^2 + 3, v(t) = t^3 - 3t^2 + 3xt + 5.$

Jelikož v případu a) je ve výrazu $v(t)$ absence x, získáme tím další podobu rozkladu původního polynomu v podobě

$$u = v(x) \circ w(x) = (x^2 - 3x + 5) \circ (x^3 + 3x + 3),$$

přestože $w(0) \neq 0$. V opačném případě, kdy v polynomu $v(t)$ bude obsaženo x, se nám nepodaří získat příslušné rozšíření s polynomem $w(x) = x^2 + 3$.

Příklad 4.2[11]

Nechť máme zadaný polynom $\boldsymbol{u(x)}$ definovaný v $\boldsymbol{Q[x]}$

$$u(x) = x^4 + x^3 + 3.$$

Naším úkolem je nalézt úplný rozklad polynomu $u(x)$. Pokračujme tedy ve výpočtu.

$$u(x) - u(0) = u(x) - 3$$
$$u(x) - 3 = x^3(x + 1)$$
$$S = \{x, x + 1, x(x + 1), x^2, x^2(x + 1), x^3, x^3(x + 1)\}$$

Jediní dělitelé, kteří splňují všechny podmínky Věty 4.1, jsou $w_1(x) = x(x + 1)$ a $w_2(x) = x^2$. Výsledkem polynomiální rozšíření polynomu u vzhledem k polynomu $w_1(x)$ je

$$v(t) = 3 - xt - t^2.$$

Výsledkem polynomiálního rozšíření polynomu u vzhledem k polynomu $w_2(x)$ je

$$v(t) = 3 + xt + t^2.$$

[11] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 191

Můžeme si povšimnout, že v obou případech je polynom $v(t)$ závislý na x. Z čehož dojdeme k závěru, že polynom $u(x)$ nelze rozložit v závislosti na námi zjištěných dělitelích. Tedy polynom $u(x)$ nazveme nerozložitelným.

4.1 Úplný rozklad polynomu

V této části kapitoly se budeme věnovat algoritmu, díky kterému dokážeme rozložit polynom úplně. Budeme tedy hledat takový rozklad, že jeho jednotlivé komponenty tvořené polynomy nižších stupňů budou již dále zaručeně nerozložitelné. Díky tomuto algoritmu najdeme posloupnost, která bude obsahovat dále již nerozložitelné polynomy $g_1, g_2, \dots, g_p$, kde pro p platí, že musí být větší než 1. Vyjádření tohoto vztahu bude pak vypadat následovně:

$$u = g_p \circ g_{p-1} \circ \dots \circ g_1, p > 1.$$

V případě, že se nám posloupnost nepodaří najít, označíme původní polynom za nerozložitelný. Je důležité zdůraznit, že našim hlavním cílem je dosáhnout rozkladu postupně. Hledáme pečlivě jednotlivou komponentu za komponentou, abychom žádnou z nich nevynechali. Níže si také ukážeme, že je možné uspořádat jednotlivé části rozkladu tak, aby každá z dílčích částí složení

$$g_i \circ g_{i-1} \circ \dots \circ g_1, 1 \leq i < p,$$

byla dělitelem $u - u_0$, kde komponenty $g_i$jsou získány pomocí polynomiálního rozšíření. Touto problematikou se budeme zabývat ve větě 4.3 a větě 4.4. Musíme zajistit, že každý polynom g_i je nerozložitelný díky aplikování podmínky minimálního stupně na dělitele výrazu $u - u_0$. To vše provedeme na základě věty 4.5. (Cohen 2003: 193)

Pojďme si tedy vysvětlit, jak nalezneme komponenty g_i (pro $i < p$) za předpokladu, že komponenty $g_1, g_2, \dots, g_{i-1}$ mohou být nalezeny. (Poslední komponent g_p vypočítáme jiným způsobem.) Pro zjednodušení zápisu mějme

$$u = g_p \circ g_{p-1} \circ \dots \circ g_{i+1} \circ g_i \circ g_{i-1} \circ \dots \circ g_1 = R \circ g_i \circ C,$$

kde

$$C = g_{i-1} \circ \dots \circ g_1$$

je prozatímní rozklad a

$$R = g_p \circ g_{p-1} \circ \dots \circ g_{i+1}$$

je rozklad, který nám zůstane poté, co nalezneme polynom g_i. V případě, že $i = 1$, zahrneme C do x. Jestliže $i < p$, pak můžeme předpokládat, že $st.[R_{(x)}] > 0$. (Cohen 2003: 193)

Věta 4.3[12]

Nechť je dán polynom u definovaný v $Q[x]$. Polynom u můžeme rozložit jako

$$u = R \circ g_i \circ C.$$

Pak pro $i < p$ je možno vybrat polynom g_i, který bude splňovat následující vlastnosti.

a) $st.[c_{(x)}] < st.[(g_i \circ C)_{(x)}] < st.[u_{(x)}]$.
b) $st.[(g_i \circ C)_{(x)}] \mid st.[u_{(x)}]$.
c) $(g_i \circ C)(0) = 0$.
d) $(g_i \circ C)(x) \mid (u(x) - u_0)$.

[12] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 193-194

Věta 4.3 nám naznačuje, že můžeme najít $g_i \circ C$ díky našemu zkoumání dělitelů výrazu $u(x) - u_0$. Musíme upozornit, že v tomto případě nezískáme polynom g_i přímo, tak jak tomu bylo u některých dělitelů výrazu $u(x) - u_0$. Místo toho získáme složený polynom $g_i \circ C$. Je to stejné jako to, co jsme prováděli v dvou krokovém algoritmu, protože ve chvíli, kdy počítáme g_1, tak C je zahrnuto do x a my získáme g_1 přímo. (Cohen 2003: 194)

Uveďme si další větu, která nám ukáže cestu k vypočítání polynomu g_iz $g_i \circ C$ a poskytne nám postup, díky kterému budeme moci říci, zda některý z námi zkoušených dělitelů výrazu $u - u_0$ přispěje k rozkladu polynomu.

Věta 4.4[13]

Předpokládejme, že polynom u definovaný v $Q[x]$ může být rozložen jako $R \circ g_i \circ C$.

a) Polynom R je nalezen díky výpočtu polynomiálního rozšíření polynomu u za podmínky $g_i \circ C$. Toto polynomiální rozšíření má koeficienty, které neobsahují proměnnou x.
b) Polynom g_i je nalezen díky výpočtu polynomiálního rozšíření polynomu $g_i \circ C$ za podmínek C. Toto polynomiální rozšíření má koeficienty, které neobsahují proměnou x.

Důkaz věty 4.4[14]

Nejprve pojďme dokázat první část Věty 4.4 a to bod a). Mějme:

$$r = r_s x^s + r_{s-1} x^{s-1} + \cdots + r_0.$$

Pozorujme, že

$$u = R \circ g_i \circ C = r_s\big(g_i(C)\big)^s + r_{s-1}\big(g_i(C)\big)^{s-1} + \cdots + r_0,$$

[13] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 194
[14] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 194-195

což je jediná možnost polynomiálního rozkladu polynomu u za podmínek $g_i(C)$. Jestliže koeficienty $r_s, r_{s-1}, \dots, r_0$ jsou racionální čísla, pak neobsahují proměnou x. Ačkoliv si můžeme povšimnout, že bod a) této věty je velice podobný větě 4.2 ve smyslu dvou krokového algoritmu, můžeme vidět, že R je pouze součástí rozkladu ve chvíli, kdy hledáme poslední komponent g_p. Pro ostatní komponenty g_i, kde $i < p$, je třeba pouze zkontrolovat, zda koeficienty R neobsahují proměnnou x.

V druhé části důkazu se věnujme bodu b). Mějme:

$$g_i(x) = a_p x^p + a_{p-1} x^{p-1} + \cdots + a_1 x + a_0.$$

Pozorujme, že

$$(g_i \circ C)(x) = a_p\big(C(x)\big)^p + a_{p-1}\big(C(x)\big)^{p-1} + \cdots + a_1 C(x) + a_0, \qquad \textbf{(4.1)}$$

což je jediná možnost polynomiálního rozkladu výrazu $g_i \circ C$ za podmínek C. Proto, aby polynom g_i byl komponentou, musí být splněna vlastnost, že jeho koeficienty musí být racionální čísla. Z tohoto důvodu neobsahují proměnnou x.

Díky následující větě získáme cestu k vhodnému získání $g_i \circ C$ takovou, aby polynom g_i byl nerozložitelný.

Věta 4.5[15]

Nechť je dán složený polynom $u = R \circ g_i \circ C$ a předpokládejme, že $g_i \circ C$ je dělitelem výrazu $u(x) - u_0$. Tento dělitel je dělitel s nejnižším stupněm, který splňuje podmínky uvedené ve Větě 4.3 a Větě 4.4. Pak lze říci, že g_i je nerozložitelný polynom.

[15] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 195

Důkaz věty 4.5[16]

Jestliže g_i je rozložitelný polynom, pak můžeme ukázat, že výraz $g_i \circ C$ nesplňuje podmínku nejnižšího stupně polynomu. Abychom to mohli náležitě dokázat, předpokládejme, že polynom g_i je rozložitelný jako

$$g_i = w \circ v,$$

kde $st.\left[v_{(x)}\right] > 1$ a $st.\left[w_{(x)}\right] > 1$. Z toho vyplývá, že $st.\left[w_{(x)}\right] < st.\left[g_{i_{(x)}}\right]$. Následně tento rozklad dosadíme do výrazu složeného polynomu u z věty 4.5. Tento tvar bude vypadat následovně:

$$u = R \circ g_i \circ C = R \circ w \circ v \circ C.$$

Aby se nám lépe s tímto výrazem pracovalo, umístíme do něj závorky a bude vypadat takto:

$$u = (R \circ w) \circ (v \circ C).$$

Díky vlastnostem, které jsme uvedli ve větě 4.1 (konkrétně vlastnosti $w(0) = 0$) můžeme předpokládat, že platí rovnost $(v \circ C)(0) = 0$. To by znamenalo, že výraz $(v \circ C)$ je dělitelem výrazu $u - u_0$. Jestliže pak platí, že

$$st.\left[(v \circ \mathrm{C})_{(x)}\right] = st.\left[v_{(x)}\right] \cdot \ st.\left[C_{(x)}\right] < st.\left[g_{i_{(x)}}\right] \cdot \ st.\left[C_{(x)}\right] = st.\left[(g_i \circ \mathrm{C})_{(x)}\right],$$

Tak výraz $g_i \circ C$ nesplňuje podmínku nejnižšího stupně polynomu. V tom případě můžeme označit polynom g_i jako nerozložitelný polynom.

[16] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 195

Pojďme si udělat malé shrnutí problematiky, se kterou jsme se právě seznámili. Věty, které jsme si zmínili v této čtvrté kapitole, nám ukazují způsob, kterým bezpečně nalezneme kompletní rozklad polynomu $u(x)$. Nejprve je nutné nalézt všechny dělitele výrazu

$u - u_0$. Abychom byli schopni najít polynom g_1, musíme zahrnout C do x a nalézt dělitele w výrazu $u - u_0$ s nejnižším stupněm. Tento dělitel w musí splňovat podmínky, které jsou uvedeny ve větě 4.3 a větě 4.4. V případě, že dojde k rovnosti $C = x$, rovnou dostáváme požadovaný výsledek a můžeme tvrdit, že $g_1 = w$, jako tomu bylo při dvou krokovém případě. Pokud zjistíme, že neexistuje žádný dělitel w, jsme nuceni polynom u označit jako nerozložitelný.

Abychom spočítali g_i $(1 < i < p)$, berme prozatím $C = g_{i-1} \circ \ldots \circ g_1$ jako rozklad a polynom w označme dělitelem výrazu $u - u_0$ nejnižšího stupně. Dělitel w splňuje podmínky zmíněné ve Větě 4.3 a Větě 4.4. V tomto případě je naší snahou nalézt polynom g_i pomocí polynomiálního rozšíření polynomu w v závislosti na C. Postup bude stejný, jako tomu bylo v rovnici **(4.1)**. Jestliže neexistují žádní dělitelé w, pak C obsahuje první z komponentů rozkladu, a to $p - 1$. Zbývá vypočítat poslední komponent, kterým je polynom g_p. Polynom g_p získáme díky výpočtu polynomiálního rozšíření polynomu u v závislosti na C. (Cohen 2003: 195-196)

Pojďme si opět ukázat vše na příkladu.

Příklad 4.3[17]

Mějme zadaný polynom

$$u(x) = x^8 + 4x^7 + 6x^6 + 4x^5 + 3x^4 + 4x^3 + 2x^2 + 1$$

Polynom $u(x) - 1$ rozložíme na jednotlivé dělitele a situace bude vypadat takto:

$$u(x) - 1 = x^2(x^4 + 2x^3 + x^2 + 2)(x + 1)^2.$$

[17] COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters), 196-197

Ačkoliv existuje celkem 17 různých dělitelů polynomu u, my díky požadavkům z věty 4.3 můžeme tento počet zúžit pouze na dělitelů 5. Těmito pěti důležitými děliteli budou

$$x^2,\ x^2+x,\ x^2+2x+1,\ x^4+2x^3+x^2,\ x^4+2x^3+x^2+2.$$

Abychom vypočítali polynom g_1, určeme si, že $C = x$ a berme v úvahu, že se mezi našimi pěti děliteli vyskytují tři, kteří jsou stupně 2. Proto tedy máme tři možnosti, jak vyjádřit výraz $g_1 \circ C$:

a) $g_1 \circ C = x^2$

$$R = t^4 + (4x+6)t^3 + (4x+3)t^2 + 2t + 1$$

b) $g_1 \circ C = x^2 + x$

$$R = t^4 + 2t^2 + 1$$

c) $g_1 \circ C = x^2 + 2x + 1$

$$R = t^4 + (2-4x)t^3 + (-1-4x)t^2 + (-2-4x)t + 1$$

Právě jsme si v jednotlivých případech vyjádřili R díky polynomiálnímu rozšíření v závislosti na parametru t, abychom jasně rozlišili koeficienty, které mohou být závislý na proměnné x. (V případě, že $C = x$, dostáváme $g_1 \circ C = g_1$ a v této situaci se nám nepodaří výpočtem získat polynomiální rozšíření výrazu $g_1 \circ C$.) Jestliže R ve výrazu b) je jediný polynom, který neobsahuje proměnou x, volíme pro další postup

$$g_1 \circ C = x^2 + x.$$

A v případě, že $C = x$, dostáváme

$$g_1 = x^2 + x.$$

Polynom g_1 jsme již nalezli, teď pojďme postupovat dále. Naší snahou bude najít polynom g_2. Určeme si, že $C = g_1$ a všimněme si, že mezi našimi pěti děliteli se nacházejí dva, které dosahují stupně 4. Lze tedy říci, že každý z těchto dvou dělitelů, je případným kandidátem na polynom $g_2 \circ C$. Opět proveďme polynomiální rozšíření pro každý z nich, jako tomu bylo ve větě 4.4. Máme tedy opět dvě podoby R.

a) $g_2 \circ C = x^4 + 2x^3 + x^2$, $g_2 = t^2$

$$R = t^2 + 2t + 1$$

b) $g_2 \circ C = x^4 + 2x^3 + x^2 + 2, g_2 = t^2 + 2$

$$R = t^2 - 2t + 1$$

V obou případech vidíme, že g_2 i R jsou bez proměnné x. Díky tomu víme, že oba tyto dělitelé nám přispějí k rozkladu polynomu u. Využijme situaci v bodu a) s použitím substituce $x = t$. Tím dostaneme $g_2 = x^2$. Pokud neexistují žádní další případní dělitelé, získáme lehce i polynom g_3. Jeho podobu zjistíme jednoduše. Aplikujeme stejný princip výpočtu jako v případě polynomu g_2. Za pomocí substituce $x = t$ v bodu b) dostáváme tedy

$$g_3 = x^2 + 2x + 1.$$

Žádní další dělitelé nepřipadají v úvahu, pokud chceme dosáhnout úplného polynomiálního rozkladu. Jsme tedy u konce a náš výsledek zapíšeme následovně:

$$u(x) = (x^2 + 2x + 1) \circ (x^2) \circ (x^2 + x).$$

5 Užití rozkladu polynomů

Rozklad polynomů může napomoci kupříkladu k výpočtu jejich hodnot v daném bodě. Máme více možností, jakým způsobem toho lze dosáhnout. Prvním z nich je pouhé dosazení do zadaného polynomu. Druhou možností je využít Hornerovo schéma. Vzhledem k jádru této bakalářské práce je nutno zmínit i třetí možnost, kterou je opět dosazení do polynomu, ale v tomto případě do polynomu v rozloženém tvaru. V následující části této kapitoly si uvedeme příklad konkrétního polynomu a vypočítáme jeho hodnotu v daném bodě všemi třemi způsoby, abychom si ukázali efektivnost jejich postupů.

5.1 Výpočet hodnot polynomů

Mějme zadaný polynom $u(x)$

$$u(x) = x^8 - 6x^4 + 11.$$

Naším cílem počítání, bude získat hodnotu tohoto polynomu v bodě 1. Výsledku můžeme dosáhnout díky různým metodám výpočtu. Pojďme si ukázat příklady těchto postupů.

5.1.1 Dosazení do zadaného polynomu v klasickém tvaru

Výpočet hodnoty polynomu dosazením do zadání je nejjednodušší varianta, kterou tento problém můžeme řešit, pokud příklad počítáme ručně, bez využití různých matematických programů.

$$u(x) = x^8 - 6x^4 + 11$$
$$u(1) = 1^8 - 6 \cdot 1^4 + 11 = \mathbf{6}$$

Díky lehkému výpočtu jsme zjistili, že hodnota zadaného polynomu v bodě 1 je rovna 6. Pojďme si ukázat druhou metodu výpočtu.

5.1.2 Využití Hornerova schématu

Hornerovo schéma jsme si již popsali v první kapitole této bakalářské práce. Princip, kterým se budeme snažit dosáhnout výsledku, tedy již známe. Pojďme si ukázat, že vytvořením Hornerova schématu nám vyjde stejný výsledek, jako v metodě dosazení do zadání.

	1	0	0	0	−6	0	0	0	11
1		1	1	1	1	−5	−5	−5	−5
	1	1	1	1	−5	−5	−5	−5	**6**

Po pečlivém vypočítání Hornerova schématu jsme zjistili, že hodnota zadaného polynomu v bodě 1 je rovna 6.

5.1.3 Dosazení do rozloženého polynomu

Pokud dostaneme zadaný rozložený polynom, je proces dosazování do tohoto výrazu velice snadný. Proto není nutné polynom skládáním přepisovat do základního tvaru. Postup bude vypadat následovně. Dosazováním a skládáním již konkrétních výsledných hodnot jednotlivých polynomů, dosáhneme jednoho číselného výsledku. Toto číslo pak nazveme hodnotou polynomu. Ukažme si tuto variantu dosazování na zadaném příkladu.

$$u(x) = x^8 - 6x^4 + 11$$
$$u(x) = (x^2 - 2x + 3) \circ (x^2 - 2) \circ (x^2)$$

Pokud chci zjistit hodnotu polynomu v bodě 1, musím ho dosadit nejprve do polynomu (x^2). Čímž dostanu příklad 1^2 a mohu říci, že hodnota tohoto polynomu je rovna jedné. Postupuji dále a získanou hodnotu dosadím do dalšího polynomu, kterým je $(x^2 - 2)$. Výpočtem $(1^2 - 2)$ dostanu výsledek (-1). Poslední částí našeho příkladu je dosazení hodnoty (-1) do posledního polynomu $(x^2 - 2x + 3)$. Jsme v závěru našeho snažení a na základě výpočtu $((-1)^2 - 2(-1) + 3) = (1 + 2 + 3) = \mathbf{6}$ můžeme vyřknout závěr. Hodnota zadaného polynomu v bodě 1 je rovna 6.

5.1.4 Zhodnocení metod

Všimněme si, že při využití všech třech způsobů určování hodnot polynomu jsme dosáhli stejného výsledku, ačkoliv jsme využili rozdílné postupy. V našem případě, kde se jednalo o polynom $u(x) = x^8 - 6x^4 + 11$, byl pro nás časově nejvýhodnější využít metodu dosazení do zadaného polynomu v klasickém tvaru.

V jiných případech tomu může být ale právě naopak a tato metoda se jednoduchou může pouze zdát. V těchto situacích je potřeba umět využít i jiné postupy řešení. Když bude zadán složitý polynom vysokého stupně, tak se snadno při dosazování do rozloženého polynomu může stát chyba. Počítat kupříkladu vysoké mocniny čísla 8 může být velice náročné. Z tohoto důvodu doporučuji využít metodu jinou. Když se zamyslíme nad využitím Hornerova schématu, dojde nám, že se jedná o postup rychlý a krásně graficky zpracovatelný. Těžké chvíle při výpočtu nám ale nastanou tehdy, kdy polynom bude mít vysoký stupeň a bude obsahovat mnoho komponent. Znázornit Hornerovo schéma pro výpočet hodnoty polynomu vysokého stupně, kterým je

například $(x^{15} + x^{14} + 7x^{13} - 4x^{11} - 3x^{10} + 2x^8 - x^7 - 5x^6 + x^4 - x^3 + 3)$, bude velice zdlouhavé a náročné. Z těchto důvodů bych doporučila využívat poslední metodu, kterou je dosazení bodu do polynomu v rozloženém tvaru. Pokud máme polynom zadaný v klasické rozložené formě, musíme nejprve jeho rozklad získat. Tento rozklad získáme pomocí algoritmu pro úplný rozklad polynomu, který jsme si společně popsali již v předešlých kapitolách. Druhou možností, jak rozklad získat, je využití matematických programů, které tuto funkci nabízí. Mezi programy, které lze pro tyto výpočty využít patří Maple, Matematica či Maxima. Pokud bychom si nechtěli programy stahovat do počítače, lze využít jinou alternativu, kterou je Wolframaplha, v kterém je snadné počítat příklady různého rázu včetně rozkladu polynomů. Pro využití tohoto programu nám stačí pouze navštívit jeho stránky a pracovat v něm on-line bez stahování.

5.2 Příklady

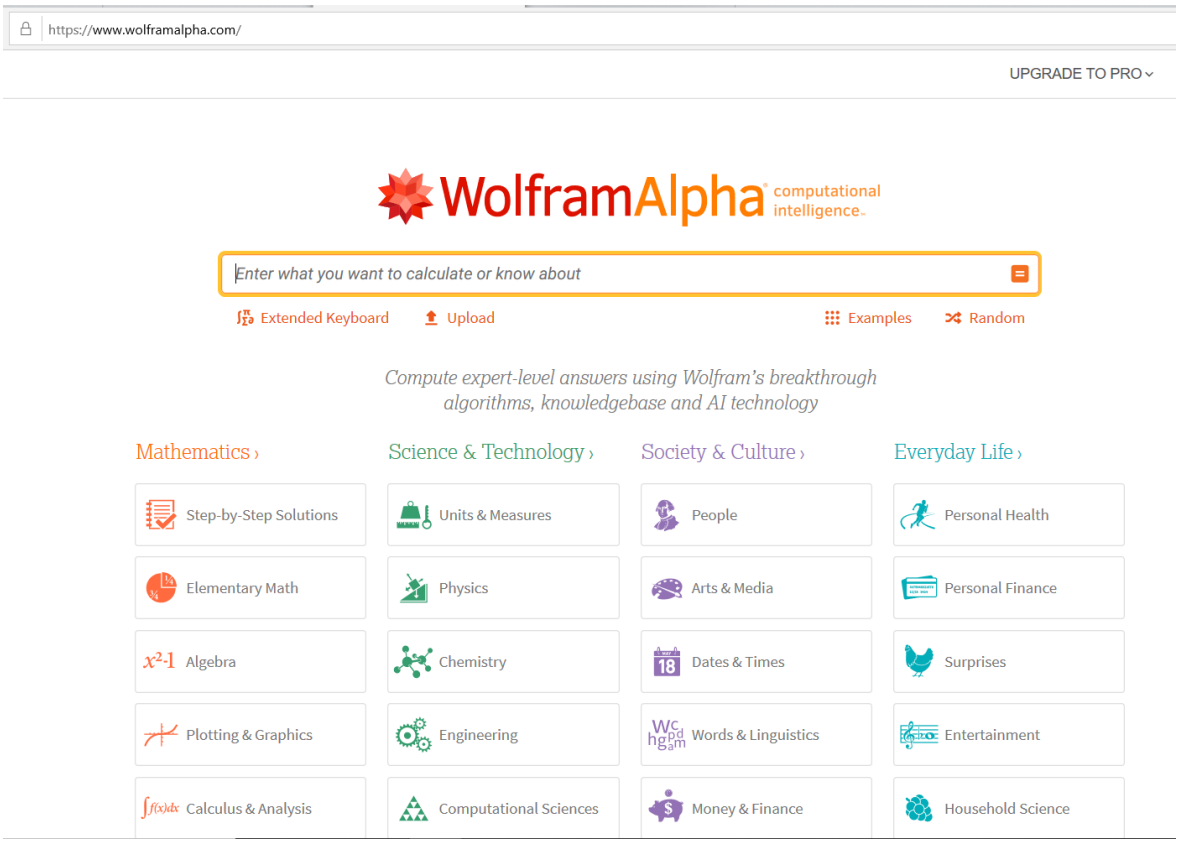
Tato podkapitola nám nabídne ukázku příkladů, kde se budeme snažit vypočítat hodnotu polynomu v daném bodě. Pro dosažení výsledku budeme využívat různé metody, které jsme si uvedli v kapitole 5.1.

Příklad 5.1

Nechť máme zadaný polynom ve tvaru

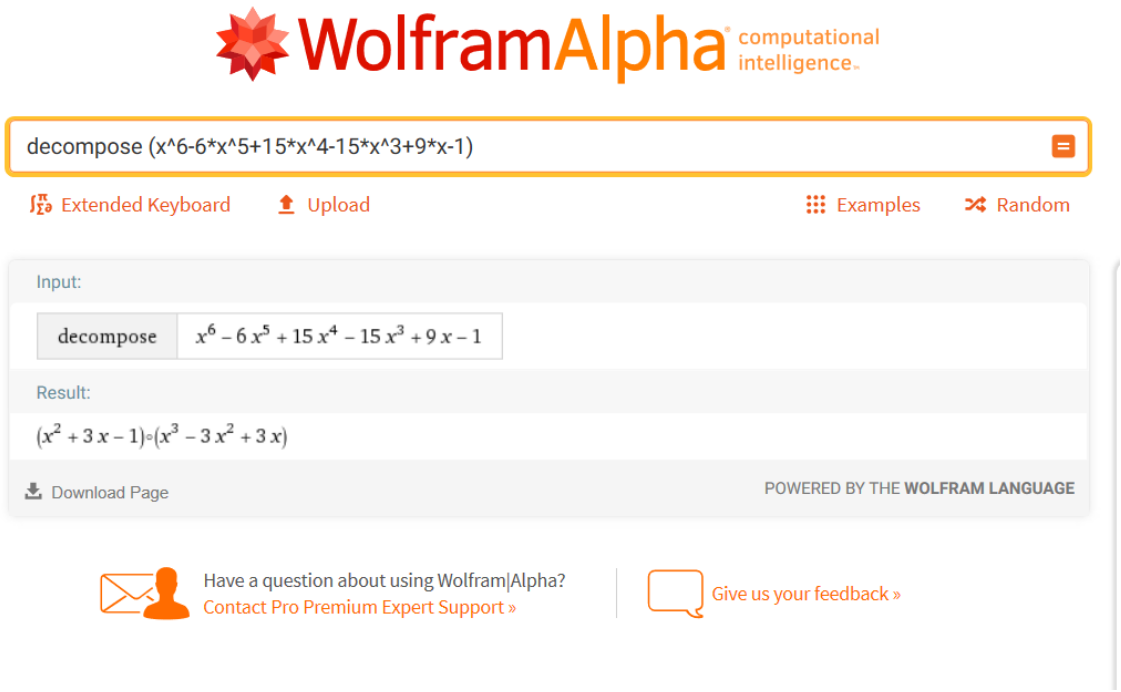
$$u(x) = x^6 - 6x^5 + 15x^4 - 15x^3 + 9x - 1.$$

Naším úkolem bude určit hodnotu polynomu u v bodě 7. Pro tento příklad využiji metodu dosazení do rozloženého tvaru polynomu u. Ukážeme si, jak lze jednoduše získat tento rozklad pomocí programu WolframAlpha. Postup je velice snadný. Poté, co program na internetu vyhledáme, přejdeme na jeho domovskou stránku viz. obrázek 1.



Obrázek 1 - Wolframalpha - domovská stránka

Na této stránce si můžeme všimnout, že program nabízí více funkcí v přírodovědných oborech. Nás ovšem budou zajímat pouze funkce matematické. Abychom nemuseli hledat konkrétní funkci pro rozklad polynomu, tak si řekneme, co zadáme do příkazového okna. Pro nás je důležitý příkaz *„decompose“*. Za tento příkaz napíšeme do závorek příslušný polynom a po stisknutí klávesy „Enter“ na klávesnici nám program tento polynom rozloží viz. obrázek 2. V případě, že polynom je nerozložitelný, program nám to sdělí.



Obrázek 2 - Wolframalpha - rozklad

V obrázku 2 můžeme vidět, že námi zadaný polynom je rozložitelný a jeho rozklad vypadá následovně:

$$u(x) = (x^2 + 3x - 1) \circ (x^3 - 3x^2 + 3x)$$

Do tohoto rozkladu dosadíme zvolený bod 7.

$$u(7) = 47\,739$$

Dosáhli jsme výsledku a můžeme tedy říci, že hodnota zadaného polynomu $u(x) = x^6 - 6x^5 + 15x^4 - 15x^3 + 9x - 1$ je v bodě 7 rovna číslu 47 739. Pro kontrolu, dosaďme číslo 7 do zadaného polynomu v původním tvaru.

$$u(7) = 7^6 - 6 \cdot 7^5 + 15 \cdot 7^4 - 15 \cdot 7^3 + 9 \cdot 7 - 1 = 47\,739$$

Výsledná čísla se u obou dvou postupů rovnají, a tudíž řekneme, že se jedná o správné výsledky.

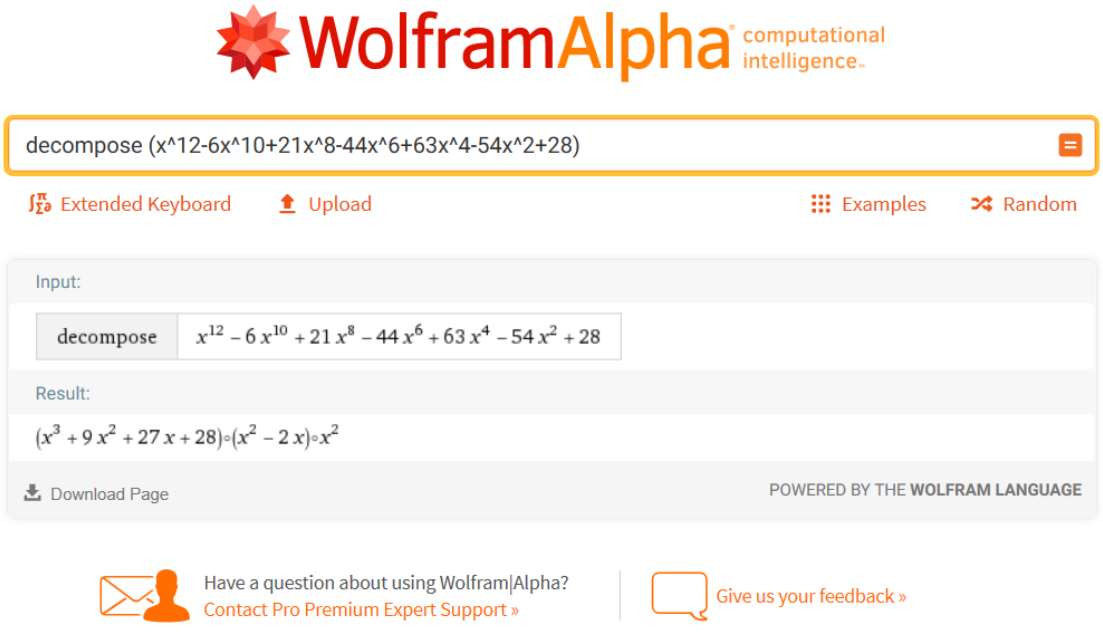
Kdybychom chtěli využít Hornerovo schéma, bylo by to v tomto případě složité a zdlouhavé, jelikož zde počítáme s vysokými koeficienty a snadno bychom mohli udělat chybu při výpočtu.

Příklad 5.2

Mějme zadaný polynom

$$u(x) = x^{12} - 6x^{10} + 21x^8 - 44x^6 + 63x^4 - 54x^2 + 28$$

Rozložme polynom $u(x)$ a vypočtěme jeho hodnotu v bodě 2. V tomto případě využít Hornerovo schéma opět není vhodné, jelikož primárním úkolem je rozložit polynom $u(x)$, k čemuž nám schéma nepomůže. Polynom $u(x)$ rozložíme pomocí programu Wolframalpha a následně do rozloženého tvaru polynomu $u(x)$ dosadíme bod 2. Pro kontrolu výsledků, budeme postupovat jako v příkladu 5.1 a dosadíme bod 2 i do složeného tvaru polynomu $u(x)$.



Obrázek 3 - Wolframaplha - rozkald 2

Na obrázku 3 vidíme, že rozkladem zadaného polynomu $u(x)$ je

$$u(x) = (x^3 + 9x^2 + 27x + 28) \circ (x^2 - 2x) \circ x^2.$$

Do tohoto tvaru dosadím bod 2, čímž získám následující výpočet hodnoty polynomu $u(x)$ v daném bodě.

$$u(2) = 512 + 576 + 216 + 28 = 1\,332$$

Pro již zmiňovanou kontrolu dosadíme bod 2 do rozloženého tvaru polynomu $u\,(x)$.

$$u(2) = 2^{12} - 6 \cdot 2^{10} + 21 \cdot 2^8 - 44 \cdot 2^6 + 63 \cdot 2^4 - 54 \cdot 2^2 + 28 = 1\,332$$

Opět vidíme, že jsme dosáhli shodných výpočtů.

Příklad 5.3

Mějme zadaný polynom

$$u(x) = x^6 - 2x^5 + x^3 + 4x^2 + 3x - 2$$

Vypočítejme hodnotu polynomu v bodě (-2). Pro tento výpočet využijme metodu dosazení do zadání v klasickém tvaru polynomu a následně výsledek ověřme vytvořením Hornerova schématu.

$$u(-2) = (-2)^6 - 2 \cdot (-2)^5 + (-2)^3 + 4 \cdot (-2)^2 + 3 \cdot (-2) - 2$$
$$= 64 + 64 - 8 + 16 - 6 - 2 = 128$$

Po dosazení jsme dospěli k výsledku, že hodnota zadaného polynomu $u(x)$ v bodě (-2) je rovna 128. Pojďme vytvořit Hornerovo schéma a výsledky postupů porovnejme.

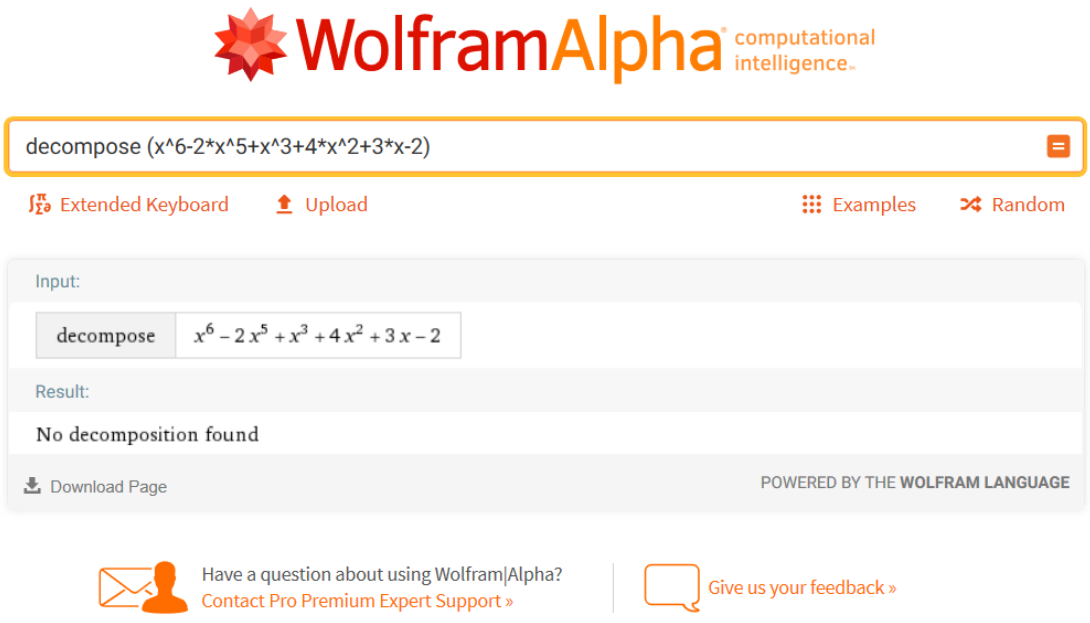
	1	−2	0	1	4	3	−2
-2		1	−4	8	−15	34	−65
	1	−4	8	−15	34	−65	**128**

Výsledky v obou případech se rovnají číslu 128. Lze tedy tvrdit, že jsme postupovali správně a hodnota polynomu $u(x) = x^6 - 2x^5 + x^3 + 4x^2 + 3x - 2$ v bodě (-2) je rovna 128.

Příklad 5.4

Vezměme si polynom z příkladu 5.3 a rozložme ho pomocí programu WolframAlpha a Maxima.

Zadejme tedy příkaz k rozložení polynomu $u(x) = x^6 - 2x^5 + x^3 + 4x^2 + 3x - 2$ do programu WolframAlpha (obrázek 3).



Obrázek 4 - Wolframalpha - nerozložitelný polynom

Z obrázku 4 je patrné, že program nenašel vhodný rozklad polynomu $u(x)$, tudíž si dovolíme tvrdit, že zadaný polynom $u(x)$ je nerozložitelný.

5.3 Řešení rovnic vyjádřené v radikálech

Na začátku této kapitoly se budeme zabývat jednoduchými algebraickými rovnicemi, které nazýváme binomické. V následující části si ukážeme, jak nám rozklad polynomů pomůže k nalezení kořenů vyjádřených v radikálech.

5.3.1 Binomické rovnice

Pojďme si nejprve definovat, co to binomická rovnice je a některé důležité pojmy, které s touto problematikou souvisí.

Definice 5.1[18]

Binomická rovnice je rovnice ve tvaru

$$ax^n + b = 0,$$

kde a, b jsou libovolná čísla a předpokládáme, že $a, b \neq 0$ a zároveň $n \in N$.

Jakoukoliv binomickou rovnici lze převést do tvaru

$$x^n + \frac{b}{a} = 0.$$

Existují speciální případy binomických rovnic, kterými jsou:

a) $n = 1$

Rovnice má tvar $ax + b = 0$ a jedná se v tomto případě o lineární rovnici.

b) $n = 2$

Rovnice má tvar $ax^2 + b = 0$ a jedná se v tomto případě o kvadratickou rovnici.

Pro snadnější postup při výpočtu si zavedeme substituci $\frac{b}{a} = c$. Poté tvar binomické rovnice bude vypadat následovně

$$x^n + c = 0.$$

Definice 5.2

[18] MATEMATIKA.CZ [nedatováno]. *Binomické rovnice* (https://matematika.cz/binomicke-rovnice, 27. 6. 2020).

Nechť je dána binomická rovnice ve tvaru

$$x^n + c = 0,$$

kde c je racionální číslo a $n \in N$ a n-tá mocnina má n kořenů. Nechť jest T_k nějaké těleso a číslo c nikoliv n-tá mocnina z toho tělesa, potom číslo $\Theta = \sqrt[n]{a}$ nazveme radikálem n-tého stupně nad T_k. (Schwarz 1940: 74)

Příklad 5.5 [19]

Mějme zadanou rovnici $x^3 - 7 = 0$. Naším úkolem je určit kořeny této rovnice vyjádřené v radikálech.

Kořeny rovnice $x^3 - 7 = 0$ jsou

$$x_1 = \sqrt[3]{7}, x_2 = \varepsilon \cdot \sqrt[3]{7}, x_3 = \varepsilon^2 \cdot \sqrt[3]{7}.$$

Zvolme $\Theta = \sqrt[3]{7}$. Potom množina kořenů vyjádřených v radikálech se skládá ze všech čísel tvaru

$$\alpha = d_0 + d_1 \cdot \sqrt[3]{7} + d_2 \cdot (\sqrt[3]{7})^2,$$

kde čísla d_0, d_1, d_2 jsou libovolná racionální čísla. V případě, že si zvolíme jiný kořen, kupříkladu $x_3 = \varepsilon \cdot \sqrt[3]{7}$, budou tvar čísel z množiny kořenů vyjádřených v radikálech vypadat takto:

$$\alpha = d_0 + d_1 \cdot \varepsilon \cdot \sqrt[3]{7} + d_2 \cdot \varepsilon^2 \cdot (\sqrt[3]{7})^2,$$

přičemž čísla d_0, d_1, d_2 jsou opět libovolná racionální čísla.

[19] SCHWARZ, Š. (1940). *O Rovnicích: Neřešitelnost rovnic vyššího než čtvrtého stupně*. (Praha: Jednota českých matematiků a fysiků v Praze), 74-75

Rovnice $x^2 - c = 0$, kde číslo c je racionální, ale nikoliv čtverec není v množině reálných čísel řešitelná. V tělese $Q(\sqrt{c})$, které dostáváme z Q adjunkcí $\sqrt{c}$, však řešitelná je. Můžeme psát, že $x_{1,2} = \pm\sqrt{c}$ a říkáme, že kořen rovnice je vyjádřen radikálem. O rovnici $x^2 - c = 0$ tvrdíme, že je řešitelná pomocí radikálů. Libovolné číslo můžeme vyjádřit radikály pouze za podmínky, že je obsaženo v tělese, které vzniklo z tělesa Q konečným počtem adjunkcí radikálů vždy z tělesa předchozího. (Schwarz 1940: 75)

Důležité je také připomenout, že binomická rovnice má n kořenů. Rovnice stupně 2., 3. a 4. stupně lze vždy řešit pomocí radikálů. Pro rovnice 5. a vyššího stupně nelze nalézt obecnou rovnici, díky které by byla v radikálech řešitelná. Ovšem to neznamená, že ji v radikálech řešit nelze. Existují speciální rovnice (např. reciproké, pro dělení kruhu) i stupňů vyšších než čtvrtého, které pomocí radikálů řešit umíme. Rovnice, které lze řešit pomocí radikálů nazýváme metacyklické. (Schwarz 1940: 76)

5.3.2 Kořeny rovnic vyjádřené v radikálech pomocí rozkladu polynomů

Rozklad polynomů nám umožní snadnější výpočet kořenů rovnice, které budeme chtít vyjádřit v radikálech. Vyjádřit kořeny rovnice v radikálech dokážeme dokonce i u některých ireducibilních polynomů. Většinou se tento způsob vyjadřování kořenů rovnic využívá v různých matematických počítačových programech.

Příklad 5.6[20]

Mějme zadaný polynom $u(x)$

$$u(x) = x^6 - 6x^5 + 15x^4 - 20x^3 + 15x^2 - 6x + 1.$$

Polynom $u(x)$ rozložíme následovně:

$$u(x) = (x^3 - 2) \circ (x^2 - 2x + 1).$$

[20] WIKIPEDIA: (2020). *Polynomial Decomposition* (https://en.wikipedia.org/wiki/Polynomial_decomposition, 24. 6. 2020)

Kořeny polynomu $u(x)$, který je ireducibilní pak jsou tyto radikály

$$x_{1,2} = 1 \pm 2^{\frac{1}{6}},$$
$$x_{3,4} = 1 \pm \frac{\sqrt{-1+\sqrt{3}i}}{2^{\frac{1}{3}}},$$
$$x_{5,6} = 1 \pm \frac{\sqrt{-1-\sqrt{3}i}}{2^{\frac{1}{3}}}.$$

Příklad 5.7[21]

Na tomto příkladu si ukážeme, jak by vypadaly kořeny vyjádřené v radikálech, když bychom využili rozložený tvar polynomu a zároveň když využijeme rozložený tvar polynomu.

Mějme zdaný polynom $u(x)$

$$u(x) = x^4 - 8x^3 + 18x^2 - 8x + 2.$$

Polynom $u(x)$ rozložíme:

$$u(x) = (x^2 + 1) \circ (x^2 - 4x + 1).$$

Rozložený tvar polynomu $u(x)$ nám nabídne kořeny

$$x_{1,2} = 2 \pm \sqrt{3 - i}$$
$$x_{3,4} = 2 \pm \sqrt{3 + i}.$$

Pokud bychom polynom $u(x)$ ponechaly v původním rozloženém tvaru a aplikovali na výpočet kořenů vzorec pro jejich výpočet, dostali bychom stejný výsledek, ovšem ve tvaru, který je velmi složitý na porozumění.

[21]WIKIPEDIA: (2020). *Polynomial Decomposition*
(https://en.wikipedia.org/wiki/Polynomial_decomposition, 24. 6. 2020)

$$2-\frac{\sqrt{\dfrac{9\left(\dfrac{8\sqrt{10i}}{3^{\frac{3}{2}}}+72\right)^{\frac{2}{3}}+36\left(\dfrac{8\sqrt{10i}}{3^{\frac{3}{2}}}+72\right)^{\frac{1}{3}}+156}{\left(\dfrac{8\sqrt{10i}}{3^{\frac{3}{2}}}+72\right)^{\frac{1}{3}}}}}{6}-\frac{\sqrt{-\left(\dfrac{8\sqrt{10i}}{3^{\frac{3}{2}}}+72\right)^{\frac{1}{3}}-\dfrac{52}{3\left(\dfrac{8\sqrt{10i}}{3^{\frac{3}{2}}}+72\right)^{\frac{1}{3}}}+8}}{2}$$

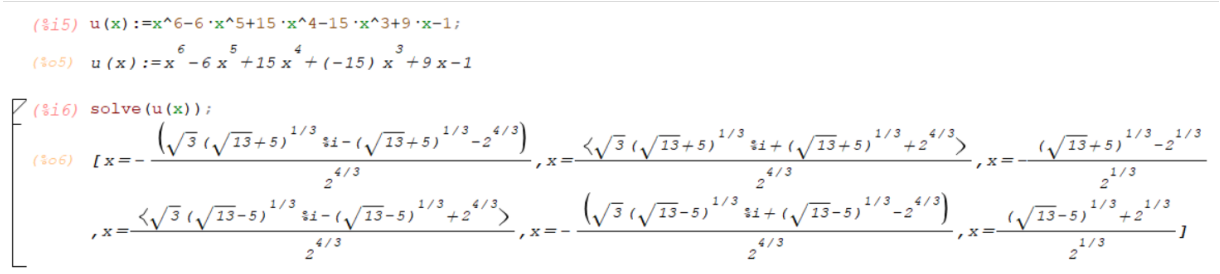
Na tomto příkladě jsme viděli, jak je v některých situacích důležité umět správně využít rozklad polynomů. Mnoho výpočtů se nám tímto způsobem může zjednodušit. Pro výpočet kořenů v radikálech můžeme využít například program Maxima, kde pomocí funkce *„solve“* nám program kořeny ukáže (viz. obrázek 4).

Příklad 5.8

V programu Maxima vypočtěme kořeny zadaného polynomu $u(x)$.

$$u(x) = x^6 - 6x^5 + 15x^4 - 15x^3 + 9x - 1$$

Nejprve si v programu Maxima musíme zadat polynom $u(x)$. Následně pak pomocí již zmiňovaného příkazu *„solve“* získáme výsledek příkladu 5.8. Výpočet programu vidíme v obrázku 5.



Obrázek 5 - Maxima - kořeny

Závěr

Cílem této práce bylo čtenáře seznámit s problematikou rozkladu polynomů, ukázat algoritmus, díky němuž rozkladu polynomů dosáhneme a uvést příklady, při nichž rozklad využíváme.

V první kapitole této práce si čtenář připomene základní pojmy a principy, které se týkají rozkladu mnohočlenů a matematické operace skládání funkcí. V následující části práce jsou definovány pojmy týkající se polynomů. Jsou zde uvedené jednotlivé příklady, které nám ilustrují zmiňované vlastnosti polynomů či matematické operace s polynomy, které budou v dalších kapitolách stěžejní, pro pochopení problematiky. Mezi ně patří zejména rozklad polynomů. Tato tématika je jádrem této práce, tudíž třetí a čtvrtá kapitola je věnována právě rozkladu polynomů. Třetí kapitola konkrétně nabízí čtenáři seznámení s Ritterovou větou o polynomiálním rozkladu. Ve čtvrté kapitole je uveden algoritmus, díky kterému dosáhneme úplného rozkladu polynomu. Tato část práce čtenáři ukáže teoretické pozadí problematiky rozkladu polynomů. Poslední kapitola je věnována výpočtu hodnot polynomů a praktickému využití rozkladu polynomů. Jsou zde zmíněny tři metody výpočtu hodnot polynomu, jimiž jsou „dosazení do zadaného polynomu v klasickém tvaru“, „Hornerovo schéma“, „dosazení do rozloženého polynomu“. Na konkrétních příkladech je ukázána vhodnost volby jedné z metod v závislosti na podobě zadaného příkladu. V závěru práce je zmíněna problematika řešení rovnic, které je vyjádřeno v radikálech.

Resumé

Tato bakalářská práce se zabývá rozkladem polynomů. Čtenáři je nejprve připomenuta problematika konkrétních operací s funkcemi. Následně jsou vysvětleny pojmy týkající se polynomů, které jsou v práci využívány. Hlavní částí je vyřčení a objasnění Ritterovy věty o polynomiálním rozkladu a vysvětlení algoritmu, kterým dosáhneme kompletního rozkladu polynomů. V práci jsou uvedeny příklady počítání hodnot polynomů, využití rozkladu polynomů a řešení rovnic vyjádřené v radikálech.

Resume

This bachelor thesis is concerned with polynomial decomposition. At the first, the readers could remember some mathematical problems relating to functions. Next, it is explained terms relating to polynomials, which are used in the next parts. Explaining Ritter´s theorem about polynomial decomposition and explaining the complete decomposition algorithm of polynomials are the main parts of this bachelor thesis. In the end, readers could see examples of counting value of the polynomial, using polynomial decomposition and solutions of equations expressed in radicals.

Zdroje

COHEN, J. S. (2003). *Computer Algebra and Symbolic Compputation: Mathematical Methods* (Natick: AK Peters).

BRABEC, S., MARTAN, F., ROZENSKÝ, Z. (1989). *Matematická analýza 1* (Praha: SNTL – Nakladatelství technické literatury)

ENGSTROM, H. T. Polynomial Substitutions. *American Journal of Mathematics*. 1941, 63(2), 249-255

OLŠÁK P. (2012). *BI- Lineární algebra* [přednáška] (Praha: České vysoké učení technické). (http://petr.olsak.net/bilin/polynomy4.pdf, 13. 4. 2020)

WIKIPEDIA: (2020). *Polynomial Decomposition* (https://en.wikipedia.org/wiki/Polynomial_decomposition, 24. 6. 2020)

SCHWARZ, Š. (1940). *O Rovnicích: Neřešitelnost rovnic vyššího než čtvrtého stupně*. (Praha: Jednota českých matematiků a fysiků v Praze).

MATEMATIKA.CZ [nedatováno]. *Binomické rovnice* (https://matematika.cz/binomicke-rovnice, 27. 6. 2020).

MAŘÍK, R. [nedatováno]. Hornerovo schéma. *Mendelova univerzita v Brně: Home Page of Robert Mařík*. (http://user.mendelu.cz/marik/wiki/pdf/algrce.pdf , 14. 6. 2020).

PAVLICOVÁ, V. (2010). *Webová aplikace pro výuku základních poznatků z matematiky na střední škole* [bakalářská práce] (Praha: Univerzita Karlova v Praze).

Seznam obrázků