UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

SYMETRICKÉ POLYNÓMY A ROZKLAD POLYNÓMU NA IREDUCIBILNÉ ČINITELE

BAKALÁRSKA PRÁCA

2014 BYSTRÍK KUBALA

UNIVERZITA KOMENSKÉHO V BRATISLAVE
FAKULTA MATEMATIKY, FYZIKY A INFORMATIKY

SYMETRICKÉ POLYNÓMY A ROZKLAD POLYNÓMU NA IREDUCIBILNÉ ČINITELE

BAKALÁRSKA PRÁCA

Študijný program:	Ekonomická a finančná matematika
Študijný odbor:	1114 Aplikovaná matematika
Školiace pracovisko:	Katedra aplikovanej matematiky a štatistiky
Vedúci práce:	RNDr. Dušan Krajčovič, CSc.

Bratislava 2014 **BYSTRÍK KUBALA**

Univerzita Komenského v Bratislave
Fakulta matematiky, fyziky a informatiky

ZADANIE ZÁVEREČNEJ PRÁCE

Meno a priezvisko študenta: Bystrík Kubala
Študijný program: ekonomická a finančná matematika (Jednoodborové štúdium, bakalársky I. st., denná forma)
Študijný odbor: 9.1.9. aplikovaná matematika
Typ záverečnej práce: bakalárska
Jazyk záverečnej práce: slovenský

Názov: Symetrické polynómy a rozklad polynómu na ireducibilné činitele / *Symetric polynomials and polynomial factorization*

Cieľ: Využitie získaných teoretických poznatkov pri riešení polynomických rovníc

Vedúci: RNDr. Dušan Krajčovič, CSc.
Katedra: FMFI.KAMŠ - Katedra aplikovanej matematiky a štatistiky
Vedúci katedry: prof. RNDr. Daniel Ševčovič, CSc.

Dátum zadania: 18.10.2013

Dátum schválenia: 14.11.2013

doc. RNDr. Margaréta Halická, CSc.
garant študijného programu

študent

vedúci práce

Abstrakt

KUBALA, Bystrík: Symetrické polynómy a rozklad polynómu na ireducibilné činitele [Bakalárska práca] - Univerzita Komenského v Bratislave. Fakulta matematiky, fyziky a informatiky. Katedra aplikovanej matematiky a štatistiky.- Vedúci bakalárskej práce: RNDr. Dušan Krajčovič, CSc. - Bratislava: FMFI UK, 2014, 46 strán.

Táto práca sa zaoberá symetrickými polynómami a rozkladom polynómu na ireducibilné činitele. Rozoberá základné algebraické štruktúry, vlastnosti polynómov a symetrických polynómov. Poskytuje základný prehľad aplikácii symetrických polynómov v Newtonových polynómoch, Schurovom polynóme, diskriminante a rezultante. Taktiež poukazuje na súvis polynómov so symetrickými polynómami pri hľadaní ireducibilných činiteľov polynómov.

Kľúčové slová: ireducibilný činiteľ, polynóm, symetrický polynóm, diskriminant, rezultant

Abstract

KUBALA, Bystrík: Symmetric polynomials and polynomial factorization [Bachelor thesis] - Comenius University in Bratislava. Faculty of Mathematics, Physics and Informatics. Department of Applied Mathematics and Statistics.- Supervisor: RNDr. Dušan Krajčovič, CSc. - Bratislava: FMFI UK, 2014, 46 p.

This thesis deals with symmetric polynomials and polynomial factorization to irreducible factors. It analyses the fundamental algebraic structure, the properties of polynomial and symmetric polynomials. It provides the basic overview how is symmetric polynomials applicable in Newtons polynomials, Schur polynomial, discriminant and resultant. The thesis also point to the relation of polynomials with symmetric polynomials to search irreducible factors.

Keywords: irreducible factor, polynomial, symmetric polynomial, discriminant, resultant

Obsah

Úvod

Matematika ako súčasť nášho života sa datuje už od počiatku existencie človeka. Tak ako aj história, tak aj algebraické rovnice boli prvýkrát zaznamenaná na hlinených tabuľkách pochádzajúcich z Babylonskej ríše. Už 2000 rokov p.n.l. starí matematici započali rozvoj mnohých odborov modernej matematiky, ku ktorým patrí aj odbor polynómov, ktorému sa budeme hlbšie venovať.

Polynómy sú výrazy pozostávajúce buď z jednej, alebo z viacerých premenných rôznych stupňov. Už od 16. storočia boli známe vzorce na výpočet polynómov 2., 3. a 4. stupňa, ale až v roku 1824 Abel dokázal, že neexistujú presné vzorce na výpočet polynómov 5. a vyšších stupňov. V 1830 Galois rozšíril Abel-Ruffinovu definíciu pre polynóm 5. a vyšších stupňov cez štúdium permutácie koreňov polynómu, a tým odštartoval Galoisovu teóriu. Táto sa zaoberá problémami polynómov vyšších stupňov.

Náš cieľ v prvej kapitole bude porozumieť základným algebraickým štruktúram, základnej teórii polynómov a rozkladu polynómu na ireducibilné činitele. Táto kapitola bude obohatená aj niekoľkými príkladmi, aby čitateľ lepšie porozumel uvedenej teórii. Ukážeme si, ako rozložiť kvadratický, kubický a kvartický polynóm na ireducibilné činitele. V tejto kapitole budeme vychádzať z literatúry [1, 2, 3, 5].

V druhej kapitole sa venujeme symetrickým polynómom a ich základným úpravám. Predstavíme si špeciálne tvary symetrických polynómov, ako sú Newtonove polynómy a Schurov polynóm [8].

A nakoniec, si v tretej kapitole ukážeme využitie symetrických polynómov. Prospešné budú pri vypočte diskriminantov a rezultantov polynómov [4].

Hlavný cieľ tejto bakalárskej práce bude oboznámiť čitateľa s teóriou polynómov a ich vzťahom so symetrickými polynómami. Táto práca bude skôr poňatá z teoretického hľadiska, ale bude aj obohatená príkladmi, ktoré lepšie pomôžu čitateľom porozumieť danú problematiku.

1 Polynómy

Táto kapitola je voľne spracovaná podľa literatúry [1, 2, 3, 5].

V tejto kapitole sme sa rozhodli venovať teórii polynómov vo viacerých bodoch:

(1) Algebraické štruktúry,

(2) Okruh polynómov,

(3) Ireducibilita a korene polynómu.

1.1 Algebraické štruktúry

Definícia 1.1. *Okruh je algebraický systém* $P = \{P, +, \times\}$ *s dvoma binárnymi operáciami (sčítanie a násobenie), v ktorom platí*

(i) *P je abelovská grupa vzhľadom na sčítanie, to znamená, že platí*

1. *komutatívny zákon:* $a + b = b + a; \forall a, b \in P,$
2. *asociatívny zákon:* $(a + b) + c = a + (b + c); \forall a, b, c \in P,$
3. *existuje nulový prvok* 0*:* $a + 0 = a; \forall a \in P,$
4. *existuje opačný prvok:* $\forall a \in P \quad \exists(-a) \in P$ *tak, že platí:* $a + (-a) = 0,$

(ii) *P je monoid vzhľadom na násobenie, to znamená, že platí*

1. *asociatívny zákon:* $(a \times b) \times c = a \times (b \times c); \forall a, b, c \in P,$
2. *existuje jednotkový prvok* 1*:* $a \times 1 = a \wedge 1 \times a = a; \forall a \in P,$

(iii) *naviac platia distributívne zákony*

1. *distributívny zákon (ľavý):* $a \times (b + c) = (a \times b) + (a \times c); \forall a, b, c \in P,$
2. *distributívny zákon (pravý):* $(a + b) \times c = (a \times c) + (b \times c); \forall a, b, c \in P.$

Ak k $a \in P$ existuje taký prvok $a^{-1} \in P$, pre ktorý platí

$$a \times a^{-1} = 1 = a^{-1} \times a,$$

tak a^{-1} nazývame inverzný prvok k prvku a.

Poznámka: Deliteľ nuly v okruhu P je taký nenulový prvok $a \in P$, ku ktorému existuje taký nenulový prvok $b \in P$, že

$$a \times b = 0.$$

Najtypickejší okruh tvorí množina celých čísel $\mathbb{Z} = \{Z, +, \times\}$ vzhľadom na operácie sčítania a násobenia. Treba si uvedomiť, že v $\mathbb{Z}$ a všeobecne v okruhoch nie je väčšinou možné deliť. Poznáme rôzne druhy okruhov. Medzi najznámejšie patria

(1) komutatívne okruhy, pre ktoré platí zákon komutatívnosti

$$a \times b = b \times a; \quad \forall a, b \in P,$$

a medzi známe komutatívne okruhy patrí $\mathbb{Z}$, konečné okruhy Z_m celých čísel modulo m a mnohé ďalšie číselné systémy,

(2) nekomutatívne okruhy, pre ktoré neplatí zákon komutatívnosti.

Nech je daný okruh P. Nasledujúcim spôsobom môžeme z neho zostrojiť nekomutatívny okruh vzhľadom na násobenie.

Príklad 1.1 Nech P je ľubovoľný okruh, potom množinu všetkých matíc $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ typu 2×2; $a, b, c, d \in P$ budeme označovať $M_2(P)$. Definujme okruh $[M_2(P), +, \times]$ pomocou nasledujúcich operácií

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \times \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}.$$

Pretože násobenie matíc je vo všeobecnosti nekomutatívne, okruh $M_2(P)$ je nekomutatívny okruh.

Polia sú komutatívne okruhy, v ktorých operácie ščítania a násobenia majú obvyklé zaužívané vlastnosti. Medzi polia patria napr. racionálne čísla $\mathbb{Q}$, reálne čísla $\mathbb{R}$, komplexné čísla $\mathbb{C}$, pole Z_p celých čísel modulo p, kde p je prvočíslo. [1]

Lema 1.2. *Nech P je okruh.* 0 *je v každom okruhu P neutrálny prvok vzhľadom na sčítanie a aj* 0 *vzhľadom na násobenie*

$$0 \times a = 0 = a \times 0; \quad \forall a \in P.$$

Dôkaz. Z toho, že $b = b + 0; \quad \forall b \in P$ platí

$$b \times a = (b + 0) \times a = b \times a + 0 \times a.$$

Z definície prvku 0 dostávame $b \times a = b \times a + 0$. Z tranzitívnosti rovnosti vyplýva, že $b \times a + 0 \times b = b \times a + 0$. Použitím zákona krátenia pre sčítanie[1] dostávame, že $0 \times a = 0$. Dôkaz druhej časti rovnosti $0 = b \times 0$ je podobný a ponecháme ho na čitateľa. [1] □

Lema 1.3. *$\forall a, b \in P$ platí*

$$(-a) \times (-b) = a \times b.$$

Dôkaz. Pretože a spĺňa

$$a + (-a) = 0,$$

tak platí

$$0 = 0 \times (-b) = (a + (-a)) \times (-b) = a \times (-b) + (-a) \times (-b).$$

Tiež platí

$$a \times (-b) + a \times b = a \times ((-b) + b) = a \times 0 = 0.$$

Použitím zákona krátenia pre sčítanie dostávame, že

$$(-a) \times (-b) = a \times b.[1]$$

□

Okruhy vo všeobecnosti majú málo zaujímavých vlastností. My sa budeme venovať dvom okruhom, ktorými sú

(1) obory integrity,

(2) polia.

Definícia 1.4. *Obor integrity je komutatívny okruh, pre ktorý platí nasledujúci zákon krátenia*

$$a \times b = a \times c \quad \wedge \quad a \neq 0 \quad \Rightarrow \quad b = c.$$

[1] zákon krátenia pre sčítanie. Ak $a + b = a + c$, tak potom $b = c; \quad \forall a, b, c \in P$.

Najznámejší obor integrity je množina celých čísel $\mathbb{Z}$. Okruh $Z_4 = \{0, 1, 2, 3\}$ nie je oborom integrity, pretože platí

$$2 \times 2 = 0; \quad ale \quad 2 \neq 0; \quad 2 \in Z_4.$$

Veta 1.5. *Komutatívny okruh P je obor integrity práve vtedy, keď súčin každých jeho dvoch nenulových prvkov je nenulový, teda platí*

$$a \neq 0 \wedge b \neq 0 \quad \Rightarrow \quad a \times b \neq 0.$$

Dôkaz. Ako prvé dokážeme pravú implikáciu sporom. Ak Veta 1.5 neplatí, tak

$$a \times b = 0 = a \times 0; \quad a \neq 0, b \neq 0,$$

a to je v spore s Definíciou 1.4, kde $c = 0$.
Ľavú implikáciu tiež dokážeme sporom. Ak neplatí Definícia 1.4, tak

$$a \times (b - c) = a \times b - a \times c = 0,$$

pričom sú obidva prvky $a, (b - c)$ nenulové, čím sa dostávame opäť k sporu. [1] □

Treba si všimnúť nasledujúcu ekvivalentnú podmienku s Vetou 1.5

$$a \times b = 0 \Rightarrow a = 0 \vee b = 0,$$

z ktorej vyplýva nasledujúci dôsledok.

Dôsledok 1.6. *Jediné idempotentné prvky každého oboru integrity sú prvky* 0 *a* 1.

Dôkaz. Podľa definície každý idempotentný prvok vyhovuje podmienke

$$c^2 = c,$$

teda

$$0 = c^2 - c = c \times (c - 1).$$

Podľa vyššie spomenutej ekvivalencie z Vety 1.5

$$c = 0 \vee c - 1 = 0 \quad \Rightarrow \quad c = 0 \vee c = 1.[1]$$

□

Inak povedané, okruh P je obor integrity práve vtedy, keď neobsahuje žiadne delitele nuly.

Lema 1.7. *Okruh Z_m je obor integrity práve vtedy, keď m je prvočíslo.*

Dôkaz. Dôkaz je možné nájsť v [2]. □

Definícia 1.8. *Pole je komutatívny okruh, v ktorom nenulové prvky tvoria grupu vzhľadom na násobenie. Pretože v každej grupe platí zákon krátenia, tak každé pole je obor integrity.*

Medzi polia patrí pole racionálnych čísel $\mathbb{Q}$, pole reálnych čísel $\mathbb{R}$, pole komplexných čísel $\mathbb{C}$, konečné polia Z_p celých čísel modulo p.

Lema 1.9. *V každom poli je definovaná operácia delenia (okrem delenia nulou), a táto operácia delenia je jednoznačná.*

Dôkaz. Dôkaz sa k nahliadnutiu nachádza v [1]. □

Veta 1.10. *Každý konečný obor integrity je poľom.*

Dôkaz. Dôkaz sa nachádza v [1]. □

Veta 1.11. *Pre podiely v ľubovoľnom poli platia nasledujúce pravidlá ($b \neq 0, d \neq 0$)*

(1) $\frac{a}{b} = \frac{c}{d} \quad \Leftrightarrow \quad a \times d = b \times c,$

(2) $\frac{a}{b} \pm \frac{c}{d} = \frac{a \times d \pm b \times c}{b \times d},$

(3) $\frac{a}{b} \times \frac{c}{d} = \frac{a \times c}{b \times d},$

(4) $\frac{a}{b} + \frac{-a}{b} = 0,$

(5) $\frac{a}{b} \times \frac{b}{a} = 1,$ *ak* $a, b \neq 0.$

Dôkaz. Dôkaz kvôli zdĺhavosti neuvádzame, ale je ho možné nájsť v [1]. □

1.2 Okruh polynómov

Nech K je pole, potom množinu všetkých polynómov s koeficientami z poľa K budeme označovať $K[x]$.

Definícia 1.12. *Polynóm s premennou $x \in K$ nazývame výraz tvaru*

$$p(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2x^2 + a_1x + a_0 = \sum_{i=0}^{n} a^i x^i,$$

kde $n \in \mathbb{N}$ a $a_i \in K$; i= 0,..., n; sa nazývajú koeficienty polynómu. Polynóm, ktorého koeficient $a_n \neq 0$ hovoríme, že je stupňa n, označujeme $st(p(x)) = n$ a polynóm, ktorého koeficienty $a_i = 0$ hovoríme, že je stupňa 0 čo označujeme $st(p(x)) = -\infty$.

Definícia 1.13. *Člen polynómu, ktorého suma mocnín premenných je najvyššieho stupňa sa nazýva vedúci člen polynómu.*

Definícia 1.14. *Normovaný polynóm je taký polynóm, ktorého koeficient pri najvyššej premennej x sa rovná 1.*

$$p(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2x^2 + a_1x + a_0$$

Uvažujme polynóm $q(x)$, $st(q(x)) = m$, taký že

$$q(x) = b_m x^m + b_{m-1}x^{m-1} + b_{m-2}x^{m-2} + ... + b_2x^2 + b_1x + b_0 = \sum_{j=0}^{m} b^j x^j.$$

Lema 1.15. *Dva polynómy p(x), st(p(x))=n a q(x), st(q(x))=m sa rovnajú práve vtedy, keď platí*

(1)

$$a_i = b_i,$$

pre ktoré sú definované obidva koeficienty; $(\forall i \leq n \wedge m)$[2],

(2) *všetky ostatné koeficienty a_i, b_i sú nulové.*

Alebo ekvivalentne môžeme tvrdiť, že dva polynómy $p(x), q(x)$ sa rovnajú práve vtedy, keď

$$st(p(x)) = st(q(x)) = n \wedge a_i = b_i; \quad \forall i = 0, 1, \ldots, n.$$

[2]označenie $n \wedge m$ znamená menšie z čísel n, m

Dôkaz. Dôkaz k nahliadnutiu nájdete v [1]. □

Dva polynómy $p(x), q(x) \in K[x]$ budeme sčítavať tak, že sčítame odpovedajúce koeficienty pri rovnakých mocninách. Nech polynóm $r(x) = p(x) + q(x)$

$$r(x) = c_s x^s + c_{s-1}x^{s-1} + c_{s-2}x^{s-2} + ... + c_2 x^2 + c_1 x + c_s,$$

potom koeficienty c_k sú dané nasledovne

$$c_k = \begin{cases} a_k + b_k, & \text{pre } k \leq m \wedge n \\ a_k, & \text{pre } m < k \leq n, \text{ak } m < n \\ b_k, & \text{pre } n < k \leq m, \text{ak } m > n, \end{cases}$$

kde $s = \max\{m, n\}$.

Podobne spravíme pre súčin dvoch polynómov $p(x), q(x)$. Ich súčin je definovaný

$$t(x) = d_{m+n}x^{m+n} + d_{m+n-1}x^{m+n-1} + d_{m+n-2}x^{m+n-2} + ... + d_2 x^2 + d_1 x + d_0,$$

kde koeficienty

$$d_k = \sum_{i+j=k} a_i b_j.$$

Pre $k \leq m \wedge n$, zrejme k-ty koeficient polynómu $t(x)$ je rovný

$$d_k = a_0 b_k + \ldots + a_k b_0. \, [1]$$

Príklad 1.1 Daný je okruh $Z_2 = \{0, 1\}$. Máme zadané dva polynómy

$$p(x) = 1 + 1x + 0x^2,$$
$$q(x) = 1 + 1x + 1x^2.$$

Potom

$$p(x) + q(x) = (1 + 1x) + (1 + 1x + 1x^2) = x^2,$$
$$p(x) \times q(x) = (1 + 1x) \times (1 + 1x + 1x^2) = 1 + x^3. \, [1]$$

Lema 1.16. *Nech L je obor integrity a $L[x]$ je množina všetkých polynómov s koeficientami z poľa L. Potom v $L[x]$ platí*

$$st(p(x) \times q(x)) = st(p(x)) + st(q(x)).$$

Dôkaz. Dôkaz možno nájsť v [1]. □

Základným problémom algebry je riešenie polynomických rovníc. Napriek tisícročnému úsiliu sa matematikom nepodarilo túto úlohu doposiaľ uspokojivo vyriešiť.

Definícia 1.17. *Polynomické rovnice sú rovnice tvaru*

$$a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_2 x^2 + a_1 x + a_0 = 0.$$

Skôr ako začneme riešiť polynomické rovnice, musíme si povedať z akej množiny $(\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C})$ môžu polynomické rovnice nadobúdať riešenia. Na jednoduchom príklade ukážeme vyššie zmienenú dôležitosť pevnej determinácie podmienok.

Príklad 1.2 Máme danú polynomickú rovnicu druhého stupňa

$$4 \times x^2 - 1 = 0, \quad \forall x \in \mathbb{N}.$$

Vidíme, že neexistuje riešenie tejto rovnice v množine $\mathbb{N}$, pretože pre riešenie x platí

$$x = \mid 1/2 \mid .$$

Riešenie tejto rovnice má tvar

$$\begin{aligned} x_1 = &\quad 1/2, \\ x_2 = &\quad -1/2, \end{aligned}$$

to znamená, že $x_1, x_2 \in \mathbb{Q}$.

Týmto príkladom sme ukázali, že záleží na správnom zadefinovaní podmienok riešenia.

Pri riešení polynomických rovníc uprednostňujeme zvyčajné aritmetické operácie sčítania, odčítania, násobenia a delenia koeficientov, ako sme práve videli a sledujeme ako tieto operácie závisia na číselnom okruhu, v ktorom pracujeme. Práve preto musíme predpokladať, že koeficienty riešených polynómov ležia v pevne zadanom okruhu. [2]

Veta 1.18. *Nech K je pole. Potom k polynómu $p(x) \in K[x]$ existuje inverzný prvok práve vtedy, keď $st(p(x)) = 0$.*

Dôkaz. Dôkaz je možné nájsť v [2]. □

Uvažujme, že K je pole. Polynóm $g(x) \in K[x]$ delí polynóm $f(x) \in K[x]$, ak existuje polynóm $h(x) \in K[x]$ taký, že $f(x) = h(x) \times g(x)$. Inak povedané $g(x)$ je deliteľ $f(x)$. Problém deliteľnosti a rozložiteľnosti v oboroch integrity je zjednodušený tým, že sa nemusíme obávať prítomnosti deliteľov nuly.
Rozklad $r = a \times b$ prvku $r \in P$, kde r je nenulový prvok a nie je deliteľ jednotky nazývame triviálny [2], ak a a b sú inverzné prvky. Inak sa nazýva netriviálny. Prvok $r \in P$ je ireducibilný, ak je nenulový, nie je deliteľom jednotky a každý rozklad prvku r je triviálny. Daný rozklad na ireducibilné činitele je súčasťou ďalšej podkapitoly.

1.3 Ireducibilita a korene polynómu

Definícia 1.19. *Nech K je pole a nech polynómy $f(x)$, $g(x) \in K[x]$. Polynóm $g(x)$ budeme nazývať triviálnym deliteľom polynómu $f(x) \in K[x]$, ak stupeň $g(x) = 0$, alebo polynómy $f(x), g(x)$ sú asociované ($f(x)/g(x)$ a zároveň $g(x)/f(x)$), označujeme $f(x) \backsim g(x)$.*

Definícia 1.20. *Nech K je pole, nech $f(x) \in K[x]$ a nech $st(f(x)) \geqq 1$. Polynóm $f(x) \in K[x]$ voláme ireducibilným[3], ak $f(x)$ nemá v okruhu $K[x]$ okrem triviálnych deliteľov žiadne iné. Inak budeme polynóm $f(x) \in K[x]$ nazývať reducibilným[4].*

Pri rozklade polynómov na ireducibilné činitele budeme vychádzať zo základnej vety aritmetiky platnej v okruhu $\mathbb{Z}$.

Definícia 1.21. *Každé číslo $n \in \mathbb{Z}$ väčšie ako 1 je buď prvočíslo, alebo sa dá rozložiť na súčin prvočísiel.*

Podobné tvrdenie je platné aj v okruhu polynómov, t.j. existuje jednoznačný rozklad polynómov na ireducibilné činitele.

Veta 1.22. *Nech K je pole. Polynóm $f(x) \in K[x]$ kladného stupňa je buď ireducibilný v K[x], alebo sa dá rozložiť na súčin ireducibilných polynómov v K[x].*

Dôkaz. Dôkaz sa nachádza v [2]. □

[3] ireducibilný = nerozložiteľný
[4] reducibilný = rozložiteľný

Nato aby sme dokázali rozkladať polynómy na ireducibilné činitele potrebujeme zistiť korene polynómu. Korene polynómu sú také čísla $\gamma \in K$, ktoré spĺňajú rovnicu polynómu

$$a_n\gamma^n + a_{n-1}\gamma^{n-1} + a_{n-2}\gamma^{n-2} + ... + a_2\gamma^2 + a_1\gamma + a_0 = 0.$$

Chceme ukázať, že číslo $\gamma \in K$ je koreň polynómu $f(x)$ práve vtedy, keď $(x-\gamma)$ delí polynóm $f(x)$ v $K[x]$. Nástroj, ktorý použijeme je delenie polynómov. Podobne ako v prípade deliteľnosti celých čísel, kde

$$a = b \times q + r; r < b; \quad a, b, q, r \in \mathbb{Z},$$

platí nasledujúca veta.

Veta 1.23. *Nech K je pole. Ak $a(x)$ a $b(x)$ sú nenulové polynómy v $K[x]$, potom existujú jediné polynómy $q(x), r(x)$, $st(r(x)) < st(b(x))$, ktoré spĺňajú*

$$a(x) = b(x) \times q(x) + r(x).$$

Dôkaz. Podiel $q(x)$ a zvyšok $r(x)$ vypočítame pomocou postupného delenia polynómov. Nech $a(x) = \sum_{k=0}^{m} a_k x^k$ a $b(x) = \sum_{k=0}^{n} b_k x^k$, potom budeme rozlišovať dva prípady

(1) ak $m < n$, tak označíme, že $q(x) = 0$ a $r(x) = a(x)$,

(2) ak $m \geq n$, tak definujeme

$$a_1(x) = a(x) - b_n^{-1} \times a_m \times x^{m-n} \times b(x) = a(x) - q_1(x) \times b(x).$$

Stupeň polynómu $a_1(x)$ je najviac $m-1$, pretože $a(x)$ a $q_1(x) \times b(x)$ majú rovnaký vedúci koeficient $b_n^{-1} \times a_m \times b_n = a_m$. Tento postup použitím matematickej indukcie budeme opakovať (najviac $m-n+1$ krát) pokým nedostaneme zvyšok

$$a_k(x) = a(x) - [\sum q_i(x)]b(x) = a(x) - q(x) \times b(x),$$

ktorý bude menšieho stupňa ako n. [2]

□

Môžeme uvažovať, že polynóm $a(x)$ má stupeň 1, γ je koreň polynómu $f(x)$ a nech platí $a(x) = (x - \gamma)$, kde $\gamma \in K$. Potom $(x - \gamma)$ je deliteľom $f(x)$, ak existuje polynóm $g(x)$ taký, že

$$f(x) = (x - \gamma) \times g(x).$$

Veta 1.24. *Nech K je pole, polynóm $f(x) \in K[x]$ a $\gamma_1, \gamma_2, ..., \gamma_m$ sú rôzne korene polynómu $f(x)$. Potom*

$$(x - \gamma_1) \times (x - \gamma_2) \times ... \times (x - \gamma_m)$$

delí polynóm $f(x) \in K[x]$.

Dôkaz. Dôkaz je možné nájsť v [2]. □

Z predchádzajúceho tvrdenia Vety 1.24 vyplýva dôležitý dôsledok.

Dôsledok 1.25. *Nech K je pole a $f(x)$ je nenulový polynóm stupňa n. Potom polynóm $f(x)$ má najviac n rôznych koreňov v K.*

Dôkaz. Dokážeme dané tvrdenie sporom. Nech polynóm $f(x)$ má $n+1$ rôznych koreňov γ_i; $i = 1, ..., n$. Potom pomocou tvrdenia Vety 1.23 dostávame, že polynóm $(x - \gamma_1) \times (x - \gamma_2) \times ... \times (x - \gamma_m)$ delí polynóm $f(x)$, to znamená, že existuje polynóm $h(x)$ a platí:

$$f(x) = (x - \gamma_1) \times (x - \gamma_2) \times ... \times (x - \gamma_m) \times h(x).$$

Týmto však prichádzame k sporu, pretože stupeň polynómu $f(x)$ je n a na pravej strane máme polynóm stupňa väčšieho ako n. □

Ireducibilné činitele hrajú analogickú úlohu ako prvočísla v aritmetike. Je prirodzené položiť si otázku, aké existujú ireducibilné činitele. Odpoveď na túto otázku závisí od poľa K.

V prvom rade, každý polynóm prvého stupňa je ireducibilný, pretože súčin dvoch polynómov s kladným stupňom má vždy stupeň ≥ 2. Z toho vyplýva, že rozklad polynómu na lineárne činitele je len špeciálnym prípadom rozkladu na ireducibilné polynómy. Napríklad platí

- v okruhu $Q[x]$ existujú ireducibilné delitele ľubovoľného stupňa,
- v okruhu $R[x]$ sú ireducibilné okrem polynómov 1. stupňa aj polynómy 2. stupňa, ktoré nemajú reálne korene.

  Príklad 1.3 Uvažujme polynóm $x^2 + x + 1$. Daný polynóm má dve komplexné riešenia a to

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

- v okruhu $C[x]$ ireducibilnými činiteľmi sú všetky polynómy 1. stupňa, pretože v $C[x]$ platí tzv. hlavná veta algebry a to, že každá algebraická rovnica kladného stupňa s koeficientami z poľa C má nejaký koreň v poli komplexných čísel.

1.4 Rozklad polynómu na ireducibilné činitele

Hlavným problémom rozkladu polynómu na ireducibilné činitele bez pomoci technických inovácií (Matlab, Wolfram Alpha) je neznalosť algoritmov pre polynómy stupňa $n \geq 5$. Preto sa najprv budeme zaoberať rozkladom polynómov 2., 3. a 4. stupňa, t.j:

Kvadratický polynóm $\longrightarrow f(x) = ax^2 + bx + c,$

Kubický polynóm $\longrightarrow g(x) = ax^3 + bx^2 + cx + d,$

Kvartický polynóm $\longrightarrow h(x) = ax^4 + bx^3 + cx^2 + dx + e.$

Existuje viacero metód ako nájsť korene týchto polynómov. My si ukážeme najviac používané metódy. Budeme predpokladať nenulovosť koeficientov a nebude záležať na množine, v ktorej budeme riešiť.

1.4.1 Kvadratický polynóm

Na získanie koreňov kvadratického polynómu hľadáme priesečníky paraboly s osami x a y. Pri výpočte koreňov si budeme pomáhať diskriminantom polynómu

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

Výpočet koreňov kvadratického polynómu:

$$\begin{aligned} ax^2 + bx + c &= 0 \\ 4a^2x^2 + 4abx + 4ac &= 0 \\ (2ax + b)^2 - b^2 + 4ac &= 0 \\ (2ax + b)^2 &= D \\ \mid 2ax + b \mid &= \sqrt{D} \\ x_{1,2} &= \frac{-b \pm \sqrt{D}}{2a} \end{aligned}$$

Diskriminant môže nadobúdať tri hodnoty:

1. $D > 0 \Rightarrow$ existujú dva rôzne korene $x_{1,2} = \frac{-b \pm \sqrt{D}}{2a}$,
2. $D < 0 \Rightarrow$ existujú dva rôzne komplexné (vždy!) $x_{1,2} = \frac{-b \pm i\sqrt{|D|}}{2a}$,
3. $D = 0 \Rightarrow$ existuje jeden dvojnásobný koreň $x_{1,2} = \frac{-b}{2a}$.

Rozklad na ireducibilné činitele bude rovný:

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

1.4.2 Kubický polynóm

Diskriminant nebudeme kvôli jeho náročnému predpisu používať. Pracovať budeme s Cardánovými vzorcami presne určenými na nájdenie koreňov kubického polynómu. Majme kubický polynóm v tvare

$$ax^3 + bx^2 + cx + d = 0,$$

kde $a, b, c, d \in \mathbb{R}$. Použitím substitúcie $x = y - \frac{b}{3a}$ dostaneme *neúplnú* kubickú rovnicu (bez kvadratického člena) v tvare:

$$y^3 + py + q = 0,$$

kde

$$\begin{aligned} p &= \frac{c}{a} - \frac{b^2}{3a^2}, \\ q &= \frac{d}{a} + \frac{2b^3}{27a^3} - \frac{bc}{3a^2}. \end{aligned}$$

Vidíme, že substitúciou sme prešli k jednoduchšiemu problému, ktorý bude pre nás ľahšie riešiteľný. Zavedieme druhú substitúciu

$$y = \alpha + \beta$$

a redukovanú kubickú rovnicu prepíšeme na tvar

$$\alpha^3 + \beta^3 + (\alpha + \beta)(3\alpha\beta + p) + q = 0.$$

V tomto bode Cardáno zaviedol druhú podmienku pre premenné α a β

$$\begin{aligned} 3\alpha\beta + p &= 0, \\ \alpha\beta &= -\frac{p}{3}, \end{aligned}$$

z ktorej dostal dve rovnice

$$\begin{aligned} \alpha^3 + \beta^3 &= -q, \\ \alpha^3\beta^3 &= -p^3/27, \end{aligned}$$

ktoré spľňajú Vietove vzorce pre kvadratickú rovnicu tvaru (α^3 a β^3 sú korene kvadratickej rovnice)

$$z^2 + qz - p^3/27 = 0.$$

Na riešenie už známej kvadratickej rovnice použijeme diskriminant a korene budú tvaru

$$\begin{aligned} \alpha^3 &= -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \\ \beta^3 &= -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}, \end{aligned}$$

ktoré spätnou substitúciou dosadíme a pomocou polárnej reprezenácie získame riešenie kubického polynómu.

1.4.3 Kvartický polynóm

Majme kvartický polynóm v tvare

$$ax^4 + bx^3 + cx^2 + dx + e = 0,$$

kde $a, b, c, d, e \in \mathbb{R}$. Použitím substitúcie $x = y - \frac{b}{4a}$ dostaneme *neúplnú* kvartickú rovnicu (bez kubického člena) v tvare:

$$y^4 + py^2 + qx + r = 0,$$

kde

$$\begin{aligned} p &= \frac{8ac - 3b^2}{8a^2}, \\ q &= \frac{b^3 - 4abc + 8a^2d}{8a^3}, \\ r &= \frac{-3b^4 + 256a^3e - 64abd^2 + 16ab^2c}{256a^4}. \end{aligned}$$

Získanú rovnicu upravíme a rozložíme na štvorec.

$$\begin{aligned} x^4 + px^2 &= -qx - r \\ (x^2 + \frac{p}{2})^2 &= -qx - r + \frac{p^2}{4} \end{aligned}$$

Ďalej do poslednej rovnice vložíme neurčitý parameter α, aby sme na pravej strane získali kvadratickú rovnicu.

$$\begin{aligned} (x^2 + \frac{p}{2})^2 + 2\alpha(x^2 + \frac{p}{2}) + \alpha^2 &= \frac{p^2}{4} - qx - r + 2\alpha(x^2 + \frac{p}{2}) + \alpha^2, \\ (x^2 + \frac{p}{2} + \alpha)^2 &= 2\alpha x^2 - qx + \frac{p^2}{4} - r + \alpha p + \alpha^2. \end{aligned}$$

Pravú stranu poslednej rovnice vieme upraviť na štvorec, preto vypočítame diskriminant

$$D = -8\alpha^3 - 8p\alpha^2 - 8(\frac{p^2}{4} - r)\alpha + q^2 = 0.$$

Diskriminant nám vyšiel ako rovnica 3. rádu v premennej α, teda nájdeme riešenie α_0 kubickej rovnice a jeho dosadením získam

$$(y^2 + \frac{p}{2} + \alpha_0 \pm (\alpha_0 + \frac{q}{4\alpha_0})\sqrt{2\alpha_0}) = 0.$$

Spätnou substitúciou nájdeme riešenie kvartického polynómu.

2 Úvod do symetrických polynómov

Symetrické polynómy sú všadeprítomné v matematike a matematickej fyzike. Napríklad sa objavujú v základnej algebre (Vietove vzorce), v teórií reprezentácie symetrických grúp a všeobecných lineárnych grupách nad $\mathbb{C}$ alebo konečnými poliami.
Prostredníctvom ich blízkeho vzťahu s teóriou reprezentácie si teória symetrických funkcií našla mnoho aplikácií v matematickej fyzike (teória superstrún).

2.1 Symetrické polynómy

V tejto podkapitole si zadefinujeme symetrické polynómy a vysvetlíme z čoho je odvodení ich názov symetrické. Ako prvé si zadefinujeme pojem permutácie, ktorý bude neskôr pre nás dôležitý.

Definícia 2.1. *Pod permutáciou konečnej množiny A rozumieme každú bijekciu na množine A, teda $\sigma : A \to A$.*

To znamená, že permutácia je jednoznačné zobrazenie množiny A.
Pripomeňme si známe Vietove vzorce, ktoré nám slúžia na vyjadrenie vzťahu medzi koreňmi polynómu a jeho koeficientami.

Definícia 2.2. *Predpokladajme, že $x_1, \ldots, x_n$ sú korene polynómu*

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_n.$$

Potom Vietove vzorce majú tvar

$$\begin{aligned}
e_1(x_1, \ldots, x_n) &= \sum_{i=1}^{n} x_i = -a_1, \\
e_2(x_1, \ldots, x_n) &= \sum_{1 \le i_1 < i_2 \le n} x_{i_1} x_{i_2} = a_2, \\
&\vdots \\
e_m(x_1, \ldots, x_n) &= \sum_{1 \le i_1 < \ldots < i_m \le n} x_{i_1} \ldots x_{i_m} = (-1)^m a_m, \\
&\vdots \\
e_n(x_1, \ldots, x_n) &= x_1 x_2 \ldots x_n = (-1)^n a_n.
\end{aligned}$$

Polynóm $e_m(x_1, \ldots, x_n)$ sa nazýva m-tý základný symetrický polynóm premenných $x_1, \ldots, x_n$ a má nasledovnú vlastnosť

$$e_m(x_{\sigma_1}, \ldots, x_{\sigma_n}) = e_m(x_1, \ldots, x_n),$$

pre všetky permutácie σ množiny $\{1, \ldots, n\}$.

Prechádzajúca vlastnosť m-tého symetrického polynómu nám dáva inšpiráciu k nasledujúcej definícii.

Definícia 2.3. *Polynóm $p(x_1, \ldots, x_n)$ nazývame symetrický polynóm, ak spĺňa*

$$p(x_{\sigma_1}, \ldots, x_{\sigma_n}) = p(x_1, \ldots, x_n),$$

pre všetky permutácie σ množiny $\{1, \ldots, n\}$. Množina všetkých symetrických polynómov premenných $x_1, \ldots, x_n$ označíme Λ_n.

Inak povedané, polynóm nazývame symetrický, ak pri zámene ľubovoľných dvoch premenných polynomická funkcia zostane nezmenená. Homogénna zložka symetrického polynómu je symetrický polynóm. [4]

Príklad 2.1 Nech je daný polynóm

$$p_k(x_1, \ldots, x_n) = x_1^k + x_2^k + \ldots + x_n^k; \quad k = 1, 2, \ldots,$$

potom je zrejme tento polynóm symetrický. Neskôr takéto polynómy budeme nazývať Newtonove polynómy.

Príklad 2.2 Každá permutácia neznámych x_1, x_2, x_3, x_4 v polynómoch

$$f_1 = x_1x_2 + x_3x_4,$$
$$f_2 = x_1x_3 + x_2x_4,$$
$$f_3 = x_1x_4 + x_2x_3,$$

dáva opäť tie isté polynómy. Chápeme ich ako polynomické funkcie, t.j. polynómy f_1, f_2, f_3 sú spolu symetrické polynómy.

Symetrické polynómy sa využívajú pri štúdiu algebraických rovníc jednej premennej. Kľúčom k úspechu sú vyššie zmienené Vietove vzorce definované v (2.2), ktoré vyjadrujú základné symetrické polynómy koreňov algebraickej rovnice pomocou jej koeficientov, ak je počet koreňov rovnice v danom poli rovný stupňu rovnice. Je jasné,

že iba symetrické polynómy v koreňoch rovnice sú dobre definované, t.j. hodnota každého ďalšieho polynómu závisí na poradí koreňov. Na druhej strane ukážeme, že každý symetrický polynóm závisí od koreňov algebraickej rovnice, ktoré môžu byť vyjadrené pomocou koeficientov tejto rovnice.

Príklad 2.3 Polynóm $p_2 = x_1^2 + x_2^2 + \ldots + x_n^2$ je symetrický. Tento polynóm po úprave na súčet základných symetrických polynómov vyzerá nasledovne

$$p_2 = e_1^2 - 2e_2.$$

Teda súčet štvorcov koreňov algebraickej rovnice

$$x^n + a_1 x^{n-1} + \ldots + a_n = 0$$

je rovný

$$p_2 = a_1^2 - 2a_2. \text{ [4]}$$

Nech $F \in \Lambda_m = \Lambda[X_1, \ldots, X_m]$ je polynóm m premenných a nech $f_1, \ldots, f_m \in \Lambda_n = \Lambda[x_1, \ldots, x_n]$ sú symetrické polynómy. Potom polynóm $F(f_1, \ldots, f_n)$ je symetrický polynóm $x_1, \ldots, x_n$. Je prirodzené položiť otázku, či existujú symetrické polynómy $f_1, \ldots, f_n$ také, že každý symetrický polynóm môže byť nimi vyjadrený. Dá sa ukázať, že jednoznačne existujú a sú to základné symetrické polynómy. Nech Λ_n je pole n premenných. Potom množinu všetkých symetrických polynómov s koeficientami z poľa Λ_n budeme označovať $\Lambda_n[x]$.

Lema 2.4. *Nech $u = ax_1^{k_1} x_2^{k_2} \ldots x_n^{k_n}$ je vedúci člen symetrického polynómu f. Potom*

$$k_1 \geq k_2 \geq \ldots \geq k_n.$$

Dôkaz. Predpokladajme, že $k_i < k_{i+1}$ pre nejaké i. Okrem u, polynóm f musí obsahovať monomiál

$$\bar{u} = ax_1^{k_1} \ldots x_i^{k_{i+1}} x_{i+1} k^i \ldots x_n^{k_n}$$

získaný z u prehodením x_i s x_{i+1}. Potom priamo vyplýva, že $st(\bar{u}) > st(u)$ a to je v spore s tvrdením, že u je vedúci člen symetrického polynómu. [4] □

Lema 2.5. *Ku každému monomiálu* $u = ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n}$ *spĺňajúcemu*

$$k_1 \geq k_2 \geq \dots \geq k_n,$$

existujú nezáporné celé čísla $l_1, \dots, l_n$ *také, že vedúci člen súčinu symetrických polynómov* $e_1^{l_1}...e_n^{l_n}$ *je rovný* u*. Navyše táto podmienka určuje* $l_1, \dots, l_n$ *jednoznačne.*

Dôkaz. Dôkaz sa nachádza v [6]. □

Veta 2.6. *Každý symetrický polynóm môže byť jednoznačne vyjadrený základnými symetrickými polynómami.*

Dôkaz. Dôkaz možno vidieť v [8]. □

Príklad 2.3 Nech je daný polynóm

$$f = p_3 = x_1^3 + x_2^3 + \dots + x_n^3.$$

Daný polynóm chceme vyjadriť v základných symetrických polynómoch. Naše výpočty sú uvedené v nasledujúcej Tabuľke 1.

m	u_m	$F_m(e_1, \dots, e_n)$	f_m
1	x_1^3	$e_1^3 = \sum_i x_i^3 + 3\sum_{i\neq j} x_i^2x_j$ $+6\sum_{i<j<k} x_ix_jx_k$	$-3\sum_{i\neq j} x_i^2x_j$ $-6\sum_{i<j<k} x_ix_jx_k$
2	$-3x_1^2x_2$	$-3e_1e_2 = -3\sum_{i\neq j} x_i^2x_j$ $-9\sum_{i<j<k} x_ix_jx_k$	$3\sum_{i<j<k} x_ix_jx_k$
3	$3x_1x_2x_3$	$3e_3 = 3\sum_{i<j<k} x_ix_jx_k$	0

Tabuľka 1: Vyjadrenie polynómu v tvare základných symetrických polynómov.

Potom výsledný polynóm zapísaný v základných polynómoch má nasledovný tvar

$$f = e_1^3 - 3e_1e_2 + 3e_3.$$

Existuje praktickejší prístup k základným symetrickým polynómom, ktorý ukážeme na ďalšom príklade.

Príklad 2.4 Nech je daný polynóm

$$f = (x_1x_2 + x_3x_4)(x_1x_3 + x_2x_4)(x_1x_4 + x_2x_3)$$

Opäť chceme daný polynóm vyjadriť v tvare základných symetrických polynómoch. Podľa Definície **??** je vedúci člen polynómu f $u = x_1^3x_2x_3x_4$. Bez počítania môžeme nájsť kandidátov $u_2, u_3, \ldots$. Najskôr všetky exponenty musia spĺnať nerovnosť z Lemy 2.4. Potom, v dôsledku toho, že f je homogénny polynóm[5] $st(f) = 6$, tak súčet exponentov musí byť rovný 6 a nakoniec kandidáti $u_2, u_3, \ldots$ musia byť menší ako u_1. V Tabuľke 2 uvedieme všetky možné monomiály, ktoré spĺňajú nasledujúce podmienky.Potom tvrdíme, že

$$f = e_1^2e_4 + ae_3^2 + be_2e_4.$$

u_1	u_2	u_3	u_4	F_m
3	1	1	1	$e_1^2 \times e_4$
2	2	2	0	e_3^2
2	2	1	1	$e_2 \times e_4$

Tabuľka 2: Monomiály.

Aby sme našli neznáme koeficienty a, b, musíme vyčísliť pár hodnôt neznámych $x_1, \ldots, x_4$.

x_1	x_2	x_3	x_4	e_1	e_2	e_3	e_4	f	
1	1	1	0	3	3	1	O	1	$a = 1$
1	1	-1	-1	0	-2	0	1	8	$-2b = 8$

Tabuľka 3: Výpočet koeficientov a a b.

Teda $a = 1$, $b = -4$ a polynóm f v základných symetrických polynómoch nadobúda

[5]Homogénny polynóm je polynóm, ktorého všetky nenulového členy majú rovnaký stupeň

tvar

$$f = e_1^2 e_4 + e_3^2 - 4e_2 e_4.$$

V prípade nehomogénnych symetrických polynómov budeme vyššie spomenutú metódu aplikovať na homogénne časti polynómu oddelene. [6]

2.2 Úplné symetrické polynómy

Budeme predpokladať postupnosť $\lambda = (\lambda_1, \ldots, \lambda_n)$ spĺňajúcu

$$\lambda_1 \geq \lambda_2 \geq \ldots \geq \lambda_n \geq 0.$$

Označíme

$$\mid \lambda \mid = \lambda_1 + \ldots + \lambda_n.$$

Ak $\mid \lambda \mid = k$, potom hovoríme, že λ je rozdelenie k, $\lambda \vdash k$. Počet nenulových λ_i, $i = 1, \ldots, n$ nazveme dĺžka lambdy a označíme $l(\lambda)$. Budeme používať množinu

$$P(k, n) = \{\lambda \vdash k \mid l(\lambda) \leq n\}$$

z rozdelenia k s dĺžkou $\leq n$. Definujme si postupnosť $\alpha = (\alpha_1, \ldots, \alpha_n)$ nezáporných celých čísel spĺňajúcu

$$x^\alpha = x_1^{\alpha_1} \ldots x_n^{\alpha_n}.$$

Nech $\lambda = (\lambda_1, \ldots, \lambda_n) \in P(k, n)$ a $S(x^\lambda)$ je symetrický polynóm. Pre $\lambda \in P(k, n)$ definujeme

$$m_\lambda(x_1, \ldots, x_n) = \sum x^\alpha,$$

kde suma prechádza cez všetky rôzne permutácie λ. Symetrické polynómy spĺňajúce podmienku zmienenú vyššie budeme nazývať základné symetrické polynómy zodpovedajúce λ.

Tvrdenie 2.7. *Množina*

$$\{m_\lambda(x_1, \ldots, x_n) \mid \lambda \in P(k, n)\}$$

je báza Λ_n^k.

Definícia 2.8. *Úplný symetrický polynóm pre každé $k \geq 0$ je suma všetkých monomiálov stupňa k taká, že*

$$h_k(x_1, \ldots, x_n) = \sum_{d_1+\ldots+d_n=k} x_1^{d_1} \ldots x_n^{d_n}.$$

Pre $k = 0$ platí, že $h_0(x_1, \ldots, x_n) = 1$ a úplný symetrický polynóm môžeme napísať ako

$$h_k(x_1, \ldots, x_n) = \sum_{\lambda \in P(k,n)} m_\lambda(x_1, \ldots, x_n).$$

Definícia 2.9. *Generujúca funkcia pre h_k je daná, ako*

$$H_n(t) = \sum_{d_1,\ldots,d_n \geq 0} x_1^{d_1} \ldots x_n^{d_n} t^{d_1+\ldots+d_n} = \frac{1}{\prod_{i=1}^{n}(1 - tx_i)}.$$

Chceme zistiť či existuje vzťah medzi úplnými a základnými symetrickými polynómami.

Veta 2.10. *Uvažujme generujúcu funkciu základnych symetrických polynómov*

$$E_n(t) = \sum_{i=0}^{n} e_i(x_1, \ldots, x_n)t^i = \prod_{i=1}^{n}(1 + tx_i).$$

Potom pre vzťah medzi symetrickými polynómami a základnými symetrickými polynómami platí

$$H(t)E(-t) = 1,$$

alebo ekvivalentne

$$\sum_{r=0}^{k}(-1)^r e_r h_{n-r} = 0; \quad \forall k \geq 1. \tag{1}$$

Dôkaz. Stanovme si nech

$$e_r(x_1, \ldots, x_n) = 0; \quad r > n.$$

Rovnicu (1) vyriešíme indukciou.

Nech $k = 1$.

$$h_1 - e_1 = 0,$$

teda

$$h_1 = e_1.$$

Pre $k = 2$

$$h_2 - e_1 h_1 + e_2 = 0,$$

teda

$$h_2 = e_1^2 - e_2 = \begin{pmatrix} e_1 & e_2 \\ 1 & e_1 \end{pmatrix}.$$

Indukciou pokračujme až pre k

$$h_k = \begin{vmatrix} e_1 & e_2 & e_3 & \dots & e_{k-1} & e_k \\ 1 & e_1 & e_2 & \dots & e_{k-2} & e_{k-1} \\ 0 & 1 & e_1 & \dots & e_{k-3} & e_{k-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & e_1 & e_2 \\ 0 & 0 & 0 & \dots & 1 & e_1 \end{vmatrix} = det(e_{1-i+j})_{1 \leq i,j \leq n}.$$

Vďaka symetrii medzi h a c v Rovnici 1, môžme predchádzajúcu maticu upraviť

$$h_k = \begin{vmatrix} h_1 & h_2 & h_3 & \dots & h_{k-1} & h_k \\ 1 & h_1 & h_2 & \dots & h_{k-2} & h_{k-1} \\ 0 & 1 & h_1 & \dots & h_{k-3} & h_{k-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & h_1 & h_2 \\ 0 & 0 & 0 & \dots & 1 & h_1 \end{vmatrix} = det(h_{1-i+j})_{1 \leq i,j \leq n}.$$

Využili sme poznatok, že

$$e_i(x_1, \dots, x_n) = 0; i < 0 \vee i > n.[8]$$

□

Tvrdenie 2.11. *Symetria medzi h a e ponúka zavedenie zobrazenia $\omega : \Lambda_n \to \Lambda_n$, ktoré sĺňa*

$$\omega(\sum_{m_1,\dots,m_n} a_{m_1,\dots,m_n} e_1^{m_1} \dots e_n^{m_n}) = \sum_{m_1,\dots,m_n} a_{m_1,\dots,m_n} h_1^{m_1} \dots h_n^{m_n},$$

spolu s nasledujúcimi podmienkami

(1) *ω je okruh homomorfizmu*

$$\omega(p+q) = \omega(p) + \omega(q); p, q \in \Lambda_n,$$
$$\omega(pq) = \omega(p)\omega(q); p, q \in \Lambda_n,$$

(2) $\omega(e_i) = h_i \quad \wedge \quad \omega(h_i) = e_i$

(3) $\omega^2 = id$ *(priamy dôsledok (1),(2)). [8]*

2.3 Newtonove polynómy

Definícia 2.12. *R-tý Newtonov polynóm, $r \geq 1$ v premenných $x_1, \ldots, x_n$ nazývame polynóm tvaru*

$$p_r(x_1, \ldots, x_n) = x_1^r + \ldots + x_n^r.$$

Veta 2.13. *Generujúca funkcia Newtonových polynómov je funkcia tvaru*

$$P_n(l) = \sum_{r\geq 1} p_r(x_1, \ldots, x_n) l^{r-1} = \sum_{i=1}^{n} \sum_{r\geq 1} x_i^r l^{r-1}$$
$$= \sum_{i=1}^{n} \frac{x_i}{1 - x_i t} = \frac{d}{dt} \lg \frac{1}{\prod_{i=1}^{n} (1 - x_i t)}.$$

Aplikovaním na generujúce funkcie $H_n(t)$ a $E_n(t)$ dostávame závislosť

$$P_n(t) = \frac{H_n(t)'}{H_n(t)} = \frac{E_n(-t)'}{E_n(-t)},$$

alebo

$$H_n(t)' = P_n(t) H_n(t),$$
$$E_n(t)' = P_n(-t) E_n(t).$$

Newtonove vzorce dostaneme ekvivalentne ako

$$k h_k = \sum_{r=1}^{k} p_r h_{k-r}, \tag{2}$$

$$k e_k = \sum_{r=1}^{k} (-1)^{r-1} p_r e_{k-r}. \tag{3}$$

Dôkaz. Opät vyriešíme Rovnicu (3) indukciou.

Nech $k = 1$.

$$p_1 - e_1 = 0,$$

teda

$$p_1 = e_1.$$

Pre $k = 2$

$$2e_2 = p_1e_1 - p_2 = \begin{pmatrix} p_1 & p_2 \\ 1 & p_1 \end{pmatrix}.$$

Pre $k = 3$

$$3e_3 = 2p_1e_2 - p_1e_1 + p_2 = \begin{pmatrix} p_1 & p_2 & p_3 \\ 2 & p_1 & p_2 \\ 0 & 1 & p_1 \end{pmatrix}.$$

Indukciou pokračujme až po k

$$ke_k = \begin{vmatrix} p_1 & p_2 & p_3 & \dots & p_{k-1} & p_k \\ k-1 & p_1 & p_2 & \dots & p_{k-2} & p_{k-1} \\ 0 & k-2 & p_1 & \dots & p_{k-3} & p_{k-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & p_1 & p_2 \\ 0 & 0 & 0 & \dots & 1 & p_1 \end{vmatrix}.$$

Taktiež môžme Rovnicu (2) prepísať ako

$$p_k = \sum_{r=1}^{k-1} (-1)^{k-r-1} e_{k-r} p_r + (-1)^{k-1} k e_k.$$

Pre $k = 1$

$$p_1 = e_1,$$

pre $k = 2$

$$p_2 = e_1p_1 - 2e_2 = \begin{pmatrix} e_1 & 2e_2 \\ 1 & e_1 \end{pmatrix}.$$

Pre $k = 3$

$$p_3 = e_1p_2 - e_2p_1 + 3e_3 = \begin{pmatrix} e_1 & e_2 & 3e_3 \\ 1 & e_1 & 2e_2 \\ 0 & 1 & e_1 \end{pmatrix}.$$

Indukciou až po k

$$p_k = \begin{vmatrix} e_1 & e_2 & e_3 & \dots & e_{k-1} & ke_k \\ 1 & e_1 & e_2 & \dots & e_{k-2} & (k-1)e_{k-1} \\ 0 & 1 & e_1 & \dots & e_{k-3} & (k-2)e_{k-2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & e_1 & 2e_2 \\ 0 & 0 & 0 & \dots & 1 & e_1 \end{vmatrix}.[8]$$

□

2.4 Schurov polynóm

V doterajších úvahách sme sa zaoberali symetrickými polynómami. V tejto podkapitole sa budeme venovať antisymetrickým polynómom a ich vzťahom so symetrickými polynómami.

Definícia 2.14. *Polynóm* $p(x_1, \dots, x_n) \in \mathbb{C}(\mathbb{x}_1, \dots, \mathbb{x}_n)$ *nazývame antisymetrický, ak*

$$p(x_{\sigma_1}, \dots, x_{\sigma_n}) = (-1)^\sigma p(x_1 \dots, x_n); \quad \sigma \in S_n.$$

Priestor všetkých antisymetrických polynómov v premenných $x_1, \dots, x_n$ *označíme* A_n.

Nech $d_1, \dots, d_n$ sú nezáporné celé čísla. Označme

$$d = (d_1, \dots, d_n)$$

a

$$a_d(x_1, \dots, x_n) = \begin{vmatrix} x_1^{d_1} & x_1^{d_2} & \dots & x_1^{d_n} \\ \vdots & \vdots & \vdots & \vdots \\ x_n^{d_1} & x_n^{d_2} & \dots & x_n^{d_n} \end{vmatrix}$$

je antisymetrický polynóm. Ak $\delta = (n-1, n-2, \ldots, 1, 0)$, tak Vandermondov determinant

$$\delta(x_1, \ldots, x_n) = \begin{vmatrix} x_1^{n-1} & x_1^{n-2} & \ldots & x_1 & 1 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ x_n^{n-1} & x_n^{n-2} & \ldots & x_n & 1 \end{vmatrix} = \prod_{1 \le i < j \le n} (x_i - x_j)$$

je tiež antisymetrický polynóm.

Veta 2.15. *Ako podpriestor $\mathbb{C}[x_1, \ldots, x_n]$ má priestor A_n nasledujúce vlastnosti:*

(1) *A_n je uzavretý vzhľadom na sčítanie,*

(2) *$A_n \times A_n \subset \Lambda_n$ a $\Lambda_n \times A_n \subset A_n$.*

Dôkaz. Dôkaz k nahliadnutiu sa nachádza v [8] □

Rovnako ako úvod do základných symetrických polynómov urobíme úvod do základných antisymetrických polynómov. Zaveďme si operátor

$$A : \mathbb{C}[x_1, \ldots, x_n] \to \mathbb{C}[x_1, \ldots, x_n],$$

ktorý spĺňa

$$(Ap)(x_1, \ldots, x_n) = \sum_{\sigma \in S_n} (-1)^\sigma p(x_{\sigma(1)}, \ldots, x_{\sigma(n)}).$$

Dá sa ukázať, že $Ap \in A_n; \quad \forall p \in \mathbb{C}[\mathbb{x}_\mathbb{1}, \ldots, \mathbb{x}_\mathbb{n}]$. Podobne z toho, že základný symetrický polynóm

$$\{m_\lambda \mid \lambda \in P(k, n), k \ge 0\}$$

formuje bázu Λ_n, sa dá dokázať, že

$$\{A_\alpha(x_1, \ldots, x_n) \mid d = (d_1, \ldots, d_n) \in \mathbb{Z}^\mathbb{n}, \mathbb{d}_\mathbb{1} > \ldots > \mathbb{d}_\mathbb{n} \ge \}$$

je báza A_n.

Lema 2.16. *Predpokladajme $d \in \mathbb{Z}^n$, $d_1 > \ldots > d_n \ge 0$. Definujme*

$$\lambda_i = d_i - (n - i),$$
$$\lambda = (\lambda_1, \ldots, \lambda_n),$$

alebo ekvivalentne

$$\lambda = d - \delta.$$

Potom λ je rozdelenie dĺžky $\leq n$.

Dôkaz. Dôkaz kvôli zdĺhavosti neuvádzame, ale je ho možné nájsť v [8]. □

Definícia 2.17. *Pre $\alpha \in P(k,n)$ je Schurov polynóm zodpovedajúci λ definovaný*

$$s_\lambda(x_1, \ldots, x_n) = \frac{A_{\lambda+\delta}(x_1, \ldots, x_n)}{A_\delta(x_1, \ldots, x_n)}.$$

Veta 2.18. *Pre kladné celé číslo*

$$\{s_\lambda \mid \lambda \in P(k,n)\}$$

je báza Λ_n^k.

Dôkaz. Dôkaz je možné nájsť v [8]. □

Veta 2.19. *Generujúci rad Schurových polynómov je rad tvaru*

$$S(x_1, \ldots, x_n, y_1, \ldots, y_n) = \sum_{d_1,\ldots,d_n \geq 0} \frac{1}{\Delta(x_1, \ldots, x_n)} \begin{vmatrix} x_1^{d_1} & \ldots & x_1^{d_n} \\ \vdots & \vdots & \vdots \\ x_n^{d_1} & \ldots & x_n^{d_n} \end{vmatrix} y_1^{d_1} \ldots y_n^{d_n}.$$

Dôkaz. Dôkaz k nahliadnutiu sa nachádza v [8]. □

Označme $\forall \lambda \in P(k,n)$ koeficient

$$\prod_{j=1}^{n} y_j^{\lambda_j + n - j} \in S(x_1, \ldots, x_n, y_1, \ldots, y_n)$$

ako $s_\lambda(x_1, \ldots, x_n)$. Nie je ťažké ukázať, že platí

$$S(x_1, \ldots, x_n, y_1, \ldots, y_n) = \Delta(y_1, \ldots, y_n) \sum_{l(\lambda) \leq n} s_\lambda(x) s_\lambda(y),$$

$$S(x_1, \ldots, x_n, y_1, \ldots, y_n) = \frac{\Delta(y_1, \ldots, y_n)}{\prod_{1 \leq i,j \leq n} (1 - x_i y_j)}.$$

Dôsledok 2.20. *Po dosadení a upravení dvoch predchádzajúcich generujúcich radov dostávame*

$$\frac{1}{\prod_{1 \leq i,j \leq n} (1 - x_i y_j)} = \sum_{l(\lambda) \leq n} s_\lambda(x) s_\lambda(y). \, [8]$$

3 Aplikácie symetrických polynómov

3.1 Vzťah medzi základnými symetrickými polynónmy a Newtonovými polynónmy

Ak chceme vyjadriť Newtonove polynómy

$$p_r(x_1, \ldots, x_n) = x_1^r + \ldots + x_n^r y$$

pomocou polynómov, ktoré závisia od základných symetrických polynómov $e_1, e_2, \ldots, e_n$, tak dostaneme rekurentné vzťahy, ktoré nazývame Newtonove vzorce.

Veta 3.1. *Newtonove vzorce sú vzorce tvaru*

$$p_r - p_{r-1}e_1 + \ldots + (-1)^{r-1}p_1 e_{r-1} + (-1)^r r e_r = 0;\ ak\ 1 \leq r \leq n, \tag{4}$$

$$p_r - p_{r-1}e_1 + \ldots + (-1)^{n-1}p_{r-n+1}e_{n-1} + (-1)^n p_{r-n}e_n = 0;\ ak\ r > n. \tag{5}$$

Dôkaz. Aby sme ich dokázali využijeme nasledovný vzťah

$$x_i^n - e_1 x_i^{n-1} + \ldots + (-1)^{n-1}e_{n-1}x_i + (-1)^n e_n = 0,$$

ktorý vynásobíme číslom $x_i^{r-n}, (r \geq n)$ a dostaneme

$$x_i^r - e_1 x_i^{r-1} + \ldots + (-1)^{n-1}e_{n-1}x_i^{r-n+1} + (-1)^n e_n x_i^{r-n} = 0.$$

Po sčítaní všetkých týchto vzťahov cez všetky $i = 1, \ldots, n$ dostaneme nielen vzťah (4), ale aj vzťah (5) pre $r = n$ ($p_0 = x_1^0 + \ldots + x_n^0 = n$). Ďalej si všimnime symetrický polynóm $f_{r,n}$, $\quad st(f_{r,n}) = r \leq n \quad$ (alebo $st(f_{r,n}) = -\infty$, ak $f_{r,n} = 0$):

$$f_{r,n}(x_1, \ldots, x_n) = p_r - p_{r-1}e_1 + \ldots + (-1)^{r-1}p_1 e_{r-1} + (-1)^r r e_r.$$

Matematickou indukciou podľa $q = n - r$ dokážeme, že $f_{r,n}$ je identicky rovný 0. Ak položíme $x_n = 0$, tak si môžeme všimnúť, že symetrické polynómy, ktoré dostaneme $(e_i)_{(0)}, (p_i)_{(0)}$ sú rovné polynómom e_i, p_i, ktoré sú definované pre $n-1$ premenných $x_1, \ldots, x_{n-1}$. Potom dostaneme rovnosť

$$\begin{aligned} f_{r,n}(x_1, \ldots, x_{n-1}, 0) &= (p_r)_0 - (p_{r-1})_0(e_1)_0 + \ldots + (-1)^{r-1}(p_1)_0(e_{r-1})_0 + (-1)^r r(e_r)_0 \\ &= f_{r,n-1}(x_1, \ldots, x_{n-1}) = 0, \end{aligned}$$

pretože $n - 1 - r = q - 1 < q$.

Vzťah $f_{r,n}(x_1, \ldots, x_{n-1}, 0) = 0$ znamená, že polynóm $f_{r,n}$ je deliteľný x_n, to znamená, že $f_{r,n} = x_n f_1$. Ak využijeme symetriu $f_{r,n}$ prídeme k záveru, že tento polynóm obsahuje ako činitele $x_1, \ldots, x_n$ a teda aj ich súčin $e_n = x_1 \ldots x_n$. Povedané inými slovami platí,

$$f_{r,n}(x_1, \ldots, x_n) = e_n(x_1, \ldots, x_n)h(x_1, \ldots, x_n).$$

Tento rozklad je možný jedine vtedy, ak $h = 0$, pretože $st(e_n) = n$ a $st(f_{r,n}) = r < n$. Teda $f_{r,n} = 0$ a tým je naša veta dokázaná. [4] □

3.2 Diskriminant polynómu

V okruhu $P[x_1, \ldots, x_n]$ budeme skúmať polynóm

$$\Delta_n = \prod_{1 \leq j < i \leq n} (x_i - x_j),$$

ktorý vyjadríme v tvare Vandermondovho determinantu

$$\Delta_n = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ x_1 & x_2 & \ldots & x_n \\ \vdots & \vdots & \vdots & \vdots \\ x_1^{n-1} & x_2^{n-1} & \ldots & x_n^{n-1} \end{vmatrix}.$$

Pretože determinant je kososymetrická funkcia svojich stĺpcov, dostávame

$$\sigma \circ \Delta_n = \varepsilon_\sigma \Delta_n$$

kde ε_σ je znamienko permutácie $\sigma \in 1, \ldots, n$. V takomto prípade Δ_n^2 je symetrický polynóm, a podľa základnej vety a symetrických polynómoch ho môžeme vyjadriť v tvare polynómu, ktorý závisí len od základných symetrických polynómov

$$\Delta_n^2 = \prod (x_i - x_j)^2 = Dis(e_1, \ldots, e_n).$$

Polynóm Dis s premennými $e_1(x_1, \ldots, x_n), \ldots, e_n(x_1, \ldots, x_n)$ budeme nazývať **diskriminantom premenných** $x_1, \ldots, x_n$. Jeho koeficienty, ako vidno patria do množiny $\mathbb{Z}$. Ak nie všetky hodnoty $x_1, \ldots, x_n$ sú rôzne, potom tento diskriminant je rovný 0, pretože aspoň jeden z činiteľov $x_i - x_j$ bude rovný 0. Tým pádom sa nám objasňuje,

prečo polynóm Dis nazývame diskriminantom.

Vhodný spôsob ako vypočítať tento diskriminant je založený na interpretácii Δ_n^2 ako súčinu Vandermondovho determinantu a jeho transpozície.

$$\Delta_n^2 = \Delta_n \Delta_n^T.$$

Ak využijeme vlastnosti násobenia matíc, dostaneme

$$Dis(e_1, \ldots, e_n) = \begin{vmatrix} n & p_1 & p_2 & \ldots & p_{n-1} \\ p_1 & p_2 & p_3 & \ldots & p_n \\ p_2 & p_3 & p_4 & \ldots & p_{n+1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{n-1} & p_n & p_{n+1} & \ldots & p_{2n-2} \end{vmatrix}, \tag{6}$$

kde p_r sú známe Newtonove polynómy. Ak vyjadríme p_r pomocou rekurentných vzťahov (4), (5) dostaneme hodnotu $Dis(e_1, \ldots, e_n)$.

Príklad 3.1 Dané sú prvé dva Newtonove polynómy vyjadrené pomocou základnych symetrických polynómov

$$p_1 = e_1$$
$$p_2 = e_1^2 - 2e_2,$$

a chceme vypočítať hodnotu $Dis(e_1, e_2)$. Potom

$$Dis(e_1, e_2) = \begin{vmatrix} 2 & e_1 \\ e_1 & e_1^2 - 2e_2 \end{vmatrix} = e_1^2 - 4e_2.$$

Nech je daný normovaný polynóm tvaru

$$f(x) = x^n + a_1 x^{n-1} + \ldots + a_{n-1} x + a_n \in P[x],$$

ktorý má v danom poli Λ_n n koreňov $c_1, \ldots, c_n$. Ako vieme z Vietových vzťahov

$$a_r = (-1)^r e_r(c_1, \ldots, c_n).$$

Definícia 3.2. *Diskriminant množiny koreňov $c_1, \ldots, c_n$ polynómu f, alebo čo je to isté ako $Dis(e_1, \ldots, e_n)$, ktorý dostaneme zámenou $(-1)^r a_r$ namiesto e_r, nazývame diskriminantom polynómu f a označujeme $D(f)$. Niekedy tiež hovoríme o diskriminante algebraickej rovnice (6). Je zrejmé, že $D(f) \in P$.*

Z Definície 3.2 vyplýva nasledovná veta.

Veta 3.3. *$D(f) = 0$ práve vtedy, keď rovnica (6) má násobné korene (aspoň jeden koreň má násobnosť > 1).*

Dôkaz. Dôkaz sa dá nájsť v [4]. □

Príklad 3.2 Chceme vypočítať diskriminant pre neúplný kubický polynóm

$$f(x) = x^3 + ax + b = 0.$$

Vypočítame si prvé štyri Newtonove polynómy v základných symetrických polynómoch

$$\begin{aligned} p_1 &= e_1 = 0, \\ p_2 &= e_1^2 - 2e_2 = -2a, \\ p_3 &= e_1^3 - 3e_1e_2 + 3e_3 = -3b, \\ p_4 &= e_1^4 - 4e_1^2e_2 + 4e_1e_3 + 2e_2^2 = 2a^2 \end{aligned}$$

a dosadíme do diskriminantu $D(f)$

$$D(f) = \begin{vmatrix} 3 & 0 & -2a \\ 0 & -2a & -3b \\ -2a & -3b & 2a^2 \end{vmatrix} = -4a^3 - 27b^2.$$

Príklad 3.3 Vypočítame diskriminant pre normovaný kvartický polynóm.

$$x^4 + ax^3 + bx^2 + cx + d = 0$$

Polynóm prevedieme na neúplny tvar, t.j. zaveďme substitúciu

$$y = x - \frac{a}{4} \quad \Rightarrow \quad y^4 + py^2 + qy + r = 0,$$

kde

$$\begin{aligned} p &= \frac{8b - 3a^2}{8}, \\ q &= \frac{a^3 - 4ab + 8c}{8}, \\ r &= \frac{-3a^4 + 256d - 64ac^2 + 16a^2b}{256}. \end{aligned}$$

Vypočítame si prvých šesť Newtonových polynómov v základných symetrických polynómoch

$$
\begin{aligned}
p_1 &= e_1 = 0,\\
p_2 &= e_1^2 - 2e_2 = -2p,\\
p_3 &= e_1^3 - 3e_1e_2 + 3e_3 = -3q,\\
p_4 &= e_1^4 - 4e_1^2e_2 + 4e_1e_3 + 2e_2^2 = 2p^2,\\
p_5 &= e_1^5 - 5e_1^3e_2 + 5e_1^2e_3 + 5e_1e_2^2 - 5e_4e_1 - 5e_2e_3 + 5e_5 = 5pq,\\
p_6 &= e_1^6 - 6e_1^4e_2 + 6e_1^3e_3 + 9e_1^2e_2^2 - 6e_1^2e_4 - 12e_1e_2e_3 + 6e_1e_5 - 2e_2^3 + 3e_3^2 + 6e_2e_4 - 6e_6\\
&= 9q^2 - 8p^3 + 6pr
\end{aligned}
$$

a dosadíme do diskriminantu $D(f)$

$$
D(f) = \begin{vmatrix}
4 & 0 & -2p & -3q\\
0 & -2p & -3q & 2p^2\\
-2p & -3q & 2p^2 & 5pq\\
-3q & 2p^2 & 5pq & 9q^2 - 8p^3 + 6pr
\end{vmatrix} = 24p^6 + 26p^3q^2 - 81q^4 - 24p^4r - 54pq^2r.
$$

Po dosadení pôvodných premenných získame diskriminant pre kvartický polynóm, ktorý ako vidíme je veľmi zložitý.

3.3 Rezultant

Základná vlastnosť diskriminantu $D(f)$, ktorú sme sformulovali v predchádzajúcej vete môžeme interpretovať ako príznak existencie spoločných koreňov (spoločných činiteľou) pre polynóm f a jeho deriváciu f'. Podstata tohoto príznaku je v Euklidovom algoritme. Na základe tohoto môžeme predpokladať, že existuje analogické kritérium, ktoré bez problémov umožňuje na základe koeficientov ľubovoľných dvoch polynómov $f, q \in K[x]$ zodpovedať na otázku, či majú spoločného deliteľa. Nech

$$
\begin{aligned}
f(x) &= a_0x^n + a_1x^{n-1} + \ldots + a_{n-1}x + a_n,\\
g(x) &= b_0x^n + b_1x^{n-1} + \ldots + b_{m-1}x + b_m,
\end{aligned}
$$

sú dva polynómy z poľa K. V tomto prípade pre $n > 0, m > 0$ nevylučujeme prípady že $a_n = 0 \vee b_n = 0$.

Definícia 3.4. *Rezultantom $Res(f,g)$ polynómov f a g nazývame polynóm závislý od ich koeficientov*

$$Res(f,g) = \begin{vmatrix} a_0 & a_1 & \dots & \dots & a_n & & \\ & a_0 & a_1 & \dots & \dots & a_n & \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ & & & a_0 & a_1 & \dots & a_n \\ b_0 & b_1 & \dots & \dots b_m & & & \\ & b_0 & b_1 & \dots & \dots & b_m & \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots \\ & & & b_0 & b_1 & \dots & b_m \end{vmatrix}.$$

V nasledujúcej vete ukážeme základnú vlastnosť rezultanta.

Veta 3.5. *$Res(f,g) = 0$ práve vtedy, keď $a_0 = 0 = b_0$ alebo polynómy f, g majú spoločný deliteľ v $K[x]$, ktorého stupeň deliteľa je > 0.*

Dôkaz. Najprv ukážeme platnosť tejto vety v prípade, že $a_0 = 0 = b_0$, t.j. f a g majú spoločného deliteľa $d(x) \in K[x]$, $st(d(x)) > 0$ je splnené práve vtedy, keď nájdeme také polynómy f_1, g_1, ktoré nie sú súčasne rovné 0, a pre ktoré platí

$$fg_1 + f_1 g = 0; \quad st(f_1) < n, \quad st(g_1) < m. \tag{7}$$

najväčší spoločný deliteľ polynómov f, g označme ako

$$h = (f,g), \quad \text{kde } st(h) > 0$$

Potom platia nasledovné rovnosti

$$f = hf_1,$$
$$g = -hg_1,$$

a teda $fg_1 + gf_1 = 0$. Okrem toho $st(f_1) < n$ a $st(g_1) < m$, to znamená, že platí (7). Ak $a_0 = 0 = b_0$, potom môžeme dosadiť

$$f_1 = f,$$
$$g_1 = -g.$$

Naopak, ak predpokladáme, že platí (7), potom $(f, g) = 1$ na základe čoho platí

$$fg_1 = -gf_1 \quad \Rightarrow \quad f/f_1, g/g_1, \text{a teda} \quad st(f) < n, \quad st(g) < m \quad \Rightarrow \quad a_0 = 0 = b_0.$$

Všeobecne ukážeme, že z (7) vyplýva $Res(f, g) = 0$. Nech

$$f_1 = c_0x^{n-1} + c_1x^{n-2} + \ldots + c_{n-1}, g_1 = d_0x^{m-1} + d_1x^{m-2} + \ldots + d_{m-1}.$$

Vypočítame koeficienty polynómu $fg_1 + f_1g$, $st(fg_1 + f_1g) \leq n+m-1$. Podmienku (7) môžeme zapísať v tvare homogénneho systému lineárnych rovníc s $n + m$ premennými $d_0, d_1, \ldots, d_{m-1}, c_0, c_1, \ldots, c_{n-1}$ ako

$$\begin{aligned}
&a_0d_0+ && \ldots + b_0c_0 \ldots = 0,\\
&a_1d_0 + a_0d_1+ && \ldots + b_1c_0 + b_0c_1 \ldots = 0,\\
&a_2d_0 + a_1d_1 + a_0d_2 && \ldots + b_2c_0 + b_1c_1 + b_0c_2 = 0,\\
&\ldots\ldots\ldots\ldots
\end{aligned} \tag{8}$$

Determinant matice tohoto systému, alebo presnejšie povedané determinant transponovanej matice je rovný presne $Res(f, g)$. Z toho vyplýva, že systém rovníc (8) má nenulové riešenie práve vtedy, keď $Res(f, g) = 0$ a každé nenulové riešenie dáva dvojicu polynómov, ktoré zodpovedajú podmienke (7). [4] □

Veta 3.6. *Nech polynómy f a g vyjadríme ako súčin lineárnych činiteľov v okruhu $K[x]$*

$$f(x) = a_0(x - \alpha_1) \ldots (x - \alpha_n),$$
$$g(x) = b_0(x - \beta_1) \ldots (x - \beta_m).$$

Potom platí, že

$$Res(f, g) = a_0^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_0^n \prod_{j=1}^{m} f(\beta_j) =$$
$$= a_0^m b_0^n \prod_{i,j} (\alpha_i - \beta_j).$$

Dôkaz. Predpokladajme najvšeobecnejší prípad, že všetky $g(\alpha_1), \ldots, g(\alpha_n)$ a všetky $f(\beta_1), \ldots, f(\beta_m)$ sú navzájom rôzne. Pretože platí $Res(g, f) = (-1)^{mn} Res(f, g)$, tak sa stačí prevedčiť o správnosti vzťahu $Res(f, g) = a_0^m \prod g(\alpha_i)$. Kvôli tomu zavedieme

novú premennú y a budeme uvažovať polynómy $f(x), g(x)-y$. Z definície (3.4) musíme zameniť b_m na $b_m - y$, čím dostávame

$$Res(f, g - y) = (-1)^n a_0^m y^n + \ldots + Res(f, g),$$

čo je polynóm premennej y, ktorého $st(Res(f, g - y)) = n$. Koeficient vedúceho člena je rovný $(-1)^n a_0^m$ a absolútny člen je rovný $Res(f, g)$. Polynóm $f(x)$ a $(g(x) - g(\alpha_i))$ s ľubovoľným koreňom α_i je deliteľný na $x - \alpha_i$. Na základe predchádzajúcej vety dostaneme, že $Res(f, g - g(\alpha_i)) = 0$. Okrem toho polynóm $Res(f, g - y)$ musí byť deliteľný polynómom $g(\alpha_i) - y; 1 \leq i \leq n$. Pretože všetky $g(\alpha_i)$ sú rôzne tak potom platí

$$Res(f, g - y) = a_0^m \prod_{i=1}^{n} (g(\alpha_i) - y).$$

Pre $y = 0$ dostaneme tvrdenie Vety 3.6. [4] □

Uvažujeme prípad nenormovaného polynómu. Potom definujeme diskriminant ako

$$D(f) = a_0^{2n-2} \prod_{1 \leq j < i \leq n} (\alpha_i - \alpha_j)^2 = [a_0^{n-1} \prod_{j<i} (\alpha_i - \alpha_j)]^2; \; a_0 \neq 0.$$

Veta 3.7. *Pre diskriminant platí nasledujúci vzťah*

$$D(f) = (-1)^{n(n-1)/2} a_0^{-1} Res(f, f'). \tag{9}$$

Dôkaz. Podľa vety (3.6) platí

$$Res(f, f') = a_0^{n-1} \prod_{i=1}^{n} f'(\alpha_i).$$

Ale platí, že

$$f'(\alpha_i) = a_0 \prod_{j \neq i} (\alpha_i - \alpha_j),$$

čo je vlastne jednoduchým dôsledkom zámeny $x = \alpha_i$ vo vzorci

$$f'(x) = a_0 \sum_{i=1}^{n} \prod_{j \neq i} (x - \alpha_j),$$

ktorý dostaneme deriváciou súčinu $f(x) = a_0 \prod_{j=1}^{n}(x - \alpha_j)$. Z toho vyplýva, že

$$Res(f, f') = a_0^{2n-1} \prod_{i=1}^{n} \prod_{j \neq i} (\alpha_i - \alpha_j) =$$

$$= a_0(-1)^{n(n-1)/2} a_0^{2n-2} \prod_{j<i} (\alpha_i - \alpha_j)^2 = a_0(-1)^{n(n-1)/2} D(f).[4]$$

□

Vzťah (9) je explicitným vyjadrením diskriminantu ľubovoľného nenormovaného polynómu.

Záver

Cieľom tejto bakalárskej práce bolo priblížiť čitateľovi teóriu polynómov a aplikácii symetrických polynómov pri hľadaní koreňov polynómov. Vysvetlili sme základné algebraické štruktúry, uviedli sme základné vlastnosti polynómov a ukázali rozklad polynómu na ireducibilné činitele. Na konci prvej kapitoly sme uviedli najznámejšie postupy na riešenie všeobecných polynomických rovníc stupňov 2., 3. a 4. Ďalej sme spravili úvod do symetrických polynómov, zaviedli dôležité tvrdenia a ukázali špeciálne tvary symetrických funkcií (Newtonove polynómy, Schurov polynóm). Nakoniec sme aplikovali všetky získané poznatky a ukázali, že diskriminant a rezultant polynómov závisí od symetrických polynómov.

Prínosom tejto práce, nielen pre čitateľa, ktorý nemusí byť vo vzťahoch polynómov a symetrických polynómov odborník, je detailné spracovanie problematiky, a aj uvádzanie ilustračných príkladov, ktoré danú problematiku uvedú na správnu mieru.

Veľkým prínosom pre autora nebolo iba prehĺbenie poznatkov o polynómoch a ich vzťahoch, ale aj získanie skúsenosti s prácou v LaTeX a písanie samotnej bakalárskej práce.

Túto prácu odporúčam všetkým, ktorý si chcú rozšíriť svoje vedomosti a polynómoch.

Zoznam použitej literatúry

[1] Birkhoff, G., Bartee, T. O.: *Aplikovaná algebra*, Alfa, Bratislava, 1985

[2] Irving, R. S.: *Integers, Polynomials, And Rings*, Springer, Seattle, 2004

[3] Katriňák, T. a kol.: *Algebra a teoretická aritmetika*, Polygrafické stredisko UK, Bratislava, 2002

[4] Kostrikin, A. I.: *Introduction to algebra*, Springer - Verlag, New York, 1982

[5] Lang, S.: *Algebra*, Springer - Verlag, New York, 2002

[6] Macdonald, I. G.: *Symmetric Function and Hall Polynomials*, Clarendon Press, Oxford, 1995

[7] Vinberg, E. B.: *A course in algebra*, Clarendon Press, Oxford, 1995

[8] Zhou, J.: *Introductions to symmetric polynomials and symmetric functions*, učebné texty, dostupné na internete (30.05.2014):
http://faculty.math.tsinghua.edu.cn/~jzhou/SymmetricF.pdf