Predslov

Učebný text je určený pre študentov učiteľského štúdia v kombinácii s matematikou. Jeho cieľom je oboznámiť študentov so základnými poznatkami o polynómoch a algebraických rovniciach. Je pokračovaním skrípt Úvod do štúdia matematiky (1996) a Algebra I (1998).

Pri výbere učiva sme mali na zreteli, aby získané vedomosti a najmä metódy práce mohli študenti, budúci učitelia, využiť vo svojej praxi.

Text sme rozdelili na dve (klasické) kapitoly. V prvej sa venujeme základným poznatkom o polynómoch a v druhej riešeniu niektorých typov algebraických (polynomických) rovníc. Kapitoly sú rozdelené na niekoľko článkov. Okrem posledného sú všetky ostatné doplnené cvičeniami a slúžia hlavne na samostatnú prácu.

Jednotlivé položky, ako definície, lemy, vety, dôsledky a príklady sú číslované priebežne číslom článku a poradovým číslom položky v článku. V prípade, ak sa budeme odvolávať na položku inej kapitoly, tak to výslovne uvedieme.

Ďakujem recenzentom za ich cenné pripomienky a návrhy. Srdečne ďakujem aj všetkým ostatným, ktorí pomohli pri realizácii tohoto textu. Ďalšie pripomienky, návrhy a podnety je možné poskytnúť napr. e-mailom na adresu **klenovca@pdf.umb.sk**.

Banská Bystrica, november 2000

autor

I. OKRUHY POLYNÓMOV

Počítanie s mnohočlenmi (polynómami) tvaru

$$a_0 + a_1 x + \cdots + a_n x^n$$

sa využíva už aj na základnej a strednej škole. Na takýto mnohočlen sa môžeme dívať buď ako na funkciu určitého typu alebo ako na algebraický výraz (pozri aj v [2], str. 65). V tejto kapitole sa budeme zaoberať hlavne deliteľnosťou polynómov, ich rozkladmi, koreňmi a polynómami viacerých neurčitých.

1 Polynómy jednej neurčitej a jednej premennej

Vieme už, že okruh polynómov jednej neurčitej nad okruhom A je okruh, ktorý vznikne adjunkciou transcedentného prvku x k okruhu A (pozri [2]). Označujeme ho $A[x]$. Jeho prvky nazývame *polynómy jednej neurčitej nad okruhom* A a budeme ich často označovať f_x, g_x, a_x (alebo skrátene f, g, a) a pod.

Nech

$$f_x = a_0 + a_1 x + \cdots + a_n x^n, \tag{1}$$

kde $a_0, a_1, \ldots, a_n \in A$, $n \in N$. Prvky $a_0, a_1, \ldots, a_n$ nazývame *koeficienty* polynómu f_x. Ak $a_n \neq 0$, tak koeficient a_n voláme *vedúcim koeficientom* a číslo n *stupňom* polynómu f_x. Ak stupeň polynómu f_x je n, tak píšeme $\operatorname{st} f_x = n$. Stupeň nulového polynómu definujeme ako $-\infty$. Každý nenulový prvok okruhu A je polynóm nultého stupňa. Ak je polynóm zapísaný v tvare (1), t.j. každá mocnina x^i sa v zápise nachádza najviac raz hovoríme, že polynóm je zapísaný v *normálnom tvare*. Polynóm, ktorého vedúci koeficient $a_n = 1$ sa nazýva *normovaný* polynóm.

Pripomeňme, že dva polynómy

$$f_x = a_0 + a_1 x + \cdots + a_r x^r, \quad g_x = b_0 + b_1 x + \cdots + \cdots + b_s x^s$$

z okruhu $A[x]$ (t.j. z okruhu polynómov jednej neurčitej nad okruhom A) sa rovnajú, ak majú rovnaký stupeň a ak odpovedajúce koeficienty sa rovnajú, teda

$$f_x = g_x \quad \text{práve vtedy, keď} \quad r = s \text{ a } a_i = b_i \quad \text{pre} \quad i = 1, 2, \ldots, r \tag{R}$$

a že súčtom polynómov

$$f_x = a_0 + a_1 x + \cdots + a_r x^r, \quad g_x = b_0 + b_1 x + \cdots + b_s x^s, \quad r \geq s$$

je polynóm

$$f_x + g_x = (a_0 + b_0) + (a_1 + b_1)x + \cdots + (a_s + b_s)x^s + a_{s+1}x^{s+1} + \cdots + a_r x^r \tag{S}$$

a ich súčinom je polynóm

$$f_x \cdot g_x = c_0 + c_1 x + \cdots + c_{r+s} x^{r+s}, \tag{N}$$

kde $c_k = \sum_{i=0}^{k} a_i b_{k-i}$, pre $k \in \{0, 1, \ldots, r+s\}$.

V tejto časti sa budeme najčastejšie zaoberať polynómami nad poľom F (t.j. okruhom polynómov $F[x]$, kde F je pole).

1.1 Poznámka. Ak napríklad $f_x \in C[x]$ a všetky jeho koeficienty sú celé čísla často hovoríme, že f_x je polynóm s celočíselnými koeficientami (nad poľom C). Podobne hovoríme o polynómoch s racionálnymi, reálnymi alebo komplexnými koeficientami. Ak zadáme (napr. v cvičení) polynóm s číselnými koeficientami, tak ho považujeme (ak neuvedieme inak) za polynóm nad vhodným číselným poľom.

Z vlastností súčtu a súčinu polynómov vyplýva nasledovné tvrdenie (podrobne sa presvedčte).

1.2 Lema. *Nech A je obor integrity a nech $f_x, g_x \in A[x]$. Potom*
a) $\mathrm{st}(f_x + g_x) \leq \max(\mathrm{st}\, f_x, \mathrm{st}\, g_x)$,
b) ak $\mathrm{st}\, f_x \geq 0$, $\mathrm{st}\, g_x \geq 0$, *tak* $\mathrm{st}(f_x \cdot g_x) = \mathrm{st}\, f_x + \mathrm{st}\, g_x$.

1.3 Veta. *a) Ak A je obor integrity, tak aj $A[x]$ je obor integrity.*
b) Ak F je pole, tak $F[x]$ je obor integrity, ale nie je pole.

Dôkaz. a) Nech $f_x, g_x \in A[x]$, $f_x \neq 0, g_x \neq 0$, t.j. $\mathrm{st}\, f_x \geq 0, \mathrm{st}\, g_x \geq 0$. Potom, podľa lemy 1.2, $\mathrm{st}(f_x \cdot g_x) \geq 0$, teda $f_x \cdot g_x \neq 0$, čo znamená, že $A[x]$ je obor integrity.

b) Každé pole F je oborom integrity a z a) potom vyplýva, že $F[x]$ je oborom integrity. Dokážeme (sporom), že $F[x]$ nie je pole. Predpokladajme, že $F[x]$ je pole. Potom ku každému nenulovému prvku $f_x \in F[x]$ existuje inverzný prvok $(f_x)^{-1} \in F[x]$. Nech $f_x \in F[x]$ a $\mathrm{st}\, f_x \geq 1$. Potom $f_x \cdot (f_x)^{-1} = 1$ a teda $\mathrm{st}(f_x \cdot (f_x)^{-1}) = \mathrm{st}\, 1$. Z lemy 1.2 ale vyplýva, že $\mathrm{st}(f_x \cdot (f_x)^{-1}) = \mathrm{st}\, f_x + \mathrm{st}(f_x)^{-1} \geq 1$, čo je spor, lebo $\mathrm{st}\, 1 = 0$.

Nech F je pole. *Polynomickou funkciou (polynómom) jednej premennej nad poľom F* voláme funkciu $f : F \to F$ danú predpisom

$$\forall x \in F \qquad f(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

kde $n \in N$, $a_0, a_1, \ldots, a_n \in F$, $a_n \neq 0$ ak $n > 0$.

Množinu všetkých takýchto funkcií budeme označovať $F\langle x\rangle$. Symbolom $f(x)$ budeme často (tak ako je to obvyklé) označovať nielen funkčnú hodnotu v bode x ale aj samotnú funkciu f.

Dve polynomické funkcie $f, g \in F\langle x\rangle$ sa rovnajú, ak

$$\forall t \in F \qquad f(t) = g(t).$$

Súčet $f + g$ a súčin $f \cdot g$ polynomických funkcií f, g sa definuje obvyklým spôsobom:

$$\begin{aligned} &\forall t \in F \qquad (f+g)(t) = f(t) + g(t), \\ &\forall t \in F \qquad (f \cdot g)(t) = f(t) \cdot g(t). \end{aligned} \tag{1}$$

Vidíme teda, že polynómy jednej neurčitej a jednej premennej sa formálne (zápismi) nelíšia, líšia sa len tým, že ich chápeme buď ako algebraické výrazy (termy) alebo ako funkcie. Preto aj pojmy stupeň polynómu, koeficienty polynómu a pod. budeme používať aj u polynómov jednej premennej tak, ako u polynómov jednej neurčitej. Každému polynómu jednej neurčitej môžeme teda priradiť jednoznačne polynóm jednej premennej nasledovným spôsobom:

$$\text{ak } f_x = a_0 + \cdots + a_n x^n \in F[x], \text{ tak } \psi(f_x) = f(x) = a_0 + \ldots a_n x^n \in F\langle x\rangle.$$

Zobrazenie $\psi : F[x] \to F\langle x\rangle$ je zrejme surjektívne, ale nie je injektívne, lebo ak napr. $F = Z_3$ a ak $f_x = x^3 + x^2$, $g_x = x^2 + x \in F[x]$, tak $f_x \neq g_x$, ale $\psi(f_x) = \psi(g_x)$ lebo $f(0) = g(0) = 0$, $f(1) = g(1) = 2$ a $f(2) = g(2) = 0$. Ak teda uvedené polynómy $x^3 + x^2$, $x^2 + x$ chápeme ako polynómy jednej neurčitej nad poľom Z_3, tak sú to rôzne polynómy, ale ak ich chápeme ako polynómy jednej premennej (t.j. funkcie) nad poľom Z_3, tak sa rovnajú.

Nech $f_x = a_0 + a_1x + \cdots + a_rx^r$, $g_x = b_0 + b_1x + \cdots + \cdots + b_sx^s$, $r \geq s$. Potom

$$\begin{aligned}\psi(f_x + g_x) =& \psi((a_0 + b_0) + \cdots + (a_s + b_s)x^s + a_{s+1}x^{s+1} + \cdots + a_rx^r) = \\ =& (a_0 + b_0) + \cdots + (a_s + b_s)x^s + a_{s+1}x^{s+1} + \cdots + a_rx^r \in F\langle x\rangle, \\ \psi(f_x) + \psi(g_x) =& (a_0 + \cdots + a_rx^r) + (b_0 + \cdots + b_sx^s) \in F\langle x\rangle\end{aligned}$$

Ľahko sa môžeme presvedčiť (s využitím komutatívnosti a distributívnosti), že pre každé $t \in F$ je

$$(a_0+b_0)+\cdots+(a_s+b_s)t^s+a_{s+1}t^{s+1}+\cdots+a_rt^r = (a_0+\cdots+a_rt^r)+(b_0+\cdots+b_st^s),$$

z čoho už vyplýva, že

$$\psi(f_x + g_x) = \psi(f_x) + \psi(g_x).$$

Analogicky je možné ukázať, že aj

$$\psi(f_x \cdot g_x) = \psi(f_x) \cdot \psi(g_x).$$

Vidíme teda, že aj polynomické funkcie môžeme sčitovať a násobiť podobne ako polynómy jednej neurčitej pomocou vzťahou (S) a (N).

V [1], príklad 10.9 sme ukázali, že množina všetkých funkcií $f : R \to R$ so sčítaním a násobením definovanými „bodovo“ t.j. vzťahmi (1) (kde $F = R$) je okruh. Pretože súčet aj súčin polynomických funkcií je opäť polynomická funkcia, tak analogicky je možné ukázať, že množina $F\langle x\rangle$, s operáciami sčítania a násobenia, definovanými vzťahmi (1) je komutatívny okruh s nulovým prvkom $f(x) = 0$ aj jednotkovým prvkom $g(x) = 1$.

1.4 Príklad. nech $F = Z_2$. Ak označíme

$$f_0(x) = 0, \quad f_1(x) = 1, \quad f_2(x) = x, \quad f_3(x) = x + 1,$$

tak $Z_2\langle x\rangle = \{f_0(x), f_1(x), f_2(x), f_3(x)\}$. Podrobne to overte.

Cvičenia

1. Polynóm $f_x = (2x + i\sqrt{3})^2(3x - i\sqrt{2})^2 - (2x - i\sqrt{3})^2(3x + i\sqrt{2})^2$ (jednej neurčitej nad poľom C) zapíšte v normálnom tvare.
2. Nájdite polynóm $f \in C\langle x\rangle$, čo najnižšieho stupňa, pre ktorý platí
   a) $f(-1) = 6, \quad f(0) = 5, \quad f(1) = 4, \quad f(2) = 9,$
   b) $f(0) = 1 - i, \quad f(1 + i) = 1 + i, \quad f(1 - i) = 3 - i.$
3. Zistite, ktoré z nasledujúcich polynómov jednej premennej nad poľom Z_3 sa rovnajú: $f_1(x) = x^2 + x$, $f_2(x) = x^3 + x^2$, $f_3(x) = x^4 + 2x + 2$, $f_4(x) = 1$, $f_5(x) = x^4 + 2x^3 + x + 2$, $f_6(x) = x^3 + 2x + 1$.
4. Nech $f_x = 3x^4 + 5x^3 + 2x^2 + 3x + 4, \quad g_x = 2x^3 + 5x^2 + x + 2$. Nájdite ich súčet a súčin, ak:
   a) $f_x, g_x \in R[x]$, b) $f_x, g_x \in Z_7[x]$ c) $f_x, g_x \in Z_6[x]$.
5. Ukážte, že každé zobrazenie $f : Z_2 \to Z_2$ je polynomickou funkciou.
6. Napíšte všetky polynómy okruhu $Z_2[x]$ stupňa najviac tretieho. Koľko je všetkých polynómov stupňa najviac k-teho ($k \in N^+$)?

2 Deliteľnosť polynómov.

V tejto časti sa budeme zaoberať deliteľnosťou polynómov jednej neurčitej nad poľom F. Mnohé z vlastností a ich dôkazy sú analogické ako pri deliteľnosti celých čísel. Najprv uvedieme vetu o delení so zvyškom.

2.1 VETA. *Nech F je pole, $f, g \in F[x]$, $g \neq 0$. Potom existuje jediná dvojica polynómov $q, r \in F[x]$, o ktorej platí*

$$f = g \cdot q + r, \quad r = 0 \text{ alebo } \operatorname{st} r < \operatorname{st} g. \tag{1}$$

DÔKAZ. Existencia. Ak $f = 0$ alebo $\operatorname{st} f < \operatorname{st} g$ je $q = 0$, $r = f$. Nech $st f \geq \operatorname{st} g$. Dôkaz urobíme matematickou indukciou vzhľadom na stupeň polynómu f. Nech $f = a_n x^n + \cdots + a_1 x + a_0$.

a) Ak $n = 0$, tak $f = a \in F$, $g = b \in F$ (lebo $\operatorname{st} g \leq \operatorname{st} f$), $q = a \cdot b^{-1}$, $r = 0$.

b) Nech q, r existujú v prípade, keď $\operatorname{st} f < n$, $n > 0$ a nech $g = b_m x^m + \cdots + b_1 x + b_0$. Zvoľme polynóm f_1 takto:

$$f_1 = f - a_n \cdot b_m^{-1} \cdot g \cdot x^{n-m}. \tag{2}$$

Pretože $\operatorname{st} f_1(x) < n$ existujú podľa indukčného predpokladu polynómy q_1, r, pre ktoré platí

$$f_1 = g \cdot q_1 + r, \quad r = 0 \text{ alebo } \operatorname{st} r < \operatorname{st} g. \tag{3}$$

Po dosadení z (3) do (2) a úprave dostávame

$$f = g \cdot (q_1 + a_n \cdot b_m^{-1} \cdot x^{n-m}) + r.$$

Ak označíme $q = q_1 + a_n \cdot b_m^{-1} \cdot x^{n-m}$ dostaneme (1).

Jednoznačnosť. Ak $\operatorname{st} f < \operatorname{st} g$ alebo $f = 0$, tak jednoznačnosť je zrejmá. Nech $\operatorname{st} f \geq \operatorname{st} g$ a nech

$$f = g \cdot q_1 + r_1, \quad r_1 = 0 \text{ alebo } \operatorname{st} r_1 < \operatorname{st} g = m$$

a tiež

$$f = g \cdot q_2 + r_2, \quad r_2 = 0 \text{ alebo } \operatorname{st} r_2 < \operatorname{st} g = m.$$

Potom

$$g \cdot (q_1 - q_2) = r_2 - r_1$$

pričom $r_2 - r_1 = 0$ alebo $\operatorname{st}(r_2 - r_1) < m$. Ak $q_1 - q_2 \neq 0$, tak $\operatorname{st}(g \cdot (q_1 - q_2)) \geq m$ a to je spor. Preto $q_1 = q_2$, z čoho vyplýva, že aj $r_1 = r_2$.

Polynóm r vo vzťahu (1) voláme *zvyšok* pri delení polynómu f polynómom g a polynóm q voláme *(čiastočný) podiel*.

Pri konkrétnom výpočte určíme jednotlivé členy podielu tak, aby rozdiel $f - g \cdot q$ bol zvyšok r, ktorý je buď nulovým polynómom, alebo $\operatorname{st} r < \operatorname{st} g$. Prakticky nájdeme podiel q a zvyšok r tak, že od polynómu f odčítame postupne vhodné násobky deliteľa g (všimnite si vzťah (2) v dôkaze predchádzajúcej vety), až kým stupeň rozdielu („zvyšku“) nie je menší ako stupeň polynómu g. Podrobne si všimnite riešenie nasledujúceho príkladu.

2.2 Príklad. Dané sú dva polynómy nad poľom reálnych čísel,

$$f_x = 2x^5 - 6x^4 + 3x^3 - 3x^2 - 3x + 2, \quad g_x = 2x^3 + 2x + 1.$$

Určte podiel q_x a zvyšok r_x, ktoré dostaneme pri delení polynómu f_x polynómom g_x.

Riešenie.

$$\begin{array}{l}
2x^5 - 6x^4 + 3x^3 - 3x^2 - 3x + 2 : 2x^3 + 2x + 1 = x^2 - 3x + \frac{1}{2} \\
-2x^5 \qquad -2x^3 \quad -x^2 \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\qquad -6x^4 \quad +x^3 - 4x^2 - 3x + 2 \\
\qquad\ \ 6x^4 \qquad\ \ +6x^2 + 3x \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\qquad\qquad\ \ x^3 + 2x^2 \qquad\ \ +2 \\
\qquad\qquad -x^3 \qquad\ \ -x - \frac{1}{2} \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\qquad\qquad\qquad\ \ 2x^2 \quad -x + \frac{3}{2}
\end{array}$$

Teda

$$q_x = x^2 - 3x + \frac{1}{2}, \quad r_x = 2x^2 - x + \frac{3}{2}.$$

Nech f, g sú polynómy jednej neurčitej nad poľom F. Budeme hovoriť, že f *delí* g (v okruhu $F[x]$ alebo nad poľom F) a písať $f \mid g$, ak existuje taký polynóm $q \in F[x]$, že $g = f \cdot q$.

Ľahko je možné (podobne ako pri deliteľnosti celých čísel) overiť nasledovné tvrdenie.

2.3 Lema. *Nech F je pole a nech f, g, $q \in F[x]$. Potom*

a) $1 \mid f \quad f \mid 0$ *pre každé* $f \in F[x]$.

b) Ak $f \mid g$, $g \mid q$ *tak* $f \mid q$.

c) Ak $f \mid g$, $f \mid q$ *tak* $f \mid u \cdot g + v \cdot q$ *pre ľubovoľné* $u, v \in F[x]$.

Budeme hovoriť, že polynómy f, g jednej neurčitej nad poľom F sú *asociované* a písať $f \sim g$, ak $f \mid g$ a $g \mid f$.

2.4 Lema. *Nech f, g sú polynómy jednej neurčitej nad poľom F. Potom $f \sim g$ práve vtedy, keď existuje nenulový prvok $c \in F$ (t.j. polynóm nultého stupňa), že $f = c \cdot g$.*

Dôkaz. Nech $f \sim g$. Ak $f = 0$, tak aj $g = 0$ a $0 = c \cdot 0$, $c \in F$. Nech $f \neq 0$. Potom (pretože $f \sim g$) $g = f \cdot h_1$, $f = g \cdot h_2$. Po dosadení dostávame $f = f \cdot (h_1 \cdot h_2)$, z čoho vyplýva (pretože v obore integrity je možné krátiť) $h_1 \cdot h_2 = 1$ čo znamená, že $\operatorname{st} h_1 = \operatorname{st} h_2 = 0$ a teda polynómy h_1, h_2 sú vlastne prvky poľa F.

Naopak, nech $f = c \cdot g$, $c \neq 0$. Potom $g \mid f$. Pretože $c \neq 0$ a F je pole, tak $c^{-1} \cdot f = c^{-1} \cdot c \cdot g$. Teda $g = c^{-1} \cdot f$, čo znamená, že aj $f \mid g$.

2.5 Príklad. Polynómy $(-1+2i)x^2+(1+i)x-2+3i$, $(2+i)x^2+(1-i)x+3+2i \in C[x]$ sú asociované, lebo

$$(-1+2i)x^2+(1+i)x-2+3i = i\cdot((2+i)x^2+(1-i)x+3+2i)$$

2.6 Definícia. Nech f, g, d sú polynómy jednej neurčitej nad poľom F. Polynóm d budeme volať najväčším spoločným deliteľom polynómov f, g (v okruhu F[x] alebo nad poľom F), ak

a) $d \mid f$, $d \mid g$,

b) ak $h \mid f$, $h \mid g$, $h \in F[x]$, tak $h \mid d$.

Analogicky sa definuje najmenší spoločný násobok polynómov.

2.7 Definícia. Nech f, g, t sú polynómy jednej neurčitej nad poľom F. Polynóm t budeme volať najmenším spoločným deliteľom polynómov f, g (v okruhu F[x] alebo nad poľom F), ak

a) $f \mid t$, $g \mid t$,

b) ak $f \mid q$, $g \mid q$, $q \in F[x]$, tak $t \mid q$.

Predchádzajúce definície je možné zovšeobecniť pre ľubovoľný konečný počet polynómov.

2.8 Lema. *Nech $d \in F[x]$ je najväčší spoločný deliteľ polynómov f, $g \in F[x]$. Potom $h \in F[x]$ je najväčší spoločný deliteľ polynómov f, g práve vtedy, keď $d \sim h$.*

Dôkaz. Nech aj h je najväčší spoločný deliteľ. Potom $d \mid h$, $h \mid d$, teda $d \sim h$.

Naopak, nech $d \sim h$. Potom $h \mid f$, $h \mid g$ (lebo $h \mid d$ a $d \mid f$, $d \mid g$) a podmienka a) definície 2.6 je splnená.

Nech teraz $q \mid f$, $q \mid g$, $q \in F[x]$. Potom $q \mid d$ a pretože $d \sim h$, tak aj $q \mid h$ a splnená je aj podmienka b) definície 2.6.

Zrejme ľubovoľný nenulový polynóm $g_x = b_n x^n + \cdots + a_0$ je asociovaný s jediným normovaným polynómom $b_n^{-1} \cdot g_x$. Ak sú teda polynómy f_x, g_x, s vedúcimi koeficientami a_n, b_n, asociované, tak $a_n^{-1} \cdot f_x = b_n^{-1} \cdot g_x$. Často sa aj polynómy, ktoré sú asociované stotožňujú a miesto symbolu $\sim$ sa používa symbol $=$.

Ak d je najväčší spoločný deliteľ polynómov f, g, tak niekedy píšeme $d = \mathrm{D}(f,g)$. Teda symbol $\mathrm{D}(f,g)$ označuje niektorý z najväčších spoločných deliteľov. Symbolom (f,g) budeme označovať ten z najväčších spoločných deliteľov, ktorý má koeficient v člene s najväčším exponentom rovný 1, (t.j. normovaný spoločný deliteľ). Ak $(f,g) = 1$, tak budeme hovoriť, že polynómy f, g sú nesúdeliteľné.

Pri hľadaní najväčšieho spoločného deliteľa dvoch polynómov budú užitočné nasledujúce dve tvrdenia, ktorých dôkazy sú jednoduché a čitateľ si ich môže urobiť sám ako cvičenie.

2.9 Lema. *Nech f_x, g_x sú polynómy jednej neurčitej nad poľom F a nech a, b sú nenulové prvky poľa F. Potom*

a) $\mathrm{D}(f_x, g_x) \sim \mathrm{D}(a \cdot f_x, b \cdot g_x)$ *(t.j.* $(f_x, g_x) = (a \cdot f_x, b \cdot g_x)$*),*

b) $\mathrm{D}(f_x, a) \sim a \sim 1$ *(t.j.* $(f_x, a) = 1$*).*

2.10 Lema. *Nech najväčší spoločný deliteľ polynómov f, g jednej neurčitej nad poľom F je $\mathrm{D}(f,g)$. Ak $f = g \cdot q + r$, $q, r \in F[x]$, tak*

$$\mathrm{D}(f,g) \sim \mathrm{D}(g,r) \quad (\textit{t.j. } (f,g) = (g,r)).$$

Na výpočet najväčšieho spoločného deliteľa dvoch polynómov existuje metóda, ktorá sa volá Euklidov algoritmus a ktorú teraz popíšeme.

Nech f, g sú nenulové polynómy jednej neurčitej nad poľom F. Potom, podľa vety 2.1, existuje jediná dvojica polynómov $q_1, r_1 \in F[x]$, že

$$f = g \cdot q_1 + r_1, \quad r_1 = 0 \text{ alebo } \operatorname{st} r_1 < \operatorname{st} g.$$

Ak $r_1 \neq 0$ tak analogicky dostávame, že

$$g = r_1 \cdot q_2 + r_2, \quad r_2 = 0 \text{ alebo } \operatorname{st} r_2 < \operatorname{st} r_1.$$

Takto môžeme postupovať ďalej. Pretože čísla $\operatorname{st} g, \operatorname{st} r_1, \operatorname{st} r_2, \ldots$ tvoria klesajúcu postupnosť nezáporných celých čísel, bude po konečnom počte krokov niektorý zvyšok nulový. Nech je to napríklad r_n. Dostaneme tak nasledovnú sústavu.

$$\begin{aligned}
f &= g \cdot q_1 + r_1, & \operatorname{st} r_1 &< \operatorname{st} g,\\
g &= r_1 \cdot q_2 + r_2, & \operatorname{st} r_2 &< \operatorname{st} r_1,\\
r_1 &= r_2 \cdot q_3 + r_3, & \operatorname{st} r_3 &< \operatorname{st} r_2,\\
&\vdots & &\vdots\\
r_{n-3} &= r_{n-2} \cdot q_{n-1} + r_{n-1}, & \operatorname{st} r_{n-1} &< \operatorname{st} r_{n-2},\\
r_{n-2} &= r_{n-1} \cdot q_n.
\end{aligned}$$

Pretože $r_{n-1} \mid r_{n-2}$ tak $\mathrm{D}(r_{n-1}, r_{n-2}) \sim r_{n-1}$ a z lemy 2.10 potom postupne dostávame, že

$$\mathrm{D}(f, g) \sim \mathrm{D}(g, r_1) \sim \cdots \sim \mathrm{D}(r_{n-2}, r_{n-1}) \sim r_{n-1}.$$

Najväčší spoločný deliteľ dvoch polynómov je teda posledný nenulový zvyšok v Euklidovom algoritme.

2.11 Veta. *Nech f, g sú polynómy jednej neurčitej nad poľom F. Potom existujú polynómy $u, v \in F[x]$, že $(f, g) = u \cdot f + v \cdot g$.*

Dôkaz. V prípade, že $f = 0$ alebo $g = 0$ je platnosť tvrdenia zrejmá. Nech teda f, g sú nenulové polynómy. Dôkaz urobíme matematickou indukciou vzhľadom na počet krokov v Euklidovom algoritme potrebných na výpočet najväčšieho spoločného deliteľa.

1. Ak je potrebný jeden krok, tak $f = g \cdot q$ a potom $(f, g) = c \cdot g = 0 \cdot f + c \cdot g$, pričom c je taký prvok poľa F, že $c \cdot g$ je normovaný polynóm.

2. Nech je potrebných $n > 1$ krokov. Predpokladajme, že pre $n - 1$ krokov je tvrdenie pravdivé. Podľa vety 2.1 je

$$f = g \cdot q + r, \quad \text{kde} \quad \operatorname{st} r < \operatorname{st} g$$

a podľa lemy 2.10 je $(f, g) = (g, r)$, pričom na výpočet (g, r) je potrebných už len $n - 1$ krokov. Preto, podľa indukčného predpokladu, je $(g, r) = v_1 \cdot g + u_1 \cdot r$, z čoho, po dosadení za r, dostávame

$$\begin{aligned}
(f, g) =& (g, r) = v_1 g + u_1 (f - gq) =\\
=& u_1 f + (v_1 - u_1 q) g = uf + vg
\end{aligned}$$

kde sme označili $u_1 = u$ a $v_1 - u_1 \cdot q = v$.

Cvičenia

1. Nájdite čiastočný podiel a zvyšok pri delení polynómu f_x polynómom g_x nad poľom C, ak
   a) $f_x = x^4 + x^3 - 5x^2 + x - 6, \quad g_x = x^3 - 8x^2 + x - 8,$
   b) $f_x = x^3 - 8x^2 + x - 7, \quad g_x = x^2 + 1,$
   c) $f_x = x^5 + 15x^2 - 31x + 15, \quad g_x = x^2 + 2x - 3,$
   d) $f_x = x^5 + 2ix^4 + (3-i)x^3 + 2ix^2 - 4x - 6i, \quad g_x = x^2 + 2ix - 3,$
   e) $f_x = 5x^6 + 4x^5 + 3x^2 + 2x + 1, \quad g_x = 7x^4 + 2x^2 - 3x + 2.$
2. Nájdite čiastočný podiel a zvyšok pri delení polynómu f_x polynómom g_x nad poľom Z_5, ak
   a) $f_x = 4x^3 + x^2 + x + 3, \quad g_x = 2x + 1,$
   b) $f_x = x^5 + 2x^4 + 4x^3 + x^2 + 2x + 2, \quad g_x = 3x^3 + 2x + 1,$
   c) $f_x = x^5 + 3x^3 + 4x^2 + 3, \quad g_x = x^3 + 2x^2 + 4x + 1,$
   d) $f_x = 4x^3 + 4, \quad g_x = 2x^2 + 3x + 2.$
3. Určte $a, b \in R$ tak, aby $g_x \mid f_x$ v okruhu $R[x]$, ak
   a) $f_x = 6x^5 + 11x^4 + 5x^3 + 5x^2 + ax + b, \quad g_x = x^2 + 1,$
   b) $f_x = x^3 + 8x^2 + 5x + a, \quad g_x = x^2 + 3x + b.$
4. Nájdite $a, b, c \in Z$ tak, aby polynóm f_x bol deliteľný polynómom g_x:
   a) $f_x = x^3 + 2x^2 + ax - 3, \quad g_x = x^2 + bx + c,$
   b) $f_x = x^3 + ax^2 + 3x + b, \quad g_x = x^2 + cx + 2.$
5. Nájdite $\mathrm{D}(f_x, g_x)$, ak
   a) $f_x = x^4 + x^3 - 5x^2 + x - 6, \quad g_x = x^3 - 8x^2 + x - 8,$
   b) $f_x = x^5 + 1, \quad g_x = x^2 + 1,$
   c) $f_x = x^4 + x^3 - 3x^2 - 4x - 1, \quad g_x = x^3 + x^2 - x - 1,$
   d) $f_x = x^6 + 3x^5 + 3x^4 + 3x^3 + 4x^2 + 6x + 4, \quad g_x = x^4 + x^3 - 3x^2 - x + 2,$
   e) $f_x = x^5 - 2x^4 + x^3 + 7x^2 - 12x + 10, \quad g_x = 3x^4 - 6x^3 + 5x^2 + 2x - 2,$
   f) $f_x = x^4 + x^3 + 2x^2 - x - 2, \quad g_x = 2x^3 + (2+i)x^2 + (-1+i)x - 1.$
6. Nájdite $\mathrm{D}(f_x, g_x)$ nad poľom Z_5, ak
   a) $f_x = x^4 + 4x^3 + 1, \quad g_x = x^3 + 3x^2 + 1,$ b) $f_x = x^4 + x^3 + 2x^2 + x + 4, \quad g_x = x^3 + x^2 + 4x + 4.$
7. Nájdite podmienku pre $a, b \in R$ tak, aby $\mathrm{D}(f_x, g_x)$ bol polynóm aspoň prvého stupňa, ak $f_x = 3x^3 + 3ax + 3b$, $g_x = 3x^2 + a$.

3 Rozklady polynómov

3.1 Definícia. Polynóm g voláme triviálnym deliteľom polynómu f v okruhu $F[x]$, ak $\operatorname{st} g = 0$ alebo $f \sim g$

3.2 Definícia. Nech f je polynóm jednej neurčitej nad poľom F stupňa väčšieho ako nula. Polynóm f voláme ireducibilným (nerozložiteľným) v $F[x]$ (alebo nad poľom F), ak f nemá v $F[x]$ okrem triviálnych deliteľov žiadne iné. V opačnom prípade sa f volá reducibilným (rozložiteľným) polynómom v $F[x]$ (alebo nad F).

Ak je teda polynóm f rozložiteľný, tak existujú také polynómy g, q, že ich stupne sú menšie ako stupeň polynómu f a $f = g \cdot q$.

3.3 Lema. *Nech p, f, g sú polynómy jednej neurčitej nad poľom F. Ak polynóm p je ireducibilný a $p \mid f \cdot g$, tak $p \mid f$ alebo $p \mid g$.*

Dôkaz. Ak p je ireducibilný, tak najväčší spoločný deliteľ polynómov p, f je alebo p alebo 1. V prvom prípade $p \mid f$, v druhom, podľa vety 2.11, je $1 = u \cdot p + v \cdot f$.

Po vynásobení obidvoch strán tejto rovnosti polynómom g dostávame

$$g = u \cdot p \cdot g + v \cdot f \cdot g$$

z čoho už vyplýva, že $p \mid g$.

3.4 Veta. *Každý polynóm $f \in F[x]$, F je pole, stupňa väčšieho ako nula možno napísať ako súčin ireducibilných polynómov. Tento súčin (rozklad) je jednoznačný s výnimkou poradia a zámeny činiteľov asociovanými.*

Dôkaz. Matematickou indukciou vzhľadom na stupeň n polynómu f.

1. Pre $n = 1$ je každý polynóm ireducibilný a teda jeho rozklad je jednoznačný.

2. Predpokladajme, že tvrdenie platí pre každý polynóm stupňa menšieho ako n. Nech f je polynóm stupňa n. Ak je ireducibilný, tak jeho rozkladom je sám polynóm f. Ak f je reducibilný, tak existujú polynómy h, g, kde $\operatorname{st} h < n$, $\operatorname{st} g < n$. Podľa indukčného predpokladu teda $h = p_1 \cdot \ldots \cdot p_k$, $g = q_1 \cdot \ldots \cdot q_l$, kde p_i pre $i \in \{1, \ldots, k\}$ aj q_j pre $j \in \{1, \ldots, l\}$ sú ireducibilné polynómy. Z toho dostávame, že

$$f = p_1 \cdot \ldots \cdot p_k \cdot q_1 \cdot \ldots \cdot q_l.$$

Ešte treba ukázať jednoznačnosť rozkladu. Predpokladáme, že každý polynóm, ktorý je súčinom menej ako n činiteľov má jednoznačný rozklad. Uvažujme rozklady

$$p_1 \cdot \ldots \cdot p_{n-1} \cdot p_n = f = q_1 \cdot \ldots \cdot q_m.$$

Ireducibilný polynóm p_n delí ľavú stranu, teda aj pravú stranu a podľa dôsledku 3.3 delí niektorý z činiteľov na pravej strane. Nech je to napr. q_j. Pretože p_n, q_j sú ireducibilné, tak $p_n \sim q_j$, teda $q_j = c \cdot p_n$, $c \in F$. Po dosadení a krátení dostávame

$$p_1 \cdot \ldots \cdot p_{n-1} = c \cdot q_1 \cdot \ldots \cdot q_{j-1} \cdot q_{j+1} \cdot \ldots \cdot q_m.$$

Teraz môžeme použiť indukčný predpoklad a tým je tvrdenie dokázané.

Každý polynóm $f = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$ je teda možné, podľa predchádzajúcej vety, napísať jednoznačne (až na poradie a asociovanosť) v tvare

$$f = q_1 \cdot q_2 \cdot \ldots \cdot q_m, \tag{1}$$

kde $q_1, q_2, \ldots, q_m$ sú ireducibilné polynómy. Každý polynóm q_i je asociovaný s jediným normovaným polynómom p_i, $i \in \{1, \ldots, m\}$. Teda pre každé $i \in \{1, \ldots, m\}$ je $q_i = c_i \cdot p_i$ ($c_i \in F$). Po dosadení do (1) dostávame

$$f = c_1 \cdot \ldots \cdot c_m \cdot p_1 \cdot \ldots \cdot p_m. \tag{2}$$

Pretože súčin normovaných polynómov je opäť normovaný polynóm, tak $c_1 \cdot \ldots \cdot c_m = a_n$. Z uvedeného a z vety 3.4 vyplýva nasledovné tvrdenie.

3.5 Dôsledok. *Nech $f = a_n x^n + \cdots + a_1 x + a_0 \in F[x]$, $n \geq 1$. Potom existujú normované a ireducibilné polynómy $p_1, \ldots, p_m$, že*

$$f = a_n \cdot p_1 \cdot \ldots \cdot p_m. \tag{3}$$

súčin (3) je jednoznačný, až na poradie činiteľov.

Je možné, že v súčine (3) sa niektoré činitele opakujú (t.j. v súčine (1) sú niektoré činitele asociované). V takom prípade môžeme súčin (3) ešte upraviť a zapísať ho v tvare

$$f = a_n \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}, \tag{4}$$

kde $p_1, \ldots, p_r$ sú navzájom rôzne normované, ireducibilné polynómy a $\alpha_1, \ldots, \alpha_r$ sú nenulové prirodzené čísla. Zápis (4) budeme nazývať *kanonickým rozkladom* polynómu f nad poľom F (v okruhu $F[x]$). V zápise (4) pripustíme niekedy aj nulové exponenty a potom hovoríme o *zovšeobecnenom rozklade.*

3.6 Veta. *Nech $f = a \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n}$ je kanonický rozklad polynómu f nad poľom F. Potom polynóm g delí polynóm f práve vtedy, keď polynóm g je možné zapísať v tvare*

$$g = b \cdot p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}, \tag{5}$$

pričom pre každé $i \in \{1, \ldots, m\}$ je $0 \leq \beta_i \leq \alpha_i$.

Dôkaz. Predpokladajme, že $g \mid f$. Potom existuje polynóm h, že $f = g \cdot h$. Ak by polynóm g obsahoval (v rozklade (5)) ireducibilný normovaný činiteľ, ktorý sa nenachádza v kanonickom rozklade polynómu f alebo by obsahoval niektorý činiteľ vo vyššej mocnine ako je v kanonickom rozklade polynnómu f, dostali by sme spor s jednoznačnosťou rozkladu.

Naopak, nech polynóm g má rozklad (5). Potom

$$\begin{aligned} f &= a \cdot p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} = \\ &= a \cdot p_1^{\beta_1+\alpha_1-\beta_1} \cdot \ldots \cdot p_n^{\beta_n+\alpha_n-\beta_n} = \\ &= a \cdot b \cdot b^{-1} \cdot p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n} \cdot p_1^{\alpha_1-\beta_1} \cdot \ldots \cdot p_n^{\alpha_n-\beta_n} = \\ &= b \cdot p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n} \cdot a \cdot b^{-1} \cdot p_1^{\alpha_1-\beta_1} \cdot \ldots \cdot p_n^{\alpha_n-\beta_n} = g \cdot h, \end{aligned}$$

kde sme označili $h = a \cdot b^{-1} \cdot p_1^{\alpha_1-\beta_1} \cdot \ldots \cdot p_n^{\alpha_n-\beta_n}$. Dostávame teda, že $g \mid f$.

V prípade, že poznáme kanonické rozklady polynómov f, g, môžeme vetu 3.6 využiť na nájdenie ich najväčšieho spoločného deliteľa a najmenšieho spoločného násobku. Normovaný najmenší spoločný násobok polynómov f, g označíme $[f, g]$.

3.7 Veta. *Nech $f = a \cdot p_1^{k_1} \cdot \ldots \cdot p_n^{k_n}$, $g = b \cdot p_1^{l_1} \cdot \ldots \cdot p_n^{l_n}$ sú zovšeobecnené rozklady polynómov f, g nad poľom F. Potom*

$$(f, g) = p_1^{r_1} \cdot \ldots \cdot p_n^{r_n}, \quad \textit{kde} \quad r_i = \min(k_i, l_i) \tag{6}$$

a

$$[f, g] = p_1^{s_1} \cdot \ldots \cdot p_n^{s_n}, \quad \textit{kde} \quad s_i = \max(k_i, l_i), \tag{7}$$

pre každé $i \in \{1, \ldots, n\}$.

Dôkaz. Z vety 3.6 vyplýva, že $(f, g) \mid f$ a $(f, g) \mid g$, teda podmienka a) definície 2.6 je splnená.

Nech $h \mid f$, $h \mid g$. Potom (podľa vety 3.6)

$$h = a \cdot p_1^{t_1} \cdot \ldots \cdot p_n^{t_n}, \quad \text{kde} \quad 0 \leq t_i \leq k_i \text{ a } 0 \leq t_i \leq l_i$$

pre každé $i \in \{1, \ldots, n\}$. To znamená, že $0 \leq t_i \leq \min(k_i, l_i) = r_i$, teda $h \mid (f, g)$ a splnená je aj podmienka b) definície 2.6.

Analogicky je možné dokázať aj rovnosť (7).

3.8 Príklad. Nech

$$f = 2(x-2)^3(x-1)(x^2+1), \quad g = (x-2)^2(x+1)(x^2+1)^2$$

sú polynómy nad poľom E. Podrobne sa presvedčte, že uvedené rozklady sú kanonické. Zápisy polynómov f, g upravíme na zovšeobecnené rozklady. Potom

$$f = 2(x-2)^3(x-1)^1(x+1)^0(x^2+1),$$
$$g = (x-2)^2(x-1)^0(x+1)(x^2+1)^2.$$

S využitím vety 3.7 dostávame

$$(f,g) = (x-2)^2(x-1)^0(x+1)^0(x^2+1) = (x-2)^2(x^2+1),$$
$$[f,g] = (x-2)^3(x-1)(x+1)(x^2+1)^2.$$

Cvičenia

1. Ukážte, že polynóm x^2+4 je v $R[x]$ ireducibilný.
2. Nájdite v $R[x]$ kanonický rozklad polynómu
   a) x^4+1,
   b) x^4-x^2+1.
3. Pomocou kanonických rozkladov nájdite (f,g) a $[f,g]$ v $R[x]$, ak $f = x^3-8$, $g = x^4+2x^3+3x^2-2x-4$.
4. Pomocou kanonických rozkladov nájdite (f,g) a $[f,g]$ v $C[x]$, ak $f = x^4+2x^2+1$, $g = x^2+(1+i)x+i$.

4 Korene polynómov.

V tejto časti sa budeme zaoberať hlavne polynómami jednej premennej (t.j. polynomickými funkciami) nad poľom F.

4.1 Definícia. Nech $f(x)$ je polynóm jednej premennej nad poľom F. Prvok $c \in F$ voláme koreňom polynómu $f(x)$, ak $f(c) = 0$.

Koreň polynómu voláme tiež *riešením* alebo *koreňom* rovnice $f(x) = 0$.

4.2 Veta. *Ak pole F má konečný počet prvkov, tak okruh $F\langle x\rangle$ má vlastné delitele nuly.*

Dôkaz. Nech $F = \{a_1, a_2, \ldots, a_n\}$, $n \in N$ a nech $f(x) = x - a_1$, $g = (x-a_2)(x-a_3)\ldots(x-a_n)$. Potom $f(x)$ ani g nie sú nulové funkcie, lebo $f(a_2) = a_2 - a_1 \neq 0$, $g(1) = (a_1-a_2)\ldots(a_1-a_n) \neq 0$, ale $f(x)\cdot g(x) = (x-a_1)(x-a_2)\ldots(x-a_n)$ je nulová funkcia.

4.3 Veta (Bézoutova). *Nech $f(x) \in F\langle x\rangle$, Kde F je pole. Prvok c je koreňom polynómu $f(x)$ práve vtedy, keď $x-c$ delí $f(x)$ (ako polynómy jednej neurčitej).*

Dôkaz. Nech $f(c) = 0$. K polynómom $f(x)$, $x-c$ (ako k polynómom jednej neurčitej a teda aj polynómom jednej premennej) existujú polynómy $q(x)$, $r(x)$, o ktorých platí

$$f(x) = (x-c)q(x) + r(x), \qquad r(x) = 0 \text{ alebo } \operatorname{st} r(x) < \operatorname{st}(x-c).$$

Pretože $\operatorname{st}(x-c) = 1$ a $\operatorname{st} r(x) < \operatorname{st}(x-c)$, čiže, $r(x) = z \in F$. Na základe predpokladu $0 = f(c) = 0 + z$, teda $z = 0$, čo znamená, že $f(x) = (x-c)q(x)$, t.j. $x-c \mid f(x)$.

Naopak, nech $x-c \mid f(x)$. Potom $f(x) = (x-c)q(x)$ a $f(c) = (0-0)q(0) = 0$, teda c je koreň.

4.4 Lema. *Nech $f(x)$ je polynóm jednej premennej nad poľom F a nech $c \in F$. Potom existuje polynóm $q(x)$, že $f(x) = (x-c)q(x) + f(c)$.*

Dôkaz. Pretože $f(x) = (x-c)q(x) + z$, $z \in F$, tak $f(c) = (c-c)q(c) + z$. Teda $z = f(c)$.

Nasledujúce tvrdenie je jednoduché a preto ho uvedieme bez dôkazu.

4.5 Lema. *Nech $f(x)$, $g(x)$, $h(x)$ sú polynómy jednej premennej nad poľom F a nech $f(x) = g(x) \cdot h(x)$. Potom c je koreň plynómu $f(x)$ vtedy a len vtedy, keď je koreňom polynómu $g(x)$ alebo koreňom polynómu $h(x)$.*

4.6 Veta. *Polynóm $f(x) \in F\langle x\rangle$ stupňa n má v poli F najviac n koreňov.*

Dôkaz. Matematickou indukciou vzhľadom na stupeň polynómu.

1. Ak $n = 0$, tak $f(x) = a_0 \neq 0$ a $f(x)$ nemá žiadne korene.

2. Predpokladajme, že tvrdenie platí pre ľubovoľný polynóm stupňa $n-1$, $n > 1$. Nech $f(x)$ je polynóm stupňa n. Nech $c \in F$ je koreň polynómu $f(x)$. Potom $f(x) = (x-c)q(x)$, kde $q(x)$ je polynóm stupňa $n-1$. Podľa indukčného predpokladu má $q(x)$ najviac $n-1$ koreňov. Z predchádzajúcej lemy vyplýva, že koreňmi polynómu $f(x)$ sú korene polynómu $q(x)$ a prvok c (a žiadne iné). Teda polynóm $f(x)$ má najviac n koreňov.

4.7 Dôsledok. *Nech F je nekonečné pole a $f(x) = a_0 + a_1x + \cdots + a_rx^r$, $g(x) = b_0 + b_1x + \cdots + b_sx^s$ polynómy jednej premennej nad F. Potom*

(R$_x$) $\quad f(x) = g(x)$ *práve vtedy, keď* $r = s$ *a* $\forall i \in \{0, 1, \ldots, r\}$, $a_i = b_i$.

Dôkaz. Ak $r = s$ a odpovedajúce koeficienty sa rovnajú, tak zrejme pre každé $t \in F$ je $f(t) = g(t)$, čo znamená, že $f(x) = g(x)$.

Naopak (sporom), nech $f(x) = g(x)$ (t.j. $f(t) = g(t)$ pre každé $t \in F$) ale nech $r \neq s$ alebo $a_i \neq b_i$, pre nejaké i. Potom $f(x) - g(x)$ je polynóm n-tého stupňa (pre vhodné $n \in N$) a jeho koreňom je každý prvok poľa F, čo je spor s vetou 4.6.

Vieme už, že pomocou vzťahou (S) a (N) môžeme počítať aj súčty a súčiny polynomických funkcií. Inak je to so vzťahom (R). Ak je však F nekonečné pole, tak dôsledok 4.7 vlastne hovorí, že zobrazenie $\psi : F[x] \to F\langle x\rangle$, ktoré sme zaviedli v prvej kapitole je aj injektívne a v takom prípade môžeme aj rovnosť polynomických funkcií určovať pomocou (R). Znamená to, že ak je pole F nekonečné, tak okruhy $F[x]$, $F\langle x\rangle$ sú izomorfné. Ak sa teda budeme zaoberať napríklad polynómami nad poľom C (E, Q) nebudeme zvlášť zdôrazňovať či je to polynóm jednej neurčitej alebo jednej premennej.

Výpočet koeficientov podielu a zvyšku pri delení dvojčlenom $x - c$ robíme obyčajne pomocou tzv. Hornerovej schémy. Výpočet pomocou tejto schémy sa opiera o nasledujúce tvrdenie.

4.8 Dôsledok. *Nech pri delení polynómu $f(x) = a_nx^n + \cdots + a_0$ lineárnym dvojčlenom $x - c$ je podiel $g(x) = b_{n-1}x^{n-1} + \cdots + b_1x + b_0$ a zvyšok $f(c)$. Potom*

(H)
$$\begin{aligned} b_{n-1} &= a_n, \\ b_{n-2} &= a_{n-1} + c \cdot b_{n-1}, \\ &\vdots \\ b_0 &= a_1 + c \cdot b_1, \\ f(c) &= a_0 + c \cdot b_0. \end{aligned}$$

Dôkaz. Podľa lemy 4.4 je $f(x) = (x-c)q(x) + f(c)$, teda

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = (x-c)(b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_1 x + b_0) + f(c).$$

Z toho porovnaním koeficientov dostávame, že

$$\begin{aligned} a_n &= b_{n-1}, \\ a_{n-1} &= b_{n-2} - c \cdot b_{n-1}, \\ a_{n-2} &= b_{n-3} - c \cdot b_{n-2}, \\ &\vdots \\ a_1 &= b_0 - c \cdot b_1, \\ a_0 &= f(c) - c \cdot b_0, \end{aligned}$$

z čoho už vyplýva (H).

Na základe tohto dôsledku zostavíme Hornerovu schému takto. Do prvého riadku napíšeme všetky (teda aj nulové) koeficienty polynómu $f(x)$. Do druhého a tretieho riadku potom postupne zapisujeme prvky b_{n-1}, $c \cdot b_{n-1}$, b_{n-2}, $c \cdot b_{n-2}$, b_{n-3}, atď. (pozri nasledujúcu tabuľku).

a_n	a_{n-1}	a_{n-2}	$\ldots$	a_1	a_0
	$c \cdot b_{n-1}$	$c \cdot b_{n-2}$	$\ldots$	$c \cdot b_1$	$c \cdot b_0$
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
b_{n-1}	b_{n-2}	b_{n-3}	$\ldots$	b_0	$f(c)$

4.9 Príklad. Určte podiel a zvyšok pri delení polynómu $f(x) = x^5 - 3x^4 + 2x - 7$ dvojčlenom $x + 2$.

Riešenie. V tomto prípade je $c = -2$ a Hornerova schéma má tvar

1	-3	0	0	2	-7
	-2	10	-20	40	-84
$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$
1	-5	10	-20	42	-91

teda $x^5 - 3x^4 + 2x - 7 = (x+2)(x^4 - 5x^3 + 10x^2 - 20x + 42) - 91$, $f(-2) = -91$.

4.10 Definícia. Prvok c poľa F voláme k-násobným koreňom polynómu $f(x) \in F\langle x \rangle$ stupňa $n \geq 2$ práve vtedy, keď $f(x) = (x-c)^k g(x)$, $g(c) \neq 0$.

Ak $k = 1$ nazývame ho obyčajne *jednoduchým* koreňom, ak $k \geq 2$ hovoríme o *viacnásobnom* koreni.

4.11 Definícia. Pole F sa volá algebraicky uzavreté, ak každý polynóm nad F stupňa $n \geq 1$ má v F aspoň jeden koreň.

Pole racionálnych čísel nie je algebraicky uzavreté lebo napríklad polynóm $x^2 - 2$ nemá racionálne korene. Podobne, ani pole reálnych čísel nie je algebraicky uzavreté lebo napríklad polynóm $x^2 + 1$ nemá reálne korene. Ako je to v poli komplexných čísel uvádza tzv. základná veta algebry, ktorú uvedieme bez dôkazu.

4.12 Veta. *Pole komplexných čísel je algebraicky uzavreté, t.j. každý polynóm aspoň prvého stupňa s komplexnými koeficientami má aspoň jeden komplexný koreň.*

Cvičenia

1. Vypočítajte neúplný podiel a zvyšok pri delení polynómu $2x^5+3x^4-13x^3+31x-15$ dvojčlenom
   a) $x-1$, b) $x+3$.
2. Číslo 2 je koreň polynómu $3x^5-16x^4+25x^3-6x^2-4x-8$. Určte jeho násobnosť.
3. Daný je polynóm $f(x)=x^7+2x^6+x^4-5x^3+3x^2+1$. Určte $f(-2)$.
4. Určte číslo a tak, aby polynóm $x^3+2x^2+ax+24$ bol deliteľný dvojčlenom $x+3$.
5. Nájdite čiastočný podiel a zvyšok pri delení polynómu $x^6+(2-2i)x^5+(1+i)x^3-(1+i)x^2+2i$ polynómom $x+1-i$.
6. Určte $a,b\in R$ tak, aby polynóm $2x^{35}-18x^{33}-5x^{15}+45x^{13}+ax^2+bx-3$ bol deliteľný polynómom x^2-4x+3.
7. Určte $a,b,c\in R$ tak, aby číslo -2 bolo aspoň trojnásobným koreňom polynómu $x^4+ax^3+bx^2+cx-24$.

5 Polynómy s číselnými koeficientami.

V tejto časti sa budeme zaoberať polynómami nad poľom C (komplexných čísel). Ak budeme požadovať, aby polynóm mal celočíselné alebo racionálne alebo reálne koeficienty, tak to zvlášť zdôrazníme.

5.1 Veta 1. *Nech $f(x)=a_nx^n+\cdots+a_1x+a_0$, $n\geq 1$, je polynóm s komplexnými koeficientami. Potom existujú komplexné čísla c_1, c_2, …, c_n, o ktorých platí*

$$f(x)=a_n(x-c_1)(x-c_2)\dots(x-c_n). \tag{1}$$

Dôkaz. Matematickou indukciou vzhľadom na stupeň polynómu.

1. Pre $n=1$ je $f(x)=a_1x+a_0=a_1(x+\frac{a_0}{a_1})$, teda $c_1=-\frac{a_0}{a_1}$.

2. Nech uvedenú vlastnosť majú všetky polynómy n-tého stupňa pre $n\geq 1$ a nech $f(x)=a_{n+1}x^{n+1}+a_nx^n+\cdots+a_1x+a_0$ je polynóm stupňa $n+1$. Podľa vety 3.4 má $f(x)$ nejaký koreň $c_1\in C$ a preto podľa Bezoutovej vety $f(x)=(x-c_1)g(x)$, kde $g(x)$ je polynóm n-tého stupňa s vedúcim koeficientom a_{n+1}. Podľa indukčného predpokladu preto existujú čísla $c_2,\dots,c_{n+1}\in C$, že

$$g(x)=a_{n+1}(x-c_2)\dots(x-c_{n+1})$$

a z toho (po dosadení) dostávame

$$f(x)=a_{n+1}(x-c_1)(x-c_2)\dots(x-c_{n+1}).$$

Lineárne činitele $x-c_1,\dots x-c_n$ nazývame *koreňové činitele* polynómu $f(x)$ a tvar (1) nazývame rozklad na koreňové činitele. Pretože lineárne činitele sú ireducibilné, tak rozklad (1) je jednoznačný, až na poradie činiteľov. Rozklad (1) môžeme ďalej upraviť na tvar

$$f(x)=a_n(x-c_1)^{k_1}\dots(x-c_r)^{k_r}, \tag{2}$$

kde činitele $x-c_1,\dots,x-c_r$ sú navzájom rôzne a $k_1,\dots,k_r\in N^+$, pričom $k_1+\cdots+k_r=n$. Tento rozklad je vlastne kanonickým rozkladom.

Ak $f(x)$ má kanonický rozklad (2), tak c_1 je k_1 násobný koreň polynómu $f(x)$, c_2 je k_2 násobný koreň polynómu $f(x)$, atď.

5.2 Dôsledok. *Polynóm $n-$tého stupňa, $n \geq 1$, s komplexnými koeficientami má v poli komplexných čísel práve n koreňov (ak každý počítame toľkokrát, aká je jeho násobnosť).*

5.3 Veta. *Ak polynóm $f(x)$ s reálnymi koeficientami má k-násobný koreň $c = a + bi$, tak má aj k násobný komplexne združený koreň $\overline{c} = a - bi$.*

Dôkaz. a) Najprv dokážeme, že ak polynóm $f(x) = a_n x^n + \cdots + a_0$ s reálnymi koeficientami má koreň $a + bi$, tak má aj koreň $a - bi$. Využijeme, že pre ľubovoľné $c_1, c_2, \ldots, c_n \in C$ platí (podrobne sa presvedčte)

$$\overline{c}_1 + \overline{c}_2 + \cdots + \overline{c}_n = \overline{c_1 + c_2 + \cdots + c_n},$$
$$\overline{c}_1 \cdot \overline{c}_2 \cdot \ldots \cdot \overline{c}_n = \overline{c_1 \cdot c_2 \cdot \ldots \cdot c_n}.$$

Nech $a + bi$ je koreň polynómu $f(x)$, t.j. nech $f(a + bi) = 0$. Potom

$$\begin{aligned} f(\overline{a+bi}) &= a_n(\overline{a+bi})^n + \cdots + a_1(\overline{a+bi}) + a_0 = \\ &= a_n\overline{(a+bi)^n} + \cdots + a_1\overline{(a+bi)} + a_0 = \\ &= \overline{a_n}\overline{(a+bi)^n} + \cdots + \overline{a_1}\overline{(a+bi)} + \overline{a_0} = \\ &= \overline{a_n(a+bi)^n} + \cdots + \overline{a_1(a+bi)} + \overline{a_0} = \\ &= \overline{a_n(a+bi)^n + \cdots + a_1(a+bi) + a_0} = \overline{f(a+bi)} = \overline{0} = 0, \end{aligned}$$

čo znamená, že aj $\overline{a+bi} = a - bi$ je koreň polynómu $f(x)$.

b) Indukciou (vzhľadom na stupeň polynómu) dokážeme, že ak $f(x)$ má k-násobný koreň $a + bi$, tak má aj k-násobný koreň $a - bi$.

1. Ak $n = 1$, tak $f(x) = a_1 x + a_0$ má jediný reálny koreň $-\frac{a_0}{a_1}$. Pre polynómy prvého stupňa teda tvrdenie platí.

2. Nech tvrdenie platí pre ľubovoľný polynóm stupňa menšieho ako n ($n \geq 2$). Nech polynóm $f(x)$ stupňa n má k-násobný koreň $a + bi$. Podľa predchádzajúcej časti dôkazu má $f(x)$ aj koreň $a - bi$ a preto je podľa vety 4.3 deliteľný nesúdeliteľnými dvojčlenmi $x - a - bi$, $x - a + bi$. Preto existuje polynóm $g(x)$, že

$$f(x) = (x - a - bi)(x - a + bi)g(x) = (x^2 - 2ax + a^2 + b^2)g(x).$$

Pretože $f(x)$ aj $x^2 - 2ax + a^2 + b^2$ sú polynómy s reálnymi koeficientami, tak aj polynóm $g(x)$ má reálne koeficienty. Polynóm $g(x)$ je stupňa $n-2$, má $k-1$-násobný koreň $a+bi$ a teda, podľa indukčného predpokladu, má aj $k-1$-násobný koreň $a-bi$. Z toho vyplýva, že polynóm $f(x)$ má k násobný koreň $a - bi$.

5.4 Dôsledok. *Ireducibilnými polynómami v $E[x]$ sú polynómy prvého stupňa a polynómy $ax^2 + bx + c$ druhého stupňa, pre ktoré $b^2 - 4ac < 0$.*

5.5 Dôsledok. *Polynóm s reálnymi koeficientami nepárneho stupňa má aspoň jeden reálny koreň.*

5.6 Veta. *Ak polynóm $f(x) = a_n x^n + \cdots + a_1 x + a_0$ s celočíselnými koeficientami má racionálny koreň $\frac{p}{q}$, kde $\mathrm{D}(p, q) = 1$, tak $p \mid a_0$ a $q \mid a_n$.*

Dôkaz. Nech $\frac{p}{q}$ je koreň polynómu $f(x)$ a nech $\mathrm{D}(p, q) = 1$. Potom

$$a_n \left(\frac{p}{q}\right)^n + \cdots + a_1 \left(\frac{p}{q}\right) + a_0 = 0.$$

Ak obidve strany tejto rovnosti vynásobíme q^n dostávame

$$a_n p^n + \cdots + a_1 p q^{n-1} + a_0 q^n = 0$$

a po úprave

$$p(a_n p^{n-1} + \cdots + a_1 q^{n-1}) = -a_0 q^n.$$

Pretože p delí ľavú stranu tejto rovnosti, tak $p \mid a_0 q^n$ a pretože $\mathrm{D}(p, q) = 1$, tak $p \mid a_0$. Analogicky je možné ukázať, že $q \mid a_n$.

5.7 Príklad. Nájdeme racionálne korene polynómu

$$f(x) = 24x^3 + 2x^2 - 11x - 3.$$

Ak má polynóm $f(x)$ racionálny koreň $\frac{p}{q}$, tak $p \mid -3$, $q \mid 24$ a teda

$$p \in \{1, 3, -1, -3\}$$
$$q \in \{1, 2, 3, 4, 6, 8, 12, 24, -1, -2, -3, -4, -6, -8, -12, -24\},$$

z čoho vyplýva, že polynóm $f(x)$ môže mať racionálne korene len z množiny

$$\left\{1, \tfrac{1}{2}, \tfrac{1}{3}, \tfrac{1}{4}, \tfrac{1}{6}, \tfrac{1}{8}, \tfrac{1}{12}, \tfrac{1}{24}, 3, \tfrac{3}{2}, \tfrac{3}{4}, \tfrac{3}{8}, -1, -\tfrac{1}{2}, -\tfrac{1}{3}, -\tfrac{1}{4}, -\tfrac{1}{6}, -\tfrac{1}{8}, -\tfrac{1}{12}, -\tfrac{1}{24}, -3, -\tfrac{3}{2}, -\tfrac{3}{4}, -\tfrac{3}{8}\right\}.$$

Môžeme sa presvedčiť, napríklad pomocou Hornerovej schémy, že jednoduchými koreňmi sú čísla $\frac{3}{4}$, $-\frac{1}{2}$, $-\frac{1}{3}$.

Cvičenia

1. Nájdite všetky korene polynómu $x^4 - 4x^2 + 8x - 4$ ak viete, že jeden jeho koreň je $1 + i$.
2. Zostrojte polynóm najmenšieho stupňa s reálnymi koeficientami, ktorý má korene: číslo 1 dvojnásobný, $1 - i$ jednoduchý, -2 jednoduchý.
3. Nájdite racionálne korene polynómu:
   a) $2x^3 + 3x^2 + 6x - 6$,
   b) $x^3 - 6x^2 + 11x - 6$,
   c) $4x^4 - 7x^2 - 5x - 1$.
4. Rozložte na koreňové činitele polynóm $16x^4 - 8x + 3$.

6 Derivácie polynómov

V matematickej analýze sa definuje derivácia reálnej funkcie ako istá limita. V algebre sa zavádza derivácia polynómu nad ľubovoľným poľom, teda aj v prípade, keď limitu nie je možné použiť.

6.1 Definícia. Nech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_2 x^2 + a_1 x + a_0$ je polynóm jednej premennej nad poľom F. Potom polynóm

$$(1) \qquad (f(x))' = f'(x) = n \times a_n x^{n-1} + (n-1) \times a_{n-1} x^{n-2} + \cdots + 2 \times a_2 x + a_1$$

sa nazýva (prvá) derivácia polynómu $f(x)$.

Pripomeňme, že ak k je prirodzené číslo a a je prvok nejakého poľa $(F, +, \cdot)$, tak symbol $k \times a$ znamená $(a + \cdots + a)_{k-\text{krát}}$.

6.2 Príklad. Ak $f(x) = 2x^5 + 3x^4 + 4x^2 + 3x + 2$ je polynóm nad poľom Z_5, tak

$$f'(x) = 5 \times 2x^4 + 4 \times 3x^3 + 2 \times 4x + 3 = 2x^3 + 3x + 3.$$

Aj z predchádzajúceho príkladu vidieť, že ak $f(x)$ je polynóm nad poľom konečnej charakteristiky a $\operatorname{st} f(x) = n \geq 1$, tak stupeň polynómu $f'(x)$ nemusí byť $n-1$. Ak je ale $f(x)$ polynóm nad poľom charakteristiky ∞ a $\operatorname{st} f(x) = n \geq 1$, tak jeho derivácia je zrejme polynóm stupňa $n-1$.

Ak nebude možný omyl, tak miesto $k \times a$ budeme písať $k \cdot a$ (alebo len ka). Rovnosť (1) zapíšeme teda stručnejšie v tvare

$$f'(x) = na_n x^{n-1} + \cdots + (n-1)a_{n-1}x^{n-2} + \cdots + 2a_2 x + a_1.$$

Vidíme, že aj keď je v algebre derivácia polynómu definovaná ako „mechanická operácia“ s jeho koeficientami a exponentami, má rovnaký tvar ako derivácia reálneho polynómu známa z matematickej analýzy. Platia aj analogické tvrdenia o derivácii súčtu a súčinu.

6.3 Veta. *Nech $f(x)$, $g(x)$ sú polynómy nad poľom F. Potom*

$$(f(x) + g(x))' = f'(x) + g'(x), \tag{2}$$

$$(f(x) \cdot g(x))' = f'(x) \cdot g(x) + f(x) \cdot g'(x), \tag{3}$$

$$\forall m \in N^+; \quad ((x-c)^m)' = m(x-c)^{m-1}. \tag{4}$$

Dôkaz. Kvôli jednoduchosti zápisov pri dôkaze rovnosti (2) predpokladajme, že

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$
$$g(x) = b_n x^n + \cdots + b_1 x + b_0.$$

Potom

$$f(x) + f(y) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0).$$

Derivovaním súčtu $f(x) + g(x)$ dostávame

$$\begin{aligned}(f(x) + g(x))' &= n(a_n + b_n)x^{n-1} + \cdots + (a_1 + b_1) = \\ &= (na_n x^{n-1} + \cdots + a_1) + (nb_n x^{n-1} + \cdots + b_1) = \\ &= f'(x) + g'(x),\end{aligned}$$

teda rovnosť (2) je pravdivá. Možno ju rozšíriť aj pre ľubovoľný počet sčítancov (podrobný dôkaz je možné urobiť matematickou indukciou).

Pre dôkaz rovnosti (3) označíme

$$f(x) = a_m x^m + \cdots + a_1 x + a_0 = \sum_{i=0}^{m} a_i x^i,$$

$$g(x) = b_n x^n + \cdots + b_1 x + b_0 = \sum_{j=0}^{n} b_i x^i.$$

Súčin polynómov $f(x)$, $g(x)$ obsahuje členy (sčítance) tvaru

$$a_i x^i b_j x^j, \quad \text{kde} \quad i \in \{1, \ldots, m\}, \quad j \in \{1, \ldots, n\}.$$

Deriváciou takéhoto člena dostávame

$$(a_i x^i b_j x^j)' = (a_i b_j x^{i+j})' = (i+j) a_i b_j x^{i+j-1} = i a_i x^{i-1} \cdot b_j x^j + a_i x^i \cdot j b_j x^{j-1} =$$
$$= (a_i x^i)' \cdot (b_j x^j) + (a_i x^i) \cdot (b_j x^j)'.$$

Potom postupnými úpravami dostávame

$$(f(x) \cdot g(x))' =$$
$$= \left(\sum_{i=0}^{m} a_i x^i \cdot \sum_{j=0}^{n} b_j x^j \right)' = \left(\sum_{i=0}^{m} \sum_{j=0}^{n} a_i x^i b_j x^j \right)' =$$
$$= \sum_{i=0}^{m} \sum_{j=0}^{n} \left(a_i x^i b_j x^j \right)' = \sum_{i=0}^{m} \sum_{j=0}^{n} \left(\left(a_i x^i \right)' \cdot \left(b_j x^j \right) + \left(a_i x^i \right) \cdot \left(b_j x^j \right)' \right) =$$
$$= \sum_{i=0}^{m} \left(a_i x^i \right)' \cdot \sum_{j=0}^{n} b_j x^j + \sum_{i=0}^{m} a_i x^i \cdot \sum_{j=0}^{n} \left(b_j x^j \right)' =$$
$$= \left(\sum_{i=0}^{m} a_i x^i \right)' \cdot \sum_{j=0}^{n} b_j x^j + \sum_{i=0}^{m} a_i x^i \cdot \left(\sum_{j=0}^{n} b_j x^j \right)' =$$
$$= f'(x) \cdot g(x) + f(x) \cdot g'(x),$$

teda rovnosť (3) je pravdivá.

Vzťah (4) dokážeme matematickou indukciou vzhľadom na m.

1. Pre $m = 1$ je $((x-c)^1)' = 1$ a $1 \cdot (x-c)^0 = 1$.
2. Ukážeme, že za predpokladu

$$((x-c)^k)' = k(x-c)^{k-1}$$

platí

$$((x-c)^{k+1})' = (k+1)(x-c)^k.$$

Postupnými úpravami s využitím indukčného predpokladu dostávame

$$((x-c)^{k+1})' = ((x-c)^k (x-c))' = k(x-c)^{k-1}(x-c) + (x-c)^k (x-c)^0 =$$
$$= k(k-c)^k + (x-c)^k = (k+1)(x-c)^k.$$

Platí teda aj vzťah (4).

6.4 Definícia. Nech $f(x)$ je polynóm jednej premennej nad poľom F a nech $k \in N$ Potom definujeme k-tu deriváciu $f^{(k)}(x)$ polynómu $f(x)$ takto:

$$f^{(1)}(x) = f'(x),$$
$$f^{(k+1)}(x) = \left(f^{(k)}(x) \right)'.$$

Ďalej sa obmedzíme len na polynómy nad poľom komplexných čísel. Zameriame sa na to, ako súvisí násobnosť koreňa polynómu s jeho deriváciami.

6.5 Veta. *Ak c je k-násobným koreňom polynómu $f(x)$, tak c je $(k-1)$-násobným koreňom polynómu $f'(x)$.*

Dôkaz. Nech c je k-násobným ($k \geq 1$) koreňom polynómu $f(x)$. Potom

$$f(x) = (x-c)^k \cdot g(x), \quad \text{pričom} \quad g(c) \neq 0$$

a

$$\begin{aligned} f'(x) &= k(x-c)^{k-1} \cdot g(x) + (x-c)^k \cdot g'(x) = \\ &= (x-c)^{k-1} \cdot (kg(x) + (x-c) \cdot g'(x)). \end{aligned}$$

Pretože pre polynóm $h(x) = kg(x) + (x-c) \cdot g'(x)$ platí

$$h(c) = kg(c) + (c-c) \cdot g'(c) = kg(c) \neq 0,$$

tak c je $(k-1)$-násobný koreň polynómu $f'(x)$.

6.6 Veta. *Nech $f(x)$ je polynóm stupňa $n \geq 2$. Potom c je k-násobným koreňom polynómu $f(x)$ vtedy a len vtedy, keď*

$$f(c) = 0, f'(c) = 0, \ldots, f^{(k-1)}(c) = 0, f^{(k)}(c) \neq 0. \tag{5}$$

Dôkaz. Nech c je k-násobným koreňom polynómu $f(x)$. Potom je (podľa vety 6.5) $(k-1)$-násobným koreňom polynómu $f'(x)$, $(k-2)$-násobným koreňom polynómu $f^{(2)}(x)$ atď., až $(k-(k-1))$-násobným (t.j. jednoduchým) koreňom polynómu $f^{(k-1)}(x)$ a nie je koreňom polynómu $f^{(k)}(x)$ (je jeho 0-násobným koreňom). Podmienky (5) sú teda splnené.

Obrátené tvrdenie budeme dokazovať sporom. Predpokladajme, že podmienky (5) sú splnené a c nie je k-násobným koreňom polynómu $f(x)$.

Ak c je l-násobným koreňom a $l < k$, tak $f^{(l)}(c) \neq 0$, čo je spor s (5).

Ak c je l-násobným koreňom a $l > k$, tak $f^{(k)}(c) = 0$, čo je opäť spor s (5).

Platí teda $k = l$, čo znamená, že c je k-násobným koreňom polynómu $f(x)$.

6.7 Príklad. Určte $a, b \in R$ tak, aby polynóm

$$f(x) = x^3 + ax^2 + bx + 1$$

mal dvojnásobný koreň $c = -2$.

Riešenie. Určíme $f'(x)$, $f(-2)$, $f'(-2)$.

$$\begin{aligned} f'(x) &= 3x^2 + 2ax + b, \\ f(-2) &= -8 + 4a - 2b + 1, \\ f'(-2) &= 12 - 4a + b. \end{aligned}$$

Podľa predchádzajúcej vety musí byť $f(-2) = f'(-2) = 0$, t.j.

$$\begin{aligned} 4a - 2b - 7 &= 0, \\ -4a + 2b + 12 &= 0. \end{aligned}$$

Z toho dostávame $a = \frac{17}{4}$, $b = 5$. Pretože $f^{(2)}(x) = 6x + 2a$ a $f^{(2)}(-2) \neq 0$, tak -2 je dvojnásobným koreňom polynómu $f(x)$.

6.8 Dôsledok. *Polynóm $f(x) \in C\langle x\rangle$ má aspoň jeden viacnásobný koreň práve vtedy, keď polynómy $f(x)$, $f'(x)$ majú spoločný deliteľ aspoň prvého stupňa.*

Dôkaz. nech $f(x)$ má k-násobný ($k \geq 2$) koreň c. Potom, podľa vety 6.6, je $f(c) = f'(c) = 0$ čo podľa vety 4.3 znamená, že $x - c$ delí polynómy $f(x)$, $f'(x)$ a existuje teda ich spoločný deliteľ aspoň prvého stupňa.

Naopak, nech $d(x)$ je spoločný deliteľ polynómov $f(x)$, $f'(x)$ a nech $\operatorname{st} d(x) \geq 1$. Potom existujú polynómy $g(x)$, $q(x)$, že

$$f(x) = d(x) \cdot g(x), \qquad f'(x) = d(x) \cdot q(x).$$

Podľa vety 4.12 má polynóm $d(x)$ koreň $c \in C$, teda $d(c) = 0$. Potom $f(c) = 0$ aj $f'(c) = 0$, čo podľa vety 6.6 znamená, že prvok c je aspoň dvojnásobným koreňom polynómu $f(x)$.

6.9 Veta. *Nech $f(x)$ je polynóm stupňa $n \geq 1$. Nech $\mathrm{D}(f(x), f'(x)) = d(x)$. Potom polynóm $F(x)$, pre ktorý platí $f(x) = d(x) \cdot F(x)$, má tie isté korene ako polynóm $f(x)$, ale všetky jednoduché.*

Dôkaz. Nech $f(x)$ má k-násobný koreň c. Potom v kanonickom rozklade polynómu $f(x)$ sa nachádza činiteľ $(x - c)^k$ a v kanonickom rozklade polynómu $f'(x)$ sa nachádza (podľa vety 6.5) činiteľ $(x - c)^{k-1}$. Preto sa v kanonickom rozklade polynómu $d(x) = \mathrm{D}(f(x), f'(x))$ nachádza (podľa vety 3.7) činiteľ $(x-c)^{k-1}$. V kanonickom rozklade polynómu $F(x)$ sa teda musí (podľa dôsledku 3.5) nachádzať činiteľ $x - c$, čo znamená, že c je jednoduchým koreňom polynómu $F(x)$.

Zostrojenie polynómu $F(x)$, ktoré je popísané v predchádzajúcej vete sa nazýva „odstraňovanie viacnásobných koreňov“.

6.10 Príklad. Hľadajme korene polynómu

$$g(x) = x^5 - 6x^4 + 16x^3 - 24x^2 + 20x - 8.$$

Tento polynóm má jediný racionálny koreň 2. Preto

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

Teraz stačí nájsť korene polynómu $f(x) = x^4 - 4x^3 + 8x^2 - 8x + 4$. Tento polynóm už nemá racionálne korene. Overíme, či má viacnásobné korene. Najväčší spoločný deliteľ polynómov $f(x)$, $f'(x)$ je polynóm $d(x) = x^2 - 2x + 2$ (podrobne sa presvedčte). Z toho dostávame, že aj $F(x) = x^2 - 2x + 2$. Koreňmi polynómu $F(x)$ sú čísla $1 + i$ a $1 - i$. Polynóm $g(x)$ má teda korene: -2 jednoduchý, $1 + i$ dvojnásobný a $1 - i$ tiež dvojnásobný.

Niekedy, napr. pri rozklade polynómu na parciálne zlomky, je užitočné vyjadriť polynóm v nejakom inom tvare. Jednu z možností popíšeme v nasledujúcej vete.

6.11 Veta. *Nech $f(x) = a_n x^n + \cdots + a_1 x + a_0$ je polynóm stupňa $n \geq 1$ nad poľom C a nech $c \in C$. Potom existujú jednoznačne určené prvky $b_0, b_1, \ldots, b_n$, že*

$$f(x) = b_n(x - c)^n + b_{n-1}(x - c)^{n-1} + \cdots + b_2(x - c)^2 + b_1(x - c) + b_0. \tag{6}$$

Dôkaz. Matematickou indukciou vzhľadom na n.

1. Nech $n = 1$. Potom podľa lemy 4.4 je $f(x) = q(x)(x-c) + f(c)$, kde polynóm $q(x)$ je nultého stupňa, t.j. $q(x) = b_1 \in C$. Ak označíme $f(c) = b_0$, tak $f(x) = b_1(x-c) + b_0$. Z vety 2.1 vyplýva, že prvky b_1, b_0 sú určené jednoznačne.

2. Predpokladajme, že tvrdenie platí pre každý polynóm stupňa menšieho ako n. Pre polynómy $f(x)$, $x-c$ (opäť podľa lemy 4.4) platí $f(x) = (x-c)q(x) + f(c)$, pričom polynóm $q(x)$ je stupňa $n-1$. Podľa indukčného predpokladu existujú teda prvky $d_0, \ldots, d_{n-1} \in C$, že

$$q(x) = d_{n-1}(x-c)^{n-1} + \cdots + d_1(x-c) + d_0.$$

Po dosadení a úprave máme

$$f(x) = d_{n-1}(x-c)^n + \cdots + d_1(x-c)^2 + d_0(x-c) + f(c).$$

Ak označíme $b_0 = f(c)$ a $b_i = d_{i-1}$ pre každé $i \in \{1, \ldots, n\}$, tak dostávame (6). Ukážeme ešte jednoznačnosť vyjadrenia. Predpokladajme, že ďalšie vyjadrenie polynómu $f(x)$ je

$$f(x) = k_m(x-c)^m + \cdots + k_2(x-c)^2 + k_1(x-c) + k_0.$$

Pretože polynóm $f(x)$ je stupňa n, tak $m = n$. Upravme obidve vyjadrenia polynómu $f(x)$:

$$f(x) = (x-c)(b_n(x-c)^{n-1} + \cdots + b_2(x-c) + b_1) + b_0,$$
$$f(x) = (x-c)(k_n(x-c)^{n-1} + \cdots + k_2(x-c) + k_1) + k_0.$$

Z toho (podľa vety 2.1) vyplýva, že

$$b_0 = k_0 \quad \text{a} \quad b_n(x-c)^{n-1} + \cdots + b_2(x-c) + b_1 = k_n(x-c)^{n-1} + \cdots + k_2(x-c) + k_1,$$

z čoho (podľa indukčného predpokladu) dostávame, že aj

$$b_1 = k_1, b_2 = k_2, \ldots, b_n = k_n,$$

čím je aj jednoznačnosť dokázaná.

Zápis polynómu $f(x)$ v tvare (6) sa volá *Taylorov rozvoj polynómu $f(x)$ podľa mocnín $x-c$* alebo *v bode (so stredom) c*. Prvky $b_0, \ldots, b_n$ sa nazývajú *koeficienty* Taylorovho rozvoja. Dá sa ukázať, že

$$b_i = \frac{f^{(i)}(c)}{i!}, \quad \text{pre každé} \quad i \in \{1, \ldots, n\},$$

pričom $f^{(0)}(c) = f(c)$, $0! = 1$.

Koeficienty $b_0, b_1, \ldots, b_n$ môžeme ale pohodlnejšie vypočítať pomocou Hornerovej schémy. Návod dáva už predchádzajúca veta. Rovnosť (6) upravme na tvar

$$f(x) = (x-c)(b_n(x-c)^{n-1} + \cdots + b_2(x-c) + b_1) + b_0.$$

Prvok b_0 je zvyšok, ktorý dostaneme pri delení polynómu $f(x)$ dvojčlenom $x-c$ (čo vieme urobiť pomocou Hornerovej schémy). Ak označíme

$$q_1(x) = b_n(x-c)^{n-1} + \cdots + b_2(x-c) + b_1,$$

tak po úprave máme

$$q_1(x) = (x-c)(b_n(x-c)^{n-2} + \cdots + b_2) + b_1$$

a opäť vidíme, že prvok b_1 je zvyšok pri delení polynómu $q_1(x)$ dvojčlenom $x-c$. Takto môžeme postupovať ďalej, takže jednotlivé čiastkové podiely budú označené $q_1(x), q_2(x), \ldots, q_n(x)$ a b_i bude zvyšok pri delení polynómu $q_i(x)$ dvojčlenom $x-c$, pre $i \in \{1, 2, \ldots, n\}$.

Výpočet koeficientov Taylorovho rozvoja polynómu pomocou Hornerovej schémy ukážeme na príklade.

6.12 Príklad. Nájdeme Taylorov rozvoj polynómu

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

podľa mocnín $x - 2$. Koeficienty b_0, b_1, b_2, b_3, b_4 nájdeme postupným delením tak, ako sme popísali vyššie.

$$\begin{array}{lllll} 1 & 3 & -2 & 3 & 1 \\ & 2 & 10 & 16 & 38 \\ \hline 1 & 5 & 8 & 19 & \lfloor 39 = b_0 \\ & 2 & 14 & 44 & \\ \hline 1 & 7 & 22 & \lfloor 63 = b_1 & \\ & 2 & 18 & & \\ \hline 1 & 9 & \lfloor 40 = b_2 & & \\ & 2 & & & \\ \hline 1 & \lfloor 11 = b_3 & & & \\ \hline \lfloor 1 = b_4 & & & & \end{array}$$

Taylorov rozvoj daného polynómu je teda

$$f(x) = (x-2)^4 + 11(x-2)^3 + 40(x-2)^2 + 63(x-2) + 39.$$

Cvičenia

1. Určte $a \in R$ tak, aby polynóm $x^3 - 5x^2 + 3x + a$ mal dvojnásobný koreň. Určte tretí koreň.
2. Nájdite Taylorov rozvoj polynómu $x^4+11x^3+45x^2+81x+55$ podľa mocnín $x + 3$.
3. Určte koeficienty polynómu $(x-2)^4+4(x-2)^3+6(x-2)^2+10(x-2)+20$.

7 Polynómy viacerých neurčitých

Okruh polynómov neurčitých $x_1, \ldots, x_n$ nad okruhom A je okruh $A[x_1, \ldots, x_n]$, ktorý vznikne adjunkciou algebraicky nezávislých prvkov (nad A) k okruhu A (pozri v [1], str. 67). Pod polynómom n neurčitých $x_1, \ldots, x_n$ nad poľom F budeme teda rozumieť výraz (term) tvaru

$$(1) \qquad a_0 x_1^{k_{01}} \cdot \ldots \cdot x_n^{k_{0n}} + a_1 x_1^{k_{11}} \cdot \ldots \cdot x_n^{k_{1n}} + \cdots + a_r x_1^{k_{r1}} \cdot \ldots \cdot x_n^{k_{rn}},$$

kde $a_1, \ldots, a_r \in F$ a $k_{ij} \in N$, $i \in \{0, \ldots, r\}$, $j \in \{1, \ldots, n\}$. Prvky $a_o, \ldots, a_r$ nazývame *koeficienty* a sčítance

$$a_0 x_1^{k_{01}} \cdot \ldots \cdot x_n^{k_{0n}},\ a_1 x_1^{k_{11}} \cdot \ldots \cdot x_n^{k_{1n}},\ \ldots,\ a_r x_1^{k_{r1}} \cdot \ldots \cdot x_n^{k_{rn}}$$

nazývame *členy* polynómu (1).

Podobne ako pre polynómy jednej neurčitej je možné ukázať, že ak F je pole, tak $F[x_1, \ldots, x_n]$ je obor integrity.

Keď budeme ďalej hovoriť o polynómoch n neurčitých, budeme mať na mysli polynómy nad nejakým číselným poľom a nebudeme to zvlášť zdôrazňovať a zapisovať. Polynómy neurčitých $x_1, \ldots, x_n$ budeme obvykle označovať $f(x_1, \ldots, x_n)$, $g(x_1, \ldots, x_n)$ a pod. Napríklad

$$f(x_1, x_2, x_3) = x_1^4 + x_1x_2x_3 + x_3^2, \quad g(x_1, x_2, x_3) = 2x_1 + x_3, \quad h(x_1, x_2, x_3) = 5$$

sú polynómy troch neurčitých (napr. nad poľom Q).

Ak sú každé dve z n-tíc $[k_{01}, \ldots, k_{0n}], \ldots, [k_{r1}, \ldots, k_{rn}]$ rôzne hovoríme, že polynóm (1) je zapísaný v *normálnom* tvare. *Stupňom člena* $ax_1^{r_1} \cdot \ldots \cdot x_n^{r_n}$, $a \neq 0$ nazývame číslo $r_1 + \cdots + r_n$ a usporiadanú n-ticu $[r_1, \ldots, r_n]$ nazývame *výškou* tohoto člena. *Stupňom polynómu* napísaného v normálnom tvare nazývame maximálny zo stupňov jednotlivých členov. Pre ľubovoľné dve výšky $[k_1, \ldots, k_n]$, $[m_1, \ldots, m_n]$ sa definuje relácia $<$ takto:

$$[k_1, \ldots, k_n] < [m_1, \ldots, m_n],$$

ak v postupnosti $m_1 - k_1, \ldots, m_n - k_n$ je prvé nenulové číslo kladné. Dá sa ukázať (presvedčte sa), že $<$ je reláciou usporiadania. Člen nenulového polynómu, ktorý má v tomto usporiadaní najväčšiu výšku sa nazýva *vedúcim členom* polynómu. Jeho výšku nazývame *výškou polynómu*.

Permutáciu $\varphi = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$ množiny $\{1, \ldots, n\}$ budeme stručne zapisovať $(i_1, i_2, \ldots, i_n)$. *Permutáciou polynómu* $f(x_1, \ldots, x_n)$ budeme nazývať polynóm $f(x_{i_1}, \ldots, x_{i_n})$, ktorý dostaneme zámenou neurčitých x_1 a $x_{i_1}, \ldots, x_n$ a x_{i_n}. Z uvedeného vyplýva, že člen $ax_1^{r_1} \cdot \ldots \cdot x_n^{r_n}$ je členom polynómu $f(x_1, \ldots, x_n)$ práve vtedy, keď $ax_{i_1}^{r_1} \cdot \ldots \cdot x_{i_n}^{r_n}$ je členom polynómu $f(x_{i_1}, \ldots, x_{i_n})$. Ak napríklad

$$f(x_1, x_2, x_3) = x_1^2x_2 + x_1x_2x_3 + x_3,$$

tak

$$f(x_2, x_3, x_1) = x_2^2x_3 + x_2x_3x_1 + x_1.$$

Všimnime si, že $f(x_1, x_2, x_3) \neq f(x_2, x_3, x_1)$.

7.2 Definícia. Polynóm $f(x_1, \ldots, x_n)$ nad poľom F sa nazýva symetrickým, ak $f(x_1, \ldots, x_n) = f(x_{i_1}, \ldots, x_{i_n})$ pre každú permutáciu $(i_1, \ldots, i_n)$.

Ľahko sa dá sa ukázať (presvedčte sa), že množina všetkých symetrických polynómov neurčitých $x_1, \ldots, x_n$ je podobor integrity oboru integrity polynómov n neurčitých $x_1, \ldots, x_n$.

7.3 Príklad. Polynóm

$$f(x_1, x_2, x_2) = x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 + x_1x_2^3x_3 + x_1^3x_2x_3 + x_1x_2x_3^3$$

je symetrický.

Všimnime si, že ak (nejaký) symetrický polynóm $f(x_1, x_2, x_3)$ obsahuje napríklad člen $x_1^2x_2$, tak musí obsahovať aj členy $x_1^2x_3$, $x_2^2x_1$, $x_2^2x_3$, $x_3^2x_1$, $x_3^2x_2$ a ak obsahuje napríklad člen $x_1x_2^3x_3$, tak musí obsahovať aj členy $x_1^3x_2x_3$, $x_1x_2x_3^3$. Zovšeobecnením tohoto pozorovania je nasledujúce tvrdenie.

7.4 Veta. *Nech polynóm $f(x_1, \ldots, x_n)$ je napísaný v normálnom tvare. Potom $f(x_1, \ldots, x_n)$ je symetrický práve vtedy, keď s každým svojim nenulovým členom $ax_1^{r_1} \cdot \ldots \cdot x_n^{r_n}$ a s každou permutáciou φ množiny $\{1, \ldots, n\}$ obsahuje aj člen $ax_{\varphi(1)}^{r_1} \cdot \ldots \cdot x_{\varphi(n)}^{r_n}$.*

Dôkaz. Nech polynóm $f(x_1, \ldots, x_n)$ je symetrický a nech $ax_1^{r_1} \cdot \ldots \cdot x_n^{r_n}$ je jeho člen. Potom $ax_{\varphi(1)}^{r_1} \cdot \ldots \cdot x_{\varphi(n)}^{r_n}$ je členom polynómu

$$f(x_{\varphi(1)}, \ldots, x_{\varphi(n)}) = f(x_1, \ldots, x_n).$$

Naopak, nech polynóm $f(x_1, \ldots, x_n)$ obsahuje s každým členom $ax_1^{r_1} \cdot \ldots \cdot x_n^{r_n}$ a s každou permutáciou φ aj člen $ax_{\varphi(1)}^{r_1} \cdot \ldots \cdot x_{\varphi(n)}^{r_n}$. Dokážeme, že $f(x_1, \ldots, x_n) = f(x_{\varphi(1)}, \ldots, x_{\varphi(n)})$ (t.j., že $f(x_1, \ldots, x_n)$ je symetrický). Stačí ukázať, že polynómy $f(x_1, \ldots, x_n)$, $f(x_{\varphi(1)}, \ldots, x_{\varphi(n)})$ obsahujú rovnaké členy.

a) Nech $ax_1^{r_1} \cdot \ldots \cdot x_n^{r_n}$ je členom polynómu $f(x_1, \ldots, x_n)$, nech φ je ľubovoľná permutácia a ψ k nej inverzná permutácia. Potom $ax_{\psi(1)}^{r_1} \cdot \ldots \cdot x_{\psi(n)}^{r_n}$ je (podľa predpokladu) členom polynómu $f(x_1, \ldots, x_n)$ a člen

$$ax_{\varphi(\psi(1))}^{r_1} \cdot \ldots \cdot x_{\varphi(\psi(n))}^{r_n} = ax_1^{r_1} \cdot \ldots \cdot x_n^{r_n}$$

je členom polynómu $f(x_{\varphi(1)}, \ldots, x_{\varphi(n)})$.

b) Nech $bx_{\varphi(1)}^{k_1} \cdot \ldots \cdot x_{\varphi(n)}^{k_n}$ je člen polynómu $f(x_{\varphi(1)}, \ldots, x_{\varphi(n)})$. Potom $bx_1^{k_1} \cdot \ldots \cdot x_n^{k_n}$ je členom polynómu $f(x_1, \ldots, x_n)$ a (podľa predpokladu) aj $bx_{\varphi(1)}^{k_1} \cdot \ldots \cdot x_{\varphi(n)}^{k_n}$ je členom polynómu $f(x_1, \ldots, x_n)$.

Z a) a b) vyplýva, že $f(x_1, \ldots, x_n) = f(x_{\varphi(1)}, \ldots, x_{\varphi(n)})$.

Symetrický polynóm, ktorý je súčtom všetkých navzájom rôznych členov $ax_{i_1}^{r_1} \cdot \ldots \cdot x_{i_n}^{r_n}$, kde $(i_1, \ldots, i_n)$ je permutácia množiny $\{1, \ldots, n\}$, nazývame *jednoduchý symetrický polynóm* vytvorený členom $ax_1^{r_1} \cdot \ldots \cdot x_n^{r_n}$. Stručne ho budeme zapisovať v tvare $\sum ax_1^{r_1} \cdot \ldots \cdot x_n^{r_n}$, kde $ax_1^{r_1} \cdot \ldots \cdot x_n^{r_n}$ je (zvyčajne) vedúcim členom daného jednoduchého symetrického polynómu. Z vety 7.4 bezprostredne vyplýva, že každý symetrický polynóm je súčtom jednoduchých symetrických polynómov. Symetrický polynóm uvedený v príklade 7.3 môžeme teda stručne zapísať takto

$$f(x_1, x_2, x_3) = \sum x_1^2 x_2 + \sum x_1^3 x_2 x_3.$$

Jednoduché symetrické polynómy tvaru

$$\begin{aligned} \sigma_1(x_1, \ldots, x_n) &= \sum x_1, \\ \sigma_2(x_1, \ldots, x_n) &= \sum x_1 x_2, \\ &\vdots \\ \sigma_n(x_1, \ldots, x_n) &= \sum x_1 x_2 \ldots x_n, \end{aligned}$$

sa volajú *základné symetrické polynómy*. Elementárny symetrický polynóm je teda taký jednoduchý symetrický polynóm, v ktorom sa všetky neurčité vyskytujú v

najviac prvej mocnine. Napríklad základné symetrické polynómy štyroch neurčitých x_1, x_2, x_3, x_4 sú

$$\begin{aligned}
\sigma_1(x_1,x_2,x_3,x_4) &= x_1+x_2+x_3+x_4,\\
\sigma_2(x_1,x_2,x_3,x_4) &= x_1x_2+x_1x_3+x_1x_4+x_2x_3+x_2x_4+x_3x_4,\\
\sigma_3(x_1,x_2,x_3,x_4) &= x_1x_2x_3+x_1x_2x_4+x_1x_3x_4+x_2x_3x_4,\\
\sigma_4(x_1,x_2,x_3,x_4) &= x_1x_2x_3x_4.
\end{aligned}$$

Nech $f(x)$ je normovaný polynóm nad poľom C. V nasledovných úvahách ho budeme zapisovať v tvare

$$f(x) = x_n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n. \tag{2}$$

Korene polynómu $f(x)$ označme $x_1, x_2, \ldots, x_n$. Potom rozklad polynómu $f(x)$ na koreňové činitele je

$$f(x) = (x-x_1)(x-x_2)\ldots(x-x_n). \tag{3}$$

Ak v (2) koreňové činitele vynásobíme, upravíme a porovnáme koeficienty vo vyjadrení (2) a (3), tak dostávame

$$\begin{aligned}
-a_1 &= x_1+x_2+\cdots+x_n = \sigma_1(x_1,\ldots,x_n),\\
a_2 &= x_1x_2+x_1x_3+\cdots+x_{n-1}x_n = \sigma_2(x_1,\ldots,x_n),\\
-a_3 &= x_1x_2x_3+x_1x_2x_4+\cdots+x_{n-2}x_{n-1}x_n = \sigma_3(x_1,\ldots,x_n),\\
&\vdots\\
(-1)^n a_n &= x_1x_2\ldots x_n = \sigma_n(x_1,\ldots,x_n).
\end{aligned} \tag{4}$$

Vzťahy (4) môžu umožniť výpočet koreňov polynómu $f(x)$, ak sú dané aj nejaké ďalšie vzťahy medzi koreňmi. V konkrétnych prípadoch, keď nemôže dôjsť k nedorozumeniu, tak miesto $\sigma_i(x_1,\ldots,x_n)$ píšeme len σ_i.

7.5 Príklad. Nájdite korene polynómu

$$f(x) = x^3 - \sqrt{2}x^2 - 5x + 5\sqrt{2},$$

ak viete, že dva z koreňov sú navzájom opačné čísla

Riešenie. Ak korene polynómu $f(x)$ označíme x_1, x_2, x_3, tak zo (4) dostávame

$$\begin{aligned}
x_1+x_2+x_3 &= \sqrt{2},\\
x_1x_2+x_1x_3+x_2x_3 &= -5,\\
x_1x_2x_3 &= -5\sqrt{2}.
\end{aligned}$$

Korene, ktoré sú opačné označme napr. x_1, x_2. Potom $x_2 = -x_1$ a z prvej rovnice dostávame, že $x_3 = \sqrt{2}$. Po dosadení do druhej rovnice a úprave máme $x_1^2 = 5$, t.j. $x_1 = \sqrt{5}$ alebo $x_1 = -\sqrt{5}$.

Ak $x_1 = \sqrt{5}$, tak $x_2 = -\sqrt{5}$, $x_3 = \sqrt{2}$.

Ak $x_1 = -\sqrt{5}$, tak $x_2 = \sqrt{5}$, $x_3 = \sqrt{2}$.

Skúškou správnosti sa presvedčíme, že vypočítané korene vyhovujú aj tretej rovnici. Koreňmi polynómu $f(x)$ sú teda čísla $\sqrt{5}$, $-\sqrt{5}$, $\sqrt{2}$.

Nech $f(x_1, x_2) = x_1^2 + x_2^2$. Tento jednoduchý symetrický polynóm môžeme ľahko vyjadriť pomocou základných symetrických polynómov. Po jednoduchej úprave dostávame

$$f(x_1, x_2) = x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 = \sigma_1^2 - 2\sigma_2.$$

Analogicky je možné vyjadriť každý jednoduchý symetrický a teda aj každý symetrický polynóm.

7.6 Veta. *Ku každému symetrickému polynómu $f(x_1, \ldots, x_n)$ existuje práve jeden polynóm $g(y_1, \ldots, y_n)$,že*

$$f(x_1, \ldots, x_n) = g(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma(x_1, \ldots, x_n)).$$

Polynóm $g(\sigma_1(x_1, \ldots, x_n), \ldots, \sigma(x_1, \ldots, x_n))$ je vlastne polynóm n neurčitých, kde neurčitými sú základné symetrické polynómy $\sigma_1, \ldots, \sigma_n$. Dôkaz vety 7.6 vynecháme, ale uvedieme príklad, riešenie ktorého naznačuje postup dôkazu.

7.7 Príklad. Pomocou základných symetrických polynómov vyjadríme jednoduchý symetrický polynóm

$$f(x_1, x_2, x_3) = x_1^2x_2 + x_1^2x_3 + x_2^2x_1 + x_2^2x_3 + x_3^2x_1 + x_3^2x_2 = \sum x_1^2x_2.$$

Vedúci člen polynómu $\sum x_1^2x_2$ je člen $x_1^2x_2$. Vedúcim členom súčinu $\sigma_1\sigma_2$ je tiež člen $x_1^2x_2$. Po vypočítaní rozdielu $\sum x_1^2x_2 - \sigma_1\sigma_2$ dostávame

$$\sum x_1^2x_2 - \sigma_1\sigma_2 = \sum x_1^2x_2 - (\sum x_1^2x_2 - 3\sigma_3)$$

(podrobne sa o tom presvedčte), z čoho vyplýva

$$f(x_1, x_2, x_3) = \sum x_1^2x_2 = \sigma_1\sigma_2 + 3\sigma_3.$$

Podobne postupujeme aj v komplikovanejších prípadoch. Symetrický polynóm je súčtom jednoduchých symetrických polynómov. Ku každému jednoduchému symetrickému polynómu nájdeme súčin základných symetrických polynómov tak, aby jeho vedúci člen bol taký istý, ako vedúci člen daného jednoduchého polynómu. Ich rozdiel má zrejme vedúci člen nižšieho stupňa. Takto postupujeme ďalej, až kým vo vyjadrení nie sú len základné symetrické polynómy.

7.8 Príklad. Napíšte polynóm, ktorého koreňmi sú druhé mocniny koreňov polynómu $f(x) = x^3 - x^2 + 2x - 1$.

Riešenie. Pre korene c_1, c_2, c_3 polynómu $f(x)$ platí

$$\begin{aligned}
\sigma_1 &= c_1 + c_2 + c_3 = 1,\\
\sigma_2 &= c_1c_2 + c_1c_3 + c_2c_3 = 2,\\
\sigma_3 &= c_1c_2c_3.
\end{aligned}$$

Potrebujeme určiť koeficienty polynómu $g(x) = x^3 + b_1x^2 + b_2x + b_3$, ktorého korene budú čísla c_1^2, c_2^2, c_3^2. Zo vzťahov (4) pre ne dostávame

$$\begin{aligned} b_1 &= -(c_1^2 + c_2^2 + c_3^2), \\ b_2 &= c_1^2c_2^2 + c_1^2c_3^2 + c_2^2c_3^2, \\ b_3 &= -c_1^2c_2^2c_3^2. \end{aligned}$$

Jednoduché symetrické polynómy $\sum c_1^2$, $\sum c_1^2c_2^2$, $\sum c_1^2c_2^2c_3^2$ vyjadríme pomocou základných symetrických polynómov:

$$\sum c_1^2 - \sigma_1^2 = \sum c_1^2 - (\sum c_1^2 + 2\sum c_1c_2) = -2\sigma_2,$$

teda $\sum c_1^2 = \sigma_1^2 - 2\sigma_2$.

$$\sum c_1^2c_2^2 - \sigma_2^2 = \sum c_1^2c_2^2 - (\sum c_1^2c_2^2 + 2\sum c_1^2c_2c_3) = -2\sum c_1^2c_2c_3 = -2\sigma_1\sigma_3,$$

teda $\sum c_1^2c_2^2 = \sigma_2^2 - 2\sigma_1\sigma_3$ a nakoniec $\sum c_1^2c_2^2c_3^2 = \sigma_3^2$. Pre koeficienty b_1, b_2, b_3 tak dostávame

$$\begin{aligned} b_1 &= -(\sigma_1^2 - 2\sigma_2) = -(1^2 - 2 \cdot 2) = 3, \\ b_2 &= \sigma_2^2 - 2\sigma_1\sigma_3 = 2^2 - 2 \cdot 1 \cdot 1 = 2, \\ b_3 &= -\sigma_3^2 = -1^2 = -1 \end{aligned}$$

a teda $g(x) = x^3 + 3x^2 + 2x - 1$.

Ak polynóm $f(x) = x_n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ má korene $x_1, x_2, \ldots, x_n$, tak prvok

$$D_n = \begin{matrix} (x_1 - x_2)^2 & (x_1 - x_3)^2 & \ldots\ldots\ldots & (x_1 - x_n)^2 \\ & (x_2 - x_3)^2 & \ldots\ldots\ldots & (x_2 - x_n)^2 \\ & & & \vdots \\ & & (x_{n-2} - x_{n-1})^2 & (x_{n-2} - x_n)^2 \\ & & & (x_{n-1} - x_n)^2 \end{matrix}$$

nazývame *diskriminant polynómu* $f(x)$. Na diskriminant D_n sa môžeme dívať aj ako na symetrický polynóm n neurčitých.

Polynóm druhého stupňa $f(x) = x^2 + a_1x + a_2$ s koreňmi x_1, x_2 má teda diskriminant $(x_1 - x_2)^2$. Ak ho vyjadríme pomocou základných symetrických polynómov a využijeme vzťahy (4), tak dostávame

$$D_n = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = (-a_1)^2 - 4a_2.$$

Podobne, aj pre polynóm tretieho stupňa $f(x) = x^3 + a_1x^2 + a_2x + a_3$ je možné vyjadriť diskriminant pomocou koeficientov v tvare

$$D_3 = a_1^2a_2^2 - 4a_1^3a_3 - 4a_2^3 + 18a_1a_2a_3 - 27a_3^2.$$

Všimnime si, že diskriminant polynómu je rôzny od nuly práve vtedy, keď nemá viacnásobné korene.

7.9 Veta. *Nech $f(x)$ je polynóm s reálnymi koeficientami, ktorý nemá viacnásobné korene. Diskriminant polynómu $f(x)$ je kladný práve vtedy, keď počet párov imaginárnych komplexne združených koreňov je číslo párne a je záporný, keď počet párov takýchto koreňov je číslo nepárne.*

Dôkaz. Pretože $f(x)$ je polynóm s reálnymi koeficientami, tak s každým koreňom c má aj komplexne združený koreň $\overline{c}$. Pre ľubovoľnú dvojicu koreňov c_i, c_j nastáva práve jedna z možností: obidva sú reálne, jeden je reálny a druhý imaginárny, obidva sú imaginárne ale nie komplexne združené, sú komplexne združené.

1. Ak c_i, c_j sú reálne, tak $(c_i - c_j)^2 > 0$.
2. Ak (napr.) c_i je reálny, c_j imaginárny, tak $(c_i - c_j)^2(c_i - \overline{c_j})^2 > 0$.
3. Ak c_i, c_j sú imaginárne ale nie komplexne združené, tak $(c_i - c_j)^2(\overline{c_i} - \overline{c_j})^2 > 0$.
4. Ak c_i, c_j sú komplexne združené, tak $(c_i - c_j)^2 < 0$.

Z 1. – 4. vyplýva tvrdenie vety.

2.10 Dôsledok. *Polynóm tretieho stupňa s reálnymi koeficientami má tri rôzne reálne korene práve vtedy, keď jeho diskriminant je kladný a má jeden reálny a dva imaginárne (komplexne združené) korene práve vtedy, keď jeho diskriminant je záporný.*

Cvičenia

1. Korene polynómu $x^3 - 3x^2 - 2x - 1$ označme c_1, c_2, c_3. Vypočítajte hodnotu výrazu
   a) $c_1^2 + c_2^2 + c_3^2$,
   b) $\frac{1}{c_1^2} + \frac{1}{c_2^2} + \frac{1}{c_3^2}$,
   c) $(c_1 - c_2)^2 + (c_1 - c_3)^2 + (c_2 - c_3)^2$.
2. Nech c_1, c_2, c_3 sú korene polynómu $x^3 - 2x^2 + x + 1$. Napíšte polynóm, ktorý má korene
   a) $c_1 + 2, \quad c_2 + 2, \quad c_3 + 2$,
   b) $c_1c_2, \quad c_1c_3, \quad c_2c_3$,
   c) $c_1 + c_2, \quad c_1 + c_3, \quad c_2 + c_3$,
   d) $c_1^2, \quad c_2^2, \quad c_3^2$.
3. Riešte sústavy rovníc
   a)
   $$\begin{aligned} x + y &= 1 \\ xy &= -2, \end{aligned}$$
   b)
   $$\begin{aligned} x^2 + y^2 &= 13 \\ xy &= 6, \end{aligned}$$
   c)
   $$\begin{aligned} x + y + z &= -3 \\ xy + xz + yz &= -1 \\ xyz &= 3, \end{aligned}$$

d)

$$\begin{aligned} x + y + z &= 2 \\ x^2 + y^2 + z^2 &= 6 \\ x^3 + y^3 + z^3 &= 8. \end{aligned}$$

II. ALGEBRAICKÉ ROVNICE

Nech $f(x) = a_n x^n + \cdots + a_1 x + a_0$ je polynóm jednej premennej nad poľom komplexných čísel. Pod *(algebraickou) rovnicou* budeme rozumieť výrokovú formu typu

$$(1) \qquad (f(x) =) \quad a_n x_n + \cdots + a_1 x + a_0 = 0.$$

V praxi je často algebraická rovnica zapísaná v tvare

$$(2) \qquad (L(x) =) \quad b_n x_n + \cdots + b_1 x + b_0 = c_m x^m + \cdots + c_1 x + c_0 \quad (= P(x)),$$

kde $L(x)$ a $P(x)$ sú polynómy nazývané pravá a ľavá strana rovnice (2). *Riešením* alebo *koreňom* rovnice (1) resp. (2) je číslo $c \in C$, pre ktoré $f(c) = 0$ resp. $L(c) = P(c)$. *Riešiť rovnicu* znamená nájsť všetky jej riešenia. Pojem „riešenie rovnice“ je možné chápať aj ako jej korene aj ako proces, ktorého cieľom je určenie množiny všetkých koreňov rovnice iným (zrozumiteľným) spôsobom, napr. vymenovaním prvkov alebo vzorcom. Určiť korene polynómu $f(x)$ resp. určiť korene rovnice $f(x) = 0$ je len rôzna formulácia tej istej úlohy.

Pri riešení rovníc často používame ekvivalentné úpravy. Miesto pôvodnej rovnice potom hľadáme riešenie rovnice s ňou ekvivalentnej (jednoduchšej), t.j. rovnice, ktorá má s pôvodnou rovnakú množinu riešení. Podrobnejšie o ekvivalentných úpravách pozri napr. v [1], kapitola 15.

Riešenie rovnice sa nazýva *algebraickým*, ak je korene možné vyjadriť pomocou jej koeficientov a použitím len operácií sčitovania, odčitovania, násobenia, delenia a odmocňovania.

V nasledujúcich článkoch sa budeme zaoberať niektorými typmi rovníc, ktoré je možné riešiť algebraicky a tzv. približným riešením rovníc.

1 Binomické rovnice

Rovnicu $x^n - a = 0$, kde $a \neq 0$ voláme *binomická rovnica*. Ak c je jej koreňom, tak často píšeme $c = \sqrt[n]{a}$ a hovoríme, že c je n-tá *(komplexná) odmocnina* čísla a. Ak a je kladné reálne číslo, tak symbol $\sqrt[n]{a}$ bude znamenať (tak, ako sme to používali aj na strednej škole) nezáporné reálne číslo b, pre ktoré je $b^n = a$. V ostatných prípadoch bude symbol $\sqrt[n]{a}$ označovať jeden z koreňov binomickej rovnice $x^n - a = 0$.

Teraz uvedieme tzv goniometrické riešenie binomickej rovnice.

1.1 Veta. *Korene binomickej rovnice*

$$(1) \qquad x^n - a = 0, \quad \textit{kde} \quad a = |a|(\cos\alpha + i\sin\alpha),$$

sú komplexné čísla

$$(2) \qquad c_k = \sqrt[n]{|a|}\left(\cos\frac{\alpha + 2k\pi}{n} + i\sin\frac{\alpha + 2k\pi}{n}\right) \quad \textit{pre} \quad k \in \{0, \ldots, n-1\}.$$

Dôkaz. Nech $c = |c|(\cos\varphi + i\sin\varphi)$ je koreňom rovnice (1). Potom $c^n = a$ a po dosadení a umocnení, pomocou Moivreovej vety, dostávame

$$|c|^n(\cos n\varphi + i\sin n\varphi) = |a|(\cos\alpha + i\sin\alpha).$$

Komplexné čísla sa rovnajú práve vtedy, keď sa rovnajú ich absolútne hodnoty a ich amplitúdy sa líšia o celočíselný násobok čísla 2π. Preto

$$|c|^n = |a|, \quad \text{a} \quad n\varphi = \alpha + 2k\pi, \quad k \in Z,$$

z čoho máme

$$|c| = \sqrt[n]{|a|} \quad \text{a} \quad \varphi = \frac{\alpha + 2k\pi}{n}, \quad k \in Z.$$

Ak je teda c koreň rovnice (1), tak

$$c = c_k = \sqrt[n]{|a|}\left(\cos\frac{\alpha + 2k\pi}{n} + i\sin\frac{\alpha + 2k\pi}{n}\right), \quad k \in Z.$$

Skúškou správnosti sa môžeme presvedčiť, že pre každé $i \in Z$ je c_k koreňom rovnice (1). Rovnica n-tého stupňa má ale v C práve n koreňov. Zvoľme len korene $c_0, \ldots, c_{n-1}$. Ukážeme, že pre $k \neq l$, $k, l \in \{0, \ldots, n-1\}$ je $c_k \neq c_l$. Predpokladajme, že $c_k = c_l$, t.j.

$$\sqrt[n]{|a|}\left(\cos\frac{\alpha + 2k\pi}{n} + i\sin\frac{\alpha + 2k\pi}{n}\right) = \sqrt[n]{|a|}\left(\cos\frac{\alpha + 2l\pi}{n} + i\sin\frac{\alpha + 2l\pi}{n}\right).$$

Potom

$$\frac{\alpha + 2k\pi}{n} = \frac{\alpha + 2k\pi}{n} + 2m\pi.$$

Z toho po úprave máme $k - l = m \cdot n$. Preto n delí $k - l$, z čoho vyplýva (lebo $0 \leq |k - l| < n$), že $k - l = 0$, t.j. $k = l$. Množina $\{c_0, \ldots, c_{n-1}\}$ je teda množinou všetkých riešení binomickej rovnice (1).

Každý z koreňov c_k rovnice (1) môžeme (s využitím Moivreovej vety) vyjadriť v tvare

$$\sqrt[n]{|a|}\left(\cos\frac{\alpha}{n} + i\sin\frac{\alpha}{n}\right) \cdot \left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right).$$

Označíme $\varepsilon_k = \left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right)$. Množina $K_n = \{\varepsilon_0, \ldots, \varepsilon_{n-1}\}$ je vlastne množinou všetkých riešení rovnice $x^n - 1 = 0$ (je to množine všetkých komplexných odmocnín jednotky). Množina K_n s operáciou násobenia komplexných čísel je cyklickou grupou (pozri v [2] príklad 4.8 a kapitolu 5). Každý prvok grupy $(K_n, \cdot)$, ktorý je jej generátorom, nazveme *primitívnym koreňom* rovnice $x^n - 1 = 0$ alebo *primitívna n-tá odmocnina* jednotky. Ak ε je primitívna n-tá odmocnina z jednotky, tak $K_n = \{1, \varepsilon, \ldots, \varepsilon^{n-1}\}$ (pozri napr. kapitolu 5 v [2]). Pretože pre každé $k \in \{0, \ldots, n-1\}$ je

$$\varepsilon_k = \left(\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}\right) = \left(\cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}\right)^k = \varepsilon_1^k,$$

tak ε_1 je jedným z generátorov grupy K_n, teda je primitívnym koreňom rovnice $x^n - 1$.

1.2 VETA. *Nech c je koreň binomickej rovnice $x^n - a = 0$ a nech ε je primitívna n-tá odmocnina jednotky. Potom $\{c, c\varepsilon, \ldots, c\varepsilon^{n-1}\}$ je množina všetkých koreňov rovnice $x^n - a = 0$.*

DÔKAZ. Pretože c je koreňom rovnice $x^n - a = 0$ a ε koreňom rovnice $x^n - 1 = 0$, tak pre každé $k \in \{0, \ldots, n-1\}$ je

$$(c \cdot \varepsilon^k)^n = c^n \cdot (\varepsilon_k)^n = c^n \cdot (\varepsilon^n)^k = c^n \cdot 1 = c^n = a$$

čo znamená, že aj $c\varepsilon^k$ je koreňom rovnice $x^n - a = 0$.

Pretože ε je primitívny koreň tak čísla $1 = \varepsilon^0, \varepsilon^1, \ldots, \varepsilon^{n-1}$ sú navzájom rôzne a teda aj (pretože $c \neq 0$) čísla $c, c\varepsilon, \ldots, c\varepsilon^{n-1}$ sú navzájom rôzne.

1.3 PRÍKLAD. Nájdeme kanonický rozklad polynómu $f(x) = x^6 + 1$ nad poľom reálnych čísel. Pre každé $x \in R$ je $x^6 + 1 > 0$, t.j. $f(x)$ nemá reálne korene. Pretože je to polynóm z reálnymi koeficientami, musí mať tri dvojice imaginárnych komplexne združených koreňov. Riešením binomickej rovnice $x^6 + 1 = 0$ ich všetky nájdeme. Číslo $-1 = \cos\pi + i\sin\pi$. Potom

$$\begin{aligned}
c_0 &= \cos\frac{\pi}{6} + i\sin\frac{\pi}{6} = \frac{\sqrt{3}}{2} + i\frac{1}{2},\\
c_1 &= \cos\frac{\pi+2\pi}{6} + i\sin\frac{\pi+2\pi}{6} = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = i,\\
c_2 &= \cos\frac{\pi+4\pi}{6} + i\sin\frac{\pi+4\pi}{6} = \cos\frac{5\pi}{6} + i\sin\frac{5\pi}{6} = -\frac{\sqrt{3}}{2} + i\frac{1}{2},\\
c_3 &= \cos\frac{\pi+6\pi}{6} + i\sin\frac{\pi+6\pi}{6} = \cos\frac{7\pi}{6} + i\sin\frac{7\pi}{6} = -\frac{\sqrt{3}}{2} - i\frac{1}{2},\\
c_4 &= \cos\frac{\pi+8\pi}{6} + i\sin\frac{\pi+8\pi}{6} = \cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2} = -i,\\
c_5 &= \cos\frac{\pi+10\pi}{6} + i\sin\frac{\pi+10\pi}{6} = \cos\frac{11\pi}{6} + i\sin\frac{11\pi}{6} = \frac{\sqrt{3}}{2} - i\frac{1}{2}.
\end{aligned}$$

Pre korene $c_0, c_1, c_2, c_3, c_4, c_5$ platí $c_0 = \overline{c_5}$, $c_1 = \overline{c_4}$, $c_2 = \overline{c_3}$. Ak teraz vypočítame súčiny koreňových činiteľov, v ktorých sa nachádzajú komplexne združené korene, dostávame ireducibilné (nad poľom R) kvadratické polynómy

$$\begin{aligned}
(x - c_0)(x - c_5) &= x^2 - \sqrt{3}x + 1,\\
(x - c_1)(x - c_4) &= x^2 + 1,\\
(x - c_2)(x - c_3) &= x^2 + \sqrt{3}x + 1.
\end{aligned}$$

Kanonický rozklad polynómu $f(x) = x^6 + 1$ nad poľom R teda je

$$x^6 + 1 = (x^2 - \sqrt{3}x + 1)(x^2 + 1)(x^2 + \sqrt{3}x + 1).$$

Cvičenia

1. Nájdite všetky riešenia binomických rovníc:
   a) $x^5 - 1 = 0$,

b) $x^9 - 343 = 0$,
c) $x^8 + 625 = 0$,
d) $x^3 + 1 - i = 0$.

2. Nájdite rozklad polynómu $f(x)$ na súčin ireducibilných polynómov nad poľom R, ak
a) $f(x) = x^6 - 1$,
b) $f(x) = x^8 - 1$,
c) $f(x) = x^4 + 2$.

2 Rovnice druhého a tretieho stupňa

Rovnica

$$ax^2 + bx + c = 0, \tag{1}$$

kde $a, b, c \in C$, $a \neq 0$, sa nazýva *kvadratická rovnica*. V prípade, že jej koeficienty sú reálne čísla, poznáme postup hľadania koreňov už zo strednej školy. Ukážeme, že analogickým postupom môžeme nájsť riešenia kvadratickej rovnice aj v prípade, že jej koeficienty sú komplexné čísla. Pre vyjadrenie koreňov v takomto prípade je potrebné poznať druhú komplexnú odmocninu komplexného čísla. S postupom hľadania druhej odmocniny komplexného čísla sme sa už čiastočne oboznámili (pozri napr. v [3] príklad 5 na strane 8). Tento postup teraz zovšeobecníme.

2.1 Lema. *Ku každému komplexnému číslu $a+bi$ existuje jeho druhá komplexná odmocnina*

$$x = \pm\left(\sqrt{\frac{1}{2}\left(\sqrt{a^2+b^2}+a\right)} + i\delta\sqrt{\frac{1}{2}\left(\sqrt{a^2+b^2}+a\right)}\right), \tag{2}$$

kde $\delta = 1$ pre $b > 0$ a $\delta = -1$ pre $b < 0$.

Dôkaz. Ak x je druhá komplexná odmocnina čísla $a+bi$, tak $x^2 = a+bi$. Číslo x je komplexné, preto $x = u + vi$, teda $(u+vi)^2 = a+bi$. Po úprave máme

$$u^2 - v^2 + 2uvi = a + bi,$$

z čoho dostávame sústavu dvoch rovníc o dvoch (reálnych) neznámych

$$\begin{aligned} u^2 - v^2 &= a, \\ 2uv &= b. \end{aligned}$$

Umocnením obidvoch rovníc na druhú a ich sčítaním dostávame

$$(u^2 + v^2)^2 = a^2 + b^2.$$

z čoho (pretože $a^2 + b^2 \geq 0$)

$$u^2 + v^2 = \sqrt{a^2 + b^2}.$$

Z rovníc $u^2 - v^2 = a$, $u^2 + v^2 = \sqrt{a^2+b^2}$ vyplýva

$$u = \pm\sqrt{\frac{1}{2}\left(\sqrt{a^2+b^2}+a\right)}, \qquad v = \pm\sqrt{\frac{1}{2}\left(\sqrt{a^2+b^2}-a\right)}.$$

Z rovnice $2uv = b$ vyplýva, že $b > 0$ práve vtedy, keď obidve čísla u, v sú buď kladné alebo záporné a $b < 0$ práve vtedy, keď jedno z nich je kladné a druhé záporné. Z toho už dostávame (2).

Priamym výpočtom sa môžeme presvedčiť, že komplexné čísla dané vzťahmi (2) sú druhou komplexnou odmocninou z čísla $a + bi$, t.j., že $x^2 = a + bi$.

Teraz nájdeme riešenie rovnice (1). Táto rovnica je ekvivalentná s rovnicou

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

S využitím „dopĺňania na štvorec“ a ďalšími úpravami polynómu $x^2 + \frac{b}{a}x + \frac{c}{a}$ postupne dostávame

$$\begin{aligned} x^2 + \frac{b}{a}x + \frac{c}{a} &= x^2 + \frac{b}{a}x + \frac{b^2}{4a^2} + \frac{c}{a} - \frac{b^2}{4a^2} = \\ &= \left(x + \frac{b}{2a}\right)^2 - \frac{b^2 - 4ac}{4a^2} = \left(x + \frac{b}{2a}\right)^2 - \left(\frac{\sqrt{b^2 - 4ac}}{2a}\right)^2 = \\ &= \left(x + \frac{b - \sqrt{b^2 - 4ac}}{2a}\right) \cdot \left(x + \frac{b + \sqrt{b^2 - 4ac}}{2a}\right), \end{aligned}$$

čo je vlastne rozklad na koreňové činitele, kde $\sqrt{b^2 - 4ac}$ je jedna konkrétne zvolená druhá komplexná odmocnina čísla $b^2 - 4ac$. Z uvedeného vyplýva nasledovné tvrdenie.

2.2 Veta. *Korene kvadratickej rovnice (1) sú komplexné čísla*

$$x_1 = \frac{-b + \sqrt{b^2 - 4ac}}{2a}, \qquad x_2 = \frac{-b - \sqrt{b^2 - 4ac}}{2a},$$

kde symbol $\sqrt{b^2 - 4ac}$ označuje jednu zvolenú druhú komplexnú odmocninu čísla $b^2 - 4ac$.

2.3 Príklad. Nájdeme riešenie rovnice $x^2 - (5 + 4i)x + 6 + 8i = 0$. V tomto prípade je $a = 1$, $b = -(5 + 4i)$, $c = 6 + 8i$. Potom

$$\sqrt{b^2 - 4ac} = \sqrt{-15 + 8i} = \pm(1 + 4i).$$

Zvolíme $\sqrt{-15 + 8i} = 1 + 4i$ a dostávame

$$x_1 = 3 + 4i, \qquad x_2 = 2.$$

Ďalej sa budeme venovať riešeniu rovnice tretieho stupňa (kubickej rovnici). Rovnica

$$ax^3 + bx^2 + cx + d = 0, \quad a \neq 0,\ a, b, c, d \in C$$

sa nazýva *kubickou rovnicou*. Každú takúto rovnicu je možné ekvivalentnou úpravou upraviť na normovaný tvar, t.j. na rovnicu tvaru

$$x^3 + a_2x^2 + a_1x + a_0 = 0. \tag{3}$$

Ak použijeme substitúciu $x = y - \frac{a_2}{3}$, tak dostaneme kubickú rovnicu

$$y^3 + py + q = 0, \tag{4}$$

kde $p = a_1 - \frac{a_2}{3}$, $q = \frac{4a_2^3}{27} - \frac{a_1 a_2}{3} + a_0$, ktorá sa nazýva *redukovanou* kubickou rovnicou (koeficient pri y^2 je 0). Zavedieme ďalšiu substitúciu $y = u + v$. Potom

$$(u+v)^3 + p(u+v) + q = 0$$

a po úprave

$$u^3 + v^3 + (3uv + p)(u+v) + q = 0.$$

Ak u, v zvolíme tak, aby $3uv + p = 0$, t.j. $uv = -\frac{p}{3}$, tak

$$u^3 + v^3 = -q \qquad \text{a} \qquad u^3 v^3 = -\frac{p^3}{27}.$$

V takomto prípade môžeme u^3, v^3 považovať (pozri (4) na str. 28) za korene kvadratickej rovnice

$$z^2 + qz - \frac{p^3}{27} = 0,$$

ktorú voláme *kvadratickou rezolventou* kubickej rovnice. Jej korene sú

$$z_1 = u^3 = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = -\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3},$$
$$z_2 = v^3 = -\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3} = -\frac{q}{2} - \frac{1}{18}\sqrt{-3D_3},$$

kde $D_3 = -4p^3 - 27q^2$ je diskriminant redukovanej kubickej rovnice (4). Pre zápis čísla $y = u + v$ máme teda celkove deväť možností. Ak označíme

$$u_1 = \sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}}$$

jednu (z troch možných) tretiu komplexnú odmocninu čísla $-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}$, tak v_1 vypočítame (jednoznačne) zo vzťahu $uv = -\frac{p}{3}$ (t.j. $v_1 = -\frac{p}{3u_1}$) a označíme ho

$$v_1 = \sqrt[3]{-\frac{q}{2} - \frac{1}{18}\sqrt{-3D_3}}.$$

Keď sme jednu z tretích komplexných odmocnín čísla $\sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}}$ označili u_1, tak ďalšie jeho dve tretie komplexné odmocniny sú, podľa vety 1.2, $u_2 = \varepsilon u_1$, $u_3 = \varepsilon^2 u_1$, kde ε je primitívny koreň rovnice $x^3 = 1$, t.j. $\varepsilon = -\frac{1}{2} + \frac{1}{2}i\sqrt{3}$. K nim príslušné čísla v_2, v_3 určíme zo vzťahu $uv = -\frac{p}{3}$:

$$v_2 = -\frac{p}{3u_2} = -\frac{p}{3u_1\varepsilon} = \frac{v_1}{\varepsilon} = v_1\varepsilon^2,$$
$$v_3 = -\frac{p}{3u_3} = -\frac{p}{3u_1\varepsilon^2} = \frac{v_1}{\varepsilon^2} = v_1\varepsilon.$$

Pre y_1, y_2, y_3 tak máme

$$\begin{aligned} y_1 &= u_1 + v_1, \\ y_2 &= u_1\varepsilon + v_1\varepsilon^2, \\ y_3 &= u_1\varepsilon^2 + v_1\varepsilon \end{aligned} \tag{5}$$

z čoho už, vzhľadom na substitúciu $x = y - \frac{a_2}{3}$, môžeme korene x_1, x_2, x_3 rovnice (3) ľahko vypočítať. Skúškou sa môžeme presvedčiť, že čísla y_1, y_2, y_3 sú koreňmi rovnice (4), resp., že čísla x_1, x_2, x_3 sú koreňmi rovnice (3).

Získané výsledky sformulujeme (pre redukovanú kubickú rovnicu) v nasledovnej vete.

2.3 Veta. *Kubická rovnica $y^3 + py + q = 0$, $p, q \in C$ má riešenie*

$$\begin{aligned} y_1 &= \sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}} + \sqrt[3]{-\frac{q}{2} - \frac{1}{18}\sqrt{-3D_3}}, \\ y_2 &= \varepsilon\sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}} + \varepsilon^2\sqrt[3]{-\frac{q}{2} - \frac{1}{18}\sqrt{-3D_3}}, \\ y_3 &= \varepsilon^2\sqrt[3]{-\frac{q}{2} + \frac{1}{18}\sqrt{-3D_3}} + \varepsilon\sqrt[3]{-\frac{q}{2} - \frac{1}{18}\sqrt{-3D_3}}, \end{aligned}$$

kde $D_3 = -4p^3 - 27q^2$ je diskriminant tejto rovnice a ε je primitívna tretia odmocnina jednej.

Riešiť kubickú rovnicu s využutím Cardanových vzorcov nie je prakticky veľmi výhodné.

2.4 Príklad. Ľahko sa presvedčíme, že korene kubickej rovnice $x^3-3x^2+x+5 = 0$ sú čísla -1, $2+i$, $2-i$. Substitúciou $x = y+1$ ju upravíme na redukovanú kubickú rovnicu $y^3-2y+4 = 0$. Jej korene sú čísla -2, $1+i$, $1-i$ (presvedčte sa). S využitím Cardanových vzorcov dostávame

$$\begin{aligned} y_1 &= \sqrt[3]{-2 + \frac{10}{9}\sqrt{3}} + \sqrt[3]{-2 - \frac{10}{9}\sqrt{3}}, \\ y_2 &= \varepsilon\sqrt[3]{-2 + \frac{10}{9}\sqrt{3}} + \varepsilon^2\sqrt[3]{-2 - \frac{10}{9}\sqrt{3}}, \\ y_3 &= \varepsilon^2\sqrt[3]{-2 + \frac{10}{9}\sqrt{3}} + \varepsilon\sqrt[3]{-2 - \frac{10}{9}\sqrt{3}}. \end{aligned}$$

Pretože y_1 je reálne číslo, tak $y_1 = 2$, čo však z daného vyjadrenia nie je bezprostredne vidieť (urobte približný výpočet koreňov y_1, y_2, y_3).

Ešte komplikovanejšia je situácia, keď kubická rovnica má všetky korene reálne, t.j. keď $D_3 > 0$. V tomto prípade sú reálne korene vyjadrené v komplexnom tvare (lebo $\sqrt{-3D_3}$ je imaginárne číslo). Uvedený postup nemá teda pre praktické výpočty veľký význam. jeho význam je však najmä teoretický a historický lebo hľadanie riešenia kubickej rovnice prispelo k vytvoreniu teórie komplexných čísel.

Poznámka. Podobným spôsobom sa dajú algebraicky riešiť aj všetky (algebraické) rovnice štvrtého stupňa. Nórsky matematik Abel a francúzsky matematik Galois dokázali, že všeobecne nemožno riešiť rovnice vyššieho ako štvrtého stupňa.

Cvičenia

1. Riešte rovnice:
   a) $x^2 - (2+i)x + 7i - 1 = 0$,
   b) $(2+i)x^2 - (5-i)x + 2 - 2i = 0$,
   c) $x^2 - (6-4i)x + 5 - 12i = 0$.
2. Polynóm $x^4 - 3x^2 + 4$ rozložte
   a) na koreňové činitele,
   b) na súčin ireducibilných polynómov s reálnymi koeficientami.
3. Nájdite rozklad polynómu $x^4 + 6x^3 + 9x^2 + 100$ na ireducibilné polynómy v $R[x]$.
4. Nájdite všetky (komplexné) korene polynómu $x^4 + 2x^2 - 24x + 72$.
5. Pomocou Cardanových vzorcov riešte rovnice:
   a) $x^3 - 9x^2 + 36x - 28 = 0$,
   b) $x^4 - 15x + 22 = 0$,
   c) $x^3 + x + 10$.

3 Reciproké rovnice

Niektoré rovnice je možné riešiť tak, že pomocou vhodnej substitúcie znížime jej stupeň. Jednoduchým príkladom sú tzv. bikvadratické rovnice, t.j. rovnice tvaru

$$x^4 + px^2 + q = 0, \quad p, q \in C,$$

ktoré riešime pomocou substitúcie $y = x^2$. Vo všeobecnosti, z rovnice

$$a_{kn}x^{kn} + a_{k(n-1)}x^{k(n-1)} + \cdots + a_k x^k + a_0 = 0 \tag{1}$$

dostávame pomocou substitúcie $y = x^k$ rovnicu

$$a_{kn}y^n + a_{k(n-1)}y^{n-1} + \cdots + a_k y + a_0 = 0. \tag{2}$$

Je možné ukázať, že každé riešenie α rovnice (1) je riešením niektorej rovnice $x^k - \beta = 0$, kde β je vhodné riešenie rovnice (2).

3.1 Príklad. Nájdeme všetky (v C) riešenia rovnice $x^6 - 5x^3 - 14 = 0$. Ak použijeme substitúciu $y = x^3$, tak dostávame rovnicu $y^2 - 5y - 14 = 0$. Korene tejto rovnice sú $y_1 = 7$, $y_2 = -2$. Riešením binomických rovníc

$$x^3 = 7 \qquad \text{a} \qquad x^3 = -2$$

dostaneme všetkých šesť koreňov pôvodnej rovnice:

$$x_1 = \sqrt[3]{7}, \qquad x_2 = \sqrt[3]{7}\left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right), \qquad x_3 = \sqrt[3]{7}\left(-\frac{1}{2} - \frac{i\sqrt{3}}{2}\right),$$

$$x_4 = -\sqrt[3]{2}, \qquad x_5 = -\sqrt[3]{2}\left(-\frac{1}{2} + \frac{i\sqrt{3}}{2}\right), \qquad x_6 = -\sqrt[3]{2}\left(-\frac{1}{2} - \frac{i\sqrt{3}}{2}\right).$$

Urobte všetky potrebné výpočty podrobne.

Zníženie stupňa rovnice pomocou vhodnej substitúcie využívame aj pri riešení tzv. reciprokých rovníc.

Polynóm

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0,\ n \geq 1,$$

sa nazýva *kladne reciprokým polynómom*, keď

$$a_i = a_{n-i}, \quad \text{pre každé} \quad i \in \{0, 1, \ldots, n\}.$$

Ak $f(x)$ je kladne reciproký polynóm, tak rovnicu $f(x) = 0$ nazývame *kladne reciprokou rovnicou.*

3.2 Veta. *Polynóm* $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ *je kladne reciprokým polynómom práve vtedy, keď pre každé* $x \neq 0$ *je*

$$f(x) = x^n f\left(\frac{1}{x}\right). \tag{3}$$

Dôkaz. Ak $f(x)$ je kladne reciproký polynóm, tak ho môžeme zapísať v tvare

$$f(x) = a_o x^n + a_1 x^{n-1} + \cdots + a_1 x + a_0.$$

Z toho, po úprave, dostávame

$$f(x) = x^n \left(a_0 + a_1 \left(\frac{1}{x}\right) + \cdots + a_1 \left(\frac{1}{x}\right)^{n-1} + a_0 \left(\frac{1}{x}\right)^n \right),$$

t.j.

$$f(x) = x^n f\left(\frac{1}{x}\right).$$

Naopak, nech $f(x) = x^n f\left(\frac{1}{x}\right)$. Potom

$$a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0 = x^n \left(a_n \left(\frac{1}{x}\right)^n + a_{n-1} \left(\frac{1}{x}\right)^{n-1} + \cdots + a_0 \right).$$

Porovnaním ľavej a pravej strany dostávame, že pre každé $i \in \{0, 1, \ldots, n\}$ je $a_i = a_{n-i}$.

3.3 Dôsledok. *Ak kladne reciproká rovnice má koreň* α*, tak má aj koreň* $\frac{1}{\alpha}$.

Dôkaz. Pretože kladne reciproká rovnica má koeficient $a_n \neq 0$ a $a_n = a_0$, tak každý jej koreň je nenulový. Ak α je koreňom kladne reciprokej rovnice $f(x) = 0$, t.j. $f(\alpha) = 0$, tak z predchádzajúcej vety dostávame, že $\alpha^n f\left(\frac{1}{\alpha}\right) = 0$, teda aj $f\left(\frac{1}{\alpha}\right) = 0$ čo znamená, že aj $\frac{1}{\alpha}$ je koreň kladne reciprokej rovnice $f(x) = 0$.

3.4 Dôsledok. *Nech $f(x)$ je kladne reciproký polynóm nepárneho stupňa. Potom $f(x) = (x+1)g(x)$, pričom $g(x)$ je kladne reciproký polynóm párneho stupňa.*

Dôkaz. Dosadením čísla -1 do (3) dostávame $(-1)^n f(-1) = f(-1)$ a po úprave máme $f(-1) = 0$, teda -1 je koreň polynómu $f(x)$. Podľa Bezoutovej vety (veta 4.3) potom $f(x) = (x+1)g(x)$, pričom $g(x)$ je polynóm párneho stupňa. Z poslednej rovnosti (pre každé $x \neq 0$) máme $f\left(\frac{1}{x}\right) = \left(\frac{1}{x}+1\right) g\left(\frac{1}{x}\right)$. Ak z posledných dvoch rovností dosadíme $f(x)$ a $f\left(\frac{1}{x}\right)$ do (3), tak po úprave dostaneme (pre $x \neq -1$)

$$g(x) = x^{n-1} g\left(\frac{1}{x}\right).$$

Priamym dosadením sa môžeme presvedčiť, že uvedený vzťah platí aj pre $x = -1$. Z vety 3.2 potom vyplýva, že $g(x)$ je kladne reciproký polynóm (párneho stupňa $n-1$).

Polynóm

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0,\ n \geq 1,$$

sa nazýva *záporne reciprokým polynómom*, keď

$$a_i = -a_{n-i}, \quad \text{pre každé} \quad i \in \{0, 1, \ldots, n\}.$$

Ak $f(x)$ je záporne reciproký polynóm, tak rovnicu $f(x) = 0$ nazývame *záporne reciprokou rovnicou*. Analogickým spôsobom, ako vetu 3.2 a dôsledky 3.3, 3.4 je možné dokázať aj nasledujúce tri tvrdenia (podrobne si ich dôkazy zapíšte).

3.5 Veta. *Polynóm $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ je záporne reciprokým polynómom práve vtedy, keď pre každé $x \neq 0$ je*

$$f(x) = -x^n f\left(\frac{1}{x}\right).$$

3.6 Dôsledok. *Ak záporne reciproká rovnice má koreň α, tak má aj koreň $\frac{1}{\alpha}$.*

3.7 Dôsledok. *Nech $f(x)$ je záporne reciproký polynóm. Potom $f(x) = (x-1)g(x)$, pričom $g(x)$ je kladne reciproký polynóm.*

Z dôsledku 3.4 a dôsledku 3.7 vyplýva, že pri riešení reciprokých rovníc sa môžeme obmedziť na kladne reciproké rovnice párneho stupňa. Kladne reciprokú rovnicu párneho stupňa je možné vyjadriť v tvare

$$a_0 x^{2m} + a_1 x^{2m-1} + \cdots + a_1 x + a_0 = 0. \tag{4}$$

Ak túto rovnicu vynásobíme výrazom $\frac{1}{x^m}$, tak po úprave dostávame

$$a_0 \left(x^m + \frac{1}{x^m}\right) + a_1 \left(x^{m-1} + \frac{1}{x^{m-1}}\right) + \cdots + a_{m-1} \left(x + \frac{1}{x}\right) + a_m = 0. \tag{5}$$

Označme (zaveďme substitúciu)

$$x + \frac{1}{x} = y. \tag{6}$$

Postupným umocňovaním a úpravami máme

$$\begin{aligned} x^2 + \frac{1}{x^2} &= y^2 - 2, \\ x^3 + \frac{1}{x^3} &= y^3 - 3y, \\ x^4 + \frac{1}{x^4} &= y^4 - 4y^2 + 2, \\ &\vdots \end{aligned}$$

Po dosadení do (5) dostávame rovnicu m-tého stupňa

$$b_m y^m + \cdots + b_0 = 0. \tag{7}$$

Po jej vyriešení (ak ju vieme riešiť) a po postupnom dosadení jej m koreňov do (6) riešime ešte m kvadratických rovníc. Ich riešenia sú už riešením rovnice (4).

3.8 Príklad. Nájdeme všetky riešenia polynómu

$$f(x) = x^6 + 2x^5 - 2x^4 + 2x^2 - 2x - 1. \tag{8}$$

Riešenie. Polynóm $f(x)$ je záporne reciproký. Jeho koreňom je číslo 1 a preto

$$f(x) = (x-1)g(x),$$

kde

$$g(x) = x^5 + 3x^4 + x^3 + x^2 + 3x + 1$$

je kladne reciproký polynóm nepárneho stupňa, má teda koreň -1 a preto

$$g(x) = (x+1)h(x),$$

kde

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

je kladne reciproký polynóm párneho stupňa. Ostáva teda vyriešiť kladne reciprokú rovnicu

$$x^4 + 2x^3 - x^2 + 2x + 1 = 0. \tag{9}$$

Ak vynásobíme túto rovnicu výrazom $\frac{1}{x^2}$ a upravíme ju, tak dostávame

$$\left(x^2 + \frac{1}{x^2}\right) + 2\left(x + \frac{1}{x}\right) - 1 = 0.$$

Použitím substitúcie $y = x + \frac{1}{x}$ máme kvadratickú rovnicu

$$y^2 + 2y - 3 = 0, \tag{10}$$

ktorá má korene $y_1 = 1$, $y_2 = -3$. Pre x teda platí

$$x + \frac{1}{x} = 1, \qquad x + \frac{1}{x} = -3,$$

z čoho dostávame dve kvadratické rovnice

$$x^2 - x + 1 = 0, \qquad x^2 + 3x + 1 = 0.$$

Ich riešením dostávame všetky riešenia rovnice (9):

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

Reciproký polynóm (8) má teda tieto korene:

$$1, \quad -1, \quad , \frac{1 + i\sqrt{3}}{2}, \quad \frac{1 - i\sqrt{3}}{2}, \quad \frac{-3 + i\sqrt{5}}{2}, \quad \frac{-3 - i\sqrt{5}}{2}.$$

Substitúcia $y = x + \frac{1}{x}$ umožňuje znížiť stupeň kladne reciprokej rovnice párneho stupňa na polovicu a previesť riešenie reciprokej rovnice na riešenie inej algebraickej rovnice. Vo všeobecnosti je možné algebraicky riešiť nanajvýš kladne reciproké rovnice deviateho stupňa (lebo tie majú koreň -1) a záporne reciproké rovnice desiateho stupňa (tie majú korene 1 a -1).

Cvičenia

1. Rovnicu $x^4 + x^2 + 1 = 0$ riešte ako
   a) bikvadratickú,
   b) reciprokú.
2. rovnicu $x^5 - 1 = 0$ riešte ako
   a) binomickú,
   b) reciprokú.
3. Riešte rovnice
   a) $x^4 - 2x^3 - x^2 - 2x + 1 = 0$,
   b) $x^4 + 2x^3 + x^2 + 2x + 1 = 0$,
   c) $x^6 + x^4 + x^2 + 1 = 0$,
   d) $4x^6 + x^4 + x^3 + x^2 - 3x + 1 = 0$.

4 Približné riešenie rovníc

Algebraickými metódami vieme riešiť len niektoré typy algebraických rovníc, ako sú napr. rovnice 2., 3., 4. stupňa, binomické rovnice, reciproké rovnice. Existujú však tzv. numerické metódy riešenia rovníc, pomocou ktorých je možné vypočítať jej korene s ľubovoľnou, dopredu zadanou presnosťou. Niektoré z týchto metód je možné použiť nielen pre algebraické rovnice, ale aj pre rovnice tvaru $f(x) = g(x)$, kde $f(x)$, $g(x)$ sú ľubovoľné reálne funkcie premennej x. Takéto metódy využíva

napr. aj výpočtový systém *Mathematica* - A System for Doing Mathematics by Computer. V príručke [5] je v kapitole 5.2 uvedené:

> Ak rovnice obsahujú len lineárne funkcie alebo polynómy nižších stupňov, na ich numerické riešenie môžeme použiť funkciu `NSolve`, ktorá nepožaduje zadanie počiatočnej hodnoty a vypočíta všetky riešenia. Ak však rovnica obsahuje komplikovanejšie funkcie, potom jej riešenie musí systém *Mathematica* hľadať s použitím numerickej metódy na riešenie nelineárnych rovníc. Tu už musíme použiť funkciu `FindRoot`, v ktorej vždy zadávame počiatočnú hodnotu premennej. Aj keď má rovnica viac riešení, `FindRoot` vráti vždy len jedno riešenie, ktoré nájde ako prvé. Ak chceme nájsť ďalšie riešenie, musíme zmeniť počiatočnú hodnotu premennej. Funkcia `FindRoot` je schopná nájsť aj komplexný koreň, ak ako počiatočnú hodnotu zadáme komplexné číslo. Ak zadáme jednu počiatočnú hodnotu, `FindRoot` použije na hľadanie koreňa Newtonovu metódu. Ak zadáme prvé dve hodnoty aproximácie, používa sa metóda sečníc. Obidve metódy sú však veľmi citlivé na voľbu počiatočnej hodnoty (resp. hodnôt). Pri nevhodnej voľbe, vzdialenej od hodnoty koreňa, budú metódy divergovať.

Stručne naznačíme hlavné myšlienky spomenutých dvoch metód, Newtonovej metódy a metódy tetív (sečníc).

Množinu všetkých bodov, ktorých súradnice x, y spĺňajú rovnicu $y = f(x)$, nazývame *grafom funkcie* $f(x)$.

Predpokladajme, že v intervale $\langle a, b\rangle$ leží práve jeden koreň c funkcie $f(x)$ a že v tomto intervale je daná funkcia rastúca alebo klesajúca a konkávna alebo konvexná. Nech napr. funkcia $f(x)$ je na intervale $\langle a, b\rangle$ rastúca (t.j. pre každé $x \in \langle a, b\rangle$ je $f'(x) > 0$) a konvexná (t.j. pre každé $x \in \langle a, b\rangle$ je $f^{(2)}(x) > 0$).

V bode $B = [b, f(b)]$ zostrojíme dotyčnicu (pozri obr. 1). Priesečník tejto dotyčnice s osou x je bod $[b_1, 0]$. Pre smernicu dotyčnice platí

$$f'(b) = \frac{f(b)}{b - b_1},$$

z čoho po úprave máme

$$b_1 = b - \frac{f(b)}{f'(b)}.$$

Ak v bode $[b_1, f(b_1)]$ zostrojíme opäť dotyčnicu, tak analogicky pre súradnicu b_2 jej priesečníka $[b_2, 0]$ s osou x dostávame

$$b_2 = b_1 - \frac{f(b_1)}{f'(b_1)}.$$

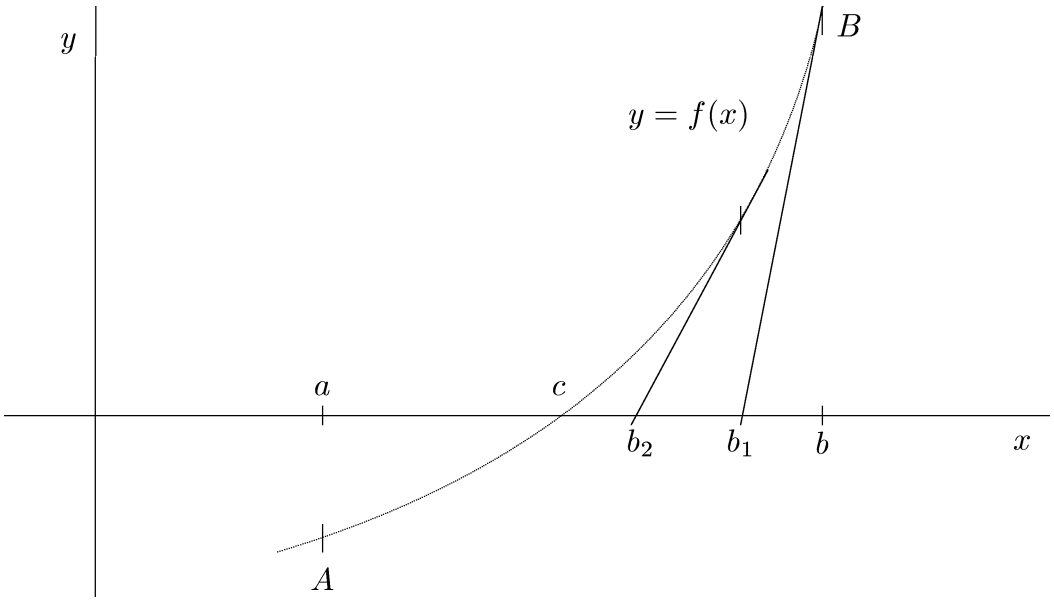
Tento postup opakujeme a dostaneme postupnosť (v tomto prípade klesajúcu)

$$b_0,\ b_1,\ b_2,\ \ldots \quad ,$$

kde

$$b_0 = b, \qquad b_{k+1} = b_k - \frac{f(b_k)}{f'(b_k)}, \quad k \in N, \tag{1}$$

o ktorej sa dá dokázať, že konverguje ku koreňu c funkcie $f(x)$.



Obr. 1

Táto metóda hľadania koreňa (presnejšie jeho približnej hodnoty) sa nazýva *Newtonova metóda* alebo *metóda totyčníc*. Všimnime si, že je nutné vhodne zvoliť krajný bod intervalu, v ktorom začneme zostrojovať dotyčnicu. Bude to ten krajný bod intervalu $\langle a, b\rangle$, v ktorom funkčné hodnoty danej funkcie a jej druhej derivácie majú rovnaké znamienko (v našom prípade to bol bod B).

Ďalšou metódou, ktorou môžeme vypočítať približnú hodnotu koreňa c je metóda tetív. Zostrojme tetivu určenú bodmi $A = [a, f(a)]$, $B = [b, f(b)]$, obr. 2. Táto tetiva pretína os x v bode $[a_1, 0]$. Smernica tejto tetivy je

$$k = \frac{f(b) - f(a)}{b - a}.$$

Ak túto smernicu vyjadríme pomocou bodov $[a, f(a)]$, $[a_1, 0]$, tak

$$k = \frac{0 - f(a)}{a_1 - a} = \frac{-f(a)}{a_1 - a},$$

teda

$$\frac{-f(a)}{a_1 - a} = \frac{f(b) - f(a)}{b - a},$$

z čoho po úprave dostávame

$$a_1 = a - \frac{b - a}{f(b) - f(a)} \cdot f(a).$$

Podobne tetiva určená bodmi $A_1 = [a_1, f(a_1)]$, B pretína os x v bode $[a_2, 0]$, kde

$$a_2 = a_1 - \frac{b - a}{f(b) - f(a_1)} \cdot f(a_1).$$

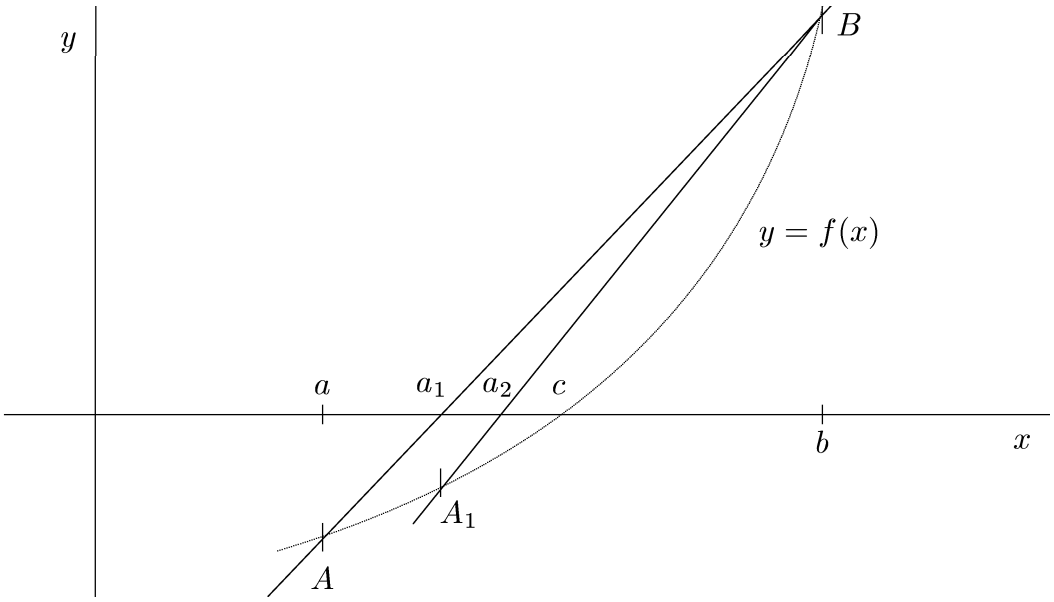
Ak tento postup opakujeme, dostaneme postupnosť (v tomto prípade rastúcu)

$$a_0,\ a_1,\ a_2,\ \ldots\quad ,$$

kde

$$a_0 = a, \qquad a_{k+1} = a_k - \frac{b - a_k}{f(b) - f(a_k)} \cdot f(a_k), \quad k \in N, \tag{2}$$

o ktorej sa dá dokázať, že konverguje ku koreňu c funkcie $f(x)$.



Obr. 2

Pri tomto postupe zostáva pevným bodom intervalu ten jeho krajný bod, v ktorom funkčné hodnoty danej funkcie a jej druhej derivácie majú rovnaké znamienko.

Analogicky postupujeme aj v ďalších prípadoch, t.j. keď daná funkcia je rastúca a konkávna alebo klesajúca a konvexná alebo klesajúca a konkávna (načrtnite si tieto jednotlivé tri prípady).

Poznámka. Tabuľky, grafy a niektoré zápisy (napr. riešení) patriace k nasledovným príkladom uvedieme v prílohe. Budú zapísané tak, ako ich znázorňuje *Mathematica* a nebudeme ich osobitne komentovať, pretože z kontextu bude ich význam zrejmý. Aj v zápisoch desatinných čísel budeme niekedy používať desatinnú bodku.

4.1 Príklad. Nájdeme približnú hodnotu kladného koreňa polynómu $f(x) = x^2 - 2$, (t.j. približnú hodnotu čísla $\sqrt{2}$)pomocou Newtonovej aj tetivovej metódy. Túto hodnotu vlastne dobre poznáme (jej približná hodnota na osem desatinných miest je 1.41421356) a budeme môcť teda porovnať, ako rýchlo sa k nej jednotlivými metódami priblížime. Pre výpočet použijeme tabuľkový editor EXCEL. Uvažujme napr interval $\langle 0.5, 2.5\rangle$, v ktorom je daná funkcia rastúca a konvexná a v ktorom leží jej kladný koreň (pozri obr. 3 v prílohe). V tabuľke (tab. 1 v prílohe) uvedieme hodnoty

$$b = b_0 = 2.5,\ b_1,\ b_2,\ \ldots,\ b_{16}$$

pre Newtonovu metódu a hodnoty

$$a = a_0 = 0.5,\ a_1,\ a_2, \ldots,\ a_{16}$$

pre metódu tetív (na osem desatinných miest). V našom prípade má (1) tvar

$$b_0 = b = 2.5, \qquad b_{k+1} = b_k - \frac{b_k^2 - 2}{2b_k}, \quad k \in N$$

a (2) má tvar

$$a_0 = a = 0.5, \qquad a_{k+1} = a_k - \frac{2.5 - a_k}{6.25 - a_k^2} \cdot (a_k^2 - 2), \quad k \in N$$

(podrobne sa presvedčte)

Dá sa ukázať (v tomto konkrétnom prípade to vidíme z tabuľky), že Newtonova metóda je rýchlejšia ako metóda tetív. Ak obidve metódy skombinujeme, tak sa ku koreňu blížime z obidvoch strán a v každom kroku je možné určiť presnosť, s akou sme sa ku hľadanému koreňu priblížili. Pre každé $i \in \{1, 2, \ldots, 16\}$ máme určený interval $\langle a_i, b_i \rangle$ v ktorom leží hľadaný koreň (t.j. poznáme ho s presnosťou do $b_i - a_i$.

Ak pre hľadanie koreňov použijeme napr výpočtový systém *Mathematica*, môžeme graf danej funkcie znázorniť a korene nájsť napr. pomocou už spomínaných príkazov `NSolve` alebo `FindRoot`. Pritom je užitočné poznať interval, v ktorom ležia všetky reálne korene danej funkcie. V prípade polynómu môžeme využiť napríklad nasledovné tvrdenie.

4.2 Lema. *nech $f(x)$ je polynóm s reálnymi koeficientami. Ak v Taylorovom rozvoji*

$$f(x) = b_n(x - c)^n + \cdots + b_1(x - c) + b_0$$

v bode $c > 0$ sú všetky jeho koeficienty kladné, tak každý reálny koreň polynómu $f(x)$ je menší ako c.

Dôkaz. Ak $x \geq c$, tak zrejme $f(x) > 0$, čo znamená, že neexistuje koreň väčší alebo rovný ako c.

4.3 Príklad. S využitím systému *Mathematica* zobrazíme graf polynómu

$$f(x) = 11x^6 - 7x^5 - 10x^4 + 29x^3 - 26x^2 + 9x - 1 \tag{3}$$

a nájdeme jeho reálne korene. Najprv nájdeme interval, v ktorom ležia všetky reálne korene. S použitím Hornerovej schémy nájdeme Taylorov rozvoj polynómu $f(x)$ podľa mocnín $x - 1$. Dostávame

$$f(x) = 11(x-1)^6 + 59(x-1)^5 + 120(x-1)^4 + 139(x-1)^3 + 96(x-1)^2 + 35(x-1) + 5.$$

Podľa lemy 4.2 sú teda všetky korene polynómu (3) menšie ako 1. Dolnú hranicu polynómu $f(x)$ nájdeme tak, že do (3) dosadíme $x = -y$. Dostávame polynóm

$$g(y) = f(-y) = 11y^6 + 7y^5 - 10y^4 - 29y^3 - 26y^2 - 9y - 1. \tag{4}$$

Nájdeme hornú hranicu c pre reálne korene polynómu (4). Číslo $-c$ je potom zrejme dolnou hranicou polynómu (3). Priamym dosadením zistíme, že $g(1) = -57$. Pomocou Hornerovej schémy zistíme, že $g(2) = 413$ (tabuľka 2 v prílohe). Pretože všetky čísla v poslednom riadku sú kladné, tak aj všetky koeficienty

$$b_0 = g(2),\ b_1,\ b_2,\ b_3,\ b_4,\ b_5,\ b_6$$

Taylorovho rozvoja polynómu $g(y)$ podľa mocnín $y - 2$ budú kladné, čo znamená (lema 4.2), že číslo 2 je hornou hranicou koreňov polynómu (4) a číslo -2 je dolnou hranicou koreňov polynómu (3). Všetky reálne korene polynómu (3) ležia teda v intervale $\langle -2, 1\rangle$. Ak zobrazíme graf tohto polynómu pomocou systému *Mathematica*, napr. v intervale $\langle -2, 2\rangle$ (obr. 4 v prílohe) vidíme, že jeden z koreňov leží v intervale $\langle -2, -1.5\rangle$. Separovať ďalšie korene, t.j. určiť intervaly, v ktorých leží práve jeden koreň, z daného obrázku zatiaľ nevieme. Ak zobrazíme graf tejto funkcie napr. v intervale $\langle -0.1, 0.8\rangle$ (obr. 5 v prílohe) vidíme, že ďalší z koreňov leží v intervale $\langle 0.2, 0.3\rangle$, ďalší v intervale $\langle 0.4, 0.5\rangle$ a posledný v intervale $\langle 0.6, 0.7\rangle$. Posledné dva korene sú zrejme imaginárne.

a) Ak zadáme (v systéme *Mathematica*) pre polynóm (3) príkaz

$$\texttt{FindRoot}[f[x] == 0, \{x, b_0\}],$$

tak *Mathematica* nájde príslušný koreň pomocou Newtonovej metódy, pričom ako počiatočnú hodnotu použije číslo b_0. Pre $b_0 = 0.7$ dostaneme koreň $x = 0.618034$ (pozri A. v prílohe).

b) Ak zadáme príkaz

$$\texttt{FindRoot}[f[x] == 0, \{x, \{a_0, b_0\}\}],$$

tak *Mathematica* nájde príslušný koreň pomocou tetivovej metódy, pričom ako prvé dve hodnoty sa použijú a_0 a b_0. Pre $a_0 = 0.6$, $b_0 = 0.7$ dostaneme $x = 0.618033$ (pozri B. v prílohe).

c) V takom jednoduchom prípade (pre systém *Mathematica*) ako je náš polynóm (3), zvládne *Mathematica* hľadanie koreňov pomocou príkazu `NSolve` bez toho, aby sme zadávali nejaké počiatočné hodnoty a vypíše aj imaginárne korene. V tomto prípade tak dostávame (pozri C. v prílohe)

$$x_1 = -1.61803, \quad x_2 = 0.216542, \quad x_3 = 0.419821, \quad x_4 = 0.618034,$$
$$x_5 = 0,5 - 0.866025\,i, \quad x_6 = 0,5 + 0.866025\,i.$$