
TEORIE ČÍSEL MNOHOČLENŮ A MNOHOČLENY V TEORII ČÍSEL

Jakub Opršal

Kurz vznikl v rámci projektu "Rozvoj systému vzdělávacích příležitostí pro nadané žáky a studenty v přírodních vědách a matematice s využitím online prostředí", Operační program Praha – Adaptabilita, registrační číslo CZ.2.17/3.1.00/31165.



Projekt A-NET je financován Evropským sociálním fondem, rozpočtem ČR a MHMP.

"Praha & EU: Investujeme do vaší budoucnosti."

TEORIE ČÍSEL MNOHOČLENŮ A MNOHOČLENY V TEORII ČÍSEL

JAKUB OPRŠAL

16. března 2011

ABSTRAKT. Polynomy (které se česky nazývají mnohočleny) mají velmi podobné vlastnosti jako celá čísla. Dá se tu uvažovat dělitelnost, mnohočlen $f(x)$ dělí $g(x)$, když existuje mnohočlen $h(x)$, že $f(x)h(x) = g(x)$. Roli prvočísel nám pak převzmou nerozložitelné polynomy. Ukážeme si, že i v mnohočlenech lze dělit se zbytkem, funguje jednoznačný rozklad na nerozložitelné polynomy a můžeme použít Euklidův algoritmus k dokázání Bézoutovy věty.

Dále se na přednášce budeme zabývat symetrickými polynomy a ukážeme si, jak se dají elegantně použít při řešení některých polynomiálních rovnic. Zajímavá je také souvislost diskriminantů se symetrickými polynomy. Diskriminant mnohočleny můžeme definovat i pro polynomy vyšších stupňů než 2. Ukážeme si, že to není jen náhodné číslo, které se zrovna vyskytuje ve vzorci pro řešení kvadratických rovnic, ale že má i mnohé další zajímavé vlastnosti.

Nakonec se budeme zabývat využitím polynomů v teorii čísel, budeme zkoumat nerozložitelnost mnohočlenů nad celými a racionálními čísly, počítat s mnohočleny modulo prvočíslo p a odvodíme si některé pěkné výsledky v klasické teorii čísel, jako například Wilsonovu větu.

MNOHOČLENY A DĚLITELNOST MNOHOČLENŮ

Mnohočlenem (nebo také *polynomem*) nad $\mathbb{R}$ (resp. $\mathbb{Q}$ nebo $\mathbb{C}$) myslíme formální součet tvaru

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0,$$

kde n je přirozené číslo a $a_i \in \mathbb{R}$ (resp. $\mathbb{Q}$, $\mathbb{C}$) pro všechna $i = 0, 1, \dots, n$. Čísla a_i nazveme *koefficienty* polynomu a největší k takové, že $a_k \neq 0$, *stupněm* mnohočleny f , značíme $\deg f$. Navíc pokládáme $\deg 0 = \infty$.¹ Člen a_0 nazýváme *absolutním členem* mnohočleny f . Všimni si, že každé nenulové reálné (racionální, komplexní) číslo je vlastně polynomem stupně nula (0 je pak polynomem stupně ∞), takovým mnohočlenům říkáme *konstantní*. Množinu všech mnohočlenů nad $\mathbb{R}$ značíme $\mathbb{R}[x]$, množinu všech mnohočlenů nad $\mathbb{Q}$ značíme $\mathbb{Q}[x]$ a podobně i množinu mnohočlenů nad komplexními čísly značíme $\mathbb{C}[x]$.

V definici mnohočleny považujeme x za abstraktní symbol, který umíme sám se sebou násobit a sčítat. Například $x \cdot x = x^2$ nebo $x + x = 2x$. x je pro nás tedy *neznámá*, se kterou se snažíme počítat, ačkoliv o ní vůbec nic nevíme.

Druhý pohled na mnohočleny (který ale není definicí) je jako na funkce z reálných čísel do reálných čísel (resp. z $\mathbb{Q}$ do $\mathbb{Q}$ nebo z $\mathbb{C}$ do $\mathbb{C}$), které hodnotě x přiřadí hodnotu součtu $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$. Tomuto budeme říkat dosazování hodnoty x do polynomu a výslednou hodnotu budeme značit $f(x)$, pro konkrétní číslo tedy třeba $f(2)$.

Je-li f polynom, pak reálné číslo a nazveme *kořenem* polynomu f , pokud platí $f(a) = 0$.

Polynomy mezi sebou umíme násobit a sčítat. Sčítání je velmi jednoduché, prostě sečteme příslušné koefficienty polynomu (u členů, které se v jednom z polynomů nevyskytují, považujeme jejich koefficienty za nulu), tj. je-li $n \geq m$, pak

$$\begin{aligned} (a_n x^n + a_{n-1} x^{n-1} + \dots + a_0) + (b_m x^m + b_{m-1} x^{m-1} + \dots + b_0) = \\ = a_n x^n + \dots + (a_m + b_m) x^m + (a_{m-1} + b_{m-1}) + \dots + (a_0 + b_0). \end{aligned}$$

¹Stupeň nulového polynomu se občas definuje i jako -1 . Různé definice reflektují různé vlastnosti tohoto polynomu. Většinou ale na konkrétní hodnotě tak nezáleží, důležité ale je, že $\deg 0 \neq 0$.

Násobení polynomů je trochu složitější. Důležité je vědět, jak se násobí x^n a x^m , totiž $x^n \cdot x^m = x^{m+n}$. Zbytek je jen roznásobení závorek. Tedy například

$$\begin{aligned}(x^2 + 2x + 2)(x^2 - 2x + 2) &= \\ &= x^2 \cdot x^2 + x^2 \cdot (-2x) + x^2 \cdot 2 + 2x \cdot x^2 + 2x \cdot (-2x) + 2x \cdot 2 + 2 \cdot x^2 + 2 \cdot (-2x) + 2 \cdot 2 = \\ &= x^4 - 2x^3 + 2x^2 + 2x^3 - 4x^2 + 4x + 2x^2 - 4x + 4 = x^4 + 4.\end{aligned}$$

Obecně násobíme-li polynomy $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ a $b_m x^m + b_{m-1} x^{m-1} + \dots + b_0$, tak dostaneme mnohočlen (který budeme psát od absolutního členu)

$$\begin{aligned}(a_n x^n + a_{n-1} x^{n-1} + \dots + a_0) \cdot (b_m x^m + b_{m-1} x^{m-1} + \dots + b_0) &= \\ &= a_0 b_0 + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + (a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0)x^3 + \dots\end{aligned}$$

Tedy koeficient u členu x_k v součinu je

$$a_0 b_k + a_1 b_{k-1} + a_2 b_{k-2} + \dots + a_k b_0.$$

Cvičení. Vynásobte polynomy $x^2 + x + 1$, $x^2 - x + 1$ a $x^2 - 1$.

Řešení. $x^6 - 1$.

Tvrzení. Jsou-li f a g polynomy, pak platí

$$\begin{aligned}\deg(f + g) &\leq \max(\deg f, \deg g), \\ \deg(f \cdot g) &= \deg f + \deg g.\end{aligned}$$

Klíčová pro nás bude definice *dělitelnosti mnohočlenů*. Dělitelnost se definuje podobně jako v celých číslech, tudíž jsou všechny vlastnosti dělitelnosti polynomů velmi podobné jako u celých čísel. Proto k nim budeme polynomy často přirovnávat. Říkáme, že polynom f *dělí* polynom g , pokud existuje polynom h tak, že $f(x) \cdot h(x) = g(x)$, tuto skutečnost zapisujeme $f \mid g$.

Tedy například platí $x + 1 \mid x^2 + 3x + 2$, neboť $x^2 + 3x + 2 = (x + 1)(x + 2)$. Konstantní polynom dělí každý jiný a nulový polynom je dělitelný každým polynomem, neboť vždy $f \cdot 0 = 0$. Všimněte si, že když polynom f dělí polynom g , tak $\deg f \leq \deg g$ a platí to dokonce i pro nulový polynom.

Cvičení. Ukažte, že polynom $x^2 + 1$ dělí polynom $x^6 + 1$.

Stejně jako celá čísla i polynomy můžeme dělit se zbytkem, o tom hovoří následující věta. Pro znění této věty definujme na chvíli stupeň nulového polynomu jako -1 .

Věta. (dělení se zbytkem) Pro každé dva polynomy f a g existují jednoznačné polynomy q a r takové, že $\deg r < \deg g$ a platí

$$f(x) = q(x)g(x) + r(x).$$

Tato věta má jeden zajímavý a užitečný důsledek. Pokud budeme dělit f mnohočlenem $x - a$, pak zbytek $r(x)$ bude stupně menšího než 1, tedy konstantní. Dostaneme tedy rovnost

$$f(x) = q(x)(x - a) + r,$$

kde r je konstanta. Navíc dosadíme-li do této rovnosti za x hodnotu a , dostaneme

$$f(a) = q(a)(a - a) + r = r.$$

Hledaný zbytek je právě hodnota polynomu f v bodě a . Shrňme toto pozorování v následujícím tvrzení.

Tvrzení. Je-li f libovolný polynom a a konstanta, pak existuje polynom q , že platí

$$f(x) = q(x)(x - a) + f(a).$$

Jinými slovy konstantní polynom $f(a)$ je zbytek polynomu f po dělení polynomem $x - a$.

Navíc platí, že a je kořen polynomu f právě tehdy, když $x - a \mid f$.

Důsledek. Každý mnohočlen f má nejvýše $\deg f$ kořenů.

Z druhé části tohoto tvrzení je vidět, že pokud polynom g dělí nějaký jiný, pak všechny kořeny polynomu g jsou i kořeny polynomu f . Protože pro každý takový kořen a platí $x - a \mid g \mid f$, tak i $x - a \mid f$.

Podobně jako v celých číslech i v polynomech definujeme *největšího společného dělitele* mnohočlenů f a g jako takový mnohočlen h , který je společným dělitelem f a g (tedy platí $h \mid f$ a $h \mid g$) a navíc každý jiný společný dělitel dělí h (čímž zaručíme, že h je „největší“ ze společných dělitelů). Největšího společného dělitele f a g značíme $\text{NSD}(f, g)$.

Největšího společného dělitele dvou polynomů můžeme počítat Euklidovým algoritmem.

Cvičení. Spočítejte největšího společného dělitele polynomů $x^4 + x^3 + 3x^2 + 2x + 2$ a $x^4 + x^2 - 2$.

Řešení. Použijeme Euklidův algoritmus, tedy budeme dělit se zbytkem

$$\begin{aligned}x^4 + x^3 + 3x^2 + 2x + 2 &= (x^4 + x^2 - 2) + (x^3 + 2x^2 + 2x + 4), \\x^4 + x^2 - 2 &= (x - 2)(x^3 + 2x^2 + 2x + 4) + (3x^2 + 6), \\x^3 + 2x^2 + 2x + 4 &= \left(\frac{1}{3}x + \frac{2}{3}\right)(3x^2 + 6) + 0.\end{aligned}$$

Největší společný dělitel je tedy $3x^2 + 6$, což ještě můžeme zjednodušit přenásobením $1/3$ na $x^2 + 2$.

Cvičení. Necht' m a n jsou přirozená čísla a d jejich největší společný dělitel. Spočítejte největšího společného dělitele polynomů $x^m - 1$ a $x^n - 1$.

Řešení. Kdyby $n = m = d$, pak zřejmě $\text{NSD}(x^m - 1, x^n - 1) = x^n - 1 = x^m - 1 = x^d - 1$. Bez újmy na obecnosti tedy předpokládejme, že $n > m$. Pak platí

$$x^n - 1 = x^{n-m}(x^m - 1) + (x^{n-m} - 1).$$

Tedy dostaneme, že $\text{NSD}(x^n - 1, x^m - 1) = \text{NSD}(x^m - 1, x^{n-m} - 1)$. Podívejme se, co se stalo s exponenty u vedoucích koeficientů. Z dvojice (n, m) jsme dostali dvojici $(m, n - m)$. Pokud stále $n - m > m$, můžeme tuto operaci zopakovat a dostaneme dvojici $(m, n - 2m)$, dále bychom dostali $(m, n - 3m)$ atd. Tedy podělíme-li číslo n číslem m se zbytkem, buď q podíl a r zbytek, dostaneme dvojici exponentů $(m, n - qm = r)$.

Dále budeme pracovat s polynomy $x^r - 1$ a $x^m - 1$ stejně, jako jsme pracovali s původními polynomy. Všimněte si, že v exponentech u vedoucích koeficientů vlastně opakujeme Euklidův algoritmus pro čísla m a n , dostaneme se tedy nakonec ke dvojici $(d, 0)$, neboli k polynomům $x^d - 1$ a $x^0 - 1 = 1 - 1 = 0$, jejichž největší společný dělitel je zřejmě $x^d - 1$. Dokázali jsme tedy, že platí

$$\text{NSD}(x^m - 1, x^n - 1) = x^{\text{NSD}(m, n)} - 1 = x^d - 1.$$

Cvičení. Jsou-li m, n přirozená čísla větší než 1, vyjádřete největšího společného dělitele $x^{2^n} + x^{2^{n-1}} + 1$ a $x^{2^m} + x^{2^{m-1}} + 1$.

Věta. (Bézoutova) Jsou-li f a g dva polynomy, pak existují polynomy k a l , že platí

$$f(x)k(x) + g(x)l(x) = \text{NSD}(f, g).$$

V celých číslech mají významné postavení prvočísla, a to díky tomu, že každé číslo lze jednoznačně zapsat jako součin prvočísel. V polynomech prvočíslem odpovídají tzv. nerozložitelné mnohočleny.

Mnohočlen f nazveme *nerozložitelným* (neboli *ireducibilním*), pokud nejde netriviálním způsobem zapsat jako součin dvou mnohočlenů, tedy neexistují mnohočleny g a h , oba stupně menšího než f , že $f(x) = g(x) \cdot h(x)$.

Tvrzení. Pro nerozložitelný mnohočlen f platí, že kdykoliv $f \mid gh$, pak $f \mid g$ nebo $f \mid h$.

Nad reálnými čísly jsou nerozložitelné mnohočleny všechny kvadratické trojčleny se záporným diskriminantem, všechny lineární mnohočleny a všechny konstantní mnohočleny. Kromě těchto tam nejsou žádné jiné, což je důsledek slavné základní věty algebry.

Věta. (Základní věta algebry) Každý polynom stupně alespoň 1 nad komplexními čísly má komplexní kořen.

Důsledek. Každý mnohočlen stupně n s komplexními koeficienty má v komplexních číslech právě n kořenů, počítáme-li je s násobností.

Věta. (o rozkladu na nerozložitelné mnohočleny) Je-li f nenulový mnohočlen, pak existuje (až na pořadí a přenásobení konstantami) jednoznačný rozklad f na součin nerozložitelných mnohočlenů.

FORMÁLNÍ DERIVACE POLYNOMŮ A NÁSOBNOST KOŘENŮ

V této kapitole nás bude zajímat násobnost kořenů. Nejlepší způsob, jak definovat násobnost kořene, je opřít se o tvrzení, které říká, že a je kořen $f(x)$ právě tehdy, když $x - a \mid f$. Tedy řekneme, že a je kořen f *násobnosti* právě n , pokud $(x - a)^n \mid f$ a $(x - a)^{n+1} \nmid f$.

Pro zjišťování násobných kořenů bude užitečné umět polynomy derivovat. My však nebudeme potřebovat derivaci, která udává směrnici tečny, místo toho si zavedeme vlastní, mnohem jednodušší, formální derivaci.

Formální derivací mnohočlenu $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ myslíme mnohočlen

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

Druhou derivací myslíme derivaci derivace, tj. $f'' = (f')'$, atd. n -tou derivací značíme $f^{(n)}$.

Lemma. Pro každé mnohočleny f a g platí

$$\begin{aligned}(f + g)' &= f' + g', \\ (fg)' &= f'g + fg'.\end{aligned}$$

Důkaz. Prvně dokážeme tvrzení o součtu. Mějme polynomy $f = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$ a $g = b_0 + b_1 x + b_2 x^2 + \dots + b_n x^n$ (n je větší ze stupňů polynomů f a g , k polynomu menšího stupně přidáme nulové koeficienty). Pokud je nejdříve sečteme a pak zderivujeme, dostaneme

$$\begin{aligned}f + g &= (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots + (a_n + b_n)x^n, \\ (f + g)' &= (a_1 + b_1) + 2(a_2 + b_2)x + \dots + n(a_n + b_n)x^{n-1}.\end{aligned}$$

Naopak spočteme-li si nejdříve derivace, máme $f' = a_1 + 2a_2 x + \dots + na_n x^{n-1}$ a podobně i $g' = b_1 + 2b_2 x + \dots + nb_n x^{n-1}$. Snadno se ověří, že součtem těchto dvou polynomů opravdu dostaneme $(f + g)'$.

Dokázat tvrzení o součinu derivací bude trochu obtížnější, začneme pro ukázkou se speciálními případy polynomu g . Pokud g je konstantní, tj. $g = c$ (pro nějaké reálné c), pak $g' = 0$ a chceme vlastně ukázat, že $(cf)' = cf'$. To ovšem není takový problém. Rozmyslete si, že nezáleží, jestli koeficienty vynásobíme před derivací, nebo až po.

Další speciální případ pro ukázkou je $g = x$. Tj. derivujeme polynom xf :

$$\begin{aligned}(xf)' &= (a_0 x + a_1 x^2 + \dots + a_n x^{n+1})' = a_0 + 2a_1 x + 3a_2 x^2 + \dots + (n+1)a_n x^n = \\ &= (a_0 + a_1 x + \dots + a_n x^n) + (a_1 x + 2a_2 x^2 + \dots + na_n x^n) = f + xf' = x'f + xf'.\end{aligned}$$

Zbytek důkazu už jen naznačíme, neděje se tu nic složitějšího jen je potřeba si vše důkladně rozepsat. Podobně jako u součinu xf můžeme postupovat při derivování $x^k f$, jen místo f vytkneme $kx^{k-1}f$ a zbyde nám jako druhý sčítanec $x^k f'$.

Nakonec už jen zbývá si uvědomit, že každý polynom g je jen součtem (konstantních) násobků polynomů $1, x, x^2$, atd. Tedy použijeme opakovaně pravidlo o derivaci součtu a dostaneme kýžené tvrzení. $\square$

Lemma. Je-li n přirozené, pak platí $((x - a)^n)' = n(x - a)^{n-1}$.

Důkaz. Toto tvrzení dokážeme matematickou indukcí podle n . Prvně je vidět, že $(x - a)' = 1$, což je tvrzení pro $n = 1$. Dále předpokládejme, že pro $n - 1$ tvrzení platí. Pak

$$((x - a)^n)' = ((x - a)(x - a)^{n-1})',$$

což podle vzorce pro derivaci součinu upravíme na

$$(x - a)'(x - a)^{n-1} + (x - a)((x - a)^{n-1})' = (x - a)^{n-1} + (x - a) \cdot (n - 1)(x - a)^{n-2} = n(x - a)^{n-1},$$

přičemž v předposlední rovnosti jsme použili indukční předpoklad. $\square$

Tvrzení. Je-li a kořen mnohočlenu f násobnosti n , pak a je kořen všech polynomů $f', f'', \dots, f^{(n-1)}$. Speciálně má-li f vícenásobný kořen, pak má společný kořen se svou derivací.

Důkaz. Budeme postupovat indukcí přes násobnost kořene a . Je-li a kořen násobnosti 1, nemáme co dokazovat. Nechť tedy tvrzení platí pro kořeny násobnosti nejvýše n . A buď a kořen f násobnosti $n+1$, ukážeme, že a je kořen násobnosti n polynomu f' , pak už bude vidět z indukčního předpokladu, že a je kořen $(f')' = f'', \dots, (f')^{(n-1)} = f^{(n)}$.

Víme, že a je kořen f násobnosti $n+1$, tedy f lze napsat ve tvaru $f = (x-a)^{n+1}g$, kde g je nějaký polynom. Zderivujeme tedy tento zápis f

$$f' = ((x-a)^{n+1}g)' = (n+1)(x-a)^n g + (x-a)^{n+1}g' = (x-a)^n((n+1)g + (x-a)g'),$$

tedy polynom $(x-a)^n$ dělí f' , což přesně znamená, že a je kořen f' násobnosti alespoň n . $\square$

Cvičení. Najděte všechny vícenásobné (alespoň dvojnásobné) kořeny polynomu $f(x) = x^3 - \sqrt{3}x^2 - 3x + 3\sqrt{3}$.

Řešení. Každý vícenásobný kořen je společný kořen polynom f a jeho derivace f' , spočtíme si tedy nejdříve derivaci

$$f'(x) = 3x^2 - 2\sqrt{3}x - 3.$$

Přitom pro každý společný kořen a polynomů f a f' musí platit $x-a \mid f$ i $x-a \mid f'$, tedy $x-a$ dělí i jejich největšího společného dělitele, který spočteme Euklidovým algoritmem:

$$\begin{aligned} f(x) &= \left(\frac{1}{3}x - \frac{1}{3\sqrt{3}}\right) f'(x) + \frac{-8}{3}(x - \sqrt{3}) \\ f'(x) &= (3x + \sqrt{3})(x - \sqrt{3}) + 0 \end{aligned}$$

Tedy největší společný dělitel f a f' je $x - \sqrt{3}$, jediný vícenásobný kořen tedy je $\sqrt{3}$. Navíc umíme určit i jeho násobnost, která je právě o jedna vyšší, než násobnost tohoto kořene polynomu $\text{NSD}(f, f')$, tedy v našem případě jde o dvojnásobný kořen polynomu f .

SYMETRICKÉ POLYNOMY

Monomem o n neznámých $x_1, x_2, \dots, x_n$ rozumíme člen tvaru

$$ax_1^{k_1}x_2^{k_2}\dots x_n^{k_n},$$

kde a je reálné (racionální, komplexní, ...) číslo a k_i jsou nezáporná celá čísla pro $i = 1, 2, \dots, n$. Číslo $k_1 + k_2 + \dots + k_n$ pak nazveme *stupněm* tohoto monomu. *Mnohočlenem o n neznámých* nazveme součet několika monomů o n neznámých $x_1, x_2, \dots, x_n$. Mnohočlen $f(x_1, x_2, \dots, x_n)$ nazveme *homogenní*, pokud mají všechny jeho monomy stejný stupeň, tento stupeň pak nazveme *stupněm homogeneity* f .

Takové mnohočleny mezi sebou můžeme násobit a sčítat. U násobení je opět nejdůležitější si uvědomit, jak se násobí monomy. Například pro dvě neznámé x a y definujeme součin monomů jako

$$ax^n y^m \cdot bx^k y^l = (ab)x^{n+k}y^{m+l}.$$

Zajímat nás budou symetrické mnohočleny. Mnohočlen f o neznámých $x_1, x_2, \dots, x_n$ nazveme *symetrický*, pokud pro libovolnou dvojici indexů i a $j = 1, 2, \dots, n$ se záměnou neznámých x_i a x_j polynom f nezmění. Speciálně polynom dvou neznámých je symetrický, pokud $f(x, y) = f(y, x)$.

Například polynom $x^2y + xy^2$ o dvou neznámých a polynomy $x_1x_2x_3$ a $x_1^2x_2 + x_2^2x_3 + x_3^2x_2 + x_1^2x_3 + x_2^2x_1 + x_3^2x_1$ o třech neznámých jsou symetrické, ale polynomy $x_1^2 + x_2^2$ a $x_1^2x_2 + x_2^2x_3 + x_3^2x_1$ o třech neznámých už symetrické nejsou.

Významné příklady symetrických polynomů jsou tzv. *elementární symetrické polynomy*. Jsou to mnohočleny

$$\begin{aligned} \sigma_1 &= x_1 + x_2 + \dots + x_n, \\ \sigma_2 &= x_1x_2 + \dots + x_1x_n + x_2x_3 + \dots + x_2x_n + \dots + x_{n-1}x_n, \\ \sigma_3 &= x_1x_2x_3 + x_1x_2x_4 + \dots + x_{n-2}x_{n-1}x_n, \\ &\vdots \\ \sigma_n &= x_1x_2x_3 \dots x_n. \end{aligned}$$

Tvrzení. (Viètovy vztahy) *Nechť $x_1, x_2, \dots, x_n$ jsou reálná čísla, pak mnohočlen $f(x)$ tvaru*

$$f(x) = x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \dots (-1)^n \sigma_n$$

má právě kořeny $x_1, x_2, \dots, x_n$ (počítáme-li je s násobností).

Úloha. Řešte soustavu rovnic

$$x^2 y + x y^2 = 6,$$

$$x + x y + y = 5.$$

Řešení. Nechť $\sigma_1 = x + y$ a $\sigma_2 = xy$, pak zadané rovnice upravíme do tvaru

$$\sigma_1 \sigma_2 = 6,$$

$$\sigma_1 + \sigma_2 = 5.$$

Tedy σ_1 a σ_2 jsou kořeny mnohočlenu $f(x) = x^2 - 5x + 6$. Tento mnohočlen má kořeny 2 a 3 (můžeme například použít vzorec pro kořeny kvadratických trojčlenů).

Mohou nastat dvě varianty. Prvně $\sigma_1 = 2$ a $\sigma_2 = 3$. Pak x a y jsou kořeny trojčlenu $g(x) = x^2 - 2x + 3$, ovšem diskriminant toho trojčlenu je $4 - 4 \cdot 3 = -8 < 0$, tedy tato rovnice nemá řešení.

Musí nastat druhá varianta $\sigma_1 = 3$ a $\sigma_2 = 2$. Tím dostaneme trojčlen $h(x) = x^2 - 3x + 2 = (x-1)(x-2)$, jehož kořeny jsou čísla x a y . Úloha má tedy dvě řešení: dvojice $x = 1, y = 2$ a $x = 2, y = 1$.

Tvrzení. *Je-li $f(x_1, x_2, \dots, x_n)$ symetrický mnohočlen, pak lze f vyjádřit jen pomocí elementárních symetrických mnohočlenů. Přesněji existuje mnohočlen $g(\sigma_1, \sigma_2, \dots, \sigma_n)$, že*

$$g(\sigma_1, \sigma_2, \dots, \sigma_n) = f(x_1, x_2, \dots, x_n).$$

Důkaz. Neuveden.

Díky tomuto tvrzení můžeme podobně jako předchozí úlohu řešit i mnohé další, jejichž zadání je zapsáno pouze pomocí symetrických polynomů. Užitečné k tomu bude znát několik vyjádření některých symetrických polynomů.

Označme $s_n = x_1^n + x_2^n + \dots + x_n^n$. Všechny tyto polynomy jsou symetrické a jdou tedy vyjádřit pomocí elementárních mnohočlenů. Platí $s_1 = \sigma_1$, vzorec pro s_2 se ještě odvodí snadno

$$s_2 = (x_1 + x_2 + \dots + x_n)^2 - 2x_1 x_2 - 2x_1 x_3 - \dots - 2x_{n-1} x_n = \sigma_1^2 - 2\sigma_2.$$

Pro ostatní se bude postupovat podobně, $s_n = \sigma_1^n + \star$, kde z přesného vyjádření $\star$ pomocí symetrických polynomů dostaneme vyjádření s_n . Platí například

$$s_3 = \sigma_1^3 - 3\sigma_1 \sigma_2 + 9\sigma_3.$$

Situace se nám velmi zjednoduší, pokud budeme pracovat jen se dvěma neznámými x_1 a x_2 , protože máme pouze dva elementární symetrické mnohočleny a také součet $(x_1 + x_2)^n$ se mnohem lépe umocňuje. Zkuste si odvodit vztahy

$$s_3 = \sigma_1^3 - 3\sigma_1 \sigma_2,$$

$$s_4 = \sigma_1^4 - 4\sigma_1^2 \sigma_2 + 2\sigma_2^2,$$

$$s_5 = \sigma_1^5 - 5\sigma_1^3 \sigma_2 + 5\sigma_1 \sigma_2^2.$$

Úloha. Řešte soustavu rovnic

$$x^5 + y^5 = 464,$$

$$x + y = 4.$$

Řešení. Označme si $\sigma_1 = x + y$ a $\sigma_2 = xy$, pro tyto symetrické mnohočleny platí stejné vzorce, co jsou uvedeny výše, speciálně $x^5 + y^5 = \sigma_1^5 - 5\sigma_1^3 \sigma_2 + 5\sigma_1 \sigma_2^2$. UVědomíme-li si, že druhá rovnice nám vlastně říká $\sigma_1 = 4$, zbyde nám jen dosadit do první, tj.

$$4^5 - 5 \cdot 4^3 \sigma_2 + 5 \cdot 4 \sigma_2^2 = 4^2 \cdot 29,$$

$$4 \cdot 35 - 5 \cdot 4^2 \sigma_2 + 5 \sigma_2^2 = 0,$$

$$\sigma_2^2 - 16\sigma_2 + 28 = 0,$$

$$(\sigma_2 - 14)(\sigma_2 - 2) = 0,$$

což je kvadratická rovnice s neznámou σ_2 , která má kořeny $\sigma_2 = 2$ a $\sigma_2 = 14$.

V prvním případě jsou tedy x a y kořeny kvadratické rovnice

$$\alpha^2 - 4\alpha + 2 = 0,$$

proto $x, y = (4 \pm \sqrt{16 - 8})/2 = 2 \pm \sqrt{2}$.

V druhém případě jsou x a y kořeny rovnice

$$\alpha^2 - 4\alpha + 14 = 0, (\alpha - 2)^2 + 10 = 0,$$

která nemá žádné řešení.

Výsledkem jsou pouze dvojice $2 + \sqrt{2}, 2 - \sqrt{2}$ a $2 - \sqrt{2}, 2 + \sqrt{2}$.

Úloha. Dokažte, že jsou-li a, b a c reálná čísla taková, že $a + b + c = 0$, pak

$$a^4 + b^4 + c^4 = 2(ab + bc + ac)^2.$$

Řešení. Mnohočlen $f(a, b, c) = a^4 + b^4 + c^4$ je symetrický v neznámých a, b a c stupně 4. Dá se tedy zapsat pomocí elementárních symetrických mnohočlenů, přičemž nám stačí uvažovat jen takové součiny symetrických mnohočlenů, které dohromady mají stupeň 4. Uvědomme si, že σ_1 má stupeň 1, σ_2 má stupeň 2 atd. Víme tedy, že existují reálná čísla α, β, γ a δ , že

$$f = \alpha\sigma_3\sigma_1 + \beta\sigma_2\sigma_1^2 + \gamma\sigma_2^2 + \delta\sigma_1^4.$$

Navíc pro zadaná čísla a, b a c platí $\sigma_1 = 0$, tedy nenulový je jen třetí člen a víme, že

$$a^4 + b^4 + c^4 = \gamma(ab + bc + ac)^2.$$

Zbývá už jen dopočítat koeficient γ , ale ten spočítáme z libovolného dosazení, které splňuje $\sigma_1 = 0$, tedy například $a = b = 1$ a $c = -2$. Platí tak

$$\begin{aligned} 1^4 + 1^4 + 2^4 &= \gamma(1 \cdot 1 + 1 \cdot (-2) + 1 \cdot (-2))^2, \\ 18 &= 9\gamma, \end{aligned}$$

odkud už je vidět, že $\gamma = 2$.

DISKRIMINANTY

Mnohočlen f nazveme *monickým*, pokud je jeho vedoucí koeficient 1, tj. f je tvaru

$$f = x^n + a_{n-1}x^{n-1} + \dots + a_0.$$

V této kapitole se budeme zabývat monickými mnohočleny, protože se pro ně vztahy pro diskriminant zjednoduší. Přitom každý polynom g je (reálným) násobkem jednoznačného monického polynomu f , budeme-li tedy definovat diskriminant g , definujeme ho jako $D(g) = D(f)$.

Diskriminant se asi poprvé objevil ve vzorci pro kořeny kvadratické rovnice. Je to kvantita přiřazená kvadratickému polynomu $f = x^2 + bx + c$, která reflektuje některé vlastnosti jeho kořenů. Jedna z takových vlastností je třeba násobnost. Všimněte si, že kvadratický polynom f má dvojnásobný kořen právě tehdy, když je diskriminant nulový. Vskutku, je-li totiž $D(f) = 0$, pak ze vzorců pro kořeny dostáváme

$$x_{1,2} = \frac{-b \pm \sqrt{D}}{2} = \frac{-b \pm \sqrt{0}}{2} = -\frac{b}{2},$$

a tedy $x_1 = x_2 = -b/2$.

Diskriminant lze ovšem přirozeně definovat i pro polynomy vyšších stupňů. Musíme ale začít s jinou definicí než $D(f) = b^2 - 4ac$. Nechť f je kvadratický monický mnohočlen s kořeny x_1 a x_2 , definujeme diskriminant f jako

$$D(f) = (x_1 - x_2)^2.$$

Všimněte si, že díky druhé mocnině v definici diskriminantu je diskriminant symetrický mnohočlen v neznámých x_1 a x_2 , tedy lze vyjádřit jen pomocí elementárních symetrických polynomů $\sigma_1 = x_1 + x_2$ a $\sigma_2 = x_1x_2$. Vskutku

$$D(f) = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = \sigma_1^2 - 4\sigma_2.$$

Když si nakonec uvědomíme, že σ_1 a σ_2 vlastně odpovídají koeficientům polynomu f (z Viètových vzorců), dostáváme, že pro kvadratický trojčlen $x^2 + bx + c$ platí

$$D(x^2 + bx + c) = (-b)^2 - 4c = b^2 - 4c.$$

Tímto vzorečkem pak můžeme diskriminant rozšířit na všechny monické kvadratické mnohočleny, přičemž jeho původní význam zůstává nezměněn.

Navíc je z definujícího vztahu vidět, že kdykoliv má f dva kořeny, je $D(f)$ nezáporný, neboť je druhou mocninou reálného čísla, a $D(f) = 0$, právě když tyto dva kořeny splývají.

Podívejme se, jak by šel z naší definice diskriminantu rychle odvodit vztah pro kořeny kvadratického trojčlenu. Řešíme vlastně soustavu rovnic

$$\begin{aligned} x_1 + x_2 &= -b, \\ x_1x_2 &= c, \end{aligned}$$

přičemž z těchto dvou rovnic jsme už odvodili, že $D(f) = (x_1 - x_2)^2$. Tedy známe druhou mocninu rozdílu a zároveň i součet čísel x_1 a x_2 . Předpokládejme navíc, že $x_1 \geq x_2$, pak přičtením vztahu $x_1 - x_2 = \sqrt{D}$ k první ze zadaných rovnic (resp. odečtením) dostaneme, že $2x_1 = -b + \sqrt{D}$ a $2x_2 = -b - \sqrt{D}$, z čehož plyne kýžený vzorec

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

Jak to ale bude vypadat pro polynomy vyšších stupňů? Je-li f mnohočlen stupně n , který má kořeny $x_1, x_2, \dots, x_n$, pak definujeme diskriminant f jako

$$D(f) = (x_1 - x_2)^2(x_1 - x_3)^2 \cdots (x_{n-1} - x_n)^2,$$

tedy jako součin druhých mocnin rozdílů všech dvojic kořenů. Pro polynomy stupně 3 nám toto dává

$$D(f) = (x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2.$$

Stejně jako v kvadratickém případě je $D(f)$ symetrický v neznámých $x_1, x_2, \dots, x_n$, protože když prohodíme libovolné dva kořeny, tak se nám hodnota díky druhým mocninám nezmění, maximálně se prohodí některé závorky. Diskriminant polynomu lze tedy vždy vyjádřit pomocí elementárních symetrických mnohočlenů, které díky Viètovým vztahům souvisí s koeficienty polynomů.

Díky tomu můžeme diskriminant vyjádřit jen pomocí koeficientů polynomu f . Pak definujeme diskriminant i pro polynomy, které nemají n kořenů, právě tímto vzorečkem.

Spočteme si například diskriminant polynomu $x^3 + ax + b$, což je polynom stupně 3, který nemá kvadratický člen. Z Viètových vzorců máme $\sigma_1 = x_1 + x_2 + x_3 = 0$, $\sigma_2 = x_1x_2 + x_2x_3 + x_1x_3 = -a$ a $\sigma_3 = x_1x_2x_3 = b$.

První věc, které si všimneme, je, že mnohočlen $D(f)$ v neznámých x_1, x_2 a x_3 je homogenní stupně 6. Navíc neboť $\sigma_1 = 0$, chceme D vyjádřit pouze pomocí σ_2 , který je homogenní stupně 2, a pomocí σ_3 , který je homogenní stupně 3. Proto aby nám seděly stupně mnohočlenů, musí být vyjádření D tvaru

$$D(x^3 + ax + b) = \alpha\sigma_2^3 + \beta\sigma_3^2,$$

protože žádným smíšeným členem nemůžeme dostat polynom stupně šest, neboť stupeň takového členu je $2k + 3l$, kde k je exponent u σ_2 a l exponent u σ_3 a $k, l > 0$, tímto způsobem ale nelze vyjádřit číslo 6. Navíc mocniny nesmíšených členů jsou jasné, neboť musíme zachovat stupeň.

Hledaný vzoreček musí fungovat pro všechny trojice kořenů x_1, x_2 a x_3 , můžeme tedy pomocí konkrétních hodnot najít koeficienty α a β . Například dosazením $x_1 = 1, x_2 = -1$ a $x_3 = 0$ dostaneme ze symetrických mnohočlenů jediný nenulový $\sigma_2 = -1$, platí tedy

$$-\alpha = D(x^3 - x) = (-1 - 1)^2(-1 - 0)^2(1 - 0)^2 = 4,$$

z čehož dostáváme, že $\alpha = -4$.

Dále dosazením $x_1 = x_2 = 1$ a $x_3 = -2$ dostaneme $\sigma_1 = 0$, $\sigma_2 = -3$ a $\sigma_3 = -2$, tedy

$$-27\alpha + 4\beta = D(x^3 + 3x - 2) = 0$$

a dopočítáme koeficient $\beta = 27\alpha/4 = -27$. Platí tedy

$$D(x^3 + ax + b) = -4a^3 - 27b^2.$$

Cvičení. Buď $a \neq 0$. Rozhodněte, zda následující mnohočleny mají vícenásobný kořen:

$$x^2 + 2ax, \quad x^3 - 3x + 2 \quad \text{a} \quad x^3 + a^2x + a^3.$$

Řešení. Diskriminant polynomu $x^2 + 2ax$ je $4a^2$, což je nenulové číslo díky tomu, že a je různé od nuly. První z polynomů nemá vícenásobné kořeny.

Diskriminant mnohočlenu $x^3 - 3x + 2$ je z výše odvozeného vzorečku roven $-4 \cdot (-3)^3 - 27 \cdot 2^2 = 4 \cdot 27 - 27 \cdot 4 = 0$. Tento kubický trojčlen může mít vícenásobný kořen, opravdu snadno ověříme, že $x^3 - 3x + 2 = (x - 1)^2(x + 2)$, tedy číslo 1 je dvojnásobný kořen.

Poslední ze zadaných mnohočlenů má diskriminant roven $-4a^6 - 27a^6 = -31a^6$, což je opět nenulové číslo, takže ani tento mnohočlen nemá vícenásobné kořeny.

Úloha. Ukažte, že diskriminant polynomu $(x^2 + 1)^2$ je 0, avšak tento polynom nemá žádné reálné kořeny, speciálně tedy nemá ani vícenásobné kořeny.

Úloha. Řešte v reálných číslech

$$x^3 - 6x - 4\sqrt{2} = 0.$$

Řešení. Spočteme-li si diskriminant tohoto polynomu, dostaneme

$$D = -4 \cdot (-6)^3 - 27 \cdot (-4\sqrt{2})^2 = 4 \cdot 6^3 - 27 \cdot 2^5 = 0,$$

tedy polynom $x^3 - 6x - 4\sqrt{2}$ má dvojnásobný kořen. Označme si ho a , poslední kořen tohoto mnohočlenu označme b . Z Viètových vztahů platí

$$\begin{aligned} 2a + b &= 0, \\ a^2 + 2ab &= -6, \\ a^2b &= 4\sqrt{2}. \end{aligned}$$

Vyřešme tuto soustavu rovnic. Z první rovnice vidíme, že $b = -2a$, dosadíme-li do poslední vztahu, máme $-2a^3 = 4\sqrt{2}$, proto $a^3 = -2\sqrt{2}$ a $a = -\sqrt{2}$, $b = 2\sqrt{2}$. Rovnice má dva reálné kořeny, dvojnásobný $-\sqrt{2}$ a jednonásobný $2\sqrt{2}$.

Úloha. Dokažte, že diskriminant polynomu f stupně 3 je kladný, právě když má f tři různé reálné kořeny.

Řešení. Ukažme nejdříve, že když má polynom f stupně 3 tři různé reálné kořeny a , b a c , tak má kladný diskriminant. To je ale ihned vidět ze vztahu

$$D(f) = (a - b)^2(b - c)^2(a - c)^2,$$

neboť všechny tři sčítance jsou druhé mocniny nenulových reálných čísel.

Naopak nechť f má kladný diskriminant. Pak víme, že f nemá dvojnásobný kořen. Předpokládejme pro spor, že f nemá tři reálné kořeny. Takový polynom má ovšem v komplexních číslech právě tři kořeny, z nichž jeden je reálný a dva jsou komplexně sdružené. Označme si je postupně c , $a + bi$ a $a - bi$ a spočteme diskriminant polynomu s těmito kořeny

$$D(f) = ((a+bi)-(a-bi))^2(c-(a+bi))^2(c-(a-bi))^2 = (2bi)^2(c-a-bi)^2(c-a+bi)^2 = -4b^2((c-a)^2+b^2).$$

Tento výraz je pro reálná a , b a c zřejmě nekladný.

Úloha. Spočítejte diskriminant mnohočlenů $x^4 + ax + b$ a $x^5 + ax + b$. Dokážete odvodit vzorec pro diskriminant mnohočlenů $x^n + ax + b$ pro $n > 1$ přirozené?

POLYNOMY NAD $\mathbb{Z}$ A $\mathbb{Q}$

Mnohočlenem nad $\mathbb{Z}$ myslíme takový mnohočlen nad $\mathbb{Q}$, jehož koeficienty jsou celá čísla. Množinu všech mnohočlenů nad $\mathbb{Z}$ značíme $\mathbb{Z}[x]$.

Všechna tvrzení o polynomech, která jsme uváděli v předcházejících kapitolách, platí beze zbytku pro polynomy nad $\mathbb{Q}$, $\mathbb{R}$ a $\mathbb{C}$, s celými čísly však máme jeden problém – nemůžeme jen tak dělit mnohočleny se zbytkem. Například podíl $x^2 + 1$ a $2x + 1$ nemá celočíselné koeficienty, neboť

$$x^2 + 1 = \left(\frac{1}{2}x - \frac{1}{4}\right)(2x + 1) + \frac{5}{4}.$$

Dělit se zbytkem můžeme bez problému jen monickými polynomy.

V polynomech nad celými čísly tedy neplatí věta o dělení se zbytkem, Bézoutova věta ani věta o jednoznačném rozkladu na nerozložitelné mnohočleny, tak jak jsou napsány v předchozích kapitolách. Naštěstí ale vždy můžeme počítat s mnohočleny nad $\mathbb{Q}$, a tak si zaručit platnost těchto vět.

Připomeňme, že polynom $f \in \mathbb{Z}[x]$ je *nerozložitelný* pokud neexistují polynomy $g, h \in \mathbb{Z}[x]$, každý stupně alespoň 1, takové, že $gh = f$.

Věta. (Gaussovo lemma) *Je-li $f \in \mathbb{Z}[x]$ nerozložitelný polynom nad $\mathbb{Z}$, pak je také nerozložitelný jako polynom nad $\mathbb{Q}$.*

Máme-li polynom nad $\mathbb{Q}$, můžeme ho snadno upravit na polynom s celočíselnými koeficienty tak, že ho vynásobíme nejmenším společným násobkem čitatelů jeho koeficientů. Gaussovo lemma tak jde použít i při důkazu nerozložitelnosti polynomů s racionálními koeficienty.

Věta. (Eisensteinovo kritérium) *Nechť $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ je polynom s celočíselnými koeficienty a nechť p je prvočíslo takové, že $p \mid a_i$ pro každé $i = 0, 1, \dots, n-1$ (tedy p dělí všechny koeficienty kromě prvního), $p \nmid a_n$ a $p^2 \nmid a_0$. Pak je mnohočlen f nerozložitelný nad $\mathbb{Q}$.*

Úloha. Dokažte, že je-li p prvočíslo, je mnohočlen $x^{p-1} + x^{p-2} + \dots + 1$ nerozložitelný nad $\mathbb{Z}$.

Řešení. Označme si $f(x) = x^{p-1} + x^{p-2} + \dots + 1$ a všimněme si, že $(x-1)f(x) = x^p - 1$. Budeme chtít použít Eisensteinovo kritérium, ale nemůžeme ho použít přímo, neboť žádný koeficient není dělitelný p . Uděláme tedy krok stranou, je-li mnohočlen $f(x)$ rozložitelný, pak je rozložitelný i mnohočlen $f(x+1)$ (stačí do rozkladu dosadit $x+1$ za x).

Přitom $xf(x+1) = (x+1)^p - 1$, tj.

$$f(x+1) = \frac{x^p + px^{p-1} + \binom{p}{2}x^{p-2} + \dots + 1 - 1}{x} = x^{p-1} + px^{p-2} + \binom{p}{2}x^{p-3} + \dots + \binom{p}{p-2}x + p.$$

Absolutní člen mnohočleny $f(x)$ je p , tedy první podmínku Eisensteinova kritéria máme splněnou ($p \mid a_0$, ale $p^2 \nmid a_0$), stejně tak je rovnou vidět, že $p \nmid a_n = 1$. Zbývá nám ukázat, že p dělí všechny ostatní koeficienty polynomu $f(x+1)$.

Koeficienty polynomu $f(x+1)$ jsou kombinační čísla tvaru $\binom{p}{k}$, kde $k = 1, 2, \dots, p-1$. Ukážeme, že tato kombinační čísla jsou pro prvočíslo p vždy dělitelná p , platí totiž

$$\binom{p}{k} = \frac{p!}{k!(p-k)!}.$$

Přitom p dělí čitatele tohoto zlomku, ale nikoliv jmenovatele, protože ve faktoriálu násobíme jen čísla menší než p , tedy p nedělí žádné z těchto čísel, ale p je prvočíslo, takže nemůže dělit ani jejich součin.

Následující tvrzení je užitečné k hledání všech racionálních kořenů mnohočleny nad $\mathbb{Q}$ nebo $\mathbb{Z}$.

Tvrzení. *Má-li mnohočlen $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$ celočíselné koeficienty, pak pro každý jeho racionální kořen $x_1 = p/q$, kde p a q jsou nesoudělná celá čísla, platí $p \mid a_0$ a $q \mid a_n$.*

Úloha. Ukažte, že je-li $f \in \mathbb{Z}[x]$ mnohočlen stupně 3, který nemá kořen v $\mathbb{Q}$, pak je ireducibilní nad $\mathbb{Z}$, a najděte rozložitelný mnohočlen stupně 3, který nemá kořen v $\mathbb{Z}$.

Řešení. Podívejme se nejprve na první část. Buď $f(x)$ polynom stupně 3, který je rozložitelný v $\mathbb{Z}$. Ukážeme, že f má racionální kořen. Platí

$$f(x) = g(x) \cdot h(x),$$

kde $g(x)$ a $h(x)$ jsou mnohočleny nenulového stupně. Porovnáme-li stupně na levé a pravé straně, zjistíme, že jediná možnost pro stupně g a h je, že jeden z nich má stupeň 1 a druhý 2. Tedy platí

$$f(x) = (ax + b)(cx^2 + dx + e),$$

pak ale racionální číslo $-b/a$ je kořenem mnohočleny f , neboť po dosazení vyjde první závorka nulová.

Abychom splnili druhou část, stačí nám najít mnohočlen, který má racionální neceločíselný kořen a má celočíselné koeficienty, a pak najdeme jeho rozklad. Zvolme třeba kořen $1/2$ a polynom

$$f_1(x) = \left(x - \frac{1}{2}\right)(x^2 + 1) = x^3 - \frac{1}{2}x^2 + x - \frac{1}{2}.$$

Tento mnohočlen ovšem nemá celočíselné koeficienty, ale to snadno napravíme přenásobením dvěma

$$f(x) = 2f_1(x) = 2x^3 - x^2 + 2x - 1.$$

Nakonec nám zbývá ověřit, že f nemá celočíselný kořen. Takový kořen a by musel být dělitelem absolutního členu mnohočleny, tj. $a \mid 1$. Máme pouze dvě možnosti ± 1 . Dosazením ověříme, že $f(1) = 2$ a $f(-1) = -6$. Opravdu f nemá celočíselný kořen, přitom se rozkládá jako $(2x - 1)(x^2 + 1)$.

Nakonec uvádíme jedno tvrzení o polynomech nad celými čísly, které lze využít v klasické teorii čísel.

Věta. Je-li $f \in \mathbb{Z}[x]$, $n \in \mathbb{N}$ a platí-li pro celá čísla a a b , že $n \mid a - b$, pak $n \mid f(a) - f(b)$.

Cvičení. Najděte mnohočlen f nad $\mathbb{Z}[x]$, který splňuje $f(3) = 15$ a $f(7) = 17$.

Řešení. Takový mnohočlen neexistuje. Zdůvodníme to výše zmíněnou větou pro čísla 3 a 7. Platí $4 \mid 7 - 3 = 4$, pro hledaný mnohočlen by tedy muselo platit $4 \mid f(7) - f(3) = 17 - 15 = 2$, což neplatí.

POLYNOMY NAD $\mathbb{Z}_p$

V této kapitole budeme pracovat s polynomy nad celými čísly, s jejichž koeficienty budeme počítat modulo prvočíslo p .

Nechť p je libovolné celé číslo (typicky prvočíslo). Řekneme, že dvě celá čísla a a b jsou *kongruentní modulo p* , pokud $p \mid a - b$. Tuto skutečnost zapisujeme $a \equiv b \pmod{p}$.

Tvrzení. Čísla a a b jsou kongruentní modulo p , právě když dávají stejný zbytek po dělení p .

Důkaz. Předpokládejme nejdříve, že a a b dávají stejný zbytek po dělení p , tedy $a = q_1p + r$ a $b = q_2p + r$. Pak $a - b = (q_1p + r) - (q_2p + r) = (q_1 - q_2)p$ a $p \mid a - b$.

Nechť naopak $a \equiv b \pmod{p}$ a nechť r_1 a r_2 jsou zbytky a q_1 a q_2 podíly po dělení a a b číslem p . Platí

$$p \mid a - b = q_1p + r_1 - q_2p - r_2 = (q_1 - q_2)p + (r_1 - r_2),$$

a protože p dělí prvního sčítance, dělí i druhého, tedy $r_1 \equiv r_2 \pmod{p}$. Přitom $r_1, r_2 < p$, tedy $-p < r_1 - r_2 < p$, ale v tomto rozmezí je jediný násobek p , totiž 0. Dostáváme, co jsme chtěli, $r_1 - r_2 = 0$. $\square$

Věta. (Malá Fermatova) Je-li p prvočíslo a a celé číslo takové, že $a \not\equiv 0 \pmod{p}$, pak platí

$$a^{p-1} \equiv 1 \pmod{p}.$$

Definujme množinu $\mathbb{Z}_p$ jako množinu všech zbytků po dělení prvočíslem p , tj. $\{0, 1, \dots, p-1\}$. Navíc na této množině budeme ještě uvažovat operace $+_n$ a $\cdot_n$ tak, aby platilo

$$a +_n b \equiv a + b \quad \text{a} \quad a \cdot_n b \equiv ab \pmod{p}.$$

Tato volba je jednoznačná, neboť jsme se omezili jen na množinu zbytků modulo p . Pokud nebude moci dojít k záměně, budeme pro stručnost psát operace $+_n$ a $\cdot_n$ jen jako $+$ a $\cdot$.

Tvrzení. Pro každé nenulové $a \in \mathbb{Z}_p$ existuje jednoznačné $b \in \mathbb{Z}_p$, že $ab = 1$. Toto b budeme značit $1/a$.

Důkaz. Nechť $a \in \{1, \dots, p-1\}$. Pak speciálně a je nesoudělné s p , neboť p je prvočíslo. Z Bézoutovy věty tedy existují celá čísla b' a n taková, že

$$ab' + np = 1.$$

Zvolme za b zbytek b' po dělení p , tedy $b' = qp + b$. V celých číslech platí

$$ab = a(b' - qp) = -aqp + ab' = -aqp - np + 1 = -(aq + n)p + 1.$$

Tedy zbytek ab po dělení p je právě 1 a platí $a \cdot_p b = 1$. Tím jsme dokázali existenci. Zbývá jednoznačnost.

Jsou-li b_1 a b_2 dva takové zbytky, pak přenásobením rovnosti $a \cdot_p b_2 = 1$ číslem b_1 dostaneme $b_1 \cdot_p a \cdot_p b_2 = b_1$. Obdobně také $b_1 \cdot_p a \cdot_p b_2 = b_2$, tedy $b_1 = b_2$. $\square$

Nad $\mathbb{Z}_p$ definujeme mnohočleny stejně jako nad ostatními obory. Důležité je, že díky dělení se nám tyto polynomy chovají tak pěkně jako polynomy nad $\mathbb{R}$ nebo $\mathbb{Q}$, speciálně je můžeme dělit se zbytkem, aniž bychom se omezovali na monické polynomy, a máme větu o jednoznačném rozkladu na nerozložitelné mnohočleny. Množinu všech mnohočlenů nad $\mathbb{Z}_p$ značíme $\mathbb{Z}_p[x]$.

Věta. (Wilsonova) *Nechť $p > 1$ je celé číslo. Pak p je prvočíslo právě tehdy, když*

$$(p-1)! \equiv -1 \pmod{p}.$$

Důkaz. Implikace, že je-li n složené, tak $(n-1)! \not\equiv -1 \pmod{n}$, je jednoduchá. Složené číslo má vlastního dělitele d , který se vyskytuje jako činitel v $(n-1)!$, tedy $d \mid (n-1)!$, a kdyby $(n-1)! \equiv -1 \pmod{n}$, pak také $d \mid (n-1)! + 1$. Z toho odvodíme $d \mid 1$, což je spor s tím, že d je vlastní dělitel n .

Opačná implikace je trochu složitější a použijeme pro ni polynomy nad $\mathbb{Z}_p$. Nechť tedy p je prvočíslo. Uvažme polynom $x^{p-1} - 1$ nad $\mathbb{Z}_p$. Pro všechny nenulové zbytky a modulo p platí

$$a^{p-1} \equiv 1 \pmod{p},$$

tedy všechny zbytky jsou kořeny tohoto polynomu. Těchto zbytků je $p-1$, musí tedy nastat rovnost polynomů (nad $\mathbb{Z}_p$)

$$x^{p-1} - 1 = (x-1)(x-2)\cdots(x-p+1).$$

Porovnáním absolutních členů pak dostaneme, že

$$1 \cdot_p 2 \cdot_p \cdots \cdot_p (p-1) = -1,$$

což po přepsání do celých čísel znamená právě $(p-1)! \equiv -1 \pmod{p}$. $\square$

MATEMATICKÁ OLYMPIÁDA

V poslední kapitole uvádíme sbírku několika příkladů na polynomy, které se objevily v několika posledních letech v celostátním kole matematické olympiády. K některým z nich uvádíme řešení, zbylé mohou posloužit jako zajímavá a účelná sbírka těžkých příkladů.

Úloha. (CK MO 49. ročník) Pro které kvadratické funkce $f(x)$ existuje taková kvadratická funkce $g(x)$, že kořeny rovnice $g(f(x)) = 0$ jsou čtyři po sobě jdoucí členy aritmetické posloupnosti a současně i kořeny rovnice $f(x)g(x) = 0$?

Řešení. Naším úkolem je najít všechny kvadratické polynomy f , pro které existuje kvadratický polynom g takový, že f a g budou splňovat podmínky v zadání. Prvně se podívejme na kořeny rovnice $f(x)g(x) = 0$, to je rovnice čtvrtého stupně, která má právě čtyři různé kořeny. Přitom víme, že jsou to právě kořeny f a g (dva a dva), označme je postupně x_1, x_2, x_3 a x_4 .

Tedy i rovnice $g(f(x)) = 0$ musí mít za kořeny všechny kořeny f a všechny kořeny g . Dosadíme-li do této rovnice kořen f , dostaneme $g(0) = 0$. Víme tedy, že jeden z kořenů g je 0. Bez újmy na obecnosti buď tedy $x_4 = 0$.

Dosadíme-li do této rovnice $x_4 = 0$, dostaneme $g(f(0)) = 0$, tedy $f(0)$ je kořen g , přitom je ale nenulový, tedy $f(0) = x_3$. Podobně po dosazení x_3 do té samé rovnice dostaneme $f(x_3) = x_3$.

Mnohočlen f je kvadratický, jeho grafem je tedy parabola. Budeme-li chtít najít x -ovou souřadnici vrcholu této paraboly, můžeme postupovat dvěma způsoby. Jednak je hledaná souřadnice aritmetický průměr kořenů f , tj. $(x_1+x_2)/2$, jednak využijeme toho, že $f(x_3) = f(0) = x_3$, a tedy hledaná souřadnice je i aritmetický průměr x_3 a $x_4 = 0$. Musí tedy platit

$$x_1 + x_2 = x_3 + x_4.$$

Odtud už je jen málo možností, jak mohou být za sebou poskládány členy aritmetické posloupnosti x_1, x_2, x_3 a x_4 . Jedna z dvojic x_1, x_2 a x_3, x_4 tvoří první a čtvrtý člen a druhá druhý a třetí. Tyto dva případy rozebereme zvlášť.

Prvně nechť 0 je první (nebo poslední) člen aritmetické posloupnosti, pak $x_3 = 3d$, $x_1 = d$ a $x_2 = 2d$. Polynom f je tedy tvaru $a(x-d)(x-2d)$, kde a je takové číslo, aby platilo $f(x_4) = x_3$, tj. $f(0) = 3d$. Dostáváme rovnici $3d = a(-d)(-2d)$, musí tedy platit $a = 3/(2d)$.

Kdyby 0 byla druhý nebo třetí člen, pak $x_3 = d$ a platí $x_1 = -d$ a $x_2 = 2d$, tedy řešením jsou polynomy $f(x) = a(x+d)(x-2d)$. Hodnotu a , podobně jako v předchozím případě, musíme zvolit tak, aby $f(x_4) = x_3$, tj. $f(0) = d$. Dostáváme tedy $d = ad(-2d)$, odkud $a = -1/(2d)$. Ověřte si, že pak platí i $f(x_3) = x_3$.

Nakonec zbývá ověřit, že jsme opravdu splnili všechny podmínky, což je ale pravda, protože zřejmě kořeny $f(x)g(x) = 0$ tvoří čtyři členy aritmetické posloupnosti a přitom jsou to i kořeny $g(f(x)) = 0$ díky tomu, že $g(0) = 0$ a $f(x_3) = f(x_4) = x_3$.

Všechny hledané kvadratické funkce f jsou tedy tvaru

$$\frac{3}{2d}(x-d)(x-2d), \quad \text{nebo} \quad -\frac{1}{2d}(x+d)(x-2d).$$

Úloha. (CK MO 50. ročník) Určete všechny mnohočleny P takové, že pro všechna reálná čísla x platí

$$P(x)^2 + P(-x) = P(x^2) + P(x).$$

Úloha. (CK MO 51. ročník) Najděte všechny dvojice reálných čísel a, b , pro které má rovnice

$$\frac{ax^2 - 24x + b}{x^2 - 1} = x$$

v oboru reálných čísel právě dvě řešení, přičemž jejich součet je 12.

Řešení. Vynásobme obě strany rovnice výrazem $x^2 - 1$ a převedme na pravou stranu, dostaneme kubickou rovnici

$$x^3 - ax^2 + 23x - b = 0.$$

Chceme, aby původní rovnice měla právě dvě reálná řešení, tedy výsledná kubická rovnice buď musí mít jeden dvojnásobný a jeden jednonásobný kořen, nebo musí mít tři různé reálné kořeny, z nichž právě jeden je ± 1 , neboť pro $x = \pm 1$ nemá původní rovnice smysl.

Podívejme se nejdříve na první případ. Kubická rovnice má tedy kořeny s, s a $12 - s$. Podle Viètových vztahů tedy platí

$$a = 12 + s,$$

$$23 = -s^2 + 24s,$$

$$b = s^2(12 - s).$$

Přitom druhý vztah má řešení $s = 1$ a $s = 23$, první hodnota je pro nás nepřijatelná, neboť pak by zadaná rovnice měla jediné řešení. Platí tedy $s = 23$, z čehož dostaneme $a = 35$ a $b = -11 \cdot 23^2 = -5819$. Rovnice má v tomto případě řešení $x = 23$ a -11 .

Pokud je jeden z kořenů -1 , pak víme, že součet všech tří kořenů je 11, neboť ze zadání součet zbylých dvou je 12. Víme tedy, že $a = 11$. Po dosazení -1 můžeme získat i hodnotu b , platí totiž

$$(-1)^3 - 11 \cdot (-1)^2 + 23 \cdot (-1) - b = 0,$$

tedy $b = -35$. Snadno uhadneme kořeny 5 a 7. Tedy dvojice $a = 11, b = -35$ vyhovuje zadání.

Podobně budeme postupovat i v případě, že je jeden z kořenů 1, součet všech tří kořenů je pak 13, tedy $a = 13$ a navíc 1 musí být kořenem kubické rovnice

$$x^3 - 13x^2 + 23x - b = 0,$$

odkud snadno dostaneme, že $b = 11$. Opět můžeme snadno uhadnout kořeny 1 a 11. V tomto případě ale zadaná rovnice nemá dvě reálná řešení, nýbrž jen jedno (číslo 11).

Úloha má tedy dvě řešení, dvojice $a = 35, b = -5819$ a $a = 13, b = -35$.

Úloha. (CK MO 53. ročník) Dokažte, že pro libovolná reálná čísla p, q, r, s za podmínek $q \neq -1$ a $s \neq -1$ platí: Kvadratické rovnice

$$x^2 + px + q = 0, \quad x^2 + rx + s = 0$$

mají v oboru reálných čísel společný kořen a jejich další kořeny jsou navzájem převrácená čísla právě tehdy, když koeficienty p, q, r, s splňují rovnosti

$$pr = (q+1)(s+1) \quad \text{a} \quad p(q+1)s = r(s+1)q.$$

(Dvojnásobný kořen kvadratické rovnice počítáme dvakrát.)

Úloha. (CK MO 57. ročník) V oboru reálných čísel řešte soustavu rovnic

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

Úloha. (CK MO 60. ročník) Předpokládejme, že reálná čísla x, y, z vyhovují soustavě rovnic

$$x + y + z = 12, \quad x^2 + y^2 + z^2 = 54.$$

Dokažte, že pak platí následující tvrzení:

- (a) Každé z čísel xy, yz, zx je alespoň 9, avšak nejvýše 25.
- (b) Některé z čísel x, y, z je nejvýše 3 a jiné z nich je alespoň 5.

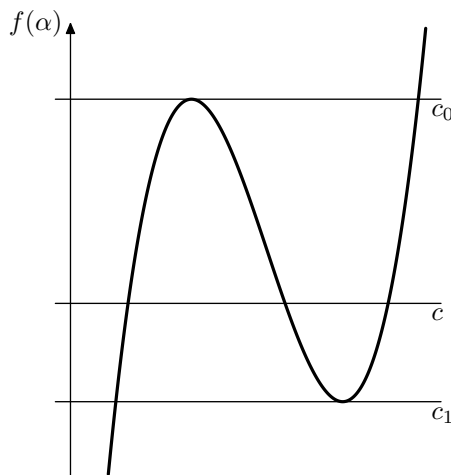
Řešení. Vyřešíme nejdříve část (b). Zadané vztahy jsou symetrické vzhledem k neznámým x, y, z , označme tedy $\sigma_1 = x + y + z$, $\sigma_2 = xy + yz + zx$ a $\sigma_3 = xyz$. Ze zadání víme, že

$$\sigma_1 = 12 \quad \text{a} \quad \sigma_1^2 - 2\sigma_2 = 54.$$

Snadno si tedy dopočteme $\sigma_2 = (144 - 54)/2 = 45$. Víme tedy, že čísla x, y, z jsou kořeny polynomu

$$f(\alpha) = \alpha^3 - 12\alpha^2 + 45\alpha + c,$$

kde c je neznámé číslo. Na hodnotě c ovšem závisí jen posunutí grafu tohoto polynomu vzhledem k ose x . Nakreslíme-li si obecný graf kubické funkce, bude vypadat jako na obrázku dole, přičemž víme, že polynom má tři reálné kořeny, takže hodnota c bude někde mezi c_0 a c_1 , které odpovídají situacím, kdy má polynom f dvojnásobný kořen.



Z obrázku je tedy vidět, že jedno z čísel x, y, z bude vlevo od levého vrcholu a druhé vpravo od pravého vrcholu (nebo spíše dolíku). Potřebujeme tedy už jen spočítat x -ové souřadnice vrcholů, ty ale

odpovídají dvojnásobným kořenům f při vhodném dosazení c . Dvojnásobný kořen f je kořenem jeho derivace, spočtěme si tedy

$$f'(\alpha) = 3\alpha^2 - 24\alpha + 45 = 3(\alpha^2 - 8\alpha + 15).$$

Tento polynom má kořeny $\alpha = 3$ a 5 , tedy hledané x -ové souřadnice jsou 3 a 5 . Tím jsme dokončili část (b). Pro zajímavost ještě dopočteme poslední kořen f . V případě dvojnásobného kořenu 3 je to 6 a v případě dvojnásobného kořenu 5 je to 2 . Z grafu tedy můžeme ještě navíc vyčíst (za předpokladu $x \leq y \leq z$), že platí

$$2 \leq x \leq 3 \leq y \leq 5 \leq z \leq 6,$$

což se nám bude hodit v části (a).

Víme, že platí $xy + yz + zx = 45$ a přitom $x + y + z = 12$. Upravujme tedy první z těchto vztahů

$$45 = xy + yz + zx = xy + z(x + y) = xy + z(12 - z), \quad xy = 45 - z(12 - z) = (6 - z)^2 + 9.$$

Okamžitě je vidět, že $xy \geq 9$. Navíc nejvyšší možnou hodnotu xy dostaneme, když $(6 - z)^2$ bude co největší, tj. z bude „co nejdále“ od 6 , přitom ale víme, že $2 \leq z \leq 6$, tedy největší možná hodnota xy je pro $z = 2$, tj. $xy \leq 4^2 + 9 = 25$. Zbývá si jen uvědomit, že stejná úvaha funguje i pro výrazy yz a xz .

LITERATURA

- [KHŠ] Kučera R., Herman J., Šimša J., *Metody řešení matematických úloh I*, Masarykova Univerzita, Brno, 2001.
- [S] Stanovský D., *Základy algebry*, Matfyzpress, Praha, 2010.
- [MO] *Archiv Matematické olympiády*, <http://www.math.muni.cz/~rvmo/>.

Úloha 1. Najděte všechny dvojice reálných čísel x, y , které splňují vztahy

$$x_1 - x_1x_2 + x_2 = 1,$$

$$x_1^2 - x_1x_2 + x_2^2 = 3.$$

Úloha 2. Najděte kořeny mnohočlenu $f \in \mathbb{R}$ a jejich násobnost, je-li

$$f(x) = x^3 - 3\sqrt{2}x^2 + 8\sqrt{2}.$$

Úloha 3. Je-li n dané přirozené číslo, spočtěte největšího společného dělitele polynomů $x^{2^{n+1}} + x^{2^n} + 1$ a $x^{2^{n+1}} - x^{2^n} + 1$.

Úloha 4. Rozhodněte, pro která reálná čísla a má mnohočlen $x^3 - 3x + a$ vícenásobný (alespoň dvojnásobný) kořen.

Úloha 5. UkaŹte, Źe polynom

$$f = x^5 - 3x^4 + 2x^3 - 2x^2 + 3x + 1$$

je nerozloŹitelný nad $\mathbb{Z}[x]$.