

Polynomy 1 – Ke kořenům a zase zpátky

Milý příteli,

vítej u prvního dílu letošního seriálu, v němž budeme brouzdat světem polynomů. *Polynom*, nebo též hezky česky *mnohočlen*, je pojem, který už jsi dost možná někdy potkal(a). Schovává se za ním výraz s proměnnou x a s koeficienty $a_0, a_1, \dots, a_n$, který může vypadat nějak takhle:

$$a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x_1 + a_0.$$

Matematiky často zajímá hledání kořenů, tedy jaká čísla za x můžeme dosadit, aby celý výraz nabyl nulové hodnoty. I nás budou kořeny na naší cestě provázet: po osvojení základních pojmů si v tomto díle ukážeme, jak s pomocí kořenů faktorizovat polynom na součin a k čemu je to dobré. Poté prozkoumáme, jak se od kořenů vrátit zpět ke koeficientům, a na úplný závěr představíme pár hezkých i špinavých triků na úlohy, v nichž hledáme neznámý polynom.

Pokud jsi potkal(a) polynomy ve škole, pravděpodobně jste jako proměnné, kořeny i koeficienty brali reálná čísla. Spousta zajímavých úloh ale vznikne tak, že místo o reálných číslech začneme přemýšlet jenom o těch celých nebo racionálních. Nebo si naopak můžeme svět reálných čísel zvětšit na komplexní čísla. Abychom podchytili co nejvíc z této rozmanitosti, budeme se teorii snažit budovat trochu obecně. Díky tomu pak budeme schopni snadno přepínat, zda zrovna hovoříme o polynomech „nad“ reálnými, celými, racionálními, ... či jakýmkoliv exotičtějšími čísly.

Seriál pro Tebe letos píše Majda Mišinová, Matěj Doležálek a Tom Flídr. Zavrtá-li se Ti do hlavy při čtení jakákoliv otázka či nejasnost, neváhej se na nás obrátit na mailových adresách magdalena.misinova@gmail.com, matej@prase.cz a tomas@flidr.name. Přejeme příjemné čtení!

O příkladech, cvičeních a úlohách

V seriálu bychom Ti rádi pomohli procvičit si počítání a řešení úloh. V textu jsou k tomuto účelu rozesety tři druhy pomůcek. **Příklady** jsou řešené ukázky, na kterých Ti chceme osvětlit nejtýpčtější metody, které se při řešení úloh hodí znát. **Cvičení** jsou zamyšlení, která by Tě měla ubezpečit v osvojení zavedených pojmů, či menší tvrzení, která je podle nás hodnotnější si nejprve zkusit sám/sama. Pokud by se Ti to nedařilo, nezoufej, na konci dílu najdeš návody k některým z nich a ještě o kousek dál řešení úplně všech. Konečně **Úlohy** jsou problémy olympiádního typu, podobně jako běžně můžeš potkat na soutěžích. Některé mohou být těžší než Cvičení, na oplátku zase ale bývají hezčí. Stejně jako cvičení jsou pak i úlohy opatřeny návody a řešeními na konci textu.

Základní definice

V tomto seriálu budeme polynomy uvažovat jen s koeficienty branými z množin, kterým říkáme *obory*. Obor je ve zkratce struktura, v níž máme význačné prvky 0 a 1 a ve které můžeme násobit, sčítat a odečítat tak, jak jsi zvyklý/zvyklá. Tím myslíme třeba to, že při sčítání nezávisí na pořadí ani na uzavírkování, že můžeme roznásobovat závorky jako $a \cdot (b+c) = ab+ac$ nebo že součin ab může být nulový, jen když je a nebo b (nebo obojí) nula. Pozor, schopnost dělit v oboru nevyžadujeme.

Příklady oborů jsou celá čísla $\mathbb{Z}$, racionální čísla $\mathbb{Q}$, reálná čísla $\mathbb{R}$ nebo komplexní čísla¹ $\mathbb{C}$. Pokud by Tě během čtení seriálu pojem „obor“ znervózňoval, klidně si představuj, že je to jen některý ze $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ či $\mathbb{C}$, neboť stejné myšlenky budou povětšinou fungovat jak s jedním konkrétním oborem, tak s libovolným jiným. Pokud jsi už někdy potkal(a) modulární aritmetiku, můžeš si jako bonus pro každé prvočíslo p představovat také $\mathbb{Z}_p$ (celá čísla modulo p), neboť to je též oborem.

Definice. Je-li R obor, pak *polynomem nad R* myslíme výraz tvaru $P(x) = a_n x^n + \cdots + a_1 x + a_0$, kde n je nějaké nezáporné celé číslo a $a_0, a_1, \dots, a_n \in R$. Množinu všech polynomů nad R v proměnné x značíme $R[x]$.

Pokud $a_n \neq 0$, nazýváme a_n *vedoucím koeficientem* polynomu P . Naproti tomu a_0 nazýváme *konstantním* nebo též *absolutním členem* polynomu P . Domluvme se také, že si v zápisu polynomů dovolíme vynechávat jedničkové koeficienty a členy s nulovým koeficientem a že záporná znaménka bude psát pomocí rozdílu: např. tedy napíšeme $x^2 - 1$ namísto striktně formálního $1x^2 + 0x + (-1)$. Podobně se domluvme, že pokud se odkážeme na koeficient s indexem větším než n , bereme, že je to nula.

Na polynomy se primárně díváme jako na výrazy s proměnnou. Přirozené je ale taky vnímat polynomy jako funkce: když máme polynom $P(x) = a_n x^n + \cdots + a_1 x + a_0 \in R[x]$ a nějaký prvek $r \in R$, můžeme jej *dosadit* a získat tak nějaký nový prvek $P(r) = a_n r^n + \cdots + a_1 r + a_0 \in R$. Když napíšeme $P(x) = Q(x)$, budeme tím myslet, že P a Q mají stejné koeficienty u každé mocniny x . Pozor, to obecně není ekvivalentní s tím, že $P(r) = Q(r)$ pro každé $r \in R$. V tomto díle tuhle situaci nepotkáme, ale nad některými obory mohou existovat polynomy, které jsou různé, ale přesto dosazením libovolného prvku dávají vždy stejnou hodnotu. (Pokud si rozumíš s obory $\mathbb{Z}_p$, můžeš si rozmyslet, že x^2 a x dávají nad $\mathbb{Z}_2$ vždy stejné hodnoty, ale přesto jsou to různé polynomy.)

Definice. O $\alpha \in R$ řekneme, že je *kořenem* polynomu P , pokud $P(\alpha) = 0$. Pokud takové $\alpha \in R$ existuje, říkáme, že P *má kořen* v R .

Definice. Je-li $P \in R[x]$ polynom $P(x) = a_n x^n + \cdots + a_1 x + a_0$ a $a_n \neq 0$, pak n nazveme *stupněm* P , což značíme jako $\deg(P) = n$. Speciálně definujeme $\deg(0) = -\infty$.

Pro nízké stupně existují zabitá názvy: polynom nazýváme *konstantním*, pokud má stupeň 0 nebo je nulový, *lineárním*, pokud má stupeň 1, *kvadratickým*, pokud má stupeň 2, *kubickým*, pokud má stupeň 3, atd.

Všimni si, že každé celé číslo je racionální a každé racionální číslo je reálné. Máme-li tedy polynom s celočíselnými koeficienty, můžeme ho interpretovat jako polynom nad $\mathbb{Z}$, nad $\mathbb{Q}$ i jako polynom nad $\mathbb{R}$. Podobně u polynomu nad $\mathbb{Z}$ můžeme koeficienty interpretovat jen jako zbytkové třídy modulo nějaké p a získat tak polynom nad $\mathbb{Z}_p$. Zápis bude mít pořád stejný, ale jeho vlastnosti se můžou značně lišit.

Cvičení 1. Najdi polynom s celočíselnými koeficienty takový, že

- (i) má kořen v $\mathbb{Q}$, ale ne v $\mathbb{Z}$,
- (ii) má kořen v $\mathbb{R}$, ale ne v $\mathbb{Q}$,
- (iii) (jen pokud znáš $\mathbb{Z}_p$) má kořen v $\mathbb{R}$, ale ne v $\mathbb{Z}_5$,
- (iv) (jen pokud znáš $\mathbb{Z}_p$) má kořen v $\mathbb{Z}_5$, ale ne v $\mathbb{R}$.

Úloha 1. Ať je dán nenulový polynom $P(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ a číslo $0 \neq r \in \mathbb{R}$, které je jeho kořenem. Najdi nějaký polynom nad $\mathbb{Q}$, jehož kořenem je $\frac{1}{r}$.

V tomto díle se budeme zabývat hlavně polynomy nad $\mathbb{R}$ (a později nad $\mathbb{C}$), v zájmu obecnosti se toho však budeme snažit co nejvíce zformulovat a dokázat nad obecným oborem.

¹Pokud se s komplexními čísly zatím nekamarádiš, nevěš hlavu – v tomto dílu vás seznámíme.

Sumy

Polynomy typicky píšeme jako součty jejich členů. Zatím jsme pro to používali notaci s třemi tečkami, která má ale jisté nevýhody. Zabírá více místa, a hlavně není vždy jednoznačná: $3 + 5 + \dots + 11$ může být jak součet lichých čísel od 3 do 11, tak součet prvočísel v témže rozsahu. Oba tyto problémy řeší zápis pomocí sum: máme-li výrazy $f_k, f_{k+1}, \dots, f_n$, jejich součet můžeme napsat jako $\sum_{j=k}^n f_j = f_k + f_{k+1} + \dots + f_n$. Například tedy polynom

$$a_n x^n + \dots + a_1 x_1 + a_0 \quad \text{můžeme napsat jako} \quad \sum_{j=0}^n a_j x^j.$$

Všimni si, že v tištěné podobě se počáteční a koncový index píšou jak nad a pod sumační symbol, tak i vedle – co do významu v tom není žádný rozdíl. Abychom mohli sumami pohodlně zapisovat polynomy, domluvme se, že x^0 vždy znamená 1, jinak bychom striktně vzato při dosazování $x = 0$ dostávali nedefinovaný výraz 0^0 .

Na pořadí sčítanců nezáleží a proměnná, přes kterou sčítáme, je použita pouze uvnitř sumy. Můžeme tak s podobou sumy trochu čachrovat – musíme si ale dát pozor, aby byl každý sčítanec zahrnut právě jednou. Například

$$\sum_{j=0}^n f_j = \sum_{j=1}^{n+1} f_{j-1} = \sum_{j=0}^n f_{n-j}.$$

Sčítat můžeme i přes více proměnných, to si lze představit jako sčítání hodnot zapsaných v políčkách nějaké tabulky. Sumy přes různé proměnné můžeme prohazovat, tak jako v tabulce nezáleží na tom, jestli sčítáme přes řádky, nebo přes sloupce:²

$$\sum_{j=1}^n \sum_{k=1}^m f_{jk} = \sum_{k=1}^m \sum_{j=1}^n f_{jk}.$$

Operace s polynomy

Když dostaneš dva polynomy, $P(x) = a_n x^n + \dots + a_1 x_1 + a_0$ a $Q(x) = b_m x^m + \dots + b_1 x_1 + b_0$, jsou v zásadě tři věci, které s nimi můžeš udělat:

- (1) Sečíst je. Potom prostě sečteš jejich koeficienty u příslušných mocnin proměnné:

$$(P + Q)(x) = \sum_{j=0}^{\max\{m,n\}} (a_j + b_j) x^j.$$

- (2) Vynásobit je. Pro mocniny neznámé pak může existovat hodně způsobů, jak ji získat jakou součin členu v p a členu v q :

$$(P \cdot Q)(x) = \sum_{j=0}^n \sum_{k=0}^m a_j b_k x^{j+k} = \sum_{\ell=0}^{n+m} \left(\sum_{j=0}^{\ell} a_j b_{\ell-j} \right) x^{\ell}.$$

- (3) Složit je, neboli dosadit jeden do druhého. Potom se stane něco hodně divokého, neboť budeme hodně násobit:

$$P(Q(x)) = \sum_{j=0}^n a_j Q(x)^j = \sum_{j=0}^n a_j \left(\sum_{k=0}^m b_k x^k \right)^j.$$

Může se zdát, že jsme občas použili nějaký nedefinovaný koeficient. Pokud nás ale zajímá koeficient na pozici vyšší, než je stupeň polynomu, řekneme prostě, že je to nula.

²Kdybychom zkoušeli sčítat nekonečně mnoho prvků, mohli bychom se dostat do problémů. Naštěstí je ale každý polynom součet konečně mnoha členů.

Tvrzení. (operace s polynomy a stupně) *Necht' P a Q jsou nenulové polynomy nad oborem R . Potom:*

- (i) $\deg(P \cdot Q) = \deg(P) + \deg(Q)$,
- (ii) $\deg(P(Q(x))) = \deg(P) \cdot \deg(Q)$,
- (iii) $\deg(P + Q) \leq \max\{\deg(P), \deg(Q)\}$. Pokud $\deg(P) \neq \deg(Q)$, pak už dokonce v předchozí nerovnosti nastane rovnost.

Cvičení 2. Najdi nad $\mathbb{R}$ polynomy P a Q takové, že $\deg(P(x) + Q(x)) < \max\{\deg(P), \deg(Q)\}$.

Kořeny

Když dostaneme nějaký polynom, nejpřirozenější otázkou je, jaké má kořeny. S řešením kvadratické rovnice ses jistě setkal(a) ve škole, tím Tě tu proto nudit nebudeme :-). Pro polynomy vyšších stupňů je hledání kořenů výrazně těžší a pro polynomy pátého a vyššího stupně je dokonce nemožné najít formulku, která by kořeny polynomu vyjádřila pomocí jeho koeficientů. Přesto můžeme o kořenech obecného polynomu říct spoustu věcí.

Tvrzení. *Je-li R obor a $P \in R[x]$ polynom s kořenem $\alpha \in R$, pak existuje polynom $Q \in R[x]$ takový, že $P(x) = (x - \alpha) \cdot Q(x)$.*

Důkaz. Uvažujme „posunutý“ polynom $\tilde{P}(x) = P(x + \alpha)$ a označme si jeho koeficienty jako $\tilde{P}(x) = a_n x^n + \dots + a_1 x + a_0$. Dosazením $x = 0$ se vynulují všechny členy kromě absolutního, takže získáme $a_0 = \tilde{P}(0)$. Na druhou stranu ale víme $\tilde{P}(0) = P(\alpha) = 0$, protože α je kořenem P . Člen $a_0 = 0$ nám tak zmizí a můžeme zapsat

$$\tilde{P}(x) = a_n x^n + \dots + a_1 x = x \cdot \underbrace{(a_n x^{n-1} + \dots + a_1)}_{=\tilde{Q}(x)},$$

kde jsme označením polynomu v poslední závorce jako $\tilde{Q}$ získali $\tilde{P}(x) = x \cdot \tilde{Q}(x)$. Nakonec ještě pojmenujme $Q(x) = \tilde{Q}(x - \alpha)$, čímž už dostaneme

$$P(x) = P((x - \alpha) + \alpha) = \tilde{P}(x - \alpha) = (x - \alpha)\tilde{Q}(x - \alpha) = (x - \alpha)Q(x). \quad \square$$

Tvrzení. *Nenulový polynom P stupně n nad oborem R má v R nanejvýš n kořenů. Pokud má n různých kořenů $\alpha_1, \dots, \alpha_n \in R$, pak už jej lze zapsat ve tvaru $P(x) = c(x - \alpha_1) \dots (x - \alpha_n)$ pro nějaké $c \in R$.*

Důkaz. Budeme postupovat matematickou indukcí. Jako základní případ vyřešíme $n = 0$, pak je P konstantní a nenulový, tedy $P(x) = c$ pro nějaké $0 \neq c \in R$. Automaticky tudíž P nemůže mít kořen, protože ať dosadíme cokoliv, výsledná hodnota bude c . Skutečně tak P má nanejvýš 0 kořenů, navíc jsme jej vyjádřili v odpovídajícím součinném³ tvaru $P(x) = c$.

Dále předpokládejme, že P je polynom stupně n a všechny polynomy stupně $n - 1$ mají nejvýše $n - 1$ kořenů. Pokud P nemá žádný kořen, pak už jsme vyhráli. Pokud má kořen $\alpha \in R$, pak z předchozího tvrzení platí $P(x) = (x - \alpha)Q(x)$ pro nějaký polynom Q . Stupeň P je o jedna vyšší než stupeň Q , takže Q má stupeň $n - 1$, a tudíž nejvýše $n - 1$ kořenů. Každý kořen P je buď α nebo kořen Q , takže P má nejvýše n kořenů. Navíc pokud P má přesně n různých kořenů, pak jich Q také musel mít $n - 1$ různých, takže $Q(x) = c(x - \alpha_1) \dots (x - \alpha_{n-1})$ pro nějaké c a kořeny $\alpha_1, \dots, \alpha_{n-1}$. Pojmenováním $\alpha_n = \alpha$ a přidáním činitele $(x - \alpha_n)$ pak máme součinný tvar i pro $P(x)$. $\square$

Speciálním důsledkem tvrzení je, že když má polynom kořenů více, je to už nutně nulový polynom. Díky tomu můžeme poznat, jestli jsou dva polynomy P a Q stejné: jejich rozdíl má stupeň

³Představujeme si, že součin s nula činiteli je prostě 1.

nejvýše $\max\{\deg(P), \deg(Q)\}$ a jeho kořeny jsou argumenty, pro něž se P a Q shodují. Pokud se tedy P a Q shodují v alespoň $\max\{\deg(P), \deg(Q)\} + 1$ bodech, je jejich rozdíl nulový polynom, tedy P a Q jsou tentýž polynom. Ještě speciálnější, pokud se P a Q shodují v nekonečně mnoha bodech, pak předchází argument funguje i bez toho, abychom něco věděli o jejich stupních.

Pojďme si to ukázat na příkladech z praxe:

Příklad. Nenulový polynom $P \in \mathbb{R}[x]$ stupně n nazveme *vteřinovým*, pokud má n různých reálných kořenů $r_1, \dots, r_n$, a navíc pro každé $j \in \{1, \dots, n\}$ splňuje $P(r_j + 1) = 1$. Najdi všechny vteřinové polynomy. (PraSe 39–3j–5)

Řešení. Nenulové konstantní polynomy vyhovují triviálně všechny (nemají žádné kořeny, takže podmínka „pro všechny kořeny“ automaticky platí), nadále se proto zabývejme jen nekonstantními P . Ukážeme, že mezi nimi vyhovují právě ty tvaru $P(x) = x + c$ pro $c \in \mathbb{R}$. Že všechny tyto vyhovují, je zřejmé.

Uvažujme tedy nekonstantní vteřinový polynom P stupně n a označme $Q(x) = P(x+1) - P(x)$. Tvrdíme, že $Q(x)$ má stupeň $n-1$. K tomu rozepíšeme $P(x) = \sum_{k=0}^n a_k x^k$. Roznásobením závorek $(x+1)^k$ podle binomické věty⁴ bude zápis polynomu $P(x+1)$ začínat

$$P(x+1) = a_n \underbrace{(x^n + nx^{n-1} + \dots)}_{(x+1)^n} + a_{n-1} \underbrace{(x^{n-1} + \dots)}_{(x+1)^{n-1}} + \dots,$$

přičemž pod trojtečkami se vždy skrývají členy stupně $n-2$ či nižšího. Podobně nám začíná $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots$, takže jejich odečtením získáme

$$Q(x) = (a_n - a_n)x^n + (a_n n + a_{n-1} - a_{n-1})x^{n-1} + \dots = na_n x^{n-1} + \dots$$

Jelikož a_n muselo být nenulové (protože $\deg(P) = n$), znamená to, že $\deg(Q) = n-1$.

Nyní si ale povšimneme, že podle zadané podmínky pro každé $j \in \{1, \dots, n\}$ platí

$$Q(r_j) = P(r_j + 1) - P(r_j) = 1 - 0 = 1.$$

Jinými slovy, polynom Q a konstantní polynom 1, jež mají oba stupeň nanejvýš $n-1$, se shodují v n různých bodech. To znamená, že už musí být totožné, tedy $Q(x) = 1$ je konstantní polynom.

Už zbývá jen vydedukovat, jak mohl vypadat původní P . Ze stupňů máme $n-1 = \deg(Q) = \deg(1) = 0$, takže P byl lineární. Navíc jsme při důkazu $\deg(Q) = n-1$ mimoděk odhalili, že vedoucím koeficientem Q je na_n . Vedoucím koeficient konstantního polynomu 1 je 1, takže $1 = na_n = 1 \cdot a_1$ nám prozrazuje jeden ze dvou koeficientů lineárního polynomu P . Musí tak být $P(x) = x + c$ pro nějaké $c \in \mathbb{R}$, což už jsme ověřili, že vyhovuje zadání. Našli jsme tak všechna řešení: nenulové konstanty a lineární polynomy s vedoucím koeficientem 1.

Příklad. Polynom $P \in \mathbb{R}[x]$ stupně 2024 splňuje $P(k) = \frac{1}{k}$ pro každé $k \in \{1, 2, \dots, 2025\}$. Urči $P(2026)$.

Řešení. Uvažme polynom $Q(x) = x \cdot P(x) - 1$. Má o 1 větší stupeň než P , takže $\deg(Q) = 2025$. Zároveň pro $k \in \{1, 2, \dots, 2025\}$ máme

$$Q(k) = kP(k) - 1 = k \cdot \frac{1}{k} - 1 = 0.$$

Nalezli jsme tak 2025 různých kořenů tohoto polynomu stupně 2025, musí se proto už jednat o všechny jeho kořeny. Navíc dostáváme součinný tvar

$$Q(x) = c(x-1)(x-2) \cdots (x-2025)$$

⁴Binomická věta říká $(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k$, kde $\binom{n}{k}$ jsou kombinační čísla.

pro nějaké zatím neznámé $c \in \mathbb{R}$. Toto c dopočítáme dosazením $x = 0$, dostaneme

$$Q(0) = c(-1)(-2) \cdots (-2025) = c(-1)^{2025} 2025!,$$

ale zároveň $Q(0) = 0 \cdot P(0) - 1 = -1$, z čehož už plyne $c = \frac{1}{2025!}$. Víme tedy už přesně, jak vypadá $Q(x)$. Abychom se dopídili $P(2026)$, dosadíme tento argument do Q a dopočteme

$$\begin{aligned} 2026 \cdot P(2026) - 1 &= Q(2026) = \frac{1}{2025!} (2026 - 1)(2026 - 2) \cdots (2026 - 2025) = \frac{1}{2025!} \cdot 2025! = 1, \\ P(2026) &= \frac{1+1}{2026} = \frac{1}{1013}. \end{aligned}$$

Úloha 2. Ať jsou a, b, c navzájem různá reálná čísla. Nahlédni bez roznásobování, na co se zjednoduší součet polynomů

$$\frac{(x-b)(x-c)}{(a-b)(a-c)} + \frac{(x-c)(x-a)}{(b-c)(b-a)} + \frac{(x-a)(x-b)}{(c-a)(c-b)}.$$

Úloha 3. Jsou dána navzájem různá reálná čísla a_1, a_2, a_3 a další reálné číslo c . Pokud víš, že řešeními rovnice

$$(x - a_1)(x - a_2)(x - a_3) = c$$

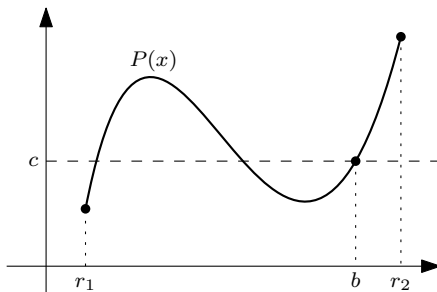
jsou tři různá $b_1, b_2, b_3 \in \mathbb{R}$, urči všechna reálná řešení rovnice

$$(x + b_1)(x + b_2)(x + b_3) = c.$$

Jeden trend, kterého si můžeš povšimnout v dosavadních tvrzeních, je to, že vždy nejprve předpokládáme, že nějaký kořen máme – obecně totiž není garantováno, že nějaký kořen existuje (to bylo k vidění ve Cvičení 1). V některých konkrétních situacích ale existenci kořenu garantovat umíme:

Cvičení 3. Každý lineární polynom nad $\mathbb{Q}$ má v $\mathbb{Q}$ kořen.

Cvičení 4. Necht má polynom $P \in \mathbb{R}[x]$ lichý stupeň. Dokaž, že potom má P kořen v $\mathbb{R}$. (Můžeš předpokládat následující: pokud čísla $r_1, r_2, c \in \mathbb{R}$ splňují $P(r_1) \leq c \leq P(r_2)$, pak existuje $b \in \mathbb{R}$ splňující $P(b) = c$.)



Úloha 4. Ať mají oba $P, Q \in \mathbb{R}[x]$ stupeň 10 a vedoucí koeficient 1. Je-li známo, že rovnice $P(x) = Q(x)$ nemá reálné řešení, dokaž, že $P(x+1) = Q(x-1)$ už reálné řešení má.

Úloha 5. Uvažujme dva kubické polynomy $F, G \in \mathbb{R}[x]$ s vedoucími koeficienty 1. Dejme tomu, že rovnice

$$F(x) = 0, \quad G(x) = 0, \quad F(x) = G(x)$$

mají dohromady 8 různých reálných řešení. Rozhodni, zda to největší a to nejmenší z nich mohou obě být řešeními $F(x) = 0$.
(PraSe 38–4p–4)

Odbočka do komplexní roviny

Nyní už dovedeme namotivovat komplexní čísla a seznámit Tě s nimi, pokud se ještě neznáte. Polynomy lichého stupně nad $\mathbb{R}$ mají vždy kořen, ty se sudým stupněm však mohou kořeny stále postrádat. Snad nejjednodušším možným příkladem je polynom $x^2 + 1$, který všude na reálné ose nabývá kladných hodnot, a proto nikde nemá kořen. Tento stav věcí matematiky raného novověku trápil natolik, až se jej rozhodli vyřešit neortodoxním způsobem – prostě si tento chybějící kořen vymysleli a začali zkoumat, k čemu dalšímu to povede.⁵ Pojďme následovat jejich cestu.

Začneme tím, že prohlásíme, že existuje jakési i (říkejme mu *imaginární jednotka*), které splňuje $i^2 = -1$. To znamená, že i bude kořenem polynomu $x^2 + 1$. *Komplexními čísly* budeme rozumět čísla tvaru $a + bi$, kde $a, b \in \mathbb{R}$, a množinu všech komplexních čísel označíme $\mathbb{C}$. Podobně jako u polynomů se domluvíme, že v zápise komplexních čísel dovolíme přirozená zjednodušení, např. tedy budeme psát i místo $0 + 1i$, 0 místo $0 + 0i$ či $1 - i$ místo $1 + (-1)i$.

Pojďme si rozmyslet, jak s komplexními čísly počítat, k tomu uvažujme $a + bi$ a $c + di$. Sčítání je snadné:

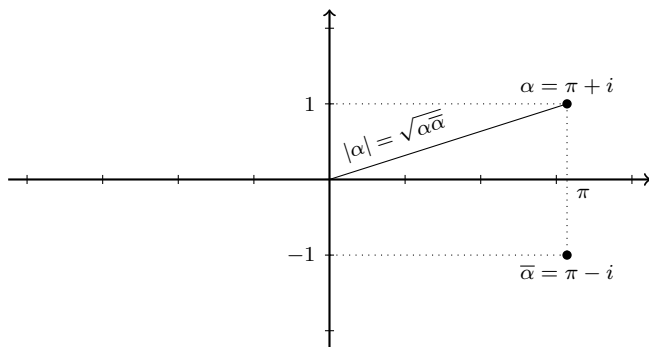
$$(a + bi) + (c + di) = (a + c) + (b + d)i,$$

podobně tak i odčítání. Při násobení dostaneme roznásobením

$$(a + bi) \cdot (c + di) = ac + adi + bci + bdi^2,$$

což s využitím $i^2 = -1$ zjednodušíme na $(ac - bd) + (ad + bc)i$, takže jde opět o komplexní číslo. Z hlediska úprav výrazů fungují tyto počty s komplexními čísly stejně jako počítání v reálných číslech – všechny obvyklé poučky jako komutativita⁶ a asociativita⁷ sčítání a násobení či roznásobování závorek zůstávají v platnosti. Teď by bylo přirozené osvětlit ještě dělení, ale to se nám prozatím vyplatí odložit a místo toho si nakreslit obrázek.

Komplexní čísla jsme zavedli jako $a + bi$ pro $a, b \in \mathbb{R}$, je tedy přirozené se na ně dívat jako na dvojice reálných čísel. Ty můžeme interpretovat jako souřadnice bodu v rovině – říkáme jí *komplexní* nebo též *Gaussova rovina*. Typicky ji kreslíme s vodorovnou, x -ovou osou reprezentující reálnou složku a svislou, y -ovou osou reprezentující imaginární složku.



Pro $\alpha = a + bi$ definujeme jeho *komplexně sdružené číslo* jako $\bar{\alpha} = a - bi$ (čti „alfa s pruhem“). V obrázku komplexní roviny to odpovídá osově souměrnosti podle reálné osy. Dále si můžeme všimnout, že

$$\alpha \cdot \bar{\alpha} = (a + bi)(a - bi) = a^2 - (bi)^2 = a^2 + b^2$$

⁵Tady velice, velice zjednodušujeme, historie je o něco složitější. Prosíme, odpusť nám to :-).

⁶„Nezávisí na pořadí.“

⁷„Nezávisí na uzavřování.“

je vždy reálné číslo. Přesněji řečeno je to dokonce druhá mocnina vzdálenosti bodu $[a, b]$ od počátku. Obvykle se proto tímto definuje absolutní hodnota komplexního čísla jako $|\alpha| = \sqrt{\alpha\bar{\alpha}} = \sqrt{a^2 + b^2}$, jež je pro každé $\alpha \neq 0$ kladná.

Cvičení 5. Ověř, že pro $\alpha, \beta \in \mathbb{C}$ platí

$$\overline{(\alpha + \beta)} = \bar{\alpha} + \bar{\beta}, \quad \overline{(\alpha \cdot \beta)} = \bar{\alpha} \cdot \bar{\beta}.$$

Z předchozího cvičení také plyne, že $|\alpha\beta| = \sqrt{(\alpha\beta)(\overline{\alpha\beta})} = \sqrt{\alpha\bar{\alpha}} \cdot \sqrt{\beta\bar{\beta}} = |\alpha| \cdot |\beta|$. To speciálně znamená, že $\alpha\beta = 0$ může nastat pouze tehdy, když $0 = |\alpha\beta| = |\alpha| \cdot |\beta|$, což je právě tehdy, když jedno z α, β má nulovou absolutní hodnotu neboli je nulou. S tímto posledním střípkem skládačky jsme tak oprávněni tvrdit, že $\mathbb{C}$ je obor – můžeme tedy nad $\mathbb{C}$ zvesela vypustit všechnu polynomiální mašinerii, kterou si vybudujeme.

Cvičení 6. Najdi všechny kořeny polynomu $x^4 + 1$ v komplexních číslech.

Cvičení 7. Rozmysli si, že v $\mathbb{C}$ dovedeme dělit libovolným nenulovým číslem pomocí rozšíření komplexně sdruženým číslem: $\frac{\alpha}{\beta} = \frac{\alpha\bar{\beta}}{\beta\bar{\beta}}$.

Zatím jsme osvětlili, jak pracovat v komplexních číslech, nemusí být ale stále jasné, proč se to vyplatí. Naše motivace započala tím, že vyrobíme kořen pro jeden konkrétní polynom. Nastává však velká magie (jejíž důkaz je bohužel nad naše možnosti) – v komplexních číslech už najednou mají kořen *všechny* (nekonstantní) polynomy. A to dokonce nejen všechny polynomy s reálnými koeficienty, ale i všechny ty, které mají komplexní koeficienty:

Věta. (základní věta algebry) Každý nekonstantní polynom $P \in \mathbb{C}[x]$ má v $\mathbb{C}$ kořen.

Se základní větou algebry v rukou už se můžeme – alespoň když pracujeme nad $\mathbb{C}$ – zbavit podmínky stylu „pokud nějaký kořen existuje ...“ a vyslovit rozklad polynomů na součinný tvar bezpodmínečně:

Důsledek. Nenulový polynom $P \in \mathbb{C}[x]$ stupně n lze zapsat ve tvaru $P(x) = c(x - \alpha_1) \cdots (x - \alpha_n)$, kde $c \in \mathbb{C}$ je vedoucí koeficient a $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ kořeny (ne nutně různé).

Důkaz postupuje prakticky stejnou indukcí jako ve verzi, kdy jsme nad obecným oborem měli existenci kořenů jako předpoklad – nebudeme jej tu proto opakovat.

Cvičení 8. Uvažujme polynom $P \in \mathbb{R}[x]$ jako polynom nad $\mathbb{C}$. Nahlédni, že pokud je $\alpha \in \mathbb{C}$ kořenem P , pak je i $\bar{\alpha}$ kořenem P .

Úloha 6. Jsou dány polynomy $F, G, H \in \mathbb{R}[x]$ splňující rovnost

$$(x^2 + x + 1)F(x) = G(x^3) + xH(x^3).$$

Dokaž, že 1 je kořenem G i H .

Věťovy vztahy

Náš dosavadní pohled na věc nabádá k tomu, že začneme s polynommem zapsaným pomocí koeficientů a chceme najít jeho kořeny. Neméně užitečná (a navíc snazší) je však cesta opačným směrem – představujeme si, že už známe kořeny, a dopočítáváme pomocí nich koeficienty. Přesně toto zařizují tzv. *Věťovy vztahy*.

Domluvmě se, že když řekneme, že polynom P má kořeny $r_1, \dots, r_n$, myslíme tím, že se faktorizuje jako $P(x) = c(x - r_1) \cdots (x - r_n)$ pro nějaké c . Pointou je, že by se nemuselo jednat o n navzájem různých kořenů, některé by se mohly opakovat – včetně těchto opakování se ale dohromady nastrádá n kořenů.

Tvrzení. (Viètovy vztahy) *Mějme polynom nad komplexními čísly $P(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$, který má kořeny $r_1, r_2, \dots, r_n$. Pak pro každé $k \in \{1, 2, \dots, n\}$ platí*

$$\sum_{1 \leq j_1 < \dots < j_k \leq n} r_{j_1} \cdot r_{j_2} \cdot \dots \cdot r_{j_k} = (-1)^k \cdot \frac{a_{n-k}}{a_n}.$$

Výraz na levé straně může vypadat děsivě, ale je to jenom sumační zápis toho, že vezmeme všechny součiny obsahující právě k různých kořenů a sečteme je. Zejména pro některé „krajní“ koeficienty vypadá výsledná formulka celkem hezky: pro $k = 1$ a $k = n$ dostaneme po řadě

$$r_1 + r_2 + \dots + r_n = -\frac{a_{n-1}}{a_n} \quad \text{a} \quad r_1 r_2 \cdot \dots \cdot r_n = (-1)^n \frac{a_0}{a_n}.$$

Další zjednodušení přichází v případě $a_n = 1$: pak je absolutní člen (až na znaménko!) součinem kořenů, zatímco druhý nejvyšší koeficient je mínus součet kořenů.

Cvičení 9.

- (i) Napiš si Viètovy vztahy pro polynom stupně 2 a pro polynom stupně 3.
- (ii) Najdi koeficienty nějakého polynomu, jehož kořeny jsou 2, 3 a 5.

Polynom ve formulaci Viètových vztahů výše jsme vzali nad komplexními čísly, protože tam máme zajištěno, že opravdu má n kořenů. Taký je ale možné postupovat obecněji:

Cvičení 10. Zformuluj Viètovy vztahy nad libovolným oborem pro polynom stupně n s kořeny $r_1, \dots, r_n$ v případě, že má vedoucí koeficient $a_n = 1$.

Pojďme si nyní ukázat, jak Viètovy vztahy použít v úlohách. Sice nám nepomohou v řešení polynomiální rovnice, často ale umožňují vyřešit úlohy týkající se kořenů, aniž bychom kořeny explicitně počítali.

Příklad. Označme α a β (komplexní) kořeny rovnice $2x^2 - 4x + 9 = 0$. Urči $\alpha^2 + \beta^2$.

Řešení. Víme, že $\alpha + \beta = -(-\frac{4}{2}) = 2$ a $\alpha\beta = \frac{9}{2}$. Nyní je naším úkolem vyrobit $\alpha^2 + \beta^2$ z $\alpha + \beta$ a $\alpha\beta$. K tomu si stačí uvědomit, že $(\alpha + \beta)^2 = \alpha^2 + 2\alpha\beta + \beta^2$, tedy

$$\alpha^2 + \beta^2 = (\alpha + \beta)^2 - 2\alpha\beta = 2^2 - 2 \cdot \frac{9}{2} = -5.$$

Na první pohled může vypadat překvapivě, že součet dvou čtverců vyšel záporně. To je ale jen tím, že α a β jsou ve skutečnosti komplexní čísla.

Příklad. Označme (komplexní) kořeny polynomu $x^3 - 3x^2 + 1$ jako α, β, γ . Najdi kubický polynom s kořeny $\alpha^2, \beta^2, \gamma^2$.

Řešení. Nejprve si shrňme Viètovy vztahy pro $x^3 - 3x^2 + 1$. Pro koeficienty u x^2 , x a 1 postupně dostáváme

$$\alpha + \beta + \gamma = -(-3) = 3, \quad \alpha\beta + \beta\gamma + \gamma\alpha = 0, \quad \alpha\beta\gamma = -1.$$

Nyní chceme pomocí těchto výrazů vyjádřit vzorečky pro $\alpha^2, \beta^2, \gamma^2$. Začneme součtem kořenů, což je až na znaménko koeficient u x^2 . Využijeme vztah $(\alpha + \beta + \gamma)^2 = \alpha^2 + \beta^2 + \gamma^2 + 2\alpha\beta + 2\beta\gamma + 2\gamma\alpha$ k vyjádření

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \beta\gamma + \gamma\alpha) = 3^2 - 2 \cdot 0 = 9.$$

Následuje koeficient u x , zde podobným využitím závorky mocněné na druhou získáme

$$\begin{aligned} \alpha^2\beta^2 + \beta^2\gamma^2 + \gamma^2\alpha^2 &= (\alpha\beta + \beta\gamma + \gamma\alpha)^2 - 2\alpha^2\beta\gamma - 2\alpha\beta^2\gamma - 2\alpha\beta\gamma^2 = \\ &= (\alpha\beta + \beta\gamma + \gamma\alpha)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma) = 0^2 - 2 \cdot (-1) \cdot 3 = 6. \end{aligned}$$

Konečně absolutní člen, který odpovídá součinu kořenů, což dá

$$\alpha^2 \beta^2 \gamma^2 = (\alpha \beta \gamma)^2 = (-1)^2 = 1.$$

Na závěr už ke spočteným výrazům musíme přidat střídající se znaménka, čímž ve výsledku dostaneme, že $\alpha^2, \beta^2, \gamma^2$ jsou kořeny polynomu $x^3 - 9x^2 + 6x - 1$.

Cvičení 11. Buď $P \in \mathbb{Q}[x]$ polynom, který má v $\mathbb{C}$ kořeny $r_1, \dots, r_n$. Pokud víš, že $r_1, \dots, r_{n-1}$ jsou ve skutečnosti racionální, nahlédni, že i r_n musí být racionální.

Úloha 7. Jsou dána komplexní čísla a, b, c, d taková, že $a + b = c + d$ a zároveň $ab = cd$. Dokaž, že $\{a, b\} = \{c, d\}$, tedy že se jedná (možná až na pořadí) o stejné dvojice.

Úloha 8. Pokud víš, že reálná čísla $a \neq b$ splňují $a^2 + 4a + 1 = b^2 + 4b + 1 = 0$, urči $\frac{a}{b} + \frac{b}{a}$.

Úloha 9. Jsou dána $a, b, c \in \mathbb{R}$ taková, že platí nerovnosti

$$a + b + c > 0, \quad ab + bc + ca > 0, \quad abc > 0.$$

Dokaž, že $a, b, c > 0$.

Úloha 10. Jsou dány kvadratické polynomy $P(x)$ a $Q(x)$ takové, že $P(Q(x))$ má čtyři různé reálné kořeny $r_1 < r_2 < r_3 < r_4$. Dokaž, že $r_1 + r_4 = r_2 + r_3$. (PraSe 43–1p–4)

Úloha 11. Jsou dána $a, b, c, d \in \mathbb{R}$, z nichž alespoň jedno je nenulové. Dokaž, že polynom $x^6 + ax^3 + bx^2 + cx + d$ nemá všechny kořeny reálné.

Úloha 12. Uvažujme celá čísla $n \geq 2$ a $p, q \geq 0$. Dokaž, že pokud existuje polynom $x^n - px^{n-1} + qx^{n-2} + a_{n-3}x^{n-3} + \dots + a_1x + a_0 \in \mathbb{C}[x]$, jehož všechny komplexní kořeny jsou nezáporná celá čísla, pak lze do roviny nakreslit p přímek protínajících se v q různých bodech.

Hledání polynomů

V olympiádě můžeš najít úlohy následujícího typu: dostaneš rovnici, v níž vystupuje nějaký neznámý polynom, případně polynomy. Tvým úkolem je pak přijít na to, které to mohou být.

Co lze s takovou úlohou dělat:

- (1) Porovnat stupně. To je poměrně jednoduché a může to možná řešení značně omezit.
- (2) Porovnat jednotlivé koeficienty. Nejsnadněji se typicky dopočítávají „krajní“ koeficienty, tzn. vedoucí, absolutní, lineární, ...
- (3) Porovnat hodnoty v určitých bodech. Často může být šikovné dosadit kořen některého polynomu, který se v úloze vyskytuje.

Kromě těchto obecných rad můžeme nabídnout už jen přání kuráže a houževnatosti – polynomiální rovnice dovedou být rozmanité a mnohdy si v nich pořádně započítáme. Ukážeme na příkladu:

Příklad. Najdi všechny dvojice nekonstantních polynomů $P, Q \in \mathbb{R}[x]$ splňující

$$P(Q(x)^3) = x \cdot P(x) \cdot Q(x)^3.$$

(PraSe 41–4p–6)

Řešení. Připomeňme, že rovnosti polynomů na levé a na pravé straně myslíme to, že mají stejné koeficienty u každé mocniny x . To ale implikuje i to, že dosazením libovolného čísla dávají stejné hodnoty, což později využijeme.

Začneme porovnáním stupňů, označme $n = \deg(P)$, $m = \deg(Q)$. Jelikož hledáme nekonstantní polynomy, půjde o kladná celá čísla. Pak na levé straně máme stupeň $n \cdot 3m$, zatímco na pravé $1 + n + 3m$. Postupně upravíme

$$3nm = n + 3m + 1,$$

$$3nm - 3m - n + 1 = 2,$$

$$(3m - 1)(n - 1) = 2.$$

Máme tedy 2 rozloženo na součin dvou (nezáporných) celých čísel, což jde jen dvěma způsoby: $1 \cdot 2$ a $2 \cdot 1$. Jelikož $3m - 1 = 1$ není možné, zbývá jenom $3m - 1 = 2$ a $n - 1 = 1$ neboli $m = 1$, $n = 2$.

Nyní víme, že Q je lineární. Jakožto reálný polynom s lichým stupněm tak má nějaký reálný kořen r . Dosazením $x = r$ do zadané rovnice získáme $P(0) = P(Q(r)^3) = r \cdot P(r) \cdot Q(r)^3 = r \cdot P(r) \cdot 0^3 = 0$, takže 0 je kořenem P .

Vytkneme činitel x odpovídající tomuto kořenu, tím dostaneme $P(x) = xR(x)$ pro nějaké $R \in \mathbb{R}[x]$. Dosazením tohoto vyjádření P pak dostaneme

$$Q(x)^3 \cdot R(Q(x)^3) = x^2 \cdot R(x) \cdot Q(x)^3.$$

Pro $a \in \mathbb{R}$ různé od r je $Q(a) \neq 0$, protože Q má jen jeden kořen, takže v těchto bodech zjednodušíme $Q(a)^3 \cdot R(Q(a)^3) = a^2 \cdot R(a) \cdot Q(a)^3$ na $R(Q(a)^3) = a^2 R(a)$. Toto má platit ve všech reálných bodech kromě jednoho, tedy v nekonečně mnoha bodech, což nám umožňuje tuto rovnost zesílit na rovnost polynomů

$$R(Q(x)^3) = x^2 \cdot R(x)$$

(jinými slovy, i když jsme nejprve museli vyloučit bod $x = r$, později ho dostaneme zpátky).

Jelikož P měl stupeň 2, R musí mít stupeň 1, takže má v $\mathbb{R}$ právě jeden kořen, označme jej s . Dosazením $x = 0$ nyní dostaneme $R(Q(0)^3) = 0$, takže $Q(0)^3 = s$. Obdobně ale taky dosazením $x = s$ dostaneme $R(Q(s)^3) = s^2 R(s) = 0$, takže i $Q(s)^3 = s$. Dohromady jsme získali $Q(0)^3 = Q(s)^3$, takže také $Q(0) = Q(s)$. Označíme-li si koeficienty Q třeba jako $Q(x) = ux + v$, kde $u \neq 0$, pak už snadno vidíme, že z $u \cdot 0 + v = us + v$ plyne $0 = s$.

Odhalili jsme tedy, že kořenem R je opět 0, takže máme $R(x) = cx$ pro nějaké $0 \neq c \in \mathbb{R}$, a tedy $P(x) = cx^2$. Navíc jsme měli $Q(0)^3 = s = 0$, tedy $Q(0) = 0$. Jelikož Q bylo taktéž lineární, zbavíme se absolutního členu, čímž zbude $Q(x) = ux$. Dosazením do $R(Q(x)^3) = x^2 R(x)$ dostaneme $c(ux)^3 = x^2 \cdot cx$, z čehož porovnáním koeficientů dostaneme $cu^3 = c$, tedy $u^3 = 1$, tedy $u = 1$.

Dokázali jsme tak, že všechna řešení musí být tvaru $(P, Q) = (cx^2, x)$ pro $0 \neq c \in \mathbb{R}$. Zkouškou už ověříme, že všechny dvojice tohoto tvaru vyhovují původní rovnici:

$$P(Q(x)^3) = c(x^3)^2 = cx^6 = x \cdot cx^2 \cdot x^3 = x \cdot P(x) \cdot Q(x)^3.$$

Prochroustal(a) ses úspěšně řešením? Dobrá práce, na dalších úlohách se můžeš procvičit:

Úloha 13. Najdi všechny nenulové polynomy $P \in \mathbb{R}[x]$, jež splňují $P(x^2) = x^2(x^2 + 1)P(x)$.

Úloha 14. Najdi všechny polynomy $P \in \mathbb{R}[x]$ splňující $xP(x - 1) = (x + 1)P(x)$.
(PraSe 34-2j-3)

Úloha 15. Najdi všechny polynomy $P \in \mathbb{R}[x]$, které splňují $P(0) = 0$ a zároveň $P(x^2 + 1) = P(x)^2 + 1$.

Úloha 16. (těžká) Jsou dány polynomy $P, Q \in \mathbb{R}[x]$, jež splňují $P(Q(x)^2 + x + 1) = Q(P(x)^2 + x + 1)$. Navíc je známo, že P má nějaký reálný kořen a Q má nějaký reálný kořen. Dokaž, že potom už $P = Q$.

Závěr

Vítej na konci prvního dílu, jsme rádi, že ses dočetl(a) až sem. Ptáš se, co očekávat v díle druhém? Namísto reálné přímky či komplexní roviny zabrousíme do světa celých čísel a prozkoumáme zákoutí, kde se polynomy potkávají s teorií čísel – těšit se můžeš například na poučku „rozdíl argumentů dělí rozdíl hodnot“ či na větu o racionálním kořenu.

Přejeme hodně úspěchu při řešení úloh 1. seriálové série a těšíme se na zdárnou shledanou u druhého dílu!

Návody ke cvičením

- Členy nejvyššího stupně se musí navzájem vyrušit.
- Umíme dělit.
- Dokaž, že pro dost velká kladná r je $P(r)$ kladné a pro dost malá záporná r je $P(r)$ záporné... anebo naopak.
- $P(\bar{\alpha}) = \overline{P(\alpha)}$.
- Pokud $a_n = 1$, skoro nic nezmění. Jen chceme, aby sis rozmyslel(a), že kromě záruky existence kořenů jsme nepoužili nic specifického pro $\mathbb{C}$:-).
- Součet kořenů je...?

Návody k úlohám

- Obrát pořadí koeficientů.
- Dosaď postupně $x = a, b, c$.
- $(x - a_1)(x - a_2)(x - a_3) - c = (x - b_1)(x - b_2)(x - b_3)$.
- Co se v rozdílech děje s členem stupně 9?
- Nemůže – zkoumej, kde polynomy F , G a $F - G$ nabývají kladných a záporných hodnot.
- Dosazuj komplexní kořeny polynomu $x^2 + x + 1$.
- Kořeny kvadratického polynomu.
- Viètovy vztahy pro polynom $x^4 + 4x + 1$.
- $(x + a)(x + b)(x + c)$.
- Dívej se na Viètovy vztahy polynomů $Q(x) - s$, kde s je kořen P .
- Předpokládej, že všech šest kořenů $r_1, \dots, r_6$ je reálných, a vyjádři $r_1^2 + \dots + r_6^2$.
- Interpretuj kořeny jako skupinky rovnoběžek.
- Stupeň určíš snadno. Potom hledej kořeny P dosazováním takových argumentů, aby se pravá strana vynulovala.
- Polynom $(x + 1)P(x)$ má vždy stejné hodnoty v $r - 1$ a r .
- Induktivně najdi nekonečně mnoho přirozených m , pro něž $P(m) = m$.
- Nejprve najdi bod, kde se P a Q shodují. Potom vyráběj další a další.

Řešení cvičení

- Příkladů je mnoho, my jsme si vybrali následující: (i) $2x - 1$, (ii) $x^2 - 2$, (iii) $x^2 - 2$, (iv) $x^2 + 1$.
- Funguje např. $P(x) = x + 1$ a $Q(x) = -x$, neboť pak $P(x) + Q(x) = 1$.
- Označíme-li si polynom $ax + b$, kde $a \neq 0$, pak je $-\frac{b}{a} \in \mathbb{Q}$ kořenem.
- Rozepišme $P(x) = \sum_{k=0}^n a_k x^k$, přičemž $a_n \neq 0$ a n je liché. BÚNO nechtě $a_n > 0$. Nejprve si rozmyslíme, že pro nějaké dost velké r je $P(r)$ kladné, jelikož člen $a_n r^n$ „přebije“ všechny ostatní. To je intuitivně celkem zjevné, ale abychom to dokázali pořádně, budeme si muset vyhrnout rukávy – pokud by Ti následující odstavec dělal potíže, klidně se jen intuitivně smíř s tím, že člen většího stupně přebije ty menší, a pokračuj dál :-).

Postupujme třeba následovně: nejprve označme $A = \max \left\{ \frac{|a_0|}{a_n}, \frac{|a_1|}{a_n}, \dots, \frac{|a_{n-1}|}{a_n} \right\} + 1$. Potom zvolme $r = \max\{1, n \cdot A\}$. Tím následně dovedeme pro každé $k \in \{0, 1, \dots, n-1\}$ odhadnout $|a_k r^k| < \frac{1}{n} a_n r^n$: pokud $a_k = 0$, pak to platí triviálně, a pokud $a_k \neq 0$, tak dostaneme

$$|a_k r^k| = |a_k| r^k \leq |a_k| r^{n-1} \leq r^n \cdot \frac{|a_k|}{nA} < r^n \cdot \frac{|a_k|}{n \cdot \frac{|a_k|}{a_n}} = \frac{1}{n} a_n r^n.$$

Sečtením tohoto odhadu přes nultý, první, $\dots$, $(n-1)$ -tý člen v $P(r)$ a aplikováním trojúhelníkové nerovnosti pak získáme, že vedoucí člen v absolutní hodnotě skutečně přebíjí všechny ostatní dohromady, neboť

$$\left| \sum_{k=0}^{n-1} a_k r^k \right| \leq \sum_{k=0}^{n-1} |a_k r^k| < n \cdot \frac{1}{n} a_n r^n = a_n r^n.$$

Tudíž v tom nejnešťastnějším možném případě, kdy by všechny nižší členy přispívali do $P(r)$ zápornými příspěvky, dostaneme

$$P(r) = a_n r^n + \sum_{k=0}^{n-1} a_k r^k \geq a_n r^n - \left| \sum_{k=0}^{n-1} a_k r^k \right| > a_n r^n - a_n r^n = 0,$$

takže $P(r)$ je kladné.

Díky tomu, že n je liché, bude obdobně $a_n(-r)^n$ natolik malé (daleko v záporném směru na číselné ose), že ostatní členy jej nedokážou přebít, takže $P(-r)$ bude záporné. Víme tedy, že P někde nabývá záporné a někde jinde kladné hodnoty. Jelikož je to reálný polynom, musí někde mezi nabývat i nuly, a tento bod je potom naším hledaným kořenem.

5. Označme $\alpha = a + bi$ a $\beta = c + di$, pak přímočaře ověříme:

$$\begin{aligned} \overline{(\alpha + \beta)} &= \overline{(a + c) + (b + d)i} = (a + c) - (b + d)i = (a - bi) + (c - di) = \bar{\alpha} + \bar{\beta}, \\ \overline{(\alpha \cdot \beta)} &= \overline{(ac - bd) + (ad + bc)i} = (ac - bd) - (ad + bc)i = (a - bi)(c - di) = \bar{\alpha} \cdot \bar{\beta}. \end{aligned}$$

6. Jsou to všechny čtyři kombinace znamének v $\pm \frac{1}{\sqrt{2}} \pm \frac{1}{\sqrt{2}}i$.

7. Je to skutečně tak, nekecali jsme. Jelikož předpokládáme $\beta \neq 0$, je $\beta\bar{\beta} = |\beta|^2$ kladné reálné číslo. Stačí tedy spočítat součin $\alpha\bar{\beta}$ a poté obě složky podělit tímto reálným číslem $|\beta|^2$.

8. Ať $P(x) = \sum_{k=0}^n c_k x^k$. Jelikož $c_k \in \mathbb{R}$, platí $c_k = \overline{c_k}$, takže dostaneme

$$P(\bar{\alpha}) = \sum_{k=0}^n c_k (\bar{\alpha})^k = \sum_{k=0}^n \overline{(c_k \alpha^k)} = \overline{\left(\sum_{k=0}^n c_k \alpha^k \right)} = \overline{P(\alpha)} = \bar{0} = 0.$$

9. (i) Pro kvadratický polynom $P(x) = a_2 x^2 + a_1 x + a_0$ s kořeny r_1, r_2 dostaneme

$$r_1 + r_2 = -\frac{a_1}{a_2} \quad \text{a} \quad r_1 r_2 = \frac{a_0}{a_2}.$$

Pro kubický $P(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$ s kořeny r_1, r_2, r_3 to pak bude

$$r_1 + r_2 + r_3 = -\frac{a_2}{a_3}, \quad r_1 r_2 + r_2 r_3 + r_3 r_1 = \frac{a_1}{a_3}, \quad \text{a} \quad r_1 r_2 r_3 = -\frac{a_0}{a_3}.$$

(ii) Kýžené kořeny si můžeme zařídit třeba tím, že si polynom zvolíme v součinném tvaru jako $(x-2)(x-3)(x-5)$. Roznásobením závorek, což odpovídá počítání Viětových vztahů, pak získáme

$$x^3 - (2+3+5)x^2 + (2 \cdot 3 + 3 \cdot 5 + 5 \cdot 2)x - 2 \cdot 3 \cdot 5 = x^3 - 10x^2 + 31x - 30.$$

10. Můžeme zformulovat třeba takto: Ať je $P(x) = x^n + \sum_{j=0}^{n-1} a_j x^j$ polynom nad oborem R a nechť má v R kořeny $r_1, \dots, r_n$. Potom pro každé $k \in \{1, 2, \dots, n\}$ platí

$$\sum_{1 \leq j_1 < \dots < j_k \leq n} r_{j_1} \cdots r_{j_k} = (-1)^k a_{n-k}.$$

11. Označme $P(x) = \sum_{k=0}^n a_k x^k$, kde jednotlivá a_k jsou racionální. Z Viětova vztahu pro a_{n-1} máme $r_1 + \dots + r_{n-1} + r_n = -\frac{a_{n-1}}{a_n}$, což upravíme na $r_n = -\left(r_1 + \dots + r_{n-1} + \frac{a_{n-1}}{a_n}\right)$. V tomto výrazu jsou na pravé straně samá racionální čísla, takže i r_n je racionální.

Řešení úloh

1. BÚNO⁸ předpokládáme $a_n \neq 0$. Stejně tak předpokládáme $a_0 \neq 0$, v opačném případě bychom vytknuli x a vzali za P polynom s menším stupněm.

Pak označme $Q(x) = a_0x^n + a_1x^{n-1} + \dots + a_{n-1}x + a_n \in \mathbb{Q}[x]$ polynom, který z P vznikne obrácením pořadí koeficientů. Pro $0 \neq t \in \mathbb{R}$ pak platí $Q(t) = t^n P(\frac{1}{t})$. Speciálně tedy pro $t = \frac{1}{r}$ dostaneme $Q(\frac{1}{r}) = \frac{1}{r^n} P(r) = \frac{0}{r^n} = 0$, takže $\frac{1}{r}$ je kořenem Q .

2. Označme zadaný součet jako polynom $P(x)$. Každý ze tří sčítanců má stupeň 2, takže také $\deg(P) \leq 2$. Dosazením $x = a$ dostaneme v prvním sčítanci $\frac{(a-b)(a-c)}{(a-b)(a-c)} = 1$, zatímco v každém ze zbylých dvou sčítanců objevíme nulovou závorku $(a-a)$. Celkem tedy $P(a) = 1$ a obdobně máme též $P(b) = P(c) = 1$. Polynomy P a 1 (konstantní polynom), oba stupně nanejvýš 2, se tak shodují ve 2 + 1 různých bodech, takže už se musí rovnat. Zjednodušíme tedy $P(x) = 1$.

3. Známe kořeny polynomu $(x-a_1)(x-a_2)(x-a_3) - c$, takže jej můžeme vyjádřit součinem jako $(x-b_1)(x-b_2)(x-b_3)$. Přesunutím c pak hned máme, že kořeny $(x-b_1)(x-b_2)(x-b_3) + c$ jsou a_1, a_2, a_3 . Naše původní tři čísla jsou tak řešeními $(x-b_1)(x-b_2)(x-b_3) = -c$. Dosazením $-x$ místo x a přenásobením rovnice mínus jedničkou pak získáme přesně rovnici $(x+b_1)(x+b_2)(x+b_3) = c$, jejímiž řešeními tak jsou $-a_1, -a_2, -a_3$.

4. Podmínka o (ne)řešitelnosti rovnic nám říká, že $P(x) - Q(x)$ nemá reálný kořen. Polynom nad $\mathbb{R}$ může nemít kořen jen tehdy, když má sudý stupeň. Pokud $P(x) = x^{10} + a_9x^9 + \dots + a_1x + a_0$ a $Q(x) = x^{10} + b_9x^9 + \dots + b_1x + b_0$, pak nám toto speciálně říká, že v rozdílu

$$P(x) - Q(x) = (a_9 - b_9)x^9 + \dots$$

musel zmizet člen stupně 9, takže $a_9 = b_9$. Teď už stačí jen vyvodit, že v $P(x+1) - Q(x-1)$ už člen stupně 9 nezmizí. K tomu spočítáme

$$\begin{aligned} P(x+1) - Q(x-1) &= \left((x^{10} + 10x^9 + \dots) + a_9(x^9 + \dots) + \dots \right) - \\ &\quad - \left((x^{10} - 10x^9 + \dots) + b_9(x^9 - \dots) + \dots \right) = \\ &= \left((10 + a_9) - (-10 + b_9) \right) x^9 + \dots = 20x^9 + \dots \end{aligned}$$

protože $a_9 - b_9 = 0$. Díky lichému stupni tak $P(x+1) - Q(x-1)$ má reálný kořen, tedy $P(x+1) = Q(x-1)$ má řešení.

5. Řešení $F(x) = G(x)$ jsou přesně kořeny polynomu $F - G$. Všimněme si, díky shodným vedoucím koeficientům se kubické členy v $F - G$ vyruší, takže půjde nanejvýš o kvadratický polynom. Dohromady nám naše tři rovnice tedy nemohou dát více než $3 + 3 + 2 = 8$ různých řešení. To, že máme všech osm, znamená, že už se dohromady jedná o všechny kořeny těchto polynomů a také že $F - G$ má skutečně stupeň 2 (a nikoliv nižší).

Ať je a ten nejmenší a b ten největší z kořenů. Pro spor předpokládejme, že jsou to oba kořeny F . Jelikož má G vedoucí koeficient 1, nabývá dostatečně daleko vlevo na číselné ose (v záporných číslech) záporné hodnoty. Zároveň na intervalu $(-\infty, a)$ nemůže měnit znaménko, protože všechny kořeny G jsou větší než a . To znamená, že $G(a) < 0$, takže $(F-G)(a) = F(a) - G(a) = -G(a) > 0$. Taktéž $F - G$ nemůže na intervalu $(-\infty, a)$ měnit znaménko, takže také všude dostatečně daleko vlevo na číselné ose nabývá kladných hodnot. Protože je $F - G$ kvadratický polynom (má sudý stupeň), znamená to, že jeho vedoucí koeficient je kladný.

Analogickou argumentací na druhé straně číselné osy zjistíme, že $G(b) > 0$, takže $(F-G)(b) < 0$, což ale implikuje, že $F - G$ má záporný vedoucí koeficient. To je spor, takže a i b nemohly být současně kořeny F .

⁸Zkratka pro „bez újmy na obecnosti“. Myslí se tím, že činíme nějaké zjednodušení nebo volbu, která nic podstatného nezmění.

6. Uvažujme komplexní kořeny polynomu $x^2 + x + 1$: dosazením snadno ověříme, že to jsou $\alpha_1 = \frac{-1+i\sqrt{3}}{2}$ a $\alpha_2 = \frac{-1-i\sqrt{3}}{2}$. Navíc to pak musí být rovnou i kořeny $(x-1)(x^2+x+1) = x^3-1$, takže $\alpha_1^3 = 1 = \alpha_2^3$. Jejich dosazením do zadané rovnosti tak pro $j \in \{1, 2\}$ dostaneme $0 = G(1) + \alpha_j H(1)$. Na to se můžeme dívat jako na soustavu dvou rovnic s neznámými $G(1)$ a $H(1)$. Odečtením rovnic od sebe dostaneme $0 = (\alpha_1 - \alpha_2)H(1) = i\sqrt{3} \cdot H(1)$, takže $H(1) = 0$. Z toho už pak snadno vyplývá $G(1) = 0$.

7. Uvažme $P(x) = (x-a)(x-b)$, $Q(x) = (x-c)(x-d)$. Použitím Viětových vztahů zjistíme, že P a Q mají totožný lineární koeficient $-(a+b) = -(c+d)$ i totožný absolutní člen $ab = cd$, takže už $P(x) = Q(x)$. Musí tedy mít i stejnou sadu kořenů $\{a, b\} = \{c, d\}$.

8. Chceme výraz $\frac{a}{b} + \frac{b}{a}$ vztáhnout k viětovským výrazům ab a $a+b$, čehož docílíme třeba pomocí

$$\frac{a}{b} + \frac{b}{a} = \frac{a^2 + b^2}{ab} = \frac{(a+b)^2 - 2ab}{ab} = \frac{(a+b)^2}{ab} - 2.$$

Dosazením $a+b = -4$, $ab = 1$ tak získáme $\frac{(-4)^2}{1} - 2 = 14$.

9. Uvažme polynom $P(x) = (x+a)(x+b)(x+c)$. Podle Viětových vztahů (anebo prostě násobením závorek) obdržíme $P(x) = x^3 + (a+b+c)x^2 + (ab+bc+ca)x + abc$. Jedná se tedy o polynom se samými kladnými koeficienty, speciálně tak dosazením jakéhokoliv $r \geq 0$ dostaneme $P(r) > 0$. Přitom ale z definice vidíme, že P má kořeny $-a, -b, -c$. Ty tak musí být záporné, což už je ekvivalentní $a, b, c > 0$.

10. Všimneme si, že P má reálný kořen $s_1 = Q(r_1)$. Rozkládá se potom tedy na $P(x) = (x-s_1) \cdot (ux+v)$ pro nějaký lineární polynom $ux+v$. Z toho pak plyne, že má P i druhý reálný kořen $s_2 = -\frac{v}{u}$. Nyní můžeme změnit úhel pohledu a na kořeny $P(Q(x))$ se dívat jako na kořeny jednoho z polynomů $Q(x) - s_1$ a $Q(x) - s_2$, načež víme, že r_1, r_2, r_3, r_4 se mezi tyto dva polynomy nějakým způsobem rozdělí do dvou dvojic.

Jelikož však $Q(x) - s_1$ a $Q(x) - s_2$ mají stejný koeficient u x (liší se totiž jen o konstantu), znamená to, že tyto dvě dvojčky kořenů dají stejný součet. To už ale vzhledem k seřazení $r_1 < r_2 < r_3 < r_4$ jde jenom tehdy, když se spáruje nejmenší s největším a poté dva prostřední spolu, tedy $r_1 + r_4 = r_2 + r_3$.

11. Ať jsou kořeny polynomu $r_1, \dots, r_6$. Koeficienty u x^5 a x^4 jsou nulové, což znamená

$$\sum_{k=1}^6 r_k = 0 = \sum_{1 \leq j < k \leq 6} r_j r_k.$$

Díky tomu dovedeme vyjádřit

$$\sum_{k=1}^6 r_k^2 = \left(\sum_{k=1}^6 r_k \right)^2 - 2 \left(\sum_{1 \leq j < k \leq 6} r_j r_k \right) = 0^2 - 2 \cdot 0 = 0.$$

Nyní pro spor předpokládejme, že všechny $r_1, \dots, r_6$ jsou reálné. Pak máme součet čtverců několika reálných čísel nulový, což mohlo nastat jen tehdy, pokud jsou všechny nulové, tedy $r_1 = \dots = r_6 = 0$. Pak je ale celý polynom roven x^6 , což je spor s předpokladem, že alespoň jedno z a, b, c, d je nenulové.

12. Označme si kořeny $r_1, \dots, r_n$. Vyberme si v rovině n navzájem nerovnoběžných přímk a přidejme ke každé nějaké její rovnoběžky tak, abychom nakonec v k -tém směru měli r_k rovnoběžek. Provedme to navíc tak, aby se žádné tři z vybraných přímk neprotly v jednom bodě – kdyby se to stalo, prostě vezmeme jednu z inkriminovaných přímek a nahradíme ji za jinou rovnoběžku.

Přímek je nyní dohromady $\sum_{k=1}^n r_k$, což je podle Viětových vztahů $-(-p) = p$. Průsečky pak odpovídají dvojicím přímek z rozdílných skupinek, takže jejich celkový počet získáme posčítáním všech součinů různých r_k , což podle Viětových vztahů dá přesně q .

13. Označme $n = \deg(P)$, potom na levé straně máme stupeň $2n$ a na pravé $2 + 2 + n$, z čehož vyvodíme $n = 4$. Nyní zkusíme dosazovat: $x = 0$ vynuluje pravou stranu, takže $P(0^2) = 0$. Dále budeme chtít za x dosazovat i komplexní hodnoty – to můžeme z toho důvodu, že i kdybychom věděli jen to, že $P(x^2) = x^2(x^2 + 1)P(x)$ platí ve všech reálných bodech x , stále to znamená, že polynomy na levé a na pravé straně uvažované nad $\mathbb{C}$ mají nekonečně mnoho bodů, kde se shodují, takže už to musí být stejné polynomy i nad $\mathbb{C}$. Můžeme tedy dosadit třeba $x = i$, čímž bude na pravé straně $i^2 + 1 = 0$, takže v důsledku $P(i^2) = 0$. Dohromady jsme tak odhalili, že P má kořeny 0 a -1 , takže $P(x) = x(x+1)Q(x)$ pro nějaký $Q \in \mathbb{R}[x]$.

S tímto vyjádřením v rovnici dostaneme $x^2(x^2+1)Q(x^2) = x^2(x^2+1)x(x+1)Q(x)$. Pro všechna nenulová $a \in \mathbb{R}$ je $a^2(a^2+1) \neq 0$, takže v těchto bodech dostaneme

$$a^2(a^2+1)Q(a^2) = a^2(a^2+1)a(a+1)Q(a) \implies Q(a^2) = a(a+1)Q(a).$$

Vzhledem k tomu, že to je rovnost v nekonečně mnoha bodech, dostáváme $Q(x^2) = x(x+1)Q(x)$.

Nyní provedeme něco podobného ještě jednou: dosadíme $x = 0$ a $x = -1$, abychom vynulovali pravou stranu, čímž zjistíme, že 0^2 a $(-1)^2 = 1$ jsou kořeny Q . Vzhledem k $\deg(Q) = \deg(P) - 2 = 2$ pak už musí být $Q(x) = cx(x-1)$ pro nějaké $0 \neq c \in \mathbb{R}$, takže $P(x) = cx(x+1)x(x-1) = cx^2(x^2-1)$. Zkouškou snadno ověříme, že všechny polynomy tohoto tvaru jsou řešeními.

14. $P(x) = 0$ zjevně funguje. Ukážeme, že žádné nenulové polynomy už nevyhovují. Označme $Q(x) = (x+1)P(x)$. Zadáni nám říká $Q(x-1) = Q(x)$, takže pokud označíme třeba $c = Q(0)$, polynom Q nabývá této hodnoty v nekonečně mnoha bodech

$$c = Q(0) = Q(1) = Q(2) = \dots$$

To už znamená, že $Q(x)$ a konstantní polynom c jsou totožné. To je ale možné jen pro $P = 0$, protože jinak by mělo Q stupeň $\deg(P) + 1 \geq 1$, což pro konstantu není možné.

15. Tvrdíme, že vyhovuje pouze $P(x) = x$. Že toto skutečně vyhovuje, je zjevné.

Nyní ať P splňuje podmínky zadání. Definujme posloupnost $a_0, a_1, \dots$ pomocí $a_0 = 0$ a rekurence $a_{n+1} = a_n^2 + 1$. Snadno pozorujeme, že to je rostoucí posloupnost. Indukcí dokážeme, že každý člen splňuje $P(a_n) = a_n$. Pro $n = 0$ to platí hned ze zadání, protože $P(0) = 0$. Dále dokážeme indukční krok: pokud $P(a_n) = a_n$, pak už taky

$$P(a_{n+1}) = P(a_n^2 + 1) = P(a_n)^2 + 1 = a_n^2 + 1 = a_{n+1}.$$

Důkaz indukci je tím hotov. Díky němu máme nekonečně mnoho různých $m \in \mathbb{R}$ splňujících $P(m) = m$. Polynom $P(x)$ a x se tak shodují v nekonečně mnoha bodech, takže musí být totožné.

16. Nejprve dokážeme, že v nějakém bodě a nastane $P(a) = Q(a)$. Máme zadáno, že P i Q mají nějaký reálný kořen, ať tedy $P(u) = 0$ a $Q(v) = 0$ pro nějaká $u, v \in \mathbb{R}$. Uvažujme polynom $R(x) = P(x)^2 - Q(x)^2$. V bodě $x = v$ má hodnotu $R(v) = P(v)^2 \geq 0$, takže R někde nabývá nezáporné hodnoty. Podobně v bodě $x = u$ dostaneme $R(u) = -Q(u)^2 \leq 0$, takže R někde nabývá taky nekladné hodnoty. „Někde mezi“ (viz Cvičení 4) už proto musí nabývat nulové hodnoty, tedy R má reálný kořen, nazvěme ho r . V něm platí $P(r)^2 = Q(r)^2$, takže když označíme $a = P(r)^2 + r + 1 = Q(r)^2 + r + 1$, dostaneme dosazením $x = r$ v zadané rovnosti, že $P(a) = Q(a)$.

Našli jsme tak jedno reálné a splňující $P(a) = Q(a)$. Teď ukážeme, že jich dokonce musí být nekonečně mnoho. Pro spor tedy předpokládejme, že jich je jen konečně mnoho. Potom si můžeme vybrat to největší z nich a označit si $b = P(a) = Q(a)$. Dosazením $x = a$ v zadané rovnici pak zjistíme, že P a Q se shodují též v $b^2 + a + 1$. Přitom ale $b^2 + a + 1 \geq a + 1 > a$, což je spor s tím, že a bylo největší číslo, kde se P a Q shodují. Takových bodů proto muselo existovat nekonečně mnoho, a tudíž $P = Q$.