

# Kořeny polynomů

Ondřej Klíma

Kořeny polynomů – p.1/25

## Hodnota polynomu v prvku

Kořen polynomu  $f$  je takový prvek  $c$ , pro nějž  $f(c) = 0$ .  
Co je  $f(c)$ ? Intuitivně: „dosazení“  $c$  do polynomu  $f$ .

Definice:

Nechť  $(R, +, \cdot)$  je okruh,

$$f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$$

polynom z  $R[x]$  a  $c \in R$ . Pak prvek

$$a_n c^n + a_{n-1} c^{n-1} + \dots + a_1 c + a_0 \in R$$

označujeme symbolem  $f(c)$  a nazýváme

**hodnota polynomu  $f$  v prvku  $c$ .**

Kořeny polynomů – p.2/25

## Věta.

Je-li  $(R, +, \cdot)$  komutativní okruh, pak pro libovolné dva polynomy  $f, g \in R[x]$  a pro libovolný prvek  $c \in R$  platí

$$(f + g)(c) = f(c) + g(c) \quad \text{a} \quad (f \cdot g)(c) = f(c) \cdot g(c).$$

Důkaz — první vztah:

$$f = a_k x^k + a_{k-1} x^{k-1} + \dots + a_1 x + a_0$$

$$g = b_n x^n + b_{n-1} x^{n-1} + \dots + b_1 x + b_0 \quad (\text{Búno: } k = n)$$

$$f + g = (a_n + b_n)x^n + \dots + (a_2 + b_2)x^2 + (a_1 + b_1)x + (a_0 + b_0)$$

$$(f + g)(c) = (a_n + b_n)c^n + \dots + (a_2 + b_2)c^2 + (a_1 + b_1)c + (a_0 + b_0)$$

$$f(c) = a_n c^n + a_{n-1} c^{n-1} + \dots + a_1 c + a_0$$

$$g(c) = b_n c^n + b_{n-1} c^{n-1} + \dots + b_1 c + b_0$$

Kořeny polynomů – p.3/25

## Vlastnost „dosazení“ pro součin

$$\text{„}(f \cdot g)(c) = f(c) \cdot g(c)\text{“}$$

**Př:**  $f = a_2 x^2 + a_1 x + a_0, \quad g = b_1 x + b_0.$

$$f \cdot g = a_2 b_1 x^3 + (a_2 b_0 + a_1 b_1) x^2 + (a_1 b_0 + a_0 b_1) x + a_0 b_0$$

$$(f \cdot g)(c) = a_2 b_1 c^3 + (a_2 b_0 + a_1 b_1) c^2 + (a_1 b_0 + a_0 b_1) c + a_0 b_0$$

$$f(c) = a_2 c^2 + a_1 c + a_0, \quad g(c) = b_1 c + b_0$$

$$f(c) \cdot g(c) = a_2 c^2 b_1 c + a_2 c^2 b_0 + a_1 c b_1 c + a_1 c b_0 + a_0 b_1 c + a_0 b_0$$

**Potřebujeme:**  $cb_0 = b_0 c, \quad cb_1 = b_1 c, \dots$

Kořeny polynomů – p.4/25

Nechť  $(R, +, \cdot)$  je komutativní okruh a  $c$  jeho prvek.  
 Zobrazení  $\text{hod}_c : R[x] \rightarrow R$  dané vztahem  $\text{hod}_c(f) = f(c)$  je homomorfismus okruhů.

Plyne z věty a rovnosti  $a(c) = a$  pro konstantní polynom  $a$ .

Co nás více zajímá — polynom jako funkce.

Tj. pro daný polynom  $f$  máme zobrazení  $\phi_f : R \rightarrow R$  dané vztahem  $\phi_f(c) = f(c)$ . (tzv. polynomická funkce)

Pozor:

toto zobrazení  $\phi_f$  zpravidla není homomorfismus okruhů.  
 Neplatí vztahy  $f(a + b) = f(a) + f(b)$ ,  $f(a \cdot b) = f(a) \cdot f(b)$ .

## Hornerovo schéma

Jak efektivně počítat  $f(c)$ ?

$$f(c) = a_n c^n + a_{n-1} c^{n-1} + \dots + a_1 c + a_0$$

$$= ((\dots((a_n \cdot c + a_{n-1}) \cdot c + a_{n-2}) \cdot c \dots + a_2) \cdot c + a_1) \cdot c + a_0$$

Příklad:

$$f = 2x^6 + 5x^5 - 2x^4 - 7x^2 + 5x - 3, \quad c = -3$$

	2	5	-2	0	-7	5	-3	
-3	2	-1	1	-3	2	-1	0	$\implies f(-3) = 0$

$$-1 = a_n \cdot c + a_{n-1}$$

$$1 = (a_n \cdot c + a_{n-1}) \cdot c + a_{n-2}$$

**Kořen** polynomu  $f \in R[x]$  je takový prvek  $c \in R$ , pro nějž  $f(c) = 0$ .

**Věta.**

Nechť  $(R, +, \cdot)$  je těleso a nechť  $f \in R[x]$  je polynom. Pak prvek  $c \in R$  je kořenem polynomu  $f$  právě tehdy, když  $(x - c) \mid f$ .

**Důkaz:** (Projde pro komutativní okruh  $R$ .)

- Pokud  $(x - c) \mid f$ , pak  $f = (x - c) \cdot g$  a  $f(c) = 0 \cdot g(c) = 0$ .
- Buď  $c$  kořen, pak dělíme se zbytkem:  $f = (x - c) \cdot q + r$ , kde  $r$  je polynom menšího stupně než  $\text{st}(x - c) = 1$ , tzn. polynom  $r$  je konstantní. Odtud  $0 = f(c) = (c - c) \cdot q(c) + r(c) = 0 + r = r$ .

V obou částech používáme předchozí větu.

## Dělení polynomem $x - c$

Dosazení  $c$  do  $f = (x - c) \cdot q + r$  dává  $f(c) = r$ .

Nechť tedy  $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ ,

$q = b_{n-1} x^{n-1} + \dots + b_1 x + b_0$ .

Porovnejme koeficienty v  $f = (x - c) \cdot q + r$ . Dostaneme:

$x^n$	$a_n = b_{n-1}$	$b_{n-1} = a_n$
$x^{n-1}$	$a_{n-1} = b_{n-2} - b_{n-1}c$	$b_{n-2} = b_{n-1}c + a_{n-1}$
$\dots$	$\dots$	$\dots$
$x^i$	$a_i = b_{i-1} - b_i \cdot c$	$b_{i-1} = b_i \cdot c + a_i$
$\dots$	$\dots$	$\dots$
$x$	$a_1 = b_0 - b_1 c$	$b_0 = b_1 c + a_0$
	$a_0 = r - b_0 c$	$r = b_0 c + a_0$

	$a_n$	$a_{n-1}$	$\dots$	$\dots$	$a_i$	$\dots$	$\dots$	$a_1$	$a_0$
$c$	$b_{n-1}$	$b_{n-2}$	$\dots$	$b_i$	$b_{i-1}$	$\dots$	$b_1$	$b_0$	$r$

	1	1	1	1	1
2	1	3	7	15	31

$$x^4 + x^3 + x^2 + x + 1 = (x - 2)(x^3 + 3x^2 + 7x + 15) + 31$$

Postup lze opakovat a dostat Taylorův rozvoj.

	1	2	3	4	5
-1	1	1	2	2	3
-1	1	0	2	0	
-1	1	-1	3		
-1	1	-2			
-1	1				

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

## Násobnost kořene

Nechť  $(R, +, \cdot)$  je těleso,  $f \in R[x]$  nenulový polynom a  $c \in R$  kořen  $f$ . Přirozené číslo  $k$  se nazývá **násobnost** kořene  $c$ , jestliže  $(x - c)^k \mid f$  a  $(x - c)^{k+1} \nmid f$ .

Poznámky:

- Pokud  $(x - c)^k \mid f$ , pak máme  $k = \text{st}((x - c)^k) \leq \text{st}(f)$ . Je tedy definice korektní.
- Kořeny násobnosti 1 se nazývají **jednoduché**.

## Věta.

Nechť  $(R, +, \cdot)$  je těleso. Pak nenulový polynom  $f$  stupně  $n$  má nejvýše  $n$  kořenů, počítáme-li je i s jejich násobností.

Přesněji: pokud má polynom  $f$  kořeny  $c_1, \dots, c_m$ , přičemž kořen  $c_i$  má násobnost  $k_i$ , pak  $k_1 + \dots + k_m \leq n$ .

Především má  $f$  jen konečně mnoho kořenů.

Důkaz:

díky jednoznačnému rozkladu na prvočinitele máme

$$(x - c_1)^{k_1} \mid f, \dots, (x - c_m)^{k_m} \mid f \implies (x - c_1)^{k_1} \dots (x - c_m)^{k_m} \mid f.$$

Porovnáním stupňů dostaneme požadované.

Tedy především  $m \leq n$ .

## Algebraicky uzavřené těleso

Pro jaká tělesa platí rovnost?

Pro těleso  $(R, +, \cdot)$  je ekvivalentní:

- nenulový polynom z  $R[x]$  stupně  $n$  má právě  $n$  kořenů,
- každý nekonstantní polynom z  $R[x]$  má kořen,
- ireducibilní polynomy v  $R[x]$  jsou právě lineární polynomy (polynomy stupně 1),
- každý nekonstantní polynom z  $R[x]$  lze vyjádřit jako součin lineárních polynomů.

Hovoříme o **algebraicky uzavřeném** tělese.

Věta: Žádné konečné těleso není algebraicky uzavřené.

Důkaz: pokud  $R = \{a_1, a_2, \dots, a_m\}$ , pak polynom  $f = (x - a_1)(x - a_2) \dots (x - a_m) + 1$  nemá kořen v  $R$ .

Všimněme si, že hodnota  $f$  je vždy 1. Tzn.  $\phi_1 = \phi_f$  — polynomické funkce polynomů 1 a  $f$  jsou stejné.

Věta: Pokud  $(R, +, \cdot)$  je nekonečné těleso, pak pro libovolné dva polynomy  $f, g \in R[x]$  platí

$$f = g \iff \phi_f = \phi_g.$$

Důkaz: pokud  $\phi_f = \phi_g$ , pak pro polynom  $f - g$  platí

$$(f - g)(c) = f(c) - g(c) = \phi_f(c) - \phi_g(c) = 0.$$

Tedy každý prvek  $R$  je kořenem  $f - g$ , tzn.  $f - g = 0$ .

Kořeny polynomů – p.13/25

## Základní věta algebry

### Základní věta algebry

Těleso  $(\mathbb{C}, +, \cdot)$  je algebraicky uzavřené.

- Každý nekonstantní polynom z  $\mathbb{C}[x]$  má kořen v  $\mathbb{C}$ .
- Ireducibilní polynomy v  $\mathbb{C}[x]$  jsou právě lineární polynomy.

Proto jsme komplexní čísla zaváděli: chtěli jsme, aby polynom  $x^2 + 1$  měl kořen.

## Věta.

Je-li  $c \in \mathbb{C}$  kořen polynomu  $f \in \mathbb{R}[x]$ , pak číslo  $\bar{c}$  komplexně sdružené s  $c$  je kořenem polynomu  $f$ .

Důkaz:

Připomeňme, že  $\bar{\cdot} : \mathbb{C} \rightarrow \mathbb{C}$  je homomorfismus okruhů.

Pro polynom  $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$  máme

$$\begin{aligned} f(\bar{c}) &= a_n \bar{c}^n + a_{n-1} \bar{c}^{n-1} + \dots + a_1 \bar{c} + a_0 \\ &= \overline{a_n c^n + a_{n-1} c^{n-1} + \dots + a_1 c + a_0} = \overline{f(c)} = 0. \end{aligned}$$

## Komplexně sdružené kořeny

Nechť  $f \in \mathbb{R}[x]$  má kořen  $c$ .

- Pokud  $c \in \mathbb{R}$  pak  $(x - c) \mid f$ .
- Pokud  $c \notin \mathbb{R}$ , pak  $\bar{c}$  je také kořen  $f$ .  
Tedy  $(x - c)(x - \bar{c}) \mid f$ , kde  $(x - c)(x - \bar{c}) \in \mathbb{R}[x]$ .

$$(x - c)(x - \bar{c}) = x^2 - (c + \bar{c})x + c \cdot \bar{c}.$$

Pro  $c = a + bi$  je  $\bar{c} = a - bi$ .

$$\text{Odtud } c + \bar{c} = 2a \in \mathbb{R}, \quad c \cdot \bar{c} = a^2 + b^2 \in \mathbb{R}.$$

- Nekonstantní polynom je dělitelný buď lineárním nebo kvadratickým polynomem (nemající reálný kořen).
- Je-li  $c \in \mathbb{C}$  kořen polynomu  $f \in \mathbb{R}[x]$  násobnosti  $k$ , pak kořen  $\bar{c}$  má násobnost  $k$ .
- Polynom  $f \in \mathbb{R}[x]$  lichého stupně má reálný kořen.



## Věta.

Ireducibilními polynomy v  $\mathbb{R}[x]$  jsou právě lineární polynomy a kvadratické polynomy nemající reálné kořeny.

Důkaz:

- Konstantní polynomy — z definice.
- Lineární polynomy — vždy ireducibilní.
- Kvadratické polynomy:
  - mající kořen — lze rozložit, (nezáporný disk.)
  - nemající kořen — ireducibilní. (záporný disk.)
- Polynomy stupně 3 a víc — lze dělit dle předchozího.

## Vietovy vztahy

Jaký je vztah mezi koeficienty polynomu a jeho kořeny?

Nechť  $f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  je normovaný polynom stupně  $n$ , který má  $n$  kořenů  $c_1, \dots, c_n$  (včetně násobností).

Pak platí:

$$-a_{n-1} = c_1 + c_2 + \dots + c_n,$$

$$a_{n-2} = c_1c_2 + c_1c_3 + \dots + c_1c_n + c_2c_3 + \dots + c_{n-1}c_n,$$

$$(-1)^k a_{n-k} = \sum_{i_1 < i_2 < \dots < i_k} c_{i_1} c_{i_2} \dots c_{i_k},$$

$$(-1)^n a_0 = c_1 c_2 \dots c_n.$$

Důkaz: porovnáním koeficientů v rovnosti

$$x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = (x - c_1)(x - c_2) \dots (x - c_n).$$

Lze z koeficientů polynomu spočítat kořeny?

- Kvadratické polynomy — pomocí diskriminantu.
- Kubické polynomy — Cardanovy vzorce.
- Polynomy čtvrtého stupně — existují vzorce.
- Obecně — ne pro  $n \geq 5$  (Abel 1824).

Galois (1830)

Kořeny polynomu  $x^5 - 4x - 2$  nelze vyjádřit pomocí odmocnin koeficientů.

Kořeny polynomů – p.19/25

## Polynomy nad $\mathbb{Z}, \mathbb{Q}$

Každý polynom  $f \in \mathbb{Q}[x]$  lze jednoznačně psát jako

$$b \cdot (a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0),$$

kde  $b \in \mathbb{Q}$ ,  $a_n, \dots, a_0 \in \mathbb{Z}$  a  $\text{nsd}(a_n, a_{n-1}, \dots, a_1, a_0) = 1$ .

Polynom  $f \in \mathbb{Z}[x]$  je ireducibilní nad  $\mathbb{Z}$  právě tehdy, když je ireducibilní nad  $\mathbb{Q}$ .

Kořeny polynomů – p.20/25

Nechť  $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$  a  $\frac{p}{q}$  je racionální kořen polynomu  $f$  takový, že  $(p, q) = 1$ .  
Pak  $q \mid a_n, p \mid a_0$ .

**Důkaz:**

nechť  $a_n \left(\frac{p}{q}\right)^n + a_{n-1} \left(\frac{p}{q}\right)^{n-1} + \dots + a_1 \frac{p}{q} + a_0 = 0$ ,  
pronásobením  $q^n$  dostaneme:

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

Protože  $p$  a  $q$  jsou nesoudělné a dělí 0 máme  $q \mid a_n$  a  $p \mid a_0$ .

- Umíme najít všechny racionální kořeny (v  $\mathbb{Q}[x]$ ).
- Také  $(qx - p) \mid f$ , tj.  $(qc - p) \mid f(c)$  pro libovolné  $c \in \mathbb{Z}$  (tímto kritériem lze dále omezit počet adeptů).

## Ireducibilní polynomy nad $\mathbb{Q}$

**Věta (Eisensteinovo kritérium)**

Bud'  $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$  polynom stupně  $n > 0$  a necht' existuje prvočíslo  $p$  takové, že  $p \mid a_{n-1}, \dots, p \mid a_0$  a zároveň  $p \nmid a_n, p^2 \nmid a_0$ .  
Pak polynom  $f$  je ireducibilní.

**Příklad:**  $x^n + p$  je ireducibilní pro libovolné  $n$  a prvočíslo  $p$ .  
Existují tedy ireducibilní polynomy libovolného stupně.

**Zdůvodnění kritéria:** pokud  $f = g \cdot h$ , kde

$$g = b_m x^m + \dots + b_1 x + b_0 \quad \text{a} \quad h = c_k x^k + \dots + c_1 x + c_0.$$

Pak  $a_0 = b_0 c_0$ , tedy prvočíslo  $p$  dělí právě jedno z  $b_0, c_0$ .  
Pokud  $p$  dělí např.  $b_0$ , tak se postupně ukáže, že  $p \mid b_i$  pro všechna  $i$ . Což je spor s  $p \nmid a_n = b_m c_k$ .

Příklad: polynom  $x^4 - x^2 - 2$  má následující rozklady na ireducibilní polynomy:

- nad  $\mathbb{Q}$   $(x^2 - 2)(x^2 + 1)$
- nad  $\mathbb{R}$   $(x - \sqrt{2})(x + \sqrt{2})(x^2 + 1)$
- nad  $\mathbb{C}$   $(x - \sqrt{2})(x + \sqrt{2})(x - i)(x + i)$

Příklad z minulé přednášky: polynom  $x^3 - 2$  má následující rozklady na ireducibilní polynomy:

- nad  $\mathbb{Q}$   $x^3 - 2$
- nad  $\mathbb{R}$   $(x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$
- nad  $\mathbb{C}$   $(x - \sqrt[3]{2})(x - \sqrt[3]{2}\varepsilon_3)(x - \sqrt[3]{2}\varepsilon_3^2)$

zde  $\varepsilon_3 = \cos \frac{2\pi}{3} + i \sin \frac{2\pi}{3}$  je třetí odmocnina z 1.

## Časté chyby

Následující tvrzení NEPLATÍ:

- polynom nemá kořen, proto je ireducibilní,
- polynom je ireducibilní nad  $\mathbb{Q}$ , tedy existuje prvočíslo splňující Eisenteinovo kritérium.

Příklady:

- $x^6 - 1$  má 6 kořenů — odmocniny z 1.  
Tedy  $f = \frac{x^6 - 1}{x^2 - 1} = x^4 + x^2 + 1$  nemá reálné kořeny.  
Přesto jde rozložit a to dokonce nad  $\mathbb{Q}$ :  
 $f = (x^2 + x + 1)(x^2 - x + 1)$ .

- Polynom  $x^3 + 4$  je ireducibilní nad  $\mathbb{Q}$ .  
Kdyby nebyl, pak má lineární faktor a tedy racionální kořen, což nemá.

Co se bude zkoušet z praktického počítání?

- racionální kořeny,
- výpočet  $f(c)$  — Hroner,
- komplexní sdruženost kořenů,
- rozklad nad  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$  (neumíme obecně).

Z teorie:

- základní věta algebry,
- popis ireducibilních polynomů nad  $\mathbb{R}, \mathbb{C}$ .