Algebra - sedmý díl

Lenka Zalabová

Ústav matematiky a biomatematiky, Přírodovědecká fakulta, Jihočeská univerzita v Českých Budějovicích

zima 2012

Obsah

Základní definice

Definition

- Buď $(R, +, \cdot)$ těleso, $f = a_n x^n + \cdots + a_1 x + a_0$ polynom z $R[x]$ a $c \in R$. Prvek

$$a_n \cdot c^n + \cdots + a_1 \cdot c + a_0$$

tělesa R se nazývá *hodnota polynomu f* v prvku c.

Základní definice

Definition

- Buď $(R, +, \cdot)$ těleso, $f = a_n x^n + \cdots + a_1 x + a_0$ polynom z $R[x]$ a $c \in R$. Prvek

$$a_n \cdot c^n + \cdots + a_1 \cdot c + a_0$$

tělesa R se nazývá *hodnota polynomu* f v prvku c.

- Hodnotu polynomu $f \in R[x]$ v prvku $c \in R$ označujeme $f(c)$.

Základní definice

Definition

- Buď $(R, +, \cdot)$ těleso, $f = a_n x^n + \cdots + a_1 x + a_0$ polynom z $R[x]$ a $c \in R$. Prvek

$$a_n \cdot c^n + \cdots + a_1 \cdot c + a_0$$

tělesa R se nazývá *hodnota polynomu* f v prvku c.

- Hodnotu polynomu $f \in R[x]$ v prvku $c \in R$ označujeme $f(c)$.

Example

Hodnota polynomu $f = 4x^2 + 2x + 1 \in \mathbb{R}[x]$ v bodě $2 \in \mathbb{R}$ je

Základní definice

Definition

- Buď $(R, +, \cdot)$ těleso, $f = a_n x^n + \cdots + a_1 x + a_0$ polynom z $R[x]$ a $c \in R$. Prvek

$$a_n \cdot c^n + \cdots + a_1 \cdot c + a_0$$

tělesa R se nazývá *hodnota polynomu* f v prvku c.

- Hodnotu polynomu $f \in R[x]$ v prvku $c \in R$ označujeme $f(c)$.

Example

Hodnota polynomu $f = 4x^2 + 2x + 1 \in \mathbb{R}[x]$ v bodě $2 \in \mathbb{R}$ je

$$4 \cdot 2^2 + 2 \cdot 2 + 1 = 21.$$

Další základní definice

Definition

Buď f polynom nad tělesem R, $c \in R$. Řekneme, že c je *kořen polynomu* f, jestliže $f(c) = 0$.

Další základní definice

Definition

Buď f polynom nad tělesem R, $c \in R$. Řekneme, že c je *kořen polynomu* f, jestliže $f(c) = 0$.

Example

Mějme polynom $x^3 - 7x + 6 \in \mathbb{R}[x]$. Pak:

- Pro prvek $2 \in \mathbb{R}$ platí $2^3 - 7 \cdot 2 + 6 = 0$ a tedy 2 je kořenem.

Další základní definice

Definition

Buď f polynom nad tělesem R, $c \in R$. Řekneme, že c je *kořen polynomu* f, jestliže $f(c) = 0$.

Example

Mějme polynom $x^3 - 7x + 6 \in \mathbb{R}[x]$. Pak:

- Pro prvek $2 \in \mathbb{R}$ platí $2^3 - 7 \cdot 2 + 6 = 0$ a tedy 2 je kořenem.
- Pro prvek $3 \in \mathbb{R}$ platí $3^3 - 7 \cdot 3 + 6 = 12$ a tedy 2 není kořenem.

Základní vlastnost

Theorem

Buď R těleso. Pak $c \in R$ je kořenem polynomu $f \in R[x]$ právě tehdy, když $(x - c)|f$.

Proof: ...

Základní vlastnost

Theorem

Buď R těleso. Pak $c \in R$ je kořenem polynomu $f \in R[x]$ právě tehdy, když $(x - c)|f$.

Proof: ...

Example

Pro polynom $x^3 - 7x + 6 \in \mathbb{R}[x]$ a jeho kořen 2 platí

$$(x^3 - 7x + 6) : (x - 2) = x^2 + 2x - 3$$

neboli

$$(x^3 - 7x + 6) = (x^2 + 2x - 3) \cdot (x - 2)$$

Násobné kořeny

Definition

- Buď R těleso, $f \in R[x]$ a $c \in R$ kořen polynomu f. Přirozené číslo k se nazývá *násobnost kořene c*, jestliže $(x-c)^k | f$ a $(x-c)^{k+1} \nmid f$.

Násobné kořeny

Definition

- Buď R těleso, $f \in R[x]$ a $c \in R$ kořen polynomu f. Přirozené číslo k se nazývá *násobnost kořene c*, jestliže $(x-c)^k | f$ a $(x-c)^{k+1} \nmid f$.
- Kořeny násobnosti jedna se nazývají *jednoduché*.

Násobné kořeny

Definition

- Buď R těleso, $f \in R[x]$ a $c \in R$ kořen polynomu f. Přirozené číslo k se nazývá *násobnost kořene c*, jestliže $(x-c)^k | f$ a $(x-c)^{k+1} \nmid f$.
- Kořeny násobnosti jedna se nazývají *jednoduché*.

Example

Pro polynom $x^3 - 7x + 6 \in \mathbb{R}[x]$ platí, že jeho kořen 2 je jednoduchý.

Násobné kořeny

Definition

- Buď R těleso, $f \in R[x]$ a $c \in R$ kořen polynomu f. Přirozené číslo k se nazývá *násobnost kořene c*, jestliže $(x-c)^k | f$ a $(x-c)^{k+1} \nmid f$.
- Kořeny násobnosti jedna se nazývají *jednoduché*.

Example

Pro polynom $x^3 - 7x + 6 \in \mathbb{R}[x]$ platí, že jeho kořen 2 je jednoduchý. Platí:

$$x^3 - 7x + 6 = (x-2)^2 \cdot (x+4) + (5x - 10)$$

Kolik má polynom kořenů?

Theorem

Buď R těleso. Pak nenulový polynom $f \in R[x]$ má nejvýše $st(f)$ kořenů, počítáme-li je i s násobností.

Proof: ...

Kolik má polynom kořenů?

Theorem

Buď R těleso. Pak nenulový polynom $f \in R[x]$ má nejvýše $st(f)$ kořenů, počítáme-li je i s násobností.

Proof: ...
Neboli: Součet násobností všech kořenů polynomu $f \in R[x]$ je menší nebo roven $st(f)$.

Příklady

1. Polynom $x^2 - 2x - 3 \in \mathbb{R}[x]$ má dva jednoduché reálné kořeny $1, -3$.

Příklady

1. Polynom $x^2 - 2x - 3 \in \mathbb{R}[x]$ má dva jednoduché reálné kořeny $1, -3$.
2. Polynom $x^2 + 1 \in \mathbb{R}[x]$ nemá žádné reálné kořeny.

Příklady

1. Polynom $x^2 - 2x - 3 \in \mathbb{R}[x]$ má dva jednoduché reálné kořeny $1, -3$.
2. Polynom $x^2 + 1 \in \mathbb{R}[x]$ nemá žádné reálné kořeny.
3. Polynom $x^2 - 2x + 1 \in \mathbb{R}[x]$ má jeden dvojnásobný kořen 1.

Příklady

1. Polynom $x^2 - 2x - 3 \in \mathbb{R}[x]$ má dva jednoduché reálné kořeny $1, -3$.
2. Polynom $x^2 + 1 \in \mathbb{R}[x]$ nemá žádné reálné kořeny.
3. Polynom $x^2 - 2x + 1 \in \mathbb{R}[x]$ má jeden dvojnásobný kořen 1.
4. Polynom $x^3 - 4x^2 + x - 4 \in \mathbb{R}[x]$ má jeden jednoduchý reálný kořen 4.

Příklady

1. Polynom $x^2 - 2x - 3 \in \mathbb{R}[x]$ má dva jednoduché reálné kořeny $1, -3$.
2. Polynom $x^2 + 1 \in \mathbb{R}[x]$ nemá žádné reálné kořeny.
3. Polynom $x^2 - 2x + 1 \in \mathbb{R}[x]$ má jeden dvojnásobný kořen 1.
4. Polynom $x^3 - 4x^2 + x - 4 \in \mathbb{R}[x]$ má jeden jednoduchý reálný kořen 4.
5. Polynom $x^2 - 2 \in \mathbb{Q}[x]$ nemá žádné racionální kořeny.

Příklady

1. Polynom $x^2 - 2x - 3 \in \mathbb{R}[x]$ má dva jednoduché reálné kořeny $1, -3$.
2. Polynom $x^2 + 1 \in \mathbb{R}[x]$ nemá žádné reálné kořeny.
3. Polynom $x^2 - 2x + 1 \in \mathbb{R}[x]$ má jeden dvojnásobný kořen 1.
4. Polynom $x^3 - 4x^2 + x - 4 \in \mathbb{R}[x]$ má jeden jednoduchý reálný kořen 4.
5. Polynom $x^2 - 2 \in \mathbb{Q}[x]$ nemá žádné racionální kořeny.
6. Polynom $x^2 - 2 \in \mathbb{R}[x]$ má dva jednoduché reálné kořeny $\pm\sqrt{2}$.

Příklady

1. Polynom $x^2 - 2x - 3 \in \mathbb{R}[x]$ má dva jednoduché reálné kořeny $1, -3$.
2. Polynom $x^2 + 1 \in \mathbb{R}[x]$ nemá žádné reálné kořeny.
3. Polynom $x^2 - 2x + 1 \in \mathbb{R}[x]$ má jeden dvojnásobný kořen 1.
4. Polynom $x^3 - 4x^2 + x - 4 \in \mathbb{R}[x]$ má jeden jednoduchý reálný kořen 4.
5. Polynom $x^2 - 2 \in \mathbb{Q}[x]$ nemá žádné racionální kořeny.
6. Polynom $x^2 - 2 \in \mathbb{R}[x]$ má dva jednoduché reálné kořeny $\pm\sqrt{2}$.
7. Polynom $x^3 + 2x \in \mathbb{Z}_3[x]$ má tři jednoduché kořeny $0, 1, 2$ (přesněji: $[0]_3, [1]_3, [2]_3$).

Ireducibilní polynomy obecně

Definition

Buď R těleso. Polynom f nad R se nazývá *ireducibilní* nad R, jestliže je nekonstantní a nelze jej rozložit na součin dvou nekonstatntních polynomů.

Ireducibilní polynomy obecně

Definition

Buď R těleso. Polynom f nad R se nazývá *ireducibilní* nad R, jestliže je nekonstantní a nelze jej rozložit na součin dvou nekonstatntních polynomů.

Example

- Polynom $x^2 - 2$ není ireducibilní nad $\mathbb{R}$, protože lze zapsat jako $(x - \sqrt{2})(x + \sqrt{2})$.
- Polynom $x^2 - 2$ je ireducibilní nad $\mathbb{Q}$, protože nemá racionální kořen a nelze tedy zapsat jako součin dvou nekonstantních racionálních polynomů.

Rozklady polynomů obecně

Theorem

Buď R těleso a $f \in R[x]$ nenulový polynom. Pak existují $k \in \mathbb{N}_0$, ireducibilní normované polynomy $p_1, \ldots, p_k \in R[x]$ a $a \in R$ tak, že

$$f = a \cdot p_1 \cdot \cdots \cdot p_k.$$

Tento rozklad polynomu f je jednoznačný (až na pořadí činitelů).

Proof: ...

Rozklady polynomů obecně

Theorem

Buď R těleso a $f \in R[x]$ nenulový polynom. Pak existují $k \in \mathbb{N}_0$, ireducibilní normované polynomy $p_1, \ldots, p_k \in R[x]$ a $a \in R$ tak, že

$$f = a \cdot p_1 \cdot \cdots \cdot p_k.$$

Tento rozklad polynomu f je jednoznačný (až na pořadí činitelů).

Proof: ...

Example

Polynom $x^3 - 2x^2 - x + 2 \in \mathbb{R}[x]$ lze rozložit jako

$$(x-2)(x-1)(x+1).$$

Základní věta algebry

Theorem

Každý nekonstantní polynom v $\mathbb{C}[x]$ má kořen v $\mathbb{C}$.

Proof: ... těžká matematická analýza

Ireducibilní polynomy nad $\mathbb{R}$

Corollary

- *Polynom $f \in \mathbb{C}[x]$ je ireducibilní nad $\mathbb{C}$ právě tehdy, když je lineární.*

Ireducibilní polynomy nad $\mathbb{R}$

Corollary

- *Polynom $f \in \mathbb{C}[x]$ je ireducibilní nad $\mathbb{C}$ právě tehdy, když je lineární.*
- *Buď $f \in \mathbb{C}[x]$ nenulový polynom s vedoucím koeficientem a. Pak f lze jednoznačně (až na pořadí činitelů) vyjádřit jako*

$$f = a(x - c_1) \dots (x - c_n),$$

kde $c_1, \dots, c_n \in \mathbb{C}$.

Ireducibilní polynomy nad $\mathbb{R}$

Corollary

- *Polynom $f \in \mathbb{C}[x]$ je ireducibilní nad $\mathbb{C}$ právě tehdy, když je lineární.*
- *Buď $f \in \mathbb{C}[x]$ nenulový polynom s vedoucím koeficientem a. Pak f lze jednoznačně (až na pořadí činitelů) vyjádřit jako*

$$f = a(x - c_1) \dots (x - c_n),$$

kde $c_1, \dots, c_n \in \mathbb{C}$.

- *Každý polynom $f \in \mathbb{C}[x]$ stupně $n > 0$ má právě n kořenů (počítáme-li je s jejich násobností).*

Ireducibilní polynomy nad $\mathbb{R}$

Theorem

Je-li komplexní číslo $a+bi$ kořenem polynomu $f \in \mathbb{R}[x]$, pak i komplexně sdružené číslo $a-bi$ je kořenem f.

Proof:

- $g := (x-a-bi)(x-a+bi) = x^2-(2a)x+(a^2+b^2) \in \mathbb{R}[x]$
- zbytek po dělení polynomem g je lineární polynom $kx+q$, $k,q \in \mathbb{R}$, který má v bodě $a+bi$ komplexní hodnotu. Výpočet implikuje, že to jde pouze když $k=q=0$.

Ireducibilní polynomy nad $\mathbb{R}$

Theorem

Je-li komplexní číslo $a+bi$ kořenem polynomu $f \in \mathbb{R}[x]$, pak i komplexně sdružené číslo $a-bi$ je kořenem f.

Proof:

- $g := (x-a-bi)(x-a+bi) = x^2-(2a)x+(a^2+b^2) \in \mathbb{R}[x]$
- zbytek po dělení polynomem g je lineární polynom $kx+q$, $k,q \in \mathbb{R}$, který má v bodě $a+bi$ komplexní hodnotu. Výpočet implikuje, že to jde pouze když $k=q=0$.

Theorem

Ireducibilní polynomy v $\mathbb{R}[x]$ jsou právě lineární polynomy a kvadratické polynomy se záporným diskriminantem.

Proof: ...

Příklady

- Polynom $x - 4$ je ireducibilní nad $\mathbb{R}$.

Příklady

- Polynom $x - 4$ je ireducibilní nad $\mathbb{R}$.
- Polynom $x^2 + 2x - 3$ není ireducibilní nad $\mathbb{R}$, protože platí $x^2 + 2x - 3 = (x - 1)(x + 3)$.

Příklady

- Polynom $x - 4$ je ireducibilní nad $\mathbb{R}$.
- Polynom $x^2 + 2x - 3$ není ireducibilní nad $\mathbb{R}$, protože platí $x^2 + 2x - 3 = (x - 1)(x + 3)$.
- Polynom $x^2 + x + 9$ je ireducibilní nad $\mathbb{R}$, protože nemá reálné kořeny.

Příklady

- Polynom $x - 4$ je ireducibilní nad $\mathbb{R}$.
- Polynom $x^2 + 2x - 3$ není ireducibilní nad $\mathbb{R}$, protože platí $x^2 + 2x - 3 = (x - 1)(x + 3)$.
- Polynom $x^2 + x + 9$ je ireducibilní nad $\mathbb{R}$, protože nemá reálné kořeny.
- Polynom $x^3 - x^2 + x - 1$ není ireducibilní nad $\mathbb{R}$, protože platí $x^3 - x^2 + x - 1 = (x - 1)(x^2 + 1)$.

Polynomy nad $\mathbb{Q}$

Pro studium polynomů nad $\mathbb{Q}$ stačí studovat polynomy s celočíselnými koeficienty. Každý polynom z $\mathbb{Q}[x]$ můžeme vynásobit součinem jmenovatelů koeficientů, abychom dostali polynom s celočíselnými koeficienty. Ten se chová ‘stejně až na násobek’ jako původní polynom.

Polynomy nad $\mathbb{Q}$

Pro studium polynomů nad $\mathbb{Q}$ stačí studovat polynomy s celočíselnými koeficienty. Každý polynom z $\mathbb{Q}[x]$ můžeme vynásobit součinem jmenovatelů koeficientů, abychom dostali polynom s celočíselnými koeficienty. Ten se chová ‘stejně až na násobek’ jako původní polynom.

Theorem

Nechť $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ je polynom s celočíselnými koeficienty a $\frac{r}{s}$ je jeho racionální kořen takový, že $NSD(r, s) = 1$. Pak platí $s|a_n$ a $r|a_0$.

Proof: ...

Polynomy nad $\mathbb{Q}$

Pro studium polynomů nad $\mathbb{Q}$ stačí studovat polynomy s celočíselnými koeficienty. Každý polynom z $\mathbb{Q}[x]$ můžeme vynásobit součinem jmenovatelů koeficientů, abychom dostali polynom s celočíselnými koeficienty. Ten se chová ‘stejně až na násobek’ jako původní polynom.

Theorem

Nechť $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ je polynom s celočíselnými koeficienty a $\frac{r}{s}$ je jeho racionální kořen takový, že $NSD(r, s) = 1$. Pak platí $s|a_n$ a $r|a_0$.

Proof: ...

Naopak to neplatí! Pomocí této věty získáme všechna racionální čísla, která mohou (a taky nemusí) být racionální kořeny. Nicméně víme, že žadné jiné racionální kořeny už neexistují.

Example

Najděte všechny adepty na racionální kořeny polynomu

$$10x^4 - 9x^3 - 23x^2 + 4.$$

Example

Najděte všechny adepty na racionální kořeny polynomu

$$10x^4 - 9x^3 - 23x^2 + 4.$$

Máme $r \in \{\pm 4, \pm 2, \pm 1\}$ a $s \in \{\pm 10, \pm 5, \pm 2, \pm 1\}$.
Dohromady dostaneme:

$$\frac{r}{s} \in \{\pm\frac{2}{5}, \pm\frac{4}{5}, \pm 2, \pm 4, \pm\frac{1}{5}, \pm 1, \pm\frac{1}{10}, \pm\frac{1}{2}\}.$$

Example

Najděte všechny adepty na racionální kořeny polynomu

$$10x^4 - 9x^3 - 23x^2 + 4.$$

Máme $r \in \{\pm 4, \pm 2, \pm 1\}$ a $s \in \{\pm 10, \pm 5, \pm 2, \pm 1\}$.
Dohromady dostaneme:

$$\frac{r}{s} \in \{\pm\frac{2}{5}, \pm\frac{4}{5}, \pm 2, \pm 4, \pm\frac{1}{5}, \pm 1, \pm\frac{1}{10}, \pm\frac{1}{2}\}.$$

Přitom kořeny polynomu jsou $\frac{2}{5}, -\frac{1}{2}, -1$ a 2. (Všechny jsou jednoduché.)

Důležité důsledky

Corollary

Nechť $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$ je polynom s celočíselnými koeficienty stupně n.

- *Je-li celé číslo c kořenem polynomu f, pak $c | a_0$.*
- *Pokud f je normovaný polynom, pak každý jeho racionální kořen je celé číslo.*

Ireducibilní polynomy nad $\mathbb{Q}$

- Na rozdíl od $\mathbb{R}[x]$, ireducibilní polynomy v $\mathbb{Q}[x]$ nelze všechny explicitně popsat.
- Na rozdíl od $\mathbb{R}[x]$, v $\mathbb{Q}[x]$ existují ireducibilní polynomy libovolného stupně.
- Ireducibilní polynomy v $\mathbb{Q}[x]$ jsou například polynomu tvaru $x^n + 2$ pro libovolné $n \in \mathbb{N}$.
- Existují kritéria, podle kterých lze ireducibilitu některých polynomů rozpoznat.

Eisensteinovo kritérium

Theorem

Buď $f = a_n x^n + \cdots + a_1 x + a_0$ polynom s celočíselnými koeficienty stupně $n > 0$. Nechť existuje prvočíslo p takové, že $p|a_{n-1}, p|a_{n-2}, \ldots, p|a_1, p|a_0$ a $p \nmid a_n$ a $p^2 \nmid a_0$. Pak polynom f je ireducibilní nad $\mathbb{Q}$.

Proof: ...

Eisensteinovo kritérium

Theorem

Buď $f = a_n x^n + \cdots + a_1 x + a_0$ polynom s celočíselnými koeficienty stupně $n > 0$. Nechť existuje prvočíslo p takové, že $p|a_{n-1}, p|a_{n-2}, \ldots, p|a_1, p|a_0$ a $p \nmid a_n$ a $p^2 \nmid a_0$. Pak polynom f je ireducibilní nad $\mathbb{Q}$.

Proof: ...

Example

Polynom $3x^4 + 15x^2 + 10$ je ireducibilní nad $\mathbb{Q}$.

Eisensteinovo kritérium

Theorem

Buď $f = a_n x^n + \cdots + a_1 x + a_0$ polynom s celočíselnými koeficienty stupně $n > 0$. Nechť existuje prvočíslo p takové, že $p|a_{n-1}, p|a_{n-2}, \ldots, p|a_1, p|a_0$ a $p \nmid a_n$ a $p^2 \nmid a_0$. Pak polynom f je ireducibilní nad $\mathbb{Q}$.

Proof: ...

Example

Polynom $3x^4 + 15x^2 + 10$ je ireducibilní nad $\mathbb{Q}$. Uvažme prvočíslo $p = 5$. Platí: $5|15, 5|10, 5 \nmid 3$ a $5^2 \nmid 10$.

Příklady

- Komplexní polynom $x^3 - 3x^2 + ix^2 + 7x + 2ix - 1 - 5i$ lze rozložit jako $(x - i)(x - 1 - i)(x - 2 + 3i)$.

Příklady

- Komplexní polynom $x^3 - 3x^2 + ix^2 + 7x + 2ix - 1 - 5i$ lze rozložit jako $(x - i)(x - 1 - i)(x - 2 + 3i)$.
- Reálný polynom $x^2 + 1$ je ireducibilní nad $\mathbb{R}$.
  Nad $\mathbb{C}$ lze $x^2 + 1$ rozložit jako $x^2 + 1 = (x - i)(x + i)$.

Příklady

- Komplexní polynom $x^3 - 3x^2 + ix^2 + 7x + 2ix - 1 - 5i$ lze rozložit jako $(x - i)(x - 1 - i)(x - 2 + 3i)$.
- Reálný polynom $x^2 + 1$ je ireducibilní nad $\mathbb{R}$.
  Nad $\mathbb{C}$ lze $x^2 + 1$ rozložit jako $x^2 + 1 = (x - i)(x + i)$.
- Racionální polynom $x^3 + 2$ je ireducibilní na $\mathbb{Q}$.
  Tento polynom má jeden reálný kořen $-\sqrt[3]{2}$ a nad $\mathbb{R}$ lze $x^3 + 2$ rozložit jako $x^3 + 2 = (x + \sqrt[3]{2})(x^2 - \sqrt[3]{2}x + \sqrt[3]{4})$ a oba tyto polynomy jsou ireducibilní nad $\mathbb{R}$.
  Polynom $x^2 - \sqrt[3]{2}x + \sqrt[3]{4}$ ma dva komplexně sdružené kořeny $x = \frac{\sqrt[3]{2}}{2} + i\frac{\sqrt{3}\sqrt[3]{2}}{2}$ a $x = \frac{\sqrt[3]{2}}{2} - i\frac{\sqrt{3}\sqrt[3]{2}}{2}$. Pak nad $\mathbb{C}$ lze $x^3 + 2$ rozložit jako
  $(x + \sqrt[3]{2})(x - \frac{\sqrt[3]{2}}{2} - i\frac{\sqrt{3}\sqrt[3]{2}}{2})(x - \frac{\sqrt[3]{2}}{2} + i\frac{\sqrt{3}\sqrt[3]{2}}{2})$.

Rozklady polynomů

V $\mathbb{C}$ a $\mathbb{R}$ a $\mathbb{Q}$ najděte rozklad následujícího polynomu na ireducibilní faktory:

$$x^6 + 5x^5 - 20x^3 - 13x^2 + 15x + 12.$$

Rozklady polynomů

V $\mathbb{C}$ a $\mathbb{R}$ a $\mathbb{Q}$ najděte rozklad následujícího polynomu na ireducibilní faktory:

$$x^6 + 5x^5 - 20x^3 - 13x^2 + 15x + 12.$$

Nad $\mathbb{Q}$ dostaneme

$$(x-1)(x+1)^2(x^2-3)(x+4).$$

Nad $\mathbb{R}$ dostaneme

$$(x-1)(x+1)^2(x-\sqrt{3})(x+\sqrt{3})(x+4).$$

Základní definice

Definition

Buď $f = a_n x^n + \cdots + a_1 x + a_0$ polynom nad tělesem R. Polynom

$$f' = n a_n x^{n-1} + \cdots + 2a_2 x + a_1 \in R[x]$$

se nazývá *derivace* polynomu f.

Základní definice

Definition

Buď $f = a_n x^n + \cdots + a_1 x + a_0$ polynom nad tělesem R. Polynom

$$f' = n a_n x^{n-1} + \cdots + 2a_2 x + a_1 \in R[x]$$

se nazývá *derivace* polynomu f.

Example

- Polynom $3x^3 - 5x^2 + x - 1 \in \mathbb{R}[x]$ má derivaci

Základní definice

Definition

Buď $f = a_n x^n + \cdots + a_1 x + a_0$ polynom nad tělesem R. Polynom

$$f' = n a_n x^{n-1} + \cdots + 2a_2 x + a_1 \in R[x]$$

se nazývá *derivace* polynomu f.

Example

- Polynom $3x^3 - 5x^2 + x - 1 \in \mathbb{R}[x]$ má derivaci $9x^2 - 10x + 1$.

Základní definice

Definition

Buď $f = a_n x^n + \cdots + a_1 x + a_0$ polynom nad tělesem R. Polynom

$$f' = n a_n x^{n-1} + \cdots + 2a_2 x + a_1 \in R[x]$$

se nazývá *derivace* polynomu f.

Example

- Polynom $3x^3 - 5x^2 + x - 1 \in \mathbb{R}[x]$ má derivaci $9x^2 - 10x + 1$.
- Polynom $2x^3 + 2x^2 + 2x + 1 \in \mathbb{Z}_3[x]$ má derivaci

Základní definice

Definition

Buď $f = a_n x^n + \cdots + a_1 x + a_0$ polynom nad tělesem R. Polynom

$$f' = n a_n x^{n-1} + \cdots + 2a_2 x + a_1 \in R[x]$$

se nazývá *derivace* polynomu f.

Example

- Polynom $3x^3 - 5x^2 + x - 1 \in \mathbb{R}[x]$ má derivaci $9x^2 - 10x + 1$.
- Polynom $2x^3 + 2x^2 + 2x + 1 \in \mathbb{Z}_3[x]$ má derivaci $x + 2$.

Základní vlastnosti

Theorem

Buď R těleso, $f, g \in R[x]$. Pak platí:

1. $(f+g)' = f' + g'$,
2. $(f \cdot g)' = f' \cdot g + f \cdot g'$.

Proof: ...

Základní vlastnosti

Theorem

Buď R těleso, $f, g \in R[x]$. Pak platí:

1. $(f+g)' = f' + g'$,
2. $(f \cdot g)' = f' \cdot g + f \cdot g'$.

Proof: ...

- Druhou derivaci polynomu f , t.j. polynom $(f')'$ budeme značit symbolem f''.
- Obecně k-tou derivaci polynomu f budeme značit symbolem $f^{(k)}$.

Charakteristika tělesa

Definition

- *Charakteristika* tělesa $(R, +, \cdot)$ je nejmenší přirozené číslo n takové, že
$$\underbrace{1 + \cdots + 1}_{n} = 0.$$
- Pokud žádné takove n neexistuje, mluvíme o tělese *charakteristiky* 0.

Charakteristika tělesa

Definition

- *Charakteristika* tělesa $(R, +, \cdot)$ je nejmenší přirozené číslo n takové, že
$$\underbrace{1 + \cdots + 1}_{n} = 0.$$
- Pokud žádné takove n neexistuje, mluvíme o tělese *charakteristiky* 0.

Example

- Tělesa $(\mathbb{Q}, +, \cdot)$ a $(\mathbb{R}, +, \cdot)$ mají charakteristiku

Charakteristika tělesa

Definition

- *Charakteristika* tělesa $(R, +, \cdot)$ je nejmenší přirozené číslo n takové, že
$$\underbrace{1 + \cdots + 1}_{n} = 0.$$
- Pokud žádné takove n neexistuje, mluvíme o tělese *charakteristiky* 0.

Example

- Tělesa $(\mathbb{Q}, +, \cdot)$ a $(\mathbb{R}, +, \cdot)$ mají charakteristiku 0.

Charakteristika tělesa

Definition

- *Charakteristika* tělesa $(R, +, \cdot)$ je nejmenší přirozené číslo n takové, že
$$\underbrace{1 + \cdots + 1}_{n} = 0.$$
- Pokud žádné takove n neexistuje, mluvíme o tělese *charakteristiky* 0.

Example

- Tělesa $(\mathbb{Q}, +, \cdot)$ a $(\mathbb{R}, +, \cdot)$ mají charakteristiku 0.
- Těleso $(\mathbb{Z}_n, +, \cdot)$ (pro n prvočíslo) má charakteristiku

Charakteristika tělesa

Definition

- *Charakteristika* tělesa $(R, +, \cdot)$ je nejmenší přirozené číslo n takové, že
$$\underbrace{1 + \cdots + 1}_{n} = 0.$$
- Pokud žádné takove n neexistuje, mluvíme o tělese *charakteristiky* 0.

Example

- Tělesa $(\mathbb{Q}, +, \cdot)$ a $(\mathbb{R}, +, \cdot)$ mají charakteristiku 0.
- Těleso $(\mathbb{Z}_n, +, \cdot)$ (pro n prvočíslo) má charakteristiku n.

Proč mluvíme o derivacích v algebře?

Theorem

Buď R těleso charakteristiky 0, $f \in R[x]$, $c \in R$ a k přirozené číslo. Pak c je k-násobným kořenem polynomu f, právě tehdy když c je kořenem polynomů $f, f', f'', \ldots, f^{(k)}$ a není kořenem polynomu $f^{(k+1)}$.

Proof: ... z definice derivace součinu

Důsledky

- Největší společný dělitel g polynomů f a f' má za kořeny právě ty prvky R, které jsou násobné kořeny f.

Důsledky

- Největší společný dělitel g polynomů f a f' má za kořeny právě ty prvky R, které jsou násobné kořeny f.
- Polynom $\frac{f}{g}$ má stejné kořeny jako f, ale všechny jsou jednoduché.

Jednoduchý příklad

- $f = (x-1)^2(x+2) = x^3 - 3x + 2$ má jeden dvojnásobný kořen 1 a jeden jednoduchý kořen -2

Jednoduchý příklad

- $f = (x-1)^2(x+2) = x^3 - 3x + 2$ má jeden dvojnásobný kořen 1 a jeden jednoduchý kořen -2
- $f' = 3x^2 - 3 = 3(x-1)(x+1)$ má jeden jednoduchý kořen 1 a jeden jednoduchý kořen -1

Jednoduchý příklad

- $f = (x-1)^2(x+2) = x^3 - 3x + 2$ má jeden dvojnásobný kořen 1 a jeden jednoduchý kořen -2
- $f' = 3x^2 - 3 = 3(x-1)(x+1)$ má jeden jednoduchý kořen 1 a jeden jednoduchý kořen -1
- $g = NSD(f, f') = x - 1$ má jeden jednoduchý kořen 1

Jednoduchý příklad

- $f = (x-1)^2(x+2) = x^3 - 3x + 2$ má jeden dvojnásobný kořen 1 a jeden jednoduchý kořen -2
- $f' = 3x^2 - 3 = 3(x-1)(x+1)$ má jeden jednoduchý kořen 1 a jeden jednoduchý kořen -1
- $g = NSD(f, f') = x - 1$ má jeden jednoduchý kořen 1
- $\frac{f}{g} = x^2 + x - 2 = (x+2)(x-1)$

Konečná tělesa

- Z dřívějška víte, že okruh $(\mathbb{Z}_n, +, \cdot)$ tvoří těleso, pokud n je prvočíslo.
- Tedy například čtyřprvkový okruh $(\mathbb{Z}_4, +, \cdot)$ není těleso.
- Existuje nějaké čtyřprvkové těleso?

Příklad $GF(4)$

- Uvažujme množinu $GF(4) = \{0, 1, x, x + 1\}$ polynomů jedné proměnné s koeficienty $0, 1$. Koeficienty považujeme za prvky tělesa $\mathbb{Z}_2$.

Příklad $GF(4)$

- Uvažujme množinu $GF(4) = \{0, 1, x, x+1\}$ polynomů jedné proměnné s koeficienty $0, 1$. Koeficienty považujeme za prvky tělesa $\mathbb{Z}_2$.
- Tato množina je uzavřená na běžné sčítání polynomů. Například
  $(x+1)+x = 2x+1 = 1, (x+1)+1 = x+2 = x$, atd.

Příklad $GF(4)$

- Uvažujme množinu $GF(4) = \{0, 1, x, x+1\}$ polynomů jedné proměnné s koeficienty $0, 1$. Koeficienty považujeme za prvky tělesa $\mathbb{Z}_2$.
- Tato množina je uzavřená na běžné sčítání polynomů. Například
  $(x+1) + x = 2x + 1 = 1, (x+1) + 1 = x + 2 = x$, atd.
- Tato množina není uzavřená na běžné násobení polynomů. Například $(x+1) \cdot (x+1) = x^2 + 2x + 1 = x^2 + 1$.

Příklad $GF(4)$

- Definujme novou operaci $\odot$ násobení polynomů na $GF(4)$ jako běžné násobení modulo polynom $x^2 + x + 1$.
- To znamená, že obvyklý součin dvou polynomů vydělíme se zbytkem polynomem $x^2 + x + 1$ a jako výsledek součinu $\odot$ vezmeme tento zbytek.

Příklad $GF(4)$

- Definujme novou operaci $\odot$ násobení polynomů na $GF(4)$ jako běžné násobení modulo polynom $x^2 + x + 1$.
- To znamená, že obvyklý součin dvou polynomů vydělíme se zbytkem polynomem $x^2 + x + 1$ a jako výsledek součinu $\odot$ vezmeme tento zbytek.
- Například $(x + 1) \odot (x + 1) =$ zbytek po dělení polynomu $(x + 1) \cdot (x + 1) = x^2 + 1$ polynomem $x^2 + x + 1$. Tedy $(x + 1) \odot (x + 1) = x$.

Příklad $GF(4)$

- Definujme novou operaci $\odot$ násobení polynomů na $GF(4)$ jako běžné násobení modulo polynom $x^2 + x + 1$.
- To znamená, že obvyklý součin dvou polynomů vydělíme se zbytkem polynomem $x^2 + x + 1$ a jako výsledek součinu $\odot$ vezmeme tento zbytek.
- Například $(x + 1) \odot (x + 1) =$ zbytek po dělení polynomu $(x + 1) \cdot (x + 1) = x^2 + 1$ polynomem $x^2 + x + 1$. Tedy $(x + 1) \odot (x + 1) = x$.
- Není těžké ověřit, že $(GF(4), +, \odot)$ je čtyřprvkové těleso.

Konečná tělesa

- Pro každé prvočíslo p a každý exponent $n \geq 1$ existuje právě jedno těleso, které má p^n prvků. Žádná jiná tělesa s konečným počtem prvků neexistují. Například neexistuje šestiprvkové těleso.

Konečná tělesa

- Pro každé prvočíslo p a každý exponent $n \geq 1$ existuje právě jedno těleso, které má p^n prvků. Žádná jiná tělesa s konečným počtem prvků neexistují. Například neexistuje šestiprvkové těleso.
- Tělesa s počtem prvků p^n pro $n \geq 2$ se konstruují podobně jako čtyřprvkové těleso $(GF(4), +, \odot)$.
  Tedy: Vezmeme všechny polynomy (včetně konstantních) stupně menšího než n s koeficienty v tělese $\mathbb{Z}_p$. Těch je celkem p^n. Na této množině sčítáme obvyklým způsobem a násobíme modulo vhodný polynom stupně n.

Shamirovo sdílení tajemství

Chceme rozdělit data D na n částí $D_1, \ldots, D_n$ tak, že:

- Ze znalosti k nebo více částí D_i lze snado spočítat D.
- Ze znalosti $k-1$ nebo méně částí nelze zjistit žádná informace o D.

... (k,n)–*prahové schéma*.

Shamirovo sdílení tajemství

Předpokládáme, že D je prvkem konečného tělesa, například $\mathbb{Z}_l$ pro vhodné prvočíslo l.

- Náhodně vybereme $k-1$ prvků $a_1, \ldots, a_{k-1} \in \mathbb{Z}_l$.
- Položíme $a_0 = D$.
- Sestavíme polynom

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1} x^{k-1}.$$

- Pro n libovolných prvků $\mathbb{Z}_l$ (například pro $i = 1, \ldots, n$) vypočítáme hodnoty polynomu f v těchto bodech (t.j. dvojice $(i, f(i))$ pro $i = 1, \ldots, n$).
- Tyto dvojice rozdělíme mezi n účastníků.

Zejména: Tajemství D známe, pokud známe polynom f.

Jak to funguje?

Theorem

Každý polynom stupně $k-1$ je jednoznačně určen svými hodnotami v libovolných k bodech.

Tedy:

- Z jakékoliv k prvkové (a víceprvkové) podmnožiny vybraných bodů lze jednoznačně určit koeficienty polynomu f, a tedy i $a_0 = D$.
- Z $(k-1)$–prvkové (a méněprvkové) podmnožiny nezjistíme nic.

Proč to funguje?

- Pro každou k–tici čísel $x_1, \ldots, x_k$ musí neznámé koeficienty $a_0, \ldots, a_n \in \mathbb{Z}_l$ splňovat

$$\begin{aligned} f(x_1) &= a_0 + a_1 x_1 + a_2 x_1^2 + \cdots + a_{k-1} x_1^{k-1} \\ f(x_2) &= a_0 + a_1 x_2 + a_2 x_2^2 + \cdots + a_{k-1} x_2^{k-1} \\ &\ldots \\ f(x_k) &= a_0 + a_1 x_k + a_2 x_k^2 + \cdots + a_{k-1} x_k^{k-1}. \end{aligned}$$

- Matice této soustavy je tzv. *Vandermondova* matice. O ní lze ukázat, že je vždy regulární (nad libovolným tělesem, protože ‘lineární algebra funguje pro libovolné těleso’).
- Tedy soustava má jedno řešení, které jednoznačně zadává polynom.

Rozklad polynomů nad konečnými tělesy

- bezčtvercová faktorizace a Berlekampův algoritmus
- Zassenhaussův algoritmus
- atd.

http://www.karlin.mff.cuni.cz/ barto/student/SkriptaKonTel.pdf, http://fox.ucw.cz/papers/factoring/factor.pdf