Algebra - šestý díl

Lenka Zalabová

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

zima 2012

Obsah

Okruhy

Definition

Množina R se dvěma operacemi $+$ a $\cdot$ se nazývá *okruh*, jestliže:

1. $(R, +)$ je komutativní grupa,
2. $(R, \cdot)$ je pologrupa s jednotkovým prvkem,
3. pro libovolné $a, b, c \in R$ platí tzv. *distributivní zákony*

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$
$$(b + c) \cdot a = b \cdot a + c \cdot a.$$

Okruh budeme označovat symbolem $(R, +, \cdot)$.

Příklady

- Trojice $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ tvoří okruhy.

Příklady

- Trojice $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ tvoří okruhy.
- Trojice $(Mat_n(\mathbb{R}), +, \cdot)$, kde $Mat_n(\mathbb{R})$ jsou reálné čtvercové matice řádu n, tvoří okruh.

Příklady

- Trojice $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ tvoří okruhy.
- Trojice $(Mat_n(\mathbb{R}), +, \cdot)$, kde $Mat_n(\mathbb{R})$ jsou reálné čtvercové matice řádu n, tvoří okruh.
- Trojice $(\mathbb{Z}_n, +, \cdot)$ tvoří okruh pro libovolné $n \in \mathbb{N}$.

Příklady

- Trojice $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ tvoří okruhy.
- Trojice $(Mat_n(\mathbb{R}), +, \cdot)$, kde $Mat_n(\mathbb{R})$ jsou reálné čtvercové matice řádu n, tvoří okruh.
- Trojice $(\mathbb{Z}_n, +, \cdot)$ tvoří okruh pro libovolné $n \in \mathbb{N}$.

Značení

- Protože v okruhu jsou dvě operace, je třeba dbát na to, aby nedošlo k jejich záměně.
- Pro operaci $+$ budeme používat aditivní terminologii, t.j. budeme hovořit o *plus*. Jednotkový prvek grupy $(R, +)$ budeme nazývat *nulový prvek* a označovat jej 0. Inverzní prvek k prvku $a \in R$ v grupě $(R, +)$ budeme nazývat *opačný prvek* a budeme jej značit $-a$.
- Pro operaci $\cdot$ budeme používat multiplikativní terminologii, t.j. budeme hovořit o *krát*. Jednotkový prvek pologrupy $(R, \cdot)$ budeme nazývat *jednotkový prvek* a označovat jej 1.
- Jednoprvkový okruh $(R, +, \cdot)$, kde $R = \{0 = 1\}$, se nazývá *triviální*. Triviální okruh je zřejmě jednoprvkový. Okruhy, které mají víc než jeden prvek, se nazývají *netriviální*.

Nějaké vlastnosti

Buď $(R, +, \cdot)$ okruh. Pak platí:

1. $a \cdot 0 = 0 \cdot a = 0$ pro libovolný prvek $a \in R$,

Nějaké vlastnosti

Buď $(R, +, \cdot)$ okruh. Pak platí:

1. $a \cdot 0 = 0 \cdot a = 0$ pro libovolný prvek $a \in R$,
2. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ pro libovolné prvky $a, b \in R$,

Nějaké vlastnosti

Buď $(R, +, \cdot)$ okruh. Pak platí:

1. $a \cdot 0 = 0 \cdot a = 0$ pro libovolný prvek $a \in R$,
2. $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$ pro libovolné prvky $a, b \in R$,
3. $a \cdot (b - c) = a \cdot b - a \cdot c$, $(b - c) \cdot a = b \cdot a - c \cdot a$ pro libovolné prvky $a, b, c \in R$,
4. atd.

Proof: ...

Další definice

Definition

- Okruh $(R, +, \cdot)$ se nazývá *komutativní*, pokud $(R, \cdot)$ je komutativní pologrupa.

Další definice

Definition

- Okruh $(R, +, \cdot)$ se nazývá *komutativní*, pokud $(R, \cdot)$ je komutativní pologrupa.
- Netriviální komutativní okruh se nazývá *obor integrity*, jestliže pro libovolné dva nenulové prvky $a, b \in R$ platí $a \cdot b \neq 0$.

Další definice

Definition

- Okruh $(R, +, \cdot)$ se nazývá *komutativní*, pokud $(R, \cdot)$ je komutativní pologrupa.
- Netriviální komutativní okruh se nazývá *obor integrity*, jestliže pro libovolné dva nenulové prvky $a, b \in R$ platí $a \cdot b \neq 0$.
- Nenulové prvky $a, b \in R$ takové, že $a \cdot b = 0$ se nazývají *dělitelé nuly*.

Další definice

Definition

- Okruh $(R, +, \cdot)$ se nazývá *komutativní*, pokud $(R, \cdot)$ je komutativní pologrupa.
- Netriviální komutativní okruh se nazývá *obor integrity*, jestliže pro libovolné dva nenulové prvky $a, b \in R$ platí $a \cdot b \neq 0$.
- Nenulové prvky $a, b \in R$ takové, že $a \cdot b = 0$ se nazývají *dělitelé nuly*.
- Invertibilní prvek pologrupy $(R, \cdot)$ se nazývá *jednotka*.

Další definice

Definition

- Okruh $(R, +, \cdot)$ se nazývá *komutativní*, pokud $(R, \cdot)$ je komutativní pologrupa.
- Netriviální komutativní okruh se nazývá *obor integrity*, jestliže pro libovolné dva nenulové prvky $a, b \in R$ platí $a \cdot b \neq 0$.
- Nenulové prvky $a, b \in R$ takové, že $a \cdot b = 0$ se nazývají *dělitelé nuly*.
- Invertibilní prvek pologrupy $(R, \cdot)$ se nazývá *jednotka*.
- Netriviální komutativní okruh se nazývá *těleso*, jestliže každý nenulový prvek $(R, \cdot)$ má inverzi.

Důležitý poznatek

Theorem

Každé těleso je obor integrity.

Proof: ...

Důležitý poznatek

Theorem

Každé těleso je obor integrity.

Proof: ...

- Naopak to obecně neplatí!

Důležitý poznatek

Theorem

Každé těleso je obor integrity.

Proof: ...

- Naopak to obecně neplatí!
- Platí pouze: Každý konečný obor integrity je těleso.

Příklady

- Okruhy $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ jsou tělesa.

Příklady

- Okruhy $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ jsou tělesa.
- Okruh $(\mathbb{Z}, +, \cdot)$ je obor integrity, který není těleso.

Příklady

- Okruhy $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ jsou tělesa.
- Okruh $(\mathbb{Z}, +, \cdot)$ je obor integrity, který není těleso.
  Co jsou jednotky v tomto okruhu?

Příklady

- Okruhy $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ jsou tělesa.
- Okruh $(\mathbb{Z}, +, \cdot)$ je obor integrity, který není těleso.
  Co jsou jednotky v tomto okruhu? ... ± 1.

Příklady

- Okruhy $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ jsou tělesa.
- Okruh $(\mathbb{Z}, +, \cdot)$ je obor integrity, který není těleso.
  Co jsou jednotky v tomto okruhu? ... ± 1.
- Okruh $(Mat_n(\mathbb{R}), +, \cdot)$, kde $Mat_n(\mathbb{R})$ jsou reálné čtvercové matice řádu n, není komutativní a obsahuje dělitele nuly.

Příklady

- Okruhy $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ jsou tělesa.
- Okruh $(\mathbb{Z}, +, \cdot)$ je obor integrity, který není těleso.
  Co jsou jednotky v tomto okruhu? ... ± 1.
- Okruh $(Mat_n(\mathbb{R}), +, \cdot)$, kde $Mat_n(\mathbb{R})$ jsou reálné čtvercové matice řádu n, není komutativní a obsahuje dělitele nuly.
  Co jsou jednotky v tomto okruhu?

Příklady

- Okruhy $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ jsou tělesa.
- Okruh $(\mathbb{Z}, +, \cdot)$ je obor integrity, který není těleso.
  Co jsou jednotky v tomto okruhu? ... ± 1.
- Okruh $(Mat_n(\mathbb{R}), +, \cdot)$, kde $Mat_n(\mathbb{R})$ jsou reálné čtvercové matice řádu n, není komutativní a obsahuje dělitele nuly.
  Co jsou jednotky v tomto okruhu? ... regulární matice.

Příklady

- Okruh $(\mathbb{Z}_n, +, \cdot)$ je komutativní okruh pro libovolné $n \in \mathbb{N}$.

Příklady

- Okruh $(\mathbb{Z}_n, +, \cdot)$ je komutativní okruh pro libovolné $n \in \mathbb{N}$.

Theorem

Okruh $(\mathbb{Z}_n, +, \cdot)$ je obor integrity právě tehdy když n je prvočíslo. V tomto případě je to přímo těleso.

Proof: ...

1. Okruhy a tělesa
2. Okruhy polynomů
3. Dělitelnost na polynomech

Definition

Buď $(R, +, \cdot)$ těleso. *Polynomem* nad tělesem R rozumíme konečný výraz

$$f = f(x) = \sum_{i=0}^{k} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k,$$

kde $a_i \in R$ pro $i = 1, \ldots, k$ jsou *koeficienty polynomu*. Předpokládáme $a_k \neq 0$ a říkame, že $f(x)$ má *stupeň* k. Píšeme $st(f) = k$.

Definition

Buď $(R, +, \cdot)$ těleso. *Polynomem* nad tělesem R rozumíme konečný výraz

$$f = f(x) = \sum_{i=0}^{k} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k,$$

kde $a_i \in R$ pro $i = 1, \ldots, k$ jsou *koeficienty polynomu*. Předpokládáme $a_k \neq 0$ a říkame, že $f(x)$ má *stupeň* k. Píšeme $st(f) = k$.

Example

Výraz $7 + \frac{2}{7}x + \pi x^2 - 9x^5$ je polynomem nad $\mathbb{R}$ stupně 5.

Množinu polynomů nad okruhem $(R, +, \cdot)$ budeme značit $R[x]$.

Sčítání na $R[x]$

Mějme polynomy
$f(x) = \sum_{i=0}^{k} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k$,
$g(x) = \sum_{i=0}^{l} b_i x^i = b_0 + b_1 x + b_2 x^2 + \cdots + b_l x^l$
a předpokládejme $l \leq k$, neboli $st(g) \leq st(f)$. Pak jejich součtem je polynom

$$(f+g)(x) = \sum_{i=0}^{k} (a_i + b_i) x^i$$
$$= (a_0 + b_0) + (a_1 + b_1) x + (a_2 + b_2) x^2 + \ldots$$
$$\cdots + (a_k + b_k) x^k$$

Sčítání na $R[x]$

Mějme polynomy
$f(x) = \sum_{i=0}^{k} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k$,
$g(x) = \sum_{i=0}^{l} b_i x^i = b_0 + b_1 x + b_2 x^2 + \cdots + b_l x^l$
a předpokládejme $l \leq k$, neboli $st(g) \leq st(f)$. Pak jejich součtem je polynom

$$\begin{aligned}(f+g)(x) = &\sum_{i=0}^{k}(a_i + b_i)x^i \\ =&(a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots \\ &\cdots + (a_k + b_k)x^k\end{aligned}$$

... sečteme koeficienty podle stupňů po složkách, požíváme vlastností tělesa R.

Násobení na $R[x]$

Mějme polynomy
$f(x) = \sum_{i=0}^{k} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k$,
$g(x) = \sum_{i=0}^{l} b_i x^i = b_0 + b_1 x + b_2 x^2 + \cdots + b_l x^l$.
Pak jejich součinem je polynom

$$(f \cdot g)(x) = \sum_{i=0}^{k+l} c_i x^i = c_0 + c_1 x + c_2 x^2 + \cdots + c_{k+l} x^{k+l},$$

kde koeficient c_i je tvaru

$$c_i = \sum_{m=0}^{i} a_m b_{i-m} = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0.$$

Násobení na $R[x]$

Mějme polynomy
$f(x) = \sum_{i=0}^{k} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_k x^k$,
$g(x) = \sum_{i=0}^{l} b_i x^i = b_0 + b_1 x + b_2 x^2 + \cdots + b_l x^l$.
Pak jejich součinem je polynom

$$(f \cdot g)(x) = \sum_{i=0}^{k+l} c_i x^i = c_0 + c_1 x + c_2 x^2 + \cdots + c_{k+l} x^{k+l},$$

kde koeficient c_i je tvaru

$$c_i = \sum_{m=0}^{i} a_m b_{i-m} = a_0 b_i + a_1 b_{i-1} + \cdots + a_i b_0.$$

... vynásobíme jako mnohočleny a srovnáme podle stupňů, při ‘srovnávání’ požíváme vlastností tělesa R.

Konkrétně

Example

Najděte součet a součin polynomů
$f(x) = 1 + 4x - 2x^2 + 5x^3$ a
$g(x) = 8 - 3x + 6x^2$
nad tělesem $\mathbb{R}$.

Konkrétně

Example

Najděte součet a součin polynomů
$f(x) = 1 + 4x - 2x^2 + 5x^3$ a
$g(x) = 8 - 3x + 6x^2$
nad tělesem $\mathbb{R}$.
Dostaneme:

$$(f+g)(x) = 9 + x + 4x^2 + 5x^3,$$
$$(f \cdot g)(x) = 8 + 29x - 22x^2 + 70x^3 - 27x^4 + 30x^5.$$

Okruh polynomů

Theorem

Buď $(R, +, \cdot)$ *těleso. Pak* $(R[x], +, \cdot)$ *se sčítáním a násobením polynomů je obor integrity.*

Proof: ...

Okruh polynomů

Theorem

Buď $(R, +, \cdot)$ *těleso. Pak* $(R[x], +, \cdot)$ *se sčítáním a násobením polynomů je obor integrity.*

Proof: ...

Polynomy nikdy nemohou tvořit těleso!

Okruh polynomů

Theorem

Buď $(R, +, \cdot)$ *těleso. Pak* $(R[x], +, \cdot)$ *se sčítáním a násobením polynomů je obor integrity.*

Proof: ...

Polynomy nikdy nemohou tvořit těleso!
... například x nemá inverzi.

Definition

Okruh $(R[x], +, \cdot)$ se nazývá *okruh polynomů nad tělesem R*.

1 Okruhy a tělesa

2 Okruhy polynomů

3 Dělitelnost na polynomech

Dělení se zbytkem

Theorem

Buď R těleso, $f \in R[x]$ polynom, $g \in R[x]$ nenulový polynom. Pak existuje právě jedna dvojice polynomů $q, r \in R[x]$ taková, že $st(r) < st(g)$ a

$$f = g \cdot q + r.$$

Proof: ...

Dělení se zbytkem

Theorem

Buď R těleso, $f \in R[x]$ polynom, $g \in R[x]$ nenulový polynom. Pak existuje právě jedna dvojice polynomů $q, r \in R[x]$ taková, že $st(r) < st(g)$ a

$$f = g \cdot q + r.$$

Proof: ...

- q ... *podíl* po dělení polynomu f polynomem g
- r ... *zbytek* po dělení polynomu f polynomem g

Příklad

Najděte podíl a zbytek při dělení polynomu f polynomem g pro

$$f = -5x^4 + 4x^2 - 3x + 4,$$
$$g = x^3 + 2x^2 - 4,$$

kde $f, g \in \mathbb{R}[x]$.

Příklad

Najděte podíl a zbytek při dělení polynomu f polynomem g pro

$$f = -5x^4 + 4x^2 - 3x + 4,$$
$$g = x^3 + 2x^2 - 4,$$

kde $f, g \in \mathbb{R}[x]$. Dostaneme

- $q = -5x + 10$
- $r = -16x^2 - 23x + 44$

Největší společný dělitel

Theorem

Buď R těleso. Pak v $R[x]$ libovolné dva nenulové polynomy mají největší společný dělitel.

Největší společný dělitel

Theorem

Buď R těleso. Pak v $R[x]$ libovolné dva nenulové polynomy mají největší společný dělitel.

- *největší společný dělitel ... je dělitelný libovolným jiným společným dělitelem.*

Proof: ... skoro stejně jako u čísel, můžeme použít Euklidův algoritmus.

Konkrétně

Najděte největší společný dělitel polynomů

$$f = x^3 - 3x^2 + 5x - 3,$$
$$g = 4x^4 + 4x^3 - 4x^2 + 20x + 24,$$

kde $f, g \in \mathbb{R}[x]$.

Konkrétně

Najděte největší společný dělitel polynomů

$$f = x^3 - 3x^2 + 5x - 3,$$
$$g = 4x^4 + 4x^3 - 4x^2 + 20x + 24,$$

kde $f, g \in \mathbb{R}[x]$.
Dostaneme polynom

$$24x^2 - 48x + 72.$$

Bezoutova rovnost

Corollary

Buď R těleso, $f, g \in R[x]$ nenulové polynomy a $h \in R[x]$ jejich největší společný dělitel. Pak existují polynomy $u, v \in R[x]$ takové, že $f \cdot u + g \cdot v = h$.

Proof ... stejně jako u čísel, můžeme použít Euklidův algoritmus.

Příklad

Najděte Bezoutovu rovnost pro polynomy z předchozího příkladu, t.j.

$$\begin{aligned} f &= x^3 - 3x^2 + 5x - 3, \\ g &= 4x^4 + 4x^3 - 4x^2 + 20x + 24. \end{aligned}$$

Příklad

Najděte Bezoutovu rovnost pro polynomy z předchozího příkladu, t.j.

$$\begin{aligned} f =& x^3 - 3x^2 + 5x - 3, \\ g =& 4x^4 + 4x^3 - 4x^2 + 20x + 24. \end{aligned}$$

Dostaneme

$$\begin{aligned} 24x^2 - 48x + 72 =& (4x^4 + 4x^3 - 4x^2 + 20x + 24) \cdot 1 \\ & -(x^3 - 3x^2 + 5x - 3) \cdot (4x + 16) \end{aligned}$$

Několik poznámek

- Je zřejmé, že největší společný dělitel dvou polynomů není určen jednoznačně.
- Dva největší společní dělitele se liší o vynásobení nenulovým prvkem z R.
- Polynom se nazývá *normovaný*, je-li jeho vedoucí koeficient roven 1.
- Pokud definujeme největší společný dělitel jako ten normovaný, pak je určen jednoznačně.