

---

# Okruhy a tělesa

Ondřej Klíma

# Vlastnosti celých čísel

---

# Vlastnosti celých čísel

---

$(\mathbb{Z}, +)$

# Vlastnosti celých čísel

---

$(\mathbb{Z}, +)$

komutativní grupa

# Vlastnosti celých čísel

---

$(\mathbb{Z}, +)$  komutativní grupa

$(\mathbb{Z}, \cdot)$

# Vlastnosti celých čísel

---

$(\mathbb{Z}, +)$

komutativní grupa

$(\mathbb{Z}, \cdot)$

monoid (asociativní  $\cdot$ , neutrální prvek 1)

# Vlastnosti celých čísel

---

$(\mathbb{Z}, +)$

komutativní grupa

$(\mathbb{Z}, \cdot)$

monoid (asociativní  $\cdot$ , neutrální prvek 1)

distributivní zákony

# Vlastnosti celých čísel

---

$(\mathbb{Z}, +)$

komutativní grupa

$(\mathbb{Z}, \cdot)$

monoid (asociativní  $\cdot$ , neutrální prvek 1)

distributivní zákony

Další vlastnosti: komutativita  $\cdot$ , uspořádání, dělitelnost, ...



# Okruhy - definice

---

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

- $(R, +)$  je komutativní grupa
- $(R, \cdot)$  je monoid
- pro libovolné  $a, b, c \in R$  platí (distributivní zákony)

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

# Okruhy - definice

---

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

- $(R, +)$  je komutativní grupa
- $(R, \cdot)$  je monoid
- pro libovolné  $a, b, c \in R$  platí (distributivní zákony)

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

Používáme aditivní terminologii pro první operaci (symbol  $+$ , neutrální prvek  $0$ , inverze  $-$ ) a multiplikativní pro druhou operaci (symbol  $\cdot$ , neutrální prvek  $1$ , případná inverze  $^{-1}$ ).

# Příklady okruhů

---

- $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$

# Příklady okruhů

---

- $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$

# Příklady okruhů

---

- $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$
- polynomy, matice

# Příklady okruhů

---

- $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$
- polynomy, matice
- $(\{a + bi \mid a, b \in \mathbb{Z}\}, +, \cdot)$  — Gaussova celá čísla

# Příklady okruhů

---

- $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$
- polynomy, matice
- $(\{a + bi \mid a, b \in \mathbb{Z}\}, +, \cdot)$  — Gaussova celá čísla
- $(\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}, +, \cdot)$

# Příklady okruhů

---

- $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$
- polynomy, matice
- $(\{a + bi \mid a, b \in \mathbb{Z}\}, +, \cdot)$  — Gaussova celá čísla
- $(\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}, +, \cdot)$
- $(\{\frac{m}{2^n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}, +, \cdot)$



# Příklady okruhů

---

- $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$
- polynomy, matice
- $(\{a + bi \mid a, b \in \mathbb{Z}\}, +, \cdot)$  — Gaussova celá čísla
- $(\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}, +, \cdot)$
- $(\{\frac{m}{2^n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}, +, \cdot)$
- $(\mathbb{P}(X), \div, \cap)$  nebo  $(\mathbb{P}(X), \div, \cup)$  ? (sami)

# Příklady okruhů

---

- $(\mathbb{Z}, +, \cdot)$ ,  $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$
- polynomy, matice
- $(\{a + bi \mid a, b \in \mathbb{Z}\}, +, \cdot)$  — Gaussova celá čísla
- $(\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}, +, \cdot)$
- $(\{\frac{m}{2^n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\}, +, \cdot)$
- $(\mathbb{P}(X), \div, \cap)$  nebo  $(\mathbb{P}(X), \div, \cup)$  ? (sami)
- $(R, +, \cdot)$  kde  $R$  je jednoprvková — triviální okruh

# Základní vlastnosti okruhů

---

$(R, +, \cdot)$  okruh, pak platí

# Základní vlastnosti okruhů

---

$(R, +, \cdot)$  okruh, pak platí

● obecná distributivita

$$a \cdot (b_1 + b_2 + \cdots + b_n) = a \cdot b_1 + a \cdot b_2 + \cdots + a \cdot b_n$$

# Základní vlastnosti okruhů

---

$(R, +, \cdot)$  okruh, pak platí

- obecná distributivita

$$a \cdot (b_1 + b_2 + \cdots + b_n) = a \cdot b_1 + a \cdot b_2 + \cdots + a \cdot b_n$$

- $a \cdot 0 = 0$  pro libovolné  $a \in R$

# Základní vlastnosti okruhů

---

$(R, +, \cdot)$  okruh, pak platí

- obecná distributivita

$$a \cdot (b_1 + b_2 + \cdots + b_n) = a \cdot b_1 + a \cdot b_2 + \cdots + a \cdot b_n$$

- $a \cdot 0 = 0$  pro libovolné  $a \in R$

- k prvku 0 neexistuje inverze vzhledem k násobení, tzn.  $(R, \cdot)$  nemůže být grupa (s výjimkou triviálního okruhu)

# Základní vlastnosti okruhů

---

$(R, +, \cdot)$  okruh, pak platí

- obecná distributivita

$$a \cdot (b_1 + b_2 + \cdots + b_n) = a \cdot b_1 + a \cdot b_2 + \cdots + a \cdot b_n$$

- $a \cdot 0 = 0$  pro libovolné  $a \in R$

- k prvku 0 neexistuje inverze vzhledem k násobení, tzn.  $(R, \cdot)$  nemůže být grupa (s výjimkou triviálního okruhu)

- $0 = 1$  právě tehdy, když  $R$  je triviální

# Základní vlastnosti okruhů

---

$(R, +, \cdot)$  okruh, pak platí

- obecná distributivita

$$a \cdot (b_1 + b_2 + \cdots + b_n) = a \cdot b_1 + a \cdot b_2 + \cdots + a \cdot b_n$$

- $a \cdot 0 = 0$  pro libovolné  $a \in R$

- k prvku 0 neexistuje inverze vzhledem k násobení, tzn.  $(R, \cdot)$  nemůže být grupa (s výjimkou triviálního okruhu)

- $0 = 1$  právě tehdy, když  $R$  je triviální  
( $a = a \cdot 1 = a \cdot 0 = 0$ )



# Základní vlastnosti okruhů

---

$(R, +, \cdot)$  okruh, pak platí

- obecná distributivita

$$a \cdot (b_1 + b_2 + \cdots + b_n) = a \cdot b_1 + a \cdot b_2 + \cdots + a \cdot b_n$$

- $a \cdot 0 = 0$  pro libovolné  $a \in R$

- k prvku 0 neexistuje inverze vzhledem k násobení, tzn.  $(R, \cdot)$  nemůže být grupa (s výjimkou triviálního okruhu)

- $0 = 1$  právě tehdy, když  $R$  je triviální  
( $a = a \cdot 1 = a \cdot 0 = 0$ )

- $a \cdot (-b) = -(a \cdot b)$  pro libovolná  $a, b \in R, \dots$

# Tělesa

---

# Tělesa

---

Netriviální komutativní okruh, kde ke každému nenulovému prvku existuje inverze vzhledem k násobení, se nazývá **těleso**.

# Tělesa

---

Netriviální komutativní okruh, kde ke každému nenulovému prvku existuje inverze vzhledem k násobení, se nazývá **těleso**.

Příklady:

# Tělesa

---

Netriviální komutativní okruh, kde ke každému nenulovému prvku existuje inverze vzhledem k násobení, se nazývá **těleso**.

Příklady:

- $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$

# Tělesa

---

Netriviální komutativní okruh, kde ke každému nenulovému prvku existuje inverze vzhledem k násobení, se nazývá **těleso**.

Příklady:

- $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$  je těleso právě tehdy, když  $n$  je prvočíslo

# Tělesa

---

Netriviální komutativní okruh, kde ke každému nenulovému prvku existuje inverze vzhledem k násobení, se nazývá **těleso**.

Příklady:

- $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$  je těleso právě tehdy, když  $n$  je prvočíslo  
( $\forall (\mathbb{Z}_6, +, \cdot)$  platí  $2 \cdot 3 = 0$ , tzn. k prvku 2 neexistuje inverze)

# Tělesa

---

Netriviální komutativní okruh, kde ke každému nenulovému prvku existuje inverze vzhledem k násobení, se nazývá **těleso**.

Příklady:

- $(\mathbb{Q}, +, \cdot)$ ,  $(\mathbb{R}, +, \cdot)$ ,  $(\mathbb{C}, +, \cdot)$
- $(\mathbb{Z}_n, +, \cdot)$  je těleso právě tehdy, když  $n$  je prvočíslo  
(V  $(\mathbb{Z}_6, +, \cdot)$  platí  $2 \cdot 3 = 0$ , tzn. k prvku 2 neexistuje inverze)
- polynomy, matice,  $(\mathbb{Z}, +, \cdot)$  — ne



# Definice v literatuře

---

**POZOR:** Odlišné definice v literatuře.

- okruh — bez 1
- okruh — komutativní
- těleso — nekomutativní
- pojem jednotka (1, resp. prvek k němuž existuje inverze vzhledem k násobení)
- **těleso = pole**

# Obor integrity

---

$(\mathbb{Z}, +, \cdot)$  není těleso (inverze pouze pro 1,  $-1$ ).

# Obor integrity

---

$(\mathbb{Z}, +, \cdot)$  není těleso (inverze pouze pro 1,  $-1$ ).

Pro libovolná nenulová čísla  $a, b$  platí

$$a \cdot b \neq 0.$$

# Obor integrity

---

$(\mathbb{Z}, +, \cdot)$  není těleso (inverze pouze pro 1,  $-1$ ).

Pro libovolná nenulová čísla  $a, b$  platí

$$a \cdot b \neq 0.$$

$\forall (\mathbb{Z}_6, +, \cdot)$  tato vlastnost neplatí.

# Obor integrity

---

$(\mathbb{Z}, +, \cdot)$  není těleso (inverze pouze pro 1,  $-1$ ).

Pro libovolná nenulová čísla  $a, b$  platí

$$a \cdot b \neq 0.$$

$\forall (\mathbb{Z}_6, +, \cdot)$  tato vlastnost neplatí.

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

# Obor integrity

---

$(\mathbb{Z}, +, \cdot)$  není těleso (inverze pouze pro  $1, -1$ ).

Pro libovolná nenulová čísla  $a, b$  platí

$$a \cdot b \neq 0.$$

$\forall (\mathbb{Z}_6, +, \cdot)$  tato vlastnost neplatí.

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

Každé těleso je obor integrity.

# Obor integrity

---

$(\mathbb{Z}, +, \cdot)$  není těleso (inverze pouze pro 1,  $-1$ ).

Pro libovolná nenulová čísla  $a, b$  platí

$$a \cdot b \neq 0.$$

$\forall (\mathbb{Z}_6, +, \cdot)$  tato vlastnost neplatí.

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

Každé těleso je obor integrity.

$(\mathbb{Z}_n, +, \cdot)$  obor integrity právě tehdy, když  $n$  je prvočíslo.

# Obor integrity

---

$(\mathbb{Z}, +, \cdot)$  není těleso (inverze pouze pro 1,  $-1$ ).

Pro libovolná nenulová čísla  $a, b$  platí

$$a \cdot b \neq 0.$$

$\forall (\mathbb{Z}_6, +, \cdot)$  tato vlastnost neplatí.

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

Každé těleso je obor integrity.

$(\mathbb{Z}_n, +, \cdot)$  obor integrity právě tehdy, když  $n$  je prvočíslo.

$(\mathbb{Z}, +, \cdot)$  obor integrity, polynomy (nad o.i.) ano, matice ne.



# Zákony o krácení

---

Další zajímavá vlastnost celých čísel:

$$a \cdot b = a \cdot c \implies b = c$$

pro libovolná celá čísla  $a, b, c$

# Zákony o krácení

---

Další zajímavá vlastnost celých čísel:

$$a \cdot b = a \cdot c \implies b = c$$

pro libovolná celá čísla  $a, b, c$  ( $a \neq 0$ ).

# Zákony o krácení

---

Další zajímavá vlastnost celých čísel:

$$a \cdot b = a \cdot c \implies b = c$$

pro libovolná celá čísla  $a, b, c$  ( $a \neq 0$ ).

V  $(\mathbb{Z}_6, +, \cdot)$  neplatí.

# Zákony o krácení

---

Další zajímavá vlastnost celých čísel:

$$a \cdot b = a \cdot c \implies b = c$$

pro libovolná celá čísla  $a, b, c$  ( $a \neq 0$ ).

V  $(\mathbb{Z}_6, +, \cdot)$  neplatí.

Souvislost s předchozí vlastností:

# Zákony o krácení

---

Další zajímavá vlastnost celých čísel:

$$a \cdot b = a \cdot c \implies b = c$$

pro libovolná celá čísla  $a, b, c$  ( $a \neq 0$ ).

V  $(\mathbb{Z}_6, +, \cdot)$  neplatí.

Souvislost s předchozí vlastností:

$$a \cdot b = a \cdot c \implies a \cdot (b - c) = 0 \implies b - c = 0 \implies b = c$$

# Zákony o krácení

---

Další zajímavá vlastnost celých čísel:

$$a \cdot b = a \cdot c \implies b = c$$

pro libovolná celá čísla  $a, b, c$  ( $a \neq 0$ ).

V  $(\mathbb{Z}_6, +, \cdot)$  neplatí.

Souvislost s předchozí vlastností:

$$a \cdot b = a \cdot c \implies a \cdot (b - c) = 0 \implies b - c = 0 \implies b = c$$

Netriviální komutativní okruh  $(R, +, \cdot)$  je obor integrity právě tehdy, když splňuje zákon o krácení:

$$(\forall a, b, c \in R)(a \neq 0, a \cdot b = a \cdot c \implies b = c).$$

# Význam oborů integrity

---

# Význam oborů integrity

---

Z okruhu  $(\mathbb{Z}, +, \cdot)$  lze "zkonstruovat" těleso  $(\mathbb{Q}, +, \cdot)$  "přidáním" inverzí vzhledem k násobení.  
Přesněji, uvažujeme "zlomky".



# Význam oborů integrity

---

Z okruhu  $(\mathbb{Z}, +, \cdot)$  lze "zkonstruovat" těleso  $(\mathbb{Q}, +, \cdot)$  "přidáním" inverzí vzhledem k násobení.

Přesněji, uvažujeme "zlomky".

Z okruhu  $(\mathbb{Z}_6, +, \cdot)$  těleso "vyrobit" nelze.

# Význam oborů integrity

---

Z okruhu  $(\mathbb{Z}, +, \cdot)$  lze "zkonstruovat" těleso  $(\mathbb{Q}, +, \cdot)$  "přidáním" inverzí vzhledem k násobení.

Přesněji, uvažujeme "zlomky".

Z okruhu  $(\mathbb{Z}_6, +, \cdot)$  těleso "vyrobit" nelze.

Konstrukce (podílového tělesa) oboru integrity  $(R, +, \cdot)$  :

# Význam oborů integrity

---

Z okruhu  $(\mathbb{Z}, +, \cdot)$  lze "zkonstruovat" těleso  $(\mathbb{Q}, +, \cdot)$  "přidáním" inverzí vzhledem k násobení.

Přesněji, uvažujeme "zlomky".

Z okruhu  $(\mathbb{Z}_6, +, \cdot)$  těleso "vyrobit" nelze.

Konstrukce (podílového tělesa) oboru integrity  $(R, +, \cdot)$  :

- množina  $R \times (R - \{0\})$
- relace ekvivalence  $(a, b) \equiv (c, d) \iff a \cdot d = b \cdot c$

# Význam oborů integrity

---

Z okruhu  $(\mathbb{Z}, +, \cdot)$  lze "zkonstruovat" těleso  $(\mathbb{Q}, +, \cdot)$  "přidáním" inverzí vzhledem k násobení.

Přesněji, uvažujeme "zlomky".

Z okruhu  $(\mathbb{Z}_6, +, \cdot)$  těleso "vyrobit" nelze.

Konstrukce (podílového tělesa) oboru integrity  $(R, +, \cdot)$  :

- množina  $R \times (R - \{0\})$
- relace ekvivalence  $(a, b) \equiv (c, d) \iff a \cdot d = b \cdot c$
- nové operace  $+$ ,  $\cdot$  na rozkladu  $R \times (R - \{0\}) / \equiv$  se definují očekávaným způsobem.

# Podokruhy

---

Podmnožina  $M$  okruhu  $(R, +, \cdot)$  se nazývá **podokruh** pokud je uzavřena na všechny operace, přesněji pokud platí

# Podokruhy

---

Podmnožina  $M$  okruhu  $(R, +, \cdot)$  se nazývá **podokruh** pokud je uzavřena na všechny operace, přesněji pokud platí

- $0 \in M$
- $a, b \in M \implies a + b \in M$
- $a \in M \implies -a \in M$

# Podokruhy

---

Podmnožina  $M$  okruhu  $(R, +, \cdot)$  se nazývá **podokruh** pokud je uzavřena na všechny operace, přesněji pokud platí

- $0 \in M$
- $a, b \in M \implies a + b \in M$
- $a \in M \implies -a \in M$
- $1 \in M$
- $a, b \in M \implies a \cdot b \in M$

# Podokruhy

---

Podmnožina  $M$  okruhu  $(R, +, \cdot)$  se nazývá **podokruh** pokud je uzavřena na všechny operace, přesněji pokud platí

- $0 \in M$
- $a, b \in M \implies a + b \in M$
- $a \in M \implies -a \in M$
- $1 \in M$
- $a, b \in M \implies a \cdot b \in M$

Příklady — podokruhy okruhu  $(\mathbb{C}, +, \cdot)$ ,  
"speciální" matice (např horní trojúhelníkový tvar).



# Podokruhy

---

Podmnožina  $M$  okruhu  $(R, +, \cdot)$  se nazývá **podokruh** pokud je uzavřena na všechny operace, přesněji pokud platí

- $0 \in M$
- $a, b \in M \implies a + b \in M$
- $a \in M \implies -a \in M$
- $1 \in M$
- $a, b \in M \implies a \cdot b \in M$

Příklady — podokruhy okruhu  $(\mathbb{C}, +, \cdot)$ ,  
"speciální" matice (např horní trojúhelníkový tvar).

Podokruh okruhu je opět okruhem (pokud uvažujeme "stejně" operace).

# Podtělesa

---

Podokruh oboru integrity je obor integrity, ale podokruh tělesa nemusí být těleso.

# Podtělesa

---

Podokruh oboru integrity je obor integrity, ale podokruh tělesa nemusí být těleso.

$\mathbb{Z}$  je podokruh  $(\mathbb{C}, +, \cdot)$ .

# Podtělesa

---

Podokruh oboru integrity je obor integrity, ale podokruh tělesa nemusí být těleso.

$\mathbb{Z}$  je podokruh  $(\mathbb{C}, +, \cdot)$ .

Podokruh  $M$  tělesa  $(R, +, \cdot)$  se nazývá **podtěleso** právě tehdy, když pro libovolný nenulový prvek  $a \in R$  platí

$$a \in M \implies a^{-1} \in M.$$

# Podtělesa

---

Podokruh oboru integrity je obor integrity, ale podokruh tělesa nemusí být těleso.

$\mathbb{Z}$  je podokruh  $(\mathbb{C}, +, \cdot)$ .

Podokruh  $M$  tělesa  $(R, +, \cdot)$  se nazývá **podtěleso** právě tehdy, když pro libovolný nenulový prvek  $a \in R$  platí

$$a \in M \implies a^{-1} \in M.$$

Příklady:  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ .

# Podtělesa

---

Podokruh oboru integrity je obor integrity, ale podokruh tělesa nemusí být těleso.

$\mathbb{Z}$  je podokruh  $(\mathbb{C}, +, \cdot)$ .

Podokruh  $M$  tělesa  $(R, +, \cdot)$  se nazývá **podtěleso** právě tehdy, když pro libovolný nenulový prvek  $a \in R$  platí

$$a \in M \implies a^{-1} \in M.$$

Příklady:  $\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$ .

Rozmyslete si  $\{a + bi \mid a, b \in \mathbb{Z}\}$ ,  $\{a + bi \mid a, b \in \mathbb{Q}\}$ ,  
 $\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ .

# Homomorfismy okruhů

---

# Homomorfismy okruhů

---

Zobrazení  $f : R \rightarrow S$  se nazývá homomorfismus okruhů  $(R, +, \cdot)$  a  $(S, \oplus, \odot)$  pokud "zachovává" operace, tj. pokud platí:



# Homomorfismy okruhů

---

Zobrazení  $f : R \rightarrow S$  se nazývá homomorfismus okruhů  $(R, +, \cdot)$  a  $(S, \oplus, \odot)$  pokud "zachovává" operace, tj. pokud platí:

- $f(a + b) = f(a) \oplus f(b)$  pro  $a, b \in R$

# Homomorfismy okruhů

---

Zobrazení  $f : R \rightarrow S$  se nazývá homomorfismus okruhů  $(R, +, \cdot)$  a  $(S, \oplus, \odot)$  pokud "zachovává" operace, tj. pokud platí:

- $f(a + b) = f(a) \oplus f(b)$  pro  $a, b \in R$
- $f(a \cdot b) = f(a) \odot f(b)$  pro  $a, b \in R$

# Homomorfismy okruhů

---

Zobrazení  $f : R \rightarrow S$  se nazývá homomorfismus okruhů  $(R, +, \cdot)$  a  $(S, \oplus, \odot)$  pokud "zachovává" operace, tj. pokud platí:

- $f(a + b) = f(a) \oplus f(b)$  pro  $a, b \in R$
- $f(a \cdot b) = f(a) \odot f(b)$  pro  $a, b \in R$
- $f(1_R) = 1_S$ .

# Homomorfismy okruhů

---

Zobrazení  $f : R \rightarrow S$  se nazývá homomorfismus okruhů  $(R, +, \cdot)$  a  $(S, \oplus, \odot)$  pokud "zachovává" operace, tj. pokud platí:

- $f(a + b) = f(a) \oplus f(b)$  pro  $a, b \in R$
- $f(a \cdot b) = f(a) \odot f(b)$  pro  $a, b \in R$
- $f(1_R) = 1_S$ .

Další vlastnosti:

# Homomorfismy okruhů

---

Zobrazení  $f : R \rightarrow S$  se nazývá homomorfismus okruhů  $(R, +, \cdot)$  a  $(S, \oplus, \odot)$  pokud "zachovává" operace, tj. pokud platí:

- $f(a + b) = f(a) \oplus f(b)$  pro  $a, b \in R$
- $f(a \cdot b) = f(a) \odot f(b)$  pro  $a, b \in R$
- $f(1_R) = 1_S$ .

Další vlastnosti:

- $f(0_R) = 0_S$

# Homomorfismy okruhů

---

Zobrazení  $f : R \rightarrow S$  se nazývá homomorfismus okruhů  $(R, +, \cdot)$  a  $(S, \oplus, \odot)$  pokud "zachovává" operace, tj. pokud platí:

- $f(a + b) = f(a) \oplus f(b)$  pro  $a, b \in R$
- $f(a \cdot b) = f(a) \odot f(b)$  pro  $a, b \in R$
- $f(1_R) = 1_S$ .

Další vlastnosti:

- $f(0_R) = 0_S$
- $f(-a) = \ominus f(a)$  pro  $a \in R$

# Homomorfismy okruhů

---

Zobrazení  $f : R \rightarrow S$  se nazývá homomorfismus okruhů  $(R, +, \cdot)$  a  $(S, \oplus, \odot)$  pokud "zachovává" operace, tj. pokud platí:

- $f(a + b) = f(a) \oplus f(b)$  pro  $a, b \in R$
- $f(a \cdot b) = f(a) \odot f(b)$  pro  $a, b \in R$
- $f(1_R) = 1_S$ .

Další vlastnosti:

- $f(0_R) = 0_S$
- $f(-a) = \ominus f(a)$  pro  $a \in R$

Bijektivním homomorfismům říkáme izomorfismy a dva okruhy jsou izomorfní pokud existuje izomorfismus mezi nimi.

# Příklady homomorfismů

---



# Příklady homomorfismů

---

Příkladem homomorfismu je komplexní konjugovanost, tj.  $f : \mathbb{C} \rightarrow \mathbb{C}$ ,  $f(a + bi) = a - bi$  je izomorfismus okruhu  $(\mathbb{C}, +, \cdot)$  na sebe.

# Příklady homomorfismů

---

Příkladem homomorfismu je komplexní konjugovanost, tj.  $f : \mathbb{C} \rightarrow \mathbb{C}$ ,  $f(a + bi) = a - bi$  je izomorfismus okruhu  $(\mathbb{C}, +, \cdot)$  na sebe.

Dále  $g : \mathbb{Z} \rightarrow \mathbb{Z}_n$ ,  $g(a) = [a]_n$  je homomorfismus okruhu  $(\mathbb{Z}, +, \cdot)$  do okruhu  $(\mathbb{Z}_n, +, \cdot)$ .

# Příklady homomorfismů

---

Příkladem homomorfismu je komplexní konjugovanost, tj.  $f : \mathbb{C} \rightarrow \mathbb{C}$ ,  $f(a + bi) = a - bi$  je izomorfismus okruhu  $(\mathbb{C}, +, \cdot)$  na sebe.

Dále  $g : \mathbb{Z} \rightarrow \mathbb{Z}_n$ ,  $g(a) = [a]_n$  je homomorfismus okruhu  $(\mathbb{Z}, +, \cdot)$  do okruhu  $(\mathbb{Z}_n, +, \cdot)$ .

Další příklady u polynomů (hodnota polynomu v bodě).

# Příklady homomorfismů

---

Příkladem homomorfismu je komplexní konjugovanost, tj.  $f : \mathbb{C} \rightarrow \mathbb{C}$ ,  $f(a + bi) = a - bi$  je izomorfismus okruhu  $(\mathbb{C}, +, \cdot)$  na sebe.

Dále  $g : \mathbb{Z} \rightarrow \mathbb{Z}_n$ ,  $g(a) = [a]_n$  je homomorfismus okruhu  $(\mathbb{Z}, +, \cdot)$  do okruhu  $(\mathbb{Z}_n, +, \cdot)$ .

Další příklady u polynomů (hodnota polynomu v bodě).  
Základní vlastnosti:

# Příklady homomorfismů

---

Příkladem homomorfismu je komplexní konjugovanost, tj.  $f : \mathbb{C} \rightarrow \mathbb{C}$ ,  $f(a + bi) = a - bi$  je izomorfismus okruhu  $(\mathbb{C}, +, \cdot)$  na sebe.

Dále  $g : \mathbb{Z} \rightarrow \mathbb{Z}_n$ ,  $g(a) = [a]_n$  je homomorfismus okruhu  $(\mathbb{Z}, +, \cdot)$  do okruhu  $(\mathbb{Z}_n, +, \cdot)$ .

Další příklady u polynomů (hodnota polynomu v bodě).

Základní vlastnosti:

- složení homomorfismů je homomorfismus

# Příklady homomorfismů

---

Příkladem homomorfismu je komplexní konjugovanost, tj.  $f : \mathbb{C} \rightarrow \mathbb{C}$ ,  $f(a + bi) = a - bi$  je izomorfismus okruhu  $(\mathbb{C}, +, \cdot)$  na sebe.

Dále  $g : \mathbb{Z} \rightarrow \mathbb{Z}_n$ ,  $g(a) = [a]_n$  je homomorfismus okruhu  $(\mathbb{Z}, +, \cdot)$  do okruhu  $(\mathbb{Z}_n, +, \cdot)$ .

Další příklady u polynomů (hodnota polynomu v bodě).

Základní vlastnosti:

- složení homomorfismů je homomorfismus
- obraz homomorfismu je podokruh

# Příklady homomorfismů

---

Příkladem homomorfismu je komplexní konjugovanost, tj.  $f : \mathbb{C} \rightarrow \mathbb{C}$ ,  $f(a + bi) = a - bi$  je izomorfismus okruhu  $(\mathbb{C}, +, \cdot)$  na sebe.

Dále  $g : \mathbb{Z} \rightarrow \mathbb{Z}_n$ ,  $g(a) = [a]_n$  je homomorfismus okruhu  $(\mathbb{Z}, +, \cdot)$  do okruhu  $(\mathbb{Z}_n, +, \cdot)$ .

Další příklady u polynomů (hodnota polynomu v bodě).  
Základní vlastnosti:

- složení homomorfismů je homomorfismus
- obraz homomorfismu je podokruh
- homomorfismus mezi tělesy je prostý

# Věta o podílovém tělese

---

Pro komutativní okruh  $(R, +, \cdot)$  jsou následující podmínky ekvivalentní

- existuje těleso  $(T, \oplus, \odot)$  a injektivní homomorfismus okruhů  $f : R \rightarrow T$ ,
- $(R, +, \cdot)$  je obor integrity.



# Věta o podílovém tělese

---

Pro komutativní okruh  $(R, +, \cdot)$  jsou následující podmínky ekvivalentní

- existuje těleso  $(T, \oplus, \odot)$  a injektivní homomorfismus okruhů  $f : R \rightarrow T$ ,
- $(R, +, \cdot)$  je obor integrity.

Podílové těleso je dokonce "nejmenší možné".

# Věta o podílovém tělese

---

Pro komutativní okruh  $(R, +, \cdot)$  jsou následující podmínky ekvivalentní

- existuje těleso  $(T, \oplus, \odot)$  a injektivní homomorfismus okruhů  $f : R \rightarrow T$ ,
- $(R, +, \cdot)$  je obor integrity.

Podílové těleso je dokonce "nejmenší možné".

Pro podílové těleso  $Q(R)$  oboru integrity  $R$  a těleso  $T$  z předchozí věty existuje injektivní homomorfismus okruhů  $f : Q(R) \rightarrow T$ .

# Věta o podílovém tělese

---

Pro komutativní okruh  $(R, +, \cdot)$  jsou následující podmínky ekvivalentní

- existuje těleso  $(T, \oplus, \odot)$  a injektivní homomorfismus okruhů  $f : R \rightarrow T$ ,
- $(R, +, \cdot)$  je obor integrity.

Podílové těleso je dokonce "nejmenší možné".

Pro podílové těleso  $Q(R)$  oboru integrity  $R$  a těleso  $T$  z předchozí věty existuje injektivní homomorfismus okruhů

$$f : Q(R) \rightarrow T.$$

Podílové těleso je určeno jednoznačně až na izomorfismus

# Shrnutí

---

# Shrnutí

---

Co se bude požadovat:

# Shrnutí

---

Co se bude požadovat:

- počítání v  $\mathbb{C}$  (cvičení)

# Shrnutí

---

Co se bude požadovat:

- počítání v  $\mathbb{C}$  (cvičení)
- okruh, obor integrity, těleso, podokruh, homomorfismus okruhů

# Shrnutí

---

Co se bude požadovat:

- počítání v  $\mathbb{C}$  (cvičení)
- okruh, obor integrity, těleso, podokruh, homomorfismus okruhů
- Tvoří množina  $\{a + b\sqrt[3]{5} \mid a, b \in \mathbb{Z}\}$  podokruh okruhu  $(\mathbb{C}, +, \cdot)$  ?



# Shrnutí

---

Co se bude požadovat:

- počítání v  $\mathbb{C}$  (cvičení)
- okruh, obor integrity, těleso, podokruh, homomorfismus okruhů
- Tvoří množina  $\{a + b\sqrt[3]{5} \mid a, b \in \mathbb{Z}\}$  podokruh okruhu  $(\mathbb{C}, +, \cdot)$  ?
- Je zobrazení  $f : \mathbb{C} \rightarrow \mathbb{R}$  dané předpisem  $f(a + bi) = a^2 + b^2$  homomorfismus okruhů ?

# Shrnutí

---

Co se bude požadovat:

- počítání v  $\mathbb{C}$  (cvičení)
- okruh, obor integrity, těleso, podokruh, homomorfismus okruhů
- Tvoří množina  $\{a + b\sqrt[3]{5} \mid a, b \in \mathbb{Z}\}$  podokruh okruhu  $(\mathbb{C}, +, \cdot)$  ?
- Je zobrazení  $f : \mathbb{C} \rightarrow \mathbb{R}$  dané předpisem  $f(a + bi) = a^2 + b^2$  homomorfismus okruhů ?

Co se nebude požadovat :

# Shrnutí

---

Co se bude požadovat:

- počítání v  $\mathbb{C}$  (cvičení)
- okruh, obor integrity, těleso, podokruh, homomorfismus okruhů
- Tvoří množina  $\{a + b\sqrt[3]{5} \mid a, b \in \mathbb{Z}\}$  podokruh okruhu  $(\mathbb{C}, +, \cdot)$  ?
- Je zobrazení  $f : \mathbb{C} \rightarrow \mathbb{R}$  dané předpisem  $f(a + bi) = a^2 + b^2$  homomorfismus okruhů ?

Co se nebude požadovat :    podílové těleso .