Okruhy

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

Okruhy

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

- $(R, +)$ je komutativní grupa,

Okruhy

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

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,

Okruhy

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

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je
  $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$
  (užíváme obvyklou konvenci o tom, že násobení má přednost před sčítáním).

Okruhy

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

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$ (užíváme obvyklou konvenci o tom, že násobení má přednost před sčítáním).

Příklady. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ jsou okruhy.

Okruhy

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

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$ (užíváme obvyklou konvenci o tom, že násobení má přednost před sčítáním).

Příklady. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ jsou okruhy.
Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, +, \cdot)$ okruh.

Okruhy

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

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$ (užíváme obvyklou konvenci o tom, že násobení má přednost před sčítáním).

Příklady. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ jsou okruhy.
Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, +, \cdot)$ okruh.
Množina všech čtvercových matic $M_{n,n}(R)$, kde R značí $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$ a $n \in \mathbb{N}$, tvoří okruh $(M_{n,n}(R), +, \cdot)$.

Okruhy

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

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$ (užíváme obvyklou konvenci o tom, že násobení má přednost před sčítáním).

Příklady. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ jsou okruhy.
Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, +, \cdot)$ okruh.
Množina všech čtvercových matic $M_{n,n}(R)$, kde R značí $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$ a $n \in \mathbb{N}$, tvoří okruh $(M_{n,n}(R), +, \cdot)$.
Množina všech polynomů $R[x]$, kde R značí $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$, tvoří okruh $(R[x], +, \cdot)$.

Okruhy

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

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a$ (užíváme obvyklou konvenci o tom, že násobení má přednost před sčítáním).

Příklady. $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ jsou okruhy.
Pro libovolné $m \in \mathbb{N}$ je $(\mathbb{Z}_m, +, \cdot)$ okruh.
Množina všech čtvercových matic $M_{n,n}(R)$, kde R značí $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$ a $n \in \mathbb{N}$, tvoří okruh $(M_{n,n}(R), +, \cdot)$.
Množina všech polynomů $R[x]$, kde R značí $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ nebo $\mathbb{C}$, tvoří okruh $(R[x], +, \cdot)$.

Příklad. $(\mathbb{N}, +, \cdot)$ okruhem není.

Okruhy

Definice. $(R, +, \cdot)$ je **okruh**, jestliže:

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$

Označení. Neutrální prvek grupy $(R, +)$ značíme 0 a nazýváme **nula okruhu** R, zatímco neutrální prvek pologrupy $(R, \cdot)$ značíme 1 a nazýváme **jednička okruhu** R.

Okruhy

Definice. $(R, +, \cdot)$ je **okruh**, jestliže:

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$

Označení. Neutrální prvek grupy $(R, +)$ značíme 0 a nazýváme **nula okruhu** R, zatímco neutrální prvek pologrupy $(R, \cdot)$ značíme 1 a nazýváme **jednička okruhu** R.
Inverzní prvek k prvku $a \in R$ v grupě $(R, +)$ se nazývá **opačný prvek**, značíme $-a$.

Okruhy

Definice. $(R, +, \cdot)$ je **okruh**, jestliže:

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$

Označení. Neutrální prvek grupy $(R, +)$ značíme 0 a nazýváme **nula okruhu** R, zatímco neutrální prvek pologrupy $(R, \cdot)$ značíme 1 a nazýváme **jednička okruhu** R.
Inverzní prvek k prvku $a \in R$ v grupě $(R, +)$ se nazývá **opačný prvek**, značíme $-a$.
Symbolem $a - b$ rozumíme $a + (-b)$.

Okruhy

Definice. $(R, +, \cdot)$ je **okruh**, jestliže:

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$

Označení. Neutrální prvek grupy $(R, +)$ značíme 0 a nazýváme **nula okruhu** R, zatímco neutrální prvek pologrupy $(R, \cdot)$ značíme 1 a nazýváme **jednička okruhu** R.
Inverzní prvek k prvku $a \in R$ v grupě $(R, +)$ se nazývá **opačný prvek**, značíme $-a$.
Symbolem $a - b$ rozumíme $a + (-b)$.
Mocninu prvku $a \in R$ v grupě $(R, +)$ nazýváme **násobek prvku** a značíme na pro libovolné $n \in \mathbb{Z}$.

Okruhy

Definice. $(R, +, \cdot)$ je **okruh**, jestliže:

- $(R, +)$ je komutativní grupa,
- $(R, \cdot)$ je pologrupa s neutrálním prvkem,
- platí distributivní zákony, tj. pro libovolné prvky $a, b, c \in R$ je $a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a.$

Označení. Neutrální prvek grupy $(R, +)$ značíme 0 a nazýváme **nula okruhu** R, zatímco neutrální prvek pologrupy $(R, \cdot)$ značíme 1 a nazýváme **jednička okruhu** R.
Inverzní prvek k prvku $a \in R$ v grupě $(R, +)$ se nazývá **opačný prvek**, značíme $-a$.
Symbolem $a - b$ rozumíme $a + (-b)$.
Mocninu prvku $a \in R$ v grupě $(R, +)$ nazýváme **násobek prvku** a značíme na pro libovolné $n \in \mathbb{Z}$.
Součet $a_1 + \cdots + a_n$ prvků okruhu R lze stručně zapsat $\sum_{i=1}^{n} a_i$.

Základní vlastnosti okruhů

Definice. Okruh $(R, +, \cdot)$ se nazývá **triviální**, má-li R jediný prvek.

Základní vlastnosti okruhů

Definice. Okruh $(R, +, \cdot)$ se nazývá **triviální**, má-li R jediný prvek.

Věta. Nechť R je okruh. Pak platí

- $\forall a \in R: \ a \cdot 0 = 0 \cdot a = 0$,

Základní vlastnosti okruhů

Definice. Okruh $(R, +, \cdot)$ se nazývá **triviální**, má-li R jediný prvek.

Věta. Nechť R je okruh. Pak platí

- $\forall a \in R : \ a \cdot 0 = 0 \cdot a = 0$,
- $\forall a, b \in R : \ (-a) \cdot b = a \cdot (-b) = -(a \cdot b)$,

Základní vlastnosti okruhů

Definice. Okruh $(R, +, \cdot)$ se nazývá **triviální**, má-li R jediný prvek.

Věta. Nechť R je okruh. Pak platí

- $\forall a \in R : \ a \cdot 0 = 0 \cdot a = 0,$
- $\forall a, b \in R : \ (-a) \cdot b = a \cdot (-b) = -(a \cdot b),$
- $\forall a, b, c \in R :$
  $a \cdot (b - c) = a \cdot b - a \cdot c, \quad (b - c) \cdot a = b \cdot a - c \cdot a,$

Základní vlastnosti okruhů

Definice. Okruh $(R, +, \cdot)$ se nazývá **triviální**, má-li R jediný prvek.

Věta. *Nechť R je okruh. Pak platí*

- $\forall a \in R: \ a \cdot 0 = 0 \cdot a = 0,$
- $\forall a, b \in R: \ (-a) \cdot b = a \cdot (-b) = -(a \cdot b),$
- $\forall a, b, c \in R:$
  $a \cdot (b - c) = a \cdot b - a \cdot c, \quad (b - c) \cdot a = b \cdot a - c \cdot a,$
- $\forall n, m \in \mathbb{N} \ \forall a_1, \ldots, a_n, b_1, \ldots, b_m \in R:$
  $(a_1 + \cdots + a_n) \cdot (b_1 + \cdots + b_m) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \cdot b_j,$

Základní vlastnosti okruhů

Definice. Okruh $(R, +, \cdot)$ se nazývá **triviální**, má-li R jediný prvek.

Věta. *Nechť R je okruh. Pak platí*

- $\forall a \in R: \ a \cdot 0 = 0 \cdot a = 0$,
- $\forall a, b \in R: \ (-a) \cdot b = a \cdot (-b) = -(a \cdot b)$,
- $\forall a, b, c \in R:$
  $a \cdot (b - c) = a \cdot b - a \cdot c, \quad (b - c) \cdot a = b \cdot a - c \cdot a$,
- $\forall n, m \in \mathbb{N} \ \forall a_1, \ldots, a_n, b_1, \ldots, b_m \in R:$
  $(a_1 + \cdots + a_n) \cdot (b_1 + \cdots + b_m) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \cdot b_j$,
- $\forall n, m \in \mathbb{Z} \ \forall a, b \in R: \ (na) \cdot (mb) = (n \cdot m)(a \cdot b)$.

Základní vlastnosti okruhů

Definice. Okruh $(R, +, \cdot)$ se nazývá **triviální**, má-li R jediný prvek.

Věta. *Nechť R je okruh. Pak platí*

- $\forall a \in R: \ a \cdot 0 = 0 \cdot a = 0$,
- $\forall a, b \in R: \ (-a) \cdot b = a \cdot (-b) = -(a \cdot b)$,
- $\forall a, b, c \in R:$
  $a \cdot (b - c) = a \cdot b - a \cdot c, \quad (b - c) \cdot a = b \cdot a - c \cdot a$,
- $\forall n, m \in \mathbb{N} \ \forall a_1, \ldots, a_n, b_1, \ldots, b_m \in R:$
  $(a_1 + \cdots + a_n) \cdot (b_1 + \cdots + b_m) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \cdot b_j$,
- $\forall n, m \in \mathbb{Z} \ \forall a, b \in R: \ (na) \cdot (mb) = (n \cdot m)(a \cdot b)$. [Věta 1.6, str. 58]

Věta. *Okruh R je triviální, právě když v něm platí $1 = 0$.*

Základní vlastnosti okruhů

Definice. Okruh $(R, +, \cdot)$ se nazývá **triviální**, má-li R jediný prvek.

Věta. *Nechť R je okruh. Pak platí*

- $\forall a \in R: \ a \cdot 0 = 0 \cdot a = 0$,
- $\forall a, b \in R: \ (-a) \cdot b = a \cdot (-b) = -(a \cdot b)$,
- $\forall a, b, c \in R:$
  $a \cdot (b - c) = a \cdot b - a \cdot c, \quad (b - c) \cdot a = b \cdot a - c \cdot a$,
- $\forall n, m \in \mathbb{N} \ \forall a_1, \ldots, a_n, b_1, \ldots, b_m \in R:$
  $(a_1 + \cdots + a_n) \cdot (b_1 + \cdots + b_m) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \cdot b_j$,
- $\forall n, m \in \mathbb{Z} \ \forall a, b \in R: \ (na) \cdot (mb) = (n \cdot m)(a \cdot b)$. [Věta 1.6, str. 58]

Věta. *Okruh R je triviální, právě když v něm platí $1 = 0$.* [Věta 1.7, str. 59]

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

Základní vlastnosti okruhů

Definice. Okruh $(R, +, \cdot)$ se nazývá **triviální**, má-li R jediný prvek.

Věta. *Nechť R je okruh. Pak platí*

- $\forall a \in R: \ a \cdot 0 = 0 \cdot a = 0$,
- $\forall a, b \in R: \ (-a) \cdot b = a \cdot (-b) = -(a \cdot b)$,
- $\forall a, b, c \in R:$
  $a \cdot (b - c) = a \cdot b - a \cdot c, \quad (b - c) \cdot a = b \cdot a - c \cdot a$,
- $\forall n, m \in \mathbb{N} \ \forall a_1, \ldots, a_n, b_1, \ldots, b_m \in R:$
  $(a_1 + \cdots + a_n) \cdot (b_1 + \cdots + b_m) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i \cdot b_j$,
- $\forall n, m \in \mathbb{Z} \ \forall a, b \in R: \ (na) \cdot (mb) = (n \cdot m)(a \cdot b)$. [Věta 1.6, str. 58]

Věta. *Okruh R je triviální, právě když v něm platí $1 = 0$.* [Věta 1.7, str. 59]

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

Definice. Prvky a, b okruhu R se nazývají **dělitelé nuly**, jestliže $a \neq 0$, $b \neq 0$, avšak $a \cdot b = 0$.

Obory integrity

Definice. Netriviální komutativní okruh R se nazývá **obor integrity**, pokud nemá dělitele nuly.

Obory integrity

Definice. Netriviální komutativní okruh R se nazývá **obor integrity**, pokud nemá dělitele nuly.

Označení. Množinu všech nenulových prvků okruhu R značíme R^*.

Obory integrity

Definice. Netriviální komutativní okruh R se nazývá **obor integrity**, pokud nemá dělitele nuly.

Označení. Množinu všech nenulových prvků okruhu R značíme R^*.

Poznámka. Netriviální komutativní okruh R je tedy obor integrity, právě když $(R^*, \cdot)$ je pologrupa.

Obory integrity

Definice. Netriviální komutativní okruh R se nazývá **obor integrity**, pokud nemá dělitele nuly.

Označení. Množinu všech nenulových prvků okruhu R značíme R^*.

Poznámka. Netriviální komutativní okruh R je tedy obor integrity, právě když $(R^*, \cdot)$ je pologrupa.

Věta. Netriviální komutativní okruh R je obor integrity, právě když v něm platí **zákon o krácení**, *tj. pro každé $a, b, c \in R$ platí*

$$a \neq 0, \ a \cdot b = a \cdot c \quad \Rightarrow \quad b = c.$$

[Věta 1.10, str. 59]

Obory integrity

Definice. Netriviální komutativní okruh R se nazývá **obor integrity**, pokud nemá dělitele nuly.

Označení. Množinu všech nenulových prvků okruhu R značíme R^*.

Poznámka. Netriviální komutativní okruh R je tedy obor integrity, právě když $(R^*, \cdot)$ je pologrupa.

Věta. Netriviální komutativní okruh R je obor integrity, právě když v něm platí **zákon o krácení**, *tj. pro každé $a, b, c \in R$ platí*

$$a \neq 0, \ a \cdot b = a \cdot c \quad \Rightarrow \quad b = c.$$ [Věta 1.10, str. 59]

Definice. Nechť R je okruh. Invertibilní prvek pologrupy $(R, \cdot)$ se nazývá **jednotka** okruhu R. Množinu všech jednotek okruhu R značíme $R^\times$.

Obory integrity

Definice. Netriviální komutativní okruh R se nazývá **obor integrity**, pokud nemá dělitele nuly.

Označení. Množinu všech nenulových prvků okruhu R značíme R^*.

Poznámka. Netriviální komutativní okruh R je tedy obor integrity, právě když $(R^*, \cdot)$ je pologrupa.

Věta. Netriviální komutativní okruh R je obor integrity, právě když v něm platí **zákon o krácení**, *tj. pro každé $a, b, c \in R$ platí*

$$a \neq 0, \ a \cdot b = a \cdot c \quad \Rightarrow \quad b = c.$$ [Věta 1.10, str. 59]

Definice. Nechť R je okruh. Invertibilní prvek pologrupy $(R, \cdot)$ se nazývá **jednotka** okruhu R. Množinu všech jednotek okruhu R značíme $R^\times$.

Poznámka. Nezaměňujte pojmy jednička a jednotka okruhu. Okruh má jedinou jedničku, kdežto jednotek může mít více.

Obory integrity

Definice. Netriviální komutativní okruh R se nazývá **obor integrity**, pokud nemá dělitele nuly.

Označení. Množinu všech nenulových prvků okruhu R značíme R^*.

Poznámka. Netriviální komutativní okruh R je tedy obor integrity, právě když $(R^*, \cdot)$ je pologrupa.

Věta. Netriviální komutativní okruh R je obor integrity, právě když v něm platí **zákon o krácení**, *tj. pro každé $a, b, c \in R$ platí*

$$a \neq 0, \ a \cdot b = a \cdot c \quad \Rightarrow \quad b = c.$$ [Věta 1.10, str. 59]

Definice. Nechť R je okruh. Invertibilní prvek pologrupy $(R, \cdot)$ se nazývá **jednotka** okruhu R. Množinu všech jednotek okruhu R značíme $R^\times$.

Poznámka. Nezaměňujte pojmy jednička a jednotka okruhu. Okruh má jedinou jedničku, kdežto jednotek může mít více. Vždy je jednička jednotkou. Okruhy s jedinou jednotkou jsou výjimečné (například okruh $\mathbb{Z}_2$).

Obory integrity

Definice. Netriviální komutativní okruh R se nazývá **obor integrity**, pokud nemá dělitele nuly.

Označení. Množinu všech nenulových prvků okruhu R značíme R^*.

Poznámka. Netriviální komutativní okruh R je tedy obor integrity, právě když $(R^*, \cdot)$ je pologrupa.

Věta. Netriviální komutativní okruh R je obor integrity, právě když v něm platí **zákon o krácení**, *tj. pro každé $a, b, c \in R$ platí*

$$a \neq 0, \ a \cdot b = a \cdot c \quad \Rightarrow \quad b = c.$$ [Věta 1.10, str. 59]

Definice. Nechť R je okruh. Invertibilní prvek pologrupy $(R, \cdot)$ se nazývá **jednotka** okruhu R. Množinu všech jednotek okruhu R značíme $R^\times$.

Poznámka. Nezaměňujte pojmy jednička a jednotka okruhu. Okruh má jedinou jedničku, kdežto jednotek může mít více. Vždy je jednička jednotkou. Okruhy s jedinou jednotkou jsou výjimečné (například okruh $\mathbb{Z}_2$). Nezaměňujte R^* a $R^\times$. Uvědomte si, že nové označení je v souladu s užívaným $\mathbb{Z}_m^\times$.

Tělesa

$R^* = R - \{0\}$ ... množina nenulových prvků okruhu R,
$R^\times = \{a \in R;\ \exists b \in R :\ a \cdot b = b \cdot a = 1\}$ ... množina invertibilních prvků pologrupy $(R, \cdot)$.

Věta. *Nechť R je okruh. Pak $(R^\times, \cdot)$ je grupa.* [[Věta 4.7, str. 25] je užita pro pologrupu $(R, \cdot)$.]

Tělesa

$R^* = R - \{0\}$ ... množina nenulových prvků okruhu R,
$R^\times = \{a \in R;\ \exists b \in R :\ a \cdot b = b \cdot a = 1\}$ ... množina invertibilních prvků pologrupy $(R, \cdot)$.

Věta. *Nechť R je okruh. Pak $(R^\times, \cdot)$ je grupa.* [[Věta 4.7, str. 25] je užita pro pologrupu $(R, \cdot)$.]

Definice. Netriviální komutativní okruh R se nazývá **těleso**, pokud je každý jeho nenulový prvek jednotkou.

Tělesa

$R^* = R - \{0\}$ ... množina nenulových prvků okruhu R,
$R^\times = \{a \in R;\ \exists b \in R :\ a \cdot b = b \cdot a = 1\}$ ... množina invertibilních prvků pologrupy $(R, \cdot)$.

Věta. *Nechť R je okruh. Pak $(R^\times, \cdot)$ je grupa.* [[Věta 4.7, str. 25] je užita pro pologrupu $(R, \cdot)$.]

Definice. Netriviální komutativní okruh R se nazývá **těleso**, pokud je každý jeho nenulový prvek jednotkou.

Věta. *Netriviální komutativní okruh R je těleso, právě když $R^* = R^\times$, tedy právě když $(R^*, \cdot)$ je grupa.*

Tělesa

$R^* = R - \{0\}$ ... množina nenulových prvků okruhu R,
$R^\times = \{a \in R;\ \exists b \in R :\ a \cdot b = b \cdot a = 1\}$ ... množina invertibilních prvků pologrupy $(R, \cdot)$.

Věta. *Nechť R je okruh. Pak $(R^\times, \cdot)$ je grupa.* [[Věta 4.7, str. 25] je užita pro pologrupu $(R, \cdot)$.]

Definice. Netriviální komutativní okruh R se nazývá **těleso**, pokud je každý jeho nenulový prvek jednotkou.

Věta. *Netriviální komutativní okruh R je těleso, právě když $R^* = R^\times$, tedy právě když $(R^*, \cdot)$ je grupa.* [Věta 1.14, str. 60]

Věta. *Každé těleso je oborem integrity.*

Tělesa

$R^* = R - \{0\}$ ... množina nenulových prvků okruhu R,
$R^\times = \{a \in R;\ \exists b \in R :\ a \cdot b = b \cdot a = 1\}$ ... množina invertibilních prvků pologrupy $(R, \cdot)$.

Věta. *Nechť R je okruh. Pak $(R^\times, \cdot)$ je grupa.* [[Věta 4.7, str. 25] je užita pro pologrupu $(R, \cdot)$.]

Definice. Netriviální komutativní okruh R se nazývá **těleso**, pokud je každý jeho nenulový prvek jednotkou.

Věta. *Netriviální komutativní okruh R je těleso, právě když $R^* = R^\times$, tedy právě když $(R^*, \cdot)$ je grupa.* [Věta 1.14, str. 60]

Věta. *Každé těleso je oborem integrity.* [Věta 1.13, str. 60]

Příklad. Okruh celých čísel $\mathbb{Z}$ je oborem integrity, který není tělesem.

Tělesa

$R^* = R - \{0\}$ ... množina nenulových prvků okruhu R,
$R^\times = \{a \in R;\ \exists b \in R :\ a \cdot b = b \cdot a = 1\}$ ... množina invertibilních prvků pologrupy $(R, \cdot)$.

Věta. *Nechť R je okruh. Pak $(R^\times, \cdot)$ je grupa.* [[Věta 4.7, str. 25] je užita pro pologrupu $(R, \cdot)$.]

Definice. Netriviální komutativní okruh R se nazývá **těleso**, pokud je každý jeho nenulový prvek jednotkou.

Věta. *Netriviální komutativní okruh R je těleso, právě když $R^* = R^\times$, tedy právě když $(R^*, \cdot)$ je grupa.* [Věta 1.14, str. 60]

Věta. *Každé těleso je oborem integrity.* [Věta 1.13, str. 60]

Příklad. Okruh celých čísel $\mathbb{Z}$ je oborem integrity, který není tělesem.

Věta. *Každý konečný obor integrity je tělesem.*

Tělesa

$R^* = R - \{0\}$ ... množina nenulových prvků okruhu R,
$R^\times = \{a \in R;\ \exists b \in R :\ a \cdot b = b \cdot a = 1\}$ ... množina invertibilních prvků pologrupy $(R, \cdot)$.

Věta. *Nechť R je okruh. Pak $(R^\times, \cdot)$ je grupa.* [[Věta 4.7, str. 25] je užita pro pologrupu $(R, \cdot)$.]

Definice. Netriviální komutativní okruh R se nazývá **těleso**, pokud je každý jeho nenulový prvek jednotkou.

Věta. *Netriviální komutativní okruh R je těleso, právě když $R^* = R^\times$, tedy právě když $(R^*, \cdot)$ je grupa.* [Věta 1.14, str. 60]

Věta. *Každé těleso je oborem integrity.* [Věta 1.13, str. 60]

Příklad. Okruh celých čísel $\mathbb{Z}$ je oborem integrity, který není tělesem.

Věta. *Každý konečný obor integrity je tělesem.* [Věta 1.17, str. 61]

Věta. *Okruh zbytkových tříd $\mathbb{Z}_m$ je oborem integrity, právě když je tělesem, což nastane, právě když m je prvočíslo.* [Věta 1.16, str. 61]

Charakteristika okruhu

Poznámka. Připomeňme, že v okruhu R pro libovolné $a \in R$, $n \in \mathbb{N}$ je $na = \underbrace{a + a + \cdots + a}_{n}$.

Charakteristika okruhu

Poznámka. Připomeňme, že v okruhu R pro libovolné $a \in R$, $n \in \mathbb{N}$ je $na = \underbrace{a + a + \cdots + a}_{n}$. Protože jedničku a nulu okruhu R značíme 1 a 0, v následující definici je rovností $n1 = 0$ nutno rozumět, že v okruhu R platí $\underbrace{1 + 1 + \cdots + 1}_{n} = 0$.

Charakteristika okruhu

Poznámka. Připomeňme, že v okruhu R pro libovolné $a \in R$, $n \in \mathbb{N}$ je $na = \underbrace{a + a + \cdots + a}_{n}$. Protože jedničku a nulu okruhu R značíme 1 a 0, v následující definici je rovností $n1 = 0$ nutno rozumět, že v okruhu R platí $\underbrace{1 + 1 + \cdots + 1}_{n} = 0$.

Definice. Nechť R je okruh. Nejmenší přirozené číslo n takové, že $n1 = 0$, se nazývá **charakteristika** okruhu R.

Charakteristika okruhu

Poznámka. Připomeňme, že v okruhu R pro libovolné $a \in R$, $n \in \mathbb{N}$ je $na = \underbrace{a + a + \cdots + a}_{n}$. Protože jedničku a nulu okruhu R značíme 1 a 0, v následující definici je rovností $n1 = 0$ nutno rozumět, že v okruhu R platí $\underbrace{1 + 1 + \cdots + 1}_{n} = 0$.

Definice. Nechť R je okruh. Nejmenší přirozené číslo n takové, že $n1 = 0$, se nazývá **charakteristika** okruhu R. Pokud takové n neexistuje (tedy pro všechna $k \in \mathbb{N}$ platí $k1 \neq 0$), řekneme, že charakteristika okruhu R je nula.

Charakteristika okruhu

Poznámka. Připomeňme, že v okruhu R pro libovolné $a \in R$, $n \in \mathbb{N}$ je $na = \underbrace{a + a + \cdots + a}_{n}$. Protože jedničku a nulu okruhu R značíme 1 a 0, v následující definici je rovností $n1 = 0$ nutno rozumět, že v okruhu R platí $\underbrace{1 + 1 + \cdots + 1}_{n} = 0$.

Definice. Nechť R je okruh. Nejmenší přirozené číslo n takové, že $n1 = 0$, se nazývá **charakteristika** okruhu R. Pokud takové n neexistuje (tedy pro všechna $k \in \mathbb{N}$ platí $k1 \neq 0$), řekneme, že charakteristika okruhu R je nula.

Označení. Charakteristiku okruhu R značíme $\operatorname{char} R$.

Charakteristika okruhu

Poznámka. Připomeňme, že v okruhu R pro libovolné $a \in R$, $n \in \mathbb{N}$ je $na = \underbrace{a + a + \cdots + a}_{n}$. Protože jedničku a nulu okruhu R značíme 1 a 0, v následující definici je rovností $n1 = 0$ nutno rozumět, že v okruhu R platí $\underbrace{1 + 1 + \cdots + 1}_{n} = 0$.

Definice. Nechť R je okruh. Nejmenší přirozené číslo n takové, že $n1 = 0$, se nazývá **charakteristika** okruhu R. Pokud takové n neexistuje (tedy pro všechna $k \in \mathbb{N}$ platí $k1 \neq 0$), řekneme, že charakteristika okruhu R je nula.

Označení. Charakteristiku okruhu R značíme $\operatorname{char} R$.

Příklady. $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$,

Charakteristika okruhu

Poznámka. Připomeňme, že v okruhu R pro libovolné $a \in R$, $n \in \mathbb{N}$ je $na = \underbrace{a + a + \cdots + a}_{n}$. Protože jedničku a nulu okruhu R značíme 1 a 0, v následující definici je rovností $n1 = 0$ nutno rozumět, že v okruhu R platí $\underbrace{1 + 1 + \cdots + 1}_{n} = 0$.

Definice. Nechť R je okruh. Nejmenší přirozené číslo n takové, že $n1 = 0$, se nazývá **charakteristika** okruhu R. Pokud takové n neexistuje (tedy pro všechna $k \in \mathbb{N}$ platí $k1 \neq 0$), řekneme, že charakteristika okruhu R je nula.

Označení. Charakteristiku okruhu R značíme $\operatorname{char} R$.

Příklady. $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$, $\operatorname{char} \mathbb{Z}_m = m$.

Charakteristika okruhu

Poznámka. Připomeňme, že v okruhu R pro libovolné $a \in R$, $n \in \mathbb{N}$ je $na = \underbrace{a + a + \cdots + a}_{n}$. Protože jedničku a nulu okruhu R značíme 1 a 0, v následující definici je rovností $n1 = 0$ nutno rozumět, že v okruhu R platí $\underbrace{1 + 1 + \cdots + 1}_{n} = 0$.

Definice. Nechť R je okruh. Nejmenší přirozené číslo n takové, že $n1 = 0$, se nazývá **charakteristika** okruhu R. Pokud takové n neexistuje (tedy pro všechna $k \in \mathbb{N}$ platí $k1 \neq 0$), řekneme, že charakteristika okruhu R je nula.

Označení. Charakteristiku okruhu R značíme $\operatorname{char} R$.

Příklady. $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$, $\operatorname{char} \mathbb{Z}_m = m$.

Věta. *Nechť R je okruh, $m = \operatorname{char} R$. Pak pro každé $a \in R$ platí $ma = 0$.*

Charakteristika okruhu

Poznámka. Připomeňme, že v okruhu R pro libovolné $a \in R$, $n \in \mathbb{N}$ je $na = \underbrace{a + a + \cdots + a}_{n}$. Protože jedničku a nulu okruhu R značíme 1 a 0, v následující definici je rovností $n1 = 0$ nutno rozumět, že v okruhu R platí $\underbrace{1 + 1 + \cdots + 1}_{n} = 0$.

Definice. Nechť R je okruh. Nejmenší přirozené číslo n takové, že $n1 = 0$, se nazývá **charakteristika** okruhu R. Pokud takové n neexistuje (tedy pro všechna $k \in \mathbb{N}$ platí $k1 \neq 0$), řekneme, že charakteristika okruhu R je nula.

Označení. Charakteristiku okruhu R značíme $\operatorname{char} R$.

Příklady. $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$, $\operatorname{char} \mathbb{Z}_m = m$.

Věta. *Nechť R je okruh, $m = \operatorname{char} R$. Pak pro každé $a \in R$ platí $ma = 0$.* [Věta 2.4, str. 62]

Věta. *Nechť R je obor integrity, pak $\operatorname{char} R$ je buď 0, nebo prvočíslo.* [Věta 2.5, str. 62]

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

- $0, 1 \in H$,

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

- $0, 1 \in H$,
- pro každé $a \in H$ platí $-a \in H$,

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

- $0, 1 \in H$,
- pro každé $a \in H$ platí $-a \in H$,
- pro každé $a, b \in H$ platí $a + b$, $a \cdot b \in H$.

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

- $0, 1 \in H$,
- pro každé $a \in H$ platí $-a \in H$,
- pro každé $a, b \in H$ platí $a + b$, $a \cdot b \in H$.

Poznámka. Největším podokruhem okruhu R (vzhledem k $\subseteq$) je celý okruh R,

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

- $0, 1 \in H$,
- pro každé $a \in H$ platí $-a \in H$,
- pro každé $a, b \in H$ platí $a + b$, $a \cdot b \in H$.

Poznámka. Největším podokruhem okruhu R (vzhledem k $\subseteq$) je celý okruh R, nejmenším podokruhem je $\{n1;\ n \in \mathbb{Z}\}$.

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

- $0, 1 \in H$,
- pro každé $a \in H$ platí $-a \in H$,
- pro každé $a, b \in H$ platí $a + b$, $a \cdot b \in H$.

Poznámka. Největším podokruhem okruhu R (vzhledem k $\subseteq$) je celý okruh R, nejmenším podokruhem je $\{n1;\ n \in \mathbb{Z}\}$.

Věta. *Nechť H je podokruh okruhu $(R, +, \cdot)$. Pak $+$ a $\cdot$ určují operace na množině H, přičemž H je okruh vzhledem k těmto operacím.*

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

- $0, 1 \in H$,
- pro každé $a \in H$ platí $-a \in H$,
- pro každé $a, b \in H$ platí $a + b$, $a \cdot b \in H$.

Poznámka. Největším podokruhem okruhu R (vzhledem k $\subseteq$) je celý okruh R, nejmenším podokruhem je $\{n1;\ n \in \mathbb{Z}\}$.

Věta. *Nechť H je podokruh okruhu $(R, +, \cdot)$. Pak $+$ a $\cdot$ určují operace na množině H, přičemž H je okruh vzhledem k těmto operacím. Je-li okruh R komutativní, pak je i okruh H komutativní.*

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

- $0, 1 \in H$,
- pro každé $a \in H$ platí $-a \in H$,
- pro každé $a, b \in H$ platí $a + b$, $a \cdot b \in H$.

Poznámka. Největším podokruhem okruhu R (vzhledem k $\subseteq$) je celý okruh R, nejmenším podokruhem je $\{n1;\ n \in \mathbb{Z}\}$.

Věta. *Nechť H je podokruh okruhu $(R, +, \cdot)$. Pak $+$ a $\cdot$ určují operace na množině H, přičemž H je okruh vzhledem k těmto operacím. Je-li okruh R komutativní, pak je i okruh H komutativní. Je-li R obor integrity, pak je i H obor integrity.*

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

- $0, 1 \in H$,
- pro každé $a \in H$ platí $-a \in H$,
- pro každé $a, b \in H$ platí $a + b$, $a \cdot b \in H$.

Poznámka. Největším podokruhem okruhu R (vzhledem k $\subseteq$) je celý okruh R, nejmenším podokruhem je $\{n1;\ n \in \mathbb{Z}\}$.

Věta. Nechť H je podokruh okruhu $(R, +, \cdot)$. Pak $+$ a $\cdot$ určují operace na množině H, přičemž H je okruh vzhledem k těmto operacím. Je-li okruh R komutativní, pak je i okruh H komutativní. Je-li R obor integrity, pak je i H obor integrity. [Věta 3.2, str. 66]

Důsledek. Každý podokruh tělesa je oborem integrity.

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

- $0, 1 \in H$,
- pro každé $a \in H$ platí $-a \in H$,
- pro každé $a, b \in H$ platí $a + b$, $a \cdot b \in H$.

Poznámka. Největším podokruhem okruhu R (vzhledem k $\subseteq$) je celý okruh R, nejmenším podokruhem je $\{n1;\ n \in \mathbb{Z}\}$.

Věta. Nechť H je podokruh okruhu $(R, +, \cdot)$. Pak $+$ a $\cdot$ určují operace na množině H, přičemž H je okruh vzhledem k těmto operacím. Je-li okruh R komutativní, pak je i okruh H komutativní. Je-li R obor integrity, pak je i H obor integrity. [Věta 3.2, str. 66]

Důsledek. Každý podokruh tělesa je oborem integrity.

Příklad. Podokruh tělesa nemusí být těleso: vždyť $\mathbb{Z}$ je podokruhem $\mathbb{Q}$.

Podokruh okruhu

Definice. Nechť $(R, +, \cdot)$ je okruh, H podmnožina množiny R. Řekneme, že H je **podokruh okruhu** R, jestliže

- $0, 1 \in H$,
- pro každé $a \in H$ platí $-a \in H$,
- pro každé $a, b \in H$ platí $a + b$, $a \cdot b \in H$.

Poznámka. Největším podokruhem okruhu R (vzhledem k $\subseteq$) je celý okruh R, nejmenším podokruhem je $\{n1;\ n \in \mathbb{Z}\}$.

Věta. *Nechť H je podokruh okruhu $(R, +, \cdot)$. Pak $+$ a $\cdot$ určují operace na množině H, přičemž H je okruh vzhledem k těmto operacím. Je-li okruh R komutativní, pak je i okruh H komutativní. Je-li R obor integrity, pak je i H obor integrity.* [Věta 3.2, str. 66]

Důsledek. *Každý podokruh tělesa je oborem integrity.*

Příklad. Podokruh tělesa nemusí být těleso: vždyť $\mathbb{Z}$ je podokruhem $\mathbb{Q}$.

Věta. *Jestliže H je podokruh okruhu R a K je podokruh okruhu H, pak je K také podokruh okruhu R.* [Zřejmé, vždyť operace $+$ a $\cdot$ se v okruhu H počítají jako v R.]

Podokruh okruhu generovaný podmnožinou okruhu

Věta. *Nechť R je okruh, I neprázdná množina taková, že pro každé $i \in I$ je dán podokruh H_i okruhu R.*

Podokruh okruhu generovaný podmnožinou okruhu

Věta. *Nechť R je okruh, I neprázdná množina taková, že pro každé $i \in I$ je dán podokruh H_i okruhu R. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podokruhů je opět podokruhem okruhu R.*

Podokruh okruhu generovaný podmnožinou okruhu

Věta. *Nechť R je okruh, I neprázdná množina taková, že pro každé $i \in I$ je dán podokruh H_i okruhu R. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podokruhů je opět podokruhem okruhu R.*

Definice. Nechť M je podmnožina okruhu R. Symbolem $\langle M \rangle$ označíme průnik všech podokruhů okruhu R, jejichž podmnožinou je množina M.

Podokruh okruhu generovaný podmnožinou okruhu

Věta. *Nechť R je okruh, I neprázdná množina taková, že pro každé $i \in I$ je dán podokruh H_i okruhu R. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podokruhů je opět podokruhem okruhu R.*

Definice. Nechť M je podmnožina okruhu R. Symbolem $\langle M \rangle$ označíme průnik všech podokruhů okruhu R, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M \rangle$ podokruhem okruhu R obsahující množinu M; evidentně je nejmenší s touto vlastností.

Podokruh okruhu generovaný podmnožinou okruhu

Věta. *Nechť R je okruh, I neprázdná množina taková, že pro každé $i \in I$ je dán podokruh H_i okruhu R. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podokruhů je opět podokruhem okruhu R.*

Definice. Nechť M je podmnožina okruhu R. Symbolem $\langle M \rangle$ označíme průnik všech podokruhů okruhu R, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M \rangle$ podokruhem okruhu R obsahující množinu M; evidentně je nejmenší s touto vlastností. Podokruh $\langle M \rangle$ nazýváme **podokruh generovaný množinou** M, množinu M nazýváme **množina generátorů podokruhu** $\langle M \rangle$.

Podokruh okruhu generovaný podmnožinou okruhu

Věta. *Nechť R je okruh, I neprázdná množina taková, že pro každé $i \in I$ je dán podokruh H_i okruhu R. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podokruhů je opět podokruhem okruhu R.*

Definice. Nechť M je podmnožina okruhu R. Symbolem $\langle M \rangle$ označíme průnik všech podokruhů okruhu R, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M \rangle$ podokruhem okruhu R obsahující množinu M; evidentně je nejmenší s touto vlastností. Podokruh $\langle M \rangle$ nazýváme **podokruh generovaný množinou** M, množinu M nazýváme **množina generátorů podokruhu** $\langle M \rangle$.

Poznámka. Zřejmě $\langle R \rangle = R$, $\langle \emptyset \rangle = \{n1;\ n \in \mathbb{Z}\}$.

Podokruh okruhu generovaný podmnožinou okruhu

Věta. *Nechť R je okruh, I neprázdná množina taková, že pro každé $i \in I$ je dán podokruh H_i okruhu R. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podokruhů je opět podokruhem okruhu R.*

Definice. Nechť M je podmnožina okruhu R. Symbolem $\langle M \rangle$ označíme průnik všech podokruhů okruhu R, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M \rangle$ podokruhem okruhu R obsahující množinu M; evidentně je nejmenší s touto vlastností. Podokruh $\langle M \rangle$ nazýváme **podokruh generovaný množinou** M, množinu M nazýváme **množina generátorů podokruhu** $\langle M \rangle$.

Poznámka. Zřejmě $\langle R \rangle = R$, $\langle \emptyset \rangle = \{n1;\ n \in \mathbb{Z}\}$.

Označení. Je-li $M = H \cup \{a_1, \ldots, a_n\}$, kde H je podokruh okruhu R a $a_1, \ldots, a_n \in R$, píšeme $H[a_1, \ldots, a_n]$ místo $\langle M \rangle$.

Podokruh okruhu generovaný podmnožinou okruhu

Věta. *Nechť R je okruh, I neprázdná množina taková, že pro každé $i \in I$ je dán podokruh H_i okruhu R. Pak průnik $\bigcap_{i \in I} H_i$ všech těchto podokruhů je opět podokruhem okruhu R.*

Definice. Nechť M je podmnožina okruhu R. Symbolem $\langle M \rangle$ označíme průnik všech podokruhů okruhu R, jejichž podmnožinou je množina M. Podle předchozí věty je $\langle M \rangle$ podokruhem okruhu R obsahující množinu M; evidentně je nejmenší s touto vlastností. Podokruh $\langle M \rangle$ nazýváme **podokruh generovaný množinou** M, množinu M nazýváme **množina generátorů podokruhu** $\langle M \rangle$.

Poznámka. Zřejmě $\langle R \rangle = R$, $\langle \emptyset \rangle = \{n1;\ n \in \mathbb{Z}\}$.

Označení. Je-li $M = H \cup \{a_1, \ldots, a_n\}$, kde H je podokruh okruhu R a $a_1, \ldots, a_n \in R$, píšeme $H[a_1, \ldots, a_n]$ místo $\langle M \rangle$.

Věta. *Nechť H je podokruh komutativního okruhu R a $a \in R$. Pak* $H[a] = \{h_0 + h_1 a + h_2 a^2 + \cdots + h_n a^n;\ n \in \mathbb{N},\ h_0, h_1, \ldots, h_n \in H\}$.

[Věta 3.12, str. 71]

Homomorfismus okruhů

Definice. Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy, $f : R \to S$ zobrazení.

Homomorfismus okruhů

Definice. Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy, $f : R \to S$ zobrazení. Řekneme, že f je **homomorfismus** okruhu R do okruhu S, jestliže

Homomorfismus okruhů

Definice. Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy, $f : R \to S$ zobrazení. Řekneme, že f je **homomorfismus** okruhu R do okruhu S, jestliže

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

Homomorfismus okruhů

Definice. Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy, $f : R \to S$ zobrazení. Řekneme, že f je **homomorfismus** okruhu R do okruhu S, jestliže

- pro každé $a, b \in R$ platí $f(a + b) = f(a) + f(b)$,
- pro každé $a, b \in R$ platí $f(a \cdot b) = f(a) \cdot f(b)$,

Homomorfismus okruhů

Definice. Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy, $f : R \to S$ zobrazení. Řekneme, že f je **homomorfismus** okruhu R do okruhu S, jestliže

- pro každé $a, b \in R$ platí $f(a + b) = f(a) + f(b)$,
- pro každé $a, b \in R$ platí $f(a \cdot b) = f(a) \cdot f(b)$,
- $f(1) = 1$.

Homomorfismus okruhů

Definice. Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy, $f : R \to S$ zobrazení. Řekneme, že f je **homomorfismus** okruhu R do okruhu S, jestliže

- pro každé $a, b \in R$ platí $f(a + b) = f(a) + f(b)$,
- pro každé $a, b \in R$ platí $f(a \cdot b) = f(a) \cdot f(b)$,
- $f(1) = 1$.

Injektivní homomorfismus se nazývá **vnoření**, bijektivní **izomorfismus**.

Homomorfismus okruhů

Definice. Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy, $f : R \to S$ zobrazení. Řekneme, že f je **homomorfismus** okruhu R do okruhu S, jestliže

- pro každé $a, b \in R$ platí $f(a + b) = f(a) + f(b)$,
- pro každé $a, b \in R$ platí $f(a \cdot b) = f(a) \cdot f(b)$,
- $f(1) = 1$.

Injektivní homomorfismus se nazývá **vnoření**, bijektivní **izomorfismus**. O okruzích R, S řekneme, že jsou izomorfní, píšeme $R \cong S$, existuje-li alespoň jeden izomorfismus $R \to S$.

Homomorfismus okruhů

Definice. Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy, $f : R \to S$ zobrazení. Řekneme, že f je **homomorfismus** okruhu R do okruhu S, jestliže

- pro každé $a, b \in R$ platí $f(a + b) = f(a) + f(b)$,
- pro každé $a, b \in R$ platí $f(a \cdot b) = f(a) \cdot f(b)$,
- $f(1) = 1$.

Injektivní homomorfismus se nazývá **vnoření**, bijektivní **izomorfismus**. O okruzích R, S řekneme, že jsou izomorfní, píšeme $R \cong S$, existuje-li alespoň jeden izomorfismus $R \to S$.

Příklad. Pro libovolné $m \in \mathbb{N}$ je zobrazení $\pi : \mathbb{Z} \to \mathbb{Z}_m$, určené předpisem $\pi(a) = [a]_m$ pro libovolné $a \in \mathbb{Z}$, surjektivní homomorfismus okruhu $(\mathbb{Z}, +, \cdot)$ celých čísel do okruhu $(\mathbb{Z}_m, +, \cdot)$ zbytkových tříd modulo m.

Homomorfismus okruhů

Definice. Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy, $f : R \to S$ zobrazení. Řekneme, že f je **homomorfismus** okruhu R do okruhu S, jestliže

- pro každé $a, b \in R$ platí $f(a + b) = f(a) + f(b)$,
- pro každé $a, b \in R$ platí $f(a \cdot b) = f(a) \cdot f(b)$,
- $f(1) = 1$.

Injektivní homomorfismus se nazývá **vnoření**, bijektivní **izomorfismus**. O okruzích R, S řekneme, že jsou izomorfní, píšeme $R \cong S$, existuje-li alespoň jeden izomorfismus $R \to S$.

Příklad. Pro libovolné $m \in \mathbb{N}$ je zobrazení $\pi : \mathbb{Z} \to \mathbb{Z}_m$, určené předpisem $\pi(a) = [a]_m$ pro libovolné $a \in \mathbb{Z}$, surjektivní homomorfismus okruhu $(\mathbb{Z}, +, \cdot)$ celých čísel do okruhu $(\mathbb{Z}_m, +, \cdot)$ zbytkových tříd modulo m.

Věta. Jsou-li $f : R \to S$ a $g : S \to T$ homomorfismy okruhů, pak také $g \circ f : R \to T$ je homomorfismem okruhů. [Věta 4.4, str. 73]

Homomorfismus okruhů, jeho jádro

Věta. *Nechť $f : R \to S$ je izomorfismus okruhů. Pak i inverzní zobrazení $f^{-1} : S \to R$ je izomorfismus okruhů.*

Homomorfismus okruhů, jeho jádro

Věta. *Nechť $f : R \to S$ je izomorfismus okruhů. Pak i inverzní zobrazení $f^{-1} : S \to R$ je izomorfismus okruhů.* [Věta 4.5, str. 73]

Důsledek. *Pro libovolné okruhy R, S, T platí: $R \cong R$;*

Homomorfismus okruhů, jeho jádro

Věta. *Nechť $f : R \to S$ je izomorfismus okruhů. Pak i inverzní zobrazení $f^{-1} : S \to R$ je izomorfismus okruhů.* [Věta 4.5, str. 73]

Důsledek. *Pro libovolné okruhy R, S, T platí: $R \cong R$; z $R \cong S$ plyne $S \cong R$;*

Homomorfismus okruhů, jeho jádro

Věta. *Nechť $f : R \to S$ je izomorfismus okruhů. Pak i inverzní zobrazení $f^{-1} : S \to R$ je izomorfismus okruhů.* [Věta 4.5, str. 73]

Důsledek. *Pro libovolné okruhy R, S, T platí: $R \cong R$; z $R \cong S$ plyne $S \cong R$; a konečně z $R \cong S$ a $S \cong T$ plyne $R \cong T$.*

Homomorfismus okruhů, jeho jádro

Věta. *Nechť $f : R \to S$ je izomorfismus okruhů. Pak i inverzní zobrazení $f^{-1} : S \to R$ je izomorfismus okruhů.* [Věta 4.5, str. 73]

Důsledek. *Pro libovolné okruhy R, S, T platí: $R \cong R$; z $R \cong S$ plyne $S \cong R$; a konečně z $R \cong S$ a $S \cong T$ plyne $R \cong T$.*

Poznámka. Zapomeneme-li v okruhu R, jak se násobí, zůstane nám aditivní grupa $(R, +)$.

Homomorfismus okruhů, jeho jádro

Věta. *Nechť $f : R \to S$ je izomorfismus okruhů. Pak i inverzní zobrazení $f^{-1} : S \to R$ je izomorfismus okruhů.* [Věta 4.5, str. 73]

Důsledek. *Pro libovolné okruhy R, S, T platí: $R \cong R$; z $R \cong S$ plyne $S \cong R$; a konečně z $R \cong S$ a $S \cong T$ plyne $R \cong T$.*

Poznámka. Zapomeneme-li v okruhu R, jak se násobí, zůstane nám aditivní grupa $(R, +)$. Každý homomorfismus okruhů $f : R \to S$ je také homomorfismem aditivních grup, je tedy $f(0) = 0$, pro každé $a \in R$ platí $f(-a) = -f(a)$, a máme jeho jádro:

Homomorfismus okruhů, jeho jádro

Věta. *Nechť $f : R \to S$ je izomorfismus okruhů. Pak i inverzní zobrazení $f^{-1} : S \to R$ je izomorfismus okruhů.* [Věta 4.5, str. 73]

Důsledek. *Pro libovolné okruhy R, S, T platí: $R \cong R$; z $R \cong S$ plyne $S \cong R$; a konečně z $R \cong S$ a $S \cong T$ plyne $R \cong T$.*

Poznámka. Zapomeneme-li v okruhu R, jak se násobí, zůstane nám aditivní grupa $(R, +)$. Každý homomorfismus okruhů $f : R \to S$ je také homomorfismem aditivních grup, je tedy $f(0) = 0$, pro každé $a \in R$ platí $f(-a) = -f(a)$, a máme jeho jádro:

Definice. Nechť $f : R \to S$ je homomorfismus okruhů. Množina $\ker f = \{a \in R;\ f(a) = 0\}$ se nazývá **jádro homomorfismu** f.

Homomorfismus okruhů, jeho jádro

Věta. *Nechť $f : R \to S$ je izomorfismus okruhů. Pak i inverzní zobrazení $f^{-1} : S \to R$ je izomorfismus okruhů.* [Věta 4.5, str. 73]

Důsledek. *Pro libovolné okruhy R, S, T platí: $R \cong R$; z $R \cong S$ plyne $S \cong R$; a konečně z $R \cong S$ a $S \cong T$ plyne $R \cong T$.*

Poznámka. Zapomeneme-li v okruhu R, jak se násobí, zůstane nám aditivní grupa $(R, +)$. Každý homomorfismus okruhů $f : R \to S$ je také homomorfismem aditivních grup, je tedy $f(0) = 0$, pro každé $a \in R$ platí $f(-a) = -f(a)$, a máme jeho jádro:

Definice. Nechť $f : R \to S$ je homomorfismus okruhů. Množina $\ker f = \{a \in R;\ f(a) = 0\}$ se nazývá **jádro homomorfismu** f.

Věta. *Homomorfismus okruhů $f : R \to S$ je injektivní, právě když* $\ker f = \{0\}$.

Homomorfismus okruhů, jeho jádro

Věta. *Nechť $f : R \to S$ je izomorfismus okruhů. Pak i inverzní zobrazení $f^{-1} : S \to R$ je izomorfismus okruhů.* [Věta 4.5, str. 73]

Důsledek. *Pro libovolné okruhy R, S, T platí: $R \cong R$; z $R \cong S$ plyne $S \cong R$; a konečně z $R \cong S$ a $S \cong T$ plyne $R \cong T$.*

Poznámka. Zapomeneme-li v okruhu R, jak se násobí, zůstane nám aditivní grupa $(R, +)$. Každý homomorfismus okruhů $f : R \to S$ je také homomorfismem aditivních grup, je tedy $f(0) = 0$, pro každé $a \in R$ platí $f(-a) = -f(a)$, a máme jeho jádro:

Definice. Nechť $f : R \to S$ je homomorfismus okruhů. Množina $\ker f = \{a \in R;\ f(a) = 0\}$ se nazývá **jádro homomorfismu** f.

Věta. *Homomorfismus okruhů $f : R \to S$ je injektivní, právě když* $\ker f = \{0\}$. [Věta 4.9, str. 74]

Příklad. Zobrazení $f : \mathbb{C} \to M_{2,2}(\mathbb{R})$, kde $f(a + bi) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ pro libovolné $a, b \in \mathbb{R}$, je vnoření tělesa $\mathbb{C}$ komplexních čísel do okruhu $M_{2,2}(\mathbb{R})$ matic typu 2×2.

Součin okruhů

Věta. *Nechť* $(R, +, \cdot)$ *a* $(S, +, \cdot)$ *jsou okruhy.*

Součin okruhů

Věta. *Nechť* $(R, +, \cdot)$ *a* $(S, +, \cdot)$ *jsou okruhy. Definujme na kartézském součinu* $R \times S$ *nové operace* $+$ *a* $\cdot$ *po složkách,*

Součin okruhů

Věta. *Nechť* $(R, +, \cdot)$ *a* $(S, +, \cdot)$ *jsou okruhy. Definujme na kartézském součinu* $R \times S$ *nové operace* $+$ *a* $\cdot$ *po složkách, tj.*

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2),$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

pro libovolné $r_1, r_2 \in R$ *a* $s_1, s_2 \in S$.

Součin okruhů

Věta. *Nechť* $(R, +, \cdot)$ *a* $(S, +, \cdot)$ *jsou okruhy. Definujme na kartézském součinu* $R \times S$ *nové operace* $+$ *a* $\cdot$ *po složkách, tj.*

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2),$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

pro libovolné $r_1, r_2 \in R$ *a* $s_1, s_2 \in S$. *Pak* $(R \times S, +, \cdot)$ *je okruh s nulou* $(0, 0)$ *a jedničkou* $(1, 1)$.

Součin okruhů

Věta. *Nechť* $(R, +, \cdot)$ *a* $(S, +, \cdot)$ *jsou okruhy. Definujme na kartézském součinu* $R \times S$ *nové operace* $+$ *a* $\cdot$ *po složkách, tj.*

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2),$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

pro libovolné $r_1, r_2 \in R$ *a* $s_1, s_2 \in S$. *Pak* $(R \times S, +, \cdot)$ *je okruh s nulou* $(0, 0)$ *a jedničkou* $(1, 1)$. *Navíc platí* $(R \times S)^\times = R^\times \times S^\times$.

Součin okruhů

Věta. *Nechť* $(R, +, \cdot)$ *a* $(S, +, \cdot)$ *jsou okruhy. Definujme na kartézském součinu* $R \times S$ *nové operace* $+$ *a* $\cdot$ *po složkách, tj.*

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2),$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

pro libovolné $r_1, r_2 \in R$ *a* $s_1, s_2 \in S$. *Pak* $(R \times S, +, \cdot)$ *je okruh s nulou* $(0, 0)$ *a jedničkou* $(1, 1)$. *Navíc platí* $(R \times S)^\times = R^\times \times S^\times$.

[Ověření je zdlouhavé, ale snadné: všechny axiomy okruhu jsou v $R \times S$ splněny, protože se operace počítají po složkách a v obou složkách tyto axiomy platí, protože jsou R a S okruhy.]

Definice. Výše popsaný okruh $(R \times S, +, \cdot)$ se nazývá **součin okruhů** $(R, +, \cdot)$ a $(S, +, \cdot)$.

Součin okruhů

Věta. *Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy. Definujme na kartézském součinu $R \times S$ nové operace $+$ a $\cdot$ po složkách, tj.*

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2),$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

pro libovolné $r_1, r_2 \in R$ a $s_1, s_2 \in S$. Pak $(R \times S, +, \cdot)$ je okruh s nulou $(0, 0)$ a jedničkou $(1, 1)$. Navíc platí $(R \times S)^\times = R^\times \times S^\times$.

[Ověření je zdlouhavé, ale snadné: všechny axiomy okruhu jsou v $R \times S$ splněny, protože se operace počítají po složkách a v obou složkách tyto axiomy platí, protože jsou R a S okruhy.]

Definice. Výše popsaný okruh $(R \times S, +, \cdot)$ se nazývá **součin okruhů** $(R, +, \cdot)$ a $(S, +, \cdot)$. Zobrazení $p_1 : R \times S \to R$ a $p_2 : R \times S \to S$ určená předpisy $p_1((r, s)) = r$, $p_2((r, s)) = s$ pro libovolné $(r, s) \in R \times S$ se nazývají **projekce** (ze součinu).

Součin okruhů

Věta. *Nechť* $(R, +, \cdot)$ *a* $(S, +, \cdot)$ *jsou okruhy. Definujme na kartézském součinu* $R \times S$ *nové operace* $+$ *a* $\cdot$ *po složkách, tj.*

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2),$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

pro libovolné $r_1, r_2 \in R$ *a* $s_1, s_2 \in S$. *Pak* $(R \times S, +, \cdot)$ *je okruh s nulou* $(0, 0)$ *a jedničkou* $(1, 1)$. *Navíc platí* $(R \times S)^\times = R^\times \times S^\times$.

[Ověření je zdlouhavé, ale snadné: všechny axiomy okruhu jsou v $R \times S$ splněny, protože se operace počítají po složkách a v obou složkách tyto axiomy platí, protože jsou R a S okruhy.]

Definice. Výše popsaný okruh $(R \times S, +, \cdot)$ se nazývá **součin okruhů** $(R, +, \cdot)$ a $(S, +, \cdot)$. Zobrazení $p_1 : R \times S \to R$ a $p_2 : R \times S \to S$ určená předpisy $p_1((r, s)) = r$, $p_2((r, s)) = s$ pro libovolné $(r, s) \in R \times S$ se nazývají **projekce** (ze součinu).

Věta. *Nechť* $(R \times S, +, \cdot)$ *je součin okruhů* $(R, +, \cdot)$ *a* $(S, +, \cdot)$.

Součin okruhů

Věta. *Nechť $(R, +, \cdot)$ a $(S, +, \cdot)$ jsou okruhy. Definujme na kartézském součinu $R \times S$ nové operace $+$ a $\cdot$ po složkách, tj.*

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2),$$
$$(r_1, s_1) \cdot (r_2, s_2) = (r_1 \cdot r_2, s_1 \cdot s_2)$$

pro libovolné $r_1, r_2 \in R$ a $s_1, s_2 \in S$. Pak $(R \times S, +, \cdot)$ je okruh s nulou $(0, 0)$ a jedničkou $(1, 1)$. Navíc platí $(R \times S)^\times = R^\times \times S^\times$.

[Ověření je zdlouhavé, ale snadné: všechny axiomy okruhu jsou v $R \times S$ splněny, protože se operace počítají po složkách a v obou složkách tyto axiomy platí, protože jsou R a S okruhy.]

Definice. Výše popsaný okruh $(R \times S, +, \cdot)$ se nazývá **součin okruhů** $(R, +, \cdot)$ a $(S, +, \cdot)$. Zobrazení $p_1 : R \times S \to R$ a $p_2 : R \times S \to S$ určená předpisy $p_1((r, s)) = r$, $p_2((r, s)) = s$ pro libovolné $(r, s) \in R \times S$ se nazývají **projekce** (ze součinu).

Věta. *Nechť $(R \times S, +, \cdot)$ je součin okruhů $(R, +, \cdot)$ a $(S, +, \cdot)$. Pak obě projekce p_1 a p_2 jsou surjektivní homomorfismy okruhů.*

[Zřejmé, protože se operace počítají po složkách.]

Čínská zbytková věta

Věta (Čínská zbytková). Nechť $m, n \in \mathbb{N}$ *a* $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ *je zobrazení určené předpisem* $f([a]_{mn}) = ([a]_m, [a]_n)$ *pro libovolné* $a \in \mathbb{Z}$.

Čínská zbytková věta

Věta (Čínská zbytková). *Nechť $m, n \in \mathbb{N}$ a $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ je zobrazení určené předpisem $f([a]_{mn}) = ([a]_m, [a]_n)$ pro libovolné $a \in \mathbb{Z}$. Pak f je homomorfismus okruhů, mezi těmito okruhy jediný.*

Čínská zbytková věta

Věta (Čínská zbytková). *Nechť* $m, n \in \mathbb{N}$ *a* $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ *je zobrazení určené předpisem* $f([a]_{mn}) = ([a]_m, [a]_n)$ *pro libovolné* $a \in \mathbb{Z}$. *Pak* f *je homomorfismus okruhů, mezi těmito okruhy jediný.*
Je-li navíc $(m, n) = 1$, *je* f *izomorfismus, a tedy* $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.

Čínská zbytková věta

Věta (Čínská zbytková). *Nechť* $m, n \in \mathbb{N}$ *a* $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ *je zobrazení určené předpisem* $f([a]_{mn}) = ([a]_m, [a]_n)$ *pro libovolné* $a \in \mathbb{Z}$. *Pak* f *je homomorfismus okruhů, mezi těmito okruhy jediný.*
Je-li navíc $(m, n) = 1$, *je* f *izomorfismus, a tedy* $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.
Je-li naopak $(m, n) > 1$, *okruhy* $\mathbb{Z}_{mn}$ *a* $\mathbb{Z}_m \times \mathbb{Z}_n$ *nejsou izomorfní.*

Čínská zbytková věta

Věta (Čínská zbytková). *Nechť $m, n \in \mathbb{N}$ a $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ je zobrazení určené předpisem $f([a]_{mn}) = ([a]_m, [a]_n)$ pro libovolné $a \in \mathbb{Z}$. Pak f je homomorfismus okruhů, mezi těmito okruhy jediný.*
Je-li navíc $(m, n) = 1$, je f izomorfismus, a tedy $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.
Je-li naopak $(m, n) > 1$, okruhy $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \times \mathbb{Z}_n$ nejsou izomorfní.

Důkaz. Protože $m \mid mn$ a $n \mid mn$, je f definováno korektně. Zřejmě je to jediné zobrazení zachovávající operaci $+$ a splňující $f([1]_{mn}) = ([1]_m, [1]_n)$, navíc zachovává i $\cdot$.

Čínská zbytková věta

Věta (Čínská zbytková). *Nechť $m, n \in \mathbb{N}$ a $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ je zobrazení určené předpisem $f([a]_{mn}) = ([a]_m, [a]_n)$ pro libovolné $a \in \mathbb{Z}$. Pak f je homomorfismus okruhů, mezi těmito okruhy jediný.*
Je-li navíc $(m, n) = 1$, je f izomorfismus, a tedy $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.
Je-li naopak $(m, n) > 1$, okruhy $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \times \mathbb{Z}_n$ nejsou izomorfní.

Důkaz. Protože $m \mid mn$ a $n \mid mn$, je f definováno korektně. Zřejmě je to jediné zobrazení zachovávající operaci $+$ a splňující $f([1]_{mn}) = ([1]_m, [1]_n)$, navíc zachovává i $\cdot$. Je-li $(m, n) = 1$, pak je $\ker f = \{[a]_{mn};\ a \in \mathbb{Z},\ m \mid a,\ n \mid a\} = \{[0]_{mn}\}$, a tedy f je injekce.

Čínská zbytková věta

Věta (Čínská zbytková). *Nechť $m, n \in \mathbb{N}$ a $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ je zobrazení určené předpisem $f([a]_{mn}) = ([a]_m, [a]_n)$ pro libovolné $a \in \mathbb{Z}$. Pak f je homomorfismus okruhů, mezi těmito okruhy jediný.*
Je-li navíc $(m, n) = 1$, je f izomorfismus, a tedy $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.
Je-li naopak $(m, n) > 1$, okruhy $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \times \mathbb{Z}_n$ nejsou izomorfní.

Důkaz. Protože $m \mid mn$ a $n \mid mn$, je f definováno korektně. Zřejmě je to jediné zobrazení zachovávající operaci $+$ a splňující $f([1]_{mn}) = ([1]_m, [1]_n)$, navíc zachovává i $\cdot$. Je-li $(m, n) = 1$, pak je $\ker f = \{[a]_{mn};\ a \in \mathbb{Z},\ m \mid a,\ n \mid a\} = \{[0]_{mn}\}$, a tedy f je injekce. Protože obě množiny mají mn prvků, je f i surjekce.

Čínská zbytková věta

Věta (Čínská zbytková). *Nechť $m, n \in \mathbb{N}$ a $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ je zobrazení určené předpisem $f([a]_{mn}) = ([a]_m, [a]_n)$ pro libovolné $a \in \mathbb{Z}$. Pak f je homomorfismus okruhů, mezi těmito okruhy jediný.*
Je-li navíc $(m, n) = 1$, je f izomorfismus, a tedy $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.
Je-li naopak $(m, n) > 1$, okruhy $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \times \mathbb{Z}_n$ nejsou izomorfní.

Důkaz. Protože $m \mid mn$ a $n \mid mn$, je f definováno korektně. Zřejmě je to jediné zobrazení zachovávající operaci $+$ a splňující $f([1]_{mn}) = ([1]_m, [1]_n)$, navíc zachovává i $\cdot$. Je-li $(m, n) = 1$, pak je $\ker f = \{[a]_{mn};\ a \in \mathbb{Z},\ m \mid a,\ n \mid a\} = \{[0]_{mn}\}$, a tedy f je injekce. Protože obě množiny mají mn prvků, je f i surjekce.
Je-li $(m, n) > 1$, pak $[\frac{mn}{(m,n)}]_{mn}$ je nenulový prvek jádra $\ker f$.

Čínská zbytková věta

Věta (Čínská zbytková). *Nechť $m, n \in \mathbb{N}$ a $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ je zobrazení určené předpisem $f([a]_{mn}) = ([a]_m, [a]_n)$ pro libovolné $a \in \mathbb{Z}$. Pak f je homomorfismus okruhů, mezi těmito okruhy jediný. Je-li navíc $(m, n) = 1$, je f izomorfismus, a tedy $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Je-li naopak $(m, n) > 1$, okruhy $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \times \mathbb{Z}_n$ nejsou izomorfní.*

Důkaz. Protože $m \mid mn$ a $n \mid mn$, je f definováno korektně. Zřejmě je to jediné zobrazení zachovávající operaci $+$ a splňující $f([1]_{mn}) = ([1]_m, [1]_n)$, navíc zachovává i $\cdot$. Je-li $(m, n) = 1$, pak je $\ker f = \{[a]_{mn};\ a \in \mathbb{Z},\ m \mid a,\ n \mid a\} = \{[0]_{mn}\}$, a tedy f je injekce. Protože obě množiny mají mn prvků, je f i surjekce.
Je-li $(m, n) > 1$, pak $[\frac{mn}{(m,n)}]_{mn}$ je nenulový prvek jádra $\ker f$.

Důsledek. *Je-li $(m, n) = 1$, pak $\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$,*

Čínská zbytková věta

Věta (Čínská zbytková). *Nechť $m, n \in \mathbb{N}$ a $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ je zobrazení určené předpisem $f([a]_{mn}) = ([a]_m, [a]_n)$ pro libovolné $a \in \mathbb{Z}$. Pak f je homomorfismus okruhů, mezi těmito okruhy jediný. Je-li navíc $(m, n) = 1$, je f izomorfismus, a tedy $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Je-li naopak $(m, n) > 1$, okruhy $\mathbb{Z}_{mn}$ a $\mathbb{Z}_m \times \mathbb{Z}_n$ nejsou izomorfní.*

Důkaz. Protože $m \mid mn$ a $n \mid mn$, je f definováno korektně. Zřejmě je to jediné zobrazení zachovávající operaci $+$ a splňující $f([1]_{mn}) = ([1]_m, [1]_n)$, navíc zachovává i $\cdot$. Je-li $(m, n) = 1$, pak je $\ker f = \{[a]_{mn};\ a \in \mathbb{Z},\ m \mid a,\ n \mid a\} = \{[0]_{mn}\}$, a tedy f je injekce. Protože obě množiny mají mn prvků, je f i surjekce.
Je-li $(m, n) > 1$, pak $[\frac{mn}{(m,n)}]_{mn}$ je nenulový prvek jádra $\ker f$.

Důsledek. *Je-li $(m, n) = 1$, pak $\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$, a tedy $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.*

Čínská zbytková věta

Věta (Čínská zbytková). *Nechť* $m, n \in \mathbb{N}$ *a* $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ *je zobrazení určené předpisem* $f([a]_{mn}) = ([a]_m, [a]_n)$ *pro libovolné* $a \in \mathbb{Z}$. *Pak* f *je homomorfismus okruhů, mezi těmito okruhy jediný.*
Je-li navíc $(m, n) = 1$, *je* f *izomorfismus, a tedy* $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$.
Je-li naopak $(m, n) > 1$, *okruhy* $\mathbb{Z}_{mn}$ *a* $\mathbb{Z}_m \times \mathbb{Z}_n$ *nejsou izomorfní.*

Důkaz. Protože $m \mid mn$ a $n \mid mn$, je f definováno korektně. Zřejmě je to jediné zobrazení zachovávající operaci $+$ a splňující $f([1]_{mn}) = ([1]_m, [1]_n)$, navíc zachovává i $\cdot$. Je-li $(m, n) = 1$, pak je $\ker f = \{[a]_{mn};\ a \in \mathbb{Z},\ m \mid a,\ n \mid a\} = \{[0]_{mn}\}$, a tedy f je injekce. Protože obě množiny mají mn prvků, je f i surjekce.
Je-li $(m, n) > 1$, pak $[\frac{mn}{(m,n)}]_{mn}$ je nenulový prvek jádra $\ker f$.

Důsledek. *Je-li* $(m, n) = 1$, *pak* $\mathbb{Z}_{mn}^\times \cong \mathbb{Z}_m^\times \times \mathbb{Z}_n^\times$, *a tedy* $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

Důsledek. *Je-li* $(m, n) = 1$, *pak pro každé* $a, b \in \mathbb{Z}$ *existuje* $c \in \mathbb{Z}$ *tak, že*

$$c \equiv a \pmod{m},$$
$$c \equiv b \pmod{n}.$$