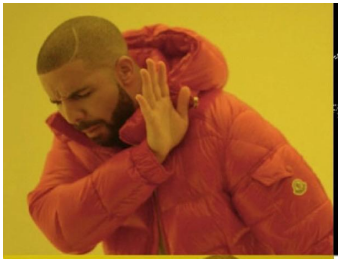
Okruhy

Algebra 2

Mgr. Markéta Trnečková, Ph.D.

Palacký University, Olomouc

Okruhy



Rings

A **ring** is a set R, together with two operations $\oplus$ and $*$, which has the following properties:

- R is a commutative group under $\oplus$
- R is associative under $*$
- **Multiplicative identity**: There is an element 1 such that $r * 1 = 1 * r = r$ for all $r \in R$
- The operation $*$ distributes over $\oplus$:

$$a * (b \oplus c) = (a * b) \oplus (a * c)$$
$$(a \oplus b) * c = (a * c) \oplus (b * c)$$

Okruhy

Definice

Okruh $\langle R, +, \cdot \rangle$ *je množina* R *se dvěma binárními operacemi* $+$ *a* $\cdot$*, které nazýváme* **sčítání** *a* **násobení**, *definovanými na* R *takové, že*

- $\langle R, + \rangle$ *je abelovská grupa*
- $\cdot$ *je asociativní*
- *pro* $a, b, c \in R$ *platí* **distributivní zákon zleva**
  $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
  a **distributivní zákon zprava**
  $(a + b) \cdot c = (a \cdot c) + (b \cdot c)$

$a \cdot b$ budeme zapisovat ab

Příklad 75

Zkuste vymyslet nějaký okruh.

Okruhy

Příklad

Zkuste vymyslet nějaký okruh.

- Podmínky okruhu platí v jakékoliv podmnožině komplexních čísel, kde množina tvoří grupu se sčítáním a je uzavřená na násobení
  $\langle \mathbb{C}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$, $\langle \mathbb{Z}, +, \cdot \rangle$

Někdy budeme vynechávat operace a psát jen množinu.

Příklad 76

Nechť R je okruh a $M_n(R)$ je kolekce všech $n \times n$ matic nad R. Operace sčítání a násobení v R nám umožňuje sčítat a násobit matice obvyklý způsobem.
Je $M_n(R)$ okruh?

Okruhy

Příklad

Nechť R je okruh a $M_n(R)$ je kolekce všech $n \times n$ matic nad R. Operace sčítání a násobení v R nám umožňuje sčítat a násobit matice obvyklý způsobem.
Je $M_n(R)$ okruh?

- Snadno ověříme, že $\langle M_n(R), + \rangle$ je abelovská grupa.
- Asociativita násobení:
  $(A \cdot (B \cdot C))_{ij} = \sum_{k=1}^{n} (a_{ik} \cdot (\sum_{l=1}^{n} b_{kl} \cdot c_{lj}))$
  Z distributivity a asociativity násobení prvků z R
  $= \sum_{k=1}^{n} \sum_{l=1}^{n} a_{ik} \cdot b_{kl} \cdot c_{lj}$
  ...
  $= \sum_{l=1}^{n} (\sum_{k=1}^{n} a_{ik} \cdot b_{kl}) \cdot c_{lj})$
- Distributivita zleva $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$
  $(A \cdot (B + C))_{ij} = \sum_{k=1}^{n} (a_{ik} \cdot (b_{kj} + c_{kj}))$
  a_{ik}, b_{kj}, c_{kj} jsou reálná čísla a na nich distributivita platí.

Okruhy

Tvrzení

Nechť R je okruh. Čtvercové matice $M_n(R)$ tvoří také okruh.

- Např. $M_n(\mathbb{Z})$, $M_n(\mathbb{Q})$, $M_n(\mathbb{R})$, $M_n(\mathbb{C})$
- Násobení není komutativní v žádném okruhu pro $n \geq 2$.

Příklad 77

Nechť F je množina reálných funkcí $f : \mathbb{R} \to \mathbb{R}$ jedné proměnné. Víme, že $\langle F, + \rangle$ je abelovská grupa se sčítáním:
$(f + g)(x) = f(x) + g(x)$.
Definujme násobení:
$(f \cdot g)(x) = f(x) \cdot g(x)$.
Ukažte, že je F okruh.

Okruhy

Příklad

Nechť F je množina reálných funkcí $f : \mathbb{R} \to \mathbb{R}$ jedné proměnné. Víme, že $\langle F, + \rangle$ je abelovská grupa se sčítáním:
$(f + g)(x) = f(x) + g(x)$.
Definujme násobení:
$(f \cdot g)(x) = f(x) \cdot g(x)$.
Ukažte, že je F okruh.

- Asociativita $\cdot$
  plyne z asociativity násobení reálných čísel
- Distributivita
  opět plyne z distributivity reálných čísel

Další příklady okruhů

Příklad 78

$n\mathbb{Z}$ je cyklická podgrupa $\mathbb{Z}$ se sčítáním.
Prvky grupy jsou násobky čísla n.
Protože $(nr)(ns) = n(nrs)$ je také násobek čísla n, takže je uzavřená na násobení.
Víme, že + a · splňuje distributivní zákony.
$\langle n\mathbb{Z}, +, \cdot \rangle$ je okruh.

Příklad 79

Uvažujme cyklickou grupu $\langle \mathbb{Z}_n, + \rangle$.
Když definujeme pro $a, b \in \mathbb{Z}_n$ součin $a \cdot b$ jako zbytek obvyklého součinu celých čísel po dělení n. (Tuto operaci nazveme **součin modulo n.**)
Snadno ukážeme, že $\langle \mathbb{Z}_n, +, \cdot \rangle$ je okruh.

Další příklady okruhů

Příklad 80

Mějme okruhy R_1, R_2, $\dots R_n$. Obdobně, jako u grup můžeme definovat **direktní součin okruhů** *R_i. Stejně jako na 3. přednášce.*
Sčítání i násobení definujeme po jednotlivých komponentách.

Poznámky k použité notaci:

- U operace násobení běžně vynecháváme $\cdot$ (ab je součin prvků a a b).
- 0 bude označovat neutrální prvek operace $+$.
- $-a$ bude označovat inverzní prvek prvku a vzhledem k operaci $+$.
- Součet n čísel a ($a + a + \cdots + a$) budeme značit $n \cdot a$.
  Toto je něco jiného než součin prvků a a n z R.
- Pokud $n < 0$, $n \cdot a$ je roven $(-a) + (-a) + \cdots + (-a)$, kde je $|n|$ sčítanců.
- $0 \cdot n = 0$
  0 vlevo je celé číslo, 0 vpravo neutrální prvek.

Okruhy

Věta 40

Pokud R je okruh, 0 neutrální prvek k operaci sčítání. Pak pro libovolné $a, b \in R$ platí:

1. $0a = a0 = 0$
2. $a(-b) = (-a)b = -(ab)$
3. $(-a)(-b) = ab$

Důkaz

$0a = a0 = 0$*:*

Dle vlastnosti okruhů ($\langle R, + \rangle$ je abelovská grupa, platí distributivní zákony) platí

$a0 + a0 = a(0 + 0) = a0 = 0 + a0$

Pak dle zákona o krácení v grupě $\langle R, + \rangle$ máme $a0 = 0$.

Obdobně $a0 + a0 = (0 + 0)a = 0a = 0 + 0a$, $0a = 0$.

Důkaz (Pokračování)

$a(-b) = (-a)b = -(ab)$:

Dle definice je $-(ab)$ *ten prvek, který dá v součtu s* ab *neutrální prvek* 0.

Musíme ukázat, že $a(-b) = -(ab)$. *Tedy* $a(-b) + (ab) = 0$. *Použitím distributivního zákona zleva:*

$a(-b) + (ab) = a(-b + b) = a0 = 0$

Obdobně

$(-a)b + (ab) = (-a + a)b = 0b = 0$

$(-a)(-b) = ab$:

Dle druhé vlastnosti $(-a)(-b) = -(a(-b))$.

Dále $-(a(-b)) = -(-(ab))$.

$-(-(ab))$ *je ten prvek, který, když přidáme k* $-(ab)$ *dá* 0,

To je ab *dle definice* $-(ab)$ *a unikátnosti inverzních prvků b grupě.*

Tedy $(-a)(-b) = ab$.

Homomorfismus

Definice

Mějme okruhy R a R'. Zobrazení $\phi : R \to R'$ nazveme **homomorfismus**, *pokud splňuje*

1. $\phi(a+b) = \phi(a) + \phi(b)$,
2. $\phi(ab) = \phi(a)\phi(b)$.

- První podmínka říká, že ϕ je homomorfismus grup $\langle R, + \rangle$ a $\langle R', + \rangle$
- Vše, co platilo pro homomorfismy grup, platí pro aditivní část okruhů
  Např. ϕ je injektivní, právě, když jeho jádro je pouze podmnožina $\{0\}$
- Druhá podmínka říká, že ϕ je homomorfismus grupoidů $\langle R, \cdot \rangle$ a $\langle R', \cdot \rangle$

Homomorfismus

Příklad 81

Nechť F je okruh reálných funkcí $\mathbb{R} \to \mathbb{R}$, kde jsou operace sčítání a násobení definovány následovně:

$(f+g)(x) = f(x) + g(x)$

$(f \cdot g)(x) = f(x) \cdot g(x)$

Že se jedná o okruh jsme ukázali v příkladu 77.

Pro každé $a \in \mathbb{R}$ můžeme definovat homomorfismus:

$\phi_a : F \to \mathbb{R}$ *následovně*

$\phi_a(f) = f(a)$.

Tento příklad známe z homomorfismu grup pro sčítání.

Ukažte, že platí podmínka homomorfismu i u okruhů (tedy pro operaci násobení).

Homomorfismus

Příklad

Nechť F je okruh reálných funkcí $\mathbb{R} \to \mathbb{R}$, kde jsou operace sčítání a násobení definovány následovně:
$(f + g)(x) = f(x) + g(x)$
$(f \cdot g)(x) = f(x) \cdot g(x)$
Pro každé $a \in \mathbb{R}$ můžeme definovat homomorfismus:
$\phi_a : F \to \mathbb{R}$ *následovně*
$\phi_a(f) = f(a)$.
Tento příklad známe z homomorfismu grup pro sčítání.
Ukažte, že platí podmínka homomorfismu i u okruhů (tedy pro operaci násobení).

- $\phi(ab) = \phi(a)\phi(b)$.
- $\phi_a(fg) = (f \cdot g)(a)$
  $= f(a) \cdot g(a)$ Dle definice násobení
  Což je rovno pravé straně.

Homomorfismus

Příklad 82

Na okruzích $\mathbb{Z}$ a $\mathbb{Z}_n$ (Že se jedná o okruh jsme si ukázali v příkladu 79) definujme zobrazení $\phi(x) = a$, kde a je zbytek po dělení n. Ukažte, že se jedná o homomorfismus pro každé n.

Homomorfismus

Příklad

Na okruzích $\mathbb{Z}$ a $\mathbb{Z}_n$ (Že se jedná o okruh jsme si ukázali v příkladu 79) definujme zobrazení $\phi(x) = a$, kde a je zbytek po dělení n. Ukažte, že se jedná o homomorfismus pro každé n.

- $\phi(a+b) = \phi(a) + \phi(b)$ už víme, že platí z teorie grup.
- $\phi(ab) = \phi(a)\phi(b)$
  $a = q_1 n + r_1$, $b = q_2 n + r_2$
  $ab = n(q_1 q_2 n + r_1 q_2 + q_1 r_2) + r_1 r_2$
  $\phi(ab)$ je zbytek po dělení n tedy je $r_1 r_2$.
  $\phi(a) = r_1$ a $\phi(b) = r_2$
  V příkladu 79 jsme právě takto definovali násobení ve zbytkových třídách, takže opravdu $\phi(a)\phi(b)$ je ten samý zbytek jako $\phi(ab)$.

Isomorfismus

Definice

Homomorfismus okruhů $\phi : R \to R'$ nazveme **isomorfismus**, *pokud je toto zobrazení bijektivní.*
Okruhy R a R' nazveme **isomorfní**.

Příklad 83

Víme, že abelovské grupy $\langle \mathbb{Z}, + \rangle$ a $\langle 2\mathbb{Z}, + \rangle$ jsou isomorfní pro zobrazení při zobrazení $\phi(x) = 2x$ pro $x \in \mathbb{Z}$. Jsou isomorfní i okruhy $\langle \mathbb{Z}, +, \cdot \rangle$ a $\langle 2\mathbb{Z}, +, \cdot \rangle$?

Isomorfismus

Příklad

Víme, že abelovské grupy $\langle \mathbb{Z}, + \rangle$ *a* $\langle 2\mathbb{Z}, + \rangle$ *jsou isomorfní při zobrazení* $\phi(x) = 2x$ *pro* $x \in \mathbb{Z}$. *Jsou isomorfní i okruhy* $\langle \mathbb{Z}, +, \cdot \rangle$ *a* $\langle 2\mathbb{Z}, +, \cdot \rangle$*?*

- NE.
- $\phi(xy) = 2xy$
- $\phi(x)\phi(y) = 2x2y = 4xy$

Okruh

Definice

Okruh, ve kterém je součin komutativní, se nazývá **komutativní okruh**.
Okruh, ve kterém má součin neutrální prvek, se nazývá **okruh s jedničkou**.
Tento neutrální prvek nazveme **jednička**.

Příklad 84

Ukažte, že pro celá čísla r *a* s*, kde* $gcd(r, s) = 1$*, jsou okruhy* $\mathbb{Z}_{rs}$ *a* $\mathbb{Z}_r \times \mathbb{Z}_s$ *isomorfní.*

Okruh

Příklad

Ukažte, že pro celá čísla r a s, kde $gcd(r,s) = 1$, jsou okruhy $\mathbb{Z}_{rs}$ a $\mathbb{Z}_r \times \mathbb{Z}_s$ isomorfní.

- Už víme, že $\langle \mathbb{Z}_{rs}, + \rangle$ i $\langle \mathbb{Z}_r \times \mathbb{Z}_s, + \rangle$ jsou abelovské grupy řádu rs s generátorem 1 respektive $(1,1)$
- $\phi : \mathbb{Z}_{rs} \to \mathbb{Z}_r \times \mathbb{Z}_s$
  $\phi(n \cdot 1) = n \cdot (1,1)$
  je isomorfismus.
- V okruhu s jedničkou zřejmě platí
  $\underbrace{(1 + \cdots + 1)}_{n \text{ sčítanců}} \underbrace{(1 + \cdots + 1)}_{m \text{ sčítanců}} = \underbrace{(1 + \cdots + 1)}_{nm \text{ sčítanců}}$
  tj. $(n \cdot 1)(m \cdot 1) = (nm \cdot 1)$
- Podmínka homomorfismu: $\phi(ab) = \phi(a)\phi(b)$.
  $\phi(nm) = (nm) \cdot (1,1) = [n \cdot (1,1)][m \cdot (1,1)] = \phi(n)\phi(m)$

Těleso

Definice

Nechť R je okruh s jedničkou $1 \neq 0$.
Prvek u je **jednotka** *R, pokud má multiplikativní inverzi v R.*
Pokud každý nenulový prvek v R je jednotka, pak se R nazývá **těleso**.
Pokud je navíc $\cdot$ komutativní, R se nazývá **komutativní těleso** *(také* **pole***).*

Příklad 85

Najděte všechny jednotky v $\mathbb{Z}_{14}$.

Těleso

Příklad

Najděte všechny jednotky v $\mathbb{Z}_{14}$.

- 1 a $-1 = 13$ jsou jednotky
- Protože $(3)(5) = 1$, vidíme, že 3 a 5 jsou jednotky
- Také $-3 = 11$ a $-5 = 9$ jsou jednotky
- Žádné další prvky v $\mathbb{Z}_{14}$ nejsou jednotky
- Žádný násobek 2, 4, 6, 8 nebo 10 nedá číslo o 1 větší než násobek 14 – mají společného dělitele 2
- Ani žádný násobek 7 nedá o 1 větší číslo než je násobek 14 (společný dělitel 7)

Těleso

Příklad 86

Určete, zda jsou okruhy $\mathbb{Z}$, $\mathbb{Q}$ a $\mathbb{R}$ tělesa.

Těleso

Příklad

Určete, zda jsou okruhy $\mathbb{Z}$, $\mathbb{Q}$ a $\mathbb{R}$ tělesa.

- $\mathbb{Z}$
  není těleso, protože např. 2 nemá multiplikativní inverzi, není to tedy jednotka v $\mathbb{Z}$
  jediné jednotky jsou 1 a -1
- $\mathbb{Q}$ i $\mathbb{R}$
  jsou komutativní tělesa

Podokruh, podtěleso

Definice

Nechť R je okruh. Jeho podmnožinu nazveme **podokruh**, *pokud spolu s indukovanými operacemi tvoří okruh.*

Definice

Nechť R je těleso. Jeho podmnožinu nazveme **podtěleso**, *pokud spolu s indukovanými operacemi tvoří těleso.*

Dělitelé nuly

Definice

Pokud a a b jsou dva nenulové prvky okruhu R takové, že $ab = 0$, pak se a a b nazývají **dělitelé nuly**.

Příklad 87 (Motivace pro zavedení dělitelů nuly)

Vyřešte následující rovnici:
$x^2 - 5x + 6 = 0$.

- $x^2 - 5x + 6 = (x - 2)(x - 3)$
- Řešení – alespoň jedna závorka musí být rovna 0 (buď $x - 2 = 0$ nebo $x - 3 = 0$) tedy 2 nebo 3

Dělitelé nuly

Příklad 88

V $\mathbb{Z}_{12}$ *vyřešte následující rovnici:*
$x^2 - 5x + 6 = 0$.

Dělitelé nuly

Příklad

V $\mathbb{Z}_{12}$ vyřešte následující rovnici:
$x^2 - 5x + 6 = 0$.

- V $\mathbb{Z}_{12}$ stále platí $a0 = 0a = 0$. Tj. řešení jsou 3 a 2
- Ale platí i $(3)(4) = (4)(3) = 0$
  $(6-2)(6-3) = (4)(3) = 0$ řešením je i 6
- Ale platí i $(9)(8) = (8)(9) = 0$
  $(11-2)(11-3) = (9)(8) = 0$ řešením je i 11
- Dále $(6)(2) = (2)(6) = (3)(8) = (8)(3) = (6)(4) = (4)(6) = (4)(9) = (9)(4) = (6)(6) = (6)(8) = (8)(6) = (6)(10) = (10)(6) = 0$
- Vidíme, že dělitelé nuly jsou čísla 2, 3, 4, 6, 8 a 9
  Všechna tato čísla jsou soudělná s 12.

Dělitelé nuly

Věta 41

V okruhu $\mathbb{Z}_n$ jsou dělitelé nuly právě ty prvky, které nejsou nesoudělná s n.

Důkaz

$\Rightarrow$: *Nechť $m \in \mathbb{Z}$, $m \neq 0$ a $gcd(m,n) = d \neq 1$*
$m\left(\frac{n}{d}\right) = \left(\frac{m}{d}\right)n$ *a $(m/d)n$ je násobek n tedy $= 0$.*
Jelikož $m \neq 0$ a $n/d \neq 0$, m je dělitel 0.

$\Leftarrow$: *Nechť $m \in \mathbb{Z}_n$ je nesoudělné s n.*
Pokud $s \in \mathbb{Z}_n$ máme $ms = 0$, tak n dělí ms. Protože m je nesoudělné s n, musí n dělit s, takže $s = 0$ v $\mathbb{Z}_n$.

Důsledek 10

Pokud p je prvočíslo, pak $\mathbb{Z}_p$ nemá dělitele nuly.

Zákon o krácení

Definice

Nechť R je okruh a $a, b, c \in R$. **Zákon o krácení** *platí v R, pokud*
$ab = ac$ takové, že $a \neq 0$ implikuje $b = c$
$ba = ca$ takové, že $a \neq 0$ implikuje $b = c$.
Těmto podmínkám říkáme **multiplikativní zákony o krácení**.

Aditivní zákony o krácení platí v R vždy. Protože $\langle R, + \rangle$ je grupa.

Zákon o krácení

Věta 42

Zákony krácení platí v okruhu R právě, když R nemá žádné dělitele nuly.

Důkaz

$\Rightarrow$: *Nechť R je okruh, ve kterém platí zákony o krácení, a uvažujme $ab = 0$ pro některé $a, b \in R$.*
Musíme ukázat, že $a = 0$ nebo $b = 0$. Pokud $a \neq 0$, pak $ab = a0$ implikuje, že $b = 0$ dle zákona o krácení.
Podobně, $b \neq 0$ implikuje $a = 0$, takže tam nemohou být žádní dělitelé nuly.

$\Leftarrow$: *Předpokládáme, že R nemá dělitele nuly a že $ab = ac$, $a \neq 0$.*
Pak $ab - ac = a(b - c) = 0$.
Protože $a \neq 0$, a protože R nemá dělitele nuly, musíme mít $b - c = 0$, takže $b = c$.
Podobný argument ukazuje $ba = ca$, $a \neq 0$ implikuje $b = c$.

Poznámky k okruhům

- Uvažujme, že R je okruh bez dělitelů nuly.
  Rovnice $ax = b$ s $a \neq 0$ v R může mít nejvýše jedno řešení x, protože pokud $ax_1 = b$ a $ax_2 = b$, pak $ax_1 = ax_2$ a dle věty o krácení máme $x_1 = x_2$.
- Pokud R má jedničku $1 \neq 0$, a a je jednotka v R s inverzí a^{-1}, pak řešení x rovnice $ax = b$ je $a^{-1}b$.
- V případě, že R je komutativní (zvláště, když je komutativní těleso), je zvykem místo $a^{-1}b$ nebo ba^{-1} psát b/a.
  Pokud by R nebylo komutativní, tak není jasné, jestli b/a má být $a^{-1}b$ nebo ba^{-1}.
- Multiplikativní inverze a^{-1} nenulového prvku a v komutativním tělese může být zapsána jako $1/a$.

Obor integrity

Definice

Obor integrity D *je komutativní okruh s jedničkou* $1 \neq 0$*, který nemá žádné dělitele nuly.*

V oboru integrity platí (multiplikativní) zákon o krácení.

V polynomech, kde jsou koeficienty z oboru integrity, můžeme řešit polynomiální rovnici rozložením polynomu na lineární faktory a položením každého faktoru nule.

Příklad 89

Určete, zda jsou následující okruhy obory integrity:

- $\mathbb{Z}$
- $\mathbb{Z}_n$
- *Direktní součin* $R \times S$ *dvou nenulových okruhů* R *a* S

Obor integrity

Příklad

Určete, zda jsou následující okruhy obory integrity:

- $\mathbb{Z}$
- $\mathbb{Z}_n$
- *Direktní součin $R \times S$ dvou nenulových okruhů R a S*

- $\mathbb{Z}$
  Je obor integrity.
- $\mathbb{Z}_n$
  Je obor integrity jen pokud je n prvočíslo.
- $R \times S$
  Není obor integrity:
  Pro $r \in R$, $s \in S$ obojí nenulové, máme
  $(r, 0)(0, s) = (0, 0)$

Obor integrity

Příklad 90

Ukažte, že přestože $\mathbb{Z}_2$ je obor integrity, okruh matic $M_2(\mathbb{Z}_2)$ má dělitele nuly.

Obor integrity

Příklad

Ukažte, že přestože $\mathbb{Z}_2$ je obor integrity, okruh matic $M_2(\mathbb{Z}_2)$ má dělitele nuly.

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Obor integrity

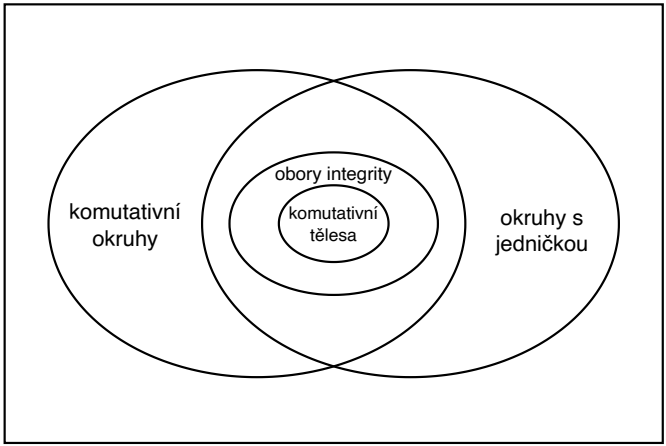
Věta 43

Každé komutativní těleso F je obor integrity.

Důkaz

Chceme ukázat, že F nemá dělitele nuly
F je komutativní okruh s jedničkou.
Nechť $a, b \in F$ a předpokládejme, že $a \neq 0$. Pokud $ab = 0$
$\left(\frac{1}{a}\right)(ab) = \left(\frac{1}{a}\right)0 = 0.$
Pak ale
$0 = \left(\frac{1}{a}\right)(ab) = \left[\left(\frac{1}{a}\right)a\right]b = 1b = b.$
$ab = 0$, $a \neq 0$ *implikuje, že* $b = 0$. *Takže nemá dělitele nuly.*

Algebraické struktury se dvěma binárními operacemi



Příklad 91

Kde jsou v obrázku tělesa?

Algebraické struktury se dvěma binárními operacemi

	$\langle R, + \rangle$					$\langle R, \cdot \rangle$				$\langle R \setminus \{0\}, \cdot \rangle$		
	uzavřenost	asociativita	komutativita	neutrální prvek (nula)	inverzní prvky	uzavřenost	asociativita	komutativita	neutrální prvek (jednička)	inverzní prvky	nemá dělitele nuly	distributivita
Polookruh	✓	✓	✓			✓	✓		✓			✓
Komut. polookruh	✓	✓	✓	✓		✓	✓	✓	✓			✓
Okruh	✓	✓	✓	✓	✓	✓	✓		✓			✓
Komut. okruh	✓	✓	✓	✓	✓	✓	✓	✓	✓			✓
Obor integrity	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓	✓
Těleso	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Komut. těleso	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Komutativní tělesa

Věta 44

Každý konečný obor integrity je komutativní těleso.

Důkaz

Existence multiplikativních inverzí: Nechť $D = \{0, 1, a_1, \ldots, a_n\}$ *je konečný obor integrity.*
Musíme ukázat, že pro všechna $a \in D$, $a \neq 0$ *existuje* $b \in D$ *takové, že* $ab = 1$.
Uvažujme $a1, aa_1, aa_2, \ldots aa_n$. *Tyto prvky jsou různé, protože* $aa_i = aa_j$ *implikuje* $a_i = a_j$ *dle zákona o krácení.*
Také, protože D *nemá dělitele nuly, žádný z těchto prvků není* 0.
Takže jsou to prvky $1, a_1, \ldots, a_n$ *v nějakém pořadí. Tj.* $a1 = 1$ *nebo* $aa_i = 1$ *pro nějaké* i.
Tedy a *má multiplikativní inverzi.*

Komutativní tělesa

Důsledek 11

Pokud p je prvočíslo, pak $\mathbb{Z}_p$ je komutativní těleso.

Důkaz

Plyne z předchozí věty a z faktu, že $\mathbb{Z}_p$ je obor integrity.

Charakteristika okruhu

Definice

Pokud pro okruh R existuje kladné číslo n takové, že $n \cdot a = 0$ pro všechna $a \in R$, tak nejmenší takové číslo se nazývá **charakteristika okruhu** R.
Pokud takové číslo neexistuje, R má **charakteristiku 0**.

Příklad 92

Jakou charakteristiku mají následující okruhy?

- $\mathbb{Z}_n$
- $\mathbb{Z}$

Charakteristika okruhu

Příklad

Jakou charakteristiku mají následující okruhy?

- $\mathbb{Z}_n$
- $\mathbb{Z}$

- $\mathbb{Z}_n$
  charakteristika je n
- $\mathbb{Z}$
  charakteristika je 0
  stejně jako $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$

Je potřeba prozkoumat všechna a, abychom určili charakteristiku okruhu?

Charakteristika okruhu

Věta 45

Nechť R je okruh s jedničkou.
Pokud $n \cdot 1 \neq 0$ pro všechna $n \in \mathbb{Z}^+$, tak R má charakteristiku 0.
Pokud $n \cdot 1 = 0$ pro nějaké $n \in \mathbb{Z}^+$, tak nejmenší takové číslo je charakteristika R.

Důkaz

Pokud $n \cdot 1 \neq 0$ pro všechna $n \in \mathbb{Z}^+$ pak zjevně nemůže mít $n \cdot a = 0$, pro všechna $a \in R$ a nějaké n. Takže dle definice má charakteristiku 0.

Předpokládejme, že n je kladné číslo takové, že $n \cdot 1 = 0$.
Pro libovolné $a \in R$:
$n \cdot a = a + a + \cdots + a = a(1 + 1 + \cdots + 1) = a(n \cdot 1) = a0 = 0.$
Což jsme chtěli dokázat.