Ideály okruhu $(R, +, \cdot)$

Definice. Nechť R je okruh. Podmnožina $I \subseteq R$ se nazývá **ideál** okruhu R, jestliže

- $I \neq \emptyset$;

Ideály okruhu $(R, +, \cdot)$

Definice. Nechť R je okruh. Podmnožina $I \subseteq R$ se nazývá **ideál** okruhu R, jestliže

- $I \neq \emptyset$;
- $\forall a, b \in I : a + b \in I$;

Ideály okruhu $(R, +, \cdot)$

Definice. Nechť R je okruh. Podmnožina $I \subseteq R$ se nazývá **ideál** okruhu R, jestliže

- $I \neq \emptyset$;
- $\forall a, b \in I : a + b \in I$;
- $\forall a \in I \ \forall r \in R : a \cdot r,\ r \cdot a \in I$.

Ideály okruhu $(R, +, \cdot)$

Definice. Nechť R je okruh. Podmnožina $I \subseteq R$ se nazývá **ideál** okruhu R, jestliže

- $I \neq \emptyset$;
- $\forall a, b \in I : a + b \in I$;
- $\forall a \in I \ \forall r \in R : a \cdot r,\ r \cdot a \in I$.

Poznámka. Pro libovolný okruh R tvoří $\{0\}$ i R ideály okruhu R.

Ideály okruhu $(R, +, \cdot)$

Definice. Nechť R je okruh. Podmnožina $I \subseteq R$ se nazývá **ideál** okruhu R, jestliže

- $I \neq \emptyset$;
- $\forall a, b \in I : a + b \in I$;
- $\forall a \in I \ \forall r \in R : a \cdot r,\ r \cdot a \in I$.

Poznámka. Pro libovolný okruh R tvoří $\{0\}$ i R ideály okruhu R. Evidentně jde o nejmenší a největší ideál okruhu R.

Ideály okruhu $(R, +, \cdot)$

Definice. Nechť R je okruh. Podmnožina $I \subseteq R$ se nazývá **ideál** okruhu R, jestliže

- $I \neq \emptyset$;
- $\forall a, b \in I : a + b \in I$;
- $\forall a \in I \ \forall r \in R : a \cdot r,\ r \cdot a \in I$.

Poznámka. Pro libovolný okruh R tvoří $\{0\}$ i R ideály okruhu R. Evidentně jde o nejmenší a největší ideál okruhu R.

Věta. Nechť $I \subseteq R$ je ideál okruhu R, pak

- I je podgrupa grupy $(R, +)$;

Ideály okruhu $(R, +, \cdot)$

Definice. Nechť R je okruh. Podmnožina $I \subseteq R$ se nazývá **ideál** okruhu R, jestliže

- $I \neq \emptyset$;
- $\forall a, b \in I : a + b \in I$;
- $\forall a \in I \ \forall r \in R : a \cdot r,\ r \cdot a \in I$.

Poznámka. Pro libovolný okruh R tvoří $\{0\}$ i R ideály okruhu R. Evidentně jde o nejmenší a největší ideál okruhu R.

Věta. Nechť $I \subseteq R$ je ideál okruhu R, pak

- I je podgrupa grupy $(R, +)$;
- $1 \in I$, právě když $I = R$.

Ideály okruhu $(R, +, \cdot)$

Definice. Nechť R je okruh. Podmnožina $I \subseteq R$ se nazývá **ideál** okruhu R, jestliže

- $I \neq \emptyset$;
- $\forall a, b \in I : a + b \in I$;
- $\forall a \in I \ \forall r \in R : a \cdot r,\ r \cdot a \in I$.

Poznámka. Pro libovolný okruh R tvoří $\{0\}$ i R ideály okruhu R. Evidentně jde o nejmenší a největší ideál okruhu R.

Věta. Nechť $I \subseteq R$ je ideál okruhu R, pak

- I je podgrupa grupy $(R, +)$;
- $1 \in I$, právě když $I = R$.

Poznámka. Podgrupa H aditivní grupy $(R, +)$ okruhu R je ideál tohoto okruhu, právě když pro každé $r \in R$ a každé $h \in H$ platí $r \cdot h, h \cdot r \in H$.

Ideál generovaný množinou

Věta. *Nechť $S \neq \emptyset$ je libovolná množina taková, že pro každé $s \in S$ je dán ideál I_s okruhu R. Pak $\bigcap_{s \in S} I_s$ je ideál okruhu R.*

Ideál generovaný množinou

Věta. *Nechť $S \neq \emptyset$ je libovolná množina taková, že pro každé $s \in S$ je dán ideál I_s okruhu R. Pak $\bigcap_{s \in S} I_s$ je ideál okruhu R.*

Důsledek. *Nechť R je okruh. Systém všech ideálů okruhu R uspořádaný inkluzí je úplný svaz.*

Ideál generovaný množinou

Věta. *Nechť $S \neq \emptyset$ je libovolná množina taková, že pro každé $s \in S$ je dán ideál I_s okruhu R. Pak $\bigcap_{s \in S} I_s$ je ideál okruhu R.*

Důsledek. *Nechť R je okruh. Systém všech ideálů okruhu R uspořádaný inkluzí je úplný svaz.*

Definice. Nechť R je okruh. Předchozí věta nám umožňuje definovat **ideál** okruhu R **generovaný množinou** $M \subseteq R$ jako průnik všech ideálů tuto množinu obsahujících.

Ideál generovaný množinou

Věta. *Nechť $S \neq \emptyset$ je libovolná množina taková, že pro každé $s \in S$ je dán ideál I_s okruhu R. Pak $\bigcap_{s \in S} I_s$ je ideál okruhu R.*

Důsledek. *Nechť R je okruh. Systém všech ideálů okruhu R uspořádaný inkluzí je úplný svaz.*

Definice. Nechť R je okruh. Předchozí věta nám umožňuje definovat **ideál** okruhu R **generovaný množinou** $M \subseteq R$ jako průnik všech ideálů tuto množinu obsahujících. Je to tedy nejmenší ideál okruhu R obsahující M, značíme jej (M).

Ideál generovaný množinou

Věta. *Nechť $S \neq \emptyset$ je libovolná množina taková, že pro každé $s \in S$ je dán ideál I_s okruhu R. Pak $\bigcap_{s \in S} I_s$ je ideál okruhu R.*

Důsledek. *Nechť R je okruh. Systém všech ideálů okruhu R uspořádaný inkluzí je úplný svaz.*

Definice. Nechť R je okruh. Předchozí věta nám umožňuje definovat **ideál** okruhu R **generovaný množinou** $M \subseteq R$ jako průnik všech ideálů tuto množinu obsahujících. Je to tedy nejmenší ideál okruhu R obsahující M, značíme jej (M).
Je-li $M = \{a_1, \ldots, a_n\}$, píšeme místo (M) také $(a_1, \ldots, a_n)$.

Ideál generovaný množinou

Věta. *Nechť $S \neq \emptyset$ je libovolná množina taková, že pro každé $s \in S$ je dán ideál I_s okruhu R. Pak $\bigcap_{s \in S} I_s$ je ideál okruhu R.*

Důsledek. *Nechť R je okruh. Systém všech ideálů okruhu R uspořádaný inkluzí je úplný svaz.*

Definice. Nechť R je okruh. Předchozí věta nám umožňuje definovat **ideál** okruhu R **generovaný množinou** $M \subseteq R$ jako průnik všech ideálů tuto množinu obsahujících. Je to tedy nejmenší ideál okruhu R obsahující M, značíme jej (M).
Je-li $M = \{a_1, \ldots, a_n\}$, píšeme místo (M) také $(a_1, \ldots, a_n)$.

Věta. *Nechť R je komutativní okruh, $a_1, \ldots, a_n \in R$.*

Ideál generovaný množinou

Věta. *Nechť $S \neq \emptyset$ je libovolná množina taková, že pro každé $s \in S$ je dán ideál I_s okruhu R. Pak $\bigcap_{s \in S} I_s$ je ideál okruhu R.*

Důsledek. *Nechť R je okruh. Systém všech ideálů okruhu R uspořádaný inkluzí je úplný svaz.*

Definice. Nechť R je okruh. Předchozí věta nám umožňuje definovat **ideál** okruhu R **generovaný množinou** $M \subseteq R$ jako průnik všech ideálů tuto množinu obsahujících. Je to tedy nejmenší ideál okruhu R obsahující M, značíme jej (M).
Je-li $M = \{a_1, \ldots, a_n\}$, píšeme místo (M) také $(a_1, \ldots, a_n)$.

Věta. *Nechť R je komutativní okruh, $a_1, \ldots, a_n \in R$. Pak $(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n;\ r_1, \ldots, r_n \in R\}$.*

Ideál generovaný množinou

Věta. *Nechť $S \neq \emptyset$ je libovolná množina taková, že pro každé $s \in S$ je dán ideál I_s okruhu R. Pak $\bigcap_{s \in S} I_s$ je ideál okruhu R.*

Důsledek. *Nechť R je okruh. Systém všech ideálů okruhu R uspořádaný inkluzí je úplný svaz.*

Definice. Nechť R je okruh. Předchozí věta nám umožňuje definovat **ideál** okruhu R **generovaný množinou** $M \subseteq R$ jako průnik všech ideálů tuto množinu obsahujících. Je to tedy nejmenší ideál okruhu R obsahující M, značíme jej (M).
Je-li $M = \{a_1, \ldots, a_n\}$, píšeme místo (M) také $(a_1, \ldots, a_n)$.

Věta. *Nechť R je komutativní okruh, $a_1, \ldots, a_n \in R$. Pak $(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n;\ r_1, \ldots, r_n \in R\}$.*

Definice. Nechť R je komutativní okruh, $a \in R$.

Ideál generovaný množinou

Věta. *Nechť $S \neq \emptyset$ je libovolná množina taková, že pro každé $s \in S$ je dán ideál I_s okruhu R. Pak $\bigcap_{s \in S} I_s$ je ideál okruhu R.*

Důsledek. *Nechť R je okruh. Systém všech ideálů okruhu R uspořádaný inkluzí je úplný svaz.*

Definice. Nechť R je okruh. Předchozí věta nám umožňuje definovat **ideál** okruhu R **generovaný množinou** $M \subseteq R$ jako průnik všech ideálů tuto množinu obsahujících. Je to tedy nejmenší ideál okruhu R obsahující M, značíme jej (M).
Je-li $M = \{a_1, \ldots, a_n\}$, píšeme místo (M) také $(a_1, \ldots, a_n)$.

Věta. *Nechť R je komutativní okruh, $a_1, \ldots, a_n \in R$. Pak $(a_1, \ldots, a_n) = \{r_1 a_1 + \cdots + r_n a_n;\ r_1, \ldots, r_n \in R\}$.*

Definice. Nechť R je komutativní okruh, $a \in R$. Ideál $(a) = \{ra;\ r \in R\}$ nazýváme **hlavní ideál** okruhu R generovaný prvkem a.

Dělitelnost v komutativním okruhu a ideály

Věta. *Nechť R je komutativní okruh, $a, b, c \in R$.*

Dělitelnost v komutativním okruhu a ideály

Věta. *Nechť R je komutativní okruh, $a, b, c \in R$.*

1. $(a) = \{x \in R;\ a \mid x\}$;

Dělitelnost v komutativním okruhu a ideály

Věta. *Nechť R je komutativní okruh, $a, b, c \in R$.*

1. $(a) = \{x \in R;\ a \mid x\}$;
2. $(a) \subseteq (b)$, *právě když* $b \mid a$;

Dělitelnost v komutativním okruhu a ideály

Věta. *Nechť R je komutativní okruh, $a, b, c \in R$.*

1. $(a) = \{x \in R;\ a \mid x\}$;
2. $(a) \subseteq (b)$, *právě když* $b \mid a$;
3. $(a) = (b)$, *právě když* $a \sim b$;

Dělitelnost v komutativním okruhu a ideály

Věta. *Nechť R je komutativní okruh, $a, b, c \in R$.*

1. $(a) = \{x \in R;\ a \mid x\}$;
2. $(a) \subseteq (b)$, *právě když* $b \mid a$;
3. $(a) = (b)$, *právě když* $a \sim b$;
4. $(a) = R$, *právě když* $a \in R^\times$;

Dělitelnost v komutativním okruhu a ideály

Věta. *Nechť R je komutativní okruh, $a, b, c \in R$.*

1. $(a) = \{x \in R;\ a \mid x\}$;
2. $(a) \subseteq (b)$, *právě když* $b \mid a$;
3. $(a) = (b)$, *právě když* $a \sim b$;
4. $(a) = R$, *právě když* $a \in R^\times$;
5. $(a) \cap (b) = (c)$, *právě když c je nejmenší společný násobek prvků a, b;*

Dělitelnost v komutativním okruhu a ideály

Věta. *Nechť R je komutativní okruh, $a, b, c \in R$.*

1. $(a) = \{x \in R;\ a \mid x\}$;
2. $(a) \subseteq (b)$, *právě když* $b \mid a$;
3. $(a) = (b)$, *právě když* $a \sim b$;
4. $(a) = R$, *právě když* $a \in R^\times$;
5. $(a) \cap (b) = (c)$, *právě když c je nejmenší společný násobek prvků a, b;*
6. $(a, b) = (c)$, *právě když c je největší společný dělitel prvků a, b a současně je c ve tvaru $c = ra + sb$ pro vhodné $r, s \in R$.*

Dělitelnost v komutativním okruhu a ideály

Věta. *Nechť R je komutativní okruh, $a, b, c \in R$.*

1. $(a) = \{x \in R;\ a \mid x\}$;
2. $(a) \subseteq (b)$, *právě když* $b \mid a$;
3. $(a) = (b)$, *právě když* $a \sim b$;
4. $(a) = R$, *právě když* $a \in R^\times$;
5. $(a) \cap (b) = (c)$, *právě když c je nejmenší společný násobek prvků a, b;*
6. $(a, b) = (c)$, *právě když c je největší společný dělitel prvků a, b a současně je c ve tvaru $c = ra + sb$ pro vhodné $r, s \in R$.*

Příklad. Ideál $(x, 2)$ okruhu $\mathbb{Z}[x]$ obsahuje právě ty polynomy $f(x) \in \mathbb{Z}[x]$, jejichž absolutní člen $f(0)$ je sudý.

Dělitelnost v komutativním okruhu a ideály

Věta. *Nechť R je komutativní okruh, $a, b, c \in R$.*

1. $(a) = \{x \in R;\ a \mid x\}$;
2. $(a) \subseteq (b)$, *právě když* $b \mid a$;
3. $(a) = (b)$, *právě když* $a \sim b$;
4. $(a) = R$, *právě když* $a \in R^\times$;
5. $(a) \cap (b) = (c)$, *právě když c je nejmenší společný násobek prvků a, b;*
6. $(a, b) = (c)$, *právě když c je největší společný dělitel prvků a, b a současně je c ve tvaru $c = ra + sb$ pro vhodné $r, s \in R$.*

Příklad. Ideál $(x, 2)$ okruhu $\mathbb{Z}[x]$ obsahuje právě ty polynomy $f(x) \in \mathbb{Z}[x]$, jejichž absolutní člen $f(0)$ je sudý. Tento ideál není hlavní, neboť z rovnosti $(x, 2) = (g)$ pro nějaké $g \in \mathbb{Z}[x]$ by plynulo, že g je největší společný dělitel prvků $x, 2 \in \mathbb{Z}[x]$.

Dělitelnost v komutativním okruhu a ideály

Věta. *Nechť R je komutativní okruh, $a, b, c \in R$.*

1. $(a) = \{x \in R;\ a \mid x\}$;
2. $(a) \subseteq (b)$, *právě když* $b \mid a$;
3. $(a) = (b)$, *právě když* $a \sim b$;
4. $(a) = R$, *právě když* $a \in R^\times$;
5. $(a) \cap (b) = (c)$, *právě když c je nejmenší společný násobek prvků a, b;*
6. $(a, b) = (c)$, *právě když c je největší společný dělitel prvků a, b a současně je c ve tvaru $c = ra + sb$ pro vhodné $r, s \in R$.*

Příklad. Ideál $(x, 2)$ okruhu $\mathbb{Z}[x]$ obsahuje právě ty polynomy $f(x) \in \mathbb{Z}[x]$, jejichž absolutní člen $f(0)$ je sudý. Tento ideál není hlavní, neboť z rovnosti $(x, 2) = (g)$ pro nějaké $g \in \mathbb{Z}[x]$ by plynulo, že g je největší společný dělitel prvků $x, 2 \in \mathbb{Z}[x]$. Ovšem 2 má jen dělitele $1, -1, 2, -2$, přičemž $2 \nmid x$, $-2 \nmid x$, a tedy by $g = \pm 1$.

Dělitelnost v komutativním okruhu a ideály

Věta. *Nechť R je komutativní okruh, $a, b, c \in R$.*

1. $(a) = \{x \in R;\ a \mid x\}$;
2. $(a) \subseteq (b)$, *právě když* $b \mid a$;
3. $(a) = (b)$, *právě když* $a \sim b$;
4. $(a) = R$, *právě když* $a \in R^\times$;
5. $(a) \cap (b) = (c)$, *právě když c je nejmenší společný násobek prvků a, b;*
6. $(a, b) = (c)$, *právě když c je největší společný dělitel prvků a, b a současně je c ve tvaru $c = ra + sb$ pro vhodné $r, s \in R$.*

Příklad. Ideál $(x, 2)$ okruhu $\mathbb{Z}[x]$ obsahuje právě ty polynomy $f(x) \in \mathbb{Z}[x]$, jejichž absolutní člen $f(0)$ je sudý. Tento ideál není hlavní, neboť z rovnosti $(x, 2) = (g)$ pro nějaké $g \in \mathbb{Z}[x]$ by plynulo, že g je největší společný dělitel prvků $x, 2 \in \mathbb{Z}[x]$. Ovšem 2 má jen dělitele $1, -1, 2, -2$, přičemž $2 \nmid x$, $-2 \nmid x$, a tedy by $g = \pm 1$. Ale $(1) = (-1) = \mathbb{Z}[x]$, spor.

Okruh hlavních ideálů

Věta. *Nechť R je netriviální komutativní okruh. Pak R je těleso, právě když R a $\{0\}$ jsou jediné ideály okruhu R.*

Okruh hlavních ideálů

Věta. *Nechť R je netriviální komutativní okruh. Pak R je těleso, právě když R a $\{0\}$ jsou jediné ideály okruhu R.*

Definice. Okruh R se nazývá **okruh hlavních ideálů**, jestliže

Okruh hlavních ideálů

Věta. *Nechť R je netriviální komutativní okruh. Pak R je těleso, právě když R a $\{0\}$ jsou jediné ideály okruhu R.*

Definice. Okruh R se nazývá **okruh hlavních ideálů**, jestliže

- R je obor integrity;

Okruh hlavních ideálů

Věta. *Nechť R je netriviální komutativní okruh. Pak R je těleso, právě když R a $\{0\}$ jsou jediné ideály okruhu R.*

Definice. Okruh R se nazývá **okruh hlavních ideálů**, jestliže

- R je obor integrity;
- každý ideál okruhu R je hlavní.

Okruh hlavních ideálů

Věta. *Nechť R je netriviální komutativní okruh. Pak R je těleso, právě když R a $\{0\}$ jsou jediné ideály okruhu R.*

Definice. Okruh R se nazývá **okruh hlavních ideálů**, jestliže

- R je obor integrity;
- každý ideál okruhu R je hlavní.

Příklady. Okruh $\mathbb{Z}$ je okruh hlavních ideálů.

Okruh hlavních ideálů

Věta. *Nechť R je netriviální komutativní okruh. Pak R je těleso, právě když R a $\{0\}$ jsou jediné ideály okruhu R.*

Definice. Okruh R se nazývá **okruh hlavních ideálů**, jestliže

- R je obor integrity;
- každý ideál okruhu R je hlavní.

Příklady. Okruh $\mathbb{Z}$ je okruh hlavních ideálů. Každé těleso je okruh hlavních ideálů.

Okruh hlavních ideálů

Věta. *Nechť R je netriviální komutativní okruh. Pak R je těleso, právě když R a $\{0\}$ jsou jediné ideály okruhu R.*

Definice. Okruh R se nazývá **okruh hlavních ideálů**, jestliže

- R je obor integrity;
- každý ideál okruhu R je hlavní.

Příklady. Okruh $\mathbb{Z}$ je okruh hlavních ideálů. Každé těleso je okruh hlavních ideálů. Okruh zbytkových tříd $\mathbb{Z}_m$ je okruh hlavních ideálů, právě když je m prvočíslo.

Okruh hlavních ideálů

Věta. *Nechť R je netriviální komutativní okruh. Pak R je těleso, právě když R a $\{0\}$ jsou jediné ideály okruhu R.*

Definice. Okruh R se nazývá **okruh hlavních ideálů**, jestliže

- R je obor integrity;
- každý ideál okruhu R je hlavní.

Příklady. Okruh $\mathbb{Z}$ je okruh hlavních ideálů. Každé těleso je okruh hlavních ideálů. Okruh zbytkových tříd $\mathbb{Z}_m$ je okruh hlavních ideálů, právě když je m prvočíslo. Okruh $\mathbb{Z}[x]$ není okruh hlavních ideálů.

Okruh hlavních ideálů

Věta. *Nechť R je netriviální komutativní okruh. Pak R je těleso, právě když R a $\{0\}$ jsou jediné ideály okruhu R.*

Definice. Okruh R se nazývá **okruh hlavních ideálů**, jestliže

- R je obor integrity;
- každý ideál okruhu R je hlavní.

Příklady. Okruh $\mathbb{Z}$ je okruh hlavních ideálů. Každé těleso je okruh hlavních ideálů. Okruh zbytkových tříd $\mathbb{Z}_m$ je okruh hlavních ideálů, právě když je m prvočíslo. Okruh $\mathbb{Z}[x]$ není okruh hlavních ideálů.

Věta. *Nechť R je těleso. Pak každý ideál okruhu polynomů $R[x]$ je hlavní.*

Okruh hlavních ideálů

Věta. *Nechť R je netriviální komutativní okruh. Pak R je těleso, právě když R a $\{0\}$ jsou jediné ideály okruhu R.*

Definice. Okruh R se nazývá **okruh hlavních ideálů**, jestliže

- R je obor integrity;
- každý ideál okruhu R je hlavní.

Příklady. Okruh $\mathbb{Z}$ je okruh hlavních ideálů. Každé těleso je okruh hlavních ideálů. Okruh zbytkových tříd $\mathbb{Z}_m$ je okruh hlavních ideálů, právě když je m prvočíslo. Okruh $\mathbb{Z}[x]$ není okruh hlavních ideálů.

Věta. *Nechť R je těleso. Pak každý ideál okruhu polynomů $R[x]$ je hlavní.*

Důsledek. *Nechť R je těleso. Pak okruh polynomů $R[x]$ je okruh hlavních ideálů.*

Okruh hlavních ideálů

Věta. *Nechť R je netriviální komutativní okruh. Pak R je těleso, právě když R a $\{0\}$ jsou jediné ideály okruhu R.*

Definice. Okruh R se nazývá **okruh hlavních ideálů**, jestliže

- R je obor integrity;
- každý ideál okruhu R je hlavní.

Příklady. Okruh $\mathbb{Z}$ je okruh hlavních ideálů. Každé těleso je okruh hlavních ideálů. Okruh zbytkových tříd $\mathbb{Z}_m$ je okruh hlavních ideálů, právě když je m prvočíslo. Okruh $\mathbb{Z}[x]$ není okruh hlavních ideálů.

Věta. *Nechť R je těleso. Pak každý ideál okruhu polynomů $R[x]$ je hlavní.*

Důsledek. *Nechť R je těleso. Pak okruh polynomů $R[x]$ je okruh hlavních ideálů.*

Věta. *Jestliže R je okruh hlavních ideálů, pak je R okruh s jednoznačným rozkladem.*

Důkaz je uveden například v knize Dummit, Foote: *Abstract Algebra* v kapitole 8.3.

Svaz ideálů

Věta. *Nechť $f : R \to S$ je homomorfismus okruhů.*

Svaz ideálů

Věta. *Nechť $f : R \to S$ je homomorfismus okruhů. Pak platí:*

1. *je-li J ideál okruhu S, pak $f^{-1}(J) = \{r \in R;\ f(r) \in J\}$ je ideál okruhu R;*

Svaz ideálů

Věta. *Nechť $f : R \to S$ je homomorfismus okruhů. Pak platí:*

1. *je-li J ideál okruhu S, pak $f^{-1}(J) = \{r \in R;\ f(r) \in J\}$ je ideál okruhu R;*
2. *jestliže f je surjektivní a I je ideál okruhu R, pak $f(I) = \{f(r);\ r \in I\}$ je ideál okruhu S.*

Svaz ideálů

Věta. *Nechť $f : R \to S$ je homomorfismus okruhů. Pak platí:*

1. *je-li J ideál okruhu S, pak $f^{-1}(J) = \{r \in R;\ f(r) \in J\}$ je ideál okruhu R;*
2. *jestliže f je surjektivní a I je ideál okruhu R, pak $f(I) = \{f(r);\ r \in I\}$ je ideál okruhu S.*

Důsledek. *Jádro libovolného homomorfismu okruhů $f : R \to S$ je ideál okruhu R, vždyť* $\ker f = f^{-1}(\{0\})$.

Svaz ideálů

Věta. *Nechť $f : R \to S$ je homomorfismus okruhů. Pak platí:*

1. *je-li J ideál okruhu S, pak $f^{-1}(J) = \{r \in R;\ f(r) \in J\}$ je ideál okruhu R;*
2. *jestliže f je surjektivní a I je ideál okruhu R, pak $f(I) = \{f(r);\ r \in I\}$ je ideál okruhu S.*

Důsledek. *Jádro libovolného homomorfismu okruhů $f : R \to S$ je ideál okruhu R, vždyť* $\ker f = f^{-1}(\{0\})$.

Věta. *Nechť $f : R \to S$ je surjektivní homomorfismus okruhů,*

Svaz ideálů

Věta. *Nechť $f : R \to S$ je homomorfismus okruhů. Pak platí:*

1. *je-li J ideál okruhu S, pak $f^{-1}(J) = \{r \in R;\ f(r) \in J\}$ je ideál okruhu R;*
2. *jestliže f je surjektivní a I je ideál okruhu R, pak $f(I) = \{f(r);\ r \in I\}$ je ideál okruhu S.*

Důsledek. *Jádro libovolného homomorfismu okruhů $f : R \to S$ je ideál okruhu R, vždyť* $\ker f = f^{-1}(\{0\})$.

Věta. *Nechť $f : R \to S$ je surjektivní homomorfismus okruhů, $\mathcal{R}$ je svaz všech ideálů okruhu R obsahujících* $\ker f$ *(uspořádaných inkluzí),*

Svaz ideálů

Věta. *Nechť $f : R \to S$ je homomorfismus okruhů. Pak platí:*

1. *je-li J ideál okruhu S, pak $f^{-1}(J) = \{r \in R;\ f(r) \in J\}$ je ideál okruhu R;*
2. *jestliže f je surjektivní a I je ideál okruhu R, pak $f(I) = \{f(r);\ r \in I\}$ je ideál okruhu S.*

Důsledek. *Jádro libovolného homomorfismu okruhů $f : R \to S$ je ideál okruhu R, vždyť* $\ker f = f^{-1}(\{0\})$.

Věta. *Nechť $f : R \to S$ je surjektivní homomorfismus okruhů, $\mathcal{R}$ je svaz všech ideálů okruhu R obsahujících* $\ker f$ *(uspořádaných inkluzí), $\mathcal{S}$ svaz všech ideálů okruhu S (uspořádaných inkluzí).*

Svaz ideálů

Věta. *Nechť $f : R \to S$ je homomorfismus okruhů. Pak platí:*

1. *je-li J ideál okruhu S, pak $f^{-1}(J) = \{r \in R;\ f(r) \in J\}$ je ideál okruhu R;*
2. *jestliže f je surjektivní a I je ideál okruhu R, pak $f(I) = \{f(r);\ r \in I\}$ je ideál okruhu S.*

Důsledek. *Jádro libovolného homomorfismu okruhů $f : R \to S$ je ideál okruhu R, vždyť* $\ker f = f^{-1}(\{0\})$.

Věta. *Nechť $f : R \to S$ je surjektivní homomorfismus okruhů, $\mathcal{R}$ je svaz všech ideálů okruhu R obsahujících* $\ker f$ *(uspořádaných inkluzí), $\mathcal{S}$ svaz všech ideálů okruhu S (uspořádaných inkluzí). Pak zobrazení $\Psi : \mathcal{R} \to \mathcal{S}$, dané předpisem*

$$\Psi(I) = \{f(r);\ r \in I\} \qquad \text{pro libovolné} \qquad I \in \mathcal{R},$$

je izomorfismus svazů.

Svaz ideálů

Věta. *Nechť $f : R \to S$ je homomorfismus okruhů. Pak platí:*

1. *je-li J ideál okruhu S, pak $f^{-1}(J) = \{r \in R;\ f(r) \in J\}$ je ideál okruhu R;*
2. *jestliže f je surjektivní a I je ideál okruhu R, pak $f(I) = \{f(r);\ r \in I\}$ je ideál okruhu S.*

Důsledek. *Jádro libovolného homomorfismu okruhů $f : R \to S$ je ideál okruhu R, vždyť* $\ker f = f^{-1}(\{0\})$.

Věta. *Nechť $f : R \to S$ je surjektivní homomorfismus okruhů, $\mathcal{R}$ je svaz všech ideálů okruhu R obsahujících* $\ker f$ *(uspořádaných inkluzí), $\mathcal{S}$ svaz všech ideálů okruhu S (uspořádaných inkluzí). Pak zobrazení $\Psi : \mathcal{R} \to \mathcal{S}$, dané předpisem*

$$\Psi(I) = \{f(r);\ r \in I\} \qquad \text{pro libovolné} \qquad I \in \mathcal{R},$$

je izomorfismus svazů. Inverzní zobrazení $\Psi^{-1} : \mathcal{S} \to \mathcal{R}$ splňuje

$$\Psi^{-1}(J) = \{r \in R;\ f(r) \in J\} \qquad \text{pro libovolné} \qquad J \in \mathcal{S}.$$

Opakování: faktorizace grup

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$.

Opakování: faktorizace grup

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Opakování: faktorizace grup

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Opakování: faktorizace grup

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Věta. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa.

Opakování: faktorizace grup

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$.*

Opakování: faktorizace grup

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Věta. Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa.

Opakování: faktorizace grup

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa. Zobrazení $\pi: G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří)*

Opakování: faktorizace grup

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa. Zobrazení $\pi: G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří) je surjektivní homomorfismus grup, jehož jádro* $\ker \pi = H$.

Opakování: faktorizace grup

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa. Zobrazení $\pi: G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří) je surjektivní homomorfismus grup, jehož jádro* $\ker \pi = H$.

Definice. Grupa G/H z předchozí věty se nazývá **faktorgrupa** grupy G podle (normální) podgrupy H.

Opakování: faktorizace grup

Nechť $(G, \cdot)$ je grupa, H její podgrupa. Každý prvek $a \in G$ určuje svou **levou třídu** $a \cdot H = \{a \cdot h;\ h \in H\}$. Přitom
$\forall a, b \in G: \quad (a \cdot H = b \cdot H \ \Leftrightarrow \ a \in b \cdot H \ \Leftrightarrow \ b^{-1} \cdot a \in H)$.

Rozklad grupy G podle podgrupy H je množina všech levých tříd $G/H = \{a \cdot H;\ a \in G\}$.

Věta. *Nechť $(G, \cdot)$ je grupa a H její normální podgrupa. Pak na rozkladu G/H lze zavést operaci $\cdot$ takto: pro libovolné $a, b \in G$ definujeme předpisem $(a \cdot H) \cdot (b \cdot H) = (a \cdot b) \cdot H$ součin levých tříd $a \cdot H$ a $b \cdot H$. Navíc platí: $(G/H, \cdot)$ je grupa. Zobrazení $\pi: G \to G/H$ dané předpisem $\pi(a) = a \cdot H$ pro libovolné $a \in G$ (tedy každý prvek grupy G je zobrazen na třídu, do níž patří) je surjektivní homomorfismus grup, jehož jádro* $\ker \pi = H$.

Definice. Grupa G/H z předchozí věty se nazývá **faktorgrupa** grupy G podle (normální) podgrupy H. Homomorfismus π se nazývá **projekce grupy G na faktorgrupu G/H.**

Faktorizace okruhů

Nechť $(R, +, \cdot)$ je okruh, I jeho ideál. Pak I je (normální) podgrupa komutativní grupy $(R, +)$, máme tedy faktorgrupu $(R/I, +)$, přičemž $R/I = \{a + I;\ a \in R\}$, kde $a + I = \{a + h;\ h \in I\}$.

Faktorizace okruhů

Nechť $(R, +, \cdot)$ je okruh, I jeho ideál. Pak I je (normální) podgrupa komutativní grupy $(R, +)$, máme tedy faktorgrupu $(R/I, +)$, přičemž $R/I = \{a + I;\ a \in R\}$, kde $a + I = \{a + h;\ h \in I\}$.

Platí $\forall a, b \in R:\quad (a + I = b + I \ \Leftrightarrow\ a \in b + I \ \Leftrightarrow\ a - b \in I)$,

Faktorizace okruhů

Nechť $(R, +, \cdot)$ je okruh, I jeho ideál. Pak I je (normální) podgrupa komutativní grupy $(R, +)$, máme tedy faktorgrupu $(R/I, +)$, přičemž $R/I = \{a + I;\ a \in R\}$, kde $a + I = \{a + h;\ h \in I\}$.

Platí $\forall a, b \in R:\quad (a + I = b + I \ \Leftrightarrow\ a \in b + I \ \Leftrightarrow\ a - b \in I)$,

a operace $+$ na R/I je definována pomocí reprezentantů:
$(a + I) + (b + I) = (a + b) + I$ pro každé $a, b \in R$.

Faktorizace okruhů

Nechť $(R, +, \cdot)$ je okruh, I jeho ideál. Pak I je (normální) podgrupa komutativní grupy $(R, +)$, máme tedy faktorgrupu $(R/I, +)$, přičemž $R/I = \{a + I;\ a \in R\}$, kde $a + I = \{a + h;\ h \in I\}$.

Platí $\forall a, b \in R:\quad (a + I = b + I \ \Leftrightarrow\ a \in b + I \ \Leftrightarrow\ a - b \in I)$,

a operace $+$ na R/I je definována pomocí reprezentantů:
$(a + I) + (b + I) = (a + b) + I$ pro každé $a, b \in R$.

Věta. Nechť I je ideál okruhu R. Na faktorgrupě $(R/I, +)$ lze definovat násobení pomocí reprezentantů, tedy
$(a + I) \cdot (b + I) = (a \cdot b) + I$ pro každé $a, b \in R$.

Faktorizace okruhů

Nechť $(R, +, \cdot)$ je okruh, I jeho ideál. Pak I je (normální) podgrupa komutativní grupy $(R, +)$, máme tedy faktorgrupu $(R/I, +)$, přičemž $R/I = \{a + I;\ a \in R\}$, kde $a + I = \{a + h;\ h \in I\}$.

Platí $\forall a, b \in R:\quad (a + I = b + I \ \Leftrightarrow\ a \in b + I \ \Leftrightarrow\ a - b \in I)$,

a operace $+$ na R/I je definována pomocí reprezentantů:
$(a + I) + (b + I) = (a + b) + I$ pro každé $a, b \in R$.

Věta. Nechť I je ideál okruhu R. Na faktorgrupě $(R/I, +)$ lze definovat násobení pomocí reprezentantů, tedy
$(a + I) \cdot (b + I) = (a \cdot b) + I$ pro každé $a, b \in R$. Pak $(R/I, +, \cdot)$ je okruh a projekce $\pi : R \to R/I$ je surjektivním homomorfismem okruhů s jádrem $\ker \pi = I$.

Faktorizace okruhů

Nechť $(R, +, \cdot)$ je okruh, I jeho ideál. Pak I je (normální) podgrupa komutativní grupy $(R, +)$, máme tedy faktorgrupu $(R/I, +)$, přičemž $R/I = \{a + I;\ a \in R\}$, kde $a + I = \{a + h;\ h \in I\}$.

Platí $\forall a, b \in R:\quad (a + I = b + I \ \Leftrightarrow\ a \in b + I \ \Leftrightarrow\ a - b \in I)$,

a operace $+$ na R/I je definována pomocí reprezentantů:
$(a + I) + (b + I) = (a + b) + I$ pro každé $a, b \in R$.

Věta. Nechť I je ideál okruhu R. Na faktorgrupě $(R/I, +)$ lze definovat násobení pomocí reprezentantů, tedy
$(a + I) \cdot (b + I) = (a \cdot b) + I$ pro každé $a, b \in R$. Pak $(R/I, +, \cdot)$ je okruh a projekce $\pi : R \to R/I$ je surjektivním homomorfismem okruhů s jádrem $\ker \pi = I$.

Definice. Okruh R/I z předchozí věty se nazývá **faktorokruh** okruhu R podle ideálu I.

Faktorizace okruhů

Nechť $(R, +, \cdot)$ je okruh, I jeho ideál. Pak I je (normální) podgrupa komutativní grupy $(R, +)$, máme tedy faktorgrupu $(R/I, +)$, přičemž $R/I = \{a + I;\ a \in R\}$, kde $a + I = \{a + h;\ h \in I\}$.

Platí $\forall a, b \in R:\quad (a + I = b + I \ \Leftrightarrow\ a \in b + I \ \Leftrightarrow\ a - b \in I)$,

a operace $+$ na R/I je definována pomocí reprezentantů:
$(a + I) + (b + I) = (a + b) + I$ pro každé $a, b \in R$.

Věta. Nechť I je ideál okruhu R. Na faktorgrupě $(R/I, +)$ lze definovat násobení pomocí reprezentantů, tedy
$(a + I) \cdot (b + I) = (a \cdot b) + I$ pro každé $a, b \in R$. Pak $(R/I, +, \cdot)$ je okruh a projekce $\pi : R \to R/I$ je surjektivním homomorfismem okruhů s jádrem $\ker \pi = I$.

Definice. Okruh R/I z předchozí věty se nazývá **faktorokruh** okruhu R podle ideálu I. Homomorfismu π říkáme **projekce okruhu R na faktorokruh R/I.**

Faktorizace okruhů

Nechť $(R, +, \cdot)$ je okruh, I jeho ideál. Pak I je (normální) podgrupa komutativní grupy $(R, +)$, máme tedy faktorgrupu $(R/I, +)$, přičemž $R/I = \{a + I;\ a \in R\}$, kde $a + I = \{a + h;\ h \in I\}$.

Platí $\forall a, b \in R:\quad (a + I = b + I \ \Leftrightarrow\ a \in b + I \ \Leftrightarrow\ a - b \in I)$,

a operace $+$ na R/I je definována pomocí reprezentantů:
$(a + I) + (b + I) = (a + b) + I$ pro každé $a, b \in R$.

Věta. Nechť I je ideál okruhu R. Na faktorgrupě $(R/I, +)$ lze definovat násobení pomocí reprezentantů, tedy
$(a + I) \cdot (b + I) = (a \cdot b) + I$ pro každé $a, b \in R$. Pak $(R/I, +, \cdot)$ je okruh a projekce $\pi : R \to R/I$ je surjektivním homomorfismem okruhů s jádrem $\ker \pi = I$.

Definice. Okruh R/I z předchozí věty se nazývá **faktorokruh** okruhu R podle ideálu I. Homomorfismu π říkáme **projekce okruhu R na faktorokruh R/I.**

Důsledek. Ideály okruhu R jsou právě jádra homomorfismů $R \to K$ okruhu R do vhodných okruhů K.

Vlastnosti faktorokruhů

Příklad. Pro libovolné přirozené číslo m máme hlavní ideál (m) okruhu $\mathbb{Z}$.

Vlastnosti faktorokruhů

Příklad. Pro libovolné přirozené číslo m máme hlavní ideál (m) okruhu $\mathbb{Z}$. Pak $(m) = \{k \cdot m;\ k \in \mathbb{Z}\} = [0]_m$,

Vlastnosti faktorokruhů

Příklad. Pro libovolné přirozené číslo m máme hlavní ideál (m) okruhu $\mathbb{Z}$. Pak $(m) = \{k \cdot m;\ k \in \mathbb{Z}\} = [0]_m$, a proto pro libovolné $a \in \mathbb{Z}$ je $a + (m) = \{a + k \cdot m;\ k \in \mathbb{Z}\} = [a]_m$.

Vlastnosti faktorokruhů

Příklad. Pro libovolné přirozené číslo m máme hlavní ideál (m) okruhu $\mathbb{Z}$. Pak $(m) = \{k \cdot m;\ k \in \mathbb{Z}\} = [0]_m$, a proto pro libovolné $a \in \mathbb{Z}$ je $a + (m) = \{a + k \cdot m;\ k \in \mathbb{Z}\} = [a]_m$. Tudíž faktorokruh $\mathbb{Z}/(m) = \mathbb{Z}_m$, okruh zbytkových tříd modulo m.

Vlastnosti faktorokruhů

Příklad. Pro libovolné přirozené číslo m máme hlavní ideál (m) okruhu $\mathbb{Z}$. Pak $(m) = \{k \cdot m;\ k \in \mathbb{Z}\} = [0]_m$, a proto pro libovolné $a \in \mathbb{Z}$ je $a + (m) = \{a + k \cdot m;\ k \in \mathbb{Z}\} = [a]_m$. Tudíž faktorokruh $\mathbb{Z}/(m) = \mathbb{Z}_m$, okruh zbytkových tříd modulo m.

Věta. Nechť I je ideál okruhu R. Pak platí:

Vlastnosti faktorokruhů

Příklad. Pro libovolné přirozené číslo m máme hlavní ideál (m) okruhu $\mathbb{Z}$. Pak $(m) = \{k \cdot m;\ k \in \mathbb{Z}\} = [0]_m$, a proto pro libovolné $a \in \mathbb{Z}$ je $a + (m) = \{a + k \cdot m;\ k \in \mathbb{Z}\} = [a]_m$. Tudíž faktorokruh $\mathbb{Z}/(m) = \mathbb{Z}_m$, okruh zbytkových tříd modulo m.

Věta. Nechť I je ideál okruhu R. Pak platí:

1. je-li R komutativní okruh, pak je R/I komutativní okruh;

Vlastnosti faktorokruhů

Příklad. Pro libovolné přirozené číslo m máme hlavní ideál (m) okruhu $\mathbb{Z}$. Pak $(m) = \{k \cdot m;\ k \in \mathbb{Z}\} = [0]_m$, a proto pro libovolné $a \in \mathbb{Z}$ je $a + (m) = \{a + k \cdot m;\ k \in \mathbb{Z}\} = [a]_m$. Tudíž faktorokruh $\mathbb{Z}/(m) = \mathbb{Z}_m$, okruh zbytkových tříd modulo m.

Věta. Nechť I je ideál okruhu R. Pak platí:

1. je-li R komutativní okruh, pak je R/I komutativní okruh;
2. R/I je triviální okruh, právě když $R = I$.

Vlastnosti faktorokruhů

Příklad. Pro libovolné přirozené číslo m máme hlavní ideál (m) okruhu $\mathbb{Z}$. Pak $(m) = \{k \cdot m;\ k \in \mathbb{Z}\} = [0]_m$, a proto pro libovolné $a \in \mathbb{Z}$ je $a + (m) = \{a + k \cdot m;\ k \in \mathbb{Z}\} = [a]_m$. Tudíž faktorokruh $\mathbb{Z}/(m) = \mathbb{Z}_m$, okruh zbytkových tříd modulo m.

Věta. Nechť I je ideál okruhu R. Pak platí:

1. je-li R komutativní okruh, pak je R/I komutativní okruh;
2. R/I je triviální okruh, právě když $R = I$.

Definice. Nechť I je ideál okruhu R. Řekneme, že I je **maximální ideál** okruhu R, jestliže $R \neq I$ a současně neexistuje žádný ideál J okruhu R splňující $I \subsetneq J \subsetneq R$.

Vlastnosti faktorokruhů

Příklad. Pro libovolné přirozené číslo m máme hlavní ideál (m) okruhu $\mathbb{Z}$. Pak $(m) = \{k \cdot m;\ k \in \mathbb{Z}\} = [0]_m$, a proto pro libovolné $a \in \mathbb{Z}$ je $a + (m) = \{a + k \cdot m;\ k \in \mathbb{Z}\} = [a]_m$. Tudíž faktorokruh $\mathbb{Z}/(m) = \mathbb{Z}_m$, okruh zbytkových tříd modulo m.

Věta. Nechť I je ideál okruhu R. Pak platí:

1. je-li R komutativní okruh, pak je R/I komutativní okruh;
2. R/I je triviální okruh, právě když $R = I$.

Definice. Nechť I je ideál okruhu R. Řekneme, že I je **maximální ideál** okruhu R, jestliže $R \neq I$ a současně neexistuje žádný ideál J okruhu R splňující $I \subsetneq J \subsetneq R$.

Poznámka. Množina všech ideálů daného okruhu R tvoří vzhledem k inkluzi úplný svaz.

Vlastnosti faktorokruhů

Příklad. Pro libovolné přirozené číslo m máme hlavní ideál (m) okruhu $\mathbb{Z}$. Pak $(m) = \{k \cdot m;\ k \in \mathbb{Z}\} = [0]_m$, a proto pro libovolné $a \in \mathbb{Z}$ je $a + (m) = \{a + k \cdot m;\ k \in \mathbb{Z}\} = [a]_m$. Tudíž faktorokruh $\mathbb{Z}/(m) = \mathbb{Z}_m$, okruh zbytkových tříd modulo m.

Věta. Nechť I je ideál okruhu R. Pak platí:

1. je-li R komutativní okruh, pak je R/I komutativní okruh;
2. R/I je triviální okruh, právě když $R = I$.

Definice. Nechť I je ideál okruhu R. Řekneme, že I je **maximální ideál** okruhu R, jestliže $R \neq I$ a současně neexistuje žádný ideál J okruhu R splňující $I \subsetneq J \subsetneq R$.

Poznámka. Množina všech ideálů daného okruhu R tvoří vzhledem k inkluzi úplný svaz. Odstraněním největšího ideálu, čímž je R, nám zůstane uspořádaná množina.

Vlastnosti faktorokruhů

Příklad. Pro libovolné přirozené číslo m máme hlavní ideál (m) okruhu $\mathbb{Z}$. Pak $(m) = \{k \cdot m;\ k \in \mathbb{Z}\} = [0]_m$, a proto pro libovolné $a \in \mathbb{Z}$ je $a + (m) = \{a + k \cdot m;\ k \in \mathbb{Z}\} = [a]_m$. Tudíž faktorokruh $\mathbb{Z}/(m) = \mathbb{Z}_m$, okruh zbytkových tříd modulo m.

Věta. Nechť I je ideál okruhu R. Pak platí:

1. je-li R komutativní okruh, pak je R/I komutativní okruh;
2. R/I je triviální okruh, právě když $R = I$.

Definice. Nechť I je ideál okruhu R. Řekneme, že I je **maximální ideál** okruhu R, jestliže $R \neq I$ a současně neexistuje žádný ideál J okruhu R splňující $I \subsetneq J \subsetneq R$.

Poznámka. Množina všech ideálů daného okruhu R tvoří vzhledem k inkluzi úplný svaz. Odstraněním největšího ideálu, čímž je R, nám zůstane uspořádaná množina. Maximální ideály okruhu R jsou právě maximální prvky v této uspořádané množině.

Maximální ideály, prvoideály

Věta. Nechť I je ideál **komutativního** okruhu R. Pak faktorokruh R/I je těleso, právě když I je maximální ideál okruhu R.

Maximální ideály, prvoideály

Věta. Nechť I je ideál **komutativního** okruhu R. Pak faktorokruh R/I je těleso, právě když I je maximální ideál okruhu R.

Definice. Nechť I je ideál okruhu R. Řekneme, že I je **prvoideál** okruhu R, jestliže $R \neq I$ a současně pro libovolné prvky $a, b \in R$ platí implikace $a \cdot b \in I \implies a \in I$ nebo $b \in I$.

Maximální ideály, prvoideály

Věta. Nechť I je ideál **komutativního** okruhu R. Pak faktorokruh R/I je těleso, právě když I je maximální ideál okruhu R.

Definice. Nechť I je ideál okruhu R. Řekneme, že I je **prvoideál** okruhu R, jestliže $R \neq I$ a současně pro libovolné prvky $a, b \in R$ platí implikace $a \cdot b \in I \implies a \in I$ nebo $b \in I$.

Věta. Nechť I je ideál **komutativního** *okruhu R. Pak faktorokruh R/I je obor integrity, právě když I je prvoideál okruhu R.*

Maximální ideály, prvoideály

Věta. Nechť I je ideál **komutativního** okruhu R. Pak faktorokruh R/I je těleso, právě když I je maximální ideál okruhu R.

Definice. Nechť I je ideál okruhu R. Řekneme, že I je **prvoideál** okruhu R, jestliže $R \neq I$ a současně pro libovolné prvky $a, b \in R$ platí implikace $a \cdot b \in I \implies a \in I$ nebo $b \in I$.

Věta. Nechť I je ideál **komutativního** *okruhu R. Pak faktorokruh R/I je obor integrity, právě když I je prvoideál okruhu R.*

Důsledek. Jestliže I je maximální ideál komutativního okruhu R, pak I je prvoideál okruhu R.

Maximální ideály, prvoideály

Věta. Nechť I je ideál **komutativního** okruhu R. Pak faktorokruh R/I je těleso, právě když I je maximální ideál okruhu R.

Definice. Nechť I je ideál okruhu R. Řekneme, že I je **prvoideál** okruhu R, jestliže $R \neq I$ a současně pro libovolné prvky $a, b \in R$ platí implikace $a \cdot b \in I \implies a \in I$ nebo $b \in I$.

Věta. Nechť I je ideál **komutativního** *okruhu R. Pak faktorokruh R/I je obor integrity, právě když I je prvoideál okruhu R.*

Důsledek. Jestliže I je maximální ideál komutativního okruhu R, pak I je prvoideál okruhu R.

Věta. Nechť R je těleso a $f \in R[x]$, $f \neq 0$, následující výroky jsou ekvivalentní:

Maximální ideály, prvoideály

Věta. Nechť I je ideál **komutativního** okruhu R. Pak faktorokruh R/I je těleso, právě když I je maximální ideál okruhu R.

Definice. Nechť I je ideál okruhu R. Řekneme, že I je **prvoideál** okruhu R, jestliže $R \neq I$ a současně pro libovolné prvky $a, b \in R$ platí implikace $a \cdot b \in I \implies a \in I$ nebo $b \in I$.

Věta. Nechť I je ideál **komutativního** *okruhu R. Pak faktorokruh R/I je obor integrity, právě když I je prvoideál okruhu R.*

Důsledek. Jestliže I je maximální ideál komutativního okruhu R, pak I je prvoideál okruhu R.

Věta. Nechť R je těleso a $f \in R[x]$, $f \neq 0$, následující výroky jsou ekvivalentní:

1. (f) *je maximální ideál okruhu* $R[x]$;

Maximální ideály, prvoideály

Věta. Nechť I je ideál **komutativního** okruhu R. Pak faktorokruh R/I je těleso, právě když I je maximální ideál okruhu R.

Definice. Nechť I je ideál okruhu R. Řekneme, že I je **prvoideál** okruhu R, jestliže $R \neq I$ a současně pro libovolné prvky $a, b \in R$ platí implikace $a \cdot b \in I \implies a \in I$ nebo $b \in I$.

Věta. *Nechť I je ideál* **komutativního** *okruhu R. Pak faktorokruh R/I je obor integrity, právě když I je prvoideál okruhu R.*

Důsledek. Jestliže I je maximální ideál komutativního okruhu R, pak I je prvoideál okruhu R.

Věta. *Nechť R je těleso a $f \in R[x]$, $f \neq 0$, následující výroky jsou ekvivalentní:*

1. (f) *je maximální ideál okruhu* $R[x]$;
2. (f) *je prvoideál okruhu* $R[x]$;

Maximální ideály, prvoideály

Věta. Nechť I je ideál **komutativního** okruhu R. Pak faktorokruh R/I je těleso, právě když I je maximální ideál okruhu R.

Definice. Nechť I je ideál okruhu R. Řekneme, že I je **prvoideál** okruhu R, jestliže $R \neq I$ a současně pro libovolné prvky $a, b \in R$ platí implikace $a \cdot b \in I \implies a \in I$ nebo $b \in I$.

Věta. Nechť I je ideál **komutativního** *okruhu R. Pak faktorokruh R/I je obor integrity, právě když I je prvoideál okruhu R.*

Důsledek. Jestliže I je maximální ideál komutativního okruhu R, pak I je prvoideál okruhu R.

Věta. Nechť R je těleso a $f \in R[x]$, $f \neq 0$, následující výroky jsou ekvivalentní:

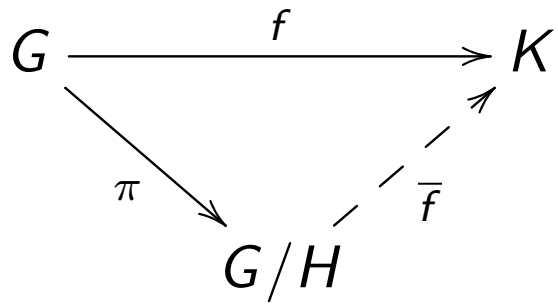
1. (f) *je maximální ideál okruhu* $R[x]$;
2. (f) *je prvoideál okruhu* $R[x]$;
3. f *je ireducibilní polynom nad* R.

Opakování: Hlavní věta o faktorgrupách

Věta (Hlavní věta o faktorgrupách). Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H.

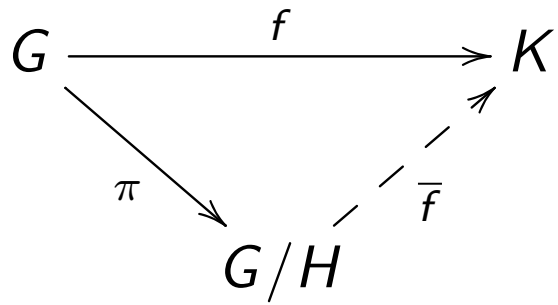
Opakování: Hlavní věta o faktorgrupách

Věta (Hlavní věta o faktorgrupách). Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H.
Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.



Opakování: Hlavní věta o faktorgrupách

Věta (Hlavní věta o faktorgrupách). Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H.
Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.

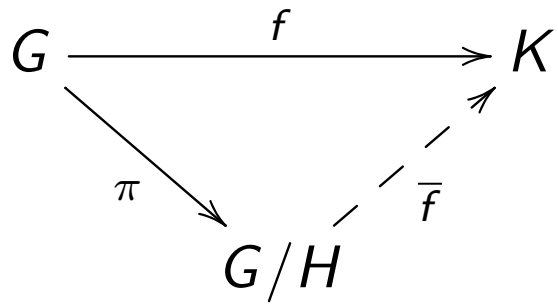


Navíc platí:

- $\overline{f}$ *je homomorfismus grup,*

Opakování: Hlavní věta o faktorgrupách

Věta (Hlavní věta o faktorgrupách). Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H.
Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.

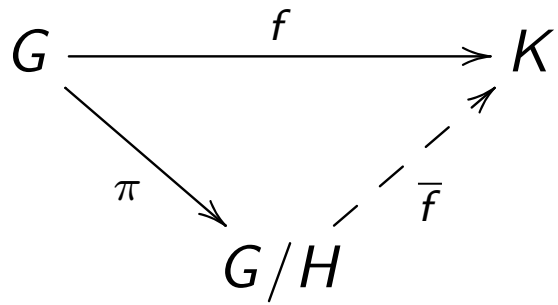


Navíc platí:

- $\overline{f}$ *je homomorfismus grup,*
- $\overline{f}$ *je injekce, právě když* $H = \ker f$,

Opakování: Hlavní věta o faktorgrupách

Věta (Hlavní věta o faktorgrupách). Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H.
Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.

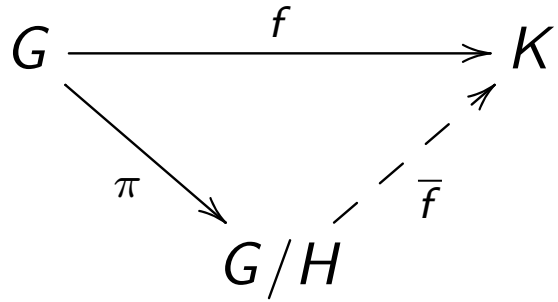


Navíc platí:

- $\overline{f}$ *je homomorfismus grup,*
- $\overline{f}$ *je injekce, právě když* $H = \ker f$,
- $\overline{f}$ *je surjekce, právě když* f *je surjekce.*

Opakování: Hlavní věta o faktorgrupách

Věta (Hlavní věta o faktorgrupách). *Nechť $f : G \to K$ je homomorfismus grup, H normální podgrupa grupy G splňující $H \subseteq \ker f$. Nechť $\pi : G \to G/H$ je projekce grupy G na faktorgrupu G/H.*
Pak existuje, a to jediné, zobrazení $\overline{f} : G/H \to K$ splňující $\overline{f} \circ \pi = f$.



Navíc platí:

- $\overline{f}$ *je homomorfismus grup,*
- $\overline{f}$ *je injekce, právě když* $H = \ker f$,
- $\overline{f}$ *je surjekce, právě když* f *je surjekce.*

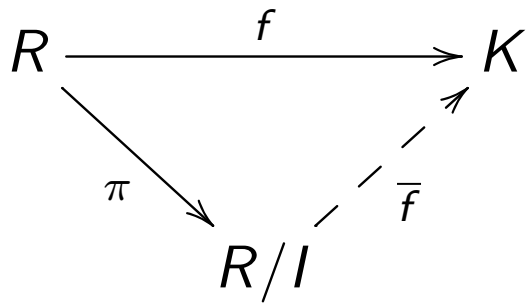
Důsledek. *Je-li $f : G \to K$ surjektivní homomorfismus grup, pak platí $G/(\ker f) \cong K$.*

Hlavní věta o faktorokruzích

Věta (Hlavní věta o faktorokruzích). Nechť $f : R \to K$ *je homomorfismus okruhů,* I *ideál okruhu* R *splňující* $I \subseteq \ker f$. *Nechť* $\pi : R \to R/I$ *je projekce okruhu* R *na faktorokruh* R/I.

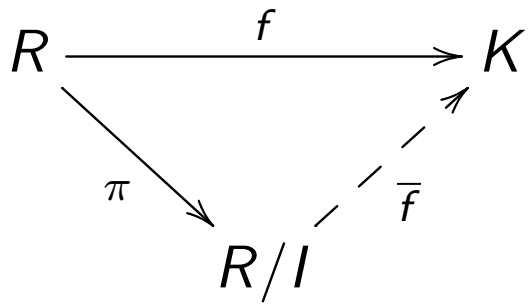
Hlavní věta o faktorokruzích

Věta (Hlavní věta o faktorokruzích). Nechť $f : R \to K$ *je homomorfismus okruhů,* I *ideál okruhu* R *splňující* $I \subseteq \ker f$. *Nechť* $\pi : R \to R/I$ *je projekce okruhu* R *na faktorokruh* R/I. *Pak existuje, a to jediné, zobrazení* $\overline{f} : R/I \to K$ *splňující* $\overline{f} \circ \pi = f$.



Hlavní věta o faktorokruzích

Věta (Hlavní věta o faktorokruzích). Nechť $f : R \to K$ je homomorfismus okruhů, I ideál okruhu R splňující $I \subseteq \ker f$. Nechť $\pi : R \to R/I$ je projekce okruhu R na faktorokruh R/I. Pak existuje, a to jediné, zobrazení $\overline{f} : R/I \to K$ splňující $\overline{f} \circ \pi = f$.

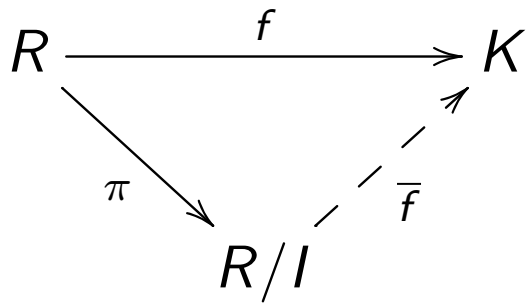


Navíc platí:

- $\overline{f}$ *je homomorfismus okruhů,*

Hlavní věta o faktorokruzích

Věta (Hlavní věta o faktorokruzích). Nechť $f : R \to K$ *je homomorfismus okruhů,* I *ideál okruhu* R *splňující* $I \subseteq \ker f$. *Nechť* $\pi : R \to R/I$ *je projekce okruhu* R *na faktorokruh* R/I. *Pak existuje, a to jediné, zobrazení* $\overline{f} : R/I \to K$ *splňující* $\overline{f} \circ \pi = f$.

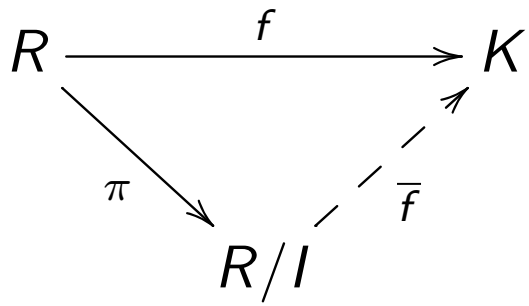


Navíc platí:

- $\overline{f}$ *je homomorfismus okruhů,*
- $\overline{f}$ *je injekce, právě když* $I = \ker f$,

Hlavní věta o faktorokruzích

Věta (Hlavní věta o faktorokruzích). Nechť $f : R \to K$ je homomorfismus okruhů, I ideál okruhu R splňující $I \subseteq \ker f$. Nechť $\pi : R \to R/I$ je projekce okruhu R na faktorokruh R/I.
Pak existuje, a to jediné, zobrazení $\overline{f} : R/I \to K$ splňující $\overline{f} \circ \pi = f$.

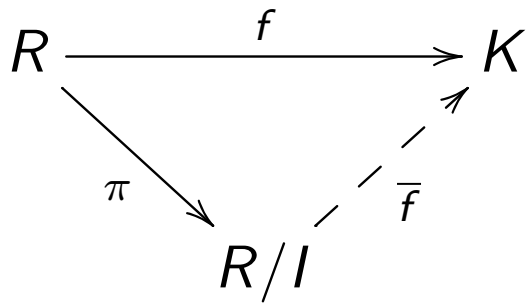


Navíc platí:

- $\overline{f}$ *je homomorfismus okruhů,*
- $\overline{f}$ *je injekce, právě když* $I = \ker f$,
- $\overline{f}$ *je surjekce, právě když* f *je surjekce.*

Hlavní věta o faktorokruzích

Věta (Hlavní věta o faktorokruzích). Nechť $f : R \to K$ *je homomorfismus okruhů,* I *ideál okruhu* R *splňující* $I \subseteq \ker f$. *Nechť* $\pi : R \to R/I$ *je projekce okruhu* R *na faktorokruh* R/I. *Pak existuje, a to jediné, zobrazení* $\overline{f} : R/I \to K$ *splňující* $\overline{f} \circ \pi = f$.



Navíc platí:

- $\overline{f}$ *je homomorfismus okruhů,*
- $\overline{f}$ *je injekce, právě když* $I = \ker f$,
- $\overline{f}$ *je surjekce, právě když* f *je surjekce.*

Důsledek. Je-li $f : R \to K$ *surjektivní homomorfismus okruhů, pak platí* $R/(\ker f) \cong K$.

Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Víme, že každý podokruh tělesa je oborem integrity.

Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Víme, že každý podokruh tělesa je oborem integrity. Pomocí explicitní konstrukce nyní ukážeme, že i naopak každý obor integrity je podokruhem vhodného tělesa.

Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Víme, že každý podokruh tělesa je oborem integrity. Pomocí explicitní konstrukce nyní ukážeme, že i naopak každý obor integrity je podokruhem vhodného tělesa. Nejprve sestrojíme pro daný komutativní okruh R „zlomky“, do jejichž jmenovatelů budeme psát prvky z jisté multiplikativní podmnožiny D.

Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Víme, že každý podokruh tělesa je oborem integrity. Pomocí explicitní konstrukce nyní ukážeme, že i naopak každý obor integrity je podokruhem vhodného tělesa. Nejprve sestrojíme pro daný komutativní okruh R „zlomky“, do jejichž jmenovatelů budeme psát prvky z jisté multiplikativní podmnožiny D.

Definice. Podmnožina D komutativního okruhu R se nazývá **multiplikativní**, jestliže $1 \in D$ a pro každé $d_1, d_2 \in D$ platí $d_1 \cdot d_2 \in D$.

Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Víme, že každý podokruh tělesa je oborem integrity. Pomocí explicitní konstrukce nyní ukážeme, že i naopak každý obor integrity je podokruhem vhodného tělesa. Nejprve sestrojíme pro daný komutativní okruh R „zlomky“, do jejichž jmenovatelů budeme psát prvky z jisté multiplikativní podmnožiny D.

Definice. Podmnožina D komutativního okruhu R se nazývá **multiplikativní**, jestliže $1 \in D$ a pro každé $d_1, d_2 \in D$ platí $d_1 \cdot d_2 \in D$.

Věta. *Nechť D je multiplikativní podmnožina komutativního okruhu R.*

Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Víme, že každý podokruh tělesa je oborem integrity. Pomocí explicitní konstrukce nyní ukážeme, že i naopak každý obor integrity je podokruhem vhodného tělesa. Nejprve sestrojíme pro daný komutativní okruh R „zlomky“, do jejichž jmenovatelů budeme psát prvky z jisté multiplikativní podmnožiny D.

Definice. Podmnožina D komutativního okruhu R se nazývá **multiplikativní**, jestliže $1 \in D$ a pro každé $d_1, d_2 \in D$ platí $d_1 \cdot d_2 \in D$.

Věta. *Nechť D je multiplikativní podmnožina komutativního okruhu R. Na množině $R \times D$ definujeme relaci $\equiv$ předpisem*

$$(a_1, d_1) \equiv (a_2, d_2) \quad \Leftrightarrow \quad \exists e \in D\colon (a_1 \cdot d_2 - a_2 \cdot d_1) \cdot e = 0$$

pro libovolné $a_1, a_2 \in R$, $d_1, d_2 \in D$.

Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Víme, že každý podokruh tělesa je oborem integrity. Pomocí explicitní konstrukce nyní ukážeme, že i naopak každý obor integrity je podokruhem vhodného tělesa. Nejprve sestrojíme pro daný komutativní okruh R „zlomky“, do jejichž jmenovatelů budeme psát prvky z jisté multiplikativní podmnožiny D.

Definice. Podmnožina D komutativního okruhu R se nazývá **multiplikativní**, jestliže $1 \in D$ a pro každé $d_1, d_2 \in D$ platí $d_1 \cdot d_2 \in D$.

Věta. *Nechť D je multiplikativní podmnožina komutativního okruhu R. Na množině $R \times D$ definujeme relaci $\equiv$ předpisem*

$$(a_1, d_1) \equiv (a_2, d_2) \quad \Leftrightarrow \quad \exists e \in D\colon (a_1 \cdot d_2 - a_2 \cdot d_1) \cdot e = 0$$

pro libovolné $a_1, a_2 \in R$, $d_1, d_2 \in D$. Pak $\equiv$ je relace ekvivalence.

Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Víme, že každý podokruh tělesa je oborem integrity. Pomocí explicitní konstrukce nyní ukážeme, že i naopak každý obor integrity je podokruhem vhodného tělesa. Nejprve sestrojíme pro daný komutativní okruh R „zlomky“, do jejichž jmenovatelů budeme psát prvky z jisté multiplikativní podmnožiny D.

Definice. Podmnožina D komutativního okruhu R se nazývá **multiplikativní**, jestliže $1 \in D$ a pro každé $d_1, d_2 \in D$ platí $d_1 \cdot d_2 \in D$.

Věta. *Nechť D je multiplikativní podmnožina komutativního okruhu R. Na množině $R \times D$ definujeme relaci $\equiv$ předpisem*

$$(a_1, d_1) \equiv (a_2, d_2) \quad \Leftrightarrow \quad \exists e \in D\colon (a_1 \cdot d_2 - a_2 \cdot d_1) \cdot e = 0$$

pro libovolné $a_1, a_2 \in R$, $d_1, d_2 \in D$. Pak $\equiv$ je relace ekvivalence.

Označení. Označme $D^{-1}R$ rozklad příslušný ekvivalenci $\equiv$, tedy $D^{-1}R = (R \times D)/\equiv$.

Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Víme, že každý podokruh tělesa je oborem integrity. Pomocí explicitní konstrukce nyní ukážeme, že i naopak každý obor integrity je podokruhem vhodného tělesa. Nejprve sestrojíme pro daný komutativní okruh R „zlomky“, do jejichž jmenovatelů budeme psát prvky z jisté multiplikativní podmnožiny D.

Definice. Podmnožina D komutativního okruhu R se nazývá **multiplikativní**, jestliže $1 \in D$ a pro každé $d_1, d_2 \in D$ platí $d_1 \cdot d_2 \in D$.

Věta. *Nechť D je multiplikativní podmnožina komutativního okruhu R. Na množině $R \times D$ definujeme relaci $\equiv$ předpisem*

$$(a_1, d_1) \equiv (a_2, d_2) \quad \Leftrightarrow \quad \exists e \in D\colon (a_1 \cdot d_2 - a_2 \cdot d_1) \cdot e = 0$$

pro libovolné $a_1, a_2 \in R$, $d_1, d_2 \in D$. Pak $\equiv$ je relace ekvivalence.

Označení. Označme $D^{-1}R$ rozklad příslušný ekvivalenci $\equiv$, tedy $D^{-1}R = (R \times D)/\equiv$. Pro libovolné $(a, d) \in R \times D$ označme $\frac{a}{d} \in D^{-1}R$ třídu obsahující (a, d).

Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Víme, že každý podokruh tělesa je oborem integrity. Pomocí explicitní konstrukce nyní ukážeme, že i naopak každý obor integrity je podokruhem vhodného tělesa. Nejprve sestrojíme pro daný komutativní okruh R „zlomky“, do jejichž jmenovatelů budeme psát prvky z jisté multiplikativní podmnožiny D.

Definice. Podmnožina D komutativního okruhu R se nazývá **multiplikativní**, jestliže $1 \in D$ a pro každé $d_1, d_2 \in D$ platí $d_1 \cdot d_2 \in D$.

Věta. *Nechť D je multiplikativní podmnožina komutativního okruhu R. Na množině $R \times D$ definujeme relaci $\equiv$ předpisem*

$$(a_1, d_1) \equiv (a_2, d_2) \quad \Leftrightarrow \quad \exists e \in D\colon (a_1 \cdot d_2 - a_2 \cdot d_1) \cdot e = 0$$

pro libovolné $a_1, a_2 \in R$, $d_1, d_2 \in D$. Pak $\equiv$ je relace ekvivalence.

Označení. Označme $D^{-1}R$ rozklad příslušný ekvivalenci $\equiv$, tedy $D^{-1}R = (R \times D)/\equiv$. Pro libovolné $(a, d) \in R \times D$ označme $\frac{a}{d} \in D^{-1}R$ třídu obsahující (a, d). Pro libovolné $a \in R$, $d \in D$ je

$$\frac{a}{d} = \{(a_1, d_1) \in R \times D;\ \exists e \in D\colon (a \cdot d_1 - a_1 \cdot d) \cdot e = 0\}.$$

Okruh zlomků komutativního okruhu R vzhledem k D

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R.*

Okruh zlomků komutativního okruhu R vzhledem k D

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R. Na $D^{-1}R$ lze definovat operace $+$ a $\cdot$ takto: pro každé $a_1, a_2 \in R$, $d_1, d_2 \in D$ definujeme*

$$\frac{a_1}{d_1} + \frac{a_2}{d_2} = \frac{a_1 \cdot d_2 + a_2 \cdot d_1}{d_1 \cdot d_2}, \qquad \frac{a_1}{d_1} \cdot \frac{a_2}{d_2} = \frac{a_1 \cdot a_2}{d_1 \cdot d_2}.$$

Okruh zlomků komutativního okruhu R vzhledem k D

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R. Na $D^{-1}R$ lze definovat operace $+$ a $\cdot$ takto: pro každé $a_1, a_2 \in R$, $d_1, d_2 \in D$ definujeme*

$$\frac{a_1}{d_1} + \frac{a_2}{d_2} = \frac{a_1 \cdot d_2 + a_2 \cdot d_1}{d_1 \cdot d_2}, \qquad \frac{a_1}{d_1} \cdot \frac{a_2}{d_2} = \frac{a_1 \cdot a_2}{d_1 \cdot d_2}.$$

Pak $(D^{-1}R, +, \cdot)$ je komutativní okruh a zobrazení $k : R \to D^{-1}R$, určené předpisem $k(a) = \frac{a}{1}$ pro každé $a \in R$, je homomorfismus okruhů.

Okruh zlomků komutativního okruhu R vzhledem k D

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R. Na $D^{-1}R$ lze definovat operace $+$ a $\cdot$ takto: pro každé $a_1, a_2 \in R$, $d_1, d_2 \in D$ definujeme*

$$\frac{a_1}{d_1} + \frac{a_2}{d_2} = \frac{a_1 \cdot d_2 + a_2 \cdot d_1}{d_1 \cdot d_2}, \qquad \frac{a_1}{d_1} \cdot \frac{a_2}{d_2} = \frac{a_1 \cdot a_2}{d_1 \cdot d_2}.$$

Pak $(D^{-1}R, +, \cdot)$ je komutativní okruh a zobrazení $k : R \to D^{-1}R$, určené předpisem $k(a) = \frac{a}{1}$ pro každé $a \in R$, je homomorfismus okruhů. Navíc platí:

- *pro každé $d \in D$ je $k(d)$ jednotka okruhu $D^{-1}R$;*

Okruh zlomků komutativního okruhu R vzhledem k D

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R. Na $D^{-1}R$ lze definovat operace $+$ a $\cdot$ takto: pro každé $a_1, a_2 \in R$, $d_1, d_2 \in D$ definujeme*

$$\frac{a_1}{d_1} + \frac{a_2}{d_2} = \frac{a_1 \cdot d_2 + a_2 \cdot d_1}{d_1 \cdot d_2}, \qquad \frac{a_1}{d_1} \cdot \frac{a_2}{d_2} = \frac{a_1 \cdot a_2}{d_1 \cdot d_2}.$$

Pak $(D^{-1}R, +, \cdot)$ je komutativní okruh a zobrazení $k : R \to D^{-1}R$, určené předpisem $k(a) = \frac{a}{1}$ pro každé $a \in R$, je homomorfismus okruhů. Navíc platí:

- *pro každé $d \in D$ je $k(d)$ jednotka okruhu $D^{-1}R$;*
- *homomorfismus k je injektivní, právě když D neobsahuje ani nulu ani žádný dělitel nuly okruhu R.*

Okruh zlomků komutativního okruhu R vzhledem k D

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R. Na $D^{-1}R$ lze definovat operace $+$ a $\cdot$ takto: pro každé $a_1, a_2 \in R$, $d_1, d_2 \in D$ definujeme*

$$\frac{a_1}{d_1} + \frac{a_2}{d_2} = \frac{a_1 \cdot d_2 + a_2 \cdot d_1}{d_1 \cdot d_2}, \qquad \frac{a_1}{d_1} \cdot \frac{a_2}{d_2} = \frac{a_1 \cdot a_2}{d_1 \cdot d_2}.$$

Pak $(D^{-1}R, +, \cdot)$ je komutativní okruh a zobrazení $k : R \to D^{-1}R$, určené předpisem $k(a) = \frac{a}{1}$ pro každé $a \in R$, je homomorfismus okruhů. Navíc platí:

- *pro každé $d \in D$ je $k(d)$ jednotka okruhu $D^{-1}R$;*
- *homomorfismus k je injektivní, právě když D neobsahuje ani nulu ani žádný dělitel nuly okruhu R.*

Důsledek. *Nechť R je obor integrity, $D = R - \{0\}$. Pak $D^{-1}R$ je těleso a $k : R \to D^{-1}R$ je vnoření.*

Okruh zlomků komutativního okruhu R vzhledem k D

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R. Na $D^{-1}R$ lze definovat operace $+$ a $\cdot$ takto: pro každé $a_1, a_2 \in R$, $d_1, d_2 \in D$ definujeme*

$$\frac{a_1}{d_1} + \frac{a_2}{d_2} = \frac{a_1 \cdot d_2 + a_2 \cdot d_1}{d_1 \cdot d_2}, \qquad \frac{a_1}{d_1} \cdot \frac{a_2}{d_2} = \frac{a_1 \cdot a_2}{d_1 \cdot d_2}.$$

Pak $(D^{-1}R, +, \cdot)$ je komutativní okruh a zobrazení $k : R \to D^{-1}R$, určené předpisem $k(a) = \frac{a}{1}$ pro každé $a \in R$, je homomorfismus okruhů. Navíc platí:

- *pro každé $d \in D$ je $k(d)$ jednotka okruhu $D^{-1}R$;*
- *homomorfismus k je injektivní, právě když D neobsahuje ani nulu ani žádný dělitel nuly okruhu R.*

Důsledek. *Nechť R je obor integrity, $D = R - \{0\}$. Pak $D^{-1}R$ je těleso a $k : R \to D^{-1}R$ je vnoření.*

Definice. Těleso $D^{-1}R$, kde R je obor integrity a $D = R - \{0\}$, se nazývá **podílové těleso** oboru integrity R. Po ztotožnění pomocí vnoření k se R stává podokruhem svého podílového tělesa.

Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Následující věta ukazuje, že konstrukce okruhu $D^{-1}R$ byla „co nejúspornější“ – množina $k(R) \cup \{k(d)^{-1}; d \in D\}$ generuje okruh $D^{-1}R$ a platí, že mezi všemi homomorfismy okruhu R do komutativních okruhů takovými, že každý prvek D zobrazují na jednotku, má homomorfismus k nejmenší jádro.

Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Následující věta ukazuje, že konstrukce okruhu $D^{-1}R$ byla „co nejúspornější“ – množina $k(R) \cup \{k(d)^{-1}; d \in D\}$ generuje okruh $D^{-1}R$ a platí, že mezi všemi homomorfismy okruhu R do komutativních okruhů takovými, že každý prvek D zobrazují na jednotku, má homomorfismus k nejmenší jádro.

Věta. Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R, nechť $D^{-1}R$ a k jsou definovány jako v předchozí větě.

Okruh zlomků komutativního okruhu R vzhledem k D

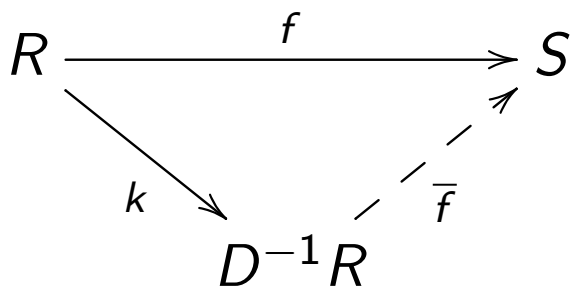
Poznámka. Následující věta ukazuje, že konstrukce okruhu $D^{-1}R$ byla „co nejúspornější“ – množina $k(R) \cup \{k(d)^{-1}; d \in D\}$ generuje okruh $D^{-1}R$ a platí, že mezi všemi homomorfismy okruhu R do komutativních okruhů takovými, že každý prvek D zobrazují na jednotku, má homomorfismus k nejmenší jádro.

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R, nechť $D^{-1}R$ a k jsou definovány jako v předchozí větě. Nechť $f : R \to S$ je homomorfismus komutativních okruhů takový, že pro každé $d \in D$ platí, že $f(d) \in S^{\times}$.*

Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Následující věta ukazuje, že konstrukce okruhu $D^{-1}R$ byla „co nejúspornější“ – množina $k(R) \cup \{k(d)^{-1}; d \in D\}$ generuje okruh $D^{-1}R$ a platí, že mezi všemi homomorfismy okruhu R do komutativních okruhů takovými, že každý prvek D zobrazují na jednotku, má homomorfismus k nejmenší jádro.

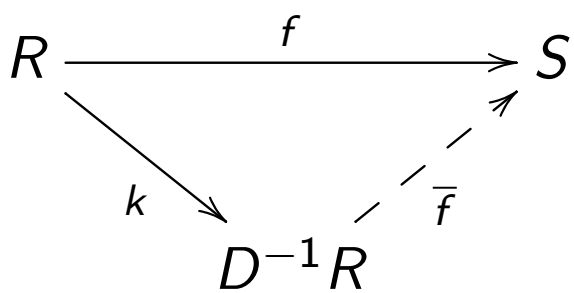
Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R, nechť $D^{-1}R$ a k jsou definovány jako v předchozí větě. Nechť $f : R \to S$ je homomorfismus komutativních okruhů takový, že pro každé $d \in D$ platí, že $f(d) \in S^{\times}$. Pak existuje, a to jediný, homomorfismus okruhů $\overline{f} : D^{-1}R \to S$ takový, že $\overline{f} \circ k = f$.*



Okruh zlomků komutativního okruhu R vzhledem k D

Poznámka. Následující věta ukazuje, že konstrukce okruhu $D^{-1}R$ byla „co nejúspornější“ – množina $k(R) \cup \{k(d)^{-1}; d \in D\}$ generuje okruh $D^{-1}R$ a platí, že mezi všemi homomorfismy okruhu R do komutativních okruhů takovými, že každý prvek D zobrazují na jednotku, má homomorfismus k nejmenší jádro.

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R, nechť $D^{-1}R$ a k jsou definovány jako v předchozí větě. Nechť $f : R \to S$ je homomorfismus komutativních okruhů takový, že pro každé $d \in D$ platí, že $f(d) \in S^\times$. Pak existuje, a to jediný, homomorfismus okruhů $\overline{f} : D^{-1}R \to S$ takový, že $\overline{f} \circ k = f$.*



Homomorfismus $\overline{f}$ je určen předpisem $\overline{f}(\frac{a}{d}) = f(a) \cdot f(d)^{-1}$ pro libovolné $a \in R$, $d \in D$.

Lokalizace komutativního okruhu R v prvoideálu P

Svou vlastností popsanou v předchozí větě je okruh $D^{-1}R$ spolu s homomorfismem k určen jednoznačně až na izomorfismus

Lokalizace komutativního okruhu R v prvoideálu P

Svou vlastností popsanou v předchozí větě je okruh $D^{-1}R$ spolu s homomorfismem k určen jednoznačně až na izomorfismus:

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R. Nechť $t : R \to T$ je homomorfismus komutativních okruhů takový, že*

- *pro každé $d \in D$ je $t(d) \in T^\times$,*

Lokalizace komutativního okruhu R v prvoideálu P

Svou vlastností popsanou v předchozí větě je okruh $D^{-1}R$ spolu s homomorfismem k určen jednoznačně až na izomorfismus:

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R. Nechť $t : R \to T$ je homomorfismus komutativních okruhů takový, že*

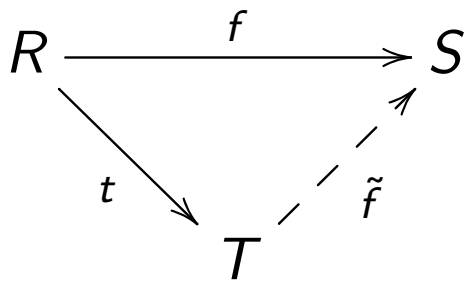
- *pro každé $d \in D$ je $t(d) \in T^\times$,*
- *pro každý komutativní okruh S a každý homomorfismus okruhů $f : R \to S$ takový, že pro každé $d \in D$ je $f(d) \in S^\times$, existuje, a to jediný, homomorfismus okruhů $\tilde{f} : T \to S$ splňující $f = \tilde{f} \circ t$.*

Lokalizace komutativního okruhu R v prvoideálu P

Svou vlastností popsanou v předchozí větě je okruh $D^{-1}R$ spolu s homomorfismem k určen jednoznačně až na izomorfismus:

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R. Nechť $t : R \to T$ je homomorfismus komutativních okruhů takový, že*

- *pro každé $d \in D$ je $t(d) \in T^\times$,*
- *pro každý komutativní okruh S a každý homomorfismus okruhů $f : R \to S$ takový, že pro každé $d \in D$ je $f(d) \in S^\times$, existuje, a to jediný, homomorfismus okruhů $\tilde{f} : T \to S$ splňující $f = \tilde{f} \circ t$.*

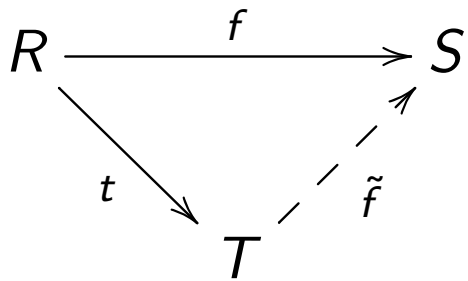


Lokalizace komutativního okruhu R v prvoideálu P

Svou vlastností popsanou v předchozí větě je okruh $D^{-1}R$ spolu s homomorfismem k určen jednoznačně až na izomorfismus:

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R. Nechť $t : R \to T$ je homomorfismus komutativních okruhů takový, že*

- *pro každé $d \in D$ je $t(d) \in T^\times$,*
- *pro každý komutativní okruh S a každý homomorfismus okruhů $f : R \to S$ takový, že pro každé $d \in D$ je $f(d) \in S^\times$, existuje, a to jediný, homomorfismus okruhů $\tilde{f} : T \to S$ splňující $f = \tilde{f} \circ t$.*



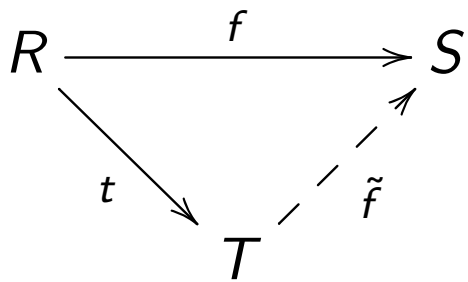
Pak pro okruh $D^{-1}R$ a homomorfismus $k : R \to D^{-1}R$ z předchozí věty platí, že $\tilde{k} : T \to D^{-1}R$ je izomorfismus okruhů splňující $k = \tilde{k} \circ t$.

Lokalizace komutativního okruhu R v prvoideálu P

Svou vlastností popsanou v předchozí větě je okruh $D^{-1}R$ spolu s homomorfismem k určen jednoznačně až na izomorfismus:

Věta. *Nechť D je multiplikativní podmnožina netriviálního komutativního okruhu R. Nechť $t : R \to T$ je homomorfismus komutativních okruhů takový, že*

- *pro každé $d \in D$ je $t(d) \in T^\times$,*
- *pro každý komutativní okruh S a každý homomorfismus okruhů $f : R \to S$ takový, že pro každé $d \in D$ je $f(d) \in S^\times$, existuje, a to jediný, homomorfismus okruhů $\tilde{f} : T \to S$ splňující $f = \tilde{f} \circ t$.*



Pak pro okruh $D^{-1}R$ a homomorfismus $k : R \to D^{-1}R$ z předchozí věty platí, že $\tilde{k} : T \to D^{-1}R$ je izomorfismus okruhů splňující $k = \tilde{k} \circ t$.

Definice. Je-li P prvoideál komutativního okruhu R, je $R - P$ multiplikativní podmnožina R a okruh $(R - P)^{-1}R$ se nazývá **lokalizace** okruhu R v prvoideálu P.

Příklady

Příklad. Podílové těleso oboru integrity $\mathbb{Z}$ je $\mathbb{Q}$.

Příklady

Příklad. Podílové těleso oboru integrity $\mathbb{Z}$ je $\mathbb{Q}$.

Příklad. Okruh $\mathbb{Z}[i] = \{x + i \cdot y; x, y \in \mathbb{Z}\}$ je obor integrity, inkluze dává jeho vnoření do $\mathbb{C}$, tj. máme injektivní homomorfismus $f : \mathbb{Z}[i] \to \mathbb{C}$, kde $f(\alpha) = \alpha$ pro $\alpha \in \mathbb{Z}[i]$.

Příklady

Příklad. Podílové těleso oboru integrity $\mathbb{Z}$ je $\mathbb{Q}$.

Příklad. Okruh $\mathbb{Z}[i] = \{x + i \cdot y; x, y \in \mathbb{Z}\}$ je obor integrity, inkluze dává jeho vnoření do $\mathbb{C}$, tj. máme injektivní homomorfismus $f : \mathbb{Z}[i] \to \mathbb{C}$, kde $f(\alpha) = \alpha$ pro $\alpha \in \mathbb{Z}[i]$. Proto podílové těleso okruhu $\mathbb{Z}[i]$ je izomorfní s $\mathbb{Q}[i] = \{\alpha \cdot \beta^{-1}; \alpha, \beta \in \mathbb{Z}[i],\ \beta \neq 0\} = \{x + i \cdot y; x, y \in \mathbb{Q}\}$.

Příklady

Příklad. Podílové těleso oboru integrity $\mathbb{Z}$ je $\mathbb{Q}$.

Příklad. Okruh $\mathbb{Z}[i] = \{x + i \cdot y; x, y \in \mathbb{Z}\}$ je obor integrity, inkluze dává jeho vnoření do $\mathbb{C}$, tj. máme injektivní homomorfismus $f : \mathbb{Z}[i] \to \mathbb{C}$, kde $f(\alpha) = \alpha$ pro $\alpha \in \mathbb{Z}[i]$. Proto podílové těleso okruhu $\mathbb{Z}[i]$ je izomorfní s $\mathbb{Q}[i] = \{\alpha \cdot \beta^{-1}; \alpha, \beta \in \mathbb{Z}[i],\ \beta \neq 0\} = \{x + i \cdot y; x, y \in \mathbb{Q}\}$.

Příklad. Podobně pro libovolné prvočíslo p podílové těleso oboru integrity $\mathbb{Z}[\sqrt{p}] = \{x + y \cdot \sqrt{p}; x, y \in \mathbb{Z}\}$ je izomorfní s tělesem $\mathbb{Q}[\sqrt{p}] = \{x + y \cdot \sqrt{p}; x, y \in \mathbb{Q}\}$.

Příklady

Příklad. Podílové těleso oboru integrity $\mathbb{Z}$ je $\mathbb{Q}$.

Příklad. Okruh $\mathbb{Z}[i] = \{x + i \cdot y; x, y \in \mathbb{Z}\}$ je obor integrity, inkluze dává jeho vnoření do $\mathbb{C}$, tj. máme injektivní homomorfismus $f : \mathbb{Z}[i] \to \mathbb{C}$, kde $f(\alpha) = \alpha$ pro $\alpha \in \mathbb{Z}[i]$. Proto podílové těleso okruhu $\mathbb{Z}[i]$ je izomorfní s $\mathbb{Q}[i] = \{\alpha \cdot \beta^{-1}; \alpha, \beta \in \mathbb{Z}[i],\ \beta \neq 0\} = \{x + i \cdot y; x, y \in \mathbb{Q}\}$.

Příklad. Podobně pro libovolné prvočíslo p podílové těleso oboru integrity $\mathbb{Z}[\sqrt{p}] = \{x + y \cdot \sqrt{p}; x, y \in \mathbb{Z}\}$ je izomorfní s tělesem $\mathbb{Q}[\sqrt{p}] = \{x + y \cdot \sqrt{p}; x, y \in \mathbb{Q}\}$.

Příklad. Je-li $R = \mathbb{Z}_{100}$ a $D = \{[2]^n_{100}; n \in \mathbb{Z}, n \geq 0\}$, pak $\ker k = \{[0]_{100}, [25]_{100}, [50]_{100}, [75]_{100}\}$ a $D^{-1}R \cong \mathbb{Z}_{25}$.

Příklady

Příklad. Podílové těleso oboru integrity $\mathbb{Z}$ je $\mathbb{Q}$.

Příklad. Okruh $\mathbb{Z}[i] = \{x + i \cdot y; x, y \in \mathbb{Z}\}$ je obor integrity, inkluze dává jeho vnoření do $\mathbb{C}$, tj. máme injektivní homomorfismus $f : \mathbb{Z}[i] \to \mathbb{C}$, kde $f(\alpha) = \alpha$ pro $\alpha \in \mathbb{Z}[i]$. Proto podílové těleso okruhu $\mathbb{Z}[i]$ je izomorfní s $\mathbb{Q}[i] = \{\alpha \cdot \beta^{-1}; \alpha, \beta \in \mathbb{Z}[i],\ \beta \neq 0\} = \{x + i \cdot y; x, y \in \mathbb{Q}\}$.

Příklad. Podobně pro libovolné prvočíslo p podílové těleso oboru integrity $\mathbb{Z}[\sqrt{p}] = \{x + y \cdot \sqrt{p}; x, y \in \mathbb{Z}\}$ je izomorfní s tělesem $\mathbb{Q}[\sqrt{p}] = \{x + y \cdot \sqrt{p}; x, y \in \mathbb{Q}\}$.

Příklad. Je-li $R = \mathbb{Z}_{100}$ a $D = \{[2]^n_{100}; n \in \mathbb{Z}, n \geq 0\}$, pak $\ker k = \{[0]_{100}, [25]_{100}, [50]_{100}, [75]_{100}\}$ a $D^{-1}R \cong \mathbb{Z}_{25}$.

Příklad. V okruhu $\mathbb{Z}$ máme kromě nulového prvoideálu $\{0\}$ také prvoideál (p) pro každé prvočíslo p.

Příklady

Příklad. Podílové těleso oboru integrity $\mathbb{Z}$ je $\mathbb{Q}$.

Příklad. Okruh $\mathbb{Z}[i] = \{x + i \cdot y; x, y \in \mathbb{Z}\}$ je obor integrity, inkluze dává jeho vnoření do $\mathbb{C}$, tj. máme injektivní homomorfismus $f : \mathbb{Z}[i] \to \mathbb{C}$, kde $f(\alpha) = \alpha$ pro $\alpha \in \mathbb{Z}[i]$. Proto podílové těleso okruhu $\mathbb{Z}[i]$ je izomorfní s $\mathbb{Q}[i] = \{\alpha \cdot \beta^{-1}; \alpha, \beta \in \mathbb{Z}[i],\ \beta \neq 0\} = \{x + i \cdot y; x, y \in \mathbb{Q}\}$.

Příklad. Podobně pro libovolné prvočíslo p podílové těleso oboru integrity $\mathbb{Z}[\sqrt{p}] = \{x + y \cdot \sqrt{p}; x, y \in \mathbb{Z}\}$ je izomorfní s tělesem $\mathbb{Q}[\sqrt{p}] = \{x + y \cdot \sqrt{p}; x, y \in \mathbb{Q}\}$.

Příklad. Je-li $R = \mathbb{Z}_{100}$ a $D = \{[2]^n_{100}; n \in \mathbb{Z}, n \geq 0\}$, pak $\ker k = \{[0]_{100}, [25]_{100}, [50]_{100}, [75]_{100}\}$ a $D^{-1}R \cong \mathbb{Z}_{25}$.

Příklad. V okruhu $\mathbb{Z}$ máme kromě nulového prvoideálu $\{0\}$ také prvoideál (p) pro každé prvočíslo p. Lokalizací $\mathbb{Z}$ v $\{0\}$ dostaneme těleso $\mathbb{Q}$, zatímco lokalizací $\mathbb{Z}$ v (p) dostáváme obor integrity $\{\frac{a}{d}; a, d \in \mathbb{Z},\ p \nmid d\} \subsetneq \mathbb{Q}$.