Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvek b **dělí** prvek a v okruhu R, neboli že prvek a **je dělitelný** prvkem b v okruhu R, píšeme $b \mid a$, jestliže existuje prvek $q \in R$ takový, že $a = q \cdot b$.

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvek b **dělí** prvek a v okruhu R, neboli že prvek a **je dělitelný** prvkem b v okruhu R, píšeme $b \mid a$, jestliže existuje prvek $q \in R$ takový, že $a = q \cdot b$. V opačném případě říkáme, že prvek b **nedělí** prvek a v okruhu R, neboli že prvek a **není dělitelný** prvkem b v okruhu R, píšeme $b \nmid a$.

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvek b **dělí** prvek a v okruhu R, neboli že prvek a **je dělitelný** prvkem b v okruhu R, píšeme $b \mid a$, jestliže existuje prvek $q \in R$ takový, že $a = q \cdot b$. V opačném případě říkáme, že prvek b **nedělí** prvek a v okruhu R, neboli že prvek a **není dělitelný** prvkem b v okruhu R, píšeme $b \nmid a$.

Věta. *Nechť R je komutativní okruh, pak platí*

- $\forall a \in R : \ 1 \mid a, \ a \mid a;$

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvek b **dělí** prvek a v okruhu R, neboli že prvek a **je dělitelný** prvkem b v okruhu R, píšeme $b \mid a$, jestliže existuje prvek $q \in R$ takový, že $a = q \cdot b$. V opačném případě říkáme, že prvek b **nedělí** prvek a v okruhu R, neboli že prvek a **není dělitelný** prvkem b v okruhu R, píšeme $b \nmid a$.

Věta. *Nechť R je komutativní okruh, pak platí*

- $\forall a \in R : \ 1 \mid a, \ a \mid a;$
- $\forall a, b, c \in R : \ a \mid b, \ b \mid c \ \Rightarrow \ a \mid c;$

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvek b **dělí** prvek a v okruhu R, neboli že prvek a **je dělitelný** prvkem b v okruhu R, píšeme $b \mid a$, jestliže existuje prvek $q \in R$ takový, že $a = q \cdot b$. V opačném případě říkáme, že prvek b **nedělí** prvek a v okruhu R, neboli že prvek a **není dělitelný** prvkem b v okruhu R, píšeme $b \nmid a$.

Věta. *Nechť R je komutativní okruh, pak platí*

- $\forall a \in R : \ 1 \mid a, \ a \mid a;$
- $\forall a, b, c \in R : \ a \mid b, \ b \mid c \ \Rightarrow \ a \mid c;$
- $\forall a, b, c \in R : \ a \mid b, \ a \mid c \ \Rightarrow \ a \mid b + c;$

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvek b **dělí** prvek a v okruhu R, neboli že prvek a **je dělitelný** prvkem b v okruhu R, píšeme $b \mid a$, jestliže existuje prvek $q \in R$ takový, že $a = q \cdot b$. V opačném případě říkáme, že prvek b **nedělí** prvek a v okruhu R, neboli že prvek a **není dělitelný** prvkem b v okruhu R, píšeme $b \nmid a$.

Věta. *Nechť R je komutativní okruh, pak platí*

- $\forall a \in R : \ 1 \mid a, \ a \mid a;$
- $\forall a, b, c \in R : \ a \mid b, \ b \mid c \ \Rightarrow \ a \mid c;$
- $\forall a, b, c \in R : \ a \mid b, \ a \mid c \ \Rightarrow \ a \mid b + c;$
- $\forall a \in R : \ a \in R^\times \ \Leftrightarrow \ a \mid 1;$

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvek b **dělí** prvek a v okruhu R, neboli že prvek a **je dělitelný** prvkem b v okruhu R, píšeme $b \mid a$, jestliže existuje prvek $q \in R$ takový, že $a = q \cdot b$. V opačném případě říkáme, že prvek b **nedělí** prvek a v okruhu R, neboli že prvek a **není dělitelný** prvkem b v okruhu R, píšeme $b \nmid a$.

Věta. *Nechť R je komutativní okruh, pak platí*

- $\forall a \in R : \ 1 \mid a, \ a \mid a;$
- $\forall a, b, c \in R : \ a \mid b, \ b \mid c \ \Rightarrow \ a \mid c;$
- $\forall a, b, c \in R : \ a \mid b, \ a \mid c \ \Rightarrow \ a \mid b + c;$
- $\forall a \in R : \ a \in R^\times \ \Leftrightarrow \ a \mid 1;$
- $\forall a, b \in R : \ a \in R^\times, \ b \mid a \ \Rightarrow \ b \in R^\times;$

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvek b **dělí** prvek a v okruhu R, neboli že prvek a **je dělitelný** prvkem b v okruhu R, píšeme $b \mid a$, jestliže existuje prvek $q \in R$ takový, že $a = q \cdot b$. V opačném případě říkáme, že prvek b **nedělí** prvek a v okruhu R, neboli že prvek a **není dělitelný** prvkem b v okruhu R, píšeme $b \nmid a$.

Věta. *Nechť R je komutativní okruh, pak platí*

- $\forall a \in R : \ 1 \mid a, \ a \mid a;$
- $\forall a, b, c \in R : \ a \mid b, \ b \mid c \ \Rightarrow \ a \mid c;$
- $\forall a, b, c \in R : \ a \mid b, \ a \mid c \ \Rightarrow \ a \mid b + c;$
- $\forall a \in R : \ a \in R^\times \ \Leftrightarrow \ a \mid 1;$
- $\forall a, b \in R : \ a \in R^\times, \ b \mid a \ \Rightarrow \ b \in R^\times;$
- $\forall a, b \in R : \ a \in R^\times \ \Rightarrow \ a \mid b.$

Dělitelnost v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvek b **dělí** prvek a v okruhu R, neboli že prvek a **je dělitelný** prvkem b v okruhu R, píšeme $b \mid a$, jestliže existuje prvek $q \in R$ takový, že $a = q \cdot b$. V opačném případě říkáme, že prvek b **nedělí** prvek a v okruhu R, neboli že prvek a **není dělitelný** prvkem b v okruhu R, píšeme $b \nmid a$.

Věta. *Nechť R je komutativní okruh, pak platí*

- $\forall a \in R : \ 1 \mid a, \ a \mid a;$
- $\forall a, b, c \in R : \ a \mid b, \ b \mid c \ \Rightarrow \ a \mid c;$
- $\forall a, b, c \in R : \ a \mid b, \ a \mid c \ \Rightarrow \ a \mid b + c;$
- $\forall a \in R : \ a \in R^\times \ \Leftrightarrow \ a \mid 1;$
- $\forall a, b \in R : \ a \in R^\times, \ b \mid a \ \Rightarrow \ b \in R^\times;$
- $\forall a, b \in R : \ a \in R^\times \ \Rightarrow \ a \mid b.$

[Věta 2.11, str. 63]

Důsledek. *Nechť R je komutativní okruh, $a_1, \ldots, a_n, b \in R$, $u_1, \ldots, u_n \in R$ libovolné. Jestliže $b \mid a_i$ pro každé $i = 1, \ldots, n$, pak $b \mid \sum_{i=1}^{n} u_i \cdot a_i$.*

Největší společný dělitel v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvky a, b jsou **asociované**, píšeme $a \sim b$, jestliže $a \mid b$ a současně $b \mid a$.

Největší společný dělitel v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvky a, b jsou **asociované**, píšeme $a \sim b$, jestliže $a \mid b$ a současně $b \mid a$.

Věta. *Nechť R je komutativní okruh. Relace asociovanosti $\sim$ je relací ekvivalence na množině R.*

Největší společný dělitel v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvky a, b jsou **asociované**, píšeme $a \sim b$, jestliže $a \mid b$ a současně $b \mid a$.

Věta. *Nechť R je komutativní okruh. Relace asociovanosti $\sim$ je relací ekvivalence na množině R.* [Věta 2.13, str. 63]

Věta. *Nechť R je obor integrity, $a, b \in R$. Pak platí $a \sim b$, právě když existuje jednotka $c \in R^\times$ tak, že $a = c \cdot b$.*

Největší společný dělitel v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvky a, b jsou **asociované**, píšeme $a \sim b$, jestliže $a \mid b$ a současně $b \mid a$.

Věta. *Nechť R je komutativní okruh. Relace asociovanosti $\sim$ je relací ekvivalence na množině R.* [Věta 2.13, str. 63]

Věta. *Nechť R je obor integrity, $a, b \in R$. Pak platí $a \sim b$, právě když existuje jednotka $c \in R^\times$ tak, že $a = c \cdot b$.* [Věta 2.15, str. 64]

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $c \mid a$, $c \mid b$, se nazývá **společný dělitel** prvků a, b.

Největší společný dělitel v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvky a, b jsou **asociované**, píšeme $a \sim b$, jestliže $a \mid b$ a současně $b \mid a$.

Věta. *Nechť R je komutativní okruh. Relace asociovanosti $\sim$ je relací ekvivalence na množině R.* [Věta 2.13, str. 63]

Věta. *Nechť R je obor integrity, $a, b \in R$. Pak platí $a \sim b$, právě když existuje jednotka $c \in R^\times$ tak, že $a = c \cdot b$.* [Věta 2.15, str. 64]

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $c \mid a$, $c \mid b$, se nazývá **společný dělitel** prvků a, b. Libovolný prvek $d \in R$ se nazývá **největší společný dělitel** prvků a, b, jestliže

- $d \mid a$, $d \mid b$,
- $\forall c \in R: \ c \mid a, c \mid b \ \Rightarrow \ c \mid d$.

Největší společný dělitel v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Řekneme, že prvky a, b jsou **asociované**, píšeme $a \sim b$, jestliže $a \mid b$ a současně $b \mid a$.

Věta. *Nechť R je komutativní okruh. Relace asociovanosti $\sim$ je relací ekvivalence na množině R.* [Věta 2.13, str. 63]

Věta. *Nechť R je obor integrity, $a, b \in R$. Pak platí $a \sim b$, právě když existuje jednotka $c \in R^\times$ tak, že $a = c \cdot b$.* [Věta 2.15, str. 64]

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $c \mid a$, $c \mid b$, se nazývá **společný dělitel** prvků a, b. Libovolný prvek $d \in R$ se nazývá **největší společný dělitel** prvků a, b, jestliže

- $d \mid a$, $d \mid b$,
- $\forall c \in R: \ c \mid a, c \mid b \ \Rightarrow \ c \mid d$.

Tedy největší společný dělitel prvků a, b je takový jejich společný dělitel, který je dělitelný každým jejich společným dělitelem.

Nejmenší společný násobek v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $a \mid c$, $b \mid c$, se nazývá **společný násobek** prvků a, b.

Nejmenší společný násobek v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $a \mid c$, $b \mid c$, se nazývá **společný násobek** prvků a, b. Libovolný prvek $d \in R$ se nazývá **nejmenší společný násobek** prvků a, b, jestliže

- $a \mid d$, $b \mid d$,
- $\forall c \in R : \ a \mid c, b \mid c \ \Rightarrow \ d \mid c$.

Nejmenší společný násobek v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $a \mid c$, $b \mid c$, se nazývá **společný násobek** prvků a, b. Libovolný prvek $d \in R$ se nazývá **nejmenší společný násobek** prvků a, b, jestliže

- $a \mid d$, $b \mid d$,
- $\forall c \in R : \ a \mid c, b \mid c \ \Rightarrow \ d \mid c$.

Tedy nejmenší společný násobek prvků a, b je takový jejich společný násobek, který dělí každý jejich společný násobek.

Nejmenší společný násobek v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $a \mid c$, $b \mid c$, se nazývá **společný násobek** prvků a, b. Libovolný prvek $d \in R$ se nazývá **nejmenší společný násobek** prvků a, b, jestliže

- $a \mid d$, $b \mid d$,
- $\forall c \in R : \ a \mid c, b \mid c \ \Rightarrow \ d \mid c$.

Tedy nejmenší společný násobek prvků a, b je takový jejich společný násobek, který dělí každý jejich společný násobek.

Poznámka. Předchozí definice mírně pozměňují dříve definované pojmy „největší společný dělitel“ a „nejmenší společný násobek“ v $\mathbb{Z}$.

Nejmenší společný násobek v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $a \mid c$, $b \mid c$, se nazývá **společný násobek** prvků a, b. Libovolný prvek $d \in R$ se nazývá **nejmenší společný násobek** prvků a, b, jestliže

- $a \mid d$, $b \mid d$,
- $\forall c \in R : \ a \mid c, b \mid c \ \Rightarrow \ d \mid c$.

Tedy nejmenší společný násobek prvků a, b je takový jejich společný násobek, který dělí každý jejich společný násobek.

Poznámka. Předchozí definice mírně pozměňují dříve definované pojmy „největší společný dělitel“ a „nejmenší společný násobek“ v $\mathbb{Z}$. Definovali jsme je totiž pomocí uspořádání podle velikosti, které v obecném okruhu nemáme k dispozici.

Nejmenší společný násobek v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $a \mid c$, $b \mid c$, se nazývá **společný násobek** prvků a, b. Libovolný prvek $d \in R$ se nazývá **nejmenší společný násobek** prvků a, b, jestliže

- $a \mid d$, $b \mid d$,
- $\forall c \in R : \; a \mid c, \, b \mid c \;\Rightarrow\; d \mid c$.

Tedy nejmenší společný násobek prvků a, b je takový jejich společný násobek, který dělí každý jejich společný násobek.

Poznámka. Předchozí definice mírně pozměňují dříve definované pojmy „největší společný dělitel“ a „nejmenší společný násobek“ v $\mathbb{Z}$. Definovali jsme je totiž pomocí uspořádání podle velikosti, které v obecném okruhu nemáme k dispozici. Dále budeme tyto pojmy používat podle nové definice, avšak zavedené označení (m, n) a $[m, n]$ ponecháme.

Nejmenší společný násobek v komutativních okruzích

Definice. Nechť R je komutativní okruh, $a, b \in R$. Libovolný prvek $c \in R$ splňující $a \mid c$, $b \mid c$, se nazývá **společný násobek** prvků a, b. Libovolný prvek $d \in R$ se nazývá **nejmenší společný násobek** prvků a, b, jestliže

- $a \mid d$, $b \mid d$,
- $\forall c \in R: \ a \mid c, b \mid c \ \Rightarrow \ d \mid c$.

Tedy nejmenší společný násobek prvků a, b je takový jejich společný násobek, který dělí každý jejich společný násobek.

Poznámka. Předchozí definice mírně pozměňují dříve definované pojmy „největší společný dělitel“ a „nejmenší společný násobek“ v $\mathbb{Z}$. Definovali jsme je totiž pomocí uspořádání podle velikosti, které v obecném okruhu nemáme k dispozici. Dále budeme tyto pojmy používat podle nové definice, avšak zavedené označení (m, n) a $[m, n]$ ponecháme. Tedy (m, n) značí *nezáporný* největší společný dělitel čísel $m, n \in \mathbb{Z}$. Podobně $[m, n]$ značí jejich *nezáporný* nejmenší společný násobek.

Ireducibilní prvek oboru integrity

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Největší společný dělitel prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost.*

Ireducibilní prvek oboru integrity

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Největší společný dělitel prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost. Také nejmenší společný násobek prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost.*

Ireducibilní prvek oboru integrity

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Největší společný dělitel prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost. Také nejmenší společný násobek prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost.* [Věta 2.17, str. 64]

Definice. Nechť R je obor integrity, $a \in R$. Řekneme, že a je **ireducibilní** prvek okruhu R, jestliže $a \neq 0$, $a \notin R^\times$ a pro každé $b, c \in R$ takové, že $a = b \cdot c$, platí $b \in R^\times$ anebo $c \in R^\times$.

Ireducibilní prvek oboru integrity

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Největší společný dělitel prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost. Také nejmenší společný násobek prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost.* [Věta 2.17, str. 64]

Definice. Nechť R je obor integrity, $a \in R$. Řekneme, že a je **ireducibilní** prvek okruhu R, jestliže $a \neq 0$, $a \notin R^\times$ a pro každé $b, c \in R$ takové, že $a = b \cdot c$, platí $b \in R^\times$ anebo $c \in R^\times$.

Příklad. Ireducibilními prvky okruhu $\mathbb{Z}$ jsou právě prvočísla a čísla k nim opačná.

Ireducibilní prvek oboru integrity

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Největší společný dělitel prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost. Také nejmenší společný násobek prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost.* [Věta 2.17, str. 64]

Definice. Nechť R je obor integrity, $a \in R$. Řekneme, že a je **ireducibilní** prvek okruhu R, jestliže $a \neq 0$, $a \notin R^\times$ a pro každé $b, c \in R$ takové, že $a = b \cdot c$, platí $b \in R^\times$ anebo $c \in R^\times$.

Příklad. Ireducibilními prvky okruhu $\mathbb{Z}$ jsou právě prvočísla a čísla k nim opačná.

Příklad. Je-li T těleso, pak v T neexistují žádné ireducibilní prvky.

Ireducibilní prvek oboru integrity

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Největší společný dělitel prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost. Také nejmenší společný násobek prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost.* [Věta 2.17, str. 64]

Definice. Nechť R je obor integrity, $a \in R$. Řekneme, že a je **ireducibilní** prvek okruhu R, jestliže $a \neq 0$, $a \notin R^\times$ a pro každé $b, c \in R$ takové, že $a = b \cdot c$, platí $b \in R^\times$ anebo $c \in R^\times$.

Příklad. Ireducibilními prvky okruhu $\mathbb{Z}$ jsou právě prvočísla a čísla k nim opačná.

Příklad. Je-li T těleso, pak v T neexistují žádné ireducibilní prvky.

Věta. *Nechť R je obor integrity, $a, b \in R$. Je-li a ireducibilní prvek okruhu R a $b \sim a$, pak je také b ireducibilní okruhu R.*

Ireducibilní prvek oboru integrity

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Největší společný dělitel prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost. Také nejmenší společný násobek prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost.* [Věta 2.17, str. 64]

Definice. Nechť R je obor integrity, $a \in R$. Řekneme, že a je **ireducibilní** prvek okruhu R, jestliže $a \neq 0$, $a \notin R^\times$ a pro každé $b, c \in R$ takové, že $a = b \cdot c$, platí $b \in R^\times$ anebo $c \in R^\times$.

Příklad. Ireducibilními prvky okruhu $\mathbb{Z}$ jsou právě prvočísla a čísla k nim opačná.

Příklad. Je-li T těleso, pak v T neexistují žádné ireducibilní prvky.

Věta. *Nechť R je obor integrity, $a, b \in R$. Je-li a ireducibilní prvek okruhu R a $b \sim a$, pak je také b ireducibilní okruhu R.*

Důkaz. Víme, že existuje jednotka $e \in R^\times$, že $a = e \cdot b$.

Ireducibilní prvek oboru integrity

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Největší společný dělitel prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost. Také nejmenší společný násobek prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost.* [Věta 2.17, str. 64]

Definice. Nechť R je obor integrity, $a \in R$. Řekneme, že a je **ireducibilní** prvek okruhu R, jestliže $a \neq 0$, $a \notin R^\times$ a pro každé $b, c \in R$ takové, že $a = b \cdot c$, platí $b \in R^\times$ anebo $c \in R^\times$.

Příklad. Ireducibilními prvky okruhu $\mathbb{Z}$ jsou právě prvočísla a čísla k nim opačná.

Příklad. Je-li T těleso, pak v T neexistují žádné ireducibilní prvky.

Věta. *Nechť R je obor integrity, $a, b \in R$. Je-li a ireducibilní prvek okruhu R a $b \sim a$, pak je také b ireducibilní okruhu R.*

Důkaz. Víme, že existuje jednotka $e \in R^\times$, že $a = e \cdot b$. Zřejmě $b \neq 0$, $b \notin R^\times$.

Ireducibilní prvek oboru integrity

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Největší společný dělitel prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost. Také nejmenší společný násobek prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost.* [Věta 2.17, str. 64]

Definice. Nechť R je obor integrity, $a \in R$. Řekneme, že a je **ireducibilní** prvek okruhu R, jestliže $a \neq 0$, $a \notin R^\times$ a pro každé $b, c \in R$ takové, že $a = b \cdot c$, platí $b \in R^\times$ anebo $c \in R^\times$.

Příklad. Ireducibilními prvky okruhu $\mathbb{Z}$ jsou právě prvočísla a čísla k nim opačná.

Příklad. Je-li T těleso, pak v T neexistují žádné ireducibilní prvky.

Věta. *Nechť R je obor integrity, $a, b \in R$. Je-li a ireducibilní prvek okruhu R a $b \sim a$, pak je také b ireducibilní okruhu R.*

Důkaz. Víme, že existuje jednotka $e \in R^\times$, že $a = e \cdot b$. Zřejmě $b \neq 0$, $b \notin R^\times$. Pro každé $x, y \in R$, $b = x \cdot y$, je $a = (e \cdot x) \cdot y$.

Ireducibilní prvek oboru integrity

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Největší společný dělitel prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost. Také nejmenší společný násobek prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost.* [Věta 2.17, str. 64]

Definice. Nechť R je obor integrity, $a \in R$. Řekneme, že a je **ireducibilní** prvek okruhu R, jestliže $a \neq 0$, $a \notin R^\times$ a pro každé $b, c \in R$ takové, že $a = b \cdot c$, platí $b \in R^\times$ anebo $c \in R^\times$.

Příklad. Ireducibilními prvky okruhu $\mathbb{Z}$ jsou právě prvočísla a čísla k nim opačná.

Příklad. Je-li T těleso, pak v T neexistují žádné ireducibilní prvky.

Věta. *Nechť R je obor integrity, $a, b \in R$. Je-li a ireducibilní prvek okruhu R a $b \sim a$, pak je také b ireducibilní okruhu R.*

Důkaz. Víme, že existuje jednotka $e \in R^\times$, že $a = e \cdot b$. Zřejmě $b \neq 0$, $b \notin R^\times$. Pro každé $x, y \in R$, $b = x \cdot y$, je $a = (e \cdot x) \cdot y$. Z ireducibility a plyne $e \cdot x \in R^\times$ nebo $y \in R^\times$, tj. $x \in R^\times$ nebo $y \in R^\times$.

Ireducibilní prvek oboru integrity

Věta. *Nechť R je komutativní okruh, $a, b \in R$. Největší společný dělitel prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost. Také nejmenší společný násobek prvků a, b, pokud existuje, je určen jednoznačně až na asociovanost.* [Věta 2.17, str. 64]

Definice. Nechť R je obor integrity, $a \in R$. Řekneme, že a je **ireducibilní** prvek okruhu R, jestliže $a \neq 0$, $a \notin R^\times$ a pro každé $b, c \in R$ takové, že $a = b \cdot c$, platí $b \in R^\times$ anebo $c \in R^\times$.

Příklad. Ireducibilními prvky okruhu $\mathbb{Z}$ jsou právě prvočísla a čísla k nim opačná.

Příklad. Je-li T těleso, pak v T neexistují žádné ireducibilní prvky.

Věta. *Nechť R je obor integrity, $a, b \in R$. Je-li a ireducibilní prvek okruhu R a $b \sim a$, pak je také b ireducibilní okruhu R.*

Důkaz. Víme, že existuje jednotka $e \in R^\times$, že $a = e \cdot b$. Zřejmě $b \neq 0$, $b \notin R^\times$. Pro každé $x, y \in R$, $b = x \cdot y$, je $a = (e \cdot x) \cdot y$. Z ireducibility a plyne $e \cdot x \in R^\times$ nebo $y \in R^\times$, tj. $x \in R^\times$ nebo $y \in R^\times$. Proto je b ireducibilní prvek okruhu R.

Okruhy s jednoznačným rozkladem

Definice. Řekneme, že R je **okruh s jednoznačným rozkladem**, jestliže

- R je obor integrity,

Okruhy s jednoznačným rozkladem

Definice. Řekneme, že R je **okruh s jednoznačným rozkladem**, jestliže

- R je obor integrity,
- každé $a \in R$, $a \neq 0$, $a \notin R^\times$, lze rozložit na součin několika ireducibilních prvků, přičemž tento součin je jednoznačný až na pořadí a asociovanost.

Okruhy s jednoznačným rozkladem

Definice. Řekneme, že R je **okruh s jednoznačným rozkladem**, jestliže

- R je obor integrity,
- každé $a \in R$, $a \neq 0$, $a \notin R^\times$, lze rozložit na součin několika ireducibilních prvků, přičemž tento součin je jednoznačný až na pořadí a asociovanost.

Příklad. Víme, že $\mathbb{Z}$ je okruh s jednoznačným rozkladem (například rozklady $6 = 2 \cdot 3 = 3 \cdot 2 = (-2) \cdot (-3) = (-3) \cdot (-2)$ se liší jen pořadím a asociovaností).

Okruhy s jednoznačným rozkladem

Definice. Řekneme, že R je **okruh s jednoznačným rozkladem**, jestliže

- R je obor integrity,
- každé $a \in R$, $a \neq 0$, $a \notin R^\times$, lze rozložit na součin několika ireducibilních prvků, přičemž tento součin je jednoznačný až na pořadí a asociovanost.

Příklad. Víme, že $\mathbb{Z}$ je okruh s jednoznačným rozkladem (například rozklady $6 = 2 \cdot 3 = 3 \cdot 2 = (-2) \cdot (-3) = (-3) \cdot (-2)$ se liší jen pořadím a asociovaností).

Příklad. Každé těleso je okruh s jednoznačným rozkladem, neboť neobsahuje žádný prvek, který by byl nenulový a nebyl jednotka.

V okruhu $\mathbb{Z}[i]$ lze dělit se zbytkem

Připomeňme, že $\mathbb{Z}[i]$ je podokruh tělesa komplexních čísel $\mathbb{C}$ generovaný množinou $\mathbb{Z} \cup \{i\}$.

V okruhu $\mathbb{Z}[i]$ lze dělit se zbytkem

Připomeňme, že $\mathbb{Z}[i]$ je podokruh tělesa komplexních čísel $\mathbb{C}$ generovaný množinou $\mathbb{Z} \cup \{i\}$. Protože je $\mathbb{Z}[i]$ podokruh tělesa, je to obor integrity.

V okruhu $\mathbb{Z}[i]$ lze dělit se zbytkem

Připomeňme, že $\mathbb{Z}[i]$ je podokruh tělesa komplexních čísel $\mathbb{C}$ generovaný množinou $\mathbb{Z} \cup \{i\}$. Protože je $\mathbb{Z}[i]$ podokruh tělesa, je to obor integrity. Ze druhé věty na straně 8 šesté přednášky plyne $\mathbb{Z}[i] = \{a + bi;\ a, b \in \mathbb{Z}\}$, neboť $i^2 = -1 \in \mathbb{Z}$.

V okruhu $\mathbb{Z}[i]$ lze dělit se zbytkem

Připomeňme, že $\mathbb{Z}[i]$ je podokruh tělesa komplexních čísel $\mathbb{C}$ generovaný množinou $\mathbb{Z} \cup \{i\}$. Protože je $\mathbb{Z}[i]$ podokruh tělesa, je to obor integrity. Ze druhé věty na straně 8 šesté přednášky plyne $\mathbb{Z}[i] = \{a + bi;\ a, b \in \mathbb{Z}\}$, neboť $i^2 = -1 \in \mathbb{Z}$.
Ukažme, že v okruhu $\mathbb{Z}[i]$ je možné dokázat větu o dělení se zbytkem (aby se dalo říct, že zbytek je „menší“ než číslo, kterým se dělilo, je třeba nějak měřit velikost zbytku).

V okruhu $\mathbb{Z}[i]$ lze dělit se zbytkem

Připomeňme, že $\mathbb{Z}[i]$ je podokruh tělesa komplexních čísel $\mathbb{C}$ generovaný množinou $\mathbb{Z} \cup \{i\}$. Protože je $\mathbb{Z}[i]$ podokruh tělesa, je to obor integrity. Ze druhé věty na straně 8 šesté přednášky plyne $\mathbb{Z}[i] = \{a + bi;\ a, b \in \mathbb{Z}\}$, neboť $i^2 = -1 \in \mathbb{Z}$.
Ukažme, že v okruhu $\mathbb{Z}[i]$ je možné dokázat větu o dělení se zbytkem (aby se dalo říct, že zbytek je „menší“ než číslo, kterým se dělilo, je třeba nějak měřit velikost zbytku).

Označení. Definujme zobrazení $N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ takto: pro libovolné číslo $\alpha \in \mathbb{Z}[i]$ klademe $N(\alpha) = |\alpha|^2$, tj. je-li $\alpha = a + bi$ pro $a, b \in \mathbb{Z}$, je $N(\alpha) = a^2 + b^2$.

V okruhu $\mathbb{Z}[i]$ lze dělit se zbytkem

Připomeňme, že $\mathbb{Z}[i]$ je podokruh tělesa komplexních čísel $\mathbb{C}$ generovaný množinou $\mathbb{Z} \cup \{i\}$. Protože je $\mathbb{Z}[i]$ podokruh tělesa, je to obor integrity. Ze druhé věty na straně 8 šesté přednášky plyne $\mathbb{Z}[i] = \{a + bi;\ a, b \in \mathbb{Z}\}$, neboť $i^2 = -1 \in \mathbb{Z}$.
Ukažme, že v okruhu $\mathbb{Z}[i]$ je možné dokázat větu o dělení se zbytkem (aby se dalo říct, že zbytek je „menší“ než číslo, kterým se dělilo, je třeba nějak měřit velikost zbytku).

Označení. Definujme zobrazení $N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ takto: pro libovolné číslo $\alpha \in \mathbb{Z}[i]$ klademe $N(\alpha) = |\alpha|^2$, tj. je-li $\alpha = a + bi$ pro $a, b \in \mathbb{Z}$, je $N(\alpha) = a^2 + b^2$.

Poznámka. Platí $N(\alpha \cdot \beta) = |\alpha \cdot \beta|^2 = |\alpha|^2 \cdot |\beta|^2 = N(\alpha) \cdot N(\beta)$.

V okruhu $\mathbb{Z}[i]$ lze dělit se zbytkem

Připomeňme, že $\mathbb{Z}[i]$ je podokruh tělesa komplexních čísel $\mathbb{C}$ generovaný množinou $\mathbb{Z} \cup \{i\}$. Protože je $\mathbb{Z}[i]$ podokruh tělesa, je to obor integrity. Ze druhé věty na straně 8 šesté přednášky plyne $\mathbb{Z}[i] = \{a + bi;\ a, b \in \mathbb{Z}\}$, neboť $i^2 = -1 \in \mathbb{Z}$.
Ukažme, že v okruhu $\mathbb{Z}[i]$ je možné dokázat větu o dělení se zbytkem (aby se dalo říct, že zbytek je „menší“ než číslo, kterým se dělilo, je třeba nějak měřit velikost zbytku).

Označení. Definujme zobrazení $N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ takto: pro libovolné číslo $\alpha \in \mathbb{Z}[i]$ klademe $N(\alpha) = |\alpha|^2$, tj. je-li $\alpha = a + bi$ pro $a, b \in \mathbb{Z}$, je $N(\alpha) = a^2 + b^2$.

Poznámka. Platí $N(\alpha \cdot \beta) = |\alpha \cdot \beta|^2 = |\alpha|^2 \cdot |\beta|^2 = N(\alpha) \cdot N(\beta)$.
Proto z $\alpha \mid \gamma$ v $\mathbb{Z}[i]$ plyne $N(\alpha) \mid N(\gamma)$ v $\mathbb{Z}$.

V okruhu $\mathbb{Z}[i]$ lze dělit se zbytkem

Připomeňme, že $\mathbb{Z}[i]$ je podokruh tělesa komplexních čísel $\mathbb{C}$ generovaný množinou $\mathbb{Z} \cup \{i\}$. Protože je $\mathbb{Z}[i]$ podokruh tělesa, je to obor integrity. Ze druhé věty na straně 8 šesté přednášky plyne $\mathbb{Z}[i] = \{a + bi;\ a, b \in \mathbb{Z}\}$, neboť $i^2 = -1 \in \mathbb{Z}$.
Ukažme, že v okruhu $\mathbb{Z}[i]$ je možné dokázat větu o dělení se zbytkem (aby se dalo říct, že zbytek je „menší“ než číslo, kterým se dělilo, je třeba nějak měřit velikost zbytku).

Označení. Definujme zobrazení $N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ takto: pro libovolné číslo $\alpha \in \mathbb{Z}[i]$ klademe $N(\alpha) = |\alpha|^2$, tj. je-li $\alpha = a + bi$ pro $a, b \in \mathbb{Z}$, je $N(\alpha) = a^2 + b^2$.

Poznámka. Platí $N(\alpha \cdot \beta) = |\alpha \cdot \beta|^2 = |\alpha|^2 \cdot |\beta|^2 = N(\alpha) \cdot N(\beta)$. Proto z $\alpha \mid \gamma$ v $\mathbb{Z}[i]$ plyne $N(\alpha) \mid N(\gamma)$ v $\mathbb{Z}$. Odtud plyne $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

V okruhu $\mathbb{Z}[i]$ lze dělit se zbytkem

Připomeňme, že $\mathbb{Z}[i]$ je podokruh tělesa komplexních čísel $\mathbb{C}$ generovaný množinou $\mathbb{Z} \cup \{i\}$. Protože je $\mathbb{Z}[i]$ podokruh tělesa, je to obor integrity. Ze druhé věty na straně 8 šesté přednášky plyne $\mathbb{Z}[i] = \{a + bi;\ a, b \in \mathbb{Z}\}$, neboť $i^2 = -1 \in \mathbb{Z}$.
Ukažme, že v okruhu $\mathbb{Z}[i]$ je možné dokázat větu o dělení se zbytkem (aby se dalo říct, že zbytek je „menší“ než číslo, kterým se dělilo, je třeba nějak měřit velikost zbytku).

Označení. Definujme zobrazení $N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$ takto: pro libovolné číslo $\alpha \in \mathbb{Z}[i]$ klademe $N(\alpha) = |\alpha|^2$, tj. je-li $\alpha = a + bi$ pro $a, b \in \mathbb{Z}$, je $N(\alpha) = a^2 + b^2$.

Poznámka. Platí $N(\alpha \cdot \beta) = |\alpha \cdot \beta|^2 = |\alpha|^2 \cdot |\beta|^2 = N(\alpha) \cdot N(\beta)$. Proto z $\alpha \mid \gamma$ v $\mathbb{Z}[i]$ plyne $N(\alpha) \mid N(\gamma)$ v $\mathbb{Z}$. Odtud plyne $\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$.

Věta (o dělení se zbytkem). Pro libovolné $\alpha, \beta \in \mathbb{Z}[i]$, $\beta \neq 0$, existují $\gamma, \delta \in \mathbb{Z}[i]$ tak, že $\alpha = \beta \cdot \gamma + \delta$ a současně $N(\delta) < N(\beta)$.

$\mathbb{Z}[i]$ je okruh s jednoznačným rozkladem

Věta. *Pro libovolné $\alpha, \beta \in \mathbb{Z}[i]$ existuje v $\mathbb{Z}[i]$ největší společný dělitel $\delta \in \mathbb{Z}[i]$, který lze spočítat pomocí Eukleidova algoritmu a který splňuje Bezoutovu rovnost, tj. existují $\sigma, \tau \in \mathbb{Z}[i]$ tak, že $\delta = \sigma\alpha + \tau\beta$.*

$\mathbb{Z}[i]$ je okruh s jednoznačným rozkladem

Věta. *Pro libovolné $\alpha, \beta \in \mathbb{Z}[i]$ existuje v $\mathbb{Z}[i]$ největší společný dělitel $\delta \in \mathbb{Z}[i]$, který lze spočítat pomocí Eukleidova algoritmu a který splňuje Bezoutovu rovnost, tj. existují $\sigma, \tau \in \mathbb{Z}[i]$ tak, že $\delta = \sigma\alpha + \tau\beta$.*

Definice. Čísla $\alpha, \beta \in \mathbb{Z}[i]$ nazýváme nesoudělná v $\mathbb{Z}[i]$, je-li 1 jejich největší společný dělitel v $\mathbb{Z}[i]$.

$\mathbb{Z}[i]$ je okruh s jednoznačným rozkladem

Věta. *Pro libovolné $\alpha, \beta \in \mathbb{Z}[i]$ existuje v $\mathbb{Z}[i]$ největší společný dělitel $\delta \in \mathbb{Z}[i]$, který lze spočítat pomocí Eukleidova algoritmu a který splňuje Bezoutovu rovnost, tj. existují $\sigma, \tau \in \mathbb{Z}[i]$ tak, že $\delta = \sigma\alpha + \tau\beta$.*

Definice. Čísla $\alpha, \beta \in \mathbb{Z}[i]$ nazýváme nesoudělná v $\mathbb{Z}[i]$, je-li 1 jejich největší společný dělitel v $\mathbb{Z}[i]$.

Důsledek. *Čísla $\alpha, \beta \in \mathbb{Z}[i]$ jsou nesoudělná v $\mathbb{Z}[i]$, právě když existují $\sigma, \tau \in \mathbb{Z}[i]$ tak, že $\sigma\alpha + \tau\beta = 1$.*

$\mathbb{Z}[i]$ je okruh s jednoznačným rozkladem

Věta. *Pro libovolné $\alpha, \beta \in \mathbb{Z}[i]$ existuje v $\mathbb{Z}[i]$ největší společný dělitel $\delta \in \mathbb{Z}[i]$, který lze spočítat pomocí Eukleidova algoritmu a který splňuje Bezoutovu rovnost, tj. existují $\sigma, \tau \in \mathbb{Z}[i]$ tak, že $\delta = \sigma\alpha + \tau\beta$.*

Definice. Čísla $\alpha, \beta \in \mathbb{Z}[i]$ nazýváme nesoudělná v $\mathbb{Z}[i]$, je-li 1 jejich největší společný dělitel v $\mathbb{Z}[i]$.

Důsledek. *Čísla $\alpha, \beta \in \mathbb{Z}[i]$ jsou nesoudělná v $\mathbb{Z}[i]$, právě když existují $\sigma, \tau \in \mathbb{Z}[i]$ tak, že $\sigma\alpha + \tau\beta = 1$.*

Důsledek. *Pro libovolná čísla $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ platí: jestliže $\alpha \mid \beta \cdot \gamma$ v $\mathbb{Z}[i]$ a současně jsou α, β nesoudělná, pak $\alpha \mid \gamma$ v $\mathbb{Z}[i]$.*

$\mathbb{Z}[i]$ je okruh s jednoznačným rozkladem

Věta. *Pro libovolné $\alpha, \beta \in \mathbb{Z}[i]$ existuje v $\mathbb{Z}[i]$ největší společný dělitel $\delta \in \mathbb{Z}[i]$, který lze spočítat pomocí Eukleidova algoritmu a který splňuje Bezoutovu rovnost, tj. existují $\sigma, \tau \in \mathbb{Z}[i]$ tak, že $\delta = \sigma\alpha + \tau\beta$.*

Definice. Čísla $\alpha, \beta \in \mathbb{Z}[i]$ nazýváme nesoudělná v $\mathbb{Z}[i]$, je-li 1 jejich největší společný dělitel v $\mathbb{Z}[i]$.

Důsledek. *Čísla $\alpha, \beta \in \mathbb{Z}[i]$ jsou nesoudělná v $\mathbb{Z}[i]$, právě když existují $\sigma, \tau \in \mathbb{Z}[i]$ tak, že $\sigma\alpha + \tau\beta = 1$.*

Důsledek. *Pro libovolná čísla $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ platí: jestliže $\alpha \mid \beta \cdot \gamma$ v $\mathbb{Z}[i]$ a současně jsou α, β nesoudělná, pak $\alpha \mid \gamma$ v $\mathbb{Z}[i]$.*

Důsledek. *Pro libovolná čísla $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ platí: jestliže α je ireducibilní prvek v $\mathbb{Z}[i]$ splňující $\alpha \mid \beta \cdot \gamma$ v $\mathbb{Z}[i]$, pak $\alpha \mid \beta$ v $\mathbb{Z}[i]$ nebo $\alpha \mid \gamma$ v $\mathbb{Z}[i]$.*

$\mathbb{Z}[i]$ je okruh s jednoznačným rozkladem

Věta. *Pro libovolné $\alpha, \beta \in \mathbb{Z}[i]$ existuje v $\mathbb{Z}[i]$ největší společný dělitel $\delta \in \mathbb{Z}[i]$, který lze spočítat pomocí Eukleidova algoritmu a který splňuje Bezoutovu rovnost, tj. existují $\sigma, \tau \in \mathbb{Z}[i]$ tak, že $\delta = \sigma\alpha + \tau\beta$.*

Definice. Čísla $\alpha, \beta \in \mathbb{Z}[i]$ nazýváme nesoudělná v $\mathbb{Z}[i]$, je-li 1 jejich největší společný dělitel v $\mathbb{Z}[i]$.

Důsledek. *Čísla $\alpha, \beta \in \mathbb{Z}[i]$ jsou nesoudělná v $\mathbb{Z}[i]$, právě když existují $\sigma, \tau \in \mathbb{Z}[i]$ tak, že $\sigma\alpha + \tau\beta = 1$.*

Důsledek. *Pro libovolná čísla $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ platí: jestliže $\alpha \mid \beta \cdot \gamma$ v $\mathbb{Z}[i]$ a současně jsou α, β nesoudělná, pak $\alpha \mid \gamma$ v $\mathbb{Z}[i]$.*

Důsledek. *Pro libovolná čísla $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ platí: jestliže α je ireducibilní prvek v $\mathbb{Z}[i]$ splňující $\alpha \mid \beta \cdot \gamma$ v $\mathbb{Z}[i]$, pak $\alpha \mid \beta$ v $\mathbb{Z}[i]$ nebo $\alpha \mid \gamma$ v $\mathbb{Z}[i]$.*

Věta. *$\mathbb{Z}[i]$ je okruh s jednoznačným rozkladem.*

$\mathbb{Z}[i]$ je okruh s jednoznačným rozkladem

Věta. *Pro libovolné $\alpha, \beta \in \mathbb{Z}[i]$ existuje v $\mathbb{Z}[i]$ největší společný dělitel $\delta \in \mathbb{Z}[i]$, který lze spočítat pomocí Eukleidova algoritmu a který splňuje Bezoutovu rovnost, tj. existují $\sigma, \tau \in \mathbb{Z}[i]$ tak, že $\delta = \sigma\alpha + \tau\beta$.*

Definice. Čísla $\alpha, \beta \in \mathbb{Z}[i]$ nazýváme nesoudělná v $\mathbb{Z}[i]$, je-li 1 jejich největší společný dělitel v $\mathbb{Z}[i]$.

Důsledek. *Čísla $\alpha, \beta \in \mathbb{Z}[i]$ jsou nesoudělná v $\mathbb{Z}[i]$, právě když existují $\sigma, \tau \in \mathbb{Z}[i]$ tak, že $\sigma\alpha + \tau\beta = 1$.*

Důsledek. *Pro libovolná čísla $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ platí: jestliže $\alpha \mid \beta \cdot \gamma$ v $\mathbb{Z}[i]$ a současně jsou α, β nesoudělná, pak $\alpha \mid \gamma$ v $\mathbb{Z}[i]$.*

Důsledek. *Pro libovolná čísla $\alpha, \beta, \gamma \in \mathbb{Z}[i]$ platí: jestliže α je ireducibilní prvek v $\mathbb{Z}[i]$ splňující $\alpha \mid \beta \cdot \gamma$ v $\mathbb{Z}[i]$, pak $\alpha \mid \beta$ v $\mathbb{Z}[i]$ nebo $\alpha \mid \gamma$ v $\mathbb{Z}[i]$.*

Věta. *$\mathbb{Z}[i]$ je okruh s jednoznačným rozkladem.*

Poznámka. Stejným postupem lze ukázat, že $\mathbb{Z}[i\sqrt{2}]$ a $\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]$ jsou okruhy s jednoznačným rozkladem.

$\mathbb{Z}[i\sqrt{5}]$ není okruh s jednoznačným rozkladem

Nechť $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}$.

$\mathbb{Z}[i\sqrt{5}]$ není okruh s jednoznačným rozkladem

Nechť $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}$. Pak R je obor integrity, protože je podokruhem $\mathbb{C}$.

$\mathbb{Z}[i\sqrt{5}]$ není okruh s jednoznačným rozkladem

Nechť $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}$. Pak R je obor integrity, protože je podokruhem $\mathbb{C}$. Definujme zobrazení $N : R \to \mathbb{Z}$ takto: pro libovolné $\alpha = a + bi\sqrt{5}$ klademe $N(\alpha) = |\alpha|^2 = a^2 + 5b^2$.

$\mathbb{Z}[i\sqrt{5}]$ není okruh s jednoznačným rozkladem

Nechť $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}$. Pak R je obor integrity, protože je podokruhem $\mathbb{C}$. Definujme zobrazení $N : R \to \mathbb{Z}$ takto: pro libovolné $\alpha = a + bi\sqrt{5}$ klademe $N(\alpha) = |\alpha|^2 = a^2 + 5b^2$.

Jestliže $\beta \mid \alpha$ v R, existuje $\gamma \in R$ tak, že $\alpha = \beta \cdot \gamma$, a tedy $N(\alpha) = |\beta \cdot \gamma|^2 = |\beta|^2 \cdot |\gamma|^2 = N(\beta) \cdot N(\gamma)$, tudíž $N(\beta) \mid N(\alpha)$ v $\mathbb{Z}$.

$\mathbb{Z}[i\sqrt{5}]$ není okruh s jednoznačným rozkladem

Nechť $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}$. Pak R je obor integrity, protože je podokruhem $\mathbb{C}$. Definujme zobrazení $N : R \to \mathbb{Z}$ takto: pro libovolné $\alpha = a + bi\sqrt{5}$ klademe $N(\alpha) = |\alpha|^2 = a^2 + 5b^2$.

Jestliže $\beta \mid \alpha$ v R, existuje $\gamma \in R$ tak, že $\alpha = \beta \cdot \gamma$, a tedy $N(\alpha) = |\beta \cdot \gamma|^2 = |\beta|^2 \cdot |\gamma|^2 = N(\beta) \cdot N(\gamma)$, tudíž $N(\beta) \mid N(\alpha)$ v $\mathbb{Z}$.

Je-li $\alpha = a + bi\sqrt{5} \in R^\times$, pak $\alpha \mid 1$ v R, a proto $N(\alpha) \mid N(1) = 1$.

$\mathbb{Z}[i\sqrt{5}]$ není okruh s jednoznačným rozkladem

Nechť $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}$. Pak R je obor integrity, protože je podokruhem $\mathbb{C}$. Definujme zobrazení $N : R \to \mathbb{Z}$ takto: pro libovolné $\alpha = a + bi\sqrt{5}$ klademe $N(\alpha) = |\alpha|^2 = a^2 + 5b^2$.

Jestliže $\beta \mid \alpha$ v R, existuje $\gamma \in R$ tak, že $\alpha = \beta \cdot \gamma$, a tedy $N(\alpha) = |\beta \cdot \gamma|^2 = |\beta|^2 \cdot |\gamma|^2 = N(\beta) \cdot N(\gamma)$, tudíž $N(\beta) \mid N(\alpha)$ v $\mathbb{Z}$.

Je-li $\alpha = a + bi\sqrt{5} \in R^\times$, pak $\alpha \mid 1$ v R, a proto $N(\alpha) \mid N(1) = 1$. Odtud $a^2 + 5b^2 = 1$, proto $b = 0$, $a = \pm 1$.

$\mathbb{Z}[i\sqrt{5}]$ není okruh s jednoznačným rozkladem

Nechť $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}$. Pak R je obor integrity, protože je podokruhem $\mathbb{C}$. Definujme zobrazení $N : R \to \mathbb{Z}$ takto: pro libovolné $\alpha = a + bi\sqrt{5}$ klademe $N(\alpha) = |\alpha|^2 = a^2 + 5b^2$.

Jestliže $\beta \mid \alpha$ v R, existuje $\gamma \in R$ tak, že $\alpha = \beta \cdot \gamma$, a tedy $N(\alpha) = |\beta \cdot \gamma|^2 = |\beta|^2 \cdot |\gamma|^2 = N(\beta) \cdot N(\gamma)$, tudíž $N(\beta) \mid N(\alpha)$ v $\mathbb{Z}$.

Je-li $\alpha = a + bi\sqrt{5} \in R^\times$, pak $\alpha \mid 1$ v R, a proto $N(\alpha) \mid N(1) = 1$. Odtud $a^2 + 5b^2 = 1$, proto $b = 0$, $a = \pm 1$. Je tedy $R^\times = \{1, -1\}$.

$\mathbb{Z}[i\sqrt{5}]$ není okruh s jednoznačným rozkladem

Nechť $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}$. Pak R je obor integrity, protože je podokruhem $\mathbb{C}$. Definujme zobrazení $N : R \to \mathbb{Z}$ takto: pro libovolné $\alpha = a + bi\sqrt{5}$ klademe $N(\alpha) = |\alpha|^2 = a^2 + 5b^2$.

Jestliže $\beta \mid \alpha$ v R, existuje $\gamma \in R$ tak, že $\alpha = \beta \cdot \gamma$, a tedy $N(\alpha) = |\beta \cdot \gamma|^2 = |\beta|^2 \cdot |\gamma|^2 = N(\beta) \cdot N(\gamma)$, tudíž $N(\beta) \mid N(\alpha)$ v $\mathbb{Z}$.

Je-li $\alpha = a + bi\sqrt{5} \in R^\times$, pak $\alpha \mid 1$ v R, a proto $N(\alpha) \mid N(1) = 1$. Odtud $a^2 + 5b^2 = 1$, proto $b = 0$, $a = \pm 1$. Je tedy $R^\times = \{1, -1\}$.

Platí $6 = 2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$, přitom tito všichni čtyři činitelé jsou ireducibilními prvky okruhu R.

$\mathbb{Z}[i\sqrt{5}]$ není okruh s jednoznačným rozkladem

Nechť $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}$. Pak R je obor integrity, protože je podokruhem $\mathbb{C}$. Definujme zobrazení $N : R \to \mathbb{Z}$ takto: pro libovolné $\alpha = a + bi\sqrt{5}$ klademe $N(\alpha) = |\alpha|^2 = a^2 + 5b^2$.

Jestliže $\beta \mid \alpha$ v R, existuje $\gamma \in R$ tak, že $\alpha = \beta \cdot \gamma$, a tedy $N(\alpha) = |\beta \cdot \gamma|^2 = |\beta|^2 \cdot |\gamma|^2 = N(\beta) \cdot N(\gamma)$, tudíž $N(\beta) \mid N(\alpha)$ v $\mathbb{Z}$.

Je-li $\alpha = a + bi\sqrt{5} \in R^\times$, pak $\alpha \mid 1$ v R, a proto $N(\alpha) \mid N(1) = 1$. Odtud $a^2 + 5b^2 = 1$, proto $b = 0$, $a = \pm 1$. Je tedy $R^\times = \{1, -1\}$.

Platí $6 = 2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$, přitom tito všichni čtyři činitelé jsou ireducibilními prvky okruhu R. Je totiž $N(2) = 4$, $N(3) = 9$, $N(1 + i\sqrt{5}) = N(1 - i\sqrt{5}) = 6$.

$\mathbb{Z}[i\sqrt{5}]$ není okruh s jednoznačným rozkladem

Nechť $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}$. Pak R je obor integrity, protože je podokruhem $\mathbb{C}$. Definujme zobrazení $N : R \to \mathbb{Z}$ takto: pro libovolné $\alpha = a + bi\sqrt{5}$ klademe $N(\alpha) = |\alpha|^2 = a^2 + 5b^2$.

Jestliže $\beta \mid \alpha$ v R, existuje $\gamma \in R$ tak, že $\alpha = \beta \cdot \gamma$, a tedy $N(\alpha) = |\beta \cdot \gamma|^2 = |\beta|^2 \cdot |\gamma|^2 = N(\beta) \cdot N(\gamma)$, tudíž $N(\beta) \mid N(\alpha)$ v $\mathbb{Z}$.

Je-li $\alpha = a + bi\sqrt{5} \in R^\times$, pak $\alpha \mid 1$ v R, a proto $N(\alpha) \mid N(1) = 1$. Odtud $a^2 + 5b^2 = 1$, proto $b = 0$, $a = \pm 1$. Je tedy $R^\times = \{1, -1\}$.

Platí $6 = 2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$, přitom tito všichni čtyři činitelé jsou ireducibilními prvky okruhu R. Je totiž $N(2) = 4$, $N(3) = 9$, $N(1 + i\sqrt{5}) = N(1 - i\sqrt{5}) = 6$. Kdyby například $1 + i\sqrt{5} = \gamma \cdot \delta$ pro nějaké $\gamma, \delta \in R - R^\times$, platilo by $N(\gamma) > 1$, $N(\delta) > 1$, $N(\gamma) \cdot N(\delta) = 6$.

$\mathbb{Z}[i\sqrt{5}]$ není okruh s jednoznačným rozkladem

Nechť $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}$. Pak R je obor integrity, protože je podokruhem $\mathbb{C}$. Definujme zobrazení $N : R \to \mathbb{Z}$ takto: pro libovolné $\alpha = a + bi\sqrt{5}$ klademe $N(\alpha) = |\alpha|^2 = a^2 + 5b^2$.

Jestliže $\beta \mid \alpha$ v R, existuje $\gamma \in R$ tak, že $\alpha = \beta \cdot \gamma$, a tedy $N(\alpha) = |\beta \cdot \gamma|^2 = |\beta|^2 \cdot |\gamma|^2 = N(\beta) \cdot N(\gamma)$, tudíž $N(\beta) \mid N(\alpha)$ v $\mathbb{Z}$.

Je-li $\alpha = a + bi\sqrt{5} \in R^\times$, pak $\alpha \mid 1$ v R, a proto $N(\alpha) \mid N(1) = 1$. Odtud $a^2 + 5b^2 = 1$, proto $b = 0$, $a = \pm 1$. Je tedy $R^\times = \{1, -1\}$.

Platí $6 = 2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$, přitom tito všichni čtyři činitelé jsou ireducibilními prvky okruhu R. Je totiž $N(2) = 4$, $N(3) = 9$, $N(1 + i\sqrt{5}) = N(1 - i\sqrt{5}) = 6$. Kdyby například $1 + i\sqrt{5} = \gamma \cdot \delta$ pro nějaké $\gamma, \delta \in R - R^\times$, platilo by $N(\gamma) > 1$, $N(\delta) > 1$, $N(\gamma) \cdot N(\delta) = 6$. Proto $N(\gamma) \in \{2, 3\}$, což je spor, protože rovnice $x^2 + 5y^2 = 2$ a $x^2 + 5y^2 = 3$ nemají řešení v $\mathbb{Z}$.

$\mathbb{Z}[i\sqrt{5}]$ není okruh s jednoznačným rozkladem

Nechť $R = \mathbb{Z}[i\sqrt{5}] = \{a + bi\sqrt{5};\ a, b \in \mathbb{Z}\}$. Pak R je obor integrity, protože je podokruhem $\mathbb{C}$. Definujme zobrazení $N : R \to \mathbb{Z}$ takto: pro libovolné $\alpha = a + bi\sqrt{5}$ klademe $N(\alpha) = |\alpha|^2 = a^2 + 5b^2$.

Jestliže $\beta \mid \alpha$ v R, existuje $\gamma \in R$ tak, že $\alpha = \beta \cdot \gamma$, a tedy $N(\alpha) = |\beta \cdot \gamma|^2 = |\beta|^2 \cdot |\gamma|^2 = N(\beta) \cdot N(\gamma)$, tudíž $N(\beta) \mid N(\alpha)$ v $\mathbb{Z}$.

Je-li $\alpha = a + bi\sqrt{5} \in R^\times$, pak $\alpha \mid 1$ v R, a proto $N(\alpha) \mid N(1) = 1$. Odtud $a^2 + 5b^2 = 1$, proto $b = 0$, $a = \pm 1$. Je tedy $R^\times = \{1, -1\}$.

Platí $6 = 2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$, přitom tito všichni čtyři činitelé jsou ireducibilními prvky okruhu R. Je totiž $N(2) = 4$, $N(3) = 9$, $N(1 + i\sqrt{5}) = N(1 - i\sqrt{5}) = 6$. Kdyby například $1 + i\sqrt{5} = \gamma \cdot \delta$ pro nějaké $\gamma, \delta \in R - R^\times$, platilo by $N(\gamma) > 1$, $N(\delta) > 1$, $N(\gamma) \cdot N(\delta) = 6$. Proto $N(\gamma) \in \{2, 3\}$, což je spor, protože rovnice $x^2 + 5y^2 = 2$ a $x^2 + 5y^2 = 3$ nemají řešení v $\mathbb{Z}$.

Jsou tedy $2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5})$ součiny ireducibilních prvků lišící se více než pořadím a asociovaností, proto R **není okruh s jednoznačným rozkladem.**

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$. Na druhou stranu 2 a $1 + i\sqrt{5}$ jsou společní dělitelé čísel α, β, a tedy $2 \mid \gamma$ a $1 + i\sqrt{5} \mid \gamma$ v R, a tedy $4 = N(2) \mid N(\gamma)$ a $6 = N(1 + i\sqrt{5}) \mid N(\gamma)$ v $\mathbb{Z}$, tedy $12 \mid N(\gamma)$.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$. Na druhou stranu 2 a $1 + i\sqrt{5}$ jsou společní dělitelé čísel α, β, a tedy $2 \mid \gamma$ a $1 + i\sqrt{5} \mid \gamma$ v R, a tedy $4 = N(2) \mid N(\gamma)$ a $6 = N(1 + i\sqrt{5}) \mid N(\gamma)$ v $\mathbb{Z}$, tedy $12 \mid N(\gamma)$. Dohromady $12 = N(\gamma) = x^2 + 5y^2$.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$. Na druhou stranu 2 a $1 + i\sqrt{5}$ jsou společní dělitelé čísel α, β, a tedy $2 \mid \gamma$ a $1 + i\sqrt{5} \mid \gamma$ v R, a tedy $4 = N(2) \mid N(\gamma)$ a $6 = N(1 + i\sqrt{5}) \mid N(\gamma)$ v $\mathbb{Z}$, tedy $12 \mid N(\gamma)$. Dohromady $12 = N(\gamma) = x^2 + 5y^2$. Taková $x, y \in \mathbb{Z}$ však neexistují.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$. Na druhou stranu 2 a $1 + i\sqrt{5}$ jsou společní dělitelé čísel α, β, a tedy $2 \mid \gamma$ a $1 + i\sqrt{5} \mid \gamma$ v R, a tedy $4 = N(2) \mid N(\gamma)$ a $6 = N(1 + i\sqrt{5}) \mid N(\gamma)$ v $\mathbb{Z}$, tedy $12 \mid N(\gamma)$. Dohromady $12 = N(\gamma) = x^2 + 5y^2$. Taková $x, y \in \mathbb{Z}$ však neexistují. Proto α, β nemají největší společný dělitel v R.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$. Na druhou stranu 2 a $1 + i\sqrt{5}$ jsou společní dělitelé čísel α, β, a tedy $2 \mid \gamma$ a $1 + i\sqrt{5} \mid \gamma$ v R, a tedy $4 = N(2) \mid N(\gamma)$ a $6 = N(1 + i\sqrt{5}) \mid N(\gamma)$ v $\mathbb{Z}$, tedy $12 \mid N(\gamma)$. Dohromady $12 = N(\gamma) = x^2 + 5y^2$. Taková $x, y \in \mathbb{Z}$ však neexistují. Proto α, β nemají největší společný dělitel v R.

Ukažme dále sporem, že čísla $1 + i\sqrt{5}$ a 2 **nemají nejmenší společný násobek v** R.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$. Na druhou stranu 2 a $1 + i\sqrt{5}$ jsou společní dělitelé čísel α, β, a tedy $2 \mid \gamma$ a $1 + i\sqrt{5} \mid \gamma$ v R, a tedy $4 = N(2) \mid N(\gamma)$ a $6 = N(1 + i\sqrt{5}) \mid N(\gamma)$ v $\mathbb{Z}$, tedy $12 \mid N(\gamma)$. Dohromady $12 = N(\gamma) = x^2 + 5y^2$. Taková $x, y \in \mathbb{Z}$ však neexistují. Proto α, β nemají největší společný dělitel v R.

Ukažme dále sporem, že čísla $1 + i\sqrt{5}$ a 2 **nemají nejmenší společný násobek v** R. Předpokládejme nyní, že ω je nejmenší společný násobek čísel $1 + i\sqrt{5}$, 2.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$. Na druhou stranu 2 a $1 + i\sqrt{5}$ jsou společní dělitelé čísel α, β, a tedy $2 \mid \gamma$ a $1 + i\sqrt{5} \mid \gamma$ v R, a tedy $4 = N(2) \mid N(\gamma)$ a $6 = N(1 + i\sqrt{5}) \mid N(\gamma)$ v $\mathbb{Z}$, tedy $12 \mid N(\gamma)$. Dohromady $12 = N(\gamma) = x^2 + 5y^2$. Taková $x, y \in \mathbb{Z}$ však neexistují. Proto α, β nemají největší společný dělitel v R.

Ukažme dále sporem, že čísla $1 + i\sqrt{5}$ a 2 **nemají nejmenší společný násobek v** R. Předpokládejme nyní, že ω je nejmenší společný násobek čísel $1 + i\sqrt{5}$, 2. Protože $4 = N(2) \mid N(\omega)$ a $6 = N(1 + i\sqrt{5}) \mid N(\omega)$, platí $12 \mid N(\omega)$.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$. Na druhou stranu 2 a $1 + i\sqrt{5}$ jsou společní dělitelé čísel α, β, a tedy $2 \mid \gamma$ a $1 + i\sqrt{5} \mid \gamma$ v R, a tedy $4 = N(2) \mid N(\gamma)$ a $6 = N(1 + i\sqrt{5}) \mid N(\gamma)$ v $\mathbb{Z}$, tedy $12 \mid N(\gamma)$. Dohromady $12 = N(\gamma) = x^2 + 5y^2$. Taková $x, y \in \mathbb{Z}$ však neexistují. Proto α, β nemají největší společný dělitel v R.

Ukažme dále sporem, že čísla $1 + i\sqrt{5}$ a 2 **nemají nejmenší společný násobek v** R. Předpokládejme nyní, že ω je nejmenší společný násobek čísel $1 + i\sqrt{5}$, 2. Protože $4 = N(2) \mid N(\omega)$ a $6 = N(1 + i\sqrt{5}) \mid N(\omega)$, platí $12 \mid N(\omega)$. Protože výše uvedený prvek α je společný násobek čísel $1 + i\sqrt{5}$, 2, je $N(\omega) \mid N(\alpha) = 36$.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$. Na druhou stranu 2 a $1 + i\sqrt{5}$ jsou společní dělitelé čísel α, β, a tedy $2 \mid \gamma$ a $1 + i\sqrt{5} \mid \gamma$ v R, a tedy $4 = N(2) \mid N(\gamma)$ a $6 = N(1 + i\sqrt{5}) \mid N(\gamma)$ v $\mathbb{Z}$, tedy $12 \mid N(\gamma)$. Dohromady $12 = N(\gamma) = x^2 + 5y^2$. Taková $x, y \in \mathbb{Z}$ však neexistují. Proto α, β nemají největší společný dělitel v R.

Ukažme dále sporem, že čísla $1 + i\sqrt{5}$ a 2 **nemají nejmenší společný násobek v** R. Předpokládejme nyní, že ω je nejmenší společný násobek čísel $1 + i\sqrt{5}$, 2. Protože $4 = N(2) \mid N(\omega)$ a $6 = N(1 + i\sqrt{5}) \mid N(\omega)$, platí $12 \mid N(\omega)$. Protože výše uvedený prvek α je společný násobek čísel $1 + i\sqrt{5}$, 2, je $N(\omega) \mid N(\alpha) = 36$. Také číslo β je společný násobek čísel $1 + i\sqrt{5}$, 2, a tedy $N(\omega) \mid N(\beta) = 24$.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$. Na druhou stranu 2 a $1 + i\sqrt{5}$ jsou společní dělitelé čísel α, β, a tedy $2 \mid \gamma$ a $1 + i\sqrt{5} \mid \gamma$ v R, a tedy $4 = N(2) \mid N(\gamma)$ a $6 = N(1 + i\sqrt{5}) \mid N(\gamma)$ v $\mathbb{Z}$, tedy $12 \mid N(\gamma)$. Dohromady $12 = N(\gamma) = x^2 + 5y^2$. Taková $x, y \in \mathbb{Z}$ však neexistují. Proto α, β nemají největší společný dělitel v R.

Ukažme dále sporem, že čísla $1 + i\sqrt{5}$ a 2 **nemají nejmenší společný násobek v** R. Předpokládejme nyní, že ω je nejmenší společný násobek čísel $1 + i\sqrt{5}$, 2. Protože $4 = N(2) \mid N(\omega)$ a $6 = N(1 + i\sqrt{5}) \mid N(\omega)$, platí $12 \mid N(\omega)$. Protože výše uvedený prvek α je společný násobek čísel $1 + i\sqrt{5}$, 2, je $N(\omega) \mid N(\alpha) = 36$. Také číslo β je společný násobek čísel $1 + i\sqrt{5}$, 2, a tedy $N(\omega) \mid N(\beta) = 24$. Proto $N(\omega) \mid 12$.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$. Na druhou stranu 2 a $1 + i\sqrt{5}$ jsou společní dělitelé čísel α, β, a tedy $2 \mid \gamma$ a $1 + i\sqrt{5} \mid \gamma$ v R, a tedy $4 = N(2) \mid N(\gamma)$ a $6 = N(1 + i\sqrt{5}) \mid N(\gamma)$ v $\mathbb{Z}$, tedy $12 \mid N(\gamma)$. Dohromady $12 = N(\gamma) = x^2 + 5y^2$. Taková $x, y \in \mathbb{Z}$ však neexistují. Proto α, β nemají největší společný dělitel v R.

Ukažme dále sporem, že čísla $1 + i\sqrt{5}$ a 2 **nemají nejmenší společný násobek v** R. Předpokládejme nyní, že ω je nejmenší společný násobek čísel $1 + i\sqrt{5}$, 2. Protože $4 = N(2) \mid N(\omega)$ a $6 = N(1 + i\sqrt{5}) \mid N(\omega)$, platí $12 \mid N(\omega)$. Protože výše uvedený prvek α je společný násobek čísel $1 + i\sqrt{5}$, 2, je $N(\omega) \mid N(\alpha) = 36$. Také číslo β je společný násobek čísel $1 + i\sqrt{5}$, 2, a tedy $N(\omega) \mid N(\beta) = 24$. Proto $N(\omega) \mid 12$. Dohromady $N(\omega) = 12$, což, jak už víme, je spor.

$R = \mathbb{Z}[i\sqrt{5}]$ neobsahuje n.s.d. nebo n.s.n. některých prvků

Označme $\alpha = (1 + i\sqrt{5})^2 = 2 \cdot (-2 + i\sqrt{5})$, $\beta = 2(1 + i\sqrt{5})$ a ukažme sporem, že α, β **nemají největší společný dělitel v** R. Předpokládejme, že $\gamma = x + yi\sqrt{5}$ je největší společný dělitel čísel α, β. Pak platí $\gamma \mid \alpha$, $\gamma \mid \beta$ v R, a tedy $N(\gamma) \mid N(\alpha) = 36$, $N(\gamma) \mid N(\beta) = 24$ v $\mathbb{Z}$, tedy $N(\gamma) \mid 12$. Na druhou stranu 2 a $1 + i\sqrt{5}$ jsou společní dělitelé čísel α, β, a tedy $2 \mid \gamma$ a $1 + i\sqrt{5} \mid \gamma$ v R, a tedy $4 = N(2) \mid N(\gamma)$ a $6 = N(1 + i\sqrt{5}) \mid N(\gamma)$ v $\mathbb{Z}$, tedy $12 \mid N(\gamma)$. Dohromady $12 = N(\gamma) = x^2 + 5y^2$. Taková $x, y \in \mathbb{Z}$ však neexistují. Proto α, β nemají největší společný dělitel v R.

Ukažme dále sporem, že čísla $1 + i\sqrt{5}$ a 2 **nemají nejmenší společný násobek v** R. Předpokládejme nyní, že ω je nejmenší společný násobek čísel $1 + i\sqrt{5}$, 2. Protože $4 = N(2) \mid N(\omega)$ a $6 = N(1 + i\sqrt{5}) \mid N(\omega)$, platí $12 \mid N(\omega)$. Protože výše uvedený prvek α je společný násobek čísel $1 + i\sqrt{5}$, 2, je $N(\omega) \mid N(\alpha) = 36$. Také číslo β je společný násobek čísel $1 + i\sqrt{5}$, 2, a tedy $N(\omega) \mid N(\beta) = 24$. Proto $N(\omega) \mid 12$. Dohromady $N(\omega) = 12$, což, jak už víme, je spor. Čísla $1 + i\sqrt{5}$ a 2 tedy nemají nejmenší společný násobek v R.