Obory integrity a dělitelnost

ZPRACUJE: Mystik

Okruhy hlavních ideálů nespadají do okruhu?

Pozn.: Pro označování uvažujeme obor integrity $(I, +, 0, -, *, 1)$

Obsah

Dělitelnost

Dělitelnost

Prvek a je dělitelný dělitelem b (značíme b|a) právě tehdy pokud platí: $\exists c \in I : a = bc$

- tj. a lze vyrobit z b vynásobením nějakým prvkem

Elementární pravidla dělitelnosti

$\forall a, b, c, d \in I$

- $a \mid 0$ (nula jde dělit čímkoli)
- $1 \mid a$ (cokoli je dělitelné 1)
- $a \mid a$ (cokoli je dělitelné samo sebou)
- $a|b \wedge b|c \Rightarrow a|c$ (dělitel mého dělitele je i můj dělitel)
- $a|b \Rightarrow a|bc$ (můj dělitel je i dělitel mého násobku)
- $a|b \wedge a|c \Rightarrow a|b + c$ (součet je dělitelný společným dělitelem sčítanců)
- $c \neq 0, a|b \Rightarrow ac|bc$ (vynásobením dělence i dělitele stejným nenulovým číslem se dělitelnost nemění)
- $a|b \wedge c|d \Rightarrow ac|bd$ (vynásobením dělenců mezi sebou a dělitelů mezi sebou se dělitelnost nemění)
- $n \in \mathbb{N}, a|b \Rightarrow a^n|b^n$ (umocnění dělence i dělitele stejným číslem dělitelnost nemění)

Jednotka oboru integrity

dělitel prvku 1

- Množinu všech jednotek oboru integrity I značíme E(I)
- Algebra (E(I), *) je abelovská grupa - tzv. grupa jednotek oboru integrity I

Asociované prvky (značíme a~b)

$\exists e \in E(I) : a = be$ (tj. asociované prvky se liší jen vynásobením některou jendotkou)

- platí $a \sim b \Leftrightarrow a|b \wedge b|a$ (asociované prvky jsou navzájem svými děliteli)
- relace ~ je kongruence na (I, *)

Triviální dělitelé

Triviální dělitelé prvku a jsou všechny jendotky a všechny prvky asociované s prvkem a

Vlastní dělitelé

Všichni netriviální dělitelé

Ireducibilní prvek

prvek, který má pouze triviální dělitele (odpovídá prvočíslům pokud $I = \mathbb{Z}$)

- pokud je a ireducibilní jsou ireducibilní i všechny prvky asociované s a

Prvočinitel

není jednotka ($p \notin E(I)$) ani nulový prvek ($p \neq 0$) a

pokud je součin dělitelný p pak je alespoň jeden činitel dělitelný p ($p|ab \Rightarrow p|a \vee p|b$)

- každý prvočinitel je ireducibilní (ale ne nutně každý ireducibilní prvek je prvočinitel)
- pokud je a prvočinitel jsou prvočiniteli i všechny prvky asociované s a

- pro $I = \mathbb{Z}$ platí p je prvočinitel $\Leftrightarrow$ p je ireducibilní

Gaussovy okruhy

Příklady Gausssových okruhů: celá čísla, reálná čísla, racionální čísla, komplexní čísla, všechna tělesa, ...

Základní vlastností Gaussových okruhů je jednoznačnost rozkladu na prvočinitele

Jednoznačnost rozkladu na prvočinitele

ke každému prvku a ($a \notin E(I), a \neq 0$) existují prvočinitelé jichž je součinem

tj. každý prvek, který není nulový nebo jendotkou lze jendoznačně rozložit na součin prvočinitelů

V Gausově okruhu platí:

- každý ireducibilní prvek je prvočinitel
- každý neprvočinitel je tvořen součinem určitých počtů (mocnin) různých (neasociovaných) prvočinitelů a jednotky
- a|b $\Leftrightarrow$ a se skládá ze stejného nebo menšího počtu výskytů jednotlivých prvočinitelů

Největší společný dělitel (NSD)

prvek, který vznikne tak, že od každého prvočinitele vezmeme jeho nejmenší počet výskytů v prvcích jejichž NSD hledáme

Nejmenší společný násobek(NSN)

prvek, který vznikne tak, že od každého prvočinitele vezmeme jeho největší počet výskytů v prvcích jejichž NSN hledáme

Svaz dělitelů

je svaz nad množinou I/~ (faktorová množina asociovaných prvků) kde je relace uspořádání definována jako $[a]_\sim \leq [b]_\sim \Leftrightarrow a|b$

Okruhy hlavních ideálů nespadají do okruhu?

Eukleidovy okruhy

- Každý Eukleidův okruh je Gausův okruh

Okruhy na kterých je definováno dělení se zbytkem

Dělení se zbytkem

- $\forall a \in I \setminus \{0\}$ (dělitel)
- $\forall b \in I$ (dělenec)
- $\exists q \in I$ (výsledek)
- $\exists r \in I$ (zbytek)
- $b = aq + r$
- $r = 0 \vee r < a$ (zbytek je nula nebo je menší než dělitel)

Eukleidův algoritmus pro NSD

```
function nsd(a, b)
    if b = 0
       return a
    else
       return nsd(b, a mod b)
```

více viz [[1] (http://cs.wikipedia.org/wiki/Eukleid%C5%AFv_algoritmus)]

Kategorie: Státnice 2011 | Matematické struktury v informatice

Stránka byla naposledy editována 28. 5. 2011 v 15:34.