## Obory a dělitelnost

*Definice.*

- okruh;
- grupa;
- obor integrity (nebo zkráceně jen „obor“): komutativní okruh s krácením;
- $a \mid b$ ($a$ dělí $b$);
- NSD (největší společný dělitel); „největší“ je míněno vzhledem k uspořádání dělitelnosti!!
- $R^*$ (invertibilní prvky);
- ireducibilní prvek (neinvertibilní, nemá netriviální rozklad);
- prvočinitel ($p \mid a \cdot b \implies p \mid a \vee p \mid b$)
- $a \mid\mid b$ (asociované prvky);
- ideál okruhu;
- hlavní ideál okruhu.

*Pozorování.*

- invertibilní prvky tvoří spolu s násobením grupu;
- $a$ je invertibilní, právě když $a \mid\mid 1$;
- v okruhu lze krátit, právě když nemá dělitele nuly (tj. $a \cdot b \implies a = 0 \vee b = 0$);
- $a \mid b \implies bR \subseteq aR$;
- $\mathbb{Z}_6$ není obor integrity ($3 \cdot 2 = 0$);
- prvočinitel je ireducibilní.

*Definice.*

- noetherovský okruh: každá ostře rostoucí posloupnost ideálů je konečná.
- Gaussův obor (ang: Unique Factorization Domain - UFD): každý prvek má jednoznačný rozklad na ireducibilní prvky (jednoznačnost až na pořadí a asociovanost).
- Obor hlavních ideálů (OHI, ang: Principle Ideal Domain - PID): každý ideál je hlavní.

*Příklad.* V okruhu $\mathbb{Z}_6$ platí $4 \cdot 4 = 4$. Z toho plyne, že neexistuje jednoznačný rozklad na prvočinitele: $4 = 2 \cdot 2 = 2 \cdot 2 \cdot 2 \cdot 2 = \dots$. Potíž je v tom, že $\mathbb{Z}_6$ není obor, a v rovnosti $4 \cdot 4 = 4$ nelze krátit čtyřku. Kvůli problémům tohoto typu o gaussovskosti mluvíme jen v oborech.

*Pozorování.* Pokud má nějaký prvek v oboru více rozkladů na ireducibilní prvky, pak neexistují NSD. Nechť jsou např.

$$r = a_1 \cdot a_2 = b_1 \cdot b_2$$

dva různé rozklady $r$ na ireducibilní prvky. Pak mají prvky $r$ a $a_1 \cdot b_1$ společné dělitele $a_1$ a $b_1$. Prvek $r$ přitom není dělitelný $a_1 \cdot b_1$, jinak by $r = a_1 \cdot a_2 = a_1 \cdot b_1 \cdot s$ dávalo díky krácení spor s růzností rozkladů. Tedy prvky $r$ a $a_1 \cdot b_1$ nemají žádného společného dělitele.

*Pozorování.* Pokud v oboru $R$ platí, že ireducibilní prvky jsou prvočinitelé, pak je každý rozklad na ireducibilní prvky jednoznačný. To však ještě neznamená, že se jedná o Gaussův obor, protože některé prvky nemusejí mít *žádný* rozklad na ireducibilní prvky. V takovém případě ovšem existuje nekonečná ostře rostoucí posloupnost hlavních ideálů.

*Příklad.* $R = x \cdot \mathbb{Q}[x] + \mathbb{Z}$ není noetherovský. Obsahuje dokonce nekonečnou rostoucí posloupnost *hlavních* ideálů:

$$xR \subsetneq \frac{x}{2}R \subsetneq \frac{x}{4}R \subsetneq \frac{x}{8}R \subsetneq \dots$$

Polynom $x$ nemá rozklad na ireducibilní prvky.

$$x = 2 \cdot \frac{x}{2} = 2 \cdot 2 \cdot \frac{x}{4} = 2 \cdot 2 \cdot 2 \cdot \frac{x}{8} = \dots$$

*Příklad.* $R = \mathbb{Z}[\sqrt{5}]$ je noetherovský, ale není Gaussův, např. proto že platí $2 \cdot 2 = (\sqrt{5}+1) \cdot (\sqrt{5}-1)$, přičemž prvky 2, $\sqrt{5}+1$ i $\sqrt{5}-1$ jsou ireducibilní (viz např. Základy algebry D. Stanovského, I,7). V každém případě je zřejmé, že 2 nedělí ani $\sqrt{5}+1$ ani $\sqrt{5}-1$, a není tedy prvočinitelem.

*Pozorování.* V Gaussově oboru je každý ireducibilní prvek prvočinitelem (oba pojmy tedy splývají).

*Pozorování.* Sjednocení řetězce ideálů je opět ideál.

*Tvrzení.* Každý obor hlavních ideálů je noetherovský.

*Pozorování.* Pokud $I$ a $J$ jsou ideály, pak množina $I + J := \{x + y \mid x \in I, y \in J\}$ je také ideál.

*Pozorování.* $d$ je NSD všech prvků $dR$.

*Tvrzení.* Každý obor hlavních ideálů je Gaussův.

*Důkaz.* Protože OHI je noetherovský, má každý prvek rozklad na ireducibilní činitele. Zbývá ukázat, že každý ireducibilní prvek je prvočinitel (z definice prvočinitele pak okamžitě plyne jednoznačnost rozkladu).

Nechť $p$ je ireducibilní prvek a $p \,|\, a \cdot b$. Chceme ukázat $p \,|\, a \vee p \,|\, b$. Uvažujme ideál $aR + pR = dR$. Z $d \,|\, p$ plyne buď $d \in R^*$ nebo $p \,|\, d$. Ve druhém případě máme $p \,|\, d \,|\, a$ a jsme hotovi. Podobně pro $bR + pR = cR$. Zbývá možnost, že $d$ i $c$ jsou invertibilní. Pak ovšem $cR = dR = R$ a existují prvky $r_1$, $s_1$, $r_2$ a $s_2$ takové, že

$$1 = (ar_1 + ps_1) = (br_2 + ps_2).$$

Dostáváme

$$1 = (ar_1 + ps_1) \cdot (br_2 + ps_2),$$

z čehož vidíme $p \,|\, 1$, což je spor s ireducibilitou $p$. □

Trik násobení jedniček zjednodušuje důkaz v porovnání s důkazem Věty 7.5. ve skriptech D. Stanovského (ten je rozložen na několik tvrzení, která jsou sama o sobě užitečná). Lze ho využít k obecnějšímu tvrzení 1.12 ve skriptech A. Drápala.

*Definice.* Eukleidův obor: lze dělit se zbytkem. (Zbytek je menší ve smyslu nějakého zobrazení $f : R \to \mathbb{N}_0$, kterému říkáme *eukleidovské*).

*Pozorování.* Je-li $f$ eukleidovské, pak $g$ definované jako $g(a) := \min\{f(ax) \mid x \in R^*\} = \min\{f(y) \mid y \,||\, a\}$ je také eukleidovské.

*Důkaz.* Zvolme $a$, $b$. Nechť $x$ je invertibilní prvek takový, že $f(bx) = g(b)$, a nechť $a = (bx)q + z$, kde $f(z) < f(bx)$. Pak $g(z) \leq f(z) < f(bx) = g(b)$, a proto $a = b(xq) + z$ je požadované dělení se zbytkem vzhledem k funkci $g$. □

Od teď tedy budeme předpokládat, že eukleidovská funkce splňuje

$$g(a) := \min\{f(ax) \mid x \in R^*\}.$$

*Pozorování.* Eukleidovská funkce $g$ splňuje $g(b) \leq g(a)$, kdykoli $b \,|\, a$, $a \neq 0$. To znamená, že $g$ nabývá nejmenší nenulové hodnoty v ideálu $bR$ na prvku $b$.

*Důkaz.* Nechť $c$ je nenulový násobek $b$ s nejmenší možnou hodnotou $g(c)$ (tedy $g(c) = \min\{g(x) \mid x \in bR, x \neq 0\}$). Existuje $z$ takové, že $b = qc + z$ a $g(z) < g(c)$. Protože $z = b - qc$ je násobek $b$, plyne z minimality $g(c)$, že $z = 0$. Tedy $c \,||\, b$ a $g(c) = g(b)$ podle definice $g$. Pokud je tedy $a$ nenulový násobek $b$, máme $g(b) = g(c) \leq g(a)$. □

*Pozorování.* Eukleidovská funkce nabývá svou nejmenší nenulovou hodnotu na všech prvcích $R^*$.

Můžeme tedy také požadovat, aby $g(1) = 1$ a $g(a) > 1$ pro neinvertibilní prvek $a$.

*Tvrzení.* Každý Eukleidovský obor je oborem hlavních ideálů.

Nejrychlejší důkaz je ve skriptech A. Drápala a je podobný důkazu předchozího pozorování.

S pomocí Eukleidova algoritmu lze důkaz přeformulovat i takto: libovolné dva prvky ideálu $I$ mají největšího společného dělitele, který je výsledkem Eukleidova algoritmu a leží tedy také v $I$. Takto postupně dostaneme NSD stále větší množiny prvků z ideálu. Protože hodnota eukleidovské funkce nemůže klesat do nekonečna, dostaneme nakonec největší společný dělitel $d$ celého ideálu a tedy $I = dR$.

**Shrnutí: Hierarchie oborů integrity.**

obory integrity
$\cup\!\!\!\!\neq$ ①
obory s NSD — rozklady na ireducibilní prvky jsou jednoznačné, pokud existují
$\cup\!\!\!\!\neq$ ②
Gaussovy obory (UFD) — NSD je "průnik rozkladů" na ireducibilní prvky
$\cup\!\!\!\!\neq$ ③
obory hlavních ideálů — NSD je lineární kombinací
$\cup\!\!\!\!\neq$ ④
Eukleidovský obor — NSD lze nalézt Eukleidovým algoritmem
$\cup\!\!\!\!\neq$ ⑤
tělesa

Příklady ukazující, že inkluze jsou ostré:

① $\mathbb{Z}[\sqrt{5}]$
Jak prvek 2, tak prvek $\sqrt{5}+1$ jsou společným dělitelem prvků 4 a $2 \cdot (\sqrt{5}+1)$ a jsou přitom neporovnatelné.

② $x \cdot \mathbb{Q}[x] + \mathbb{Z}$
Jak jsme viděli, polynom $x$ nemá v tomto oboru rozklad na ireducibilní prvky. Skutečnost, že existují NSD plyne z vlastností $\mathbb{Q}[x]$ a $\mathbb{Z}[x]$ (zatím bez důkazu).

③ $\mathbb{Q}[x, y]$ Ideál polynomů stupně alespoň jedna, tedy $xR + yR$, zjevně není hlavní.

④ Bez důkazu.

$$\mathbb{Z}[\frac{1+\sqrt{-19}}{2}]$$

⑤ $\mathbb{Z}$.