Ideály

Uvažujme pro jednoduchost komutativní okruh R s jednotkovým prvkem.

Definice. Ideálem okruhu R budeme rozumět každou podmnožinu I okruhu R, která je uzavřena vzhledem ke sčítání a která „vydrží“ násobení libovolným prvkem okruhu R, tj. jsou splněny následující dva požadavky:

(i) $\forall\, a, b \in I \quad a + b \in I$,
(ii) $\forall\, a \in I \quad \forall\, r \in R \quad ra \in I$.

Příklad. V oboru integrity $\mathbb{Z}$ celých čísel je ideálem množina všech násobků libovolného, konkrétně zvoleného čísla $a \in \mathbb{Z}$. Jedním ideálem je tedy jednoprvková množina obsahující nulu (násobky nuly), druhým ideálem je celé $\mathbb{Z}$ (násobky jedničky, resp. minus jedničky), dalšími ideály jsou množiny všech sudých čísel (násobky čísla 2, resp. -2), všech čísel dělitelných třemi, resp. dělitelných čtyřmi, resp. dělitelných pěti atd. Je evidentní, že součet dvou prvků kterékoli z výše uvedených množin je opět jejím prvkem a rovněž násobek prvku té které množiny libovolným celým číslem je opět jejím prvkem (násobek sudého čísla je sudým číslem, násobek čísla dělitelného třemi je opět dělitelný třemi atd.). Jiné ideály obor integrity $\mathbb{Z}$ nemá, jak uvidíme dále.

Příklad. V oboru integrity $T[x]$ všech polynomů nad tělesem T jsou ideály všechny množiny, které jsou tvořeny násobky libovolně zvoleného polynomu $f(x)$. Ideálem je např. množina všech násobků polynomu x^2, resp. množina všech násobků polynomu $3x^2 + 5x - 5$ apod. Snadno se opět ukáže, že jsou splněny požadavky (i) a (ii). Jiné ideály obor integrity $T[x]$ nemá, jak uvidíme dále.

Příklad. Jedinými ideály tělesa T je jednoprvková množina $\{0\}$ a celá množina T. Pokud by totiž byla množina I ideálem v tělese T a v I existoval nějaký nenulový prvek a, musel by v I být podle požadavku (ii) i prvek $a^{-1} \cdot a = 1$, a následně i prvek $b \cdot 1 = b$ pro každé $b \in T$. Tedy by bylo $I = T$.

Věta. Průnikem libovolného souboru ideálů okruhu R je opět ideál.

Důkaz. Provede se úplně stejně jako důkaz faktu, že průnikem libovolného souboru podprostorů vektorového prostoru je podprostor.

Definice. Ideálem generovaným podmnožinou M okruhu R budeme rozumět průnik všech ideálů, které množinu M obsahují. Ideál generovaný jedním prvkem se nazývá hlavní.

Připomeňme, že definici ideálu generovaného podmnožinou umožňuje předchozí věta. Následující věta je obdobou věty o lineárním obalu podmnožiny vektorového prostoru. Dokáže se obdobným postupem.

Věta. Ideál generovaný podmnožinou M okruhu R je roven množině

$$\{\Sigma r_i a_i \,;\, a_i \in M,\, r_i \in R\}.$$

Ideál generovaný prvkem $a \in R$ (tj. hlavní ideál) je tedy roven množině $\{ra \,;\, r \in R\}$.

Definice. Obor integrity se nazývá oborem integrity hlavních ideálů, jestliže je každý jeho ideál hlavní.

Každý ideál oboru integrity hlavních ideálů je tedy generován jedním prvkem.

Výše uvedené tři příklady $\mathbb{Z}$, $T[x]$, T jsou příklady oborů integrity hlavních ideálů.

V tělese jsou jen dva ideály – jsou generovány nulovým prvkem, resp. jednotkovým prvkem.

To, že je obor integrity celých čísel oborem integrity hlavních ideálů (viz následující věta), je důsledkem tzv. věty o dělení se zbytkem. Ze stejného důvodu je i obor integrity $T[x]$ polynomů jedné neurčité oborem integrity hlavních ideálů (umíme dělit polynom polynomem, tj. stanovit podíl a zbytek).

Věta. Obor integrity $\mathbb{Z}$ celých čísel je oborem integrity hlavních ideálů.

Důkaz. Nechť I je ideál oboru integrity $\mathbb{Z}$. Jestliže I obsahuje pouze nulu, je generován nulou, a je tedy hlavní. Jestliže I obsahuje nějaký nenulový prvek, obsahuje i kladný prvek (záporný prvek z I stačí vynásobit číslem -1 a dostaneme kladný prvek z I). Nechť je a **nejmenší** kladný prvek obsažený v I. Předpokládejme, že $b \in I$ je libovolně zvolený prvek. Vydělíme jej prvkem a:

$$b = a \cdot q + r, \quad \text{kde} \quad 0 \leq r < a.$$

Potom je $r = b - a \cdot q \in I$, neboť $b, a \cdot q \in I$. Případ $0 < r$ vede ke sporu, neboť a je nejmenší kladné číslo ideálu I. Je tedy $r = 0$ a každý prvek $b \in I$ je násobkem prvku a.

Úplně stejně se dokáže, že $T[x]$ je oborem integrity hlavních ideálů. Místo a se zvolí polynom z I, který má nejmenší stupeň ze všech polynomů v I. Tedy platí následující věta.

Věta. Obor integrity $T[x]$ polynomů jedné neurčité je oborem integrity hlavních ideálů.

Obtížněji se ukáže, že obor integrity Gaussových celých čísel $\mathbb{Z}$[i] je rovněž oborem integrity hlavních ideálů.

V partii o podobnosti matic je třeba si uvědomit, že všechny anulující polynomy dané matice A tvoří ideál v $T[\lambda]$ (součet anulujících polynomů i násobek anulujícího polynomu jsou opět anulující polynomy matice A), zvolit anulující polynom nejmenšího možného stupně (s koeficientem 1 u nejvyšší mocniny λ), tj. tzv. minimální polynom matice A, a ukázat pomocí věty o dělení polynomů se zbytkem, že každý anulující polynom matice A je násobkem jejího minimálního polynomu.

Poznámka. Pro nekomutativní okruhy, resp. okruhy bez jednotkového prvku je situace složitější. V prvním případě se uvažují levé, pravé a oboustranné ideály, ve druhém případě je ideál generovaný množinou vyjádřen komplikovaněji.