Moduly nad komutativními okruhy[1]

Nahradíme-li v definici vektorového prostoru těleso za obecný okruh, dostaneme struktury zvané moduly. Aplikace teorie modulů sahají od celočíselné lineární algebry (moduly nad okruhem $\mathbb{Z}$) až po lineární reprezentace grup.

Definice. *Modulem* nad komutativním okruhem $\mathbf{R} = (R, +^{\mathbf{R}}, -^{\mathbf{R}}, \cdot^{\mathbf{R}}, 0)$, nebo krátce $\mathbf{R}$-*modulem*, rozumíme algebraickou strukturu $\mathbf{M} = (M, +, -, 0, (r\cdot) : r \in R)$ splňující následující podmínky:

(1) $(M, +, -, 0)$ je abelovská grupa;
(2) pro každé $r, s \in R$ a $m, m_1, m_2 \in M$ platí

$$r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2, \quad (r +^{\mathbf{R}} s) \cdot m = r \cdot m + s \cdot m, \quad (r \cdot^{\mathbf{R}} s) \cdot m = r \cdot (s \cdot m).$$

(Abychom odlišili sčítání a násobení v okruhu od sčítání a skalárního násobení v modulu, doplňujeme okruhové operace indexy.)

Příklad. Každou abelovskou grupu lze považovat za $\mathbb{Z}$-modul, skalární násobení je definováno $n \cdot a = a + \ldots + a$, resp. $-a - a - \ldots - a$.

Life hack pro přednášku z komutativní algebry: Většinu základních tvrzení o modulech stačí pochopit pro abelovské grupy, pro ostatní okruhy (přinejmenším pro obory hlavních ideálů) to bude nejspíš fungovat podobně.

Příklad. Vektorové prostory nad tělesem $\mathbf{T}$ lze považovat za moduly na různými okruhy. Každý z těchto pohledů má své výhody.

- Vektorový prostor nad $\mathbf{T}$ je přesně totéž jako $\mathbf{T}$-modul.
- Uvažujme vektorový prostor $\mathbf{T}^n$ a $n \times n$ matici A. Prostor $\mathbf{T}^n$ lze považovat také za $\mathbf{T}[x]$-modul, přičmž skalární násobení polynomem f se interpretuje jako násobení vektoru maticí $f(A)$.
- Vektorový prostor $\mathbf{T}^n$ lze považovat také za $\mathbf{M}_n(\mathbf{T})$-modul, kde $\mathbf{M}_n(\mathbf{T})$ je okruh matic, skalární součin matice krát vektor se definuje jako maticové násobení. Tento okruh ale není komutativní, tímto příkladem se nebudeme zabývat.

Pozor: Základní aritmetika v modulech je stejná jako ve vektorových prostorech (lineární kombinace, podmoduly vs. podprostory), ale naprostá většina netriviálních výsledků lineární algebry v obecných modulech neprojde, problém nastává už kolem pojmu báze podprostoru.

Příklad. Libovolný komutativní okruh $\mathbf{R}$ lze považovat za modul nad $\mathbf{R}$ vzhledem ke skalárnímu násobení $r \cdot m = r \cdot_{\mathbf{R}} m$ pro všechna $r, m \in R$.

Definice. Podstruktury modulu se nazývají *podmoduly*. Tedy podmnožina $K \subseteq M$ tvoří podmodul modulu $\mathbf{M}$, pokud $0 \in K$ a $-a \in K$, $a + b \in K$ a $r \cdot a \in K$ pro každé $a, b \in K$ a $r \in R$. Značíme $\mathbf{K} \leq \mathbf{M}$.

Příklad. Podmoduly abelovských grup (jakožto $\mathbb{Z}$-modulů) jsou totéž co podgrupy. Podmoduly vektorových prostorů nad tělesem (jakožto $\mathbf{T}$-modulů) jsou totéž co podprostory.

[1] David Stanovský, 20. října 2020

Příklad. Podmoduly $\mathbf{T}[x]$-modulů jsou totéž co podprostory invariantní vůči akci dané skalárním násobením prvkem x. Konkrétně, je-li násobení dané maticí A, jde o podprostory W takové, že $Aw \in W$ pro každé $w \in W$.

Příklad. Podmoduly okruhu $\mathbf{R}$ považovaného za $\mathbf{R}$-modul jsou totéž co ideály.

Přímočaře se adaptuje také pojem homomorfismu a faktormodulu.

Definice. Zobrazení $\varphi : M \to N$ je *homomorfismem* modulů $\mathbf{M} \to \mathbf{N}$, pokud pro každé $a, b \in M$ a $r \in R$ platí

$$\varphi(a+b) = \varphi(a) + \varphi(b) \quad \text{a} \quad \varphi(r \cdot a) = r \cdot \varphi(a).$$

Jádro homomorfismu se definujeme jako $\mathrm{Ker}(\varphi) = \{a \in M : \ \varphi(a) = 0\}$ a opět je snadné dokázat, že tvoří podmodul $\mathbf{M}$ a že homomorfismus je prostý právě tehdy, když je jeho jádro triviální (analogie tvrzení z lineární algebry).

Faktormoduly se konstruují pomocí podmodulů, tj. čím je v grupách normální podgrupa a v okruzích ideál, tím je v modulech podmodul.

Definice. Je-li $\mathbf{K}$ podmodulem $\mathbf{R}$-modulu $\mathbf{M}$, definujeme faktormodul $\mathbf{M}/\mathbf{K}$ pomocí relace

$$a \sim b \quad \Leftrightarrow \quad a - b \in K.$$

Tj. prvky jsou bloky této ekvivalence, $[a] + [b] = [a+b]$, $r \cdot [a] = [r \cdot a]$ atd. Sami si dokažte, že jde o kongruenci, tj. že jsou modulové operace na třídách ekvivalence dobře definovány, a že výsledná struktura je $\mathbf{R}$-modul (je to stejný princip jako v případě grup či okruhů).

Analogickým způsobem se dokáže také věta o homomorfismu a věty o izomorfismu. Konkrétně:

Věta 0.1 (věta o homomorfismu)**.** *Buď $\varphi : \mathbf{M} \to \mathbf{N}$ homomorfismus $\mathbf{R}$-modulů.*

(1) *Je-li $\mathbf{K} \leq \mathbf{Ker}(\varphi)$ podmodul $\mathbf{M}$, pak je zobrazení*

$$\psi : \mathbf{M}/\mathbf{K} \to \mathbf{N}, \qquad [a] \mapsto \varphi(a)$$

dobře definované a je to grupový homomorfismus.

(2) (1. věta o izomorfismu) $\mathbf{M}/\mathbf{Ker}(\varphi) \simeq \mathbf{Im}(\varphi)$.

Tvrzení 0.2 (2. věta o izomorfismu)**.** *Buď $\mathbf{M}$ modul a $\mathbf{N}$ jeho podmodul.*

(1) *Je-li $\mathbf{K} \leq \mathbf{N} \leq \mathbf{M}$, pak je $\mathbf{N}/\mathbf{K}$ podmodulem modulu $\mathbf{M}/\mathbf{K}$.*

(2) *Je-li $\mathbf{L}$ podmodul modulu $\mathbf{M}/\mathbf{N}$, pak existuje podmodul $\mathbf{K} \leq \mathbf{M}$ takový, že $\mathbf{L} = \mathbf{K}/\mathbf{N}$.*

(3) *Pro $\mathbf{K} \leq \mathbf{N} \leq \mathbf{M}$ platí*

$$(\mathbf{M}/\mathbf{K})/(\mathbf{N}/\mathbf{K}) \simeq \mathbf{M}/\mathbf{N}.$$

Poznámka pro zvídavé. Jedním ze základních a velmi užitečných výsledků teorie modulů je klasifikace konečně generovaných modulů nad obory hlavních ideálů (možná znáte klasifikaci konečných abelovských grup, to je speciální případ). Kdysi se to na komutativních okruzích učilo, ale nedalo se to pořádně stíhat, tak už se to neučí.

Ideál I se nazývá *primární*, pokud $ab \in I$ implikuje $a^k \in I$ nebo $b^k \in I$ pro nějaké $k \in \mathbb{N}$.

Věta 0.3 (klasifikace konečně generovaných modulů nad obory hlavních ideálů)**.** *Buď* $\mathbf{R}$ *obor hlavních ideálů a* $\mathbf{M}$ *konečně generovaný* $\mathbf{R}$*-modul. Pak existují* $m, n \geq 0$ *a vlastní primární ideály* $u_1R, \ldots, u_mR$ *takové, že*

$$\mathbf{M} \simeq \mathbf{R}^n \times \mathbf{R}/u_1R \times \cdots \times \mathbf{R}/u_mR.$$

Čísla m, n *jsou určena jednoznačně a ideály* $u_1R, \ldots, u_mR$ *jednoznačně až na pořadí.*

Příklad. Podíváme se, co říká Věta 0.3 pro různé obory $\mathbf{R}$.

- $\mathbf{R} = \mathbf{T}$ těleso: pro vektorové prostory dostaneme známý fakt, že každý konečně generovaný vektorový prostor nad tělesem $\mathbf{T}$ je izomorfní $\mathbf{T}^n$ pro nějaké n (tělesa žádné vlastní ideály nemají, tedy $m = 0$).
- $\mathbf{R} = \mathbb{Z}$: pro abelovské grupy dostaneme rozklad $\mathbb{Z} \times \mathbb{Z}_{p_1^{k_1}} \times \mathbb{Z}_{p_n^{k_n}}$„ neboť primární ideály jsou právě ideály $p^k\mathbb{Z}$, kde p je prvočíslo.
- $\mathbf{R} = \mathbf{T}[x]$: pro vektorové prostory s akcí danou maticí A dostaneme, s trochou práce, větu o *Jordanově normální formě* pro matici A.