Učební texty k přednášce ALGEBRAICKÉ STRUKTURY
Michal Marvan, Matematický ústav
Slezská univerzita v Opavě

15. Moduly

Definice. Buď R okruh, buď M množina na níž jsou zadány binární operace "+": $M\times M\to M$, $(a,b)\mapsto a+b$, nulární operace "0" $\in M$, unární operace "$-$": $M\to M$, $a\mapsto -a$, a po jedné unární operaci "r": $M\to M$, $a\mapsto r\cdot a$, tak, že $(M,+,0,-)$ je abelovská grupa a pro všechny prvky $a,b\in M$, $r,s,\in R$ platí

1° $r(a+b)=ra+rb$,
2° $r(sa)=(r\cdot s)a$,
3° $1a=a$,
4° $(r+s)a=ra+sa$.

Pak se M nazývá *modul nad okruhem* R nebo krátce R*-modul* a značí se $(M,+,0,-,R)$. Grupa $(M,+,0,-)$ se nazývá *aditivní grupa* modulu M.

Je-li R pole, pak místo modul říkáme *vektorový prostor*.

Příklady. (1) Všechny vektorové prostory.

(2) Každá abelovská grupa $(A,+,0,-)$ je modulem nad okruhem $\mathbf{Z}$, zavedeme-li unární operace $a\mapsto na$, $n\in\mathbf{Z}$, předpisem

$$na:=\begin{cases}\underbrace{a+\cdots+a}_{n} & \text{pro } n>0,\\ 0 & \text{pro } n=0,\\ \underbrace{-a-\cdots-a}_{-n} & \text{pro } n<0.\end{cases}$$

(3) Každý okruh R je R-modul, zavedeme-li unární operace předpisem $ra=r\cdot a$. Podmínky 1°–4° vyplývají z axiomů okruhu.

(4) Buď V vektorový prostor nad polem P, buď $X:V\to V$ lineární zobrazení. Pro polynom $p\in P[x]$, $p=a_mx^m+\cdots+a_1x+a_0$, položíme $pX=p(X)=a_mX^m+\cdots+a_1X+a_0\,\mathrm{id}$, kde $X^k=X\circ\cdots\circ X$ (k-krát). Zřejmě je pX opět lineární zobrazení $V\to V$ pro každé $p\in P[x]$, a platí $(p+q)(X)=p(X)+q(X)$, $1(X)=\mathrm{id}$. Vzniká tak struktura $P[x]$-modulu na V.

Tvrzení. *Buď $(A,+,0,-)$ abelovská grupa. Pak existuje právě jeden způsob, jak na A zadat strukturu $\mathbf{Z}$-modulu tak, aby $(A,+,0,-)$ byla jeho aditivní grupa.*

Důkaz. Existence: Viz Příklad (2).

Jednoznačnost: Podle 3° musí být $1a=a$ pro každé $a\in A$, načež $2a=a+a$ podle 4°, a podobně $na=a+\cdots a$ (n-krát). Dále nutně $0a=0$, což ověříme odečtením $0a$ od obou stran rovosti $0a+0a=(0+0)a=0a$. Nakonec $(-1)a+a=(-1)a+1a=(-1+1)a=0a=0$, a proto $(-1)a=-a$, načež $(-n)a=(-1\cdot n)a=(-1)(na)=-(na)$ pro libovolné $n>0$.

Tvrzení. *Buď $(V,+,0,-,P)$ vektorový prostor, buď $X:V\to V$ lineární zobrazení. Pak existuje právě jeden způsob, jak strukturu P-modulu na V rozšířit na strukturu $P[x]$-modulu tak, aby platilo $xv=X(v)$ pro každé $v\in V$.*

Důkaz. Existence: Viz Příklad (4).

Jednoznačnost: Pro prvky $p\in P$ je $pv=p\cdot v$ předepsáno (strukturou P-modulu na V). Pro $x\in P[x]$ je předepsáno $xv=X(v)$. Načež $x^2(v)=(x\cdot x)(v)=(x(x(v))=X(X(v))=$

$(X \circ X)(v) = X^2(v)$ a podobně $x^n(v) = X^n(v)$. Nakonec, $(a_m x^m + \cdots + a_1 x + a_0)(v) = (a_m X^m + \cdots + a_1 X + a_0 \,\mathrm{id})(v)$ podle 1°.

R-modul je algebra se signaturou $(+, 0, -, (r)_{r\in R})$, přičemž operace $+, 0, -$ mají po řadě aritu $2, 0, 1$ a operace r jsou unární.

Tvrzení. (1) *Každá podalgebra R-modulu je R-modul.*
(2) *Každá faktorová algebra R-modulu je R-modul.*
(3) *Součin R-modulů je R-modul.*

Důkaz. Ověření je podobné jako u grup a okruhů a je přenecháno čtenáři jako jednoduché cvičení.

Definice. Podalgebra R-modulu se nazývá *R-podmodul*. Faktorová algebra R-modulu se nazývá *faktorový R-modul*.

Také u R-modulů existuje jednojednoznačný vztah mezi kongruencemi a třídami obsahujícími 0. Situace je velmi prostá, protože jako třída obsahující 0 se může vyskytovat libovolný podmodul.

Tvrzení. *Buď $(M, +, 0, -, R)$ R-modul.*
(1) *Je-li κ kongruence na M, pak je $[0]_\kappa$ R-podmodul v M.*
(2) *Je-li N podmodul v M, pak je relace $\equiv_N$, zadaná předpisem $a \equiv_N b \Leftrightarrow a - b \in N$, kongruence R-modulu M.*

Důkaz. Cvičení.

Tvrzení. *Buď A nějaký R-modul, buď $X \subseteq A$ podmnožina. Pak pro podmodul $\bar{X}$ generovaný podmnožinou X platí $\bar{X} = \{r_1 x_1 + \cdots + r_k x_k \mid r_1, \ldots, r_k \in R, x_1, \ldots, x_k \in X\}$.*

Důkaz. Množina $\{r_1 x_1 + \cdots + r_k x_k \in A \mid r_1, \ldots, r_k \in R, x_1, \ldots, x_k \in X\}$ je podmodul v A a obsahuje X. A naopak, každý podmodul v A obsahující X obsahuje všechny prvky $r_1 x_1 + \cdots + r_k x_k$, kde $r_1, \ldots, r_k \in R$, $x_1, \ldots, x_k \in X$.

Součty modulů

Součin $A \times B$ modulů A, B se alternativně značí $A \oplus B$ a nazývá se též *součet* modulů. Jeho typickou vlastností je tzv. univerzální vlastnost součtu.

Tvrzení. *Buďte A, B dva R-moduly, $A \oplus B := A \times B$ jejich součin. Zaveďme zobrazení $\iota_A : A \to A \oplus B$, $a \mapsto (a, 0)$ a zobrazení $\iota_B : B \to A \oplus B$, $b \mapsto (0, b)$.*
Buď C další R-modul a $f : A \to C$, $g : B \to C$ dva homomorfismy. Pak existuje právě jeden homomorfismus $h : A \oplus B \to C$ takový, že $h \circ i_A = f$, $h \circ i_B = g$.

Důkaz. Existence: Pro $a \in A$, $b \in B$ položme $h(a, b) = f(a) + g(b) \in C$. Pak $h \circ \iota_A(a) = h(a, 0) = f(a)$, $h \circ \iota_B(b) = h(0, b) = g(b)$. Ukažme ještě, že h je homomorfismus. Sčítání: Pro libovolná $(a_1, b_1), (a_2, b_2) \in A \oplus B$ máme $h((a_1, b_1) + (a_2, b_2)) = h(a_1 + a_2, b_1 + b_2) = f(a_1 + a_2) + g(b_1 + b_2) = f(a_1) + f(a_2) + g(b_1) + g(b_2) = f(a_1) + g(b_1) + f(a_2) + g(b_2) = h(a_1, b_1) + h(a_2, b_2)$. Ostatní operace: Cvičení.
Jednoznačnost: Jest $h(a, 0) = h \circ \iota_A(a) = f(a)$, $h(0, b) = h \circ \iota_B(b) = g(b)$, a tedy $h(a, b) = h((a, 0) + (0, b)) = h(a, 0) + h(0, b) = f(a) + g(b)$.

Zobrazení ι_A, ι_B jsou injektivní homomorfismy. Ztotožníme-li sobě odpovídající prvky a a $\iota_A(a)$, a podobně b a $\iota_B(b)$, ztotožní se moduly A, B s podmoduly v $A \oplus B$. V následujícím tvrzení se předpokládá, že takové ztotožnění je provedeno.

Tvrzení. *Každý prvek R-modulu $A \oplus B$ lze právě jedním způsobem vyjádřit jako součet $a + b$ prvku $a \in A$ a $b \in B$.*

Důkaz. Existence: Obecný prvek v $A \oplus B$ je $(a, b) = (a, 0) + (0, b) = \iota_A(a) + \iota_B(b)$, což je $a + b$ při uvedeném ztotožnění.

Jednoznačnost: Rovnost $\iota_A(a_1) + \iota_B(b_1) = \iota_A(a_2) + \iota_B(b_2)$ znamená $(a_1, 0) + (0, b_1) = (a_2, 0) + (0, b_2)$, to jest, $(a_1, b_1) = (a_2, b_2)$, a tedy ($a_1 = a_2$ a $b_1 = b_2$.

Součet nekonečně mnoha modulů též existuje, avšak odlišuje se od jejich součinu.

Konstrukce. Buď $\{A_j\}_{j \in J}$ nějaký systém R-modulů. Položme

$$\bigoplus_{j \in J} A_j = \Big\{ (a_j)_{j \in J} \in \prod_{j \in J} A_j \;\Big|\; a_j = 0 \; \forall\, j \in J \text{ kromě konečně mnoha} \Big\}.$$

Definujme ještě $\iota_i : A_i \to \bigoplus_{j \in J} A_j$. Pro $a \in A_i$ budiž $\iota_i(a) \in \prod_{j \in J} A_j$, $(\iota_i(a))_j = a$ jestliže $i = j$ a $(\iota_i(a))_j = 0$ jinak.

Lze snadno ověřit, že $\bigoplus_{j \in J} A_j$ je R-podmodul v $\prod_{j \in J} A_j$ a že ι_j jsou homomorfismy. (Cvičení.)

Tvrzení. *Buď C nějaký R-modul, budte $f_j : A_j \to C$ homomorfismy. Pak existuje právě jeden homomorfismus $h : \bigoplus_{j \in J} A_j \to C$ takový, že $h \circ \iota_j = f_j$ pro každé $j \in J$.*

Důkaz. Cvičení. Návod: Položíme $h((a_j)_{j \in J}) = \sum_{j \in J} f_j(a_j)$.

Zobrazení ι_j jsou opět injektivní homomorfismy. Ztotožníme-li sobě odpovídající prvky a a $\iota_j(a)$, $a \in A_j$, ztotožní se moduly A_j s podmoduly v $\bigoplus_{j \in J} A_j$. V následujícím tvrzení se předpokládá, že takové ztotožnění je provedeno.

Tvrzení. *Každý prvek R-modulu $\bigoplus_{j \in J} A_j$ lze právě jedním způsobem vyjádřit jako součet $a_{j_1} + \cdots + a_{j_k}$ prvků $a_{j_1} \in A_{j_1}, \ldots, a_{j_k} \in A_{j_k}$.*

Důkaz. Existence: Pro obecný prvek (a_j) v $\bigoplus_{j \in J} A_j$ je $a_j \neq 0$ jen pro konečně mnoho indexů, označme je $j_1, \ldots, j_k$. Pak $(a_j) = \iota_{j_1}(a_{j_1}) + \cdots + \iota_{j_k}(a_{j_k})$, což je $a_{j_1} + \cdots + a_{j_k}$ při uvedeném ztotožnění.

Jednoznačnost: Cvičení.

Volné moduly

Definice. Buď dán modul F a množina X spolu se zobrazením $i : X \to F$. Řekneme, že modul F je *volný* nad množinou X, jestliže pro každý modul M a každé zobrazení $f : X \to M$ existuje právě jeden homomorfismus modulů $f^\# : F \to M$ takový, že $f^\# \circ i = f$.

Všimněme si, že podmínka jednoznačnosti homomorfismu znamená, že jsou-li h_1, h_2 dva homomorfismy $F \to M$ takové, že $h_1 \circ i = h_2 \circ i$, pak $h_1 = h_2$. Vskutku, $h_1 = (h_1 \circ i)^\# = (h_2 \circ i)^\# = h_2$.

Často se stává, že množina X je přímo podmnožinou modulu F_X a zobrazení i je vložením této podmnožiny. Pak je $f^\# \circ i$ totéž, co $f^\#|_X$.

Příklad. Každý konečněrozměrný vektorový prostor je volný nad kteroukoliv svou bází. Jedná se o známé tvrzení z lineární algebry.

Příklad. Okruh R je volný R-modul nad množinou $\{1\}$.

Tvrzení. *Jsou-li F_1, F_2 dva volné moduly nad touž množinou X, pak jsou izomorfní.*

Důkaz. Buďte $i_1 : X \to F_1$, $i_2 : X \to F_2$ příslušná zobrazení. Z definice volného modulu vyplývá existence homomorfismu $i_2^\# : F_1 \to F_2$ takového, že $i_2^\# \circ i_1 = i_2$ a homomorfismu $i_1^\# : F_2 \to F_1$ takového, že $i_1^\# \circ i_2 = i_1$. Ukažme, že homomorfismy $i_2^\#, i_1^\#$ jsou vzájemně inverzní, to jest, že $i_1^\# \circ i_2^\# = \mathrm{id}_{F_1}$ a $i_2^\# \circ i_1^\# = \mathrm{id}_{F_2}$. První rovnost ověříme výpočtem $i_1^\# \circ i_2^\# \circ i_1 = i_1^\# \circ i_2 = i_1 = \mathrm{id}_{F_1} \circ i_1$. Druhou rovnost ověříme analogicky.

Ukážeme si nyní, jak lze zkonstruovat volný R-modul F_X nad jakoukoliv množinou X, i nekonečnou. Poznamenejme, že podle předchozí věty je jakýkoliv volný R-modul nad touž množinou X izomorfní modulu F_X.

Konstrukce. Buď X libovolná množina. Označme F_X množinu všech zobrazení $a : X \to R$ takových, že $a(x) = 0$ pro všechna $x \in X$ kromě konečně mnoha. Opatřeme F_X strukturou R-modulu definovanou předpisem $(a + b)(x) = a(x) + b(x)$, $0(x) = 0$, $(-a)(x) = -(a(x))$ a $(ra)(x) = r(a(x))$ pro libovolná $a, b \in F_X$ a $r \in R$. Zaveďme zobrazení $i : X \to F$ předpisem $x \mapsto i_x$, kde $i_x : X \to R$ je přiřazení $x \mapsto 1$, $y \mapsto 0$ pro $y \neq x$.

Podmínka "$a(x) = 0$ pro všechna $x \in X$ kromě konečně mnoha" znamená, že pro existuje množina $Z_a \subset X$ taková, že $a|_{Z_a} = 0$ a množina $X \setminus Z_a$ je konečná.

Ověřte jako cvičení, že se skutečně jedná o R-modul.

Tvrzení. *R-modul F_X je volný nad množinou X.*

Důkaz. Buď M libovolný R-modul a $f : X \to M$ libovolné zobrazení. Existence homomorfismu $f^\#$: Definujme zobrazení $f^\# : F_X \to M$ předpisem

$$a \mapsto \sum_{x \in X} a(x)\, f(x).$$

(Na pravé straně stojí součet prvků $a(x)\, f(x)$ modulu M, z nichž jen konečně mnoho je nenulových, a proto je takový součet korektně definován i když je množina X případně nekonečná.)

Ověřme nejprve, že $f^\#$ je homomorfismus. Tak například, pro sčítání máme $f^\#(a + b) = \sum_x (a + b)(x) f(x) = \sum_x (a(x) + b(x)) f(x) = \sum_x a(x)\, f(x) + \sum_x b(x) f(x) = f^\#(a) + f^\#(b)$. Pro ostatní operace se postupuje analogicky.

Dále, $f^\# \circ i = f$, protože $f^\# \circ i(x) = f^\#(i_x) = \sum_y i_x(y) f(y) = f(x)$. Poslední rovnost plyne z faktu, že $i_x(y) = 0$ pro všechna $y \in X$ kromě jediného případu $y = x$, kdy je $i_x(x) = 1$.

Jednoznačnost homomorfismu $f^\#$: Cvičení.

Zobrazení $i : X \to F_X$ je zřejmě injektivní. Ztotožníme-li prvky $x \in X$ s jejich obrazy $i(x) \in F_X$, můžeme psát $X \subset F_X$. V následujícím tvrzení předpokládáme, že je takové ztotožnění provedeno.

Tvrzení. *Každý prvek $a \neq 0$ R-modulu F_X můžeme právě jedním způsobem zapsat ve tvaru $a = r_1 x_1 + \cdots + r_k x_k$, kde $r_1, \ldots, r_k \in R$ jsou libovolná nenulová, $x_1, \ldots, x_k \in X$ jsou po dvou různá.*

Důkaz. Existence: Uvažujme o obecném prvku R-modulu F_X, to jest, o zobrazení $a : X \to R$, kde $a(x) \neq 0$ jen pro konečně mnoho prvků z X, označme je $x_1, \ldots, x_k$, kde $k > 0$ pokud $a \neq 0$. Snadno se ověří, že pro všechna $x \in X$ platí $a(x) = a(x_1)i(x_1)(x) + \cdots + a(x_k)i(x_k)(x)$. Tudíž, $a = a(x_1)i(x_1) + \cdots + a(x_k)i(x_k)$. Při ztotožnění $x_1 = i(x_1), \ldots, x_k = i(x_k)$ a položíme-li $r_1 = a(x_1), \ldots, r_k = a(x_k)$, obdržíme hledané vyjádření.

Jednoznačnost: Nechť $r_1 i(x_1) + \cdots + r_k i(x_k) = s_1 i(y_1) + \cdots + s_l i(y_l)$, kde $x_1, \ldots, x_k$ jakož i $y_1, \ldots, y_l$ jsou po dvou různé a všechna $r_1, \ldots, r_k, s_1, \ldots, s_l$ jsou různá od nuly.

Na levé i pravé straně rovnosti jsou zobrazení $X \to R$, která musí nabývat stejných hodnot pro všechna $x \in X$. Pro $x = x_1$ dostáváme na levé straně r_1. Kdyby $y_j \neq x_1$ pro všechna j, pak by na pravé straně stála nula a $r_1 = 0$, což není možné. Proto existuje j_1 takové, že $x_1 = y_{j_1}$, ale toto j_1 je jediné, takže na pravé straně stojí s_{j_1}, a pak $r_1 = s_{j_1}$. Nyní odečteme rovnost $r_1 i(x_1) = s_{j_1} i(y_{j_1})$ od rovnosti původní a pokračujeme indukcí.

Důsledek. *Množina X generuje R-modul F_X.*

Existuje alternativní popis volného R-modulu:

Cvičení. $F_X \cong \bigoplus_{x \in X} R_x$, kde $R_x = R$ pro každé $x \in X$.