Učební texty k přednášce ALGEBRAICKÉ STRUKTURY
Michal Marvan, 2004
Matematický ústav v Opavě

2. Algebraické struktury

Množina opatřená algebraickou strukturou se nazývá algebra. Prakticky důležité algebry dané signatury zpravidla splňují ještě nějaké axiomy (jako je např. komutativní či asociativní zákon pro některou z binárních operací) a podle toho náležejí do určité třídy algeber, např. třídy všech polí či grup. Mnohé pojmy a konstrukce moderní algebry však závisí jen na výskytu algebraických operací, kdežto na platnosti axiomů už nikoliv. V několika následujících přednáškách se zaměříme právě na takové konstrukce. Mezi nejdůležitější patří podalgebry, homomorfismy algeber, faktorové algebry a součiny algeber. Zmíněné konstrukce se vždy týkají algeber jednoho a téhož typu. Například, abychom mohli definovat homomorfismus mezi okruhy, musíme vědět, které operace na obou okruzích jsou ‚sčítání,' které jsou ‚násobení,' atd. Proto je zvykem zvolit společnou indexovou množinu I a operace označovat indexy z I; operace se stejnými indexy přitom musí mít stejnou aritu. Tak například pro okruhy můžeme za příslušnou indexovou množinu zvolit přímo množinu symbolů $+, 0, -, \cdot, 1$, přičemž arity jsou po řadě $2, 0, 1, 2, 0$.

Definice. Buď I nějaká množina, buď $n : I \to \mathbf{N}$ nějaké zobrazení. Dvojice (I, n) se nazývá *signatura*. Přirozené číslo $n(i)$ (hodnota zobrazení n na prvku $i \in I$) se zpravidla značí n_i.

Příklad. Signatura okruhů je dvojice (I, n), kde $I = \{+, 0, -, \cdot, 1\}$ a $n_+ = 2$, $n_0 = 0$, $n_- = 1$, $n_\bullet = 2$, $n_1 = 0$.

Definice. Buď A množina. Řekneme, že je na A zadána *algebraická struktura* signatury (I, n), je-li pro každé $i \in I$ zadána nějaká algebraická operace α_i arity n_i. Množina A spolu s operacemi α_i, $i \in I$, se pak nazývá *algebra* signatury (I, n). Označujeme ji $(A, (\alpha_i)_{i \in I})$ nebo zkráceně A, jsou-li algebraické operace zřejmé z kontextu. Samotná množina A se nazývá *nosič* algebry $(A, (\alpha_i)_{i \in I})$.

Upřesněme, že dvě algebry jsou si rovny, mají-li stejné signatury (I, n), stejné nosiče A a stejné algebraické operace α_i na A pro každé $i \in I$.

Příklad (Aditivní grupa reálných čísel). Zobrazení $\alpha_+ : \mathbf{R}^2 \to \mathbf{R}$ definované předpisem $\alpha_+(x, y) = x + y$ je binární operace na množině $\mathbf{R}$, zobrazení $\alpha_- : \mathbf{R} \to \mathbf{R}$ takové, že $\alpha_-(x) = -x$ je unární operace na $\mathbf{R}$ a prvek $0 \in \mathbf{R}$ je nulární operace na $\mathbf{R}$. Množina $\mathbf{R}$ reálných čísel spolu s uvedenými algebraickými operacemi $\alpha_+ : \mathbf{R}^2 \to \mathbf{R}$, $\alpha_0 \in \mathbf{R}$, $\alpha_- : \mathbf{R} \to \mathbf{R}$, je příkladem algebry se signaturou $I = \{+, 0, -\}$, $n_+ = 2$, $n_0 = 0$, $n_- = 1$. Nazývá se aditivní grupa reálných čísel.

Příklad (Multiplikativní grupa nenulových reálných čísel). Na množině $\mathbf{R}^* := \mathbf{R} \setminus \{0\}$ je předpisem $\beta_+(x, y) = x \cdot y$ zadána binární operace $\beta_+ : \mathbf{R}^{*2} \to \mathbf{R}^*$. Zobrazení $\beta_- : x \mapsto x^{-1}$ je unární operací na téže množině $\mathbf{R}^*$. Nakonec, nulární operace β_0 budiž zadána jako prvek $1 \in \mathbf{R}^*$. Opět vzniká algebraická struktura, tentokrát na množině $\mathbf{R}^*$. Nazývá se multiplikativní podle toho, že binární operací je násobení. Všimněte si však, že jsme použili stejné signatury jako u aditivní abelovské grupy $\mathbf{R}$.

Příklad (Vektorový prostor). Každý vektorový prostor V nad polem P je abelovskou grupou vzhledem k operacím $+, 0, -$, tj. algebrou signatury $\{+, 0, -\}$, $n_+ = 2, n_0 = 0, n_- = 1$. Tzv. vnější operace $P \times V \to V$ (násobení skalárem), však není algebraickou operací v námi zavedeném smyslu. Jak jsme se již zmínili dříve, násobení skaláry $p \in P$ je možné a účelné chápat jako unární operace $V \to V$, $v \mapsto pv$, po jedné pro každý skalár p. Vektorový prostor pak bude algebrou signatury (I, n), kde $I = \{+, 0, -\} \cup P$ a $n_+ = 2$, $n_0 = 0$, $n_- = 1$, $n_p = 1$ pro každé $p \in P$.

Poznámka. Uvažujeme-li o třídě algeber splňujících nějaké axiomy, může se nám stát, že některá z algebraických konstrukcí povede k jejich porušení, přestože výchozí algebry tyto axiomy splňovaly. Například, jak uvidíme, součin dvou a více polí není nikdy polem (zatímco součin grup je vždy grupou). Vyjasnění podobných otázek je však věcí té které teorie (polí, grup, apod.) a bude probráno v kapitolách věnovaných takovým konkrétním teoriím.

Odvozené operace. Je-li $(A, (\alpha_i)_{i \in I})$ algebra, nazýváme operace α_i též *základní operace*. Můžeme totiž získávat další, tzv. *odvozené operace* jejich skládáním. Příkladem může být binární operace odečítání $\delta : \mathbf{R}^2 \to \mathbf{R}$, zadaná předpisem $\delta(a,b) = \alpha_+(a, \alpha_-(b)) = a + (-b) = a - b$. Jiným příkladem může být ternární operace sčítání $\sigma : \mathbf{R}^3 \to \mathbf{R}$ zadaná předpisem $\sigma(a,b,c) = \alpha_+(a, \alpha_+(b,c)) = a + (b + c)$. Je zřejmé, že při zadávání algebraické struktury není nutno odvozené operace uvádět.

Definice. Buďte $(A, (\alpha_i)_{i \in I})$ algebra signatury (I, n). Pro každé $m \in \mathbf{N}$ vždy existuje m projekcí $\mathrm{pr}_i : A^m \to A$, $(a_1, \ldots, a_m) \mapsto a_i$, $i = 1, \ldots, m$. Každá projekce je m-ární operace na A, byť poněkud triviální. *Odvozené operace* definujeme následujícími dvěma pravidly:

1. Každá základní operace α_i a každá projekce je odvozená operace.
2. Je-li α základní operace arity n a jsou-li $f_1, \ldots, f_n$ odvozené operace jedné a téže arity m, pak je m-ární operace $\alpha(f_1, \ldots, f_m)$, daná předpisem
$$\alpha(f_1, \ldots, f_n) : (x_1, \ldots, x_m) \mapsto \alpha(f_1(x_1, \ldots, x_m), \ldots, f_n(x_1, \ldots, x_m)),$$
zase odvozená operace.

Jde o rekurzívní definici. Pravidlem 1 je určena jakási výchozí množina odvozených operací, pravidlem 2 se tato množina postupně v libovolně mnoha krocích rozšiřuje. Operace, které není možno získat uvedeným postupem, odvozenými operacemi nejsou.

Příklad. Jsou-li základní operace zvoleny jako unární minus $\alpha_1(x_1) = -x_1$ a binární plus $\alpha_2(x_1, x_2) = x_1 + x_2$, pak je binární minus zadané předpisem $\delta(x_1, x_2) = x_1 - x_2 = x_1 + (-x_2)$ odvozenou operací. Lze ji získat ve dvou krocích:

1. $f_1 := \alpha_1(\mathrm{pr}_2)$;
2. $f_2 := \alpha_2(\mathrm{pr}_1, f_1) = \alpha_2(\mathrm{pr}_1, \alpha_1(\mathrm{pr}_2))$.

Vskutku, $f_1(x_1, x_2) = -x_2$ a $f_2(x_1, x_2) = x_1 + (-x_2)$.

Cvičení. Ukažte, že unární algebraická operace $\psi : \mathbf{R} \to \mathbf{R}$, $x \mapsto \frac{1}{2}x$ není odvozenou operací okruhu $\mathbf{R}$.

Návod: Ukažte, že pro každou odvozenou operaci g okruhu $\mathbf{R}$ platí, že $g(1)$ je celé číslo, kdežto $\psi(1)$ není celé číslo.

Cvičení. (Jste-li obeznámeni s teorií množin.) Buď dána konečná nebo spočetná množina základních operací na nekonečné množině A. Dokažte, že na A existují algebraické operace, které nejsou odvozené.

Návod: Ukažte, že množina všech odvozených operací na A je nejvýše spočetná zatímco množina všech operací na A je nespočetná.

Za zmínku stojí fakt, že volba základních operací je do značné míry věcí dohody či spíše tradice.

Příklad. Pokračujme v příkladu s odvozenou binární operací odečítání. Můžeme ji a nulu prohlásit za základní operace. Unární minus poté můžeme definovat jako odvozenou operaci $-a = 0 - a$ a sčítání definovat jako další odvozenou operaci $a + b = a - (-b)$. To znamená, že strukturu grupy lze stejně dobře zadat pomocí jedné binární operace ‚−' a jedné nulární operace ‚0'. Obě volby jsou zřejmě ekvivalentní v tom smyslu, že v obou případech je možné skládáním obdržet tytéž *množiny odvozených operací*.