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

1. Algebraické operace

Zadat algebraickou strukturu na nějaké množině je totéž co zadat soubor tzv. algebraických operací.

Definice. Buď A množina, buď $n \in \mathbf{N}$ přirozené číslo. Řekneme, že je na A zadána *n-ární algebraická operace*, zkráceně *n-ární operace*, je-li zadáno nějaké zobrazení $\alpha : A^n \to A$. Číslo n se pak nazývá *arita* operace α. Zde A^n označuje kartézskou mocninu $A \times A \times \cdots \times A$ ($n$krát).

Dále řekneme, že je na A zadána *nulární* operace, je-li zadán některý prvek z A. Arita nulární operace je definována jako číslo 0.

Místo 1-ární říkáme *unární*. Unární operace je tudíž zobrazení $\alpha : A \to A$. Místo 2-ární říkáme *binární*. Binární operace je tudíž zobrazení $\alpha : A \times A \to A$.

Operace arity 3 (říkáme jim *ternární*) a obecně arity vyšší než 2 se v algebře obvykle vyskytují jako tzv. operace odvozené. Jednoduchým příkladem může být ternární operace $(a, b, c) \mapsto a + (b + c)$, odvozená z binární operace $+$. Operace vyšší arity než 2, které nejsou odvozené z operací binárních, jsou v algebře výjimkou.

Uveďme některé dobře známé příklady algebraických operací a struktur. Začněme číselnými obory klasické algebry ($\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$) se čtyřmi základními aritmetickými operacemi – sčítáním, odečítáním, násobením a dělením. Dvě z uvedených binárních operací lze převést na unární: Binární operace odečítání je vlastně přičítání opačného prvku a dělení je zase násobení převrácenou hodnotou neboli inverzním prvkem. Proto místo binárních operací odečítání a dělení pracujeme s unárními operacemi ‚$-$‘ a ‚$^{-1}$‘. Abstrakcí pak obdržíme následující významné algebraické struktury:

Abelovské grupy. Abelovská grupa je množina A s binární operací $+$, nulární operací 0 a unární operací $-$ takovými, že pro všechna $a, b, c \in A$ platí

$$
\begin{aligned}
&1^\circ \quad a + b = b + a,\\
&2^\circ \quad a + (b + c) = (a + b) + c,\\
&3^\circ \quad a + 0 = a,\\
&4^\circ \quad a + (-a) = 0.
\end{aligned}
$$

Symboly operací $+, 0, -$ použité v definici abelovské grupy jsou charakteristické pro tzv. *aditivní zápis* abelovské grupy. Alternativní *multiplikativní zápis* používá symboly $\cdot, 1, ^{-1}$. Jiný rozdíl mezi aditivními a multiplikativními abelovskými grupami není.

Příklad. Množiny $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ jsou aditivní abelovské grupy s obvyklými operacemi $+, 0, -$. Množiny $\mathbf{Q}^* := \mathbf{Q} \setminus \{0\}$, $\mathbf{R}^* := \mathbf{R} \setminus \{0\}$, $\mathbf{C}^* := \mathbf{C} \setminus \{0\}$ jsou multiplikativní abelovské grupy s obvyklými operacemi $\cdot, 1, ^{-1}$.

Okruhy. Nejtypičtějšími strukturami klasické algebry jsou bezesporu okruhy. Jde o abelovské grupy s přidanou binární operací $\cdot$, nulární operací 1 a dodatečnými axiomy

$$5^\circ \quad a \cdot b = b \cdot a,$$
$$6^\circ \quad a \cdot (b \cdot c) = (a \cdot b) \cdot c,$$
$$7^\circ \quad a \cdot 1 = a,$$
$$8^\circ \quad a \cdot (b + c) = a \cdot b + a \cdot c.$$

Například množiny $\mathbf{Z}, \mathbf{Q}, \mathbf{R}, \mathbf{C}$ jsou okruhy s obvyklými operacemi $+, 0, -, \cdot, 1$.

V okruzích nemáme k dispozici dělení, a právě proto se okruhy hodí pro rozvíjení teorie dělitelnosti. A skutečně, ukazuje se, že dělitelnost celých čísel a polynomů lze vyložit jednotně v rámci teorie okruhů, přičemž okruh $\mathbf{Z}$ celých čísel a okruh $P[x]$ polynomů s koeficienty z pole P jsou potom jen speciální případy. Teorie dělitelnosti je však obsahem jiné přednášky, a proto se jí v tomto textu věnovat nebudeme. Upozorněme jen, že možnost dělení se zbytkem nevyplývá z axiomů okruhu.

Poznamenejme, že shora uvedené okruhy se plným jménem nazývají *komutativní asociativní okruhy s jedničkou*. Z uvedených podmínek lze slevit a definovat okruhy nekomutativní, případně neasociativní nebo bez jedničky.

Pole. *Pole* je okruh, v němž platí dodatečný axiom

$$9^\circ \quad \bigvee_{a \in A \setminus \{0\}} \bigvee_{b \in A} a \cdot b = 1.$$

Prvek $b = a^{-1}$ se nazývá *inverzní prvek* k prvku a.

Příklad. Pole $\mathbf{R}$ reálných čísel, pole $\mathbf{C}$ komplexních čísel a pole $\mathbf{Q}$ čísel racionálních.

Cvičení. Je-li A pole, pak $A \setminus \{0\}$ je multiplikativní abelovská grupa. Dokažte.

Návod: Ukažte nejprve, že $a \mapsto a^{-1}$ je zobrazení $A \setminus \{0\} \to A \setminus \{0\}$. Axiomy 1° až 4° multiplikativní grupy jsou pak právě axiomy 5° až 7° a 9° pole P.

S každým polem P jsou proto spojeny dvě abelovské grupy: *aditivní grupa* pole P je grupa na množině P s operacemi $+, 0, -$, *multiplikativní grupa* pole P je grupa na množině $P^* = P \setminus \{0\}$ s operacemi $\cdot, 1, ^{-1}$.

Zobrazení $a \mapsto a^{-1}$ je unární operace na množině $A \setminus \{0\}$ ale nikoliv na množině A. Pole proto není algebraická struktura se šesti operacemi $+, 0, -, \cdot, 1, ^{-1}$.

Příklad. Množina $\mathbf{Z}_2 = \{0, 1\}$ je dvouprvkovým polem, jsou-li operace $+$, $\cdot$, $-$ a $^{-1}$ zadány tabulkami

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

$-$	
0	1
1	0

$^{-1}$	
0	—
1	1

(Ověřte!). V každém počítači jsou obvody, které realizují operace pole $\mathbf{Z}_2$: $+$ je XOR, $\cdot$ je AND a $-$ je NOT.

Pozoruhodné je, že vztah $1 + 1 = 0$ není ve sporu s axiomy pole. Poznamenejme ještě, zatím bez důkazu, že konečné pole o n prvcích existuje pro každé $n \in \mathbf{N}$ tvaru $n = p^k$, kde p je prvočíslo a $k \in \mathbf{N}$.

Někdy se zavádějí tzv. *parciální* operace. Jsou to zobrazení $U \to A$, kde U je nějaká podmnožina v A^n (nazývá se definiční obor parciální operace). Operace s $U = A^n$ se pak nazývají *úplné*. Například pole by mohlo být chápáno jako algebra s úplnými operacemi $+, 0, -, \cdot, 1$ a parciální operací $^{-1}$. Studium parciálních algeber však přesahuje rámec této přednášky.

Vektorové prostory. Buď P pole. Vektorový prostor V nad P je aditivní abelovská grupa s operacemi $+, 0, -$, které jsou pořadě binární, nulární a unární. Dále je na množině V zavedeno *násobení skalárem*, obvykle jako zobrazení $P \times V \to V$, které není operací v námi zavedeném smyslu. Nicméně, násobení každým jednotlivým skalárem $r \in P$ je unární operací $r : V \to V$, $v \mapsto rv$. Vektorový prostor proto můžeme chápat jako algebru s operacemi $+, 0, -$ a množinou unárních operací $\{ r \}_{r \in P}$. Axiomy vektorového prostoru jsou čtenáři jistě známy.

Příklad. Typickým příkladem je množina n-tic

$$P^n = \{(x_1, \dots, x_n) \mid x_1, \dots, x_n \in P\}$$

pro libovolné $n \in \mathbf{N}$. V případě $P = \mathbf{R}$ lze prostor $\mathbf{R}^n$ (se zvoleným skalárním součinem) ztotožnit s prostorem vektorů reálného n-rozměrného eukleidovského prostoru se zvolenou kartézskou souřadnou soustavou. Tuto korespondenci vlastně popisuje Descartesova analytická geometrie z XVIII století.

Grupy. Abelovské grupy jsou speciální případy obecných grup. Nazýváme tak struktury s operacemi $*, 1, ^{-1}$ splňujícími axiomy

$$\begin{aligned} &\text{i}^\circ && a * (b * c) = (a * b) * c, \\ &\text{ii}^\circ && a * 1 = 1 * a = a, \\ &\text{iii}^\circ && a * a^{-1} = a^{-1} * a = 1. \end{aligned}$$

Bylo by velmi neobvyklé, kdybychom nekomutativní binární operaci označili symbolem $+$. Používá se však i jiných symbolů než $*$, nejčastěji $\cdot$ nebo $\circ$.

Historicky se jako první objevily *grupy permutací*. Bylo to začátkem XVIII století při studiu problému, kdy je algebraická rovnice řešitelná v radikálech (kdy lze řešení rovnice vyjádřit vzorci sestavenými z koeficientů, aritmetických operací pole $\mathbf{C}$ a odmocnin).

Příklad. (1) Permutací na množině M rozumíme bijekci $M \to M$; množina $\mathcal{P}M$ všech permutací na množině M je grupa vzhledem k binární operaci ‚$\circ$' (skládání permutací), unární operaci ‚$^{-1}$' (opačná permutace) a nulární operaci ‚id' (identická permutace). Je-li množina M alespoň dvouprvková, pak je grupa $(\mathcal{P}M, \circ, ^{-1}, \mathrm{id})$ neabelovská.

Několik následujících cvičení umožňuje pochopit nulární operaci jako speciální případ n-ární operace pro $n = 0$.

Cvičení. Pro libovolné $n \in \mathbf{N}$ nalezněte bijektivní zobrazení mezi kartézskou mocninou A^n a množinou všech zobrazení z n-prvkové množiny $\{1, \dots, n\}$ do množiny A.

V analogii s tímto výsledkem definujme nultou kartézskou mocninu množiny A jako množinu všech zobrazení z prázdné (tj. 0-prvkové) množiny $\emptyset$ do A.

Cvičení. Ukažte, že $\emptyset \subset \emptyset \times A$ je jediné zobrazení $\emptyset \to A$.

Odvodili jsme tak výsledek, že kartézská mocnina A^0 je jednoprvková množina $\{\emptyset\}$. Je zřejmé, že zadání zobrazení $\alpha : A^0 \to A$ je pak totéž, co zadání prvku $\alpha(\emptyset)$ z množiny A. Je tedy možné alternativně definovat nulární operaci na množině A jako zobrazení $A^0 \to A$, tedy prostě tak, že připustíme $n = 0$ v naší definici n-ární operace.