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

4. Kongruence

Definice. Buď $(A, (\alpha_i)_{i\in I})$ nějaká algebra signatury (I, n). Buď $\rho \subseteq A \times A$ relace ekvivalence na A. Řekneme, že ρ je *kongruence*, jestliže pro každou operaci α_i arity $n_i > 0$ platí *podmínka kompatibility*

$$a_1 \,\rho\, b_1, \ldots, a_{n_i} \,\rho\, b_{n_i} \Rightarrow \alpha_i(a_1, \ldots, a_n) \,\rho\, \alpha_i(b_1, \ldots, b_n).$$

(Pro nulární operace žádná podmínka kompatibility není.)

Každá ekvivalence, jako je ρ, vytváří rozklad $A = \bigcup_{a\in A}[a]_\rho$ množiny A na podmnožiny $[a]_\rho := \{b \in A \mid b\rho a\}$. Říkáme, že $[a]_\rho$ je *třída* určená prvkem $a \in A$, připomeňme, že vždy $a \in [a]_\rho$. Dva prvky určují tutéž třídu, $[a]_\rho = [b]_\rho$, právě když jsou ekvivalentní: $a\rho b$. Jsou-li však dvě třídy různé, pak jsou dokonce disjunktní.

Cvičení. Dokažte uvedená tvrzení o třídách ekvivalence.

Množina $\{[a]_\rho \bmod a \in A\}$ všech tříd ekvivalence ρ se značí A/ρ a nazývá se *faktorová množina* množiny A podle ekvivalence ρ.

Tvrzení. *Buď ρ kongruence na algebře $(A, (\alpha_i)_{i\in I})$, buď A/ρ příslušná faktorová množina. Pak na množině A/ρ existují operace $\bar\alpha_i$, $i \in I$, splňující*
(1) *Je-li $n_i = 0$, pak $\bar\alpha_i = [\alpha_i]_\rho$*
(2) *Je-li $n_i > 0$, pak $\bar\alpha_i([a_1]_\rho, \ldots, [a_{n_i}]_\rho) = [\alpha_i(a_1, \ldots, a_{n_i})]_\rho$ pro libovolné prvky $a_1, \ldots, a_{n_i} \in A$.*
Operace $\bar\alpha_i$ jsou podmínkami (1), (2) *určeny jednoznačně.*

Důkaz. V případě nulárních operací není co dokazovat.
Je-li $n_i > 0$, pak je předpisem $\bar\alpha([a_1]_\rho, \ldots, [a_n]_\rho) = [\alpha(a_1, \ldots, a_n)]_\rho$ korektně definováno zobrazení $(A/\rho)^n \to A/\rho$ jen tehdy, když je třída $[\alpha(a_1, \ldots, a_n)]_\rho$ (výsledek operace) jednoznačně určena již samotnými třídami $[a_1]_\rho, \ldots, [a_n]_\rho$ (a nezávisí na výběru jejich reprezentantů $a_1, \ldots, a_n$). Jinak řečeno, pro stejné argumenty, $[a_1]_\rho = [b_1]_\rho, \ldots, [a_n]_\rho = [b_n]_\rho$ musíme dostat stejné výsledky, $[\alpha_i(a_1, \ldots, a_n)]_\rho = [\alpha_i(b_1, \ldots, b_n)]_\rho$. To je však totéž co podmínka kompatibility.

Definice. Buď ρ kongruence na algebře $(A, (\alpha_i)_{i\in I})$. Algebra $(A/\rho, (\bar\alpha_i)_{i\in I})$ z předchozího tvrzení se nazývá *faktorová algebra* algebry A podle kongruence ρ.

Příklad. Uvažujme o okruhu $(\mathbf{Z}, +, 0, -, 1, \cdot)$. Buď $m > 1$ přirozené číslo. Definujme relaci $\equiv_m$ na množině $\mathbf{Z}$ předpisem $a \equiv_m b \Leftrightarrow m|(a - b)$. Čteme a je kongruentní s b modulo m. Platí:

1. $\equiv_m$ je kongruence na $\mathbf{Z}$.
2. $a \equiv_m b$ právě tehdy, když a, b dávají stejný zbytek po dělení číslem m.
3. Třídy ekvivalence $\equiv_m$ jsou množiny $[r]_m := \{r + km \mid k \in \mathbf{Z}\}$, tzv. *zbytkové třídy* modulo m.
4. Počet různých tříd je roven číslu m. Obvykle volíme $r = 0, \ldots, m - 1$. Prvky třídy $[r]_m$ jsou pak právě čísla n, jejichž zbytek po dělení číslem m je roven r.

Důkaz je snadným cvičením.

Ad 1. Je nutno dokázat, že $\equiv_m$ je relace ekvivalence splňující podmínky kompatibility vzhledem k operacím $+, -, \cdot$. Předveďme alespoň důkaz kompatibility vzhledem k násobení. Nechť tedy $a_1 \equiv_m b_1$ a $a_2 \equiv_m b_2$. Pak je $a_1 = b_1 + k_1 m$, $a_2 = b_2 + k_2 m$ pro nějaká čísla $k_1, k_2 \in \mathbf{Z}$, a tedy $a_1 a_2 = (b_1 + k_1 m)(b_2 + k_2 m) = b_1 b_2 + (k_1 b_2 + b_1 k_2 + k_1 k_2 m)m$. Vidíme, že $a_1 a_2 \equiv_m b_1 b_2$, což se mělo dokázat.

Faktorová algebra $\mathbf{Z}/\equiv_m$ se značí $\mathbf{Z}_m$ a nazývá se *okruh zbytkových tříd* modulo m. Popis algebraických operací v $\mathbf{Z}_m$ je následující: $[a]_m + [b]_m = [a+b]_m$, $[a]_m \cdot [b]_m = [ab]_m$, $-[a]_m = [-a]_m$; nulární operace jsou $[0]_m$ a $[1]_m$. Není těžké ověřit, že $\mathbf{Z}_m$ je opět okruh.

Výpočty v okruhu zbytkových tříd mohou usnadnit řešení některých úloh z elementární teorie čísel. Uveďme několik opravdu jednoduchých příkladů:

Cvičení. Ukažte, že číslo $3^p + 4^q - 7^r$ je dělitelné šesti pro všechna $p, q, r \in \mathbf{N}$.

Řešení: Počítejme v okruhu zbytkových tříd modulo 6. Především $[3^p + 4^q - 7^r]_6 = [3^p]_6 + [4^q]_6 - [7^r]_6 = [3]_6^p + [4]_6^q - [7]_6^r$. Dále $[3]_6^2 = [3]_6 \cdot [3]_6 = [9]_6 = [3]_6$, odtud snadno plyne, že $[3]_6^p = [3]_6$ pro každé celé $p > 1$. Podobně $[4]_6^2 = [4]_6 \cdot [4]_6 = [16]_6 = [4]_6$, a tedy analogicky $[4]_6^q = [4]_6$ pro každé celé $q > 1$. Do třetice, $[7]_6^r = [1]_6^r = [1]_6$. Dohromady $[3]_6^p + [4]_6^q - [7]_6^r = [3]_6 + [4]_6 - [1]_6 = [3 + 4 - 1]_6 = [0]_6$, což ukončuje důkaz.

Cvičení. Ukažte, že alespoň jedno z celých čísel a, b, c splňujících rovnost $a^2 + b^2 = c^2$ je dělitelné třemi.

Řešení: Počítejme v okruhu zbytkových tříd modulo 3. Především $[a]_3^2 + [b]_3^2 = [a^2 + b^2]_3 = [c^2]_3 = [c]_3^2$. Ale $[0]_3^2 = [0]_3$, zatímco $[1]_3^2 = [1]_3$ stejně jako $[2]_3^2 = [1]_3$. Jsou pak jen tři možnosti, jak dosáhnout výsledku $[a]_3^2 + [b]_3^2 = [c]_3^2$: (1) $[a]_3 = [b]_3 = [c]_3 = [0]_3$, (2) $[a]_3 = [c]_3 = [1]_3$, $[b]_3 = [0]_3$, (3) $[b]_3 = [c]_3 = [1]_3$, $[a]_3 = [0]_3$. Ve všech třech případech je však alespoň jedna třída nulová.