3. Věty o homomorfismech a kongruencích

3.1 Lemma. *Ať na množině A i na množině B je dána operace α četnosti n. Jsou-li $f : A \to B$ a $g : A \to B$ zobrazení slučitelná s α, tak $\{a \in A;\ f(a) = g(a)\}$ je uzavřená na α.*

Důkaz. Ať $a_i \in A$ a $f(a_i) = g(a_i)$ pro $1 \leq i \leq n$. Pak $f(\alpha_A(a_1, \ldots, a_n)) = \alpha_B(f(a_1), \ldots, f(a_n)) = \alpha_B(g(a_1), \ldots, g(a_n)) = g(\alpha_A(a_1, \ldots, a_n))$. $\square$

3.2 Tvrzení. *Ať $f : A \to B$, $g : A \to B$ jsou homomorfismy algeber $A = A(\alpha_1, \ldots, \alpha_k)$ a $B = B(\alpha_1, \ldots, \alpha_k)$. Potom $\{a \in A;\ f(a) = g(a)\}$ je podalgebra algebry A.*

Důkaz. $\{a \in A;\ f(a) = g(a)\}$ je podle 3.1 uzavřená na všechny operace α_i, $1 \leq i \leq k$. Je to tedy podalgebra A. $\square$

3.3 Důsledek. *Ať $f : A \to B$, $g : A \to B$ jsou homomorfismy algeber $A = A(\alpha_1, \ldots, \alpha_k)$ a $B = B(\alpha_1, \ldots, \alpha_k)$. Jestliže X generuje A a $f(a) = g(a)$ pro každé $a \in X$, tak $f = g$.*

Důkaz. $\{a \in A;\ f(a) = g(a)\}$ je podalgebra A, která obsahuje X. Ovšem jediná podalgebra A, jež obsahuje X, je přímo A. $\square$

Buď ρ ekvivalence na množině A. Každou ekvivalenci na A/ρ lze podle 1.9 jednoznačně vyjádřit jako σ/ρ, kde σ obsahuje ρ. Je-li $A = A(\alpha_1, \ldots, \alpha_n)$ algebra a ρ kongruence, je přirozené se tázat, kdy bude σ/ρ kongruence algebry A/ρ. Ukážeme, že σ/ρ je kongruence A/ρ právě když je σ kongruence A.

3.4 Lemma. *Buď ρ ekvivalence na množině A, jež je slučitelná s operací $\alpha = \alpha_A$ na A. Buď $\sigma \supseteq \rho$ další ekvivalence na A. Pak σ je slučitelné s α_A právě když σ/ρ je slučitelné s $\alpha_{A/\rho}$.*

Důkaz. Označme n četnost operace α a ať $a_1, \ldots, a_n$ a $b_1, \ldots, b_n$ jsou prvky A. Podle 1.8 je $(a_i, b_i) \in \sigma$ právě když $([a_i]_\rho, [b_i]_\rho) \in \sigma/\rho$. Předpokládejme, že $(a_i, b_i) \in \sigma$ platí pro všechna i, $1 \leq i \leq n$. Pak ekvivalence σ je slučitelná s α_A právě když pro libovolnou takovou volbu prvků a_i a b_i platí $(\alpha(a_1, \ldots, a_n), \alpha(b_1, \ldots, b_n)) \in \sigma$, zatímco ekvivalence σ/ρ je slučitelná s $\alpha_{A/\rho}$ právě když pro libovolné takové a_i a b_i platí $([\alpha(a_1, \ldots, a_n)]_\rho, [\alpha(b_1, \ldots, b_n)]_\rho) \in \sigma/\rho$. Poslední podmínka je ovšem, opět podle 1.8, shodná s podmínkou $(\alpha(a_1, \ldots, a_n), \alpha(b_1, \ldots, b_n)) \in \sigma$. $\square$

Z dokázaného lemmatu okamžitě plyne:

3.5 Tvrzení. *Buď ρ kongruence algebry $A = A(\alpha_1, \ldots, \alpha_k)$ a ať $\sigma \supseteq \rho$ je ekvivalence na A. Potom σ/ρ je kongruence algebry A/ρ právě když σ je kongruence algebry A.*

Buď dána $A = A(\alpha_1, \ldots, \alpha_k)$. Triviální ekvivalence id_A i universální ekvivalence $A \times A$ jsou slučitelné s každou operací α_i, $1 \leq i \leq k$, takže obě tyto ekvivalence patří mezi kongruence algebry A. Těmto kongruencím se říká *nevlastní*, zatímco ostatní kongruence algebry A jsou *vlastní*. Nemá-li algebra A vlastní kongruence a má-li přitom alespoň dva prvky, nazýváme ji *jednoduchou*.

Kongruenci ρ algebry $A = A(\alpha_1, \ldots, \alpha_k)$ nazveme *maximální*, jestliže

(i) $\rho \neq A \times A$ a

(ii) pro každou kongruenci σ algebry A ze $\sigma \supseteq \rho$ plyne $\sigma = \rho$ nebo $\sigma = A \times A$.

Algebra $A = A(\alpha_1, \ldots, \alpha_k)$ je tedy jednoduchá právě tehdy, když id_A je maximální kongruence A.

3.6 Tvrzení. *Buď ρ kongruence algebry $A = A(\alpha_1, \ldots, \alpha_k)$. Potom A/ρ je jednoduchá algebra právě když ρ je maximální kongruence algebry A.*

Důkaz. Všechny kongruence A/ρ mají podle 3.5 tvar σ/ρ, kde σ obsahuje ρ. Mezi $A \times A$ a ρ proto neleží žádná další kongruence právě tehdy, když neleží žádná kongruence mezi $(A \times A)/\rho = (A/\rho) \times (A/\rho)$ a $\rho/\rho = \mathrm{id}_{A/\rho}$. $\square$

Nyní obrátíme svou pozornost na Tvrzení 1.10 a ukážeme, jak ho vztáhnout na algebry. Následující věty patří v algebře k těm nejužívanějším.

3.7 Lemma. *Ať je na množině A i na množině B dána operace α četnosti n a ať $f : A \to B$ je zobrazení slučitelné s α. Ať dále ρ je ekvivalence A slučitelná s α. Zobrazení $g : A/\rho \to B$ slučitelné s α a takové, že $f = g \circ \mathrm{nat}_\rho$, existuje právě když $\rho \subseteq \ker f$. Je-li $\rho \subseteq \ker f$, je g určeno jednoznačně, $g([a]_\rho) = f(a)$ pro každé $a \in A$ a $\ker g = (\ker f)/\rho$.*

Důkaz. Vzhledem k 1.10 je třeba pouze dokázat, že v případě $\rho \subseteq \ker f$ je zobrazení g dané vztahem $g([a]_\rho) = f(a)$ slučitelné s α. Ať $a_1, \ldots, a_n \in A$. Pak $g(\alpha_{A/\rho}([a_1]_\rho, \ldots, [a_n]_\rho)) = g([\alpha_A(a_1, \ldots, a_n)]_\rho) = f(\alpha_A(a_1, \ldots, a_n))$, což je rovno $\alpha_B(f(a_1), \ldots, f(a_n)) = \alpha_B(g([a_1]_\rho), \ldots, g([a_n])_\rho))$. $\square$

Ze 3.7 bezprostředně dostáváme:

3.8 Tvrzení. (Věta o homomorfismu.) *Buď dán homomorfismus $f : A \to B$ algeber $A = A(\alpha_1, \ldots, \alpha_k)$ a $B = B(\alpha_1, \ldots, \alpha_k)$, a ať ρ je kongruence A. Homomorfismus $g : A/\rho \to B$ takový, že $f = g \circ \mathrm{nat}_\rho$, existuje právě když $\rho \subseteq \ker f$. Je-li $\rho \subseteq \ker f$, pak je g určeno jednoznačně, $g([a]_\rho) = f(a)$ pro každé $a \in A$ a $\ker g = (\ker f)/\rho$. Přitom g je izomorfismus právě když je f surjektivní a platí $\ker f = \rho$.*

3.9 Důsledek. (1. věta o izomorfismu.) *Ať $f : A \to B$ je surjektivní homomorfismus algeber $A = A(\alpha_1, \ldots, \alpha_k)$ a $B = B(\alpha_1, \ldots, \alpha_k)$. Pak $[a]_{\ker f} \mapsto f(a)$ je izomorfismus algeber $A/\ker f$ a B.*

3.10 Důsledek. (2. věta o izomorfismu.) *Ať $A = A(\alpha_1, \ldots, \alpha_k)$ je algebra a $\rho \subseteq \sigma$ jsou její kongruence. Pak $[[a]_\rho]_{\sigma/\rho} \mapsto [a]_\sigma$ je izomorfismus $A/\rho \big/ \sigma/\rho \simeq A/\sigma$.*

Důkaz. Podle 3.8 lze $\mathrm{nat}_\sigma : a \mapsto [a]_\sigma$ faktorizovat přes ρ, takže $[a]_\rho \mapsto [a]_\sigma$ je homomorfismus $A/\rho \to A/\sigma$. Jeho jádrem je podle 3.8 kongruence σ/ρ a zbytek plyne z 3.9. $\square$