2. Operace, algebry, homomorfismy a kongruence

Je-li A množina, tak A^n, $n \geq 1$ bude značit, jak je obvyklé, kartézský součin $A \times \cdots \times A$ o n činitelích. Prvky A^n jsou všechny n–tice $(a_1, \ldots, a_n)$, kde $a_1, \ldots, a_n$ jsou prvky A. Všimněte si, že bychom také mohli A^n definovat jako množinu všech zobrazení z $\{1, \ldots, n\}$ do A. Při takové definici je pak přirozené A^0 definovat jako množinu všech zobrazení z $\emptyset$ do A. Ovšem $\emptyset \times A = \emptyset$, takže takové zobrazení existuje právě jedno, a je to opět $\emptyset$. Je tedy $A^0 = \{\emptyset\}$.

Operací četnosti $n \geq 0$ na množině A rozumíme každé zobrazení A^n do A. Operace četnosti 0 je tudíž zobrazení $\{\emptyset\}$ do A, čili pro každé $a \in A$ existuje právě jedna operace f_a četnosti 0 taková, že $f_a(\emptyset) = a$. Operaci f_a a prvek a můžeme ztotožnit, neboť se liší jen formálně. Operací četnosti 0 proto prostě pro nás bude vybrání nějakého prvku množiny A.

Operace četnosti nula se nazývá nulární operace, operace četnosti jedna unární operace, četnosti dva binární operace a četnosti tři ternární operace. Mluvíme také o n–ární operaci f, přičemž n se nazývá *aritou* f.

Lze se setkat s prefixovým, infixovým a sufixovým zápisem operace — v případě binární operace je $f(a, b)$ prefixový, afb infixový a $(a, b)f$ či $(a, b)^f$ sufixový zápis.

Často bude pro nás výhodné, abychom operace na dvou různých množinách (například A a B) značili stejně (například $+$). Pokud budeme v takovém případě potřebovat v zápise rozlišit mezi oběma operacemi, připojíme k označení operace vhodný index (například označení množiny, píšeme pak $+_A$ a $+_B$).

Buď na množině A dána operace α četnosti n. O podmnožině $C \subseteq A$ řekneme, že je *uzavřená na* α právě když $\alpha(c_1, \ldots, c_n) \in C$ pro všechna $c_1, \ldots, c_n \in C$. Všimněte si, že pokud je α nulární operace, tak $C \subseteq A$ je uzavřená na α právě když $\alpha_A \in C$.

2.1 Tvrzení. *Ať je na množině A dána operace α. Potom soustava všech podmnožin A, které jsou uzavřené na α, tvoří uzávěrový systém nad A.*

Důkaz. Buď C_j, $j \in J \neq \emptyset$, množiny uzavřené na $\alpha : A^n \to A$. Jestliže $c_1, \ldots, c_n \in C_j$ pro všechna $j \in J$, je i $\alpha(c_1, \ldots, c_n) \in C_j$ pro všechna $j \in J$. $\square$

Ať na množinách A a B je dána operace α (stejné) četnosti $n \geq 0$. O *zobrazení* $f : A \to B$ řekneme, že je *slučitelné* s operací α, jestliže pro libovolné $a_1, \ldots, a_n \in A$ platí

$$f\alpha_A(a_1, \ldots, a_n) = \alpha_B(f(a_1), \ldots, f(a_n)).$$

Všimněte si, že v případě $n = 0$ je f slučitelná s α právě když $f(\alpha_A) = \alpha_B$.

2.2 Tvrzení. *Ať je na množinách A, B a C dána operace α četnosti $n \geq 0$. Buď $f : A \to B$ a $g : B \to C$ zobrazení slučitelná s α. Potom je i $g \circ f : A \to C$ zobrazení slučitelné s operací α.*

Je-li $f : A \to B$ bijektivní zobrazení slučitelné s α, je $f^{-1} : B \to A$ také zobrazení slučitelné s α.

Důkaz. Buď $a_1, \ldots, a_n \in A$. Potom $(g \circ f)(\alpha_A(a_1, \ldots, a_n))$ je rovno $g(\alpha_B(f(a_1), \ldots, f(a_n))) = \alpha_C(g(f(a_1)), \ldots, g(f(a_n)))$. Ať je $f : A \to B$ bijektivní a ať $b_1, \ldots, b_n \in B$. Potom existují $a_i \in A$, že $b_i = f(a_i)$, $1 \leq i \leq n$, takže z $f(\alpha_A(a_1, \ldots, a_n)) = \alpha_B(b_1, \ldots, b_n)$ plyne $f^{-1}(\alpha_B(b_1, \ldots, b_n)) = \alpha_A(f^{-1}(b_1), \ldots, f^{-1}(b_n))$. $\square$

Typeset by $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX

2.3 Tvrzení. *Předpokládejme, že na A i na B je dána operace α četnosti n, a ať $f : A \to B$ je zobrazení slučitelné s α. Je-li $C \subseteq A$ množina uzavřená na α, je $f(C)$ rovněž uzavřená na α. Specielně je tedy* $\mathrm{Im}(f)$ *uzavřená na α. Naopak, je-li $D \subseteq B$ uzavřená na α, je $f^{-1}(D)$ také uzavřená na α.*

Proof. Buď $b_1, \dots, b_n \in f(C)$. Pak existují $a_1, \dots, a_n \in C$, že $b_1 = f(a_1), \dots, b_n = f(a_n)$. Tudíž $\alpha(b_1, \dots, b_n) = \alpha(f(a_1), \dots, f(a_n)) = f(\alpha(a_1, \dots, a_n)) \in f(C)$.

Buď nyní $D \subseteq B$ uzavřená na α a ať $a_1, \dots, a_n \in f^{-1}(D)$. Prvky $f(a_1), \dots, f(a_n)$ jsou z D, takže $f(\alpha(a_1, \dots, a_n)) = \alpha(f(a_1), \dots, f(a_n)) \in D$, a tedy $\alpha(a_1, \dots, a_n) \in f^{-1}(D)$. $\square$

Buď α operace četnosti n na A. O *relaci* ρ na A řekneme, že je *slučitelná* s α, jestliže pro libovolná $a_1, \dots, a_n \in A$ a $b_1, \dots, b_n \in A$ taková, že $a_1 \rho b_1, \dots, a_n \rho b_n$, platí $\alpha(a_1, \dots, a_n)\ \rho\ \alpha(b_1, \dots, b_n)$. Všimněte si, že s nulární operací je slučitelná každá reflexivní relace. Všimněte si také, že triviální ekvivalence id_A i universální ekvivalence $A \times A$ jsou slučitelné s libovolnou operací α.

2.4 Tvrzení. *Buď α operace četnosti n na A. Potom všechny relace (resp. ekvivalence) na A slučitelné s α tvoří uzávěrový systém nad $A \times A$.*

Důkaz. Buďte $a_1, \dots, a_n \in A$ a $b_1, \dots, b_n \in A$ takové, že $a_1 \rho_j b_1, \dots, a_n \rho_j b_n$ pro všechna $j \in J \neq \emptyset$, kde ρ_j jsou relace na A slučitelné s α. Potom pro každé $j \in J$ platí $\alpha(a_1, \dots, a_n)\ \rho_j\ \alpha(b_1, \dots, b_n)$. $\square$

2.5 Tvrzení. *Ať na množinách A a B je dána operace α téže četnosti n. Je-li $f : A \to B$ zobrazení slučitelné s α, tak* $\ker f$ *je ekvivalence slučitelná s α.*

Proof. Ať $a_1, \dots, a_n \in A$ a $b_1, \dots, b_n \in A$ jsou takové, že $f(a_1) = f(b_1), \dots, f(a_n) = f(b_n)$. Potom $f(\alpha(a_1, \dots, a_n)) = \alpha(f(a_1), \dots, f(a_n)) = \alpha(f(b_1), \dots, f(b_n)) = f(\alpha(b_1, \dots, b_n))$. $\square$

Buď ρ ekvivalence na A slučitelná s operací $\alpha : A^n \to A$. Na A/ρ definujeme operaci α tak, že jsou-li $B_1, \dots, B_n$ ekvivalenční třídy ρ, přičemž $a_1 \in B_1, \dots, a_n \in B_n$, položíme $\alpha(B_1, \dots, B_n) = [\alpha(a_1, \dots, a_n)]_\rho$. Jinak vyjádřeno, $\alpha([a_1]_\rho, \dots, [a_n]_\rho) = [\alpha(a_1, \dots, a_n)]_\rho$ pro libovolná $a_1, \dots, a_n \in A$.

Je ovšem třeba dokázat, že takto lze operaci α na A/ρ skutečně definovat, tj. že takováto definice je korektní. Pro $b_1 \in B_1, \dots, b_n \in B_n$ platí $a_1 \rho b_1, \dots, a_n \rho b_n$, takže podle definice slučitelnosti je $\alpha(a_1, \dots, a_n)\ \rho\ \alpha(b_1, \dots, b_n)$, a tedy $[\alpha(a_1, \dots, a_n)]_\rho = [\alpha(b_1, \dots, b_n)]_\rho$. Hodnota $\alpha(B_1, \dots, B_n)$ je tedy nezávislá na tom, které prvky $a_i \in B_i$, $1 \le i \le n$, jsme vybrali.

2.6 Tvrzení. *Buď α operace četnosti n na A a ρ ekvivalence na A slučitelná s α. Potom přirozené zobrazení* $\mathrm{nat}_\rho : A \to A/\rho$ *je slučitelné s α.*

Důkaz. Buď $a_1, \dots, a_n \in A$. Potom $\mathrm{nat}_\rho(\alpha_A(a_1, \dots, a_n)) = [\alpha_A(a_1, \dots, a_n)]_\rho = \alpha_{A/\rho}([a_1]_\rho, \dots, [a_n]_\rho) = \alpha_{A/\rho}(\mathrm{nat}_\rho(a_1), \dots, \mathrm{nat}_\rho(a_n))$. $\square$

Množinu A spolu s operacemi $\alpha_1, \dots, \alpha_k$ na A nazýváme *algebrou* na A. Někdy tuto algebru označujeme samostatným symbolem, pak například píšeme $B = A(\alpha_1, \dots, \alpha_k)$ a říkáme, že A je *nosičem* algebry B. Častěji algebru i její nosič označujeme stejným symbolem. Pak píšeme například $A = A(\alpha_1, \dots, \alpha_n)$ (tento zápis je sice trochu nelogický, leč zcela běžný).

V dalším textu budou $+$, $\cdot$, $\circ$, $\wedge$, $\vee$ (a případné od nich odvozené varianty) označovat vždy binární operace. Naopak $^{-1}$, $-$ a $'$ značí unární operace a $\mathbf{0}$, $\mathbf{1}$ nulární operace.

Algebra $S = S(\cdot)$ se nazývá *pologrupa*, jestliže $\cdot$ splňuje asociativní zákon (tj. $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ pro libovolná $a, b, c \in S$). Prvek $e \in S$ se nazývá *neutrální*, jestliže $a \cdot e = e \cdot a = a$ pro libovolné $a \in S$.

2.7 Tvrzení. *Pologrupa $S(\cdot)$ obsahuje nanejvýš jeden neutrální prvek.*

Důkaz. Buď $e, f \in S$ neutrální prvky. Pak $e = e \cdot f = f$ $\square$

Algebra $S = S(\cdot, \mathbf{1})$ se nazývá *monoid*, jestliže $S(\cdot)$ je pologrupa a $\mathbf{1}$ je její neutrální prvek.

Příklady pologrup a monoidů:

A. Buď $\mathbb{N}$ množina všech přirozených čísel $\{1, 2, \dots\}$, $\mathbb{N}_0$ množina všech nezáporných celých čísel $\{0, 1, 2, \dots\}$ a $\mathbb{Z}$ množina všech celých čísel $\{\dots, -2, -1, 0, 1, 2, \dots\}$. Potom $\mathbb{N}(\cdot, 1)$, $\mathbb{N}_0(\cdot, 1)$, $\mathbb{Z}(\cdot, 1)$ jsou monoidy, $\mathbb{N}_0(+, 0)$ a $\mathbb{Z}(+, 0)$ jsou rovněž monoidy, ale $\mathbb{N}(+)$ je pologrupa bez neutrálního prvku.

B. Položme $Bool = \{\mathrm{T}, \mathrm{F}\}$ a definujme na $Bool$ binární operaci $\cdot$ odpovídající logickému 'AND' (tj. $\mathrm{T} \cdot \mathrm{F} = \mathrm{F} \cdot \mathrm{T} = \mathrm{F} \cdot \mathrm{F} = \mathrm{F}$ a $\mathrm{T} \cdot \mathrm{T} = \mathrm{T}$). Potom $Bool(\cdot, \mathrm{T})$ je monoid.

C. Buď $\mathbb{A}$ nějaká abeceda. Potom množina $\mathbb{A}^+$ všech neprázdných slov nad $\mathbb{A}$ je pologrupa vzhledem k operaci konkatenace (tj. $a_1 \dots a_n \cdot b_1 \dots b_m$ je rovno slovu $a_1 \dots a_n b_1 \dots b_m$). Přidáme-li k $\mathbb{A}^+$ prázdné slovo λ, dostaneme množinu, jež se obvykle značí $\mathbb{A}^*$. $\mathbb{A}^*(\cdot, \lambda)$ je monoid.

D. Je-li Ω libovolná množina, tak množina T_Ω všech zobrazení z Ω do Ω je monoid vzhledem k operaci skládání zobrazení $\circ$ a neutrálnímu prvku id_Ω. $T_\Omega(\circ, \mathrm{id}_\Omega)$ se nazývá *transformační monoid* množiny Ω.

Pologrupa (monoid) se nazývá *komutativní*, jestliže $a \cdot b = b \cdot a$ pro všechny prvky a, b této pologrupy (monoidu). V příkladech A a B jsou uvedeny komutativní monoidy, monoidy z příkladů C a D jsou (obecně vzato) nekomutativní.

Buď dána algebra $A = A(\alpha_1, \dots, \alpha_n)$. Řekneme, že množina $C \subseteq A$ je *podalgebra* A, jestliže C je uzavřená na všechny operace $\alpha_1, \dots, \alpha_n$. Z 1.2 a 2.1 okamžitě dostáváme:

2.8 Tvrzení. *Všechny podalgebry algebry $A = A(\alpha_1, \dots, \alpha_n)$ tvoří uzávěrový systém nad A.*

Podalgebru C algebry $A(\alpha_1, \dots, \alpha_n)$ chápeme skutečně jako algebru, tj. předpokládáme, že je vybavena operacemi $\alpha_1, \dots, \alpha_n$, jež jsou zúžením původních operací na A.

Podalgebře monoidu se říká podmonoid, podalgebře pologrupy podpologrupa, a podobně i u dalších typů algeber.

Je-li A algebra a $\mathcal{C}$ uzávěrový systém jejích podalgeber, tak $\mathrm{cl}_{\mathcal{C}}(B)$ se pro $B \subseteq A$ obvykle nazývá podalgebra *generovaná množinou B*.

Buď $A = A(\alpha_1, \dots, \alpha_n)$ a $B = B(\alpha_1, \dots, \alpha_n)$ dvě algebry, a ať $f : A \to B$ je zobrazení. Toto zobrazení nazveme *homomorfismem*, jestliže f je slučitelné s každou operací α_i, $1 \le i \le n$. Z 2.2 plyne

2.9 Tvrzení. *Buď dány algebry $A = A(\alpha_1, \dots, \alpha_n)$, $B = B(\alpha_1, \dots, \alpha_n), C = C(\alpha_1, \dots, \alpha_n)$ a homomorfismy $f : A \to B$, $g : B \to C$. Potom $g \circ f : A \to C$ je také homomorfismus. Je-li $f : A \to B$ bijektivní, je $f^{-1} : B \to A$ rovněž homomorfismus.*

2.10 Tvrzení. *Buď $f : A \to B$ homomorfismus algeber $A = A(\alpha_1, \dots, \alpha_n)$ a $B = B(\alpha_1, \dots, \alpha_n)$. Je-li C podalgebra A, je $f(C)$ podalgebra B. Specielně je* $\operatorname{Im} f$ *podalgebrou B. Naopak, je-li D podalgebra B, je $f^{-1}(D)$ podalgebra A.*

Homomorfismus $f : A \to B$ se nazývá *izomorfismus*, je-li f bijektivní. Izomorfní algebry mají stejnou strukturu a liší se jen označením svých prvků.

Homomorfismus $f : A \to A$ se nazývá *endomorfismus*, bijektivní endomorfismus se nazývá *automorfismus*. Množina všech endomorfismů se značí $\operatorname{End}(A)$. Množina všech automorfismů se značí $\operatorname{Aut}(A)$.

2.11 Tvrzení. *Buď dána algebra $A = \Omega(\alpha_1, \dots, \alpha_n)$. Potom* $\operatorname{End}(A)$ *je podmonoid monoidu T_Ω.*

Důkaz. $\mathrm{id}_A \in \operatorname{Aut}(A) \subseteq \operatorname{End}(A)$ a z $f, g \in \operatorname{End}(A)$ plyne podle 2.9 $g \circ f \in \operatorname{End}(A)$. $\square$

Příklady podalgeber a homomorfismů:

A. Je-li $S(\cdot, \mathbf{1})$ monoid, je $\{\mathbf{1}\}$ podmonoid S. Například $\{0\}$ je podmonoid $\mathbb{Z}(+, 0)$. Buď $n \in \mathbb{Z}$. Pak $n\mathbb{Z} = \{na;\, a \in \mathbb{Z}\}$ je podmonoid $\mathbb{Z}(+, 0)$ a podpologrupa $\mathbb{Z}(\cdot)$. Pro $-1 \neq n \neq 1$ ovšem $n\mathbb{Z}$ není podmonoid $\mathbb{Z}(\cdot, 1)$. Zobrazení $\varphi : \mathbb{Z}(+, 0) \to n\mathbb{Z}(+, 0)$, $\varphi(a) = na$ pro každé $a \in \mathbb{Z}$, je izomorfismus, jestliže $n \neq 0$.

B. Zobrazení $\theta : \mathbb{Z}(\cdot, 1) \to \mathit{Bool}(\cdot, \mathrm{T})$ takové, že $\theta(a) = \mathrm{T}$ pro $a \neq 0$ a $\theta(0) = \mathrm{F}$, je surjektivní homomorfismus. Naopak, $\beta : \mathit{Bool}(\cdot, \mathrm{T}) \to \mathbb{Z}(\cdot, 1)$, $\beta(\mathrm{T}) = 1$, $\beta(\mathrm{F}) = 0$ je injektivní homomorfismus. Z 2.10 plyne, že $\operatorname{Im}(\beta) = \{0, 1\}$ je podmonoid $\mathbb{Z}(\cdot, 1)$ (to lze samozřejmě nahlédnout také přímo).

Poznámka. Při definici homomorfismu z algebry $A = A(\alpha_1, \dots, \alpha_n)$ do algebry $B = B(\alpha_1, \dots, \alpha_n)$ jsme předpokládali, že operace jsou v oboru algebrách označeny stejně. V předchozím příkladu ovšem neutrální prvek z $\mathbb{Z}$ je 1 a v *Bool* je T. Přesto i zde hovoříme o homomorfismu. Důležité totiž je, aby bylo jasné, která operace v B odpovídá které operaci v A, nikoliv zcela shodné formální označení. V tomto duchu budeme s homomorfismy zacházet i jinde – je to tak pružnější než pracovat s korektnější, ale těžkopádnou definicí, ve které by se formálně specifikovalo, která operace bude odpovídat které.

C. Definujme $\sigma : \mathbb{A}^* \to \mathbb{N}_0$ tak, že pro $a_1, \dots, a_n \in \mathbb{A}$ je $\sigma(a_1 \dots a_n) = n$ (σ udává tedy délku slova). Zobrazení σ je homomorfismus $\mathbb{A}^*$ na $\mathbb{N}_0$.

D. Ať $\Omega \neq \emptyset$. Zobrazení $\omega \in T_\Omega$ nazveme *konstantním*, jestliže existuje $a \in \Omega$ takové, že $\omega(b) = a$ pro každé $b \in \Omega$. Potom množina všech konstantních zobrazení C_Ω tvoří podpologrupu T_Ω. Množina $C_\Omega \cup \{\mathrm{id}_\Omega\}$ je podmonoidem T_Ω.
Zobrazení $\omega : \Omega \to \Omega$ se nazývá *permutace*, je-li bijektivní. Složení dvou permutací je opět permutace, takže množina S_Ω všech permutací tvoří podmonoid T_Ω. Tomuto podmonoidu se říká *symetrická grupa*. Symetrickou grupu na množině $\{1, 2, \dots, n\}$ značíme S_n.
Definujme zobrazení $\tau : T_\Omega \to \mathit{Bool}$ tak, že pro $\omega \in T_\Omega$ je $\tau(\omega) = \mathrm{T}$, je-li ω permutace a $\tau(\omega) = \mathrm{F}$, není-li ω permutace. Zobrazení τ je homomorfismus právě když Ω je konečná množina.

Je-li B podalgebra algebry A, tak zobrazení *inkluze* $i_B : B \to A$, $i_B(b) = b$ pro každé $b \in B$, je zjevně injektivní homomorfismus.

Buď dána algebra $A = A(\alpha_1, \dots, \alpha_n)$. Ekvivalenci ρ na A nazveme *kongruencí algebry* A, jestliže je slučitelná s každou operací α_i, $1 \leq i \leq n$. Z 2.4 a 1.2 dostáváme

2.12 Tvrzení. *Buď $A = A(\alpha_1, \dots, \alpha_n)$ algebra. Všechny její kongruence tvoří uzávěrový systém nad $A \times A$.*

2.13 Tvrzení. *Buď $f : A \to B$ homomorfismus algeber. Potom je* $\ker f$ *kongruence algebry A.*

Konečně z 2.6 okamžitě odvodíme

2.14 Tvrzení. *Buď ρ kongruence algebry A. Potom přirozené zobrazení* nat_ρ : $A \to A/\rho$ *je homomorfismus a* $\rho = \ker \mathrm{nat}_\rho$.

Příklady kongruencí:

A. Pro $a, b \in \mathbb{Z}$ a $n \in N$ pišme $a \equiv b \bmod n$ (a je kongruentní s b modulo n) právě když n dělí $a - b$. Je zřejmé, že $\bmod n$ je kongruence jak $\mathbb{Z}(+, 0)$, tak $\mathbb{Z}(\cdot, 1)$.
B. $\ker \theta$ je kongruence $\mathbb{Z}(\cdot, 1)$, která má dvě ekvivalenční třídy – v jedné leží nula a v druhé všechna ostatní přirozená čísla.
C. $\ker \sigma$ je kongruence $\mathbb{A}^*$, kde ve stejné ekvivalenční třídě leží slova stejné délky.
D. $\ker \tau$ má ekvivalenční třídy S_Ω a $T_\Omega \setminus S_\Omega$. Ekvivalence $\ker \tau$ je kongruence právě když množina $\Omega \neq \emptyset$ je konečná.

Buď A a B dvě množiny, a ať $f : A \to B$ je bijektivní zobrazení. Předpokládejme, že na A je definována operace četnosti $n \geq 0$. Pak můžeme na B definovat jediným způsobem operaci α tak, aby zobrazení f bylo s α slučitelné — pro $b_1, \dots, b_n \in B$ takové, že $b_1 = f(a_1), \dots, b_n = f(a_n)$, je totiž vztah $\alpha_B(b_1, \dots, b_n) = \alpha_B(f(a_1), \dots, f(a_n)) = f(\alpha_A(a_1, \dots, a_n))$ jednoznačnou definicí hodnoty $\alpha_B(b_1, \dots, b_n)$. Takto definovanou operaci α_B nazýváme operací *indukovanou* bijektivním *zobrazením* f.

Buď nyní dána algebra $A = A(\alpha_1, \dots, \alpha_k)$ a bijektivní zobrazení $f : A \to B$. Definujme algebru $B = B(\alpha_1, \dots, \alpha_k)$ tak, že operace $\alpha_1, \dots, \alpha_k$ na B jsou indukovány zobrazením f. Pak $f : A \to B$ je izomorfismus a o $B = B(\alpha_1, \dots, \alpha_k)$ mluvíme jako o *algebře indukované* f.

Je-li ρ ekvivalence na A, tak podmnožinu T množiny A nazýváme *transversálou* ρ, jestliže pro každé $a \in A$ existuje právě jedno $b \in T$ takové, že platí $a \rho b$. Jinými slovy, T je transversála právě když každá ekvivalenční třída ρ obsahuje přesně jeden prvek T. Z definice je tedy zřejmé, že zobrazení $b \mapsto [b]_\rho$ je bijekcí mezi T a A/ρ. V případě, že $A = A(\alpha_1, \dots, \alpha_k)$ je algebra a ρ je kongruence A, tak zobrazení inverzní k $b \mapsto [b]_\rho$ bijektivně zobrazuje A/ρ na T, a indukuje tak na T operace $\alpha_1, \dots, \alpha_k$. Je-li například $\alpha = \alpha_1$ četnosti n a $b_1, \dots, b_n$ jsou prvky T, tak $\alpha_T(b_1, \dots, b_n)$ je definováno jako ten (jednoznačně určený) prvek $b \in T$, pro který platí $(b, \alpha_A(b_1, \dots, b_n)) \in \rho$. Algebru $T = T(\alpha_1, \dots, \alpha_n)$ nazveme algebrou *indukovanou transversálou* T kongruence ρ.

Na závěr této kapitoly zmíníme ještě několik jednoduchých vlastností monoidů.

Prvek a monoidu $S = S(\cdot, \mathbf{1})$ se nazývá *zprava invertibilní*, jestliže existuje takové $b \in S$, že platí $a \cdot b = \mathbf{1}$. Podobně definujeme prvek *zleva invertibilní*.

2.15 Lemma. *Ať pro prvky a, b, c monoidu $S(\cdot, \mathbf{1})$ platí $a \cdot b = \mathbf{1} = c \cdot a$. Potom je b rovno c.*

Důkaz. $b = \mathbf{1} \cdot b = (c \cdot a) \cdot b = c \cdot (a \cdot b) = c \cdot \mathbf{1} = c$. □

Invertibilním nazveme každý prvek, který je současně invertibilní zleva i zprava. Podle 2.15 pro každý invertibilní prvek $a \in S$ existuje jednoznačně určené $b \in S$, jež splňuje $a \cdot b = \mathbf{1} = b \cdot a$. Prvku b se říká prvek *inverzní* (vzhledem k a).

2.16 Lemma. *Uvažme monoid $S = S(\cdot, \mathbf{1})$.*

(i) *Ať $b \in S$ je inverzní prvek invertibilního prvku $a \in S$. Potom b je rovněž invertibilní a a je jeho inverzní prvek.*
(ii) *Ať $a \in S$ je inverzní vzhledem k $b \in S$ a $c \in S$ je inverzní vzhledem k $d \in S$. Potom $a \cdot c$ je inverzní prvek prvku $d \cdot b$.*

Důkaz. (i) je zřejmé a (ii) plyne z $(ac) \cdot (db) = a \cdot (cd) \cdot b = a \cdot b = \mathbf{1} = d \cdot c = d \cdot (ba) \cdot c = (db) \cdot (ac)$. □

2.17 Důsledek. *Invertibilní prvky monoidu $S(\cdot, \mathbf{1})$ tvoří podmonoid.*