3. Věty o homomorfismech a kongruencích

1. Uvažme abecedu $\mathbb{A}$ a monoid slov $\mathbb{A}^*$. Buď $M = M(\cdot, \mathbf{1})$ nějaký další monoid. Dokažte, že každé zobrazení $g : \mathbb{A} \to M$ lze jednoznačně rozšířit na homomorfismus $\mathbb{A}^* \to M$ (tj. že existuje právě jeden homomorfismus $f : \mathbb{A}^* \to M$ takový, že $f(a) = g(a)$ pro všechna $a \in \mathbb{A}$). Uvědomte si, že cvičení 2.7 popisuje specielní případ $M = \mathbb{A}^*$.

2. Ať $f : A \to B$ je homomorfismus algeber, ať $X \subseteq A$ generuje podalgebru A_1 algebry A a ať $f(X)$ generuje podalgebru B_1 algebry B. Dokažte, že B_1 je rovno $f(A_1)$.

3. Ať $f : A \to B$ je homomorfismus a ať X generuje A. Pomocí předchozího cvičení dokažte, že f je surjektivní právě když $f(X)$ generuje B.

4. Říkáme, že algebru A lze generovat k prvky, $k \in \mathbb{N}_0$, jestliže existuje konečná množina X o k prvcích, jež generuje A. Může být neprázdná algebra generována 0 prvky (tj. prázdnou množinou)?

5. Nechť $S = S(\cdot)$ je pologrupa a ať X je podmnožina S. Dokažte, že podpologrupa A generovaná množinou X se shoduje s množinou všech prvků S, které lze vyjádřit jako $x_1 \dots x_k$, kde $x_i \in X$ pro $1 \le i \le k$ a $k \in \mathbb{N}$.

6. Uvažte algebry (a) $\mathbb{N}(+)$, (b) $\mathbb{N}_0(+)$, (c) $\mathbb{N}_0(+, 0)$, (d) $\mathbb{N}(\cdot, 1)$, (e) $\mathbb{Z}(+, 0)$, (f) $\mathbb{Z}(+, -, 0)$, (g) $\mathbb{Z}(+, \cdot, -, 0, 1)$. U každé určete minimální k, pro které je daná algebra generována k prvky.

7. Množina X generátorů algebry A se nazývá minimální, jestliže $X \setminus \{x\}$ negeneruje A pro všechna $x \in X$. U všech algeber v předchozí úloze ověřte, že obsahují alespoň jednu minimální množinu generátorů. Určete, které z nich obsahují právě jednu minimální množinu generátorů. (Existují ovšem i algebry, které nemají žádnou minimální množinu generátorů. Takové algebry nemohou samozřejmě být konečné. Nejjednodušším příkladem se mi zdá být $\mathbb{Q}(+, -, 0)$, kde $\mathbb{Q}$ značí racionální čísla. Lze ukázat, že $\mathbb{Q}(+, -, 0)$ nemá minimální množinu generátorů. Neznám žádný důkaz tohoto tvrzení, který nepoužívá alespoň trochu z teorie Abelových grup. Bylo by zajímavé takový důkaz nalézt.)

8. Buď α a β nějaké permutace množiny Ω. Dokažte, že $\{f \in T_\Omega;\ \alpha \circ f \circ \alpha^{-1} = \beta \circ f \circ \beta^{-1}\}$ tvoří podmonoid transformačního monoidu T_Ω.

9. Buď ρ relace na $\mathbb{Q}$ (nebo na $\mathbb{R}$) definovaná vztahem $a \rho b \Leftrightarrow a - b \in \mathbb{Z}$. Dokažte, že ρ je kongruence $\mathbb{Q}(+, -, 0)$ (nebo $\mathbb{R}(+, -, 0)$).

10. Dokažte, že $U_\mathbb{R} = \{a \in \mathbb{C};\ |a| = 1\}$ je podalgebra $\mathbb{C}(\cdot, {}^{-1}, 1)$ (kde $\mathbb{C}$ označuje komplexní čísla). Dokažte, že $U_\mathbb{Q} = \{\sin r2\pi + i \cos r2\pi;\ r \in \mathbb{Q}\}$ je podalgebra $U_\mathbb{R}(\cdot, {}^{-1}, 1)$.

11. (pokračování předchozích dvou cvičení) Dokažte, že $\mathbb{Q}/\rho\ (+, -, 0)$ je izomorfní $U_\mathbb{Q}(\cdot, {}^{-1}, 1)$, a že $\mathbb{R}/\rho\ (+, -, 0)$ je izomorfní $U_\mathbb{R}(\cdot, {}^{-1}, 1)$.

Odpovědi

1. Je-li f homomorfimus, tak nutně musí platit $f(a_1 \dots a_n) = f(a_1) \dots f(a_n) = g(a_1) \dots g(a_n)$ a $f(\lambda) = \mathbf{1}$. Takto definované zobrazení $f : \mathbb{A}^* \to M$ vskutku homomorfismus je, neboť pro libovolná slova $v = a_1 \dots a_n$ a $w = b_1 \dots b_m$ máme $f(vw) = g(a_1) \dots g(a_n) g(b_1) \dots g(b_m) = f(v) f(w)$.

2. $f(A_1)$ je podalgebra B, která obsahuje $f(X)$, a tím i B_1. Z $B_1 \subseteq f(A_1)$ plyne $B_1 \subseteq \operatorname{Im} f$, a tedy $f f^{-1}(B_1) = B_1$. Ovšem $f^{-1}(B_1)$ obsahuje X, a tím i A_1, a $f^{-1}(B_1) \supseteq A_1$ dává $B_1 = f f^{-1}(B_1) \supseteq f(A_1)$.

3. Protože X generuje A, tak $f(X)$ generuje $f(A)$.

4. Ano, může, a to v případě, že jsou v ní definovány nulární operace. Podalgebra generovaná prázdnou množinou se totiž shoduje s podalgebrou generovanou množinou všech konstant určených zadanými nulárními operacemi.

5. Označme B množinu všech prvků, jež lze vyjádřit jako slova nad X. Zjevně platí $B \subseteq A$. Na druhou stranu je B podpologrupa, která obsahuje X, takže platí i $B \supseteq A$.

6. (a) 1, (b) 2, (c) 1, (d) je třeba nekonečně mnoho generátorů — například všechna prvočísla, (e) 2, (f) 1, (g) 0.

7. Jednoznačně určené minimální množiny generátorů: (a) $\{1\}$, (b) $\{0, 1\}$, (c) $\{1\}$, (d) $\{p;\ p \text{ prvočíslo }\}$, (g) $\emptyset$. V případě (e) například $\{-1, 1\}$ nebo $\{-1, 4\}$ nebo $\{-5, 4\}$ a podobně. V případě (f) například $\{-1\}$ nebo $\{1\}$ nebo $\{5, 7\}$ a podobně.

8. Přímý důkaz je samozřejmě možný, elegantnější však je využít 3.2 a skutečnosti, že pro každou permutaci γ je zobrazení $f \mapsto \gamma \circ f \circ \gamma^{-1}$ automorfismus transformačního monoidu T_Ω.

9. $a - b \in \mathbb{Z}$ a $b - c \in \mathbb{Z}$ dává $a - c \in \mathbb{Z}$, takže ρ je zjevně ekvivalence. Je-li $a \rho b$ a $c \rho d$, je $(a + c) - (b + d)$ celé číslo, takže ρ je slučitelná s $+$. Slučitelnost s unárním $-$ je očividná.

10. Prvá část plyne z toho, že $|a||b| = |ab|$ pro všechna $a, b \in \mathbb{C}$. Pro důkaz druhé části je třeba využít skutečnosti, že $(\sin r2\pi + i \cos r2\pi) \cdot (\sin s2\pi + i \cos s2\pi)$ se rovná $(\sin(r + s)2\pi + i \cos(r + s)2\pi$.

11. Zobrazení $r \mapsto \sin r2\pi + i \cos r2\pi$ je surjektivní homomorfismus z $\mathbb{R}$ na $U_{\mathbb{R}}$, a z $\mathbb{Q}$ na $U_{\mathbb{Q}}$. Jeho jádrem je kongruence ρ, takže požadované izomorfismy plynou z 1. věty o izomorfismu.