Matematický ústav Slezské univerzity v Opavě
Učební texty k přednášce ALGEBRA I, zimní semestr 2000/2001
Michal Marvan

2. Homomorfismy

V souvislosti se strukturami se v moderní matematice studují i zobrazení, která strukturu tím či oním způsobem zachovávají. V algebře zachovávají algebraické operace a nazývají se homomorfismy. Invertibilní homomorfismy se nazývají izomorfismy.

1. Homomorfismy

Definice. Buďte $(A, *)$, $(B, \dagger)$ dvě pologrupy. Zobrazení $f : A \to B$ se nazývá *homomorfismus pologrup*, jestliže pro každé dva prvky $a_1, a_2 \in A$ platí

$$f(a_1 * a_2) = f(a_1) \dagger f(a_2). \tag{1}$$

Značí se $f : (A, *) \to (B, \dagger)$.

Buďte $(A, *, e_A)$, $(B, \dagger, e_B)$ dva monoidy. Zobrazení $f : A \to B$ se nazývá *homomorfismus monoidů*, jestliže je homomorfismem pologrup $(A, *) \to (B, \dagger)$ a navíc platí

$$f(e_A) = e_B. \tag{2}$$

Značí se $f : (A, *, e_A) \to (B, \dagger, e_B)$.

Buďte $(A, *, e_A, {}^{-1})$, $(B, \dagger, e_B, {}^{-1})$ dvě grupy. Zobrazení $f : A \to B$ se nazývá *homomorfismus grup*, jestliže je homomorfismem monoidů $(A, *, e_A) \to (B, \dagger, e_B)$ a navíc pro každé $a \in A$ platí

$$f(a^{-1}) = \bigl(f(a)\bigr)^{-1}. \tag{3}$$

Značí se $f : (A, *, e_A, {}^{-1}) \to (B, \dagger, e_B, {}^{-1})$.

Podmínka (1) znamená: je jedno, jestli nejdříve násobíme a potom zobrazujeme nebo nejdříve zobrazujeme a potom násobíme. Podmínka (2) znamená: neutrální prvek se zobrazí na neutrální prvek. Podmínka (3) znamená: je jedno, jestli nejdříve invertujeme a potom zobrazujeme nebo nejdříve zobrazujeme a potom invertujeme.

Příklad. Na množině $A = \{\heartsuit, \spadesuit, \diamondsuit, \clubsuit\}$ resp. $B = \{\square, \blacksquare\}$ máme zadán součin „$\odot$“ resp. „$\dagger$“ tabulkou

$\odot$	$\heartsuit$	$\spadesuit$	$\diamondsuit$	$\clubsuit$
$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$
$\spadesuit$	$\heartsuit$	$\spadesuit$	$\heartsuit$	$\spadesuit$
$\diamondsuit$	$\heartsuit$	$\heartsuit$	$\diamondsuit$	$\diamondsuit$
$\clubsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$	$\clubsuit$

resp.

$\dagger$	$\square$	$\blacksquare$
$\square$	$\square$	$\square$
$\blacksquare$	$\square$	$\blacksquare$

Zobrazení $f : A \to B$ zadané předpisem $f : \heartsuit \mapsto \square$, $\spadesuit \mapsto \blacksquare$, $\diamondsuit \mapsto \square$, $\clubsuit \mapsto \blacksquare$ je homomorfismus pologrup.

Podmínku $f(a_1 \odot a_2) = f(a_1) \dagger f(a_2)$ lze bezprostředně ověřit pro všech 16 dvojic $(a_1, a_2) \in A \times A$. Jinak: Zobrazení f představuje přiřazení jedné z „barev“ $\square$, $\blacksquare$ symbolům $\heartsuit$, $\spadesuit$, $\diamondsuit$, $\clubsuit$. Podmínku (1) lze vyjádřit i rčením: „*barva součinu je součin barev*.“ A to se snadno ověří porovnáním tabulek operací „$\odot$“ a „$\dagger$“.

Cvičení. Ukažte, že zobrazení $f_2 : \mathbf{Z} \to \mathbf{Z}$, zadané předpisem $n \mapsto 2n$, je homomorfismus grup $(\mathbf{Z}, +, 0, -) \to (\mathbf{Z}, +, 0, -)$.

Příklad. Uvažujme o monoidu slov $(S_A, \cdot, \omega)$ nad abecedou A. Nechť zobrazení $f : S_A \to S_A$ slovu $\alpha \in S_A$ přiřazuje jeho délku $\ell(\alpha) \in \mathbf{N}$. Například $f($🔨○□○$) = 4$. Pak je f homomorfismus monoidů $(S_A, \cdot, \omega) \to (\mathbf{N}, +, 0)$.

Tvrzení. *Buďte $f : A \to B$ a $g : B \to C$ homomorfismy pologrup (monoidů, grup). Pak jejich složení $g \circ f : A \to C$ je homomorfismus pologrup (monoidů, grup).*

Důkaz. Pro pologrupy, řekněme $(A, *)$, $(B, \dagger)$, $(C, \ddagger)$: Protože f je homomorfismus, pro každé dva prvky $a_1, a_2 \in A$ platí $f(a_1 * a_2) = f(a_1) \dagger f(a_2)$. Protože g je homomorfismus, platí následovně $g(f(a_1) \dagger f(a_2)) = g(f(a_1)) \ddagger g(f(a_2))$. Celkově

$$\begin{aligned}(g \circ f)(a_1 * a_2) &= g(f(a_1 * a_2) = g(f(a_1) \dagger f(a_2)) = g(f(a_1)) \ddagger g(f(a_2)) \\ &= (g \circ f)(a_1) \ddagger (g \circ f)(a_2),\end{aligned}$$

což se mělo ukázat. Pro monoidy resp. grupy: cvičení.

Všimněte si, že asociativita operací ani další axiomy nehrají žádnou roli v definici homomorfismu. Mohou však být podstatné ve větách o homomorfismech, jako například v následujícím tvrzení.

Tvrzení. *Buďte $(A, *, e_A, {}^{-1})$, $(B, \dagger, e_B, {}^{-1})$ dvě grupy. Buď $f : A \to B$ homomorfismus pologrup: $(A, *) \to (B, \dagger)$. Pak f je homomorfismus grup: $(A, *, e_A, {}^{-1}) \to (B, \dagger, e_B, {}^{-1})$.*

Vidíme, že definici homomorfismu grup bychom mohli formulovat i v podstatně redukované podobě: *Homomorfismus grup je homomorfismus příslušných pologrup.* Upřednostnili jsme obecné schéma, podle něhož je homomorfismus zobrazení zachovávající všechny operace.

Důkaz. (a) Nejdříve ukážeme, že $f(e_A) = e_B$. Vyjdeme z rovnosti

$$f(e_A) = f(e_A * e_A) = f(e_A) \dagger f(e_A).$$

Protože B je grupa, existuje prvek $f(e_A)^{-1}$ inverzní k prvku $f(e_A)$. Vynásobíme-li jím obě strany, obdržíme

$$e_B = f(e_A) \dagger f(e_A)^{-1} = f(e_A) \dagger f(e_A) \dagger f(e_A)^{-1} = f(e_A),$$

což se mělo ukázat.

(b) Dále ukážeme, že $f(a^{-1}) = f(a)^{-1}$ pro každé $a \in A$. Máme ovšem

$$f(a) \dagger f(a^{-1}) = f(a * a^{-1}) = f(e_A) = e_B.$$

[používáme již dokázaný fakt (a)]. Tím je dokázáno, že prvek $f(a^{-1})$ je inverzní k prvku $f(a)$.

Cvičení. Ukažte, že analogické tvrzení neplatí pro monoidy. To jest, ukažte, že existují monoidy A, B a homomorfismus pologrup $f : A \to B$, který není homomorfismem monoidů.

Návod: $A = B = \{1, 2\}$ s operací $a * b = \min\{a, b\}$ a neutrálním prvkem 1.

Cvičení. 1. Uvažujme o monoidu slov $(S_A, \cdot, \omega)$ nad abecedou A. Buď $(M, *, 1)$ libovolný monoid, buď $f : A \to M$ libovolné zobrazení. Ukažte, že potom existuje jediný homomorfismus monoidů $F : (S_A, \cdot, \omega) \to (M, *, 1)$ takový, že $F(a) = f(a)$ pro každé $a \in A$.
Návod: Položte $F(a_{i_1} \dots a_{i_n}) = f(a_{i_1}) \dots f(a_{i_n})$.

2. Najděte všechna zobrazení $f : A \to S_A$ taková, že homomorfismus $F : (S_A, \cdot, \omega) \to (S_A, \cdot, \omega)$ je izomorfismus.

Cvičení. Buď $f : A \to B$ homomorfismus pologrup (monoidů, grup). Označme

$$\operatorname{Im} f = \{ f(a) \mid a \in A \}.$$

Pak je $\operatorname{Im} f$ podpologrupa (podmonoid, podgrupa) v B. Dokažte.

2. Izomorfismy

Definice. *Izomorfismus* pologrup (monoidů, grup) A, B je homomorfismus $f : A \to B$ pologrup (monoidů, grup), který je bijektivní.

Izomorfismy struktur jsou obecně definovány jako homomorfismy, k nimž existují homomorfismy inverzní. V případě pologrup, monoidů, grup (a ostatních algebraických struktur) nemusíme existenci inverzního homomorfismu explicitně vyžadovat, protože platí následující tvrzení:

Tvrzení. *Buď $f : A \to B$ izomorfismus pologrup (monoidů, grup). Pak je $f^{-1} : B \to A$ opět izomorfismus pologrup (monoidů, grup).*

Důkaz. Pro pologrupy $(A, *)$, $(B, \dagger)$: Má se ukázat, že $f^{-1}(b_1 \dagger b_2) = f^{-1}(b_1) * f^{-1}(b_2)$. Protože f je (jako každá bijekce) injektivní, stačí ukázat rovnost obrazů, tj.

$$f\big(f^{-1}(b_1 \dagger b_2)\big) = f\big(f^{-1}(b_1) * f^{-1}(b_2)\big).$$

Zatímco na levé straně máme ihned $b_1 \dagger b_2$, na pravé straně dostáváme $f\big(f^{-1}(b_1) * f^{-1}(b_2)\big) = f\big(f^{-1}(b_1)\big) \dagger f\big(f^{-1}(b_2)\big) = b_1 \dagger b_2$, tedy totéž, čímž je důkaz hotov.

Pro monoidy resp. grupy: cvičení.

Příklady. (1) Identické zobrazení je vždy izomorfismus.

(2) Označme $\mathbf{R}_{>0} := \{ r \in \mathbf{R} \mid r > 0 \}$. Pak $(\mathbf{R}_{>0}, \cdot, 1, ^{-1})$ je grupa (cvičení). Zobrazení $\exp : \mathbf{R} \to \mathbf{R}_{>0}$, zadané předpisem $x \mapsto e^x$, je homomorfismus grup $(\mathbf{R}, +, 0, -) \to (\mathbf{R}_{>0}, \cdot, 1, ^{-1})$, protože pro libovolná dvě čísla $x, y \in \mathbf{R}$ platí $\exp(x + y) = e^{x+y} = e^x e^y = (\exp x) \cdot (\exp y)$.

Tento homomorfismus je bijektivní, a tedy izomorfismus:

$$\exp : (\mathbf{R}, +, 0, -) \to (\mathbf{R}_{>0}, \cdot, 1, ^{-1}).$$

Inverzní izomorfismus je logaritmus

$$\ln : (\mathbf{R}_{>0}, \cdot, 1, ^{-1}) \to (\mathbf{R}, +, 0, -).$$

Původně byly logaritmy vynalezeny jako prostředek k násobení (kladných) reálných čísel: násobení v grupě $(\mathbf{R}_{>0}, \cdot, 1, ^{-1})$ bylo převedeno na sčítání v izomorfní grupě $(\mathbf{R}, +, 0, -)$. Hodnoty funkcí ln a exp ovšem bylo nutno vyhledávat v tabulkách.

Sčítat lze i graficky (nanášením úseček na společnou přímku). Spojením obou principů vzniklo logaritmické pravítko, užitečný nástroj, který vytlačila teprve digitální éra.

Definice. Řekneme, že dvě pologrupy (monoidy, grupy) A, B jsou izomorfní, jestliže existuje izomorfismus $A \to B$. Zapisujeme $A \cong B$.

Tvrzení. *Pro libovolné tři pologrupy (monoidy, grupy) A, B, C platí*
(i) $A \cong A$ *(reflexivita);*
(ii) *Jestliže $A \cong B$, pak $B \cong A$ (symetrie);*
(iii) *Jestliže $A \cong B$, $B \cong C$, pak $A \cong C$ (tranzitivita).*

Důkaz. (i) Identické zobrazení id_A je izomorfismus. (ii) Zobrazení inverzní k izomorfismu je izomorfismus. (iii) Složení homomorfismů je homomorfismus, složení bijekcí je bijekce, a proto složení izomorfismů je izomorfismus.

Můžeme také říci, že na libovolné množině algebraických struktur je izomorfismus relací ekvivalence.

Příklad. $(\mathbf{R}_{>0}, \cdot, 1, ^{-1}) \cong (\mathbf{R}, +, 0, -)$. Izomorfismů $(\mathbf{R}, +, 0, -) \to (\mathbf{R}_{>0}, \cdot, 1, ^{-1})$ existuje velmi mnoho, např. $x \mapsto a^x$ pro libovolné $a \in \mathbf{R}_{>0}$, $a \neq 1$. Ověřte.

Problém k řešení. Není pravda, že $(\mathbf{Q}_{>0}, \cdot, 1, ^{-1}) \cong (\mathbf{Q}, +, 0, -)$, kde $\mathbf{Q}$ je množina všech racionálních čísel a $\mathbf{Q}_{>0}$ je množina všech kladných racionálních čísel. Dokažte.

3. Faktorové algebry

Buď $(A, \cdot)$ pologrupa. Buď dán rozklad $\{ A_i \}_{i \in I}$ na množině A. Množinu všech tříd rozkladu označíme $\tilde{A}$; nazývá se *faktorová množina*:

$$\tilde{A} = \{ [a] \mid a \in A \}$$

(připomeňme, že $[a]$ označuje třídu A_i obashující prvek a; ta je podle definice rozkladu jediná). Nechť platí *podmínka kompatibility*

$$\text{jestliže } [a'] = [a],\ [b'] = [b],\ \text{pak } [a' \cdot b'] = [a \cdot b]. \tag{$*$}$$

Platí-li implikace $(*)$, pak třída $[a \cdot b]$ závisí jen a jen na třídách $[a]$, $[b]$ a ne na konkrétním výběru prvků a, b, které v nich leží („reprezentantů“). Můžeme ji proto považovat za výsledek násobení tříd a označit $[a] \dagger [b]$. Pravidlem

$$[a] \dagger [b] := [a \cdot b]\,. \tag{$**$}$$

je na množině $\tilde{A}$ zavedena binární operace „†“.

Příklad. Na množině $A = \{ \heartsuit, \spadesuit, \diamondsuit, \clubsuit \}$ zaveďme rozklad na dvě třídy: $A_1 = \{ \heartsuit, \diamondsuit \}$ a $A_2 = \{ \spadesuit, \clubsuit \}$:

A_1	A_2
$\heartsuit$	$\spadesuit$
$\diamondsuit$	$\clubsuit$

Máme $[\heartsuit] = A_1$, $[\spadesuit] = A_2$, $[\diamondsuit] = A_1$, $[\clubsuit] = A_2$. Množina $\tilde{A}$ je dvouprvková množina $\{ A_1, A_2 \}$.

Již dříve jsme zavedli binární operaci „$\odot$“ tabulkou

$\odot$	$\heartsuit$	$\spadesuit$	$\diamondsuit$	$\clubsuit$
$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$	$\heartsuit$
$\spadesuit$	$\heartsuit$	$\spadesuit$	$\heartsuit$	$\spadesuit$
$\diamondsuit$	$\heartsuit$	$\heartsuit$	$\diamondsuit$	$\diamondsuit$
$\clubsuit$	$\heartsuit$	$\spadesuit$	$\diamondsuit$	$\clubsuit$

Z tabulky je patrno, že platí implikace $(*)$, a proto je možné zavést násobení „$\dagger$“ tříd podle návodu $(**)$. Faktorová algebra bude mít dva prvky, $\{\heartsuit, \diamondsuit\}$ a $\{\spadesuit, \clubsuit\}$ a její binární operace bude zadána tabulkou

$\dagger$	$\{\heartsuit, \diamondsuit\}$	$\{\spadesuit, \clubsuit\}$
$\{\heartsuit, \diamondsuit\}$	$\{\heartsuit, \diamondsuit\}$	$\{\heartsuit, \diamondsuit\}$
$\{\spadesuit, \clubsuit\}$	$\{\heartsuit, \diamondsuit\}$	$\{\spadesuit, \clubsuit\}$

(Všimněte si, že označíme-li naše dvě třídy symboly $\square$, $\blacksquare$, obdržíme přesně algebru z příkladu na první straně.)

Tvrzení. *Je-li A pologrupa (monoid, grupa) splňující podmínku $(*)$, pak i příslušná faktorová algebra $\tilde{A}$ je pologrupa (monoid, grupa).*

Důkaz. Buď $(A, \cdot)$ pologrupa. Ověřme asociativní zákon pro násobení tříd: $[a] \dagger ([b] \dagger [c]) = [a] \dagger [b \cdot c] = [a \cdot (b \cdot c)] = [(a \cdot b) \cdot c] = [a \cdot b] \dagger [c] = ([a] \dagger [b]) \dagger [c]$.

Buď $(A, \cdot, e)$ monoid. Ověřme, že třída $[e]$ je neutrální prvek v pologrupě $\tilde{A}$: $[a] \dagger [e] = [a \cdot e] = [a]$, podobně $[e] \dagger [a] = [a]$.

Buď $(A, \cdot, e, ^{-1})$ grupa. Ověřme, že třída $[a^{-1}]$ je inverzní prvek k prvku $[a]$ v monoidu $\tilde{A}$: $[a] \dagger [a^{-1}] = [a \cdot a^{-1}] = [e]$, podobně $[a^{-1}] \dagger [a] = [e]$.

Poznamenejme, že z jednoznačnosti inverzních prvků v monoidu pak plyne, že třída $[a^{-1}]$ je jednoznačně určena třídou $[a]$. Je proto korektní ji označovat $[a]^{-1}$.

Cvičení. Buď $\tilde{A}$ faktorová algebra pologrupy (monoidu, grupy) A. Buď $p : A \to \tilde{A}$ zobrazení $a \mapsto [a]$. Ukažte, že p je homomorfismus pologrup (monoidů, grup).

4. Zbytkové třídy

Pro každé přirozené číslo $m > 1$ zkonstruujeme faktorovou grupu $\mathbf{Z}_m$ aditivní grupy $\mathbf{Z}$. Grupa $\mathbf{Z}_m$ bude mít m prvků.

Zaveďme podmnožiny $[i]_m \subset \mathbf{Z}$:

$$
\begin{aligned}
[0]_m &= \{km \mid k \in \mathbf{Z}\} = \{\dots,\ -2m,\ -m,\ 0,\ m,\ 2m, \dots\}, \\
[1]_m &= \{1 + km \mid k \in \mathbf{Z}\} = \{\dots,\ 1-2m,\ 1-m,\ 1,\ 1+m,\ 1+2m, \dots\}, \\
[2]_m &= \{2 + km \mid k \in \mathbf{Z}\} = \{\dots,\ 2-2m,\ 2-m,\ 2,\ 2+m,\ 2+2m, \dots\}, \\
&\ \vdots \\
[i]_m &= \{i + km \mid k \in \mathbf{Z}\} = \{\dots,\ i-2m,\ i-m,\ i,\ i+m,\ i+2m, \dots\}. \\
&\ \vdots
\end{aligned}
$$

Zřejmě $j \in [i]_m$ právě tehdy, když existuje číslo $k \in \mathbf{Z}$ takové, že $j = i + km$.

Všimněme si, že pro $i = 0, \ldots, m-1$ třída $[i]_m$ obsahuje právě ta celá čísla a, pro něž i je zbytkem při celočíselném dělení čísla a přirozeným číslem m, říká se jim proto *zbytkové třídy*. Ale všechny možné zbytky při dělení číslem m jsou právě $0, 1, \ldots, m-1$, takže každé číslo $a \in \mathbf{Z}$ leží v právě jedné ze tříd $[0]_m, [1]_m, \ldots, [m-1]_m$. Tudíž, třídy $[0]_m, [1]_m, \ldots, [m-1]_m$ tvoří rozklad množiny $\mathbf{Z}$.

Příslušnou faktorovou množinu označujeme

$$\mathbf{Z}_m = \{ [0]_m, [1]_m, \ldots, [m-1]_m \}.$$

Ověříme podmínku $(*)$. Předpokládejme, že $[a]_m = [a']_m$ a $[b]_m = [b']_m$. Pak $a' \in [a]_m$ a $b' \in [b]_m$, a tedy $a' = a + km$, $b' = b + lm$ pro vhodná $k, l \in \mathbf{Z}$, načež $a' + b' = a + km + b + lm = a + b + (k+l)m \in [a+b]_m$. Tudíž, $[a+b]_m = [a'+b']_m$.

Na m-prvkové množině $\mathbf{Z}_m$ potom vzniká binární operace $(**)$, kterou pro jednoduchost označíme zase $+$, zadaná předpisem

$$[a]_m + [b]_m = [a+b]_m.$$

Faktorová grupa $(\mathbf{Z}_m, +, [0]_m, -)$ je komutativní *aditivní grupa zbytkových tříd modulo m*.

Na $\mathbf{Z}_m$ můžeme analogicky zavést i binární operaci násobení předpisem

$$[a]_m \cdot [b]_m = [a \cdot b]_m.$$

Podmínka $(*)$ se ověří podobně. Předpokládejme opět, že $[a]_m = [a']_m$ a $[b]_m = [b']_m$, tj. $a' = a + km$, $b' = b + lm$ pro vhodná $k, l \in \mathbf{Z}$, načež $a' \cdot b' = (a+km)(b+lm) = ab + (kb + la + klm)m \in [ab]_m$. Tudíž, $[a'b']_m = [ab]_m$.

Faktorový monoid $(\mathbf{Z}_m, \cdot, [1]_m)$ je komutativní *multiplikativní monoid zbytkových tříd modulo m*.

Příklad. Nechť $m = 5$. Následující tabulka naznačuje rozložení množiny všech celých čísel do pěti tříd:

$[0]_5$		-5	0	5	
$[1]_5$		-4	1	6	
$[2]_5$	$\cdots$	-3	2	7	$\cdots$
$[3]_5$		-2	3	8	
$[4]_5$		-1	4	9	

Aditivní grupa $\mathbf{Z}_5$ resp. multiplikativní monoid $\mathbf{Z}_5$ mají tabulky

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

resp.

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(číslo i označuje třídu $[i]_5$).

Cvičení. Ukažte, že číslo $n^4 - 1$ je dělitelné pěti pro každé n nedělitelné pěti.

Návod: Číslo n je dělitelné pěti právě tehdy, když $[n]_5 = [0]_5$. Tudíž, pro n nedělitelné pěti je $[n]_5$ jedna ze tříd $[1]_5$, $[2]_5$, $[3]_5$, $[4]_5$. Spočtěte $[n^4 - 1]_5 = [n]_5 \cdot [n]_5 \cdot [n]_5 \cdot [n]_5 - [1]_5$ pro $n = 1, 2, 3, 4$.

5. Kongruence

Víme, že rozkladu na množině A odpovídá relace ekvivalence $\equiv$ definovaná předpisem: $x \equiv y$ právě tehdy, když $[x] = [y]$. Podmínku $(*)$ potom můžeme ekvivalentně zapsat ve tvaru

$$\text{jestliže } a' \equiv a,\ b' \equiv b,\ \text{pak } a' \cdot b' \equiv a \cdot b. \tag{$*'$}$$

Relace ekvivalence splňující podmínku $(*')$ se nazývá *kongruence*.

Cvičení. Ukažte, že rozkladu množiny $\mathbf{Z}$ na zbytkové třídy $[\,\cdot\,]_m$ odpovídá kongruence $\equiv_m$ definovaná předpisem $a \equiv_m b \Leftrightarrow m \mid a - b$.

Cvičení. Buď $h : (A, \cdot) \to (B, *)$ homomorfismus pologrup (monoidů, grup).

(1) Ukažte, že relace $\sim$ zadaná předpisem

$$x \sim y \quad \Leftrightarrow \quad h(x) = h(y)$$

je kongruence na pologrupě (monoidu, grupě) A.

(2) Ukažte, že faktorová algebra $\tilde{A}$ podle kongruence $\sim$ je izomorfní podalgebře $\operatorname{Im} h$.
Návod: Izomorfismus $\tilde{A} \leftrightarrow \operatorname{Im} h$ zadejte předpisem $[a] \leftrightarrow f(a)$.