3.2. Grupoidy

V této kapitole se budeme zabývat algebrami s jediným nosičem a jedin ou základní /výchozí/ binární operací. Pokud má tato operace vlastnost JE / viz definice 3.1/, pak algebra má navíc odvozenou nulární operaci jednotkov ého prvku. Má-li operace také vlastnost IN /viz definice 3.1/, pak má algeb ra navíc také odvozenou unární operaci inverzního prvku.

Definice 3.2.1:

Nejdůležitějšími algebrami s jedinou výchozí binární operací jsou:

- ***Grupoid***: algebra s jedinou univerzální operací
  platí axiómy: UN
- ***Pologrupa***: asociativní grupoid
  platí axiómy: UN,AS
- ***Monoid***: pologrupa s jednotkovým prvkem
  platí axiómy: UN,AS,JE
- ***Grupa***: monoid, jehož každý prvek je invertovatelný
  platí axiómy: UN,AS,JE,IN
- ***Abelova grupa***: komutativní grupa
  platí axiómy: UN,AS,JE,IN,KO

Příklady 3.2.1:

Označení:

- Nosiče:
  A ... abeceda /konečná množina symbolů/
  A^+ ... množina všech neprázdných slov nad abecedou A
  A^* ... množina všech slov nad abecedou A
  N ... množina přirozených čísel: {1,2,...}
  Z ... množina nezáporných celých čísel: {0,1,2,...}
  Z_m ... množina zbytkových tříd modulo m: {0,1,2,...,m-1}
  I ... množina celých čísel: {...,-2,-1,0,1,2,...}
  R ... množina reálných čísel
- Operace:
  . ... binární operace zřetězení /katenace/
  e ... nulární operace jednotk. prvku vzhledem k operaci zřetězení
  + ... binární operace číselného součtu
  0 ... nulární operace jednotk. prvku vzhledem k operaci sčítání
  -() .. unární operace inverzního prvku vzhledem k operaci sčítání
  * ... binární operace číselného součinu
  1 ... nulární operace jednotk. prvku vzhledem k operaci násobení
  $()^{-1}$.. unární operace inverzního prvku vzhledem k operaci násobení
- Příklady:
  1. $\langle A^+;. \rangle$ ..... pologrupa neprázdných slov nad abecedou A
  2. $\langle A^*;.,e \rangle$ ..... /volný/ monoid generovaný množinou symbolů A
  3. <N;+> ..... komutativní pologrupa
  4. <Z;+,0> ..... komutativni monoid
  5. <N;*,1> ..... komutativní monoid
  6. <I;+,0,-()> ... Abelova grupa
  7. <I;*,1> ..... komutativní monoid
  8. <R;+,0,-()> ... Abelova grupa
  9. $\langle R;*,1,()^{-1} \rangle$ .. Abelova grupa
  10. <R;(x+y)/2> .. komutativní grupoid

- Další příklady:

11. ***Transformační pologrupa*** na množině A: množina všech zobrazení množiny A do sebe spolu s operací skládání zobrazení.
12. ***Transformační monoid*** na množině A: transformační pologrupa zahrnující i identické zobrazení, které je jednotkovým prvkem monoidu.
13. ***Transformační grupa*** na množině A: množina všech bijekcí množiny A na sebe. Identická bijekce je jednotkovým prvkem. Ke každé bijekci existuje inverzní zobrazení, které je opět bijekcí.

Ve zbytku této kapitoly se budeme zabývat pouze grupami. Grupu $\langle G;.,()^{-1},1\rangle$ s nosičem G, základní binární grupovou operací . /tzv. grupové násobení - budeme užívat multiplikativní terminologii i notaci/, odvozenou unární operací $()^{-1}$ /operace inverzního prvku/ a odvozenou nulární operací 1 /jednotkový prvek/, budeme stručněji označovat pouze $\langle G;.\rangle$, nebo dokonce pouze G. Předpokládáme, že pro grupové operace platí axiómy UN,AS,JE,IN. Na teorii grup můžeme pohlížet jako na formální teorii zahrnující predikátovou logiku, ve které axiómy UN,AS,JE,IN jsou specifickými axiómy specifikujícími primitivní binární funkční symbol ".". V zájmu srozumitelnějšího výkladu však pojmeme teorii grup jako neformalizovanou axiomatickou teorii.

Věta 3.2.1:

Nechť $\langle G;.\rangle$ je grupa a $a,b,c\in G$. Potom platí:

1. $a.b=a.c \Rightarrow b=c$ /***pravidlo o krácení zleva***/.
   $b.a=c.a \Rightarrow b=c$ /***pravidlo o krácení zprava***/.
2. Rovnice $a.x=b$ má jediné řešení $x=a^{-1}.b$.
   Rovnice $y.a=b$ má jediné řešení $y=b.a^{-1}$.

Důkaz:

1.

Důkazem pravidla o krácení zleva je následující řetěz implikací /pravidlo o krácení zprava se dokáže zcela obdobně/:

(1)	$a.b=a.c$	předpoklad
(2)	$a^{-1}.(a.b)=a^{-1}.(a.c)$	z (1) podle UN
(3)	$(a^{-1}.a).b=(a^{-1}.a).c$	z (2) podle AS
(4)	$1.b=1.c$	z (1) podle IN
(5)	$b=c$	z (1) podle JE

2. Skutečnost, že $x=a^{-1}.b$ je řešením rovnice $a.x=b$ ověříme dosazením. Skutečnost, že se jedná o jediné řešením dokážeme sporem.

Poznámka 3.2.1:

Věta 3.2.1 platí obráceně v následujícím smyslu: každá pologrupa, ve které platí pravidlo o krácení /nebo ve které rovnice $a.x=b$, $y.a=b$ jsou řešitelné/, je grupou.

Věta 3.2.2:

Nechť $\langle G;.\rangle$ je grupa s aspoň dvěma prvky. Potom $\langle G;.\rangle$ neobsahuje nulový prvek vzhledem ke grupovému násobení.

Důkaz:

Sporem. Nechť grupa s aspoň dvěma prvky obsahuje nulový prvek 0. Každá grupa musí podle axiómu JE obsahovat jednotkový prvek 1. Mohou nastat dvě možnosti $0=1$ nebo $0\neq$

1. Kdyby nastala prvá možnost, pak $x=x.1=x.0=0$ pro všechna $x\in$ G a tedy G je tvořená jediným prvkem 0. Kdyby nastala druhá možnost, pak vzhledem k tomu, že $0.x=x.0=0$ pro všechna $x\in$ G /definiční vlastnost nulového prvku/, není prvek 0 invertibilní a tedy $\langle G;.\rangle$ není grupa.

Definice 3.2.2:

$\langle H;.,()^{-1},1\rangle$ je ***podgrupou*** grupy $\langle G;.,()^{-1},1\rangle$, jestliže platí:

- $H \subseteq G$
- H je uzavřená vzhledem ke všem grupovým operacím, tj. platí-li
  (1) $a,b \in H \Rightarrow a.b \in H$,
  (2) $a \in H \Rightarrow a^{-1} \in H$,
  (3) $1 \in H$.

Poznámky 3.2.2:

1. Pojem podgrupy je specializací pojmu podalgebry /viz definice 3.1.2/.
2. Konjunkce podmínek (1),(2),(3) je ekvivalentní s následující jedinou podmínkou:
   (4) $a,b \in H \Rightarrow a.b^{-1} \in H$.
   Důkaz:
   - $(1) \wedge (2) \wedge (3) \Rightarrow (4)$: ... evidentní
   - $(4) \Rightarrow (1) \wedge (2) \wedge (3)$:
     (3): $a \in H \Rightarrow a,a \in H \Rightarrow a.a^{-1} \in H \Rightarrow 1 \in H$
     (2): $b \in H \Rightarrow 1,b \in H \Rightarrow 1.b^{-1} \in H \Rightarrow b^{-1} \in H$
     (1): $a,b \in H \Rightarrow a,b^{-1} \in H \Rightarrow a.(b^{-1})^{-1} \in H \Rightarrow a.b \in H$

Příklady 3.2.2:

1. Aditivní grupa celých čísel je podgrupou aditivní grupy reálných čísel.
2. Grupa translací /rotací/ je podgrupou grupy transformací souřadnic v rovině.
3. Grupy $\langle G;.\rangle$, $\langle \{1\};.\rangle$ jsou tzv. nevlastní podgrupy grupy $\langle G;.\rangle$.

Věta 3.2.3:

Průnik libovolného systému podgrup dané grupy je opět podgrupa dané grupy.

Důkaz:

Tvrzení dokážeme pouze pro případ dvou podgrup $\langle H;.\rangle, \langle K;.\rangle$ grupy $\langle G;.\rangle$. Nechť $a,b \in H \cap K$. Potom také $a,b \in H,K$. Protože H,K jsou podgrupy jest také $a.b^{-1} \in H,K$. Je tedy $a.b^{-1} \in H \cap K$ a tedy $H \cap K$ je podgrupou grupy G /viz definice a poznámka 3.2.2/.

Definice 3.2.3:

Řád grupy $\langle G;.\rangle$ je počet prvků grupy /tj. nosiče G/. Řád grupy může být konečný nebo nekonečný.

Řád prvku $a \in G$ ***grupy*** $\langle G;.\rangle$ je nejmenší přirozené číslo n takové, že platí

$$a^n = 1$$

/kde 1 je jednotka grupového násobení/, pokud takové n existuje. Jestliže takové n neexistuje, pak říkáme, že prvek a je nekonečného řádu.

Definice 3.2.4:

Cyklická podgrupa grupy $\langle G;.\rangle$ ***generovaná prvkem*** $a \in G$ je grupa tvořená všemi mocninami prvku a, tj. grupa

$$\langle \{...,a^{-2},a^{-1},1,a,a^2,a^3,...\};.\rangle .$$

Cyklická grupa je grupa tvořená mocninami jediného prvku. Řád tohoto prvku, tzv. ***generátoru grupy***, je roven řádu grupy.

Příklady 3.2.3:

1. Množina všech mocnin libovolného prvku grupy tvoří cyklickou podgrupu této grupy.
2. Aditivní grupa celých čísel je nekonečnou cyklickou grupou s gnerátorem 1.
3. Aditivní grupa násobků daného celého čísla tvoří nekonečnou cyklickou podgrupu aditivní grupy celých čísel.
4. Aditivní grupa zbytkových tříd modulo m je konečnou cyklickou grupou řádu m. Generátorem grupy je třída $\underline{1}$.

Definice 3.2.5:

Nechť $\langle G;. \rangle$ je grupa a nechť $M \subseteq G$. ***Podgrupou*** /grupy $\langle G;. \rangle$/ ***generovanou množinou generátorů*** M nazýváme grupu $\langle [M];. \rangle$, kde

$$[M]=\{x_1^{k1}.x_2^{k2}...x_n^{kn}: x_i \in M, ki \in \{1,-1\} \text{ pro } i=1,2,...,n; n \in N\}.$$

Poznámky 3.2.3:

1. Zpravidla požadujeme, aby prvky množiny M byly v grupě $\langle G;. \rangle$ nezávislé, tj. aby žádný prvek z M nebyl v $\langle G;. \rangle$ vyjadřitelný pomocí ostatních prvků z M prostřednictvím grupových operací součinu a inverze.
2. $\langle [M];. \rangle$ je nejmenší podgrupa grupy $\langle G;. \rangle$ obsahující množinu M.
3. Je-li [M]=G, pak říkáme, že M je množinou generátorů grupy $\langle G;. \rangle$.

Příklady 3.2.4:

1. ***Cyklická permutace*** (1/4,2/1,3/2,4/3) /transformující skupinu (1,2,3,4) na skupinu (4,1,2,3)/ a ***transpoziční permutace*** (1/2,2/1,3/3,4/4) /měnící pořadí prvých dvou prvků ve skupině (1,2,3,4) / tvoří dvouprvkovou množinu generátorů grupy všech permutací prvků množiny {1,2,3,4}.
2. Množina všech transpozic /permutací zaměňujících pozice dvou různých prvků/ tvoří množinu generátorů grupy všech permutací. uvažujeme-li množinu n prvků, pak libovolnou jejich permutaci můžeme vyjádřit jako součin /kompozici/ nejvýše n-1 transpozicí.

Věta 3.2.4:

Nechť $\langle H;. \rangle$ je podgrupou grupy $\langle G;. \rangle$. Označme

- $Hg=\{h.g: h \in H\}$ pro libovolné $g \in G$,
- $gH=\{g.h: h \in H\}$ pro libovolné $g \in G$. **11**

Potom:

1. Systémy podmnožin $\{Hg: g \in G\}$, resp. $\{gH: g \in G\}$ množiny G tvoří rozklad množiny G.
2. Je-li grupa $\langle G;. \rangle$ konečná, pak všechny třídy těchto rozkladů mají stejný počet prvků jako množina H.

Důkaz:

Důkaz provedeme jen pro systém $\{Hg: g \in G\}$ /důkaz pro systém $\{gH: g \in G\}$ je obdobný/. Třeba dokázat:

1. Každý prvek $g \in G$ patří do nějaké množiny Hg.
2. Mají-li množiny Hg a Hg' společný nějaký prvek, pak jsou totožné.
3. Množina H a každá množina systému Hg mají stejný počet prvků.

Ad 1) $1\in H \Rightarrow 1.g\in Hg \Rightarrow g\in Hg$, tj. libovolný prvek $g\in G$ patří do nějaké množiny Hg.

Ad 2) Nechť množiny Hg a Hg' mají společný prvek a, tj.

$$a=h.g=h'g',$$

kde $h,h'\in H$. Odtud dostáváme

$$g=h^{-1}.h'.g'.$$

Je-li nyní $x\in Hg$, pak $x=h''.g$ a tedy také $x=h''.h^{-1}.h'.g$, neboli $x=h'''.g$, tj. $x\in Hg'$. Stejným způsobem dokážeme opačnou implikaci $x\in Hg' \Rightarrow x\in Hg$. Platí tedy $Hg=Hg'$.

Ad 3) Zřejmě platí pro každé $g\in G$ $card(Hg) \leq card(H)$. Kdyby $card(Hg) < card(H)$, pak musí existovat $h,h'\in H$ taková, že $h\neq h'$ a $hg=h'g$. Odtud krácením dostáváme spor $h=h'$. Musí tedy platit $card(Hg)=card(H)$.

Definice 3.2.6:

Množiny systému Hg /resp. gH/, z předchozí věty 3.2.4, nazýváme ***pravými /levými/ třídami rozkladu grupy*** $\langle G;.\rangle$ ***podle podgrupy*** $\langle H;.\rangle$.

Platí-li $Hg=gH$ pro všechna $g\in G$, pak podgrupu $\langle H;.\rangle$ nazýváme ***invariantní podgrupou*** grupy $\langle G;.\rangle$.

Poznámka 3.2.4:

Je-li H invariantní podgrupa grupy G, pak ke každému $g\in G$ existují prvky $h',h''\in H$ takové, že $g.h'=h''g$, neboli $g=h''.g.(h')^{-1}$.

Věta 3.2.5 /Lagrangeova/**:**

Nechť $\langle H;.\rangle$ je podgrupou konečné grupy $\langle G;.\rangle$. Potom řád podgrupy $\langle H;.\rangle$ dělí řád grupy $\langle G;.\rangle$.

Důkaz:

Nechť n je řád grupy G, m řád podgrupy H a r počet pravých /levých/ tříd rozkladu grupy G podle podgrupy H. Podle věty 3.2.4 mají všechny třídy stejný počet prvků rovný počtu prvků podgrupy H a tedy musí platit $n=rm$, tj. m dělí n.

Důsledky:

1. Řád každého prvku grupy je dělitelem řádu grupy.
2. Každá grupa prvočíselného řádu je cyklická a každý její nejednotkový prvek je jejím generátorem.

Definice 3.2.7:

Morfismus grupy $\langle G;.\rangle$ do grupy $\langle G';*\rangle$ je zobrazení $h:G\to G'$ takové, že

$$h(a.b)=h(a)*h(b).$$

Jádro morfismu je množina vzorů prvku $1'\in G'$ v zobrazení h.

Poznámky 3.2.5:

1. Pojem grupového morfismu je specializací obecného pojmu morfismu algeber /viz definice 3.1.3/.
2. Vlastnost morfismu musí přirozeně platit i pro odvozené grupové operace: operaci jednotkového a inverzního prvku:
   - $h(1)=1'$

     Důkaz: $h(a)=h(a.1)=h(a)*h(1)=h(a)*1' \Rightarrow h(1)=1'$

- $(h(a))^{-1}=h(a^{-1})$
  Důkaz: $1'=h(1)=h(a.a^{-1})=h(a)*h(a^{-1}) \Rightarrow (h(a))^{-1}=h(a^{-1})$

Věta 3.2.6:

Jádro morfismu grupy $\langle G;.\rangle$ do grupy $\langle G';*\rangle$ je podgrupa grupy $\langle G;.\rangle$.

Důkaz:

Podle definice a poznámky 3.2.2 stačí dokázat:

$$h(a)=1' \wedge h(b)=1' \Rightarrow h(a.b^{-1})=1'.$$

Důkazem je následující řetěz rovností:

$$h(a.b^{-1})=h(a).h(b^{-1})=1'.(h(b))^{-1}=1'.(1')^{-1}=1'.1'=1'.$$

Příklady 3.2.5:

1.
Zobrazení h(A)=det(A) je epimorfismem multiplikativní grupy regulárních čtvercových matic /daného řádu n, tj.typu n× n/ do multiplikativní grupy nenulových reálných čísel. Jádrem morfismu je množina čtvercových matic jejichž determinant je roven 1. Tato množina představuje podgrupu multiplikativní grupy regulárních čtvercových matic.

2.
Zobrazení h(x)=log(x) je isomorfismem multiplikativní grupy kladných reálných čísel do aditivní grupy reálných čísel.

Definice 3.2.8:

Kongruence na grupě $\langle G;.\rangle$ je ekvivalence $\approx$ na G taková, že

$$a\approx a' \wedge b\approx b' \Rightarrow a.b\approx a'.b'.$$

Jádro kongruence je třída $\underline{\mathbf{1}}$ prvků ekvivalentních s jednotkovým prvkem $1\in G$.

Poznámky 3.2.6:

1.
Pojem kongruence na grupě je specializací obecného pojmu kongruence na algebře /viz definice 3.1.4/.

2.
Vlastnost kongruence musí přirozeně platit i pro odvozenou grupovou operaci inverzního prvku, tj.

$$a\approx b \Rightarrow a^{-1}\approx b^{-1}.$$

Důkaz:

$$a\approx b \Rightarrow a.b^{-1}\approx b.b^{-1} \Rightarrow a.b^{-1}\approx 1 \Rightarrow$$

$$\Rightarrow a^{-1}.a.b^{-1}\approx a^{-1} \Rightarrow b^{-1}\approx a^{-1} \Rightarrow a^{-1}\approx b^{-1}$$

Věta 3.2.7:

Jádro kongruence na grupě $\langle G;.\rangle$ je podgrupou grupy $\langle G;.\rangle$.

Důkaz:

Třeba dokázat $a,b\in\underline{\mathbf{1}} \Rightarrow a.b,\ a^{-1}\in\underline{\mathbf{1}}$.

- $a,b\in\underline{\mathbf{1}} \Rightarrow a\approx 1 \wedge b\approx 1 \Rightarrow a.b\approx 1 \Rightarrow a.b\in\underline{\mathbf{1}}$,
- $a\in\underline{\mathbf{1}} \Rightarrow a\approx 1 \Rightarrow a^{-1}\approx 1^{-1} \Rightarrow a^{-1}\approx 1 \Rightarrow a^{-1}\in\underline{\mathbf{1}}$.

Věta 3.2.8:

Každá kongruence na grupě je jednoznačně určena svým jádrem.

Důkaz:

Nechť ρ a σ jsou dvě kongruence na grupě $\langle G;.\rangle$. Máme dokázat:

$$(\forall x)[x\rho 1 \Leftrightarrow x\sigma 1] \Rightarrow (\forall x,y)[x\rho y \Leftrightarrow x\sigma y].$$

Důkazem je následující řetěz ekvivalencí:

$$x\rho y \Leftrightarrow x.y^{-1}\rho yy^{-1} \Leftrightarrow x.y^{-1}\rho 1 \Leftrightarrow x.y^{-1}\sigma 1 \Leftrightarrow x.y^{-1}.y\sigma 1.y \Leftrightarrow x\sigma y.$$

Definice 3.2.9:

Faktorová grupa grupy $\langle G;.\rangle$ podle kongruence $\approx$ je grupa $\langle G/\approx ;\underline{.}\rangle$, kde

- $G/\approx$ je faktorová množina množiny G podle ekvivalence $\approx$,
- $\underline{.}$ je operace mezi prvky $\underline{\mathbf{x}},\underline{\mathbf{y}}\in G/\approx$ definovaná takto:

$$\underline{\mathbf{x}} \ \underline{.} \ \underline{\mathbf{y}} =_{def} \underline{x.y} .$$

Poznámka 3.2.7:

Pojem faktorové grupy je specializací obecného pojmu faktorové algebry /viz definice 3.1.5/.

Příklad 3.2.6:

Aditivní grupa zbytkových tříd modulo m, tj. grupa $\langle Z_m;\underline{+}\rangle$ je faktorovou grupou aditivní grupy celých čísel $\langle I;+\rangle$ podle kongruence $\approx$ (mod m).

Věta 3.2.8:

Všechny třídy faktorové grupy mají stejnou mohutnost.

Věta 3.2.9:

Nechť G je grupa. Potom následující tři tvrzení jsou ekvivalentní:

(1) H je invariantní podgrupou grupy G.

(2) Pravý /levý/ rozklad grupy G podle podgrupy H definuje kongruenci ρ na G a to takovou, že H je třídou kongruence ρ obsahující $1\in G$.

(3) Podgrupa H je jádrem morfismu grupy G do faktorové grupy G/ρ.

Věta 3.2.10:

Každá nekonečná cyklická grupa je isomorfní s aditivní grupou celých čísel.

Důkaz:

Nechť $\langle G;.\rangle=\langle\{..,a^{-2},a^{-1},a^0,a^1,a^2,..\};.\rangle$ je libovolná nekonečná cyklická grupa a $\langle I;+\rangle=\langle\{..,-2,-1,0,1,2,..\};+\rangle$ aditivní grupa celých čísel. Isomorfismus je zprostředkován zobrazením

$$h: I\rightarrow G, \quad h(i)=a^i,$$

které je evidentně bijekcí a pro které je splněna vlastnost morfismu

$$h(i+j)=h(i).h(j), \text{ neboli } a^{i+j}=a^i.a^j.$$

Věta 3.2.11:

Každá konečná cyklická grupa řádu m je isomorfní s aditivní grupou zbytkových tříd modulo m.

Důkaz:

Nechť $\langle G;.\rangle=\langle\{a^0,a^1,a^2,..,a^{m-1}\};.\rangle$ je libovolná konečná cyklická grupa m-tého řádu a $\langle Z_m;\underline{+}\rangle=\langle\{\underline{\mathbf{0}},\underline{\mathbf{1}},\underline{\mathbf{2}},..,\underline{\mathbf{m-1}}\};\underline{+}\rangle$ aditivní grupa zbytkových tříd modulo m. Isomorfismus mezi oběma grupami je zprostředkován zobrazením

$$h: Z_m\rightarrow G, \quad h(\underline{\mathbf{i}})=a^i,$$

které je evidentně bijekcí a pro které je splněna vlastnost morfismu

$$h(\underline{\mathbf{i}} \ \underline{+} \ \underline{\mathbf{j}})=h(\underline{\mathbf{i}}).h(\underline{\mathbf{j}}), \text{ neboli } a^{i+j}=a^i.a^j.$$

Definice 3.2.10:

Symetrická grupa stupně n je grupa všech bijektivních zobrazení n-prvkové množiny na sebe, neboli /ztotožníme-li prvky s jejich indexy/ grupa všech permutací množiny {1,2,...,n}. Řád symetrické grupy stupně n je n!.

Symetrická grupa S(M) ***na množině*** M je grupa všech bijektivních zobrazení této množiny na sebe.

Věta 3.2.12 /Cayleyova reprezentační věta/**:**

Každá konečná grupa <G;.> je isomorfní s nějakou podgrupou symetrické grupy na množině G. Neboli: každá konečná grupa je isomorfní s nějakou grupou permutací.

Důkaz:

Nechť $\langle G;.\rangle=\langle\{a_1,a_2,..,a_n\};.\rangle$ je libovolná konečná grupa a $\langle S(G);\circ\rangle$ symetrická grupa na množině G /n-tého stupně/. Definujme zobrazení $h: G\to S(G)$ přiřazující každému prvku $a\in G$ funkci $f_a\in S(G)$ takto:

$$f_a(x)=x.a$$

Funkce $f_a(x)$ je vskutku bijekcí, neboť:

- $x_1\neq x_2 \Rightarrow x_1.a\neq x_2.a \Rightarrow f_a(x_1)\neq f_a(x_2)$, tj. f_a je injektivní,
- rovnice $x.a=y$ /tj. $f_a(x)=y$/ má jediné řešení x, tj. f_a je surjektivní.

Zobrazení h má vlastnost morfismu $h(a.b)=h(a)\circ h(b)$, neboť $f_{a.b}(x) = x.(a.b) = (x.a).b = f_b(f_a(x)) = (f_a\circ f_b)(x)$. Zobrazení h je injektivní $/a\neq b \Rightarrow a.1\neq b.1 \Rightarrow f_a(1)\neq f_b(1) \Rightarrow f_a\neq f_b$/, ale nemusí být surjektivní.

Množina obrazů grupy G tvoří podgrupu $\langle h(G);\circ\rangle$ symetrické grupy $\langle S(G);\circ\rangle$. Tato podgrupa je isomorfní s grupou $\langle G;.\rangle$.