Homomorfismy grup

Algebra 2

Mgr. Markéta Trnečková, Ph.D.

Palacký University, Olomouc

Třídy ekvivalence

Připomenutí:

- **Levá třída H obsahující a**: $aH = \{ah | h \in H\}$
- **Pravá třída H obsahující a**: $Ha = \{ha | h \in H\}$
- Každá třída (levá i pravá) rozkladu G podle H má stejný počet prvků jako H
- H podgrupa konečné grupy G. Pak $|H|$ je dělitel $|G|$
- Každá grupa s prvočíselným řádem je cyklická
- Každá konečně generovaná abelovská grupa G je isomorfní direktnímu součinu cyklických grup ve tvaru
  $\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}} \times \mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$,
  kde p_i jsou prvočísla, ne nutně různá, a $r_i \in \mathbb{N}$.
- Nechť $(a_1, \ldots, a_n) \in \prod_{i=1}^{n} G_i$. Pokud a_i je konečného řádu r_i v G_i, pak řád $(a_1, \ldots, a_n)$ v $\prod_{i=1}^{n} G_i$ je roven lcm všech r_i.
- Nechť G je cyklická grupa s n prvky, která je generovaná a a $b = a^s \in G$.
  b generuje cyklickou podgrupu $H \leq G$ obsahující n/d prvků, kde d je $gcd(n, s)$.

Rozložitelnost grupy

Definice

Grupa G je **rozložitelná**, *pokud je isomorfní s direktním součinem dvou vlastních netriviálních podgrup. Jinak je* **nerozložitelná**.

Příklad 60

Jsou následující grupy rozložitelné?

1. $\mathbb{Z}_4$
2. $\mathbb{Z}_6$

Rozložitelnost grupy

Příklad

Jsou následující grupy rozložitelné?

1. $\mathbb{Z}_4$
2. $\mathbb{Z}_6$

1. $\mathbb{Z}_4$ – není
   - Netriviální podgrupy – $\langle 2 \rangle = \{0, 2\}$
   - $\mathbb{Z}_2 \times \mathbb{Z}_2$ není isomorfní s $\mathbb{Z}_4$. **Proč?**
   - V $\mathbb{Z}_2 \times \mathbb{Z}_2$ platí $a + a = e$ pro všechna a
2. $\mathbb{Z}_6$ – je
   - Netriviální podgrupy – $\langle 2 \rangle = \{0, 2, 4\}$, $\langle 3 \rangle = \{0, 3\}$
   - $\mathbb{Z}_2 \times \mathbb{Z}_3$ je isomorfní s $\mathbb{Z}_6$. **Ověřte.**

Rozložitelnost grupy

Věta 27

Konečně nerozložitelné grupy jsou právě cyklické grupy s řádem, který je mocnina prvočísla.

Důkaz

Nechť G je konečná nerozložitelná abelovská grupa.
Podle základní věty konečně generovaných abelovských grup je isomorfní s direktním součinem cyklických grup s řádem, který je mocnina prvočísla.
Protože G je nerozložitelná, tento součin se musí se skládat z jedné cyklické grupy, jejíž řád je prvočíslo.
Nechť p je prvočíslo.
Pak $\mathbb{Z}_{p^r}$ je nerozložitelná, protože pokud by $\mathbb{Z}_{p^r}$ byla isomorfní s $\mathbb{Z}_{p^i} \times \mathbb{Z}_{p^j}$, kde $i + j = r$, pak každý prvek musí mít řád nejvýše $p^{\max(i,j)} < p^r$. (Protože $p^{\max(i,j)}$ je lcm čísel p^i a p^j.)

Rozložitelnost grupy

Věta 28

Pokud m dělí řád konečné abelovské grupy G, pak má G podgrupu řádu m.

Důkaz

Dle základní věty rozložitelnosti abelovských grup, můžeme ke G najít isomorfní direktní součin

$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}}$,

kde p_i nemusí být různá. Protože $(p_1)^{r_1}(p_2)^{r_2} \dots (p_n)^{r_n}$ je řád G, pak m musí být ve tvaru $(p_1)^{s_1}(p_2)^{s_2} \dots (p_n)^{s_n}$, kde $0 \leq s_i \leq r_i$.

Dle věty 11 $(p_i)^{r_i - s_i}$ generuje cyklickou podgrupu $\mathbb{Z}_{(p_i)^{r_i}}$ řádu, který je podílem $\frac{(p_i)^{r_i}}{d}$, kde $d = gcd((p_i)^{r_i}, (p_i)^{r_i - s_i})$.

$gcd((p_i)^{r_i}, (p_i)^{r_i - s_i})$ je $(p_i)^{r_i - s_i}$. Takže $(p_i)^{r_i - s_i}$ generuje cyklickou podgrupu $\mathbb{Z}_{(p_i)^{r_i}}$ řádu $\frac{(p_i)^{r_i}}{(p_i)^{r_i - s_i}} = (p_i)^{s_i}$.

Vidíme, že $\langle (p_1)^{r_1 - s_1} \rangle \times \langle (p_2)^{r_2 - s_2} \rangle \times \cdots \times \langle (p_n)^{r_n - s_n} \rangle$ je požadovaná podgrupa řádu m.

Rozložitelnost grupy

Věta 29

Pokud $m \in \mathbb{Z}$ není dělitelné druhou mocninou žádného prvočísla, pak každá abelovská grupa řádu m je cyklická.

Důkaz

Nechť G je abelovská grupa s takovým řádem m, Pak je isomorfní s
$\mathbb{Z}_{(p_1)^{r_1}} \times \mathbb{Z}_{(p_2)^{r_2}} \times \cdots \times \mathbb{Z}_{(p_n)^{r_n}}$
kde $m = (p_1)^{r_1}(p_2)^{r_2} \dots (p_n)^{r_n}$.
Protože m není dělitelné druhou mocninou žádného prvočísla, musí všechna $r_i = 1$ a p_i různá prvočísla.
G je tedy isomorfní s $\mathbb{Z}_{p_1 p_2 \dots p_n}$ a tedy je cyklická. (důsledek 6).

Rozložitelnost grupy

Příklad 61

Určete, zda je grupa zadaná tabulkou níže rozložitelná.

$*$	e					
e	e					
			e			
		e				
				e		
					e	
						e

Jaký je její řád?
Jaké má netriviální podgrupy?

Homomorfismus grupy

Definice

Zobrazení ϕ grupy G do grupy G' je **homomorfismus**, *pokud je pro všechna $a, b \in G$ splněna podmínka homomorfismu:*
$\phi(ab) = \phi(a)\phi(b)$.

Tvrzení

Mezi libovolnými dvěma grupami G a G' vždy existuje alespoň jeden homomorfismus $\phi : G \to G'$:
$\phi(g) = e'$ *pro všechna $g \in G$.*
Tomuto homomorfismu říkáme **triviální homomorfismus**.

Jak ověříme, že se jedná o homomorfismus?

Homomorfismus grupy

Tvrzení

Nechť $\phi : G \to G'$ je homomorfismus G na G' (je surjektivní). Pokud G je abelovská, pak i G' je abelovská.

Důkaz

Máme $a, b \in G$ takové, že $\phi(a) = a'$ a $\phi(b) = b'$.
Protože G je abelovská, musí platit $ab = ba$.
ϕ je homomorfismus, platí tedy:
$a'b' = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = b'a'$
Takže je G' také abelovská.

Homomorfismus grupy

Zkuste dokázat následující tvrzení.

Tvrzení

Nechť S_n je symetrická grupa na n-prvkové množině a $\phi : S_n \to \mathbb{Z}_2$ definované jako:

$$\phi(\sigma) = \begin{cases} 0 & \text{pokud } \sigma \text{ je sudá permutace} \\ 1 & \text{pokud } \sigma \text{ je lichá permutace} \end{cases}$$

je homomorfismus.

Homomorfismus grupy

Tvrzení

Nechť S_n je symetrická grupa na n-prvkové množině a $\phi : S_n \to \mathbb{Z}_2$ definované jako:

$$\phi(\sigma) = \begin{cases} 0 & \text{pokud } \sigma \text{ je sudá permutace} \\ 1 & \text{pokud } \sigma \text{ je lichá permutace} \end{cases}$$

je homomorfismus.

Důkaz

Musíme ukázat, že $\phi(\sigma\mu) = \phi(\sigma) + \phi(\mu)$ pro všechny $\sigma, \mu \in S_n$. Stačí ověřit 4 případy:

- *σ je lichá, μ je lichá*
  σ i μ můžeme zapsat jako součin lichého počtu transpozic ($\phi(\sigma) = 1$, $\phi(\mu) = 1$), pak $\sigma\mu$ je zapsáno jako součin sudého počtu transpozic ($\phi(\sigma\mu) = 0$).
  $\phi(\sigma) + \phi(\mu) = 1 + 1 = 0$ v $\mathbb{Z}_2$
- *σ je lichá, μ je sudá*
- *σ je sudá, μ je lichá*
- *σ je sudá, μ je sudá*

Homomorfismus grupy

Tvrzení

Nechť F je aditivní grupa všech funkcí zobrazující $\mathbb{R}$ do $\mathbb{R}$. $\mathbb{R}$ je aditivní grupa reálných čísel a $c \in \mathbb{R}$.
Zobrazení $\phi_c : F \to \mathbb{R}$ definované:
$\phi_c(f) = f(c)$ je homomorfismus.
Toto zobrazení nazýváme **homomorfismus vyhodnocení**.

Součet funkcí f a g je funkce $f + g$ jejíž hodnota v x je $f(x) + g(x)$.

Homomorfismus grupy

Tvrzení

Nechť F je aditivní grupa všech funkcí zobrazující $\mathbb{R}$ do $\mathbb{R}$. $\mathbb{R}$ je aditivní grupa reálných čísel a $c \in \mathbb{R}$.
Zobrazení $\phi_c : F \to \mathbb{R}$ definované:
$\phi_c(f) = f(c)$ je homomorfismus.
Toto zobrazení nazýváme **homomorfismus vyhodnocení**.

Důkaz

$\phi_c(f+g) = (f+g)(c) = f(c) + g(c) = \phi_c(f) + \phi_c(g)$
Podmínka homomorfismu je splněna.

Homomorfismus grupy

Tvrzení

Nechť $\mathbb{R}^n$ je aditivní grupa sloupcových vektorů s n složkami.
Tato grupa je zjevně isomorfní direktnímu součinu $\mathbb{R}$ se sebou n násobně.
A je $m \times n$ matice reálných čísel. Zobrazení $\phi(v) = Av$ pro všechny $v \in \mathbb{R}^n$ je homomorfismus.
Toto zobrazení nazýváme **lineární transformace**.

Homomorfismus grupy

Tvrzení

Nechť $\mathbb{R}^n$ je aditivní grupa sloupcových vektorů s n složkami.
Tato grupa je zjevně isomorfní direktnímu součinu $\mathbb{R}$ se sebou n násobně.
A je $m \times n$ matice reálných čísel. Zobrazení $\phi(v) = Av$ pro všechny $v \in \mathbb{R}^n$ je homomorfismus.
Toto zobrazení nazýváme **lineární transformace**.

Důkaz

Pro $v, w \in \mathbb{R}^n$ platí:
$\phi(v + w) = A(v + w) = Av + Aw = \phi(v) + \phi(w)$

Homomorfismus grupy

Tvrzení

Nechť $r \in \mathbb{Z}$ a $\phi_r : \mathbb{Z} \to \mathbb{Z}$ je definované předpisem $\phi_r(n) = rn$ pro všechna $n \in \mathbb{Z}$. ϕ_r je pro všechna $r \in \mathbb{Z}$ homomorfismus.

Homomorfismus grupy

Tvrzení

Nechť $r \in \mathbb{Z}$ a $\phi_r : \mathbb{Z} \to \mathbb{Z}$ je definované předpisem $\phi_r(n) = rn$ pro všechna $n \in \mathbb{Z}$. ϕ_r je pro všechna $r \in \mathbb{Z}$ homomorfismus.

Důkaz

Pro všechna $m, n \in \mathbb{Z}$ platí
$\phi_r(m+n) = r(m+n) = rm + rn = \phi_r(m) + \phi_r(n)$.
Všimněme si, že pro $r = 0$ je ϕ_0 triviální homomorfismus.
ϕ_1 *je identita.*
ϕ_1 *a* ϕ_{-1} *jsou surjektivní, pro ostatní surjekce neplatí.*

Homomorfismus grupy

Tvrzení

Nechť $G = G_1 \times G_2 \times \cdots \times G_n$ *je direktní součin grup.*
Projekce $\pi_i : G \to G_i$, *kde*
$\pi_i(g_1, g_2, \ldots, g_n) = g_i$,
je homomorfismus, pro všechna $i = 1, \ldots, n$.

Homomorfismus grupy

Tvrzení

Nechť $G = G_1 \times G_2 \times \cdots \times G_n$ je direktní součin grup.
Projekce $\pi_i : G \to G_i$, *kde*
$\pi_i(g_1, g_2, \ldots, g_n) = g_i$,
je homomorfismus, pro všechna $i = 1, \ldots, n$.

Důkaz

Přímo plyne z toho, že operace G odpovídá v i-té komponentě operaci G_i.

Homomorfismus grupy

Tvrzení

Nechť $\gamma : \mathbb{Z} \to \mathbb{Z}_n$ je zobrazení dané $\gamma(m) = r$, kde r je zbytek po dělení čísla m číslem n. Ukažte, že **redukce modulo** n γ *je homomorfismus.*

Homomorfismus grupy

Tvrzení

Nechť $\gamma : \mathbb{Z} \to \mathbb{Z}_n$ je zobrazení dané $\gamma(m) = r$, kde r je zbytek po dělení čísla m číslem n. Ukažte, že **redukce modulo** n γ *je homomorfismus.*

Důkaz

Musíme ukázat, že $\gamma(s+t) = \gamma(s) + \gamma(t)$ pro $s, t \in \mathbb{Z}$.
Z věty o celočíselném dělení víme:
$s = q_1 n + r_1$, $t = q_2 n + r_2$, *kde* $0 \leq r_i < n$ *pro* $i = 1, 2$.
Pokud $r_1 + r_2 = q_3 n + r_3$ *pro* $0 \leq r_3 < n$, *pak*
$s + t = q_1 n + r_1 + q_2 n + r_2 = (q_1 + q_2 + q_3)n + r_3$
takže $\gamma(s+t) = r_3$.
Z toho vidíme, že $\gamma(s) = r_1$, $\gamma(t) = r_2$ *a že součet* $r_1 + r_2$ *v* $\mathbb{Z}_n$ *je také* r_3.
Takže $\gamma(s+t) = \gamma(s) + \gamma(t)$.
γ *je homomorfismus.*

Vlastnosti homomorfismů

Věta 30

Složení homomorfismů je opět homomorfismus.

Důkaz

Nebudeme dokazovat, znáte z dřívějšího studia.

Definice

Nechť ϕ *je zobrazení* X *do* Y *a nechť* $A \subseteq X$ *a* $B \subseteq Y$.
Obraz $\phi[A]$ **množiny** A **v** Y **při** ϕ *je* $\{\phi(a) | a \in A\}$.
Množinu $\phi[A]$ *nazýváme* **obor hodnot** *zobrazení* ϕ.
Inverzní obraz $\phi^{-1}[B]$ *v* X *je* $\{x \in X | \phi(x) \in B\}$.

Vlastnosti homomorfismů

Věta 31

Nechť ϕ je homomorfismus grupy G do grupy G'.

1. *Pokud je e neutrální prvek G, pak $\phi(e)$ je neutrální prvek e' v G'.*
2. *Pokud $a \in G$, pak $\phi(a^{-1}) = \phi(a)^{-1}$.*
3. *Pokud H je podgrupa G, pak $\phi[H]$ je podgrupa G'.*
4. *Pokud K' je podgrupa G', pak $\phi^{-1}[K']$ je podgrupa G.*

ϕ zachovává neutrální prvek, inverzní prvky a podgrupy.

Důkaz

Nechť $\phi : G \to G'$ je homomorfismus.

1. $\phi(a) = \phi(ae) = \phi(a)\phi(e)$.
   Násobením zleva $\phi(a)^{-1}$ dostaneme $e' = \phi(e)$.
   $\phi(e)$ je neutrální prvek v G'.

Vlastnosti homomorfismů

Důkaz (Pokračování)

2. *Rovnice* $e' = \phi(e) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1})$ *ukazuje, že* $\phi(a^{-1}) = \phi(a)^{-1}$
3. *Nechť* H *je podgrupa* G, $\phi(a)$ *a* $\phi(b)$ *jsou libovolné prvky z* $\phi[H]$.
   $\phi(a)\phi(b) = \phi(ab)$, *takže vidíme, že* $\phi(a)\phi(b) \in \phi[H]$, *takže* $\phi[H]$ *je uzavřená na operaci* G'.
   Spolu s tím, že $e' = \phi(e)$ *a* $\phi(a^{-1}) = \phi(a)^{-1}$, *dostaneme, že* $\phi[H]$ *je podgrupa* G'.
4. *Nechť* K' *je podgrupa* G'. *Předpokládejme, že* $a, b \in \phi^{-1}[K']$.
   Pak $\phi(a)\phi(b) \in K'$, *protože* K' *je podgrupa.*
   $\phi(ab) = \phi(a)\phi(b)$ *ukazuje, že* $ab \in \phi[K']$.
   Takže $\phi^{-1}[K']$ *je uzavřená na operaci z* G.
   Také K' *musí obsahovat neutrální prvek* $e' = \phi(e)$, *takže* $e \in \phi^{-1}[K']$.
   Pokud $a \in \phi^{-1}[K']$, *pak* $\phi(a) \in K'$, *takže* $\phi(a)^{-1} \in K'$.
   Ale $\phi(a)^{-1} = \phi(a^{-1})$, *takže* $a^{-1} \in \phi^{-1}[K']$.
   Z toho plyne, že $\phi^{-1}[K']$ *je podgrupa* G.

Jádro homomorfismu

Definice

Nechť $\phi : G \to G'$ je homomorfismus grup. Podgrupa
$\phi^{-1}[\{e'\}] = \{x \in G | \phi(x) = e'\}$
se nazývá **jádro** ϕ.
Značíme $Ker(\phi)$.

Zjevně $\{e'\}$ je podgrupa G', takže dle předchozí věty $\phi^{-1}[\{e'\}]$ je podgrupa grupy G.

Jádro homomorfismu

Věta 32

Nechť $\phi : G \to G'$ je homomorfismus grup, $H = Ker(\phi)$ a $a \in G$.
Podmnožina $\phi^{-1}[\{\phi(a)\}] = \{x \in G | \phi(x) = \phi(a)\}$
je levá třída aH a také pravá třída Ha rozkladu G dle podgrupy H.
Tyto dva rozklady jsou navíc stejné.

Důkaz

Chceme ukázat, že $\{x \in G | \phi(x) = \phi(a)\} = aH$.
Předpokládejme, že $\phi(x) = \phi(a)$. Pak
$\phi(a)^{-1}\phi(x) = e'$, kde e' je neutrální prvek G'.
Víme, že $\phi(a)^{-1} = \phi(a^{-1})$, tedy $\phi(a^{-1})\phi(x) = e'$.
Protože ϕ je homomorfismus, máme
$\phi(a^{-1})\phi(x) = \phi(a^{-1}x)$ takže $\phi(a^{-1}x) = e'$.
Což ale ukazuje, že $a^{-1}x \in H = Ker(\phi)$, takže $a^{-1}x = h$ pro nějaké $h \in H$ a $x = ah \in aH$.
To ukazuje, že $\{x \in G | \phi(x) = \phi(a)\} \subseteq aH$

Jádro homomorfismu

Důkaz (Pokračování)

Chceme ukázat, že opačný směr.
Předpokládejme, že $y \in aH$, *takže* $y = ah$ *pro nějaké* $h \in H$. *Pak*
$\phi(y) = \phi(ah) = \phi(a)\phi(h) = \phi(a)e' = \phi(a)$,
takže $y \in \{x \in G | \phi(x) = \phi(a)\}$.

Důkaz, že $\{x \in G | \phi(x) = \phi(a)\} = Ha$ *by byl obdobný a necháme jako cvičení.*

Jádro homomorfismu

Příklad 62

Pro komplexní čísla z_1 a z_2 platí $|z_1 z_2| = |z_1||z_2|$.
Funkce absolutní hodnoty $|\cdot|$ je homomorfismus grupy $\mathbb{C} - \{0\}$ s násobením na grupu $\mathbb{R}^+$ s násobením.
Protože $\{1\}$ je podgrupa $\mathbb{R}^+$, víme, že čísla na jednotkové kružnici tvoří podgrupu grupy G.
Třídy rozkladu $\mathbb{C} - \{0\}$ odpovídající tomuto homomorfismu jsou kružnice se středem v počátku.
Každá kružnice je homomorfismem zobrazena na její průnik s kladnou částí reálné osy (její poloměr).

Jádro homomorfismu

Příklad 63

Nechť D je aditivní grupa všech diferencovatelných reálných funkcí jedné proměnné a F je aditivní grupa všech reálných funkcí jedné proměnné.
Je derivace ($\phi : D \to F$, kde $\phi(f) = f'$) homomorfismus? Pokud ano, jak vypadá jeho jádro?

Jádro homomorfismu

Příklad

Nechť D je aditivní grupa všech diferencovatelných reálných funkcí jedné proměnné a F je aditivní grupa všech reálných funkcí jedné proměnné.
Je derivace ($\phi : D \to F$, kde $\phi(f) = f'$) homomorfismus? Pokud ano, jak vypadá jeho jádro?

- Ano, je homomorfismus, protože:
  $\phi(f + g) = (f + g)' = f' + g' = \phi(f) + \phi(g)$
- Jádro:
  $Ker(\phi)$ jsou všechny funkce, pro které platí $f' = 0$, což jsou všechny konstantní funkce
- Konstantní funkce tvoří podgrupu C grupy D
- Třída funkcí, které se zobrazí na x^2:
  Jednou z takových funkcí je $\frac{x^3}{3}$
  Dle předchozí věty jsou to tedy funkce $\frac{x^3}{3} + C$

Jádro homomorfismu

Důsledek 7

Homomorfismus grup $\phi : G \to G'$ je injektivní zobrazení, právě když $Ker(\phi) = \{e\}$.

Důkaz

Pokud $Ker(\phi) = \{e\}$, pak pro každé $a \in G$ jsou prvky zobrazené do $\phi(a)$ přesně prvky z levé třídy $a\{e\} = \{a\}$, což ukazuje, že ϕ je injektivní.

Předpokládejme, že ϕ je injektivní. Pak víme, že $\phi(e) = e'$.
Protože ϕ je injektivní, vidíme, že existuje jen jeden prvek zobrazený na e', takže $Ker(\phi) = \{e\}$.

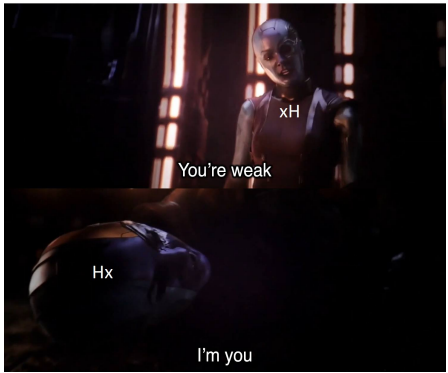
Nyní, abychom dokázali, že jsou dvě grupy isomorfní, stačí najít homomorfismus ϕ, že platí $Ker(\phi) = \{e\}$ a je toto zobrazení surjektivní.

Normální podgrupa

Definice

Podgrupa H grupy G je **normální**, *pokud její levé a pravé třídy koincidují, tedy když $gH = Hg$ pro všechna $g \in G$.*

Normal subgroups be like



Normální podgrupa

Tvrzení

Všechny podgrupy abelovských grup jsou normální.

Důsledek 8

Pokud $\phi : G \to G'$ je homomorfismus grup, $Ker(\phi)$ je normální podgrupa G.

Důkaz

Přímo plyne z předchozí věty.