Algebraické struktury s jednou binární operací

Algebra 2

Mgr. Markéta Trnečková, Ph.D.

Palacký University, Olomouc

Základní pojmy, které znáte z dřívějška

Základní věta algebry:
Algebra nám často dává víc, než od ní chceme.

- Binární relace
- Binární operace
- Grupoidy
- Pologrupy
- Grupy
- Homomorfismus

Jak je definovaná binární relace?

Binární relace

Definice

Binární relace *je uspořádaná trojice* $\langle A, B, R \rangle$*, kde* A *a* B *jsou libovolné množiny a* R *je podmnožinou kartézského součinu* $A \times B$*.*

Příklad 1

Jsou dány množiny $A = \{1, 2, 3, 4, 5\}$ *a* $B = \{a, b, c, d, e\}$ *uveďte příklad relací mezi* A *a* B*, mezi* B *a* A *a na množině* A*.*

Vlastnosti relací

Reflexivita, symetrie, asymetrie, antisymetrie, tranzitivita

Binární relace – vlastnosti

- **Reflexivní**: $\forall x \in A : (x, x) \in R$
- **Symetrická**: $\forall x, y \in A : (x, y) \in R \Rightarrow (y, x) \in R$
- **Antisymetrická**: $\forall x, y \in A : (x, y) \in R \wedge (y, x) \in R \Rightarrow x = y$
- **Asymetrická**: $\forall x, y \in A : (x, y) \in R \Rightarrow (y, x) \notin R$
- **Tranzitivní**: $\forall x, y, z \in A : (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$

Příklad 2

Na množině $M = \{a, b\}$ najděte všechny relace, které nejsou tranzitivní ani antisymetrické.

- **Ekvivalence**: reflexivní, symetrická, tranzitivní

Zobrazení

Definice

Nechť A a B jsou neprázdné množiny a f je binární relace mezi A a B. f se nazývá **zobrazení** *A do B, má-li následující vlastnosti:*

- $\forall a \in A, \exists b \in B : (a, b) \in f$.
- *Jestliže* $(a, b_1) \in f$ *a* $(a, b_2) \in f$, *pak* $b_1 = b_2$.

Zapisujeme: $f : A \to B$, $b = f(a)$.
b *je* **obraz** *prvku* a.
a *je* **vzor** *prvku* b.
$f(A) = \{f(a) | a \in A\}$ – **obraz množiny** A.

- **Surjekce**: Je-li $f(A) = B$.
- **Injekce**: $\forall x_1, x_2 \in A, x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$.
- **Bijekce**: Pokud je surjekce i injekce.

Binární operace

Definice

Binární operací *nazveme každé zobrazení* $f : A \times A \to A$.

Příklad 3

Rozhodněte, zda je operace $\circ$ *binární operací na* $\mathbb{Z}$.

$a \circ b = 3a + 3b$

Grupoid

Definice

Grupoidem *nazveme dvojici* $\langle S, * \rangle$*, kde* S *je množina a* $*$ *je binární operace na* S*.*

- **Komutativita**: $\forall a, b \in S : a * b = b * a$.
- **Asociativita**: $\forall a, b, c \in S : (a * b) * c = a * (b * c)$.
- **Neutrální prvek**: $\exists e \in S : \forall a \in S, a * e = e * a = a$.
- **Inverzní prvky**: $\forall a \in S, \exists a^{-1} \in S : a * a^{-1} = n_0$.

Příklad 4

Platí pro grupoid $\langle \mathbb{Z}, \circ \rangle$*, kde* $\circ$ *je definovaná* $a \circ b = 3a + 3b$ *asociativita, komutativita, existence neutrálního prvku a inverzních prvků?*

Struktury s jednou binární operací

$\langle S, * \rangle$

	$*$ binární operace	$*$ asociativní	$*$ komutativní	neutrální prvek	inverzní prvky
Grupoid	✓				
Pologrupa	✓	✓			
Monoid	✓	✓		✓	
Grupa	✓	✓		✓	✓
Abelovská grupa	✓	✓	✓	✓	✓

Izomorfismus

Definice

Nechť $\langle S, * \rangle$ a $\langle S', *' \rangle$ jsou dva grupoidy. Zobrazení $\phi : S \to S'$ nazveme **homomorfismus**, *jestliže $\forall x, y \in S$ platí*
$\phi(x * y) = \phi(x) *' \phi(y)$.
Je-li ϕ homomorfismus a bijekce, pak se nazývá **izomorfismus**.

Definice

Nechť $\langle S, * \rangle$ a $\langle S', *' \rangle$ jsou dva grupoidy. Pokud existuje izomorfismus $\phi : S \to S'$ nazveme grupoidy **izomorfní**.
Značíme: $S \simeq S'$.

Izomorfismus

Příklad 5

Rozhodněte, zda grupoidy $(A, \star)$ *a* $(B, \circ)$ *jsou izomorfní.* $A = \{1, 2, 3, 4\}$, $B = \{😐, 😊, ☹, 😶\}$ *a operace jsou dány následujícími tabulkami.*

$\star$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\circ$	😐	😊	☹	😶
😐	😐	😊	☹	😶
😊	😊	😶	😐	☹
☹	☹	😐	😶	😊
😶	😶	☹	😊	😐

Jak zjistíme, že jsou dva grupoidy izomorfní?

1. Definujeme $\phi : A \to B$
2. Ukážeme, že je ϕ bijektivní (surjektivní a injektivní)
3. Ukážeme, že je ϕ homomorfismus

Izomorfismus

Příklad

Rozhodněte, zda grupoidy $(A, \star)$ a $(B, \circ)$ jsou izomorfní. $A = \{1, 2, 3, 4\}$, $B = \{😐, 😊, ☹, 😶\}$ a operace jsou dány následujícími tabulkami.

$\star$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\circ$	😐	😊	☹	😶
😐	😐	😊	☹	😶
😊	😊	😶	😐	☹
☹	☹	😐	😶	😊
😶	😶	☹	😊	😐

Definujeme $\phi : A \to B$:

$\phi(1) =$ 😐
$\phi(2) =$ 😊
$\phi(3) =$ ☹
$\phi(4) =$ 😶

Ukážeme, že je ϕ bijektivní:

Surjekce ✓
Injekce ✓

Izomorfismus

Příklad

Rozhodněte, zda grupoidy $(A, \star)$ *a* $(B, \circ)$ *jsou izomorfní.* $A = \{1, 2, 3, 4\}$, $B = \{😐, 😀, ☹, 😶\}$ *a operace jsou dány následujícími tabulkami.*

$\star$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

$\circ$	😐	😀	☹	😶
😐	😐	😀	☹	😶
😀	😀	😶	😐	☹
☹	☹	😐	😶	😀
😶	😶	☹	😀	😐

Ukážeme, že je ϕ homomorfismus:
$\phi(x \star y) = \phi(x) \circ \phi(y)$.

Izomorfismus

Příklad 6

Mějme $2\mathbb{Z} = \{2n | n \in \mathbb{Z}\}$. Je $\langle \mathbb{Z}, + \rangle$ izomorfní s $\langle 2\mathbb{Z}, + \rangle$? + je klasické sčítání celých čísel.

Jak dokázat, že dva grupoidy NEJSOU izomorfní?

Izomorfismus

Jak dokázat, že dva grupoidy NEJSOU izomorfní?

- Neexistuje bijekce $\phi : S \to S'$ splňující podmínku homomorfismu.
- Zkoušet všechny bijekce a testovat podmínku homomorfismu je složité.
- Až na případ, kdy žádná bijekce neexistuje. **Kdy neexistuje žádná bijekce?**
- Bijekce neexistuje, pokud mají množiny různou kardinalitu.
- **Kardinalita** (mohutnost): počet prvků množiny.

Příklad 7

Grupoidy $\langle \mathbb{Q}, + \rangle$ *a* $\langle \mathbb{R}, + \rangle$ *nejsou izomorfní. Proč?*

Izomorfismus

Jak dokázat, že dva grupoidy NEJSOU izomorfní?

- Izomorfní grupoidy jsou grupoidy, které se chovají stejně.
- **Strukturální vlastnost** – je vlastnost, která je sdílená všemi izomorfnímu grupoidy.
- Pokud existuje bijektivní zobrazení $\phi : S \to S'$, pak při dokazování, že nejsou izomorfní hledáme strukturální vlastnost, kterou jedna má a druhá ne.

Příklad 8

Grupoidy $\langle \mathbb{Z}, \cdot \rangle$ a $\langle \mathbb{N}, \cdot \rangle$ nejsou izomorfní.

- Mají stejnou kardinalitu.
- Existuje bijekce (několik). **Uveďte nějakou.**
- V $\langle \mathbb{Z}, \cdot \rangle$ existují dva prvky, pro které platí $x = x \cdot x$ (1 a 0)
- V $\langle \mathbb{N}, \cdot \rangle$ existuje pouze jeden (1)

Strukturální vlastnost

Příklad 9

Které z následujícího jsou strukturální vlastnosti a které ne?

- *Množina má 4 prvky.*
- *Prvek* 🚗 *patří do množiny.*
- *Operace se značí + a nazývá se sčítání.*
- $x * x = x$, $\forall x \in S$.
- S *je podmnožina* $\mathbb{C}$.
- *Operace je komutativní.*
- *Rovnice* $a * x = b$ *má řešení* x *v* S *pro všechna* $a, b \in S$.

Strukturální vlastnost

Příklad

Které z následujícího jsou strukturální vlastnosti a které ne?

- *Množina má 4 prvky.* **ANO**
- *Prvek* 🚗 *patří do množiny.* **NE**
- *Operace se značí* $+$ *a nazývá se sčítání.* **NE**
- $x * x = x$, $\forall x \in S$. **ANO**
- S *je podmnožina* $\mathbb{C}$. **NE**
- *Operace je komutativní.* **ANO**
- *Rovnice* $a * x = b$ *má řešení* x *v* S *pro všechna* $a, b \in S$. **ANO**

Neutrální prvek

Definice

Nechť $\langle S, * \rangle$ je grupoid. Prvek $e \in S$ se nazývá **neutrální prvek** *pro $*$, pokud $e * s = s * e = s$ pro všechna $s \in S$.*

Věta 1

Grupoid $\langle S, * \rangle$ má nejvýše jeden neutrální prvek. Tj. pokud existuje neutrální prvek, tak je unikátní.

Důkaz

Předpokládejme, že e a $\overline{e}$ jsou dva neutrální prvky v S.

- *Protože e je neutrální prvek, platí $e * \overline{e} = \overline{e}$.*
- *Protože $\overline{e}$ je neutrální prvek, platí $\overline{e} * e = e$.*

Takže $e = \overline{e}$.

Zjevně je existence neutrálního prvku strukturální vlastnost.

Neutrální prvek

Věta 2

Předpokládejme, že $\langle S, * \rangle$ má neutrální prvek e. Pro isomorfismus $\phi : S \to S'$ platí, že $\phi(e)$ je neutrální prvek v S'.

Důkaz

Nechť $s' \in S'$. Musíme ukázat, že $\phi(e) *' s' = s' *' \phi(e) = s'$.
Protože ϕ je izomorfismus, je to bijekce $S \to S'$.
Existuje tedy $s \in S$ takové, že $\phi(s) = s'$.
Pro neutrální prvek $e \in S$ platí $e * s = s * e = s$.
Protože ϕ je funkce, dostaneme
$\phi(e * s) = \phi(s * e) = \phi(s)$.
To díky tomu, že je ϕ izomorfismus můžeme přepsat na
$\phi(e) *' \phi(s) = \phi(s) *' \phi(e) = \phi(s)$.
Vybrali jsme $s \in S$ takové, že $\phi(s) = s'$, dostaneme, tedy
$\phi(e) *' s' = s' *' \phi(e) = s'$.

Isomorfismus

Příklad 10

Dokažte, že grupoidy $\langle \mathbb{Q}, + \rangle$ a $\langle \mathbb{Z}, + \rangle$ nejsou isomorfní.

Isomorfismus

Příklad

Dokažte, že grupoidy $\langle \mathbb{Q}, + \rangle$ a $\langle \mathbb{Z}, + \rangle$ nejsou isomorfní.

- Obě množiny mají stejnou kardinalitu – existuje mnoho bijekcí.
- Musíme najít strukturální vlastnost, kterou jedna má a druhá ne.
- Rovnice $x + x = c$ má řešení pro všechna $c \in \mathbb{Q}$, ale ne v $\mathbb{Z}$.
  Například $x + x = 3$ nemá v Z řešení.

Isomorfismus

Příklad 11

Dokažte, že grupoidy $\langle M_2(\mathbb{R}), \cdot \rangle$ *(*$M_2(\mathbb{R})$ *je množina reálných matic* 2×2 *a* $\cdot$ *je klasické násobení matic) a* $\langle \mathbb{R}, \cdot \rangle$ *nejsou isomorfní.*

Isomorfismus

Příklad

Dokažte, že grupoidy $\langle M_2(\mathbb{R}), \cdot \rangle$ ($M_2(\mathbb{R})$ je množina reálných matic 2×2 a $\cdot$ je klasické násobení matic) a $\langle \mathbb{R}, \cdot \rangle$ nejsou isomorfní.

- Množiny mají stejnou kardinalitu.
- Násobení čísel je komutativní, ale násobení matic není.

Grupa

Definice

Grupoid $\langle G, * \rangle$ nazýváme **grupa**, *pokud je operace $*$ asociativní, v G existuje neutrální prvek a ke každému prvku existuje inverzní prvek.*
Řád grupy – *mohutnost množiny G ($|G|$).*
Abelovská grupa – *pokud je $*$ komutativní.*

Příklad 12

Rozhodněte, které z následujících grupoidů jsou grupy:

1. $\langle \mathbb{Z}^+, + \rangle$
2. $\langle \mathbb{Z}_0^+, + \rangle$
3. $\langle \mathbb{Z}, + \rangle$

Grupa

Příklad

Rozhodněte, které z následujících grupoidů jsou grupy:

1. $\langle \mathbb{Z}^+, + \rangle$
2. $\langle \mathbb{Z}_0^+, + \rangle$
3. $\langle \mathbb{Z}, + \rangle$

1. NE. Neexistuje neutrální prvek.
2. NE. Existuje neutrální prvek, ale ne inverze pro všechny prvky (např. 1).
3. ANO. Je to abelovská grupa.

Grupa

Příklad 13

Označme $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ *a definujme* $+_n : \mathbb{Z}_n \times \mathbb{Z}_n \to \mathbb{Z}_n$ *předpisem*
$a +_n b = (a + b)(\mod n)$
$\forall a, b \in \mathbb{Z}_n$.
Ukažte, že pro všechna $n \in \mathbb{N}$ *je* $\mathbb{Z}_n$ *abelovská grupa.*

Vlastnosti grup

Věta 3

Pokud $\langle G, * \rangle$ *je grupa, pak platí* **zákony krácení zleva i zprava**.
$a * b = a * c$ *implikuje* $b = c$
$b * a = c * a$ *implikuje* $b = c$
pro všechna $a, b, c \in G$.

Důkaz

Předpokládejme, že $a * b = a * c$. *V grupě existuje inverzní prvek* a' *k prvku* a.
$a' * (a * b) = a' * (a * c)$.
Dle asociativního zákona
$(a' * a) * b = (a' * a) * c$.
Protože $a' * a = e$ *dostaneme*
$e * b = e * c$
e *je neutrální prvek, tedy* $e * b = b$ *a odtud*
$b = c$.
Stejným způsobem bychom dokázali i $b * a = c * a$ *implikuje* $b = c$.

Vlastnosti grup

Věta 4

Pokud $\langle G, * \rangle$ je grupa, $a, b \in G$, pak $a * x = b$ a $y * a = b$ mají v G unikátní řešení.

Důkaz

Existence alespoň jednoho řešení:

Předpokládejme $a * x = b$. Řešení této rovnice je $a' * b$.

$a * (a' * b) = b$

Dle asociativity

$(a * a') * b = b$

Dle definice inverzního prvku

$e * b = b$

Dle vlastnosti neutrálního prvku e

$b = b$

Takže doopravdy je $a' * b$ řešením $a * x = b$.

Podobně má $y * a = b$ řešení $b * a'$.

Vlastnosti grup

Důkaz (Pokračování)

Unikátnost řešení:

Předpokládejme $a * x = b$ *má dvě řešení* x_1 *a* x_2.

$a * x_1 = b$ *a* $a * x_2 = b$.

Pak

$a * x_1 = a * x_2$.

Dle zákona o krácení

$x_1 = x_2$.

Podobně pro $y * a = b$.

Řešení rovnic $a * x = b$ a $y * a = b$ nemusí být obecně stejná. Pouze pokud je $*$ komutativní.

Vlastnosti grup

Věta 5

V grupě $\langle G, * \rangle$ existuje pro všechna $x \in G$ jen jeden neutrální prvek e
$e * x = x * e = x$.
Pro každý prvek $a \in G$ existuje pouze jeden prvek a'
$a' * a = a * a' = e$.

Důkaz

Unikátnost e:
Dokázali jsme ve Větě 1 pro grupoid.

Unikátnost a':
Předpokládejme, že $a \in G$ má dva inverzní prvky $a', a'' \in G$.
$a' * a = a * a' = e$ *a* $a'' * a = a * a'' = e$.
Pak
$a * a' = a * a''$
Dle zákona o krácení dostaneme
$a' = a''$

Vlastnosti grup

Důsledek 1

V grupě $\langle G, * \rangle$ *platí pro všechna* $a, b \in G$, *že* $(a * b)' = b' * a'$

Důkaz

$(a * b) * (a * b)' = e$
$(a * b) * (b' * a') = e$
$a * (b * b') * a' = e$
$a * e * a' = e$
$(a * e) * a' = e$
$a * a' = e$

Podgrupy

Definice

Pokud je $\langle G, * \rangle$ grupa a $H \subseteq G$ je uzavřená na $*$ a H s indukovanou operací $*$ je také grupa, pak říkáme, že $\langle H, * \rangle$ je **podgrupa** *grupy G.*
Zapisujeme $H \leq G$.

Definice

Pokud je $\langle G, * \rangle$ grupa a $H \subseteq G$. Řekneme, že H s indukovanou operací $*$ je **podgrupa** *grupy G, pokud platí*

- $\forall a, b \in H : a * b \in H$
- $e \in H$
- $\forall a \in H : a' \in H$

Podmínky v druhé definici můžeme nahradit jednou jedinou $\forall a, b \in H : a * b' \in H$.

Podgrupy

Příklad 14

Rozhodněte, zda platí:

- $\langle \mathbb{Z}, + \rangle \leq \langle \mathbb{R}, + \rangle$
- $\langle \{2k | k \in \mathbb{Z}\}, + \rangle \leq \langle \mathbb{Z}, + \rangle$
- $\langle \{0, 2, 4, \dots\}, + \rangle \leq \langle \mathbb{Z}, + \rangle$

Podgrupy

Příklad

Rozhodněte, zda platí:

- $\langle \mathbb{Z}, + \rangle \leq \langle \mathbb{R}, + \rangle$
- $\langle \{2k | k \in \mathbb{Z}\}, + \rangle \leq \langle \mathbb{Z}, + \rangle$
- $\langle \{0, 2, 4, \dots\}, + \rangle \leq \langle \mathbb{Z}, + \rangle$

- $\langle \mathbb{Z}, + \rangle \leq \langle \mathbb{R}, + \rangle$ ANO
- $\langle \{2k | k \in \mathbb{Z}\}, + \rangle \leq \langle \mathbb{Z}, + \rangle$ ANO
- $\langle \{0, 2, 4, \dots\}, + \rangle \leq \langle \mathbb{Z}, + \rangle$ NE, neobsahuje inverzní prvky

Podgrupy

Každá grupa G má dvě podgrupy: G a $\{e\}$

Definice

Podgrupa H grupy G se nazývá **nevlastní**, *pokud $H = G$. Ostatní podgrupy se nazývají* **vlastní**.

Definice

Podgrupa H grupy G se nazývá **triviální**, *pokud $H = \{e\}$. Ostatní podgrupy se nazývají* **netriviální**.

Podgrupy

Příklad 15

Existují dvě různé grupy řádu 4.

$\langle \mathbb{Z}_4, + \rangle$

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

Kleinova 4-grupa $\langle V = \{e, a, b, c\}, \circ \rangle$

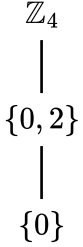
$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Najděte všechny netriviální podgrupy grupy $\langle \mathbb{Z}_4, + \rangle$.
Najděte všechny netriviální podgrupy grupy Kleinovy 4-grupy.
S jakou grupou je isomorfní grupa $\langle \{1, i, -1, -i\}, \cdot \rangle$*?*

Podgrupy

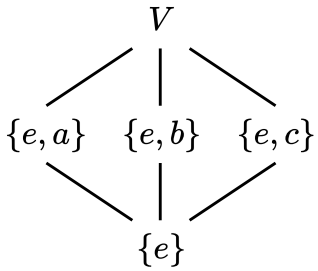
Najděte všechny netriviální podgrupy grupy $\langle \mathbb{Z}_4, + \rangle$.
Pouze podgrupa $\{0, 2\}$

Hessův diagram uspořádání $\leq$ – diagram, kde čára z G do H představuje vztah $H < G$.



Podgrupy

Najděte všechny netriviální podgrupy grupy Kleinovy 4-grupy V. $\{e, a\}$, $\{e, b\}$, $\{e, c\}$



Podgrupy

S jakou grupou je isomorfní grupa $\langle\{1, i, -1, -i\}, \cdot\rangle$?

$\mathbb{Z}_4$

$\langle \mathbb{Z}_4, + \rangle$

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

$\langle \{1, i, -1, -i\}, \cdot \rangle$

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Cyklické grupy

Věta 6

Nechť $\langle G, * \rangle$ *je grupa a* $a \in G$. *Pak*
$\langle H = \{a^n | n \in \mathbb{Z}\}, * \rangle$
$(a^n = \underbrace{a * \cdots * a}_{n\times}, a^0 = e)$
je nejmenší podgrupa grupy G, *která obsahuje* a.
Každá podgrupa obsahující a *obsahuje* H.

Důkaz

H je podgrupa:

- $\forall a, b \in H : a * b \in H$
  $a^r * a^s = a^{r+s}$ *pro* $r, s \in \mathbb{Z}$, *pak vidíme, že součin dvou prvků z* H *je opět v* H
- $e \in H$
  $a^0 = e$, *takže* $e \in H$
- $\forall a \in H : a' \in H$
  Pro $a^r \in H$ *máme* $a^{-r} \in H$, *takové že* $a^r * a^{-r} = a^0 = e$

Cyklické grupy

Důkaz (Pokračování)

H je nejmenší podgrupa obsahující a:
Každá podgrupa G obsahující a musí obsahovat H.

- *Podgrupa je uzavřená na operaci $*$, pokud obsahuje a musí obsahovat i a^n ($n \in \mathbb{N}$).*
- *Podgrupa musí obsahovat neutrální prvek a^0*
- *Podgrupa obsahující a musí obsahovat i jeho inverzi a^{-1} (a její násobky, tedy obecně a^{-n})*

Cyklické grupy

Příklad 16

Mějme grupu $\mathbb{Z}_{12}$, kolik prvků má podgrupa obsahující 3?

Cyklické grupy

Příklad

Mějme grupu $\langle \mathbb{Z}_{12}, + \rangle$, kolik prvků má podgrupa obsahující 3?

- $3 \in H$
- Obsahuje neutrální prvek $0 \in H$
- $3 + 3 = 6$, tj. $6 \in H$
- $6 + 3 = 9$, tj. $9 \in H$
- Inverze 3 je 9, inverze 6 je 6
- $H = \{0, 3, 6, 9\}$

Příklad 17

Mějme grupu $\langle \mathbb{Z}_{12}, + \rangle$. Jak vypadá nejmenší podgrupa obsahující 5?

Cyklické grupy

Definice

Nechť $\langle G, * \rangle$ je grupa a $a \in G$. Pak podgrupu $\langle H = \{a^n | n \in \mathbb{Z}\}, * \rangle$ nazýváme **cyklická podgrupa G generovaná prvkem** a.
Značíme $\langle a \rangle$.

Definice

Prvek a grupy G **generuje** *G a a je* **generátor** *grupy G, pokud $\langle a \rangle = G$.*

Definice

Pokud existuje prvek $a \in G$, který generuje G, grupu G nazýváme **cyklická grupa**.

Cyklické grupy

Příklad 18

Jsou následující grupy cyklické? Pokud ano, jaké mají generátory?

$\langle \mathbb{Z}_4, + \rangle$

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

Kleinova 4-grupa $\langle V = \{e, a, b, c\}, \circ \rangle$

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Cyklické grupy

Příklad

Je $\langle \mathbb{Z}_4, + \rangle$ cyklická? Pokud ano, jaké má generátory?

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

- ANO, je cyklická
- Generátory: 1 a 3
  $\langle 1 \rangle = \langle 3 \rangle = \mathbb{Z}_4$

Cyklické grupy

Příklad

Je Kleinova 4-grupa $\langle V = \{e, a, b, c\}, \circ \rangle$ cyklická? Pokud ano, jaké má generátory?

$\circ$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

- NE
- $\langle a \rangle$, $\langle b \rangle$, $\langle c \rangle$ jsou podgrupy o dvou prvcích
- $\langle e \rangle$ je podgrupa o jednom prvku

Cyklické grupy

Příklad 19

Grupa $\langle \mathbb{Z}, + \rangle$ je cyklická grupa. Jaké jsou její generátory?

Příklad 20

Grupy $\langle \mathbb{Z}_n, +_n \rangle$, kde $n \in \mathbb{N}$ jsou cyklické. Pokud $n > 1$, pak 1 a $n - 1$ jsou generátory. Může jich existovat více.

Cyklické grupy

Příklad 21

Uvažujme $\langle \mathbb{Z}, + \rangle$. Jak vypadá $\langle 3 \rangle$?

- Musí obsahovat 0
- Musí obsahovat 3 a všechny jeho násobky
  $3,\ 3+3=6,\ 3+3+3=9,\ \ldots$
- Musí obsahovat -3 a všechny jeho násobky
  $-3,\ -3+-3=-6,\ -3+-3+-3=-9,\ \ldots$
- Tuto grupu značíme $3\mathbb{Z}$
- Obecně $\langle n \rangle = n\mathbb{Z}$

Cyklické grupy

Definice

Nechť a je prvek grupy $\langle G, * \rangle$. Pokud je cyklická podgrupa grupy G konečná, pak **řád** a *je řád $|\langle a \rangle|$ této cyklické podgrupy.*
Pokud není cyklická grupa konečná, říkáme, že a je **nekonečného řádu**.

Jakého řádu jsou prvky, které generují G?

Příklad 22

Jaký má řád grupa $\langle \mathbb{Z}_6, + \rangle$? Určete řády všech prvků grupy a určete generátory této grupy.

Vlastnosti cyklických grup

Věta 7

Každá cyklická grupa je abelovská.

Důkaz

Nechť G *je cyklická grupa a* a *je její generátor*
$G = \langle a \rangle = \{a^n | n \in \mathbb{Z}\}$.
Pro $g_1, g_2 \in G$ *existuje* $r, s \in \mathbb{Z}$ *takové, že* $g_1 = a^r$ *a* $g_2 = a^s$.
Pak
$g_1 g_2 = a^r a^s = a^{r+s} = a^{s+r} = a^s a^r = g_2 g_1$.
Takže G *je abelovská.*

Vlastnosti cyklických grup

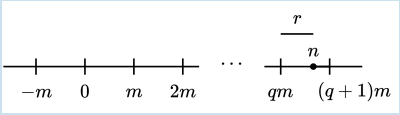
Věta 8 (Celočíselné dělení)

Pro $m \in \mathbb{N}$, $n \in \mathbb{Z}$ *existují unikátní čísla* $q, r \in \mathbb{Z}$ *taková, že* $n = mq + r$ *a* $0 \leq r \leq m$.
q *se nazývá* **(celočíselný) podíl** n *a* m.
r *se nazývá* **zbytek** *po dělení* n *číslem* m.

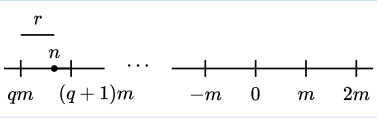
Důkaz

Triviální.

$n \geq 0$, $q \geq 0$



$n < 0$, $q < 0$



This meme is trivial and left as an exercise to the reader

Vlastnosti cyklických grup

Příklad 23

Najděte podíl q a zbytek r, když 38 vydělíme 7 dle předchozí věty.

- Kladné násobky 7: 7, 14, 21, 28, 35, 42, ...
- 35 je násobek 7, který nám dá nezáporný zbytek menší než 7
  $38 = 35 + 3 = 7(5) + 3$
- Podíl $q = 5$ a zbytek $r = 3$

Příklad 24

Najděte podíl q a zbytek r, když -38 vydělíme 7 dle předchozí věty.

Vlastnosti cyklických grup

Věta 9

Podgrupa cyklické grupy je také cyklická.

Důkaz

G je cyklická grupa generovaná prvkem a, H je podgrupa G.
Pokud $H = \{e\}$, pak $H = \langle e \rangle$ je cyklická.
Pokud $H \neq \{e\}$, pak $a^n \in H$ pro nějaké $n \in \mathbb{N}$.
Nechť $m \in \mathbb{N}$ je nejmenší číslo takové, že $a^m \in H$.
Tvrdíme, že $c = a^m$ generuje H. $H = \langle a^m \rangle = \langle c \rangle$.
Musíme ukázat, že každé $b \in H$ je mocnina c.
Protože $b \in H$ a $H \leq G$, máme, že $b = a^n$ pro nějaké n.
Z věty o celočíselném dělení najdeme q a r takové, že
$n = mq + r$ pro $0 \leq r < m$.
Pak $a^n = a^{mq+r} = (a^m)^q a^r$, takže $a^r = (a^m)^{-q} a^n$.
Protože $a^n \in H$, $a^m \in H$ a H je grupa, takže $(a^m)^{-q} \in H$.

Vlastnosti cyklických grup

Důkaz (Pokračování)

Protože m je nejmenší číslo v $\mathbb{N}$ takové, že $a^m \in H$ a $0 \leq r < m$, musíme mít $r = 0$.
To znamená, že $n = qm$ a
$b = a^n = (a^m)^q = c^q$
a tedy že b je mocnina c.

Důsledek 2

Podgrupy $\mathbb{Z}$ se sčítáním jsou právě grupy $n\mathbb{Z}$ pro $n \in \mathbb{Z}$.

Největší společný dělitel

Definice

Nechť $r, s \in \mathbb{N}$. *Kladný generátor* d *cyklické grupy*
$H = \{nr + ms | n, m \in \mathbb{Z}\}$
se sčítáním, je **největší společný dělitel** *(gcd)* r *a* s.
Zapisujeme $d = gcd(r, s)$.

- d je dělitel r i s, protože $r = 1r + 0s$ a $s = 0r + 1s$
- Protože $d \in H$, dá se vyjádřit pomocí r a s: $d = nr + ms$, pro nějaká $n, m \in \mathbb{Z}$.
- Každé celé číslo, které je dělitelem r i s dělí d (dělí pravou stranu rovnice, musí dělit i levou).
- d tedy musí být největší číslo, které je dělitelem r i s.

Největší společný dělitel

Příklad 25

Najděte $gcd(42, 72)$.

- Kladní dělitelé 42: 1, 2, 3, 6, 7, 14, 21 a 42
- Kladní dělitelé 72: 1, 2, 3, 6, 8, 9, 12, 18, 24, 36 a 72
- Největší společný dělitel je 6
- $6 = (3)(72) + (-5)(42)$

Příklad 26

Určete $gcd(12, 25)$.

Největší společný dělitel

Definice

Dvě přirozená čísla se nazývají **nesoudělná** *(též* **relativní prvočísla***), pokud je jejich* $gcd()$ *roven* 1*.*

Tvrzení

Pokud r *a* s *jsou nesoudělná a pokud* r *dělí* sm*, pak* r *dělí* m*.*

Důkaz

Pokud jsou r *a* s *nesoudělná, můžeme napsat* $1 = ar + bs$*, pro nějaká* $a, b \in \mathbb{Z}$*.*
Násobením m *dostaneme* $m = arm + bsm$*.*
Teď r *dělí i* arm *i* bsm*, protože* r *dělí* sm*.*
Takže je r *dělitelem i levé strany, tj.* r *dělí* m*.*

Struktura cyklických grup

Věta 10

Nechť je cyklická grupa s generátorem a.

- *Pokud je řád G nekonečný, je G isomorfní s $\langle \mathbb{Z}, + \rangle$.*
- *Pokud má G konečný řád n, je G isomorfní s $\langle \mathbb{Z}_n, +_n \rangle$.*

Důkaz

G má nekonečný řád: $\forall m \in \mathbb{N},\ a^m \neq e$

Tvrdíme, že žádné dva různé exponenty h a k nám nedají stejné prvky a^h a a^k v G.
Předpokládejme, že $a^h = a^k$ a $h > k$. Pak
$a^h a^{-k} = a^{h-k} = e$,
což je v rozporu s předpokladem.
Každý prvek tedy může být vyjádřen jako a^z pro unikátní $z \in \mathbb{Z}$.

Struktura cyklických grup

Důkaz (Pokračování)

Izomorfismus pro nekonečný řád:

Žádné dva různé exponenty h a k nám nedají stejné prvky a^h a a^k v G.
Zobrazení $\phi : G \to \mathbb{Z}$ dané $\phi(a^i) = i$ je bijektivní.
Navíc platí $\phi(a^i a^j) = \phi(a^{i+j}) = i + j = \phi(a^i) + \phi(a^j)$
tedy ϕ je izomorfismus.

Struktura cyklických grup

Důkaz (Pokračování)

G má řád n: Pro nějaké $m \in \mathbb{N}$, $a^m = e$.
Nechť n je nejmenší kladné číslo takové, že $a^n = e$.
Pokud $s \in \mathbb{Z}$ a $s = nq + r$ pro $0 \leq r < n$, pak
$a^s = a^{nq+r} = (a^n)^q a^r = e^q a^r = a^r$
Pokud $0 < k < h < n$ a $a^h = a^k$, tak $a^{h-k} = e$ a $0 < h - k < n$.
To je v rozporu s výběrem n, takže prvky
$a^0 = e, a, a^2, \ldots, a^{n-1}$ *jsou všechny různé a jsou to prvky G.*
Izomorfismus:
Zobrazení $\phi : G \to \mathbb{Z}_n$ dané $\phi(a^i) = i$ pro $i = 0, 1, \ldots n-1$ je tedy bijekce G na $\mathbb{Z}_n$.
Protože $a^n = e$, vidíme, že $a^i a^j = a^k$, kde $k = i +_n j$.
$\phi(a^i a^j) = i +_n j = \phi(a^i) +_n \phi(a^j)$.
ϕ je izomorfismus.