Cykly, orbity a alternující grupy

Algebra 2

Mgr. Markéta Trnečková, Ph.D.

Palacký University, Olomouc

Třídy ekvivalence

Připomenutí:

- **Ekvivalencí** nazýváme binární relaci R na množině X, která je reflexivní, tranzitivní a symetrická.
- Relace ekvivalence určuje jednoznačně **rozklad množiny** (faktormnožinu) X na třídy ekvivalence.
- **Rozkladem** rozumíme takovou množinu $Y \subseteq \mathcal{P}(X)$ podmnožin množiny X takovou, že sjednocením této množiny dostaneme X a každé dva prvky Y jsou disjunktní.
- **Třídy ekvivalence** jsou právě podmnožiny X, přičemž každá třída ekvivalence obsahuje právě všechny takové prvky z množiny X, že každé dva v rámci této třídy jsou navzájem ekvivalentní ve smyslu dané relace.
- Platí to i naopak – každý rozklad Y množiny X určuje jednoznačně právě jednu relaci ekvivalence.

Třídy ekvivalence

Tvrzení

Každá permutace σ množiny A označuje přirozený rozklad A do tříd takových, že $a, b \in A$ jsou ve stejné třídě, právě když $b = \sigma^n(a)$ pro nějaké $n \in \mathbb{Z}$.

Jde tedy o rozklad daný relací ekvivalence $\sim$:
$a \sim b$, právě když $b = \sigma^n(a)$ pro nějaké $n \in \mathbb{Z}$. Pro všechna $a, b \in A$.

Důkaz

Ověříme, že jde o ekvivalenci.
Reflexivita: Zjevné. $a \sim a$, protože $a = \iota(a) = \sigma^0(a)$.
Symetrie: Pokud $a \sim b$, tak $b = \sigma^n(a)$ pro nějaké $n \in \mathbb{Z}$. Pak ale $a = \sigma^{-n}(b)$ a tak $b \sim a$.
Tranzitivita: Pokud $a \sim b$ a $b \sim c$, pak $b = \sigma^n(a)$ a $c = \sigma^m(b)$ pro nějaké $n, m \in \mathbb{Z}$.
Substitucí dostaneme $c = \sigma^m(\sigma^n(a)) = \sigma^{n+m}(a)$ a tedy $a \sim c$.

Orbity

Definice

Nechť σ je permutace množiny A. Třídy ekvivalence $\sim$ se nazývají **orbity**.

Příklad 37

Orbity permutace ι jsou všechny jednoprvkové podmnožiny množiny A.

Příklad 38

Najděte orbity permutace σ:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$$

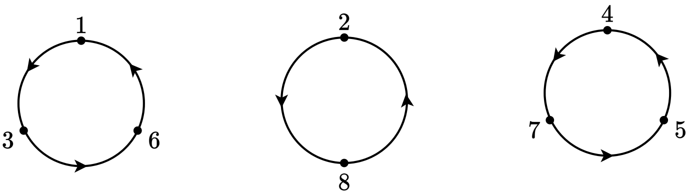
Orbity

Příklad

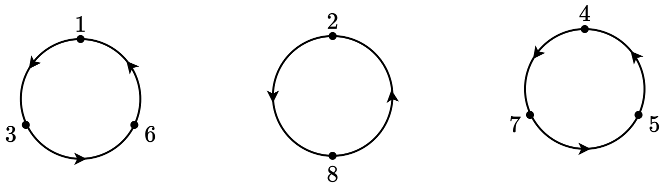
Najděte orbity permutace σ:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}$$

- Orbita obsahující 1.
  $1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma} 6 \xrightarrow{\sigma} 1 \xrightarrow{\sigma} 3 \xrightarrow{\sigma}$
  $\dots$
  Tedy: $\{1, 3, 6\}$
- Orbita obsahující 2:
  $2 \xrightarrow{\sigma} 8 \xrightarrow{\sigma} 2 \xrightarrow{\sigma} \dots$
  Orbita: $\{2, 8\}$
- Orbita obsahující 4:
  $4 \xrightarrow{\sigma} 7 \xrightarrow{\sigma} 5 \xrightarrow{\sigma} 4 \xrightarrow{\sigma} \dots$
  Orbita: $\{4, 5, 7\}$



Orbity



- Každá kružnice vyjadřuje permutaci v S_8.
- První je permutace
  $$\mu = \begin{pmatrix} \mathbf{1} & 2 & \mathbf{3} & 4 & 5 & \mathbf{6} & 7 & 8 \\ \mathbf{3} & 2 & \mathbf{6} & 4 & 5 & \mathbf{1} & 7 & 8 \end{pmatrix}$$
  Rotuje 1, 3 a 6 stejně jako σ a ostatní nechává na místě.

Příklad 39

Jak vypadají orbity permutace μ?

Orbity

Příklad

Jak vypadají orbity permutace μ?

- Orbity: $\{1, 3, 6\}$, $\{2\}$, $\{4\}$, $\{5\}$, $\{7\}$, $\{8\}$
- Na zakreslení této orbity by nám stačila jedna kružnice. Jednoprvkové vynecháváme.
- Permutacím, které můžeme vyjádřit jednou orbitou, říkáme **cykly**.

Definice

Permutace $\sigma \in S_n$ je **cyklus**, *pokud má nejvýše jednu orbitu obsahující více než jeden prvek.*
Délka *cyklu je počet prvků v největší orbitě.*

Cykly

Příklad 40

Rozhodněte, zda je permutace σ cyklus a pokud ano, jaká je jeho délka?

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 3 & 4 & 5 & 6 & 7 & 2 & 8 & 9 & 10 \end{pmatrix}$$

Cykly

Příklad

Rozhodněte, zda je permutace σ cyklus a pokud ano, jaká je jeho délka?

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 1 & 3 & 4 & 5 & 6 & 7 & 2 & 8 & 9 & 10 \end{pmatrix}$$

- Ano. Délka cyklu je 6.

- Zjednodušená notace – cyklus budeme zapisovat následujícím způsobem $\sigma = (2, 3, 4, 5, 6, 7)$
  Ale také $\sigma = (3, 4, 5, 6, 7, 2)$, $\sigma = (4, 5, 6, 7, 2, 3)$ ...
- Toto budeme chápat tak, že
  $2 \xrightarrow{\sigma} 3$, $3 \xrightarrow{\sigma} 4$, $4 \xrightarrow{\sigma} 5$, $5 \xrightarrow{\sigma} 6$, $6 \xrightarrow{\sigma} 7$, $7 \xrightarrow{\sigma} 2$
- Vše, co se v této notaci nevyskytuje, nechá na místě.
- Jediný problém, že z tohoto zápisu nevyčteme množinu, na které je σ definovaná.

Cykly

Cykly jsou speciální permutace, můžeme s nimi provádět permutační součin.

Věta 16

Každá permutace σ konečné množiny je součin disjunktních cyklů.

Disjunktní cykly jsou cykly, kde v žádných dvou cyklech není stejné číslo.

Důkaz

Nechť $B_1, B_2, \ldots, B_r$ jsou orbity σ a μ_i je cyklus definovaný jako

$$\mu_i(x) = \begin{cases} \sigma(x) & \text{pro } x \in B_i \\ x & \text{jinak} \end{cases}$$

Zjevně $\sigma = \mu_1 \mu_2 \ldots \mu_r$.

Protože B_i jsou třídy ekvivalence, tak jsou disjunktní, a tedy i μ_i jsou disjunktní, pro $i \in \{1, \ldots, r\}$.

Cykly

Poznámky:

- Součin cyklů obecně nemusí být cyklus.
  Například:
  $$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} = (1,3,6)(2,8)(4,7,5)$$
- Permutační součin obecně není komutativní, násobíme-li disjunktní cykly, můžeme jejich pořadí zaměňovat.
- Protože jsou orbity permutace unikátní, reprezentace permutace jakou součin disjunktních cyklů (z nichž žádný není identita) je unikátní, až na pořadí činitelů.

Příklad 41

Vyjádřete permutaci σ jako součin disjunktních cyklů.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}$$

Cykly

Příklad

Vyjádřete permutaci σ jako součin disjunktních cyklů.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix}$$

- Cykly: $(1,6)$, $(2,5,3)$
- Prvek 4 nemění pozici
- Vyjádření:
$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 4 & 3 & 1 \end{pmatrix} = (1,6)(2,5,3)$$
- Nebo také $(2,5,3)(1,6)$

Příklad 42

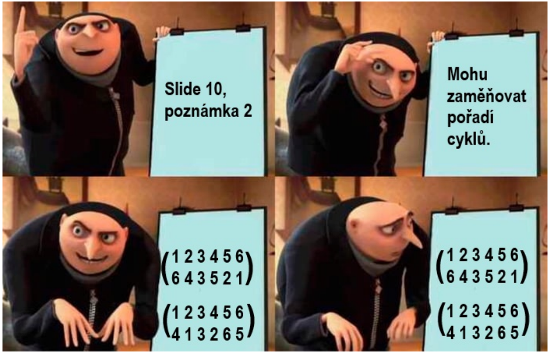
Uvažujme cykly $(1,4,5,6)$ a $(2,1,5)$ v S_6. Jak vypadá permutační součin těchto cyklů?

Cykly

Příklad

Uvažujme cykly $(1,4,5,6)$ *a* $(2,1,5)$ *v* S_6. *Jak vypadá permutační součin těchto cyklů?*

- $(1,4,5,6)(2,1,5) =$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 4 & 3 & 5 & 2 & 1 \end{pmatrix}$$
- $(2,1,5)(1,4,5,6) =$
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix}$$
- Jak je možné, že jsou výsledky různé?
- Jsou výsledné součiny cykly?



Transpozice

Definice

Cyklus délky 2 se nazývá **transpozice***.*

- Zjevně každé přeuspořádání posloupnosti $1, 2, \ldots, n$ může být dosaženo opakovanými záměnami dvojic čísel.
- Transpozice vymění dvě čísla a ostatní nechává na místě.
- Každý cyklus můžeme vyjádřit jako permutační součin transpozic.
- Zjevně platí:
  $(a_1, a_2, \ldots, a_n) = (a_1, a_n)(a_1, a_{n-1}) \ldots (a_1, a_3)(a_1, a_2)$

Příklad 43

Vyjádřete cyklus $(1, 4, 5, 6)$ na S_6 jako součin transpozic.

Transpozice

Příklad

Vyjádřete cyklus $(1,4,5,6)$ *na* S_6 *jako součin transpozic.*

- $(1,4,5,6) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 5 & 6 & 1 \end{pmatrix}$
- $(1,4,5,6) = (1,6)(1,5)(1,4)$
- $(1,4)$: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 1 & 5 & 6 \end{pmatrix}$
- $(1,5)$: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 5 & 1 & 6 \end{pmatrix}$
- $(1,6)$: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 5 & 6 & 1 \end{pmatrix}$

Transpozice

Důsledek 4 (Věty 16)

Libovolná permutace konečné množiny o alespoň dvou prvcích je součin transpozic.

Příklad 44

Vyjádřete permutaci $\sigma = (1,6)(2,5,3)$ *jakou součin transpozic.*

Transpozice

Příklad

Vyjádřete permutaci $\sigma = (1,6)(2,5,3)$ *jakou součin transpozic.*

$(1,6)(2,5,3) = (1,6)(2,3)(2,5)$

Můžeme vyjádřit i jiným způsobem?

Příklad 45

Jak vyjádříme identitu v S_n *(*$n \geq 2$*) jako součin transpozic?*

Transpozice

Příklad

Jak vyjádříme identitu v S_n $(n \geq 2)$ jako součin transpozic?

$(1, 2)(2, 1)$

Poznámky:

- Každou permutaci konečné množiny s alespoň dvěma prvky je možné vyjádřit součinem transpozic.
- Transpozice nemusí být disjunktní.
- Permutace není jedinečná.
- Počet transpozic použitých k reprezentaci dané permutace musí být buď vždy sudý, nebo vždy lichý.

Transpozice

Věta 17

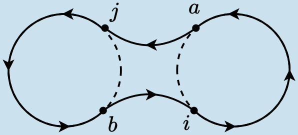
Žádná permutace v S_n nemůže být vyjádřena jako součin sudého počtu transpozic i lichého počtu transpozic.

Ve skriptech naleznete důkaz i pomocí lineární algebry.

Důkaz

Nechť $\sigma \in S_n$ a $\tau = (i, j)$ je transpozice v S_n. Tvrdíme, že počet orbit σ a $\sigma\tau$ se liší o 1.

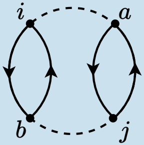
Předpokládejme, že i a j jsou v <u>různých orbitách</u> σ.
Zapíšeme σ jako součin disjunktních cyklů – první bude obsahovat j a druhý i.
Můžeme to zapsat jako $(b, j, \times, \times, \times)(a, i, \times, \times, \times)$
Součinem s τ dostaneme $\tau\sigma = (i, j)\sigma$
$(i, j)(b, j, \times, \times, \times)(a, i, \times, \times, \times) = (a, j, \times, \times, \times, b, i, \times, \times, \times)$



Transpozice

Důkaz

Předpokládejme, že i a j jsou ve stejné orbitě σ.
Můžeme pak orbitu zapsat jako $(a, i, \times, \times, \times, b, j, \times, \times, \times)$
Součinem dostaneme $\tau\sigma = (i, j)\sigma$
$(i, j)(a, i, \times, \times, \times, b, j, \times, \times, \times) = (a, j, \times, \times, \times)(b, i, \times, \times, \times)$
Původní orbita je rozdělena na dvě.



Ukázali jsme, že počet orbit $\tau\sigma$ se liší od počtu orbit σ o 1. Permutace identity ι má n orbit. Takže počet orbit dané permutace $\sigma \in S_n$ se liší od n buďto o liché nebo o sudé číslo, ne obojí.

Liché/sudé permutace

Definice

Permutace konečné množiny je **lichá** *nebo* **sudá***, podle toho, jestli ji lze vyjádřit jako součin sudého, nebo lichého počtu transpozic.*

Příklad 46

Určete jestli jsou následující permutace v S_6 liché nebo sudé.

1. *Identita ι.*
2. *Permutace $(1, 4, 5, 6)(2, 1, 5)$*

Liché/sudé permutace

Příklad

Určete jestli jsou následující permutace v S_6 liché nebo sudé.

1. *Identita* ι.
2. *Permutace* $(1,4,5,6)(2,1,5)$

1. Protože $\iota = (1,2)(2,1)$, pak je sudá.
2. Permutaci $(1,4,5,6)(2,1,5)$ můžeme vyjádřit pomocí transpozic následovně:
   $(1,6)(1,5)(1,4)(2,5)(2,1)$,
   což je 5 transpozic, tedy je lichá.

Alternující grupy

Věta 18

Pokud $n \geq 2$, tak kolekce všech sudých permutací množiny $\{1, 2, \ldots, n\}$ tvoří grupu řádu $n!/2$ symetrické grupy S_n.

Důkaz

Počet prvků S_n je $n!$. My tvrdíme, že počet sudých permutací je $n!/2$ (tedy je stejný počet sudých a lichých permutací).
Nechť A_n je množina sudých permutací v S_n a B_n je množina lichých permutací.
Definujeme bijekci $A_n \to B_n$ (to stačí k tomu, abychom dokázali, že mají stejný počet prvků).
Nechť τ je pevně daná transpozice v S_n. Ta existuje, protože $n \geq 2$. Bez újmy na obecnosti si zvolíme třeba $\tau = (1, 2)$.
Definujeme zobrazení $\lambda_\tau(\sigma) = \tau\sigma$.
Zjevně, pokud je σ sudá, je $\tau\sigma$ lichá. Je to tedy doopravdy zobrazení do B_n.
Pokud by pro $\sigma, \mu \in A_n$ platilo $\lambda_\tau(\sigma) = \lambda_\tau(\mu)$, pak $(1, 2)\sigma = (1, 2)\mu$ a protože S_n je grupa, máme $\sigma = \mu$ – je injektivní.

Alternující grupy

Důkaz (Pokračování)

$\tau = (1,2) = \tau^{-1}$, *takže pro* $\rho \in B_n$ *platí*
$\tau^{-1}\rho \in A_n$ *a* $\lambda_\tau(\tau^{-1}\rho) = \tau(\tau^{-1}\rho) = \rho$
– je surjektivní.
Chceme dokázat, že se jedná o grupu.
Součin dvou sudých permutací je opět sudý. (uzavřenost)
Pro $n \geq 2$, *má* S_n *transpozici* $(1,2)$ *a* $\iota = (1,2)(1,2)$ *je sudá permutace. (existence neutrálního prvku).*
Pokud je ρ *vyjádřeno jako součin transpozic, vzato v opačném pořadí je* ρ^{-1}. *Inverze sudé permutace je zase sudá permutace. (existence inverzních prvků).*

Definice

Podgrupu grupy S_n *sestávající se ze sudých permutací nazýváme* **alternující grupa***.*
Značíme A_n.

Levé a pravé třídy grup

Věta 19

Nechť H je podgrupa G. Definujme relace $\sim_L$ a $\sim_R$ na G takto:
$a \sim_L b$, právě když $a^{-1}b \in H$,
$a \sim_R b$, právě když $ab^{-1} \in H$.
Pak $\sim_L$ a $\sim_R$ jsou ekvivalence na G.

Důkaz

Ukážeme, že $\sim_L$ je ekvivalence (u $\sim_R$ bychom postupovali obdobně).
Reflexivita: Nechť $a \in G$. Pak $a^{-1}a = e$ a $e \in H$ (H je podgrupa). Takže $a \sim_L a$.
Symetrie: Předpokládáme, že $a \sim_L b$. Pak $a^{-1}b \in H$. Protože H je podgrupa $(a^{-1}b)^{-1} \in H$ a $(a^{-1}b)^{-1} = b^{-1}a$, takže $b^{-1}a \in H$ a tedy $b \sim_L a$.
Tranzitivita: Nechť $a \sim_L b$ a $b \sim_L c$. Pak $a^{-1}b \in H$ a $b^{-1}c \in H$. Protože H je podgrupa $(a^{-1}b)(b^{-1}c) \in H$. $(a^{-1}b)(b^{-1}c) = a^{-1}c$. Takže $a \sim_L c$.

Levé a pravé třídy grup

- Víme, že ekvivalence indukuje rozklad.
- Předpokládejme, že $a \in G$. Třída obsahující a obsahuje všechna $x \in G$ taková, že $a \sim_L x$.
- Tedy taková x, pro která platí $a^{-1}x \in H$.
- $a^{-1}x = h$ pro nějaké $h \in H$. Nebo také jinak, když platí $x = ah$ pro nějaké $h \in H$.
- Třída obsahující a je $\{ah | h \in H\}$.
- Označíme si to aH.
- Obdobně třída rozkladu odpovídající $\sim_R$ obsahující $a \in G$ značíme Ha a vypadá následovně $\{ha | h \in H\}$.

Definice

Nechť H je podgrupa grupy G.
Podmnožina $aH = \{ah | h \in H\}$ je **levá třída** *H obsahující a.*
Podmnožina $Ha = \{ha | h \in H\}$ je **pravá třída** *H obsahující a.*

Levé a pravé třídy grup

Příklad 47

Jak vypadají levé třídy podgrupy $3\mathbb{Z}$ grupy $\mathbb{Z}$?

Levé a pravé třídy grup

Příklad

Jak vypadají levé třídy podgrupy $3\mathbb{Z}$ grupy $\mathbb{Z}$?

Levou třídu $3\mathbb{Z}$ je $m + 3\mathbb{Z}$

- Pro $m = 0$:
  $0 + 3\mathbb{Z} = \{\dots, -9, -6, -3, 0, 3, 6, 9, \dots\}$
- Pro $m = 1$:
  $1 + 3\mathbb{Z} = \{\dots, -8, -5, -2, 1, 4, 7, 10, \dots\}$
- Pro $m = 2$:
  $2 + 3\mathbb{Z} = \{\dots, -7, -4, -1, 2, 5, 8, 11, \dots\}$

Zjevně jsou tyto tři třídy rozkladem $\mathbb{Z}$.

Jak by vypadaly pravé třídy rozkladu?

Levé a pravé třídy grup

Tvrzení

Pro podgrupu H abelovské grupy G, jsou rozklady G na levé a pravé třídy podgrupy H stejné.

Příklad 48

Grupa $\mathbb{Z}_6$ je abelovská. Najděte rozklad $\mathbb{Z}_6$ na třídy podle podgrupy $H = \{0, 3\}$.

Levé a pravé třídy grup

Příklad

Grupa $\mathbb{Z}_6$ je abelovská. Najděte rozklad $\mathbb{Z}_6$ na třídy podle podgrupy $H = \{0, 3\}$.

- Třída obsahující 0: $\{0, 3\}$.
- Třída obsahující 1: $1 + \{0, 3\} = \{1, 4\}$.
- Třída obsahující 2: $2 + \{0, 3\} = \{2, 5\}$.

$+_6$	0	3	1	4	2	5
0	0	3	1	4	2	5
3	3	0	4	1	5	2
1	1	4	2	5	3	0
4	4	1	5	2	0	3
2	2	5	3	0	1	4
4	5	2	0	3	4	1

Třídy rozkladu spolu s operací, kterou vidíme v tabulce (operace na 3 barvách) tvoří grupu. Později si tuto grupu pojmenujeme **faktorová grupa**.

Levé a pravé třídy grup

Příklad 49

Pro symetrickou grupu S_3 vezmeme její podgrupu $\langle \mu_1 \rangle = \{\rho_0, \mu_1\}$. Najděte její levé a pravé třídy dle této podgrupy.

Grupa S_3:

$$\rho_0 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \rho_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \rho_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

$$\mu_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \mu_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \mu_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Permutační součin můžeme popsat tabulkou:

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Levé a pravé třídy grup

Příklad

Pro symetrickou grupu S_3 vezmeme její podgrupu $\langle \mu_1 \rangle = \{\rho_0, \mu_1\}$. Najděte její levé a pravé třídy dle této podgrupy.

- Levé:
  $H = \{\rho_0, \mu_1\}$
  $\rho_1 H = \{\rho_1\rho_0, \rho_1\mu_1\} = \{\rho_1, \mu_3\}$
  $\rho_2 H = \{\rho_2\rho_0, \rho_2\mu_1\} = \{\rho_2, \mu_2\}$
- Pravé:
  $H = \{\rho_0, \mu_1\}$
  $H\rho_1 = \{\rho_0\rho_1, \mu_1\rho_1\} = \{\rho_1, \mu_2\}$
  $H\rho_2 = \{\rho_0\rho_2, \mu_1\rho_2\} = \{\rho_2, \mu_3\}$

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Rozklady jsou různé.

Levé a pravé třídy grup

- Levé:
  $H = \{\rho_0, \mu_1\}$
  $\rho_1 H = \{\rho_1\rho_0, \rho_1\mu_1\} = \{\rho_1, \mu_3\}$
  $\rho_2 H = \{\rho_2\rho_0, \rho_2\mu_1\} = \{\rho_2, \mu_2\}$

$\circ$	ρ_0	μ_1	ρ_1	μ_3	ρ_2	μ_2
ρ_0	ρ_0	μ_1	ρ_1	μ_3	ρ_2	μ_2
μ_1	μ_1	ρ_0	μ_2	ρ_2	μ_3	ρ_1
ρ_1	ρ_1	μ_3	ρ_2	μ_2	ρ_0	μ_1
μ_3	μ_3	ρ_1	μ_1	ρ_0	μ_2	ρ_2
ρ_2	ρ_2	μ_2	ρ_0	μ_1	ρ_1	μ_3
μ_2	μ_2	ρ_2	μ_3	ρ_1	μ_1	ρ_0

- Pravé:
  $H = \{\rho_0, \mu_1\}$
  $H\rho_1 = \{\rho_0\rho_1, \mu_1\rho_1\} = \{\rho_1, \mu_2\}$
  $H\rho_2 = \{\rho_0\rho_2, \mu_1\rho_2\} = \{\rho_2, \mu_3\}$

$\circ$	ρ_0	μ_1	ρ_1	μ_2	ρ_2	μ_3
ρ_0	ρ_0	μ_1	ρ_1	μ_2	ρ_2	μ_3
μ_1	μ_1	ρ_0	μ_2	ρ_1	μ_3	ρ_2
ρ_1	ρ_1	μ_3	ρ_2	μ_1	ρ_0	μ_2
μ_2	μ_2	ρ_2	μ_3	ρ_0	μ_1	ρ_1
ρ_2	ρ_2	μ_2	ρ_0	μ_3	ρ_1	μ_1
μ_3	μ_3	ρ_1	μ_1	ρ_2	μ_2	ρ_0

Z tabulek vidíme, že ani v jednom případě nedostaneme grupu.

Levé a pravé třídy grup

Příklad 50

Vypočítejte levé a pravé třídy pro podgrupu $\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$

Levé a pravé třídy grup

Příklad

Vypočítejte levé a pravé třídy pro podgrupu $\langle \rho_1 \rangle = \{\rho_0, \rho_1, \rho_2\}$

- <u>Levé</u>:
  $H = \{\rho_0, \rho_1, \rho_2\}$
  $\mu_1 H = \{\mu_1\rho_0, \mu_1\rho_1, \mu_1\rho_2\} = \{\mu_1, \mu_2, \mu_3\}$

$\circ$	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_0	ρ_0	ρ_1	ρ_2	μ_1	μ_2	μ_3
ρ_1	ρ_1	ρ_2	ρ_0	μ_3	μ_1	μ_2
ρ_2	ρ_2	ρ_0	ρ_1	μ_2	μ_3	μ_1
μ_1	μ_1	μ_2	μ_3	ρ_0	ρ_1	ρ_2
μ_2	μ_2	μ_3	μ_1	ρ_2	ρ_0	ρ_1
μ_3	μ_3	μ_1	μ_2	ρ_1	ρ_2	ρ_0

Třídy jsou stejné a zjevně dostáváme grupu isomorfní se $\mathbb{Z}_2$

Levé a pravé třídy grup

Tvrzení

Každá třída (levá i pravá) rozkladu grupy G dle podgrupy H má stejný počet prvků, jako H.

Důkaz

Předpokládáme, že $H \leq G$. Chceme ukázat, že každá třída má stejný počet prvků. Navíc je tento počet stejný, jako počet prvků H.
Najdeme bijektivní zobrazení $H \to gH$ podgrupy pro pevně zvolené $g \in G$.
$\phi(h) = gh$ pro $h \in H$.
Toto zobrazení je zjevně surjektivní. Musíme dokázat ještě, že je injektivní.
Uvažujme $\phi(h_1) = \phi(h_2)$, pro $h_1, h_2 \in H$.
Pak $gh_1 = gh_2$. Díky větě o krácení máme $h_1 = h_2$.
Stejným způsobem bychom dokazovali i zobrazení pro pravé třídy $\phi' : H \to Hg$.

Lagrangeova věta

Věta 20 (Lagrangeova věta)

Nechť H je podgrupa konečné grupy G. Pak $|H|$ je dělitel $|G|$.

Důkaz

Nechť $n = |G|$ a $m = |H|$.
Víme, že každá třída rozkladu G dle H má m prvků.
Nechť r je počet tříd v rozkladu G dle H.
Pak musíme mít $n = rm$, takže m je skutečně dělitel n.

Lagrangeova věta

Důsledek 5

Každá grupa s prvočíselným řádem je cyklická.

Důkaz

Nechť G *je grupa s prvočíselného řádu a* $a \in G$, $a \neq e$.
Pak cyklická podgrupa $\langle a \rangle$ *má alespoň dva prvky* a *a* e.
Ale podle Lagrangeovy věty musí řád $m \geq 2$ *podgrupy* $\langle a \rangle$ *dělit prvočíslo* p. *Musíme tedy mít* $m = p$ *a* $\langle a \rangle = G$. *Tedy* G *je cyklická.*

Protože víme, že každá cyklická grupa řádu p je isomorfní s $\mathbb{Z}_p$, vidíme, že existuje jenom jedna grupa (až na isomorfismy) daného řádu.

Lagrangeova věta

Věta 21

Řád prvku konečné grupy je dělitelem řádu té grupy.

Důkaz

Protože víme, že řád prvku je totéž jako řád cyklické podgrupy generované tímto prvkem, vidíme, že to přímo vyplývá z Lagrangeovy věty.

Index podgrupy

Definice

Nechť H je podgrupa grupy G. Počet levých tříd rozkladu G podle H se nazývá **index H v G**.
Značíme $(G : H)$

Index může být konečný i nekonečný.
Pokud je řád konečný, zřejmě $(G : H) = |G|/|H|$. **Proč?**

Příklad 51

Pro grupu $G = \langle \mathbb{Z}_{16}, + \rangle$ určete index $(G : H)$ pro podgrupu $H = \langle 2 \rangle$.

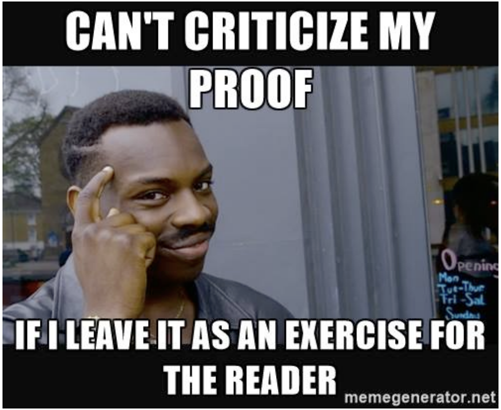
Index podgrupy

Věta 22

Uvažujme podgrupy H, K grupy G, takové, že $K \leq H \leq G$ a předpokládejme, že $(H : K)$ a $(G : H)$ jsou konečné. Pak $(G : K)$ je také konečný a platí
$(G : K) = (G : H)(H : K)$.

Důkaz

Zjevné.



Direktní součin grup

Definice

Kartézský součin *množin* $S_1 \times S_2 \times \cdots \times S_n$ *je množina všech* n*-tic* $(a_1, \ldots, a_n)$, *kde* $a_i \in S_i$, *pro* $i = 1, \ldots, n$.
Značíme $S_1 \times S_2 \times \cdots \times S_n$ *nebo* $\prod_{i=1}^{n} S_i$

Direktní součin grup

Věta 23

Nechť $\langle G_1, \circ_1\rangle, \dots \langle G_n, \circ_n\rangle$ *jsou grupy. Pro* $(a_1, \dots, a_n), (b_1, \dots b_n) \in \prod_{i=1}^n G_i$ *definujeme* $(a_1, \dots, a_n) \circ (b_1, \dots b_n) = (a_1 \circ_1 b_1, \dots, a_n \circ_n b_n)$.
Pak $\langle \prod_{i=1}^n G_i, \circ\rangle$ *je grupa a nazýváme ji* **direktní součin grup**.

Důkaz

Protože $a_i, b_i \in G_i$ *a* G_i *je grupa, platí, že* $a_i \circ_i b_i \in G_i$. *Takže opravdu* $\circ$ *definuje operaci na* $\prod_{i=1}^n G_i$. *(uzavřenost)*
Asociativita v $\prod_{i=1}^n G_i$ *vyplývá z asociativity v každé komponentě.*
Neutrální prvek. Nechť e_i *jsou neutrální prvky v* G_i*, pak je neutrální prvek* $(e_1, \dots, e_n)$.
Inverzní prvky. Pokud a_i^{-1} *je inverze* a_i *v* G_i*, pak zjevně* $(a_1^{-1}, \dots, a_n^{-1})$ *je inverze prvku* $(a_1, \dots, a_n)$.

Direktní součin grup

Příklad 52

Jak vypadá grupa $\mathbb{Z}_2 \times \mathbb{Z}_3$? Je tato grupa cyklická?

- Grupa má $2 \cdot 3 = 6$ prvků:
  $(0,0)$, $(0,1)$, $(0,2)$, $(1,0)$, $(1,1)$, $(1,2)$
- Aby byla grupa cyklická, potřebujeme její generátor $(1,1)$
  $(1,1) = (1,1)$
  $(1,1) + (1,1) = (0,2)$
  $(1,1) + (1,1) + (1,1) = (1,0)$
  $(1,1) + (1,1) + (1,1) + (1,1) = (0,1)$
  $(1,1) + (1,1) + (1,1) + (1,1) + (1,1) = (1,2)$
  $(1,1) + (1,1) + (1,1) + (1,1) + (1,1) + (1,1) = (0,0)$
- Tato grupa je isomorfní se $\mathbb{Z}_6$.

Direktní součin grup

Příklad 53

Jak vypadá grupa $\mathbb{Z}_2 \times \mathbb{Z}_2$? Je tato grupa cyklická?

- Grupa má $2 \cdot 2 = 4$ prvků:
  $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$
- Aby byla grupa cyklická, potřebujeme její generátor
- $(1,1)$:
  $(1,1) = (1,1)$
  $(1,1) + (1,1) = (0,0)$
- $(0,1)$:
  $(0,1) = (0,1)$
  $(0,1) + (0,1) = (0,0)$
  $\ldots$
- Žádný prvek nevygeneruje celou grupu.
- Víme, že existují jen dvě grupy řádu 4 ($\mathbb{Z}_4$ a Kleinova 4-grupa)
- Grupa není cyklická, takže musí být isomorfní s Kleinovou 4-grupou

Direktní součin grup

Příklad 54

Jak vypadá grupa $\mathbb{Z}_3 \times \mathbb{Z}_3$? Je tato grupa cyklická?

Podobně, jako v předchozím příkladu. Vyzkoušejte sami.

Direktní součin grup

Věta 24

Grupa $\mathbb{Z}_m \times \mathbb{Z}_n$ *je cyklická a isomorfní s* $\mathbb{Z}_{mn}$, *právě když* m *a* n *jsou nesoudělná.*

Důkaz

Uvažujme podgrupu grupy $\mathbb{Z}_m \times \mathbb{Z}_n$ *generovanou* $(1,1)$.
Víme, že řád této cyklické podgrupy je nejmenší mocnina $(1,1)$, *která nám dá* $(0,0)$.
První komponenta $1 \in \mathbb{Z}_m$ *dá* 0 *pouze po* m *sečtení,* $2m$ *sečtení,* ...
První komponenta $1 \in \mathbb{Z}_n$ *dá* 0 *pouze po* n *sečtení,* $2n$ *sečtení,* ...
Abychom dostali $(0,0)$, *musí být počet sčítanců násobek* m *i* n. *To bude* mn *pouze tehdy, když jsou nesoudělné. V takovém případě* $(1,1)$ *generuje cyklickou grupu řádu* mn, *takže je isomorfní se* $\mathbb{Z}_{mn}$.
Naopak, předpokládejme, že $gcd(m,n) = d > 1$. *Pak* mn/d *je dělitelné* m *i* n.
Pak platí $(r,s) \in \mathbb{Z}_m \times \mathbb{Z}_n$ $\underbrace{(r,s) + \cdots + (r,s)}_{mn/d \text{ sčítanců}} = (0,0)$
Takže žádný $(r,s) \in \mathbb{Z}_m \times \mathbb{Z}_n$ *nemůže vygenerovat celou grupu. Tedy* $\mathbb{Z}_m \times \mathbb{Z}_n$ *není cyklická a isomorfní se* $\mathbb{Z}_{mn}$.

Direktní součin grup

Důsledek 6

Grupa $\prod_{i=1}^{n} \mathbb{Z}_i$ *je cyklická a isomorfní se* $\mathbb{Z}_{m_1 m_2 \dots m_n}$ *právě tehdy, když jsou čísla* m_i *po dvou nesoudělná.*

- Pokud n můžeme zapsat jako součin mocnin různých prvočísel $n = (p_1)^{n_1}(p_2)^{n_2}\dots(p_r)^{n_r}$
- $\mathbb{Z}_n$ isomorfní s $\mathbb{Z}_{(p_1)^{n_1}} \times \mathbb{Z}_{(p_2)^{n_2}} \times \dots \times \mathbb{Z}_{(p_r)^{n_r}}$

Příklad 55

Najděte direktní součin grup isomorfní s $\mathbb{Z}_{72}$.

Direktní součin grup

Příklad

Najděte direktní součin grup isomorfní s $\mathbb{Z}_{72}$.

$\mathbb{Z}_8 \times \mathbb{Z}_9$

Změna pořadí činitelů v součinu nám dá také isomorfní grupu.

Řád prvku v direktním součinu grup

Definice

Nechť $r_1, r_2, \dots, r_n \in \mathbb{N}$. *Jejich* **nejmenší společný násobek** *(*lcm*) je kladný generátor cyklické grupy všech společných násobků* r_i*, tj. cyklická grupa všech celých čísel dělitelných každým* r_i*, pro* $i \in 1, \dots, n$.

Z definice a z dřívějšího studia cyklických grup vidíme, že lcm čísel $r_1, r_2, \dots, r_n$ je nejmenší kladné číslo, které je násobkem každého r_i.

Řád prvku v direktním součinu grup

Věta 25

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*.*

Důkaz

Podobně jako v důkazu věty 24.
Aby mocnina $(a_1, \ldots, a_n)$ *dala* $(e_1, \ldots, e_n)$ *musí ta mocnina být násobek* r_1*, abychom dostali v první komponentě* e_1*, násobek* r_2*, aby ve druhé komponentě byl* e_2*, ...*

Příklad 56

Zjistěte řád prvku $(8, 4, 10)$ *v grupě* $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$*.*

Řád prvku v direktním součinu grup

Příklad

Zjistěte řád prvku $(8, 4, 10)$ *v grupě* $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$.

- $gcd(8, 12) = 4$, 8 má řád $\frac{12}{4} = 3$ v $\mathbb{Z}_{12}$
- $gcd(4, 60) = 4$, 4 má řád $\frac{60}{4} = 15$ v $\mathbb{Z}_{60}$
- $gcd(10, 24) = 2$, 10 má řád $\frac{24}{2} = 12$ v $\mathbb{Z}_{24}$
- $lcm(3, 15, 12) = 60$
- $(8, 4, 10)$ má v grupě $\mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$ řád 60

Generátory direktního součinu grup

Tvrzení

Direktní součin n cyklických grup, kde každá je $\mathbb{Z}$ nebo $\mathbb{Z}_m$ pro nějaké $m \in \mathbb{N}$, je generovaný n n-ticemi
$(1,0,\dots,0)$, $(0,1,\dots,0)$, $\dots$, $(0,0,\dots,1)$.

Takový direktní součin je možné generovat i méně prvky.

Příklad 57

Jakými prvky jsou generovány následující grupy?

1. $\mathbb{Z} \times \mathbb{Z}_2$
2. $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_{35}$

Generátory direktního součinu grup

Příklad

Jakými prvky jsou generovány následující grupy?

1. $\mathbb{Z} \times \mathbb{Z}_2$
2. $\mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_{35}$

1. $(1, 0)$ a $(0, 1)$
2. $(1, 0, 0)$, $(0, 1, 0)$, $(0, 0, 1)$
   ale také jen $(1, 1, 1)$

Direktního součinu grup

Definice

Direktní součin grup G_i $\prod_{i=1}^{n} G_i$ definovaný dříve také nazýváme **vnější součin** *grup G_i.*
Můžeme ho však definovat i pomocí grup $\overline{G_i} = \{(e_1, e_2, \ldots, e_{i-1}, a_i, e_{i+1}, \ldots, e_n) | a_i \in G_i\}$.
Všechny komponenty až na i-tou obsahují neutrální prvek.
V takovém případě mluvíme o **vnitřním součinu** *grup $\overline{G_i}$.*

Zřejmě je $\overline{G_i}$ isomorfní s G_i. **Jak vypadá isomorfismus?**

Konečně generované abelovské grupy

Věta 26 (Základní věta konečně generovaných abelovských grup)

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 $r_i \in \mathbb{N}$.
*Tento součin je unikátní až na možné přeuspořádání činitelů, tj. počet (***Bettiho číslo** *G) činitelů $\mathbb{Z}$ je unikátní a mocniny $(p_i)^{r_i}$ jsou unikátní.*

Důkaz

Vynechán.

Příklad 58

Najděte všechny abelovské grupy, až na isomorfismy, řádu 360.

Konečně generované abelovské grupy

Příklad

Najděte všechny abelovské grupy, až na isomorfismy, řádu 360.

- $360 = 2^3 3^2 5$
- Všechny možnosti:
  1. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
  2. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
  3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
  4. $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
  5. $\mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$
  6. $\mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
- Existuje 6 různých abelovských grup (až na isomorfismy) řádu 360.

Konečně generované abelovské grupy

Příklad 59

Najděte všechny abelovské grupy, až na isomorfismy, řádu 4.

Dříve jsme uvedli, že existují jen 2. $\mathbb{Z}_4$ a Kleinova 4-grupa.