

NI-MPI přednáška 9

Algebra I

Štěpán Starosta

13. 11. 2024

FIT ČVUT

Hledání skrytých podobností ...

Uvažujme následující objekty:

- množina \mathbb{Z} celých čísel a jejich sčítání,
- množina matic $\mathbb{R}^{n,n}$ s operací násobení matic,
- množinu relací na množině A s operací skládání relací,
- množinu $\{0, 1, 2, 3\}$ s operací násobení modulo 4,
- množinu konečných automatů a jejich skládání,
- množinu všech konečných řetězců nad zadanou abecedou a jejich spojování,
- množinu všech barev a operaci „míchání“,
- ...

Co mají společného?

Společná struktura!

Všechny uvedené objekty mají stejnou strukturu. Skládají se ze dvou ingrediencí:

- Neprázdne (konečné či nekonečné) **množiny objektů**.
- **Binární operace**, která každé dvojici objektů z této množiny jednoznačně přiřadí objekt z uvažované množiny.

Obecně se tedy jedná o dvojici množina a binární operace na ní a proto budeme (většinou) používat značení (M, \cdot) (multiplikativní zápis) resp. $(M, +)$ (aditivní zápis), resp. (M, \circ) (obecný zápis), kde

- M je **neprázdna** množina,
- a pro binární operaci platí $\cdot : M \times M \rightarrow M$, resp. $+ : M \times M \rightarrow M$, resp. $\circ : M \times M \rightarrow M$.

O co jde v teorii grup?

- Dvojici „množina a binární operace na ní“ mohou, jak bylo dříve na příkladech ukázáno, tvořit velice odlišné struktury. My je budeme klasifikovat podle vlastností, které mají.
- O této dvojici nás budou zajímat například následující otázky: Je operace asociativní? Je komutativní? Existují v množině prvky s vlastnostmi jako má jednička a nula v číselných množinách? ...
- Obecná algebra se dále zabývá **bohatšími** strukturami jako jsou okruhy, tělesa a další. S těmi se setkáme později během semestru.

A proč to děláme?

Pokud dokážeme nějaké tvrzení pro obecnou strukturu (M, \circ) , kde \circ je asociativní operace, bude (automaticky) toto tvrzení platit pro všechny konkrétní struktury s asociativní binární operací. Důkaz tohoto tvrzení se zredukuje na (triviální) důkaz asociativity operace!

*Obecnou strukturu můžeme chápat jako **nadřazený objekt**, od kterého konkrétní struktury **dědí** všechny jeho vlastnosti.*

Příklad „dědičnosti“ (1/4)

Na množině nenulových reálných čísel dokážeme následující větu:

Věta 23.1

Pro všechna $b, c \in \mathbb{R} \setminus \{0\}$ má rovnice $bx = c$ jediné řešení $x = \frac{c}{b}$.

Důkaz.

Následující rovnosti jsou za předpokladu $b, c \in \mathbb{R} \setminus \{0\}$ ekvivalentní.

$$bx = c \quad \{\text{vyděl } b, \text{ lze pro } \forall b \neq 0\}$$

$$\frac{bx}{b} = \frac{c}{b} \quad \{\text{použijeme asociativitu násobení}\}$$

$$\frac{b}{b}x = \frac{c}{b} \quad \{\text{víme, že pro lib. } b \neq 0 \text{ je } \frac{b}{b} = 1\}$$

$$1x = \frac{c}{b} \quad \{\text{pro lib. nenulové } d \text{ je } 1d = d\} \quad \square$$

Co jsme potřebovali: asociativitu, umět dělit nenulovým reálným číslem, existenci jedničky.

Je operace násobení matic asociativní?

Příklad „dědičnosti“ (2/4)

Uvažujme nyní množinu M všech matic z $\mathbb{R}^{n,n}$ s operací násobení matic.

- Je operace násobení matic asociativní?

Ano. Pro $\forall A, B, C \in M$ platí $A(BC) = (AB)C$.

- Existuje jednička (neutrální prvek) vůči maticovému násobení?

Ano. Jednotková matice E má vlastnost $EA = AE = A$ platící pro $\forall A \in M$.

- Existuje ke každé matici $A \in M$ matice inverzní?

Neexistuje! Musíme se omezit na množinu všech **regulárních** matic z M , označovanou též $M_{\text{reg}} := \{A \in M \mid A \text{ je regulární}\}$.

Poznámka: Všechna tato tvrzení již známe z Lineární algebry!

Příklad „dědičnosti“ (3/4)

Máme vše co potřebujeme, větu můžeme přeformulovat pro matice:

Věta 23.2

Pro všechna $B, C \in M_{\text{reg}}$ má rovnice $BX = C$ jediné řešení $X = B^{-1}C$.

Důkaz.

Následující rovnosti jsou za předpokladu $B, C \in M_{\text{reg}}$ ekvivalentní.

$$\begin{aligned} BX &= C && \{\text{vynás. inverz. prvkem } B^{-1} \text{ zleva, existuje pro } \forall B\} \\ B^{-1}(BX) &= B^{-1}C && \{\text{přesuneme závorky díky asociativitě}\} \\ (B^{-1}B)X &= B^{-1}C && \{\text{víme, že pro lib. } B \text{ je } B^{-1}B = E\} \\ EX &= B^{-1}C && \{\text{pro lib. matici } D \text{ je } ED = D\} \\ X &= B^{-1}C \end{aligned}$$



Co jsme potřebovali: asociativitu, existenci inverzní matice, existenci jednotkové matice.

Příklad „dědičnosti“ (4/4)

Dvojici (M, \circ) , kde $\circ : M \times M \rightarrow M$, platí asociativní zákon, existuje neutrální prvek a ke každému prvku b existuje inverzní prvek (značený b^{-1}) budeme říkat **grupa**.

Obecná věta pak bude znít:

Věta 23.3

Pro libovolné prvky b, c z grupy (M, \circ) má rovnice $b \circ x = c$ jediné řešení $x = b^{-1} \circ c$.

Důkaz.

Následující rovnosti jsou ekvivalentní.

$$b \circ x = c$$

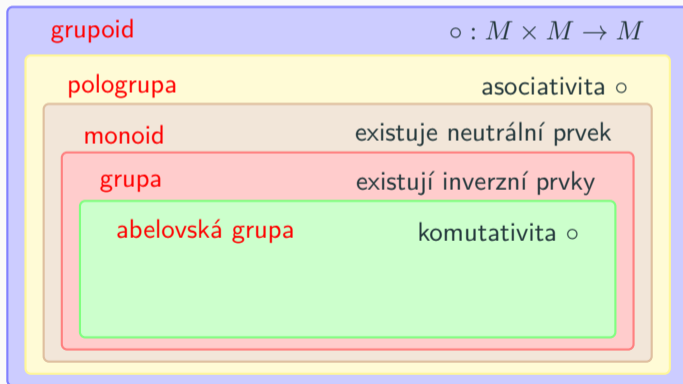
$$b^{-1} \circ (b \circ x) = b^{-1} \circ c$$

$$(b^{-1} \circ b) \circ x = b^{-1} \circ c$$

$$x = b^{-1} \circ c \quad \square$$

Množiny s jednou binární operací

Libovolnou dvojici tvořenou neprázdnou množinou a binární operací na ní, $(M, \circ : M \times M \rightarrow M)$, budeme nazývat **grupoid**. Následným přidáváním dalších požadavků na operaci \circ získáváme další struktury...



Definice 24.1

Grupoid (*magma*) je uspořádaná dvojice (M, \circ) , kde M je libovolná neprázdná množina a \circ je binární operace na M .

- **Plogrupa** (*semigroup*) je grupoid (M, \circ) , pro který je \circ asociativní operace.
- **Monoid** je pologrupa (M, \circ) , ve které existuje **neutrální prvek** $e \in M$ takový, že

$$\text{pro všechna } a \in M \text{ platí } e \circ a = a \circ e = a.$$

- **Grupa** (*group*) je monoid (M, \circ) , ve kterém ke každému $a \in M$ existuje **inverzní prvek** $b \in M$ takový, že

$$b \circ a = a \circ b = e.$$

- **Komutativní (abelovská) grupa** je grupa (M, \circ) , kde \circ je komutativní operace.

První příklady

- Pro dvojici $(\mathbb{Z}, +)$ platí asociativní i komutativní zákon, neutrálním prvkem je 0 a inverzní prvek k prvku a je prvek $-a$, součet dvou celých čísel je celé číslo, **jedná se tedy o abelovskou grupu**.
- Pro dvojici $(\mathbb{R} \setminus \{0\}, \cdot)$ platí asociativní i komutativní zákon, neutrálním prvkem je 1 a inverzní prvek k (nenulovému) prvku a je $\frac{1}{a}$, součin dvou nenulových reálných čísel je nenulové reálné číslo, **jedná se tedy o abelovskou grupu**.
- Pro dvojici (M_{reg}, \cdot) platí asociativní zákon, neutrální prvek i inverzní prvky existují (k $A \in M_{\text{reg}}$ je inverzním prvkem inverzní matice A^{-1}), ale neplatí komutativní zákon! **Jedná se tedy o grupu, nikoli ovšem vždy abelovskou**. Příklad nekomutujících matic:

$$\begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \neq \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 2 & 3 \end{pmatrix}.$$

Otázka: Je součin dvou regulárních matic regulární matice?

- Na grupoid, monoid, atd. se můžeme dívat jako na matematický (abstraktní) objekt či **třídu**, pro který je definována nějaká neprázdná množina a binární operace s danými vlastnostmi.
- Pro tyto abstraktní třídy můžeme dokázat různá tvrzení (jako např. Větu o řešení „lineární“ rovnice pro grupy).
- Pokud potom pro nějakou instanci (M, \circ) ukážeme, že je grupoid, monoid, atp., znamená to, že všechny tato tvrzení „zdědí“ a nemusíme je tedy dokazovat zvlášť.

Poznámky ke značení a terminologii

- O množině M také mluvíme jako o **nosiči** (*carrier*) grupy $G = (M, \circ)$.
- Zápisem $a \in G$, kde $G = (M, \circ)$, máme na mysli $a \in M$.

Značení 24.2

obecný zápis

$$(M, \circ)$$

neutrální prvek: e

inverzní prvek k $a \in M$: a^{-1}

$$\underbrace{a \circ a \circ \cdots \circ a}_{n-1 \text{ operací}} = a^n$$

$$a^0 = e$$

$$a^n \circ a^{-n} = e$$

multiplikativní zápis

$$(M, \cdot)$$

neutrální prvek: 1

inverzní prvek k $a \in M$: a^{-1}

$$\underbrace{a \cdot a \cdots a}_{n-1 \text{ operací}} = a^n$$

$$a^0 = 1$$

$$a^n \cdot a^{-n} = 1$$

aditivní zápis

$$(M, +)$$

neutrální prvek: 0

inverzní prvek k a : $-a$

$$\underbrace{a + a + \cdots + a}_{n-1 \text{ operací}} = n \times a$$

$$0 \times a = 0$$

$$(n \times a) + ((-n) \times a) = 0$$

Uzavřenost množiny vůči binární operaci

V definici klademe na binární operaci \circ podmínku, aby byla „binární operací na M “, což znamená, že výsledek aplikování binární operace na dva prvky z M opět patří do M , stručněji $\circ : M \times M \rightarrow M$. Též říkáme, že **množina M je uzavřená vůči \circ** .

Příklad 24.3

Dvojice (\mathbb{Z}^-, \cdot) záporných celých čísel s klasickým násobením není ani grupoid, neboť \mathbb{Z}^- není uzavřená vůči násobení: například $(-1) \cdot (-1) = 1 \notin \mathbb{Z}^-$.

Uzavřenost či neuzavřenost vůči binární operaci nemusí být vždy očividná:

Příklad 24.4

Uvažujme dvojici (M_{troj}, \cdot) dolních trojúhelníkových matic s klasickým maticovým násobením. Je M_{troj} vůči operaci \cdot uzavřená?



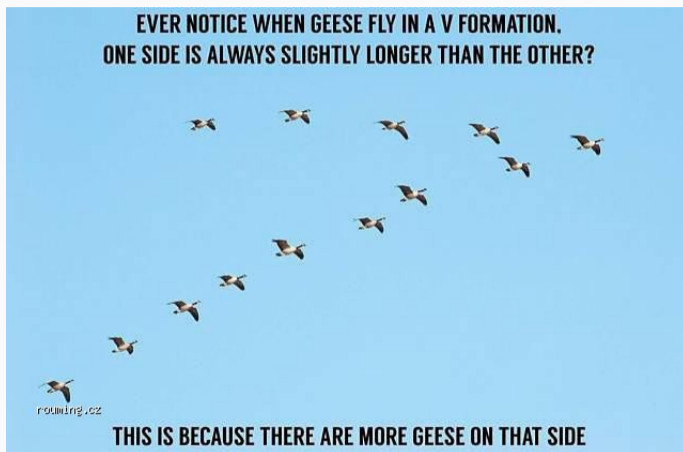
Ověřování vlastností (M, \circ)

Máme-li zadanou dvojici „množina a operace“ a chceme-li zjistit, jestli se jedná o grupoid, pologrupu, monoid, (abelovskou) grupu, můžeme systematicky postupovat (nepřekvapivě) v následujícím pořadí:

- 1 Je množina **uzavřená** vůči operaci? Pokud ano, je to grupoid, pokud ne, konec.
- 2 Je operace **asociativní**? Pokud ano, je to pologrupa, pokud ne, konec.
- 3 Existuje **neutrální prvek**? Pokud ano, je to monoid, pokud ne, konec.
- 4 Existuje ke každému prvku **inverzní prvek**? Pokud ano, je to grupa, pokud ne, konec.
- 5 Je operace **komutativní**? Pokud ano, je to abelovská grupa, pokud ne, konec.

Většinou jsou „důkazy“ v jednotlivých krocích jednoduché až očividné. Někdy ne.

Ověřování vlastností (M, \circ)



Uvedená „kuchařka“ je úplně zbytečná pokud znáte definice pojmů a chápete jejich hierarchii.

Příklad č. 1

Příklad 25.1

Uvažujme grupoid (\mathbb{Q}, \circ) , kde binární operace \circ je definována jako aritmetický průměr:

$$a \circ b := \frac{a + b}{2}.$$

Jedná se o grupoid / pologrupu / monoid / grupu?

Pro racionální čísla a a b je výraz $\frac{a+b}{2}$ racionální číslo. Jde tedy o **grupoid**.

V pologrupě musí platit asociativní zákon. Tvrdíme, že pro takto definovanou operaci \circ *neplatí* a dokážeme to *protipříkladem*:

$$(2 \circ -2) \circ 4 = 0 \circ 4 = 2 \quad \text{ale} \quad 2 \circ (-2 \circ 4) = 2 \circ 1 = \frac{3}{2}.$$

Skutečně, pro takto zvolené prvky \mathbb{Q} asociativní zákon neplatí a nejedná se proto o pologrupu. Z toho je již jasné, že \mathbb{Q} s takto definovanou operací není ani monoid a ani grupa.

Příklad č. 2

Příklad 25.2

Uvažujme grupoid (\mathbb{R}^+, \circ) , kde binární operace \circ je definována takto:

$$a \circ b := \frac{a \cdot b}{a + b}.$$

Jedná se o pologrupu / monoid / grupu?

Poznámka: $\mathbb{R}^+ = (0, +\infty)$.

$$\begin{aligned}(a \circ b) \circ c &= \{ \text{definice } \circ \} = \frac{a \cdot b}{a + b} \circ c = \{ \text{definice } \circ \} = \frac{\frac{a \cdot b}{a + b} \cdot c}{\frac{a \cdot b}{a + b} + c} = \\ &= \frac{(a \cdot b) \cdot c}{a \cdot b + c \cdot (a + b)} = \frac{a \cdot (b \cdot c)}{a \cdot (b + c) + b \cdot c} = \frac{a \cdot \frac{b \cdot c}{b + c}}{a + \frac{b \cdot c}{b + c}} = \\ &= \{ \text{definice } \circ \} = a \circ \frac{c \cdot b}{c + b} = \{ \text{definice } \circ \} = a \circ (b \circ c).\end{aligned}$$

Asociativní zákon platí a jedná se o pologrupu.

Příklad č. 2

(...pokračování...)

Dokázali jsme, že (\mathbb{R}^+, \circ) je **pologrupa**, je to též monoid? Neboli existuje neutrální prvek $e \in \mathbb{R}^+$ tak, že

$$(\forall a \in \mathbb{R}^+)(e \circ a = a \circ e = a) ?$$

Neutrální prvek e musí pro všechna $a \in \mathbb{R}^+$ splňovat rovnici

$$(a \circ e = a) \Rightarrow \left(\frac{a \cdot e}{a + e} = a \right) \Rightarrow (a \cdot e = a \cdot (a + e)) \Rightarrow (e = a + e) \Rightarrow (0 = a),$$

která ale platí pouze pro $a = 0$. Neutrální prvek tedy neexistuje a o monoid se nejedná.

Příklad č. 3

Příklad 25.3

Uvažujme grupoid (\mathbb{R}, \cdot) , kde za binární operaci \cdot bereme klasické násobení čísel.

Jedná se o pologrupu / monoid / grupu?

Asociativita \cdot je známá vlastnost násobení reálných čísel. Jedná se tedy o pologrupu.

Aby se jednalo o monoid, musí existovat neutrální prvek. Existuje?

Pro neutrální prvek e musí platit: $(\forall a \in \mathbb{R})(e \cdot a = a \cdot e = a)$ a takový prvek v \mathbb{R} existuje a je to číslo 1.

Grupoid (\mathbb{R}, \cdot) je tedy dokonce **monoid**.

A je to grupa? Neboli, existuje ke každému reálnému číslu a číslo a^{-1} , tak že $a \cdot a^{-1} = a^{-1} \cdot a = 1$?

Existuje, ovšem pouze pokud a není nula. O grupu se tedy nejedná.

Z definice plyne, že každá grupa je monoid, každý monoid je pologrupa a každá pologrupa je grupoid. To můžeme symbolicky zapsat takto:

$$\text{grupoid} \supset \text{pologrupa} \supset \text{monoid} \supset \text{grupa} .$$

Díky předchozím třem příkladům můžeme tuto hierarchii o něco zpřesnit:

$$\text{grupoid} \not\supseteq \text{pologrupa} \not\supseteq \text{monoid} \not\supseteq \text{grupa} ,$$

neboť jsme našli grupoid, který není pologrupou, pologrupu, která není monoidem a monoid, který není grupou.

Základní cvičení 16.1

Určete, které z následujících číselných množin s uvedenou operací tvoří grupoid / pologrupu / monoid / grupu / abelovskou grupu. Pokud existuje, najděte neutrální prvek a zjistěte, jak vypadají inverzní prvky.

(a) $(\mathbb{R}_0^+, +)$,

(b) (\mathbb{R}_0^+, \cdot) ,

(c) $(\mathbb{R} \setminus \{0\}, \div)$,

(d) $(\mathbb{Q}, -)$,

(e) (\mathbb{Q}, \cdot) ,

(f) $(\mathbb{Q}, +)$.

Cvičení ii

Základní cvičení 16.3

Mějme množinu $M = \{0, 1, \dots, n - 1\}$. Rozhodněte, zda tvoří dvojice (M, \circ) grupoid / pologrupu / monoid / grupu / abelovskou grupu pokud je operace „ \circ “

- (a) sčítání modulo n .
- (b) násobení modulo n .

Příklad: grupa \mathbb{Z}_n^+

Příklad 25.4 (\mathbb{Z}_n^+)

Pro kladné $n \in \mathbb{N}$ je

$$\mathbb{Z}_n^+ := (\{0, 1, \dots, n-1\}, +_n),$$

kde $+_n$ je sčítání modulo n , abelovská grupa.

- Množina $\mathbb{Z}_n := \{0, 1, \dots, n-1\}$ je množina zbytkových tříd po dělení n . Množina M je uzavřená vůči operaci sčítání modulo n .
- Uvažme $a, b, c \in \mathbb{Z}_n$ libovolné, potom existují $j_i, k_i \in \mathbb{Z}$, $i = 1, 2$, tak, že

$$(a +_n b) +_n c = (a +_n b) + c + j_1 n = (a + b) + c + (k_1 + j_1)n,$$

$$a +_n (b +_n c) = a + (b +_n c) + j_2 n = a + (b + c) + (k_2 + j_2)n.$$

Díky asociativitě $+$ tedy platí

$$(a +_n b) +_n c \equiv a +_n (b +_n c) \pmod{n}$$

a dle definice $+_n$ pak i $(a +_n b) +_n c = a +_n (b +_n c)$.

- Neutrálním prvkem vůči $+_n$ je 0.
- Inverzním prvkem k $a \in \mathbb{Z}_n$, $a \neq 0$, je $n - a$. Inverzním prvkem k 0 je 0.

Příklad: grupa \mathbb{Z}_n^\times (1 ze 2)

Příklad 25.5 (\mathbb{Z}_n^\times)

Pro kladné $n \in \mathbb{N}$, $n \geq 2$, je

$$\mathbb{Z}_n^\times := (\{k \in \{1, \dots, n-1\} : k \text{ a } n \text{ jsou nesoudělná}\}, \times_n),$$

kde \times_n je násobení modulo n , abelovská grupa.

Tvrdíme: jsou-li k a ℓ z $\{1, \dots, n-1\}$ nesoudělná s n , pak i $k \times_n \ell$ je nesoudělné s n .

Důkaz sporem: buďte k a ℓ nesoudělná s n a $d \in \{0, \dots, n-1\}$ takové, že $k\ell = jn + d$ pro nějaké $j \in \mathbb{Z}$. Předpokládejme, že d je soudělné s n . Jelikož d je soudělné s n , existuje prvočíslo dělící čísla d i n , které musí dělit i k nebo ℓ , což je spor.

Máme tedy **uzavřenost** množiny vzhledem k dané operaci.

Asociativita operace \times_n plyne z asociativity násobení reálných čísel podobně jako v předcházejícím příkladě.

Neutrální prvek je 1.

Příklad: grupa \mathbb{Z}_n^\times (2 ze 2)

Inverzní prvky: je-li k nesoudělné s n , existují $\alpha, \beta \in \mathbb{Z}$ tak, že

$$\alpha k + \beta n = 1 \quad \Rightarrow \quad \alpha k \equiv 1 \pmod{n}.$$

Jelikož je takové číslo α nesoudělné s n , tak $\alpha \pmod{n}$ je hledaný inverzní prvek.

\times_n je **komutativní**. \mathbb{Z}_n^\times je tedy skutečně abelovská grupa.

Nemohlo by v nosiči být více zbytků po dělení n (vzhledem k \times_n)?

Ne, čísla **soudělná s** n nemají inverzní prvek: uvažujme jakékoli číslo $1 < k < n$ soudělné s n .

Předpokládejme, že ℓ je inverzní prvek k prvku k , tedy že platí $k\ell \equiv 1 \pmod{n}$. Tedy pro nějaké j platí $k\ell = 1 + jn$, a tedy $1 = k\ell - jn = d(\frac{k}{d}\ell - j\frac{n}{d})$, kde $d, d > 1$, je společný faktor k a n . Tím dostaneme spor, tedy k prvku k bychom nenašli inverzní prvek.

\mathbb{Z}_n^+ je aditivní modulární grupa (celých čísel) modulo n .

\mathbb{Z}_n^\times je multiplikativní modulární grupa (celých čísel) modulo n .

Jiná běžná značení: \mathbb{Z}_n^* , $(\mathbb{Z}/n\mathbb{Z})^\times$.

Věta 26.1

V monoidu existuje právě jeden neutrální prvek.

Důkaz.

Bud' (G, \circ) monoid a e nějaký neutrální prvek (z definice víme, že tam alespoň jeden je!). Dokážeme *sporem*, že e je jediný neutrální prvek.

Pro spor předpokládejme, že v monoidu existuje další neutrální prvek \bar{e} různý od e , tj. $e \neq \bar{e}$. Potom platí

$$\bar{e} = \bar{e} \circ e = e,$$

kde jsme použili vlastnost neutrálního prvku danou definicí. Tím dostáváme spor s tím, že \bar{e} a e jsou různé. □

Jednoznačnost inverzního prvku

Věta 26.2

V grupě má každý prvek právě jeden inverzní prvek.

Důkaz.

Bud' (G, \circ) grupa, a libovolný prvek této grupy a nějaký k němu inverzní prvek b (z definice grupy víme, že tam alespoň jeden je). Dokážeme *sporem*, že b je jediný inverzní prvek.

Pro spor předpokládejme, že v grupě existuje jiný inverzní prvek c různý od b . Potom platí

$$c = c \circ e = c \circ (a \circ b) = (c \circ a) \circ b = e \circ b = b,$$

kde e je neutrální prvek. Tím dostáváme spor s tím, že c a b jsou různé. □

Značení 26.3

V souladu se zavedeným značením 24.2 značíme inverzní prvek k prvku a grupy (G, \circ) pro obecné (multiplikativní) značení takto:

$$a^{-1},$$

a pro aditivní značení takto:

$$-a.$$

Cayleyho tabulka pro konečné grupy

Pokud má množina M z dvojice (M, \circ) konečný počet prvků, lze její strukturu (danou operací \circ) kompletně zachytit v tzv. **Cayleyho tabulce**, jejíž konstrukce je zřejmá z následujícího příkladu.

Příklad 27.1

Uvažujme grupu \mathbb{Z}_4^+ . Jelikož má její nosič 4 prvky, bude mít Cayleyho tabulka 4 řádky a 4 sloupce označené těmito čtyřmi prvky (takže bude typicky znázorněná jako tabulka 5x5).

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Nyní do pole na řádku m a v sloupci n vyplníme výsledek $m +_4 n = m + n \pmod{4}$. Například do řádku 2 a sloupce 3 vyplníme $2 + 3 \pmod{4} = 1$.

Jak poznat různé věci z Cayleyovy tabulky

Cayleho tabulka skýtá o dané množině a operaci veškeré informace. Některé vlastnosti lze z tabulky vyčíst velmi snadno, jiné už hůře:

- **Uzavřenost** množiny M vůči operaci \circ poznáme tak, že všechny pole tabulky obsahují prvky z množiny M .
- **Asociativitu** operace z tabulky poznáme těžko (projděte všechny trojice prvků a ověřte splnění asociativity...).
- **Neutrální prvek** e v tabulce poznáme tak, že v „jeho“ řádku a sloupci se přesně opakují označení řádku a sloupce tabulky.
- **Inverzní prvek** k prvku a najdeme tak, že najdeme v příslušně označeném řádku a sloupci neutrální prvek e ...
- Operace je **komutativní**, pokud je tabulka symetrická vůči hlavní diagonále.

Poznámka: Cayleho tabulka není příliš praktická v případě, kdy množina M má velký počet prvků.

Cayleyho tabulka a latinský čtverec (1/4)

Otázka: Lze z Cayleyho tabulky snadno poznat, jestli se jedná o tabulku grupy?

Odpověď: Skoro.

Věta 27.2

Cayleyho tabulka každé grupy tvoří latinský čtverec.

- **Latinský čtverec** pro n prvkovou množinu M je matice $n \times n$ taková, že v každém řádku i sloupci jsou vždy všechny prvky množiny M .
- Větu dokážeme tak, že dokážeme jinou větu, ze které už bude důkaz této věty triviálně vyplývat.
- Bohužel ne každá Cayleyho tabulka tvořící latinský čtverec je tabulkou grupy. Později si ukážeme protipříklad.

Cayleyho tabulka a latinský čtverec (2/4)

Věta 27.3

V každé grupě lze *jednoznačně dělit*.

Tzn.: V každé grupě (G, \circ) mají pro libovolné $a, b \in G$ rovnice

$$a \circ x = b \quad a \quad y \circ a = b \quad \text{jediné řešení.}$$

Tuto větu jsme dokázali dříve v této přednášce ještě před zavedením pojmu grupa, přesto zde uvedeme další důkaz, lehce „algebraičtější“.

Důkaz.

Jelikož se jedná o grupu, každý prvek má (jediný) inverzní prvek, a snadno tedy zjistíme, že řešením rovnic jsou prvky $a^{-1} \circ b$ resp. $b \circ a^{-1}$.

Jednoznačnost se dokáže sporem: necht' existuje řešení $x_1 \neq a^{-1} \circ b$, potom

$$x_1 = (a^{-1} \circ a) \circ x_1 = a^{-1} \circ (a \circ x_1) = a^{-1} \circ b. \quad \square$$

Cayleyho tabulka a latinský čtverec (3/4)

Nyní dokážeme předchozí větu, která říká že Cayleyho tabulka grupy je latinský čtverec:

Důkaz.

Dokážeme to sporem:

- Předpokládejme, že tabulka nějaké grupy (G, \circ) není latinský čtverec.
- To znamená, že v nějakém řádku nebo sloupci se jeden prvek, označme jej b , opakuje dvakrát. Bez újmy na obecnosti předpokládejme, že je to v řádku n ve sloupcích m_1 a m_2 .

\circ	\dots	m_1	\dots	m_2	\dots
\vdots		\vdots		\vdots	
n	\dots	b	\dots	b	\dots
\vdots		\vdots		\vdots	

- Z toho ale okamžitě vyplývá, že rovnice $n \circ x = b$ má dvě různá řešení m_1 a m_2 , což je **spor s předchozí větou!**



Cayleyho tabulka a latinský čtverec (4/4)

- Ukázali jsme, že to, že Cayleyho tabulka je latinský čtverec, je *nutnou* podmínkou pro to, aby daná množina a operace byla grupou.
- Jak ukazuje následující protipříklad, nejedná se o podmínku *postačující*.

Příklad 27.4

Uvažujme množinu $M = \{a, b, c\}$ s operací zadanou touto Cayleyho tabulkou:

\circ	a	b	c
a	b	a	c
b	c	b	a
c	a	c	b

Tato tabulka tvoří latinský čtverec, ale přesto není tabulkou grupy. (Proč?)

Cayleyho graf grupy

Vizualizovat konečnou grupu $G = (M, \circ)$ lze dále pomocí Cayleyho orientovaného grafu (V, E) , kde

- **vrcholy** grafu V jsou prvky grupy, tj. $V = M$,
- **orientovaná hrana** (a, b) patří do E , právě když $b = a \circ c$ pro jisté $c \in N$.

Množinu N vhodně zvolíme předem (většinou neobsahuje neutrální prvek grupy G ; typicky jde o generující množinu, viz příští přednáška). Hrany lze pro přehlednost obarvit podle příslušnosti k c .

Podobně jako u Cayleyho tabulek platí, že se Cayleyho grafy hodí pro grupy s menším počtem prvků. Lépe v nich navíc vynikne struktura grupy (viz dále).

Pokud by grupa nebyla abelovská, museli bychom kreslit i hrany (a, b) pro $a = b \circ c$ pro $c \in N$.

Cayleyho graf grupy: příklad \mathbb{Z}_4^+

