

PARTIE Z TEORIE MNOŽIN

Intuitivně $\rightarrow$ množina = soubor objektů, které jsou dobře rozličitelné prvky množiny.

Přijme $a \in A, a \notin A$.

úkus: $B \subset A$ připsat i $B = A$

$B \cup A, B \cap A, A \times B, A \setminus B$, doplněk

$|A|$ = počet prvků množiny ($\in \mathbb{N} \cup \{\infty\}$)

$\bigcup_{\alpha \in I} A_\alpha, \bigcap_{\alpha \in I} A_\alpha$

$P(A) = \{M; M \subset A\}; P(\emptyset) = \{\emptyset\}$.

Problémy:

Russellův paradox: S množina všech množin, které nejsou svým vlastním prvkem

$$S = \{X \mid X \notin X\}.$$

$$S \in S \Leftrightarrow S \notin S.$$

Cantorův paradox: $|M| < |P(M)|$

S množina všech množin

$$P(S) \subset S, \text{ proto } |P(S)| \leq |S|$$

$\rightarrow$ řešení a rozlišení A i da, množina = A i da, která může být prvkem jiné A i da.

$\rightarrow$ axiomatická teorie množin.

Zermelo - Frankel } 1. pol. 20. stol.
Gödel - Bernays

Relace, zobrazení

Def: Jsou-li $M_1, \dots, M_n$ množiny, pak relace $R \subset M_1 \times M_2 \times \dots \times M_n$.

Nyčastěji $M_1 = \dots = M_n = M$... n -ární relace na M

$n=2$

binární relace z M_1 do M_2
 X do Y .

$n=2$ $X=Y$

binární relace na X

Expozice $(x, y) \in R$ píšeme $x R y$.

Def: Inverzní relace R^{-1} k relaci $R \subset X \times Y$ je $R^{-1} \subset Y \times X$

$$R^{-1} = \{(y, x) \in Y \times X \mid (x, y) \in R\}.$$

Pro relace $R \subset X \times Y$, $S \subset Y \times Z$ je složená relace $S \circ R$

$$S \circ R = \{(x, z) \in X \times Z \mid \exists y \in Y \text{ tak, že } (x, y) \in R, (y, z) \in S\}$$

Diagonála (rovnost) na X :

$$I_X \subset X \times X, \quad I_X = \{(x, x) \mid x \in X\}.$$

Zobrazení (funkce) z X do Y je relace $\Gamma_f \subset X \times Y$

splňující: $\forall x \in X \exists$ nejvýše jedno $y \in Y$ tak, že

$$(x, y) \in \Gamma_f. \quad (\forall (x_1, y_1), (x_2, y_2) \in \Gamma_f \text{ platí } x_1 = x_2 \Rightarrow y_1 = y_2)$$

Někdy: Γ_f ... graf funkce, píšeme $f(x) = y$
nebo $f: x \mapsto y$.

Definicií obor $\text{Dom } f = \{x \in X \mid \exists y \in Y \text{ tak, že } (x, y) \in \Gamma_f\} \subset X$

Obor hodnot $\text{Im } f = \{y \in Y \mid \exists x \in X \text{ tak, že } (x, y) \in \Gamma_f\} \subset Y$

Pozn. I_X je graf identického zobrazení $1_X: x \mapsto x$.

Def: operace n -ární $\text{na } X$ $F: \underbrace{X \times \dots \times X}_n \rightarrow X$ tj. $(n+1)$ -ární relace na X
 $n=2, n=1, n=0$.

3

Platí: Složením zobrazení vznikne zobrazení.
Skládání je asociativní.

Def: Zobrazení je prosté (injektivní), když $\forall x_1, x_2 \in \text{Dom } f \text{ platí}$
 $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$
na (surjektivní), když $\forall y \in Y \exists x \in X \text{ tak, že}$
 $f(x) = y$.

Zobrazení $g: Y \rightarrow X$ je levé (prave) inverzní k $f: X \rightarrow Y$,
když $g \circ f = 1_X$ ($f \circ g \neq 1_Y$).

Platí: Zobrazení $f: X \rightarrow Y$ (def. všude na X) je
injektivní, resp. surjektivní, právě když existuje
levé, resp. pravé inverzní zobrazení.

• Pokud existují obě, pak se rovnají a jsou
hovorová se zobrazením inverzním k f , tj. f^{-1} .

dk: $\exists g: Y \rightarrow X$ tak, že $g \circ f = 1_X \Rightarrow f$ injektivní:

Vezmeme $x_1, x_2 \in X$ tak, že $f(x_1) = f(x_2)$. Pak

$$x_1 = (g \circ f)(x_1) = (g \circ f)(x_2) = x_2. \quad \text{OK}$$

• f injektivní $\Rightarrow \exists$ levá inverze:

Definujeme $g: Y \rightarrow X$:

Je-li $y \in \text{Im } f$, polož $g(y) = \cancel{x}$, kde $f(x) = y$. (Takev x je
právě jedno a injektivní y)

Je-li $y \notin \text{Im } f$, polož $g(y) = \text{libo}$, např. x_0 libovol.

Odtud $(g \circ f)(x) = x \quad \forall x \in X$.

• $\exists g: Y \rightarrow X$ tak, že $f \circ g = 1_Y \Rightarrow f$ surjektivní:

$\forall y \in Y$ tedy platí $(f \circ g)(y) = f(\underbrace{g(y)}_{\in X}) = y$. Proto $\text{Im } f = Y$.

- f surjektivní $\Rightarrow \exists$ prava' inverze

Definujeme $g: Y \rightarrow X$:

Pro každé y je $f^{-1}(\{y\})$ neprázdne' (ne surjektivní),
 zvol $x \in f^{-1}(\{y\})$ a polož $g(y) = x$. Pak $f(g(y)) = f(x) = y$
 tj. $f \circ g = 1_Y$
 je prava' inv.

- Necht' $g_L \circ f = 1_X, f \circ g_R = 1_Y$. Pak

$$g_L = g_L \circ 1_Y = g_L \circ f \circ g_R = 1_X \circ g_R = g_R.$$

Pozor! Zámětel v předposledním puntíku, jak máme, že
 můžeme vybírat? Axiom výběru bude.

Důsledek: $f: X \rightarrow Y, g: Y \rightarrow Z$

$\tilde{f}: Y \rightarrow X, \tilde{g}: Z \rightarrow Y$ leva' inverze k f, g .

Pak $\tilde{f} \circ \tilde{g}$ je leva' inverze k $g \circ f$, tj. $(\tilde{f} \circ \tilde{g}) \circ (g \circ f) = 1_X$

Podobně pro prava' inverze.

Důsledek důsledku: Složením prostých zsmiků prosté,
 složením surjektivních je surjektivní.

Množiny funkcí:

Def: Jsou-li X, Y množiny, pak značíme

$$Y^X = \{ f \mid f: X \rightarrow Y \} \subset \mathcal{P}(X \times Y).$$

Kurátorského
mocnin

! už uvažujme f definované všude na X .

Posu: Je-li $Y = \emptyset, X \neq \emptyset$, pak $\emptyset^X = \emptyset$.

Když $X = \emptyset, Y$ libv., pak $\Gamma_f = \{ (a, b) \mid a \in \emptyset, b \in Y \}$
 $= \emptyset \times Y$

Jediná podmnožina $\Gamma_f \subset \emptyset \times Y$ je $\emptyset$,

$$\text{tj. } Y^\emptyset = \{ \emptyset \}.$$

Proto: $|\emptyset^X| = 0$ pro $X \neq \emptyset$

$|Y^\emptyset| = 1$ pro Y libv.

Posu: Pro konečné množiny X^m , když $|X| = m$
 nebo n^X , když $|Y| = n$.

Když X, Y konečné, pak $|Y^X| = |Y|^{|X|}$.

Př: $X^{\{1,2\}} (= X^2) = \{ f \mid f: \{1,2\} \rightarrow X \} \cong \{ (f(1), f(2)) \mid f: \{1,2\} \rightarrow X \} = X \times X$

Př: Stejně $X^n \cong \underbrace{X \times X \times \dots \times X}_{n\text{-krát}}$
 vzájemně jednoznačně

Př: $\{0,1\}^X (= 2^X) = \{ f \mid f: X \rightarrow \{0,1\} \} \cong \mathcal{P}(X)$
 bijekce $M \mapsto \chi_M \in \{0,1\}^X$
 Ato charakteristické fce $M \subset X$

Př: $\chi_M: X \rightarrow \{0,1\}^X$
 je def. $\chi_M = \{(a,1) \mid a \in M\} \cup \{(b,0) \mid b \in X \setminus M\}$.

$$\chi_M(a) = \begin{cases} 1 & \text{po } a \in M \\ 0 & \text{po } a \in X \setminus M. \end{cases}$$

Def: Řekneme, že množiny A, B jsou ekvivalentní, jestliže mezi nimi existuje bijekce. $\rightarrow$ slovo ekvivalence přijde.

Platí: pokud X, Y, S, T množiny, pak

- $(S \times T)^X \simeq S^X \times T^X$
- $S^{X \times Y} \simeq (S^X)^Y$
- $S^{X \cup Y} \simeq S^X \times S^Y$

dk: ověření, či sám.

Def: Speciální typ zobrazení = operace.
 Je-li X množina, $n \in \mathbb{N}$. Zobrazení $f: X^n \rightarrow X$
 je n -ární operace na X

- $n=2$ binární $f: X \times X \rightarrow X$
- $n=1$ unární $f: X \rightarrow X$
- $n=0$ nulární $f: X^0 = \{\emptyset\} \rightarrow X$

Pozn: nulární operace je výběr vyjádřujícího prvku.

Vlastnosti relace

5

Def: Relace $R \subset X \times X$ je

reflexivní, když $\forall x \in X$ je xRx , tj. $I_X \subset R$.

symetrická, když $\forall x, y \in X$ je $xRy \Leftrightarrow yRx$, tj. $R = R^{-1}$.

transitivní, když $\forall x, y, z \in X$ je $xRy \wedge yRz \Rightarrow xRz$, tj. $R \circ R \subset R$.

antisymetrická, když $\forall x, y \in X$ je $xRy \wedge yRx \Rightarrow x = y$, tj. $R \cap R^{-1} \subset I_X$.

Pozn: silně antisymetrická $\forall x, y$ $xRy \Rightarrow yRx$, tj. $R \cap R^{-1} = \emptyset$.

trichotomická $\forall x, y$ xRy nebo yRx nebo $x = y$.

Ekvivalence

Def: Relace $\sim$ na množině X je ekvivalence,
jestli reflexivní, symetrická, transitivní (RST).

Př: Nejmenší (ve smyslu inkluze) je I_X , tedy rovnost.
největší je $X \times X$, tj. kartézský součin.

Def: Třída ekvivalence $\sim$ k danému prvku $x \in X$:

$$[x]_{\sim} = \{y \in X \mid y \sim x\}$$

někdy bez $\sim$.

Př: $\sim$ na A^* , slova stejné délky
 $\sim$ na $\mathbb{R}^2$, vektory stejné normy (kradice)
 $\sim$ na $\mathbb{P}(V)$, podmnožiny stejné množinosti?

Lemma: Necht $\sim$ je ekvivalence na X . Potom $\forall x, y \in X$

platí: 1) $x \sim y \Leftrightarrow [x] = [y]$

2) $x \not\sim y \Leftrightarrow [x] \cap [y] = \emptyset$.

tj. každé dvě třídy jsou buď shodné nebo disjunktní.

dk: 1) $\Rightarrow x \sim y$, pak $\exists k \in [x]$ je $k \sim x \sim y$, tj. $x \sim y$, proto $k \in [y]$. Stejně $[y] \subset [x]$.
 $\Leftarrow [x] = [y] \Rightarrow x \in [y]$ tj. $x \sim y$.

2) $\Rightarrow k \in [x] \cap [y]$, pak $k \sim x$ a $k \sim y \Rightarrow x \sim y$.
 $\Leftarrow x \sim y$, pak $y \in [x]$, tj. $y \in [x] \cap [y] \neq \emptyset$.

Def: Je-li $\sim$ ekvivalence na $X \neq \emptyset$, pak

$$X/\sim = \{ [x]_\sim \mid x \in X \} \subset \mathcal{P}(X), \quad \text{ne } \mathcal{P}(\mathcal{P}(X))$$

6

je faktormnožina X podle $\sim$.

Zobrazem' $p_\sim: X \rightarrow X/\sim$

$x \mapsto [x]_\sim$ se nazývá projekce X na $X/\sim$

Pozn. Z tvrzení platí $X = \bigcup_{A \in X/\sim} A$ disjunktne.

Naopak každému rozkladu X na disjunktne sjednocem' odpovídá ekvivalence $\sim$ tak, že množiny v rozkladu jsou třídy této ekvivalence.

Př: $f: X \rightarrow Y$ zobrazem', definuj:

$$E_f = \{ (x_1, x_2) \in X \times X \mid f(x_1) = f(x_2) \}$$

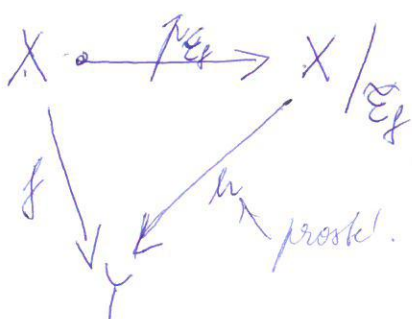
E_f je ekvivalence, která rozkládá X na $X = \bigcup_{y \in \text{Im } f} f^{-1}(\{y\})$.

Naopak:

$\sim \subset X \times X$ je ekvivalence, $p_\sim: X \rightarrow X/\sim$ projekce

Pak $E_{p_\sim} = \sim$.

Lze vyjádřit komutativním diagramem.



~~$E_{p_\sim} = \sim$~~

25.9.
koniec

Uspořádaní

7

Def: Relace $\leq$ na X je uspořádaní na X , když je reflexivní, antisymetrická, transitivní (RAT).
Prvky jsou porovnatelné, když $x \leq y$ nebo $y \leq x$.

Pozn: Obecně existují neporovnatelné prvky.

- Známe $x < y$, jestliže $x \leq y$ a $x \neq y$.
 $x \leq y$ a tedy $y \geq x$.

Def: Uspořádaní $\leq$ je úplné (lineární), jestliže každé dva prvky jsou porovnatelné.

Plat: (Zákon trichomie): V úplném uspoř. množině
je $\forall x, y \in X$ jedna ze tří:
 $x < y$ nebo $x = y$ nebo $x > y$.

Plat: Je-li $\leq$ uspořádaní na X a $A \subset X$, pak $\leq_A = \leq|_A$ (AxA)
je uspořádaní na A . Je-li $\leq$ úplné na X , je
 $\leq_A$ úplné na A .

Def: Nepřázdna úplné uspořádaná podmnožina $A \subset X$
se nazývá řetězec v X .

- x je minimální, jestliže $\forall y \in X: y \leq x \Rightarrow y = x$
- x je nejmenší (první), jestliže $\forall y \in X: y \not\leq x$.
- x je maximální, jestliže $\forall y \in X: y \geq x \Rightarrow y = x$
- x je největší (poslední), jestliže $\forall y \in X: y \leq x$.

Plat: Nejmenší prvek je minimální, ne naopak.
Největší prvek je maximální, ne naopak.

Nejmenší (největší) jsou jednoznačné, min/max ne.
V úplné uspořádané množině platí splývají.

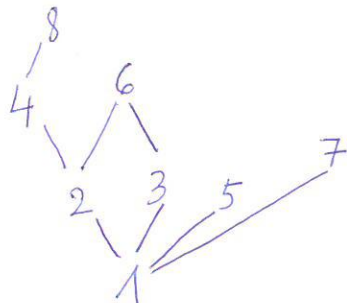
Příklady uspořádání:

$$(\mathbb{Z}, \leq), (\mathbb{Z}, =), (\mathcal{P}(X), \subset), (\mathbb{Z}, |), (\mathbb{Q}, \leq)$$

dělení

8

Př: Dělitelnost v množině $\{1, 2, 3, 4, 5, 6, 7, 8\}$



1 je minimální i nejmenší
 7, 5, 6, 8 maximální, ale ne největší.
 nepř. 5 není porovnatelné s 6.

Hasse diagram:

Prvky spojené, když $x \leq y$ a není z tak, že $x \leq z \leq y$.
 x leží pod y (Transitivní redukce)

Def: Uspořádání na X je dobré, jestliže každá neprázdná podmnožina X má nejmenší prvek.

Plat: Každá dobře uspořádaná je úplně uspořádaná.

dk: Vezmeme $x, y \in X$. Podmnožina $\{x, y\}$ má min. prvek, buď x , tj. $x \leq y$.

Def: Zobrazení $f: X_1 \rightarrow X_2$ dvou uspořádaných množin $(X_1, \leq_1), (X_2, \leq_2)$ je izomorfismus (podobnost) uspořádaných množin, jestliže f je bijekce a $\forall x, y \in X_1$ platí $x \leq_1 y \Rightarrow f(x) \leq_2 f(y)$.
 Řekneme, že X_1, X_2 jsou podobně uspořádané.

Pozn: Pokud jsou x podobně uspořádaných množin, je uspořádaná úplně, resp. dobře, platí to i pro druhé.

Př: $(\mathbb{N}, \leq)$ dobře uspoř.
 $(\mathbb{Z}, \leq)$ není dobře uspoř.

Pozn: 1 množiny ekvivalentní množinami podobně
 $(\mathbb{Z}, \leq), (\mathbb{Q}, \leq)$.

9

Def: Je-li $(M, \leq)$ úplně uspořádaná množina,
 $a \in M$, pak $M_a = \{x \in M \mid x < a\}$
 je úsek množiny M určený prvkem a .

Věta: (princip transfinite indukce):

Nechť $(M, \leq)$ je dobře uspořádaná množina, $A \subset M$.
 Jestliže A splňuje podmínku

$$\forall x \in M, M_x \subset A \Rightarrow x \in A, \quad (*)$$

potom $A = M$.

Důk: Je-li $M \neq \emptyset$, pak nejmenší prvek $x_0 \in M$ leží v A , protože
 x_0 nejmenší, pak $M_{x_0} = \emptyset \subset A \Rightarrow x_0 \in A$.

To je první krok indukce, nemůžeme (zapsat) zůstat.

Důk: A volíme jako množinu prvků splňujících naše tvrzení.
 Když se povede ukázat, že z faktů platnosti tvrzení
 pro všechny prvky úseku M_a plyne platnost pro a ,
 pak tvrzení platí vždy.

Důk: Když $(M, \leq)$ je $(\mathbb{N}, \leq)$ je to standardní indukce.
 Může být i jiný případ, např. $\{a_1, a_2, a_3, \dots, b\}$
 uspořádané takto. Je to dobře uspoř., ale dk. pro M_a
 je jiného typu.

dk: Necht' A splňuje $(*)$, ale $A \neq M$. Pak $M \setminus A \neq \emptyset$
 a existuje nejmenší prvek $x \in M \setminus A$, ozn. a .
 M_a je disj. s $M \setminus A$, tj. $M_a \subset A$. Z $(*)$ plyne $a \in A$, spor.

Peanovy axiomy

10

zavádí přirozená čísla (resp. N_0) jako minimální množinu obsahující 0 a s každým prvkem i jeho následníka, 0 nem' následníkem, následující množina.

Def: Peanovy axiomy:

Čísla nazýváme čísla jsou uspoř. trojice $(N_0, \sigma, 0)$, kde N_0 je množina, σ je unární operace na N_0 , 0 je nulární operace na N_0 , a splňují:

- (1) σ je prostě zobrazení (následník)
- (2) $0 \notin \sigma(N_0)$
- (3) $\forall M \subset N_0$ platí: $0 \in M, \sigma(M) \subset M \Rightarrow M = N_0$.

Pozn: Axiom (3) je princip matematické indukce.

Důsledek: • $\sigma(N_0) = N_0 \setminus \{0\}$.

• $\forall n \in N_0$ je $\sigma(n) \neq n$.

dle: • Dle (2) $\sigma(N_0) \subset N_0 \setminus \{0\}$. Chci ukázat =, tj. že množina $M = \sigma(N_0) \cup \{0\} = N_0$, to je (3).

$0 \in M$ triviálně, $\sigma(M) = \sigma(N_0) \subset M$, proto $M = N_0$ ok.

• Zase indukci $\sigma(0) \neq 0$ podle (2).

Vezmu $M = \{n \in N_0 \mid \sigma(n) \neq n\}$, chci $M = N_0$.

První krok $0 \in M$ ok.

$\sigma(M)$? $\sigma(\sigma(n)) = \sigma(n)$ by implikovalo $\sigma(n) = n$ dle (1).

Proto $\sigma(M) \subset M$, tj. $M = N_0$.

Pozn: Nejprve indukci klasicky, čili platnost ověříme pro 0 a pak pro $\sigma(n)$ z platnosti pro n .

Posu: konstrukce $(N_0, \sigma, 0)$ splňující P.A.

dle J. von Neumanna $\rightarrow$ Ar. von Neumannova úsk.

(i) $\emptyset \in \omega$

(ii) $\forall A \in \omega$ platí $A \cup \{A\} \in \omega$

$\sigma: \omega \rightarrow \omega$ definuji pro $A \in \omega$: $\sigma(A) = A \cup \{A\}$.

Pak uspoř. trojice $(\omega, \sigma, \emptyset)$ splňuje P.A.

$\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset, \{\emptyset, \{\emptyset\}\}\}, \dots$

Definice rekursí

- zdať se jednoduše, ale dk netriviální

Věta: (Princip definice rekursí): Necht' S je množina, $a \in S$,

$g: S \rightarrow S$. Pak existuje právě jedno zobrazení

$h: N_0 \rightarrow S$ tak, že

(1) $h(0) = a$

(2) $\forall n \in N_0$ platí $h(\sigma(n)) = g(h(n))$.

dlh: pouze jednoznačnost:

Pokud h_1, h_2 splňují, pak $h_1 = h_2$ indukci.

$h_1(0) = h_2(0)$ z (1)

Necht' pro $n \in N_0$ platí $h_1(n) = h_2(n)$.

Pak ze (2)

$$h_1(\sigma(n)) \underset{(2)}{=} g(h_1(n)) \underset{(2)}{=} g(h_2(n)) \underset{(2)}{=} h_2(\sigma(n)).$$

Proto OK.

Na'nak d'kazu existence

Dobře def. množina:

$$\mathcal{H} = \{ A \subseteq \mathbb{N} \times S \mid \exists m \in \mathbb{N}_0, \{ A \text{ je obrazem } : \{ k \in \mathbb{N} \mid k \leq m \} \rightarrow S, \\ A(0) = a, \forall k < m \text{ platí } A(\sigma(k)) = g(A(k)) \}$$

Pak položíme

$$h = \{ (n, x) \in \mathbb{N} \times S \mid \exists A \in \mathcal{H} \text{ tak, že } A(n) = x \}$$

Pak se ukáže:

- 1) h je obrazem.
- 2) h definované všude na $\mathbb{N}$.
- 3) h splňuje (1) a (2).

niz Bukovský str. 28. $\rightarrow$ na ev. když někde čas

Iterace zobrazení $f: X \rightarrow X$:

Zvolim $S = X^X$ pro množinu X .

$$a = 1_X$$

$$g: X^X \rightarrow X^X \text{ dano } g(\varphi) = f \circ \varphi$$

pro předem zvolené f .

Pak $\exists!$ $h: \mathbb{N}_0 \rightarrow X^X$ tak, že $h(0) = 1_X$

$$h(\sigma(n)) = f \circ h(n).$$

$$h(n) = f^n.$$

Zapisujeme $f^0 = 1_X$
 $f^{\sigma(n)} = f \circ f^n$

Př: Speciálně iterativní zobrazení $\sigma: \mathbb{N}_0 \rightarrow \mathbb{N}_0$,

Plat: $\sigma^n(0) = n, \forall n \in \mathbb{N}_0$.

dk: indukci $\sigma^0(0) = 1_{\mathbb{N}_0}(0) = 0$.

$$\sigma^n(0) = n$$

$$\sigma^{\sigma(n)}(0) \stackrel{\text{def. iterace}}{=} (\sigma \circ \sigma^n)(0) \stackrel{\text{def. skládání}}{=} \sigma(\sigma^n(0)) \stackrel{\text{IP}}{=} \sigma(n) \quad \text{ok.}$$

Další tvrzení o iteracích:

Plat: Necht $f, g: X \rightarrow X$ komutují (~~tedy~~ $f \circ g = g \circ f$) Pak

$$\bullet \forall m, n \in \mathbb{N}_0 \text{ je } f^n \circ g^m = g^m \circ f^n$$

$$\bullet \forall m \in \mathbb{N}_0 \text{ je } (f \circ g)^m = f^m \circ g^m$$

$$\bullet \forall m, n \in \mathbb{N}_0 \text{ je } (f^m)^n = (f^n)^m$$

dk: Všechno indukci, například ev.

Aritmetika na $\mathbb{N}_0$

13

Def: Na $\mathbb{N}_0$ definujeme binární operace
sčítání a násobení takto: $+, \cdot: \mathbb{N}_0 \times \mathbb{N}_0 \rightarrow \mathbb{N}_0$.

Pro $m, n \in \mathbb{N}_0$ je $m+n := \sigma^n(m)$
 $m \cdot n := (\sigma^m)^n(0)$.

Navečer zavádíme $1 = \sigma(0)$.

Pozn: V dalším je konvence, že $\cdot$ je před $+$ i bez závozu.

Platí: $\forall n \in \mathbb{N}_0$ $n+0 = n$ protože $\sigma^0(m) = 1_{\mathbb{N}_0}(m) = m$ ok.

$\forall m, n \in \mathbb{N}_0$ $m + \sigma(n) = \sigma(m+n)$ protože $\sigma^{\sigma(n)}(m) = (\sigma \circ \sigma^n)(m)$

$$\sigma(\sigma^n(m)) = \sigma(m+n) \quad \text{ok.}$$

$\forall m \in \mathbb{N}_0$ $m \cdot 0 = 0$ protože $(\sigma^m)^0(0) = 1_{\mathbb{N}_0}(0) = 0$ ok.

$\forall m, n \in \mathbb{N}_0$ $m \cdot \sigma(n) = m \cdot n + m$ protože

$$\begin{aligned} (\sigma^m)^{\sigma(n)}(0) &= (\sigma^m \circ \sigma^n)(0) = \sigma^m(\underbrace{(\sigma^n)^1(0)}_{m \cdot n}) = \\ &= \sigma^m(m \cdot n) = m \cdot n + m. \quad \text{ok.} \end{aligned}$$

$f^1 = f$ pro každé $f: X \rightarrow X$,

$$\text{protože } f^1 = f^{\sigma(0)} = f \circ (f^0) = f \circ 1_X = f$$

$\forall n \in \mathbb{N}_0$ $n+1 = \sigma(n)$, viz bod 2, kde $m + \sigma(n) = \sigma(m+n)$
 $n + \underbrace{\sigma(0)}_{=1} = \sigma(n+0) = \sigma(n)$.

nebo z def, $n+1 = \sigma^1(n) = \sigma(n)$.

$\forall n \in \mathbb{N}_0$ $n \cdot 1 = n$ protože $n \cdot 1 = (\sigma^n)^1(0) = \sigma^n(0) = n$.

Pro iterace funkce $f: X \rightarrow X$ platí:

$$\forall m, n \in \mathbb{N}_0 \quad f^m \circ f^n = f^{m+n}$$

dle: indukci na n při pevném m :

$$\cdot f^m \circ f^0 = f^m \circ 1_X = f^m = f^{m+0}$$

$$\cdot f^m \circ f^{\delta(n)} = f^m \circ f \circ f^{\delta(n-1)} \stackrel{\text{komutace}}{=} f \circ f^m \circ f^{\delta(n-1)} = f \circ f^{m+\delta(n-1)} = f^{m+\delta(n)} = f^{m+\delta(n)}$$

Věta: Sčítání na $\mathbb{N}_0$ je asociativní operace a komutativní, 0 je neutrálním prvkem.

Navíc platí

Zákon křádeu: $\forall m, n, k \in \mathbb{N}_0: m+k = n+k \Rightarrow m=n$

a pravidlo $\forall m, n \in \mathbb{N}_0: m+n = 0 \Leftrightarrow m=n=0$.

dle: komutativita:

$$m+n = \sigma^{m+n}(0) = (\sigma^m \circ \sigma^n)(0) \stackrel{\text{komutace iter. prvk.}}{=} (\sigma^n \circ \sigma^m)(0) = \sigma^{n+m}(0) = n+m$$

asociativita:

$$(m+n)+k = \sigma^k(m+n) = \sigma^k(\sigma^{m+n}(0)) = (\sigma^k \circ \sigma^m \circ \sigma^n)(0)$$

$$m+(n+k) = \sigma^{m+k}(m) = \sigma^{m+k}(\sigma^n(0)) = (\sigma^m \circ \sigma^k \circ \sigma^n)(0) \stackrel{\text{komutace + asociativita iterace, sčítání}}{=} (\sigma^m \circ \sigma^n \circ \sigma^k)(0)$$

o neutrální: už bylo.

křádeu: σ prosté $\Rightarrow \sigma^k$ prosté $\forall k \in \mathbb{N}_0$.

$$m+k = n+k \quad \downarrow \quad \sigma^k(m) = \sigma^k(n) \Rightarrow m=n$$

pravidlo: $\Leftarrow 0+0=0$ už bylo.

$\Rightarrow m$ nebo $n \neq 0 \Rightarrow m+n \neq 0$. Komut, takže BČNO $m \neq 0$.

$$m+n = \sigma^n(m) \stackrel{\substack{n \neq 0, \exists k \in \mathbb{N}_0 \\ \text{tak, že } n = \sigma(k)}}{=} \sigma^{\sigma(k)}(m) = (\sigma \circ \sigma^k)(m) = \sigma(\sigma^k(m)) \neq 0$$

přímý axiom

Pro iterace funkce $f: X \rightarrow X$ dále platí:

15

$$\bullet \forall m, n \in \mathbb{N}_0 \quad (f^m)^n = f^{m \cdot n}$$

dl: indukci na n při pevném m .

$$\bullet (f^m)^0 = 1_X = f^0 = f^{m \cdot 0}$$

$$\bullet (f^m)^{S(n)} = f^m \circ (f^m)^n = f^m \circ f^{m \cdot n} = f^{m \cdot n + m} = f^{m \cdot S(n)}$$

Věta: Násobení v $\mathbb{N}_0$ je komutativní a asociativní binární operace, kde 1 je neutrálním prvkem.

Navíc platí

Distributivita vůči sčítání: $\forall m, n, k \in \mathbb{N}_0$

$$(m+n) \cdot k = m \cdot k + n \cdot k$$

Pravidlo: $\forall m, n \in \mathbb{N}_0 \quad m \cdot n = 0 \Leftrightarrow m = 0$ nebo $n = 0$.

dl: komutativita.

$$m \cdot n = (\sigma^m)^n(0) = \overset{m \cdot n = S^n}{\sigma^{m \cdot n}}(0) = (\sigma^n)^m(0) = n \cdot m$$

z odst. iterací

asociativita

$$(m \cdot n) \cdot k = (\sigma^{m \cdot n})^k(0) = ((\sigma^m)^n)^k(0) = (\sigma^m)^{n \cdot k}(0) = m \cdot (n \cdot k)$$

1 neutrální $m \cdot 1 = (\sigma^m)^1(0) = \sigma^m(0) = m$

distributivita: $\forall m, n, k$ indukci na k pro pevném m, n .

$$\bullet (m+n) \cdot 0 = 0 = 0 + 0 = 0 + n \cdot 0$$

$$\bullet (m+n) \cdot S(k) = (m+n)k + (m+n) = m \cdot k + n \cdot k + m + n = (mk + m) + (nk + n) = m \cdot S(k) + n \cdot S(k) \quad \text{ok}$$

Pravidlo: ukažeme $m \neq 0$ a $n \neq 0 \Leftrightarrow m \cdot n \neq 0$

$$m = S(k), \text{ pak } m \cdot n = m \cdot S(k) = mk + m \neq \underset{\neq 0}{m \cdot 0} + \dots$$

dle pravidla pro +

Uspořádaní na N_0

16

Def: Pro $m, n \in N_0$ pokládáme
 $m \leq n$ když $\exists x \in N_0$ tak, že $m + x = n$.

Platí: Relace $\leq$ na N_0 je uspořádaní. Nartě.

- $\forall n \in N_0, 0 \leq n$.
- $\forall n \in N_0, n < \sigma(n)$
- $\forall n \in N_0 \setminus \{0\}, 1 \leq n$.

Dle: Dikaz, že $\leq$ je uspořádaní:

1) reflexivita: $\forall n \in N_0$ je $n = n + 0$, proto $n \leq n$.

2) antisym: Necht pro $m, n \in N_0$ je $m \leq n$ a $n \leq m$. Tj. $\exists x, y \in N_0$
tak, že $n = m + x$ a $m = n + y$. Proto
 $n = m + x + y = n + 0$, ke kterému kráčíme pak $x + y = 0$ a podle pravidla o nule je $x = y = 0$.

3) transitiv: Odtud $n = m + 0 = m$.
Necht $m, n, k \in N_0$: $m \leq n, n \leq k$. Pak $\exists x, y \in N_0$
tak, že $n = m + x, k = n + y$. Dosadíme,
tj. $k = m + (x + y)$, proto $m \leq k$.

Dikaz, že $\forall n \in N_0, 0 \leq n$: $\forall n$ máme $n = 0 + n$, tj. $n \geq 0$
 $n < \sigma(n)$: $\forall n$ máme $\sigma(n) = n + 1$, proto $\sigma(n) \geq n$.
Zdroveč $n \neq \sigma(n)$ a odtud $n < \sigma(n)$.

Dikaz, že $\forall n \in N_0 \setminus \{0\}$ je $1 \leq n$. indukci:

$A = \{0\} \cup \{n \in N_0 \mid 1 \leq n\}$. Chci ukázat, že $A = N_0$.

$0 \in A \checkmark$

Ať A platí pro n . Bud $n = 0$, pak $\sigma(n) = 1 \geq 1$ k reflex. $\checkmark$
nebo $n \geq 1$, pak $\sigma(n) > n \geq 1$, proto z tranz. $\checkmark$.

Pozn: Dle Arricu' neleží mezi 0 a 1 žádný prvek, tj.
 $0 < 1$ a pokud $0 \leq n \leq 1$, pak $n = 0$ nebo $n = 1$.

Pozn: $m < n$ když $m \leq n$ a $m \neq n$, tj. $\exists x \in N_0, x \neq 0$ tak, že
 $n = m + x$.
(když $x = 0$, pak $n = m + 0 = m$.)

17

Tvrzení: (monotonie uspořádání na $\mathbb{N}_0$):

Pro všechna $m, n, k \in \mathbb{N}_0$ platí:

$$\bullet m < n \Rightarrow m+k < n+k$$

$$\bullet m < n \wedge k \neq 0 \Rightarrow m \cdot k < n \cdot k.$$

dk: $\bullet m < n$ je def, když $\exists x \in \mathbb{N}_0 \overset{x \neq 0}{\text{tak, že } n = m+x}$. Proto

$$\Rightarrow n+k = m+x+k = (m+k)+x \text{ a odtud } m+k < n+k.$$

$$\Rightarrow n \cdot k = (m+x) \cdot k = m \cdot k + x \cdot k, \text{ dle zákona o násobení } x \cdot k \neq 0. \\ \text{proto } m \cdot k < n \cdot k.$$

Tvrzení:

Pro všechna $m, n \in \mathbb{N}_0$ platí $m < n \Rightarrow \sigma(m) \leq n$.

dk: z příkl. $\exists x \in \mathbb{N}_0, x \neq 0$ tak, že $n = m+x$.

Protože $x \neq 0, \exists y \in \mathbb{N}_0$ tak, že $x = \sigma(y) = y+1$.

$$\text{Pak } n = m + \sigma(y) = m + y + 1 = m + 1 + y = \sigma(m) + y.$$

$$\text{Odtud } \sigma(m) \leq n.$$

Věta: Uspořádání $\leq$ na $\mathbb{N}_0$ je dobré (a proto úplné).

dk: $\exists$ def. nutno ukázat, že každá neprázdná podmnožina $\mathbb{N}_0$ má nejmenší prvek.

Zvolme $A \subset \mathbb{N}_0$, množina i prázdná.

Def: $M_A = \{ k \in \mathbb{N}_0 \mid \forall m \in A \text{ platí } k \leq m \}$
je množina dolních kámar množiny A v $\mathbb{N}_0$.

$$\text{ukážeme } M_A \cap A = \emptyset \Rightarrow M_A = \mathbb{N}_0. \quad (*)$$

indukcí: $0 \in M_A$, protože $\forall m \in \mathbb{N}$ je $0 \leq m$.

$$\text{chci } k \in M_A \Rightarrow \sigma(k) \in M_A.$$

$$k \in M_A \Rightarrow \forall m \in A \text{ je } k \leq m \Rightarrow k < m. \text{ Proto } \sigma(k) \leq m. \\ \Rightarrow k \notin A, \text{ tj. } k \neq m \text{ tj. } \sigma(k) \in M_A.$$

$$\text{Proto } M_A \cap A = \emptyset \Rightarrow A = \emptyset.$$

Zvolme $A \neq \emptyset$. Tj. obsahuje n .

18

Pro něj $n < \sigma(n)$. Z toho platí $\sigma(n) \notin M_A$, tudíž $M_A \neq N_0$.

Dle výše uvedené implikace $\otimes$ nutně $M_A \cap A \neq \emptyset$.

Volíme $m_0 \in M_A \cap A$, což je prvek, který splňuje

$\forall m \in A$ je $m_0 \leq m$, tj. je nejmenším prvkem v A . $\square$

Pozn. Ukázali jsme vlastně, že každá neprázdna podmnožina $\tau \mathbb{N}$ obsahuje nějakou svou dolní hranici.

Tvorba (křáclů pro násobení)

$\forall m, n, k \in \mathbb{N}_0 \setminus \{0\}$ platí $m \cdot k = n \cdot k \Rightarrow m = n$.

dk: platí pro $k=1$ $m = m \cdot 1 = n \cdot 1 = n$ $\checkmark$

Sporem. předel. $m \cdot k = n \cdot k$ a přitom $m \neq n$.

$\xrightarrow{\text{z úplnosti uspořádání}}$ Proto buď $m > n$ nebo $n > m$, BŮDO $n > m$, tj.

$\exists j \in \mathbb{N}_0 \setminus \{0\}$ tak, že $n = m + j$.

Máme $m \cdot k = (m + j) \cdot k = m \cdot k + j \cdot k$

Z křáclů pro sčítání máme $m \cdot k + 0 = m \cdot k + j \cdot k \Rightarrow j \cdot k = 0$.

Z pravidla pro nulu u násobení je $j=0$ nebo $k=0$,

ale $k \neq 0$ z předel., proto $j=0$, tudíž $n = m + 0 = m$. $\checkmark$

Opakování Peanových axiomů:

Def: $(N_0, \sigma, 0)$ N_0 množina, $\sigma: N_0 \rightarrow N_0$, $0 \in N_0$

(1) σ prosté (2) $0 \notin \sigma(N_0)$ (3) $\forall M \subset N_0: 0 \in M, \sigma(M) \subset M \Rightarrow M = N_0$.

Iterace zobrazení $f^0 = 1_x$, $f^{\sigma(n)} = f \circ f^n$

Aritmetické operace $m+n := \sigma^n(m)$
 $m \cdot n = (\sigma^m)^n(0)$

Sečítání: asociativní, komutativní, 0 neutrální

krácení: $m+k = n+k \Rightarrow m = n$

zákon nuly: $m+n=0 \Leftrightarrow m=n=0$

Násobení: asociativní, komutativní, 1 neutrální

distributivita: $(m+n)k = mk + nk$

zákon nuly: $m \cdot n = 0 \Leftrightarrow m=0$ nebo $n=0$

Uspořádaní $m \leq n$ když $\exists x: m+x = n$
pern. $m < n$ když

Moluitnost množin

19

Def: Množiny M, N mají stejnou moluitnost (kardinalitu), pokud jsou ekvivalentní (tj. existuje bijekce $M \rightarrow N$).
Píšeme $\text{card}(M) = \text{card}(N)$ (Dříve také $M \sim N$).

Def: Množina M je subvalentní množině N , když existuje injektivní zobrazení $f: M \rightarrow N$.

Pozn: M subvalentní N znamená N je ekvivalentní nějaké $\tilde{M} \subset N$.

Připomenutí: Množina je spočetná, je-li ekvivalentní $\aleph_0$.
Konkrétně, když je ekvivalentní $\{1, 2, \dots, n\}$ pro nějaké $n \in \mathbb{N}$.
Spočetné sjednocení spočetných je spočetné.

dle $\mathbb{Q} \sim \mathbb{N}$, $\mathbb{Z} \sim \mathbb{N} \rightarrow$ na cv.

$\mathbb{R}$ je nespočetná (Cantorovo diag. schéma)

$\mathbb{R} \sim \mathbb{R}^2$ přes rozvoj (viz Prop. from the Book.)

Všechy dlouhé intervaly $()$, $[]$, $(]$, $[)$ mají stejnou moluitnost. (viz /)

Všechy intervaly (velikosti) mají stejnou.

Open interval je ekv. $\mathbb{R}$.

ozn: $\mathcal{C}(\text{continuum}) = \text{card}(\mathbb{R})$.

V: Každá nekonečná množina obsahuje spočetnou podmnožinu.

dle: $|C| = +\infty$, vyberáme $D = \{d_1, d_2, \dots\}$ spočetnou takto:

d_1 libo. $\in C$, d_2 libo. $\in C \setminus \{d_1\}$, obecně d_n libo. $\in C \setminus \{d_1, \dots, d_{n-1}\}$.

Protože C nekonečná, tak $C \setminus \{d_1, \dots, d_{n-1}\} \neq \emptyset \quad \forall n$.

ozn: $\aleph_0 = \text{Card}(\aleph_0)$ „alef nula“.

Z v. plyne, že $\aleph_0$ je nejmenší nekonečná kardinalita.

Pozn: dle se zda' jednoznačný, ale možnost výběru z nekonečného systému vyžaduje Axiom výběru.

Def: Necht M je libovolná množina. Zobrazení 20

$f: P(M) \setminus \{\emptyset\} \rightarrow M$ takové, že

$\forall X \subset M, X \neq \emptyset$ je $f(X) \in X$ se nazývá
selektor (výběrová funkce) na M .

Axiom výběru Pro každou množinu M existuje selektor na M .

Budeme o tom mluvit detailněji později.

Abychom se vyrovnali s různými nekonečnými,
pavedeme si na nich uspořádání.

Def: M je subvalentní množinou N , když
existuje injekce $f: M \rightarrow N$.

Pozn: M je subvalentní N , když je ekvivalentní
s nějakou podmnožinou množiny N .

Je to uspořádání?

1) Reflexivita M je subvalentní sama sobě

2) Transitivita M, N, P , injekce $f: M \rightarrow N, g: N \rightarrow P$, pak
složením $g \circ f: M \rightarrow P$ je injekce a tedy
 M je subvalentní P .

3) Antisymetrie - samo určité ne, protože
 M subv. N a N subv. M neznamená $M=N$

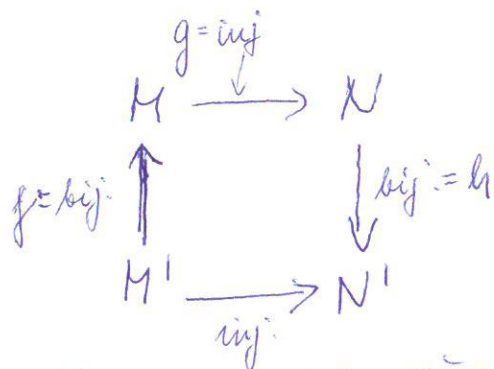
Př. $\{1,2\} \rightarrow \{2,3\}$ ale nerovná se.

Co třeba, nahradit = ekvivalentní množin?

Tj. poradit uspořádání na třídách $[]_{\sim}$?

Bern: Kompatibilita subvalence a ekvivalence: 21

Nechť $M \sim M'$ a $N \sim N'$. Když M je subvalentní N ,
pak M' je subvalentní N' .



obrazem' hogo f: $M' \rightarrow N'$
je injekce.

→ tj. subvalenci lze přenést na třídy ekvivalence.

Nutno dokázat antisymetrii; tj. $[M]_N \text{ subv. } [N]_N$
a $[N]_N \text{ subv. } [M]_N$, pak $[M]_N = [N]_N$.

Věta: (Cantor - Bernstein - Schröder):

Jestliže pro množiny M, N platí, že M je
subvalentní N a N je subvalentní M , pak
 M je ekvivalentní N .

Lemma: Necht' M, N jsou množiny a $\varphi: M \rightarrow M$ je injekce.
Taková, že $\varphi(M) \subset N \subset M$. Pak $M \sim N$.

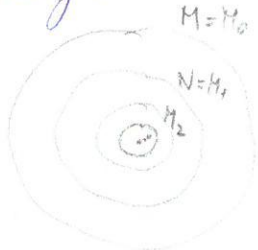
dle: Vyrobím posloupnost množin $M_0 := M, M_1 := N$.

$$M_{2k} := \varphi^k(M_0); \quad M_{2k+1} := \varphi^k(M_1)$$

Z předl. víme $M_1 \subset M_0$ odkud $M_{2k+1} = \varphi^k(M_1) \subset \varphi^k(M_0) = M_{2k}$ $\forall k$

a $\varphi(M_0) \subset M_1$ plyne $M_{2k+2} = \varphi^{k+1}(M_0) \subset \varphi^k(M_1) = M_{2k+1}$.

Proto je řetězec $M_0 \supset M_1 \supset M_2 \supset \dots \supset M_{2k} \supset M_{2k+1} \supset M_{2k+2} \supset \dots$



Zdokreň mi me

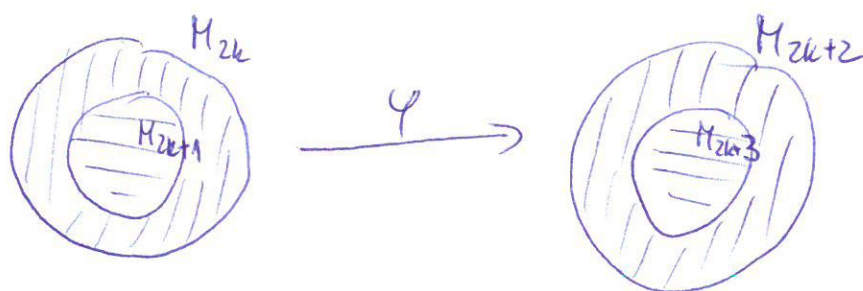
22

$$M_{2k+2} = \varphi^{k+1}(M_0) = \varphi(\varphi^k(M_0)) = \varphi(M_{2k})$$

$$M_{2k+3} = \varphi^{k+1}(M_1) = \varphi(\varphi^k(M_1)) = \varphi(M_{2k+1})$$

$\varphi|_{M_{2k}} : M_{2k} \rightarrow M_{2k+2}$ je bijekce

$\varphi|_{M_{2k+1}} : M_{2k+1} \rightarrow M_{2k+3}$ je bijekce.



Tedy φ je bijekce mezi $M_{2k} \setminus M_{2k+1} \rightarrow M_{2k+2} \setminus M_{2k+3}$.

Položíme $P = \bigcap_{k=0}^{\infty} M_k$.

Pak následující zjednocení je disjunktivní

$$M = P \cup \left(\bigcup_{k=0}^{+\infty} (M_k \setminus M_{k+1}) \right) =$$

$$= P \cup \left(\bigcup_{k=0}^{+\infty} (M_{2k} \setminus M_{2k+1}) \right) \cup \left(\bigcup_{k=0}^{+\infty} (M_{2k+1} \setminus M_{2k+2}) \right)$$

$$N = P \cup \left(\bigcup_{k=1}^{+\infty} (M_k \setminus M_{k+1}) \right) =$$

Definujeme $\psi : M \rightarrow N$ takto

$$\psi(x) = \begin{cases} x & \text{pro } x \in P \cup \bigcup_{k=0}^{+\infty} (M_{2k+1} \setminus M_{2k+2}) \\ \varphi(x) & \text{pro } x \in \bigcup_{k=0}^{+\infty} (M_{2k} \setminus M_{2k+1}) \leftarrow \text{šrafované} \end{cases}$$

Možnosti:

24

- 1) A subvalentní B , B subvalentní $A \xRightarrow{\text{CBS}} A \sim B$
- 2) A subvalentní B , B není subv. $A \Rightarrow \text{card}(A) < \text{card}(B)$
- 3) A není subv. B , B subvalentní $A \Rightarrow \text{card}(A) > \text{card}(B)$
- 4) A není subv. B , B není subv. $A \Rightarrow ?$

Musíme ukázat, že 4) nelze, tj. platí trichotomie.

↳ Bude třeba axiom vytknutí, spec. jeho ekvivalentní formulace $\rightarrow$ věta o dobrém uspořádání !

Věta (Zermelo): Každou množinu M lze dobře uspořádat.

Vlastnosti uspořádání kardinalit:

Věta (Cantor): Pro libv. množinu M platí $\text{card}(M) < \text{card}(P(M))$.

dk: Ukážeme, že M je subvalentní $P(M)$ a že není ekvivalentní.

Zřejmé $f: M \rightarrow P(M): x \mapsto \{x\}$ je prosté.

Nicméně nemůže existovat surjektivní zobrazení $M \rightarrow P(M)$.

Sporem. Necht $g: M \rightarrow P(M)$ je surjektivní.

Dku. $D := \{x \in M \mid x \notin g(x)\}$.

Ze surjektivty plyne, že $\exists d \in M$ tak, že $g(d) = D$.

Zjistíme, zda $d \in D$. Z definice D platí $d \in g(d) = D$, právě když $d \notin g(d) = D$. To je spor.

Důsledek: Nelze zavést univerzální množinu $\mathcal{U}$ všech množin. Jinak by $\exists M \in \mathcal{U}$

$$M \approx \{ \{x\} \mid x \in M \} \subset \mathcal{U} \text{ a proto}$$

$\mathcal{U}$ by mělo mít největší ze všech mohutností!

$\text{Ale } \text{card}(P(\mathcal{U})) > \text{card } \mathcal{U}$, přičemž

$P(\mathcal{U}) \in \mathcal{U}$, což implikuje $\text{card}(P(\mathcal{U})) \leq \text{card}(\mathcal{U})$ spor.

Pozn: Pro každé dvě množiny M, N platí

$N \subset M$, pak $\text{card}(N) \leq \text{card}(M)$.

Ža prosté zobrazení $N \rightarrow M$ volíme id.

Ordinální a kardinální čísla

26

Def: Dvě ^{úplně uspořádané} množiny mají stejný ordinální typ, pokud jsou podobně uspořádané ($\exists$ bijekce, která zachovává uspořádání).
Dvě dobře uspořádané množiny s podobným uspořádáním mají stejné ordinální číslo (ordinal).
Píšeme $\text{ord } A = \text{ord } B$

Pozn: Všechny konečné úplně usp. množiny mají stejný ord. typ, jsou podobné $\{0, \dots, n-1\} = (N_0)_n$ s přir. uspořádáním, tj. jsou dobře uspořádané. Značíme $n = \text{ord } \{0, \dots, n-1\}$.

Pozn: Na ordinálních číslech pak zavedeme operace a uspořádání, ukážeme, že je dobré $\rightarrow$ (Pozor, nelze zavést množinu všech ord. č., tj. bude neoproteno jistě)

Def: Uspořádané sjednocení $M_1 + M_2$

pro $(M_1, \leq_1), (M_2, \leq_2)$ je $(M_1 \dot{\cup} M_2, \leq)$, kde

$$\forall x, y \in M_1: x \leq y \Leftrightarrow x \leq_1 y$$

$$\forall x, y \in M_2: x \leq y \Leftrightarrow x \leq_2 y$$

$$\forall x \in M_1, \forall y \in M_2: x < y.$$

Uspořádaný kartézský součin $M_1 \cdot M_2$

pro $(M_1, \leq_1), (M_2, \leq_2)$ je $(M_1 \times M_2, \leq)$, kde

$$\forall x_1, y_1 \in M_1, \forall x_2, y_2 \in M_2 \text{ stanovíme}$$

$$(x_1, x_2) \leq (y_1, y_2) \Leftrightarrow (x_2 <_2 y_2) \text{ nebo } (x_2 = y_2 \wedge x_1 <_1 y_1)$$

tj. opět lexikografické uspořádání.

Př: $M_1 = M_2 = \{a < b\}$, pak $(a, a) < (b, a) < (a, b) < (b, b)$.

Platí: jsou-li M_1, M_2 úplně (dobře) uspořádané, pak také splňují $M_1 + M_2$ i $M_1 \cdot M_2$. $\rightarrow$ rozmysli

Def: Necht A, B jsou množiny dobře uspořádané,
 $\alpha = \text{ord } A, \beta = \text{ord } B$. Zavedeme

$$\alpha + \beta := \text{ord}(A+B)$$

$$\alpha \cdot \beta = \text{ord}(A \cdot B)$$

Pozor! Nejsou to komutativní operace!

Známé: $\omega := \text{ord } \mathbb{N}_0$ ($\mathbb{N}_0$ je standardně usp.)

$$n := \text{ord} \{0, 1, \dots, n-1\} = \text{ord}((\mathbb{N}_0)_n) \leftarrow \text{n uspoř. prvků z } \mathbb{N}_0.$$

$$0 := \text{ord } \emptyset$$

Př: $\boxed{1 + \omega = \omega}$

$$\{b\} \cup \{a_0, a_1, a_2, \dots\}$$

$$b < a_0 < a_1 < a_2 < a_3 < \dots$$

$\hookrightarrow$ Podobně uspořádání
 ke standardnímu usp. na $\mathbb{N}_0$

obdobně

$$\{b_1, b_2, \dots, b_m\} \cup \{a_1, a_2, a_3, \dots\} \quad b_1 < b_2 < \dots < b_m < a_1 < a_2 < \dots$$

$$\boxed{m + \omega = \omega}$$

Alé! $\boxed{\omega + 1 \neq \omega}$

$$\{a_0, a_1, a_2, \dots\} \cup \{b\} \quad a_0 < a_1 < a_2 < \dots < b$$

Dobře uspořádaná s posledním prvkem (v $\mathbb{N}_0$ není)

Navíc $\omega + 1 \neq \omega + 2 \neq \omega + 3, \dots$ všechny od sebe různé.

Př: $\boxed{\omega + \omega}$

$$\{a_1, a_2, a_3, \dots\} \cup \{b_1, b_2, b_3, \dots\} \quad a_1 < a_2 < a_3 < \dots < b_1 < b_2 < b_3 < \dots$$

Obdobně $\omega + \omega + \omega, \omega + \omega + \omega + \omega, \dots$

Pozn: Je třeba ověřit, že to je asociativní. Zřejmé! $\rightarrow \omega$

Př: $2 \cdot \omega$

28

$\{1, 2\} \times \mathbb{N}$... Píšeme pro $(1, k) \leftrightarrow a_k$
 $(2, k) \leftrightarrow b_k$

četná lex. uspořádání dává

$$a_1 < b_1 < a_2 < b_2 < a_3 < b_3 < \dots$$

zřejmě podobné $\mathbb{N}_0$. Proto $2 \cdot \omega = \omega$

$\omega \cdot 2$

$\mathbb{N} \times \{1, 2\}$ Píšeme $(k, 1) \leftrightarrow a_k$
 $(k, 2) \leftrightarrow b_k$

$$a_1 < a_2 < a_3 < \dots < b_1 < b_2 < b_3 < \dots$$

Proto $\omega \cdot 2 = \omega + \omega$

Pozn: Kdybychom chtěli ukázat, že $\omega + \omega \neq \omega$,
jak např. tím, že všechny $\in \mathbb{N}_0$ jsou konečné,
kdyžto $\mathbb{N} \cdot \{1, 2\}$ obsahuje nekonečné úseky

podobné $n \cdot \omega = \omega$ ale $\omega \cdot n = \underbrace{\omega + \omega + \dots + \omega}_{n\text{-krát}}$

Př: množina $\mathbb{N}_0 \times \mathbb{N}_0$ uspořádaná

$$\begin{aligned} a_0 &< a_1 < a_2 < \dots \\ < b_0 < b_1 < b_2 < \dots \\ < c_0 < c_1 < c_2 < \dots \\ &< \dots \end{aligned}$$

Dle sčítání je to $\omega + \omega + \omega + \dots$

Dle násobení je to $\omega \cdot \omega = \omega^2$

Proto $\omega^2 = \omega + \omega + \omega + \dots$

Pozn: Lze ukázat, že platí $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ distrib. zákon
obecně neplatí $(\beta + \gamma)\alpha = \beta\alpha + \gamma\alpha$

Lemma: Necht M je dobře uspořádaná, $N \subset M$.

Je-li $f: M \rightarrow N$ izomorfismus usp. množin,
pak $\forall x \in M$ platí $x \leq f(x)$.

dk: Transfinitní indukce. $A = \{x \in M \mid x \leq f(x)\}$.

Vyberu $a \in M$ tak, že $M_a \subset A$. Chci ukázat, že pak $a \in A$.

To už bude implikovat $A = M$.

Sporem: Kdyby $a \notin A$, tak $f(a) < a$. Protože

f je izomorfismus, platí $f(f(a)) < f(a)$.

Zároveň ale $f(a) < a$ implikuje $f(a) \in M_a \subset A$.

Takže $f(a) \leq f(f(a))$. To je spor.

! Využívám fakt, že M je dobře uspořádaná, jen tomu totiž platí transfinitní indukce!

Věta: Dvě dobře uspořádané množiny nemají podobnou strukturu podle uspořádání.

dk: Necht M je dobře uspořádaná. Sporem:

Připel, že $a \in M$ a $f: M \rightarrow M_a$ je podobnost.

Proto $f(a) \in M_a$, tj. $f(a) < a$.

Ale lemma implikuje, že $a \leq f(a)$. Spor.

Důsledek: Necht A, B jsou dobře usp., $\alpha = \text{ord } A, \beta = \text{ord } B$.

Jestliže $\alpha \leq \beta$ a současně A, B nejsou podobné,

pak $\exists b \in B$ tak, že A je podobná B_b a naopak,

je-li A podobná B_b pro nějaké $b \in B$, nebude $\alpha = \beta$.

Lze tedy psát:

$$\alpha < \beta \iff \alpha \leq \beta \wedge \alpha \neq \beta \iff \exists b \in B \text{ tak, že } A \text{ je podobná } B_b.$$

$$\iff \exists b \in B \text{ tak, že } \alpha = \text{ord } B_b$$

Uspořádání na ordinálních číslech

29

Zavedeme pomocí pojmu úsek α ^{úplně} $(M, \leq)$, tj. $M_\alpha = \{x \in M \mid x < \alpha\}$.
pro prvek $\alpha \in M$.

Pozn: $\forall (M, \leq)$ ^{úplně} pro dva prvky $a, b \in M$ platí

$$a \leq b \Leftrightarrow M_a \subset M_b$$

$$a < b \Leftrightarrow M_a \subsetneq M_b.$$

Pokud $a < b$, pak M_b - úplně uspoř. množina $(M_b, \leq)$
platí $(M_b)_a = M_a$.

Def: Pro dobře uspořádané množiny A, B ,

$\alpha = \text{ord } A$, $\beta = \text{ord } B$, klademe

$\alpha \leq \beta$, kdež A je ^{= podobná} izomorfní s B nebo nějakým
jejím úsekem.

Pozn: Nezávisí na volbě $\tilde{A}, \tilde{B}$ se stejným $\alpha = \text{ord } \tilde{A}$, $\beta = \text{ord } \tilde{B}$
ordinálním číslem.

Platí: Takto definovaná relace je uspořádaná.
(pozor, ord. č. neboli množ.)

dk: Reflexivita ... křepme!

Transitivita ... křepme!

Antisymetrie? Dokažeme dokonce trichotomií.
(úplnost usp.)

Postupně. Nejprve antisym.

Důsledek:

Uspořádaná ord. čísel $\leq$ je antisymetrická.

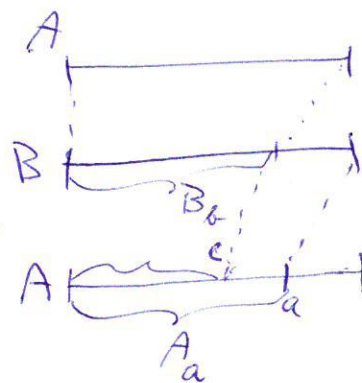
dh: Necht $\alpha \leq \beta, \beta \leq \alpha, \alpha \neq \beta$ (sporem). Tzn.

A je podobná B_α , B podobná A_α pro nějaké $a \in A, b \in B$.

Pak $\exists c \in A$ tak, že B_α je

podobná A_c , tj.

A je podobná A_c . spor s větou.



Chceme ještě ukázat, že usp. ord. čísel je úplná (jak platí trichotomie).

Ekvivalentně: Jou-li A, B dobře uspořádané množiny, pak se aspoň jedna dá podobně zobrazit na úsek druhé.

K důkazu bude třeba:

- 1) Nepřechujeme s třídou všech množin, aby nastal problém. Místo toho zvolíme dostatečně velkou množinu U , aby měly množiny, které budeme uvažovat, byly $\subset P(U)$. Při dk. porovnatelnosti A, B stačí $U = A \cup B$.
- 2) Ze všech dobře uspořádaných množin, které jsou si podobné (tj. mají stejné ordinální číslo) si zvolíme reprezentanta, a tím bude množina všech ordinálních čísel $< \alpha$.
např. $\alpha = \text{ord } A$, kde $A = \{0, 1, \dots, \alpha-1\}$.
podobně $\omega = \text{ord } A$, kde $A = \mathbb{N}_0 = \{0, 1, 2, \dots\}$

Formálně: Necht U je dostatečně velká množina.

32

$$\tilde{W} := \{ \text{ord } A \mid A \text{ je dobře uspořádaná } A \in \mathcal{P}(U) \}.$$

Pro zvolenou $C \in \mathcal{P}(U)$ dobře uspořádanou označíme $\gamma = \text{ord } C$ a

$$W(\gamma) := \{ \beta \in \tilde{W} \mid \beta < \gamma \}.$$

Pozn: • Kdyby $\leq$ bylo úplně uspořádané, byl by $W(\gamma)$ úsek v množině všech ord. čísel. Ale! 1) nevíme, zda je úplně, 2) může obsahovat množ. všech ord. čísel. Ale stejně jako u úseků:

$$\forall \delta \in W(\gamma) \text{ platí } W(\delta) \subsetneq W(\gamma).$$

• Navíc platí

$$W(\alpha) = \{ \text{ord } A_b \mid b \in A \}$$

→ máme A dobře uspoř. $\alpha = \text{ord } A$, pak $\forall \beta = \text{ord } B \in \tilde{W}$ platí $\beta < \alpha$, právě když $\beta = \text{ord } A_b$ pro nějaké $b \in A$.

• Zobrazení $f: A \rightarrow W(\alpha)$, které pro $b \in A$ přiřadí
 $f(b) = \text{ord } A_b$

je podobnost dobře uspořádaných množin.
(je to surjektivní, zachovává uspoř., tj. je injektivní a podob.)

• Proto $\alpha = \text{ord } A = \text{ord } W(\alpha)$.

Lemma: Bud' α, β ordinální čísla. Položme
 $\gamma = \text{ord}(W(\alpha) \cap W(\beta))$. Potom platí:

- 1) $W(\alpha) \cap W(\beta) = W(\gamma)$ a $\gamma \leq \beta, \gamma \leq \alpha$.
- 2) Nenastane současně $\gamma < \beta, \gamma < \alpha$.

dh: 1) Označme $C = W(\alpha) \cap W(\beta)$. Dokažme $C = W(\gamma)$.

Prvně $C \neq \emptyset$, protože $0 = \text{ord } \emptyset \in C$.

C je dobře uspořádaná ($C \subset W(\alpha)$, kde $W(\alpha)$ je dobře usp.)

Předpokládejme a) $C = W(\alpha)$. Pak

$$\begin{aligned} \gamma &= \text{ord } C = \text{ord } W(\alpha) = \alpha \\ \text{tj. } C &= W(\alpha) = W(\gamma) \end{aligned}$$

b) $C \subsetneq W(\alpha)$. Pak

$$(*) \quad \forall \xi \in C \quad \forall \eta \in W(\alpha) \setminus C \quad \text{platí} \quad \xi < \eta$$

(plyne z toho, že ξ a η jsou prvky dobře usp. množiny, tedy porovnatelné, a navíc $\xi \neq \eta$, jelikož leží v disj. množinách. Možnost $\eta < \xi$ vyloučíme, protože pak by $\eta < \xi < \beta$, což znamená $\eta \in W(\alpha) \cap W(\beta) = C$, spor s jistou volbou. $\xi \in C \subset W(\beta)$)

Vezmeme nejmenší prvek množiny $W(\alpha) \setminus C$, označ. σ .

Z vlastností výše $W(\sigma) \subset W(\alpha)$, a $(*)$ $W(\sigma) \supset C$.

Naopak σ je nejmenší v $W(\alpha) \setminus C$, tj. $W(\sigma) \cap (W(\alpha) \setminus C) = \emptyset$,
 tj. $W(\sigma) \subset C$. Proto $W(\sigma) = C$.

Odtud máme

$$\begin{aligned} \gamma &= \text{ord } C = \text{ord } W(\sigma) = \sigma < \alpha \\ \text{tj. } C &= W(\sigma) = W(\gamma) \end{aligned}$$

Tím je dokázána 1) předešlého tvrzení, kdy je $\gamma = \alpha$ a kdy $\gamma < \alpha$,
 podobně to funguje pro $\gamma \leq \beta$.

2) Když současně $\gamma < \beta$ a $\gamma < \alpha$, pak

& 1) máme $\gamma \in W(\alpha) \cap W(\beta) = W(\gamma)$ tj: $\gamma < \gamma$, spor.

34

Věta: Pro uspořádání ordinalních čísel platí trichomie (tj. je to úplně uspořádání na tride ord. čísel)

dk: Předpokl. $\alpha = \text{ord } A$, $\beta = \text{ord } B$, chceme ukázat porovnatelnost α, β . Voleme $A, B \subset U$, tj: $\alpha, \beta \in \tilde{W}$. $\textcircled{+}$

Z lemmatu plyne tři možnosti

(i) $\gamma = \alpha$ a $\gamma = \beta$, tj: $\alpha = \beta$

(ii) $\gamma = \alpha$ a $\gamma < \beta$, tj: $\alpha < \beta$

(iii) $\gamma < \alpha$ a $\gamma = \beta$, tj: $\beta < \alpha$.

Z lemmatu $W(\alpha) \cap W(\beta)$.
Pro $\gamma = \text{ord}(W(\alpha) \cap W(\beta))$ platí
jedna ze 3 možností.

Čtvrtá možnost není.

Důsledek: Mohutnost každých dvou dobře uspořádaných množin jsou porovnatelné.

dk: Ordinalní čísla jsou porovnatelná (bijekce na množinu nebo její úsek).

$$\text{ord } A \leq \text{ord } B \Rightarrow \text{card } A \leq \text{card } B$$

Pozn: Implikace nejde obrátit, nemáme, zda bijekce zachová uspořádání.

Důsledek: Pokud platí věta o dobrém uspořádání, lze porovnat mohutnost každých dvou množin.

Věta o dobrém uspořádání (Zermelo): Na každé množině lze definovat dobré uspořádání.

Pozn: Z každé třídy ^{numérin} ordinálního čísla α vyberáme reprezentanta $W(\alpha)$

ord. č. α numérin ord. čísel $< \alpha$ uspořádané do pořádkového typu α .

0	$\emptyset$... konvence
1	$\{0\}$
2	$\{0, 1\}$
3	$\{0, 1, 2\}$
$\vdots$	
ω	$\{0, 1, 2, \dots\}$
$\omega+1$	$\{0, 1, 2, \dots, \omega\}$
$\omega+2$	$\{0, 1, 2, \dots, \omega, \omega+1\}$
$\vdots$	
$\omega \cdot 2 = \omega + \omega$	$\{0, 1, 2, \dots, \omega, \omega+1, \omega+2, \dots\}$
$\omega \cdot 2 + 1$	$\{0, 1, 2, \dots, \omega, \omega+1, \omega+2, \dots, \omega \cdot 2\}$
$\omega \cdot 2 + 2$	$\{0, 1, 2, \dots, \omega, \omega+1, \omega+2, \dots, \omega \cdot 2, \omega \cdot 2 + 1\}$
$\vdots$	

Def: Ordinalní čísla $\omega, \omega+1, \dots$, jejichž ordinalní typy nemají poslední prvek, se nazývají limitní ord. č.

např. $\omega, \omega \cdot 2, \omega \cdot 3, \omega \cdot 4, \omega \cdot 5, \dots, \omega^2, \omega^2 + \omega, \omega^2 + \omega \cdot 2, \dots$

Ordinalní čísla, jejichž ordinalní typy mají poslední prvek, jsou nelimitní.

Plati: Pro každé ord. č. α je $\alpha+1$ jeho následovníkem,
tj. $\alpha+1$ je nejmenší ordinal větší než α .

dk: $\alpha = \text{ord } A$ pro dobře usp. A . zvolím $b \notin A, B := A \cup \{b\}$.

Pak $\text{ord } B = \alpha+1$, le je největší v $B, A = B \setminus \{b\}$ je největší
úsek v B , tedy α je největší ordinal č. $< \alpha+1$.

ne smyslu
inkluse

Platí: Ordinalní čísla jsou dobře uspořádána. 36

Formálně přesněji:

Je-li $(M, \leq)$ uspořádaná množina, jejímiž prvky jsou ordinally a uspořádání $\leq$ je dáno uspořádáním ordin. čísel, pak M je dobře uspořádána.

dk: Necht' $A \subset M$, $A \neq \emptyset$. Jestliže A má právě jeden prvek, je jistě dobře usp.

Necht' A má alespoň 2 prvky.

Volme $\alpha, \beta \in A$, $\alpha < \beta$.

Pak $\alpha \in A \cap W(\beta) \subset W(\beta)$, přičemž $W(\beta)$ je dobře usp, tedy $A \cap W(\beta)$ má nejmenší prvek, kt. ozn. δ .

Nutně $\delta \leq \alpha < \beta$.

Dokažeme, že δ je nejmenší i v A .

Kdyby $\exists \gamma \in A$, $\gamma \leq \delta$, pak $\gamma < \beta$ tj. $\gamma \in A \cap W(\beta)$.

Z minimality δ v $A \cap W(\beta)$ plyne $\delta \leq \gamma$. Proto $\delta = \gamma$.

Pozn: Každému ord. číslu přiřadíme mohutnost

$$\alpha = \text{ord } A \mapsto \text{card } A.$$

Zřejmě je toto přiřazení zobrazující (pro A' tak, že $\alpha = \text{ord } A'$ platí zároveň i pro $\text{card } A = \text{card } A'$)

Platí $\text{ord } A \leq \text{ord } B \Rightarrow \text{card } A \leq \text{card } B$

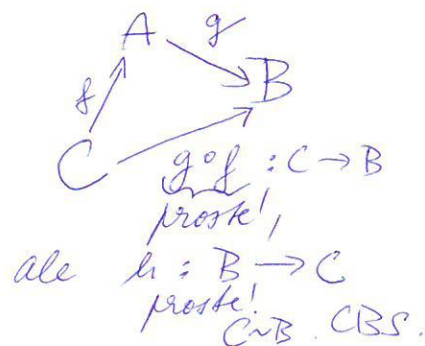
$\text{card } A < \text{card } B \Rightarrow \text{ord } A < \text{ord } B$

Pozn: Může nastat, že $\text{ord } A < \text{ord } B$ a přitom $\text{card } A = \text{card } B$, např. $\text{ord} \{a_0 < a_1 < \dots < b\} = \omega + 1 > \omega$, ale v obou případech stejná cardinalita

Pozn: Pro konečné množ. $\text{ord } A < \text{ord } B \Leftrightarrow \text{card } A < \text{card } B$ a přiřazení $\text{ord } A \mapsto \text{card } A$ je bijekce.

Nastc pou-li $\alpha < \beta < \gamma$ ord. čísla množin A, B, C
 a platí $\text{card} A = \text{card} C$, pak i $\text{card} B = \text{card} A = \text{card} C$.

dl: je totiž $g: A \rightarrow B$ podobnost
 $h: B \rightarrow C$ podobnost
 $f: C \rightarrow A$ bijekce



Důsledek: Ordinalní čísla se stejnou mocností
 tvoří interval (tj. podmnožinu $I \subset M$ takovou, že $\forall \alpha, \beta \in I. \alpha < \beta < \gamma \Rightarrow \beta \in I$).

- Tento interval nemá největší prvek
 (s každým ord. č. β obsahuje i $\beta+1$, které má stejnou mocnost)
- Tento interval má minimální prvek
 (dle řady výše je dobře usp.)
- Tento min. prvek μ je limitní ord. číslo,
 jinak jeho ordinalní typ má poslední prvek ν
 a platí $\nu < \mu$, přitom nek. nic mezi nimi,
 tedy $\mu = \nu+1$, takže mají stejnou mocnost a
 μ není minimální.
- Je-li $(A, \leq)$ taková, že $\text{ord} A = \mu$, pak toto uspořádání
 má vlastnost, že A má mocnost ostře větší než
 každý její úsek.

Def: Nejmenší ordinalní číslo dané mocnosti
 se nazývá kardinalní číslo.

Pozn: Kardinalní čísla jsou tímto dobře uspořádané,
 lze je indexovat ordinalními čísly.

375

Tworem': Každé kard. číslo má dobře definované
následníka, tj. je-li μ kard. číslo, pak $\exists$ kard. č.
 ν tak, že $\mu < \nu$ a mezi nimi není další kard. číslo.
neboli -

dk: Víme, že k $\mu \exists \nu > \mu$. (skrze potenciální množinu)
Vezmeme množinu kard. čísel $X = \{\text{card } M = \gamma \mid \mu < \gamma \leq \nu\}$.
Kard. čísla jsou ord. čísla spec. typu, víme, že
každá množina ord. čísel je dobře uspořádaná, tj.
 X má minimální prvek. To je hledané
kard. číslo.

Cantorova knačim' alef pro transfinite kard. č.

38

$$\aleph_0, \aleph_1, \aleph_2, \dots, \aleph_\omega, \aleph_{\omega+1}, \dots$$

↳ mezi seřitými kard. čísly musí ležet mocnina kontinua, tj. $2^{\aleph_0}$. $\rightarrow$ Hypotéza kontinua $\aleph_1 = 2^{\aleph_0}$.

Hypotéza kontinua

Připomeňme si, že $\text{card}(\mathbb{R}) =: c$ (continuum)

$$\text{card } P(\mathbb{N}_0) = \text{card } 2^{\mathbb{N}_0}.$$

Stačí ukázat, že $\mathbb{R} \sim P(\mathbb{N}_0) \sim 2^{\mathbb{N}_0}$,
 $\uparrow$ uě bylo

dokonce, že $(0,1] \sim P(\mathbb{N}_0) \setminus \{\emptyset\}$.

Ujímme Cantor-Bernstein:

$$f: P(\mathbb{N}_0) \setminus \{\emptyset\} \rightarrow (0,1]: \quad A \rightarrow \sum_{i \in A} 10^{-i} \text{ prostě!}$$

$$g: (0,1] \rightarrow P(\mathbb{N}_0) \setminus \{\emptyset\}: \quad 0.b_1b_2b_3\ldots \rightarrow \{b_i \cdot 10^i \mid i \in \mathbb{N}\}_{\text{maj}} \\ \uparrow \text{nekonečný binární řád.}$$

Povíme si o $\aleph_1$:

Označme $M := \{ \text{ord } A : A \text{ dobře usp. množina, } A \subset \mathbb{N}_0 \}$

Položme $\omega_1 = \text{ord } M$, $\aleph_1 = \text{card } M$.

Théorème: Se knacem'm výše platí:

- 1) M je nespočetná, tj. $\aleph_0 < \aleph_1$.
- 2) $M = W(\omega_1)$
- 3) ω_1 je nejmenší ord. číslo odpovídající mohutnosti $\aleph_1$, tj. je to $\text{card } M$.
- 4) $\aleph_1$ je následovníkem $\aleph_0$ (dle uspořádání kard. čísel).

dle: Ze všech množin (dobře usp.) s ord. číslem ω_1 vyberu reprezentanta $W(\omega_1)$

tj. $\text{ord } M = \omega_1 = \text{ord } W(\omega_1)$.

Pro každé $\alpha \in M$ je $\alpha = \text{ord } W(\alpha)$, kde $W(\alpha)$ je nejvýš spočetná.

Proto $M_\alpha = M \cap W(\alpha)$ je nejvýš spočetná.

Stejně (kvůli podobnosti) $(W(\omega_1))_\alpha = W(\alpha)$ je nejvýš spočetná.

Odtud $\omega_1 = \text{ord } W(\omega_1) \in M \Rightarrow W(\omega_1) \subset M$.

- 1) Kdyby M byla spočetná, pak $\omega_1 \in M$, a proto $M_{\omega_1} = M \cap W(\omega_1) = W(\omega_1)$,
tedy $M \sim W(\omega_1)$, ale i $M_{\omega_1} \sim W(\omega_1)$, takže $W(\omega_1)$ je podobné
svému ^{podob.} úseku. ^{podob.} spor.

- 2) Kdyby $\alpha \notin W(\omega_1)$, tj. $\alpha \geq \omega_1$, pak $\alpha = \text{ord } A$, kde A
je nespočetná dobře usp., tj. $\alpha \notin M$. Odtud $M \subset W(\omega_1)$,
tedy $M = W(\omega_1)$.

- 3) Je-li A dobře usp. $\text{card } A = \aleph_1$, pak je nespočetná,
a tedy $\text{ord } A \notin M$, proto $\text{ord } A \geq \omega_1$.

- 4) Necht A je ~~dobře~~ ^{libv.} množ. Pak, že $\text{card } A < \aleph_1$. Chci $\text{card } A \leq \aleph_0$.
Dle Zermela lze A dobře uspořádat. Označ $\alpha = \text{ord } A$.
Ale $\text{card } A < \aleph_1$ implikuje $\alpha < \omega_1$, tj. $\alpha \in W(\omega_1) = M$. Proto A je nejvýš ^{spec.} spočetná.
 $\text{card } A \leq \aleph_0$

Důsledek: Platí $\aleph_1 \leq 2^{\aleph_0}$.

~~40~~

dl: z Cantorovy věty $\aleph_0 < 2^{\aleph_0}$, přičemž $\aleph_1$ je nejmenší kard. č. větší než $\aleph_0$. CBD.

Hypotéza kontinua říká $\aleph_1 = 2^{\aleph_0}$.

Obecněji $\aleph_{\alpha+1} = 2^{\aleph_\alpha}$

pro každé ordinální číslo α .

Pozn: • $\aleph_\omega$ je první kardinální číslo, o kterém lze ukázat, že $\aleph_\omega > 2^{\aleph_0}$.

• Hypotéza $2^{\aleph_0} = \aleph_m$ je bezesporná $\forall m \in \mathbb{N}$.

Skrmuti' ordinalnu' a kardinalnu' cisla:

Def: Dve dobre usporadane mnoziny maji stejne ord. cislo, jsou-li podobne usporadane.
 $\text{ord } A = \text{ord } B$.

Operace na ord. cislech $\alpha = \text{ord } A, \beta = \text{ord } B$
 $\alpha + \beta := \text{ord}(A + B)$
 $\alpha \cdot \beta := \text{ord}(A \cdot B)$

Asociativni, ale ne komutativni operace.

Relace $\leq$ na ord. cislech: $\alpha = \text{ord } A \leq \beta = \text{ord } B$,
kdyz A je podobna B nebo uisku B .

$\rightarrow$ je reflexivni, tranzitivni, antisymetricka.

Pozn: Antisymetrie vyuziva, ze kazda dobre usporadana mnozina nem' podobna' kazdemu svemu uisku!

Lze dokazat, ze ordinalni cisla kazdych dvou dobre uspor. mnozin jsou porovnatelne.

$\Rightarrow$ máme uplne usporadani na tucle dobre usp. mn.

Ke kazdemu ordinalni cislu volime mnozina:

$$\text{ord } A = \alpha = \text{ord } W(\alpha), \text{ kde } W(\alpha) = \{\text{ord } A_a \mid a \in A\}$$

$\uparrow$ množina všech ordinalních čísel menších než α .

Axiom výběru, Zermelova věta

Zornovo lemma

41

3 ekvivalentní výroky:

AV: Na každé množině M existuje sektor,
tj. zobrazení $f: P(M) \setminus \{\emptyset\} \rightarrow M$ tak, že
 $\forall X \subset M, X \neq \emptyset$ platí $f(X) \in X$.

Věta o dobrém uspořádání (Zermelo):

Každou množinu M lze dobře uspořádat.

Zornovo lemma:

Jestliže v dané neprázdné uspořádané množině M má každý řetězec horní prvek, pak M obsahuje maximální prvek.

Dokážeme (naznačíme):

AV $\Leftrightarrow$ Zermelo

↖ ↗
Zornovo l.

Zermelo $\Rightarrow$ AV :

42

Na M avedeme dobře' uspořádaní.

Z něj pak definujeme selektor takto:

$\forall X \in \mathcal{P}(M), X \neq \emptyset: f(X) :=$ nejmenší' prvek $x \in X$.

AV $\Rightarrow$ Zermelo :

Na M máme selektor, chceme zavést dobře' uspořádaní.

Myšlenka: nejmenší' $\in M$ je $f(M)$,
nejmenší' reční' je $f(M \setminus \{f(M)\})$, atd.

Formálně:

$\mathcal{R}$ označme množinu relací $\subset M \times M$ tak, že:

- $\exists A \in M$, pro které $R \subset A \times A$,
- (A, R) je dobře' uspořádaná
- $\forall x \in A$ platí $f(M \setminus A_x) = x$.

$\uparrow$ úsek $\sim A$ k prvku x
při uspořádaní R .

Nutno ověřit:

-) $\forall R_1, R_2 \in \mathcal{R}$ platí $R_1 \subset R_2$ nebo $R_2 \subset R_1$
-) $\bigcup \mathcal{R} := \bigcup \{ (x, y) \in M \times M \mid \exists R \in \mathcal{R} : (x, y) \in R \} \in \mathcal{R}$
-) $\bigcup \mathcal{R}$ je dobře' uspořádaní na M .

Zermelo $\Rightarrow$ Zorn

43

Dáno uspořádaní $\leq$ na M (ne nutně úplné, natož dobré),

kteří splňuje předpoklady Zornova l.,
tj. každý řetězec $\tau (M, \leq)$ má horní hranici.

Pomocí dobrého uspořádaní $\leq$ na M
najdeme prvek $\alpha \in M$, který je maximální při $\leq$.

Definujeme $A \subset M$ takto:

$$A = \{ x \in M \mid \forall y \in M : y \in M, y \prec x \Rightarrow y \leq x \}.$$

$\Leftarrow$ transfinite rekursí, tj. podle dobrého
uspořádaní na M procházíme prvky $x \in M$
a u každého rozhodneme, jestli zařadit do A .

Platí: $\bullet$ A existuje a je jednoznačně def.

$\bullet$ A je řetězec τM .

$\neq$ předpokladu Zorna má řetězec A
horní hranici τM , tj. prvek $a \in M$ takový,
že $\forall x \in A$ platí $a \geq x$.

Prvek a je maximální τM ,

sporem: $\exists b \in M$ tak, že $b > a$.

Nutně $b \in A$ z definice A , protože
při konstrukci A jsme na b narazili
a museli bychom ho do A zařadit.

Zornovo lemma $\Rightarrow$ AV

44

Na M avedeme množinu $\mathcal{G}$ částicových selektorů, na ni uspořádání, ověříme předpoklady Zorna. Maximální prvek $\alpha \mathcal{G}$ bude selektor na M .

$\mathcal{G}$ = množina zobrazení $g: \mathcal{F} \rightarrow M$,
kde $\mathcal{F} \subset \mathcal{P}(M) \setminus \{\emptyset\}$ a $g(X) \in X$ pro $x \in \mathcal{F}$.

Uspořádání $\sqsubseteq$ na $\mathcal{G}$:

$g_1 \sqsubseteq g_2$, pokud g_2 je rozšířením g_1 ,

tj. $\mathcal{F}_2 \supset \mathcal{F}_1$ a $g_2|_{\mathcal{F}_1} = g_1$.

Uvažujeme řetězec $\tilde{\mathcal{G}} \subset \mathcal{G}$.

Horní krajní řetězec $\tilde{\mathcal{G}}$ bude zobrazení h :

$h: \bigcup \{\text{Dom } g \mid g \in \tilde{\mathcal{G}}\} \rightarrow M$

$h(x) = g(x)$ pro libovolné g tak, že $x \in \text{Dom } g$.

Pak nutně $h(x) \in X$, tj. $h \in \mathcal{G}$.

Zornovo lemma implikuje existenci

maximálního prvku $\alpha \mathcal{G}$, označme ho f :

$f: \mathcal{F}_{\max} \rightarrow M$. Ověříme, že to je selektor na M .

Stačí ukázat, že $\mathcal{F}_{\max} = \mathcal{P}(M) \setminus \{\emptyset\}$.

Sporem: Kdyby $\exists X \in \mathcal{P}(M) \setminus \{\emptyset\}, X \notin \mathcal{F}_{\max}$,

pak rozšíříme f na $\mathcal{F}_{\max} \cup \{X\}$

dodefinováním $f(x) = a \in X$

vybrat a jedinou
množinu

To je spor s maximalitou f .

Použítí Zornova lemmatu:

Věta: V každém vektorovém prostoru existuje báze.

dk: V prostoru V označme

$$M = \{ A \subset V \mid A \text{ je lin. nezávislá množina} \}$$

Pokud B je maximální prvek v M (vůči inkluzi),
pak B je báze V (A: LN množina, její lin. obal je V).

↳ stačí ukázat, že $[B]_{\text{lin}} = V$. Kdyby ne,

pak $\exists v \in V \setminus [B]_{\text{lin}}$. Proto $C := B \cup \{v\}$ je LN

A: $C \in M$, přičemž $B \subset C$, takže spor s maximalitou prvku B .

Maximální prvek B najdeme ze Zornova lemmatu.

Ověříme předpoklad Zorna:

Vezmeme řetězec $F \subset M$ a najdeme horní závoru.

Tedy, že $UF := \bigcup_{X \in F} X$ je horní závorou F v M .

Stačí ukázat, že UF je LN.

sporem: Kdyby LZ, pak existuje konečná množina $v_1, v_2, \dots, v_n \in UF$, která je LZ.

Nutně $\forall i \exists X_i \in F$ tak, že $v_i \in X_i$.

Ale F je řetězec, tedy $\exists j$ tak, že

$v_i \in X_j \quad \forall i \in \{1, \dots, n\}$.

To by ale znamenalo, že X_j není LN,

což je spor s $X_j \in F \subset M$.

Proto existuje B maximální v M a to je báze prostoru V .

Pologrupy

1

Def: Necht $n \in \mathbb{N}_0$. Řekneme, že ω je n -ární operace na množině $M \neq \emptyset$, když ω je $(n+1)$ -ární relace na M taková, že

$$\forall x_1, \dots, x_n, y, z \in M \text{ platí}$$
$$(x_1, \dots, x_n, y) \in \omega \wedge (x_1, \dots, x_n, z) \in \omega \Rightarrow y = z$$

Pozn: ω je zobrazení $\omega: M^n \rightarrow M$

znááme $y = \omega(x_1, \dots, x_n)$.

Operace nulární $n=0$... výběr vy'znač. prvku
unární $n=1$... přičtení $1-?$
binární $n=2$

Def: Univerzální algebra je dvojice (M, Ω) , kde
 M je neprázdná (nosič algebry)
 Ω je neprázdná množina operací na M

Pozn: Často ztotožňujeme (M, Ω) a M , je-li jasné,
o jaké operace se jedná.

Def: Grupoid je univ. algebra s jedinou binární operací.

Def: Pologrupa je grupoid, ve kterém platí asoc. zákon.

Ekv. Pologrupa je uspořádaná dvojice $(M, *)$

$M \neq \emptyset$, $*$ je binární operace taková, že

$$\forall a, b, c \in M: (a * b) * c = a * (b * c)$$

Pologrupa je komutativní, pokud navíc

$$\forall a, b \in M \quad a * b = b * a$$

Pr: $(\mathbb{Z}, -)$ není ani asociativní, ani komutativní
 $(\mathbb{Q}, \oplus) \oplus: a \oplus b = \frac{a+b}{2}$ je komutativní,
 ale ne asociativní. 2

Def: Značení pro uspořádaný součin prvků pologrupy $(M, *)$:

Pro $a_1, \dots, a_n \in M$ $\prod_{j=1}^n a_j$ je prok:

$$\prod_{j=1}^1 a_j := a_1, \quad \prod_{j=1}^{n+1} a_j := \left(\prod_{j=1}^n a_j \right) * a_{n+1} \quad \text{pro } n \geq 1.$$

Např: $\prod_{j=1}^4 a_j = ((a_1 * a_2) * a_3) * a_4.$

Věta: V pologrupě $(M, *)$ pro libovolná $n, a_1, \dots, a_n \in M$
 výraz $a_1 * a_2 * \dots * a_n$ nezávisí na rozmístění závorek.

Lemma: Necht $(M, *)$ je pologrupa, $m, n \in \mathbb{N}$, $a_1, \dots, a_{n+m} \in M$.

Pak $\prod_{j=1}^m a_j * \prod_{j=1}^n a_{m+j} = \prod_{j=1}^{m+n} a_j.$

dk: indukcí na m při pevném n

$m=1$ definice

$$\begin{aligned} m \rightarrow m+1 \quad & \prod_{j=1}^m a_j * \prod_{j=1}^{n+1} a_{m+j} \stackrel{\text{def}}{=} \prod_{j=1}^m a_j * \left(\prod_{j=1}^n a_{m+j} * a_{m+n+1} \right) \stackrel{\text{asoc.}}{=} \\ & \left(\prod_{j=1}^m a_j * \prod_{j=1}^n a_{m+j} \right) * a_{m+n+1} \stackrel{\text{IP}}{=} \prod_{j=1}^{m+n} a_j * a_{m+n+1} \stackrel{\text{def}}{=} \prod_{j=1}^{m+n+1} a_j \end{aligned}$$

dk věty:

Pro $n=1, n=2, n=3$ ^{triv.} ^{asoc. zákon.} triv.

Pak indukce na n . Necht' platí pro výrazy kratší než n .

Při vyčíslení výrazu $a_1 * a_2 * \dots * a_n$ se jakkoliv
rozmístěními závorekami dostaneme nakonec

$u * v$, kde $u, v \in M$ jsou nějak osazované

$u = a_1 * \dots * a_r, v = a_{r+1} * \dots * a_n$. Z IP nezávisí
na tom, jak vyčísleno, proto $u = \prod_{j=1}^r a_j, v = \prod_{j=1}^{n-r} a_{j+r}$.

Z Lemmatu plyne tvrzení věty.

Pozor ke značením:

multiplicativní zápis $*$ = $\cdot$, často $\cdot$ vynecháváme.

$$\forall n \in \mathbb{N}: a^n := \prod_{j=1}^n a$$

aditivní zápis $*$ = $+$

$\forall n \in \mathbb{N}$ platí $1 \times a = a, (n+1) \times a = n \times a + a$.

Pozn: z věty pak plyne $\forall m, n: a^m \cdot a^n = a^{m+n}$
 $(a^m)^n = a^{n \cdot m}$.

Def: Monoid je pologrupa s neutrálním prvkem,
tj. $(M, *, e)$, kde $*$ je binární a e nulární operace na M
splňující 1) $*$ je asociativní
2) $\forall x \in M$ je $e * x = x * e = x$.

Pozn: U multipl.-zápisu často $e=1$, u aditivního $e=0$
jedinkový prvek nulový prvek.

Uvědomění: V každém monoidu existuje právě jeden neutrální prvek.

4

dl: Je-li e, f neutrální, pak $f = f * e = e$.

Pozn: V monoidu každému $a^0 := e$, resp. $0 \cdot a = 0$
 $\in \hat{N}$ $\in \hat{M}$

Pr: $(N, \cdot, 1), (N_0, +, 0), (\{1\}, \cdot, 1), (\{0\}, +, 0)$

V jistém smyslu stejné.

Def: Homomorfismus pologrup $(M, *)$, $(\tilde{M}, \tilde{*})$ je zobrazení $f: M \rightarrow \tilde{M}$, které splňuje

$$\forall x, y \in M: f(x * y) = f(x) \tilde{*} f(y).$$

Homomorfismus monoidů $(M, *, e)$, $(\tilde{M}, \tilde{*}, \tilde{e})$ je homomorfismus pologrup $(M, *)$, $(\tilde{M}, \tilde{*})$, pro který navíc $f(e) = \tilde{e}$.

Pozn! Ne každý homomorfismus pologrup splňuje $f(e) = \tilde{e}$.

Např: $D = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\}$ operací násobení matic
 Δ a $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ jako neut. pr.
je monoid.

Zobrazení $f: \{1\} \rightarrow D: f(1) = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$

je homomorfismus pologrup, ale ne monoidů.

Def: Monomorfismus - prostý | Endomorfismus je $A \rightarrow A$
epimorfismus - na | automorfismus je $A \rightarrow A$ bijekce.
izomorfismus - bijekce

Pr: Monoid konečných slov nad abecedou A .

Abeceda $A = \{a_1, \dots, a_n\}$ navržením různých symbolů.

$$A^* = \bigcup_{k=0}^{\infty} A^k, \quad \text{kde } A^k \text{ je } k\text{-násobný kart. součin}$$

$$A^0 = \{\emptyset\}$$

Operace $\circ$: Pro $k, l \in \mathbb{N}_0$ píšeme $\circ: A^k \times A^l \rightarrow A^*$

$$(x_1, \dots, x_k) \circ (y_1, \dots, y_l) = (x_1, \dots, x_k, y_1, \dots, y_l) \in A^{k+l} \subset A^*$$

Přepisujeme $\emptyset = \varepsilon$... prázdné slovo

$$(x_1, \dots, x_k) = x_1 x_2 \dots x_k \text{ slovo délky } k.$$

Operace $\circ$ je křátkové slovo.

Pr: Monoid $\{0,1\}^*$ je izomorfní monoidu

$$\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{N}_0, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = 1 \right\}$$

Δ maticovým násobením a $e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

HINT: Každou matici lze rozložit na součin matic $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ a $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$.

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & a+b \\ c & c+d \end{pmatrix} \quad \left(\begin{array}{l} \text{Pr:} \\ \text{ku sh. 4,5} \end{array} \right)$$

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a+b & b \\ c+d & d \end{pmatrix}$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ c & d \end{pmatrix}$$

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ a+c & b+d \end{pmatrix}$$

Každá matice ..., u které je jeden
x řádků $\geq$ druhý nebo jeden
x sloupců $\geq$ druhý lze rozložit.

Jak vypadá matice, u které to nejde?

1) $a > b$ pak $c < d$.

$$1 = ad - bc > b(d - c)$$

tg: nutně $b = 0$, odtud $ad = 1$, tg:
 $a = d = 1$ a pak $c = 0$

2) $a < b$ pak $c > d$.

$$1 = ad - bc < b(\underbrace{d - c}_{< 0}) \leq 0 \text{ nejde.}$$

$$\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} = \begin{pmatrix} 3 & 1 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \underbrace{\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}}_b \underbrace{\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}}_a =$$

$$= \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 3 & 4 \\ 2 & 3 \end{pmatrix} \longleftrightarrow a b b a$$

5

Def: Element a v pologrupě $(M, *)$

je nazývá absorbující, pokud

$\forall b \in M$ platí $ab = ba = a$.

Pologrupa s absorbujícím prvkem se nazývá muloid.

Lemma: V muloidu existuje právě jeden absorb. prvek.

dk: Je-li a, b absorbující, pak $a \cdot b = b \cdot a = b$.

Pr: V monoidu $(M, \cdot, 1)$ je 0 absorbující element.

Lemma: Každou pologrupu lze rozšířit na monoid,
každou pologrupu lze rozšířit na muloid.

dk: Snadno. Je-li $(M, *)$ pologrupa, a
má-li neutrální prvek, pak je to monoid.
Ještěže nemá neutrální prvek, pak
zvolíme e symbol tak, $e \notin M$.

Na množině $M \cup \{e\}$ dodefinujeme $e * x = x * e = x$
pro všechna $x \in M$ a také $e * e = e$.

Pak $(M \cup \{e\}, *, e)$ je monoid. (vědomit si asociat.)

Obdobně: Má-li $(M, *)$ absorbující element, pak
je to muloid. Nemá-li, pak zvolím $a \notin M$
a na $M \cup \{a\}$ dodefinujeme $x * a = a * x = a \quad \forall x \in M$
a také $a * a = a$. Pak $(M \cup \{a\}, *, a)$ je muloid.

Pr: $(\mathbb{N}_0, \cdot, 0)$ je „muloidní uzavřen“ monoidu $(\mathbb{N}, \cdot, 1)$.

Pr: $(\{3, 4, 5, \dots\}, +)$ je pologrupa, $(\{0, 3, 4, 5, \dots\}, +, 0)$ je monoid.

Df: Prvek x v monoidu M se nazývá invertibilní (nebo někdy jednotka!), pokud existuje $y \in M$ tak, že $xy = yx = e$.
 Takové y se nazývá inverzí k x , značíme x^{-1} (v multiplik. verzi).

Pozn: Ke každému $x \in M$ existuje nejvýše jeden inverzní prvek. Kdyby y, y' byly inverzí, pak
 $y' = y' \cdot e = y'(xy) = (y'x)y = ey = y$.

Monoid, ve kterém jsou všechny prvky invertibilní se nazývá grupa.

Př: $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$, operace násobení mod 6, $e = 1, a = 0$.

Invertibilní: 1, protože $1^{-1} = 1$
 5, protože $5^{-1} = 5$

Ostatní invertibilní nejsou: $xy = 1 \pmod{6}$ pro $x, y \in \mathbb{Z}$
 implikuje $x \wedge y \perp 6$.

Př: $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, operace nás. mod 5, $e = 1, a = 0$

Invertibilní 1, protože $1^{-1} = 1$

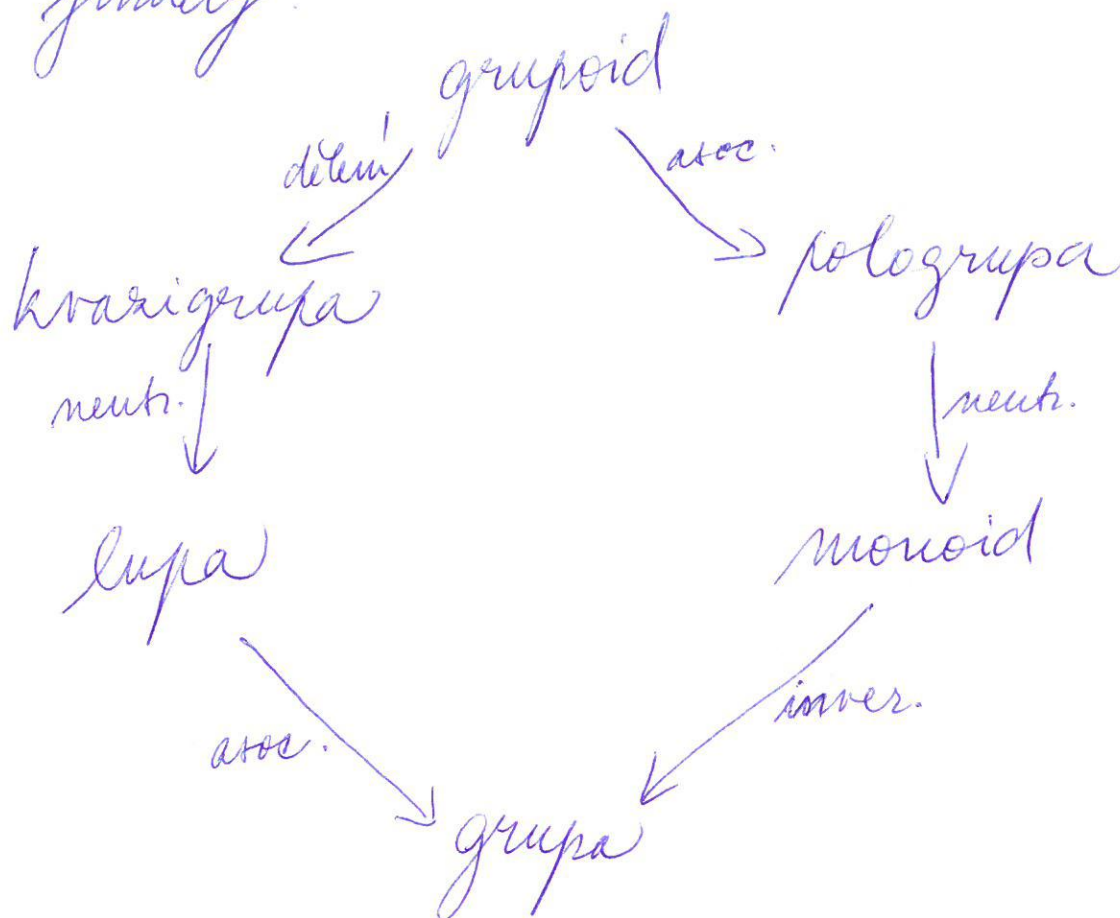
$$2^{-1} = 3$$

$$3^{-1} = 2$$

$$4^{-1} = 4$$

$\rightarrow (\mathbb{Z}_5, \cdot \pmod{5})$ grupa.

Pozn: Od grupoidu ke grupě se lze dostat jinudy: 7



Def: Kvarigrupa je grupoid $(M, *)$, kde operace $*$ splňuje: $\forall a, b \in M \exists x, y \in M$ tak, že

$$a * x = b$$

$$y * a = b$$

Právě x, y jsou dány jednoznačně, tj:

$$a * x = a * \tilde{x} \Rightarrow x = \tilde{x} \quad \text{levé krátění}$$

$$y * a = \tilde{y} * a \Rightarrow y = \tilde{y} \quad \text{právé krátění}$$

Značení: $\rightarrow x = a \backslash b$ levé dělení
 $\rightarrow y = b / a$ pravé dělení

Pr: $(\mathbb{Z}, -), (\mathbb{Q} \setminus \{0\}, \div)$

Def: Kvarigrupa $(M, *)$ s neutr. prvkem $e * x = x * e = x \quad \forall x \in M$ je lupa.

Cayleova tabulka operace $\ast$:

7,5

Př: $M = \{a, b, c\}$

	a	b	c
a	$a \ast a$	$a \ast b$	$a \ast c$
b	$b \ast a$	$b \ast b$	$b \ast c$
c	$c \ast a$	$c \ast b$	$c \ast c$

Podmínka dělení u kvazigrup zaručuje, že tabulka je latinský čtverec, tj. v každém řádku i sloupci je každý prvek právě jednou.

Př: Nejmenší lupa, která není grupou, je řádu 5. Takových neizomorfních je 5. Např.:

	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

Je vidět :- je to kvazigrupa (díky tabulce latinský $\square$)

- má neut. prvek e

- není asoc.

$$(ab)d = cd = a$$

$$a(bd) = ac = d$$

Navíc má spec. vlastnost

$$\forall x \in M \text{ je } x^2 = e \text{ involutivní prvek}$$

Twissen! V každé kvazigrupě platí kritérium.

V každé konечné grupoidu s kritériem je dělení, tj. je to kvazigrupa.

dlk: První tvrzení OK a def.

7,65

Druhé tvrzení: musím dokažat, že $*$ splňuje

$\forall a, b \in M \exists x, y \in M$ jednorázově tak, že

$$a * x = b$$

$$y * a = b.$$

1) jednorázovost: x kladem, viz důkaz

2) existence: V Cayleyově tabulce je díky kladem
 x každému řádku každý prvek
(i sloupce)

nejing'se jednou. Je-li konečné,
musíme pokrýt celý řádek, tj:

je tam právě jednou.

To znamená, že M je koasigrupa. ^{pro konečné}

↳ lze přes ukázat, že násobení zleva prohrom a je injekce a surjekce

Pozn: Druhé tvrzení neplatí bez konečnosti.

Napr. $(\mathbb{N}, +)$ je grupoid s kladem (stačí jednoráz. díky komut.)

$\forall m, n, k$ platí $m+k = n+k \Rightarrow m=n$
(viz Peano)

ale nemám dělení:

$a+x = b$ nemá nutně řešení $\forall a, b \in \mathbb{N}$

Grupy

18

Def: Grupa je čtveřice $(G, *, \iota, e)$, kde
 G je neprázdná množina
 $*$ je binární operace na G
 ι je unární operace na G
 e je nulární operace na G ,
které splňují

- 1) $\forall x, y, z \in G: x * (y * z) = (x * y) * z$ asociativ.
- 2) $\forall x \in G: x * e = e * x = x$ neutrl. prvek
- 3) $\forall x \in G: x * \iota(x) = \iota(x) * x = e$ inverzní prvek

Pokud navíc

4) $\forall x, y \in G: x * y = y * x$ komutat. zákon
říkáme, že grupa je komutativní
(abelova, abelovská).

Pozn: Grupa je monoid, ve kterém má každý prvek inverzi.

Pozn: V multiplikačním kápisu: $e=1, \iota(x)=x^{-1}$
V aditivním kápisu: $e=0, \iota(x)=-x$.

Pozn: Jsou-li operace zřejmé z kontextu, říkáme, že máme grupu G .

Věta: Necht' G je grupa. Potom $\forall a, b, c \in G$
platí: $ac = bc \vee ca = cb \Rightarrow a = b$.
Sro. krácejí.

dk: Když $ac = bc$, dostaneme

$$a = acc^{-1} = bcc^{-1} = b.$$

Když $ca = cb$, máme

$$a = c^{-1}ca = c^{-1}cb = b.$$

Důsledek: Rovnice $ax = b$ pro dané $a, b \in G$
má právě jedno řešení $x = a^{-1}b \in G$.

Rovnice $xa = b$ pro $a, b \in G$ má
právě jedno řešení $x = ba^{-1} \in G$.

dk: Prvek $a^{-1}b$ je řešením (dosazením).

Naopak je-li x řešením, pak

$$ax = b = aa^{-1}b \Rightarrow x = a^{-1}b.$$

Obdobně druhá strana.

Důsledek:

10

- 1) $\forall a, u \in G$ platí $au = a \vee ua = a \Rightarrow u = e$
- 2) $\forall a, u \in G$ platí $au = e \vee ua = e \Rightarrow u = a^{-1}$
- 3) $\forall a \in G$ platí $(a^{-1})^{-1} = a$
- 4) $\forall a, b \in G$ platí $(ab)^{-1} = b^{-1}a^{-1}$.

Pozn: 1) $\Rightarrow$ jednoznačnost neut. prvku
2) $\Rightarrow$ jednoznačnost inverze
3, 4) platí v grupě

dl: 1) $au = a$ krátíme $u = e$

2) $au = e = aa^{-1}$ krátíme $u = a^{-1}$

3) $(a^{-1})^{-1}a^{-1} = e = aa^{-1}$ krátíme sprava $(a^{-1})^{-1} = a$

4) $(ab)^{-1}ab = e = b^{-1}b = b^{-1}a^{-1}ab$ krátíme sprava $(ab)^{-1} = b^{-1}a^{-1}$

Pozn: Z důsledků odvoztíme následující:

kromě a^n pro $n \in \mathbb{Z}, n > 0$
máme $a^0 = e$ a $a^n = (a^{-1})^{-n}$ pro $n < 0$ } $\sim$ multiplik. uzavřenost

Stejně jako v každém grupoidu $a^p a^q = a^{p+q}, (a^p)^q = a^{pq}$.

Tam to platilo pro všechna $p, q \in \mathbb{N}$. Lze obecně pro $p, q \in \mathbb{Z}$:
 $\hookrightarrow$ uvidíme

Př: Triviální grupa $(\{1\}, \cdot, ^{-1}, 1)$ stejně jako $(\{0\}, +, -, 0)$
Grupa celých čísel $(\mathbb{Z}, +, ^{-1}, 0)$ abelská.

Def: jsou-li $(G, *, e)$, $(\tilde{G}, \tilde{*}, \tilde{e})$ grupy, 11
pak zobrazení $f: G \rightarrow \tilde{G}$ je homomorfismem
grup, jestliže $\forall a, b \in G \quad f(a * b) = f(a) \tilde{*} f(b)$.

Platí: 1) $f(e) = \tilde{e}$

2) $\forall a \in G \quad f(\iota(a)) = \tilde{\iota}(f(a))$

dk: 1) $f(e) = f(e * e) = f(e) \tilde{*} f(e)$, z čísel' $f(e) = \tilde{e}$.

2) $f(a) \tilde{*} f(\iota(a)) = f(a * \iota(a)) = f(e) = \tilde{e}$, opět z čísel' $f(\iota(a)) = \tilde{\iota}(f(a))$.

Pozn: Ne každý homomorfismus pologrup byl homo-
morfismem monooidů, ale struktura grupy (čísel')
už zaručuje, že stačí homomorf. $(G, *) \rightarrow (\tilde{G}, \tilde{*})$,
aby byl i grupový.

Def: Opět pojmy, monomorf, epimorf, izomorf, endomorf,
automorf.

Platí: Zobrazení $f: \mathbb{Z} \rightarrow G$, kde G je grupa
dane' $f(m) = a^m$ pro zvolený $a \in G$
je homomorfismus, tj. $\forall m, n \quad a^{m+n} = a^m \cdot a^n$
a navíc platí $\forall m, n \quad (a^m)^n = a^{m \cdot n}$.

Známe! jsou-li grupy $G, \tilde{G}$ izomorfní, značíme $G \cong \tilde{G}$.

Další příklady grup:

12

- 1) Triviální grupa $(\{1\}, \cdot, ^{-1}, 1) \simeq (\{0\}, +, -, 0)$
- 2) $(\mathbb{Z}, +, -, 0)$
- 3) $(\mathbb{Z}_n, + \bmod n, - \bmod n, 0)$:

Def: Na $\mathbb{Z}$ definujeme relaci $a \equiv b \bmod n, a, b \in \mathbb{Z}$.
Pro dané $n \in \mathbb{N}$ „ a je kongruentní b modulo n “,
jestliže $n \mid a - b$, tj. a, b mají stejné zbytky
po dělení n .

Poru: $\cdot \equiv \bmod n$ je ekvivalence na $\mathbb{Z}$

$$\left. \begin{array}{l} a \equiv b \bmod n \\ c \equiv d \bmod n \end{array} \right\} \Rightarrow \begin{array}{l} a + c \equiv b + d \bmod n \\ a \cdot c \equiv b \cdot d \bmod n \end{array}$$

$$\text{speciálně } a^k \equiv b^k \bmod n$$

$$ka \equiv k \cdot b \bmod n$$

Platí: $\mathbb{Z}_n = \{0, 1, \dots, n-1\}$ s operací $+ \bmod n$,

neutrálním prvkem 0,

opacným k a ve tvaru $n-a$

je abelská grupa.

Vlastně třídy ekvivalence $\equiv \bmod n$ na $\mathbb{Z}$.

$\rightarrow$ Je-li $a \in \mathbb{Z}_n$, pak $n-a \in \mathbb{Z}_n$ a platí $a + (n-a) = n \equiv 0 \bmod n$

$$4) M = \left\{ \underbrace{\cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}}_{a_k = e^{\frac{2\pi i}{n}k}} \mid k=1, \dots, n \right\}$$

12,25

$C_n = (M, \cdot, ^{-1}, 1=a_n)$ grupa n -tých odmocnin $\times 1$
s operacemi jako v $\mathbb{C}$.

Plati' $a_k \cdot a_l = a_{k+l}$ pro $k+l \leq n$

$a_k \cdot a_l = a_{k+l-n}$ pro $k+l > n$

$$a_k \cdot a_{n-k} = a_n = e^{\frac{2\pi i}{n}n} = 1 \quad \text{tj.} \quad a_k^{-1} = a_{n-k}$$

$$e^{-\frac{2\pi i}{n}k} = e^{\frac{2\pi i}{n}(n-k)}$$

$$\varphi: \mathbb{Z}_n \rightarrow C_n : \varphi(k) = a_k = e^{\frac{2\pi i}{n}k}$$

je izomorfismus grup.

5) Je $\mathbb{Z}_n$ grupa vzhledem k $\cdot \bmod n$?

$(\mathbb{Z}_n, \cdot \bmod n, 1)$ je monoid

Alé! 0 nemá inverzi.

Je $\mathbb{Z}_n^* = \{1, \dots, n-1\}$ grupa vzhledem k $\cdot \bmod n$?

Je-li n složené číslo, pak každé $k \in \mathbb{Z}_n^*$
soudělné s n nemá inverzi.

$$\text{důk.} \quad a \cdot k \equiv 1 \bmod n \Rightarrow ak = 1 + ln, \text{ ale } \gcd(k, n) > 1. \quad \text{spor.}$$

Plati': $\mathbb{Z}_p^* = \{1, \dots, p-1\}$ s operací $\cdot \bmod n$ je grupa:
neutrálním prvkem je 1
inverze ke každému $k \in \mathbb{Z}_p^*$ existuje.

Některé to znají z DMT.

Lemma: Pro $a, b \in \mathbb{Z}$ neobě nuly existují $\text{nsd}(a, b)$.

Navíc existují $x, y \in \mathbb{Z}$ tak, že $ax + by = \text{nsd}(a, b)$.

dk: Vůně $a^2 + b^2 \neq 0$. Ozn. $M = \{ax + by \mid x, y \in \mathbb{Z}\}$

Dokažeme, že $d = \min \{|k| \mid k \in M \setminus \{0\}\}$ je $\text{nsd}(a, b)$.

Zřejmě $d \in M \setminus \{0\}$.

Ukážeme $d \mid a$, jinak $a = kd + r$, $r \neq 0$.

Ale $r \in M$, $r < d$, takže spor.

Stejně $d \mid b$.

Jestliže $d' \mid a$ a také $d' \mid b$, pak d' dělí každý prvek v M , takže také $d' \mid d$.

To je přesně def. $\text{nsd}(a, b)$: Takové $d \in \mathbb{N}$, že

• $d \mid a$, $d \mid b$

• $\forall d'$ tak, že $d' \mid a$, $d' \mid b$ platí $d' \mid d$.

Pozn. $\text{nsd}(a, b)$ je def. $\rightarrow$ užijeme až na znaménko:

Je-li d_1, d_2 nsd, pak $d_1 \mid d_2$ a $d_2 \mid d_1 \Rightarrow d_1 = kd_2 = jkd_1$

Proto $jk = \pm 1 \Rightarrow j = k = \pm 1$.

Často $\text{nsd} \in \mathbb{N}$.

Pozn. Pro $\text{nsd}(a, b) = 1$ píšeme $a \perp b$.

Důsledek lemma: Necht $n \in \mathbb{N}$, $a \in \mathbb{Z}$, $a \perp n$.

Potom existuje $x \in \mathbb{Z}$ řešení $ax \equiv 1 \pmod{n}$.

dk: $ax - ny = 1$ má řeš. z lemma, protože $\text{nsd}(a, n) = 1$.

Příklad č. 5)

12,75

$(\mathbb{Z}_p^*, \cdot \bmod p, ^{-1} \bmod p, 1)$ je grupa.

že každému $a \in \mathbb{Z}_p^*$ existuje inverze $a \cdot \bar{a} \equiv 1 \bmod p$
protože $a \perp p$.

6) Vektorový prostor $(V, +, -, \vec{0})$ je abelovská grupa.

6,5) Je-li T těleso, pak

$(T, +, -, 0)$ je abelovská grupa

$(T^*, \cdot, ^{-1}, 1)$ je grupa, kde $T^* = T \setminus \{0\}$.

Pozn. • 0 tělesech bude pořadí více.

• V lin. algebře s řáděto

těleso s komutativním násobením,

g: $(T^*, \cdot, ^{-1}, 1)$ abelovská.

7) Symetrická grupa:

13

Pro $X \neq \emptyset$ Zavedeme $S_X := \{f \in X^X \mid f \text{ bijekce}\}$.

operace skládání $\circ$, inverzní zob., 1_X .

Pro $|X| = n \in \mathbb{N}$ píšeme S_n , zobrazení f je permutace.

standardně volíme $X = \{1, 2, \dots, n\}$.

Súde' permutace A_n ... tzv. alternující grupa.

6) Dihedralní grupa:

D_{2n} obsahuje všechny izometrie pravidelného n -úhelníka na sebe (tzv. symetrické transformace).

n rotací kolem středu

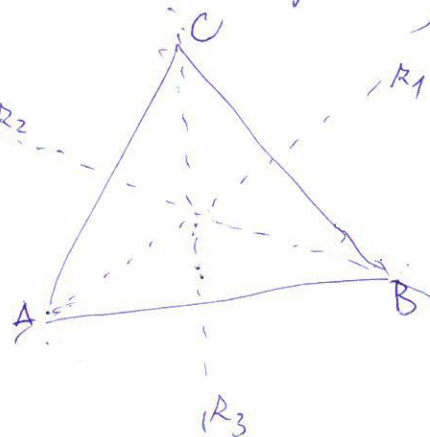
n zrcadlení podle os symetrie

$$|D_{2n}| = 2n$$

rot. = r_1, r_2, r_3 rotace

$$\hookrightarrow \text{úhel } 0 \rightarrow \frac{2\pi}{3}, \frac{4\pi}{3}$$

zrcadlení r_1, r_2, r_3



Pozn. $D_6 \simeq S_3$ izomorfismus je dán zobrazením permutací vrcholů

např. $(A, C, B) \rightarrow r_1$

$(B, C, A) \rightarrow r_3$

$(B, A, C) \rightarrow r_3$

$(C, A, B) \rightarrow r_2$

$(C, B, A) \rightarrow r_2$

$(A, B, C) \rightarrow r_1$

Maticové grupy: Pro těleso T :

14

• Obecná lineární grupa:

$$GL(n, T) := (\{A \in T^{n \times n} \mid \det A \neq 0\}, \cdot, {}^{-1}, I)$$

• Speciální lineární gr.

$$SL(n, T) := (\{A \in T^{n \times n} \mid \det A = 1\}, \cdot, {}^{-1}, I)$$

• Orthogonální grupa

$$O(n, T) := (\{A \in T^{n \times n} \mid AA^T = I\}, \cdot, {}^{-1}, I)$$

• Unitární grupa pro $T = \mathbb{C}$

$$U(n) := (\{A \in \mathbb{C}^{n \times n} \mid AA^* = I\}, \cdot, {}^{-1}, I)$$

kde A^* je hermitovský sdružený k A .

Pozn: $SL(n, T)$ a $O(n, T)$ jsou „podgrupy“ $GL(n, T)$
 $U(1)$ je izomorfní s grupou komplexních jednotek.

Podgrupy

15

Def: Podgrupa grupy G je taková podmnožina, která je uzavřená vůči všem operacím v G .

Spec: Necht' $(G, *, \iota, e)$ je grupa, $H \subset G$.

H je podgrupa grupy G , když $(H, *, \iota, e)$ s operacemi zůstává na H je sama grupa.

- Aj:
- (1) $e \in H$
 - (2) $\forall a \in H, \iota(a) \in H$
 - (3) $\forall a, b \in H, a * b \in H$

Pozn: Nem' nutno ověřovat vše. Pro $H \neq \emptyset$ je (1) důst. (2) a (3), protože $a \in H$ dle (2) má $\iota(a) \in H$ a dle (3) $a * \iota(a) = e \in H$.

Věta: Je-li G grupa a $\emptyset \neq H \subset G$. Jestliže pro všechna $a, b \in H$ platí $ab^{-1} \in H$, pak H je podgrupou grupy G .

dle: Ověříme (1), (2), (3).

$\exists H \neq \emptyset$ existuje $a \in H$. Pak $a^{-1}a = e \in H$.

Pro libovolné $b \in H$ je $b^{-1} = b^{-1}e \in H$.

Pro $a, b \in H$ je $a^{-1} \in H$, aj: $(a^{-1})^{-1}b = ab \in H$.

Př: Každá grupa má dvě triv. nevlastní podgrupy, a to triviální podgrupu $\{e\}$ a sebe sama.

Def: Necht' G, H jsou grupy a $f: G \rightarrow H$ jech homomorfismus. Značíme $\text{Ker} f := f^{-1}(\{e_H\})$, $\text{Im} f := f(G)$.
 $\text{Ker} f$ je jádro homomorfismu, $\text{Im} f$ je obraz homomorfismu.

Věta: Necht $f: G \rightarrow H$ je homomorfismus grup G, H .

Potom $\text{Ker} f \subset G$, $\text{Im} f \subset H$ jsou podgrupy.

Navic $\text{Ker} f = \{e_G\}$, ^{právě} když f je monomorfismus.

dlk: $\text{Ker} f$ podgrupa? $\text{Ker} f \neq \emptyset$, protože $e_G \in \text{Ker} f$.

$$a, b \in \text{Ker} f \Rightarrow f(a) = f(b) = e_H$$

$$f(a^{-1}b) = (f(a))^{-1}f(b) = e_H^{-1}e_H = e_H \Rightarrow a^{-1}b \in \text{Ker} f \quad \checkmark$$

• $\text{Im} f$ podgrupa? $\text{Im} f \neq \emptyset$, protože $e_H \in \text{Im} f$.

$$a, b \in \text{Im} f \Rightarrow \exists u, v \in G \text{ tak, že } a = f(u), b = f(v).$$

$$a^{-1}b = (f(u))^{-1}f(v) = f(u^{-1}v), \text{ tj. } a^{-1}b \in \text{Im} f \quad \checkmark$$

• $\text{Ker} f = \{e_G\}$, ověřme, že f prostý.

dlk: Když pro $a, b \in G$ platilo

$$f(a) = f(b), \text{ pak } (f(a))^{-1}f(b) = e_H$$

$$\text{tj. } f(a^{-1}b) = e_H.$$

Ale máme, že $\text{Ker} f = \{e_G\}$, proto $a^{-1}b = e_G$, tj. $a = b$.

• Naopak: f prostý, ověřme, že $\text{Ker} f = \{e_G\}$.

$$\text{Když } a \neq e \text{ platilo do } \text{Ker} f, \text{ pak } f(a) = f(e_G) = e_H.$$

Ale f prostý, tj. $f(a) \neq f(e_G)$. Spor.

Vštnu zobecníme nasledovne:

17

Věta: Necht' $f: G \rightarrow H$ je homomorfismus grup.

Je-li $G' \subset G$ podgrupa, pak $f(G') \subset H$ je podgrupa.

Je-li $H' \subset H$ podgrupa, pak $f^{-1}(H') \subset G$ je podgrupa.

dk: ověřme podobně jako u výše.

• Nujm $f(G') \neq \emptyset$ protože obsahuje $f(e_G) = e_H$.

Pro-li $a, b \in f(G')$, pak $a = f(u)$, $b = f(r)$ pro nějaké $u, r \in G'$.

$$a^{-1}b = (f(u))^{-1}f(r) = f(u^{-1}r) \Rightarrow a^{-1}b \in f(G'). \quad \checkmark$$

• $f^{-1}(H') \neq \emptyset$ protože $f^{-1}(H')$ obsahuje $f^{-1}(e_H) \ni e_G$.

Pro-li $a, b \in f^{-1}(H')$, pak $f(a), f(b) \in H'$. Pak

$$f(a^{-1}b) = (f(a))^{-1}f(b) \in H', \text{ proto } a^{-1}b \in f^{-1}(H'). \quad \checkmark$$

Pr: Zobrazení $\det: GL(n, T) \rightarrow T^*$

je homomorfismus (platí $\det(A \cdot B) = \det A \cdot \det B$)

$$\text{Ker}(\det) = \{A \in GL(n, T) \mid \det A = 1\} = SL(n, T),$$

což je podgrupa $GL(n, T)$.

Pr: Zobrazení $\text{sgn}: S_n \rightarrow \mathbb{C}_2 = (\{\pm 1\}, \cdot, i^{-1}, 1)$

je homomorfismus ($\text{sgn}(\pi \cdot \sigma) = \text{sgn} \pi \cdot \text{sgn} \sigma$)

$$\text{Ker}(\text{sgn}) = \{\pi \in S_n \mid \text{sgn} \pi = +1\} = A_n \text{ podgrupa } S_n$$

Pr: Zobrazení $f: \mathbb{Z}_n \rightarrow \mathbb{C}^*: k \rightarrow e^{\frac{2\pi i}{n}k}$ je homomorf.

$\text{Im } f = \mathbb{C}_n$ je podgrupa $\mathbb{C}^*$.

Věta: (Cayleova): Každá grupa je izomorfní s nějakou ^{pod} grupou ^{grupy} permutací.

dk: Najdeme izomorfismus $f: G \rightarrow f(G)$ podgrupa S_G ,
či stačí najít monomorfismus $f: G \rightarrow S_G = (G^G, \circ, i, i^{-1})$

K prvků $a \in G$ přiřadíme $\pi_a: G \rightarrow G: x \mapsto ax$.

- Je $\pi_a \in S_G$? musí to být bijekce.

Ano je, protože $ax = y \Leftrightarrow x = a^{-1}y$.

Takže prostě i na.

- Je přiřazení $f(a) = \pi_a$ prostě?

Pro $a, b \in G$ máme

$$f(a) = \pi_a, f(b) = \pi_b$$

Když $a \neq b$, pak $\pi_a(1) = a \neq b = \pi_b(1)$.

Tedy $\pi_a \neq \pi_b$.

- Je přiřazení $f(a) = \pi_a$ vůbec homomorfismus?

Pro $a, b \in G$ máme

$$f(a) = \pi_a, f(b) = \pi_b$$

$$f(ab) = \pi_{ab} : \pi_{ab}(x) = abx = a(bx) = (\pi_a \circ \pi_b)(x),$$

$$\text{takže } f(ab) = \pi_{ab} = \pi_a \circ \pi_b = f(a) \circ f(b) \quad \checkmark$$

Důsledek: Každou grupu o n prvcích lze izomorfně vložit do grupy S_n .

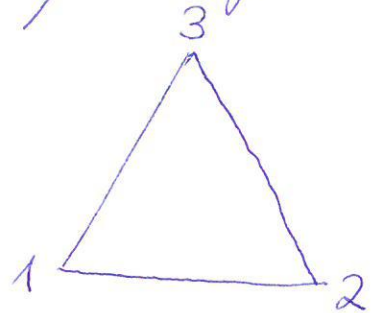
Pr: $\mathbb{Z}_3 = (\{0,1,2\}, + \bmod 3) \simeq \mathbb{C}_3 = (\{e^{\frac{2\pi i}{3}k} \mid k=0,1,2\}, \cdot)$ 18,5

$\simeq \left\{ \begin{pmatrix} \cos(\frac{2\pi i}{3}k) & -\sin(\frac{2\pi i}{3}k) \\ \sin(\frac{2\pi i}{3}k) & \cos(\frac{2\pi i}{3}k) \end{pmatrix} \mid k=0,1,2 \right\}, \cdot$

$\simeq A_3 = \left(\left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\}, \circ \right)$

což je podgrupa S_3

↑
řešení symetrie



notace
rovnoramenného
trojúhelníka

$f: \mathbb{Z}_3 \longrightarrow S_3$ homomorfismus $\text{Im } f = f(\mathbb{Z}_3) = A_3$
 f je izomorfismus $\mathbb{Z}_3$ a A_3

Def: Je-li G grupa, pak značíme

$$\text{Aut } G := \left(\{ f: G \rightarrow G \mid f \text{ automorfismus} \}, \circ, {}^{-1}, 1_G \right)$$

grupa automorfismů grupy G .

Pozn: $\text{Aut } G$ je opravdu grupa (krajně)

• $\text{Aut } G$ je podgrupa S_G .

Pr: $\text{Aut } \mathbb{Z} \simeq \mathbb{Z}_2$, protože $\text{Aut } \mathbb{Z} = \{ \text{id}, f: k \mapsto -k \}$

Jediné endomorfismy jsou $f(n) = n \cdot f(1)$, ale
z pořadovosti surjektivit plyne $f(1) = \pm 1$ (1 musí být
nebo).

Pr: $\text{Aut } \mathbb{Z}_3 \simeq \mathbb{Z}_2$. Automorfismus φ musí $\varphi(0) = 0$,
leč identity už jen $\varphi(1) = 2, \varphi(2) = 1$,
což je takový automorfismus ($\varphi(x+y) = \varphi(x) + \varphi(y)$).

Věta: Průnik libovolného systému podgrup dané grupy je podgrupa.

dh: G grupa, $H_\alpha \subset G$ podgrupa pro $\alpha \in I$ index množ. I .

Položíme $H := \bigcap_{\alpha \in I} H_\alpha$. Dokažme, že je to podgrupa.

$H \neq \emptyset$, protože $e \in H_\alpha \forall \alpha \in I$, tj. $e \in H$.

Pokud $a, b \in H$, pak $\forall \alpha \in I$ $a, b \in H_\alpha$, tj. $a^{-1}b \in H_\alpha$,
tj. $a^{-1}b \in H$.

Důsledek: Necht' G je grupa, $\emptyset \neq X \subset G$ libv. podmnožina.

Pak v G existuje nejmenší podgrupa obsahující X .
ve smyslu inkluze

dh: je to $\bigcap \{H \mid H \text{ podgrupa } G, H \supset X\}$.

Def: Označíme $\langle X \rangle_G =$ nejmenší podgrupa v G obsahující X .

Nazýváme podgrupa grupy G generovaná množ. X .

Někdy místo $\langle \{x_1, \dots, x_n\} \rangle_G$ značíme $\langle x_1, \dots, x_n \rangle_G$.

Věta: Necht' G je grupa, $\emptyset \neq X \subset G$ podmnožina.

Pak $\langle X \rangle_G = \{a_1^{k_1} a_2^{k_2} \dots a_m^{k_m} \mid m \in \mathbb{N}, a_1, \dots, a_m \in X, k_1, \dots, k_m \in \mathbb{Z}\}$.

Pozn: V aditivním zápisu pro konečnou $X = \{x_1, \dots, x_n\}$:

$\langle x_1, \dots, x_n \rangle_G = \{k_1 x_1 + k_2 x_2 + \dots + k_n x_n \mid k_1, \dots, k_n \in \mathbb{Z}\}$

tj. analogie lin. obalu, lze chápat jako grupový obal.

dlh: označme H množinu na PS .

20

1) $\langle X \rangle_G \subset H$: Pro každé $x \in X$ lze volit $m=1$, $a_1=x$, $k_1=1$.

Odtud $H \neq \emptyset$ a navíc snadno vidíme, že H je podgrupa ($\forall a, b \in H$ je $a^{-1}b \in H$)

Protože $\langle X \rangle_G$ je nejmenší podgrupa pbs. X ,
tj. $\langle X \rangle_G \subset H$.

2) $H \subset \langle X \rangle_G$: Pro $m \in \mathbb{N}$, $a_1, \dots, a_m \in X$, $k_1, \dots, k_m \in \mathbb{Z}$ plyne,
že $a_1^{k_1} \dots a_m^{k_m} \in \langle X \rangle_G$, protože $a_i \in X$ a
 $\langle X \rangle_G$ je podgrupa, tedy uzavřená na operaci.

Př: Pro každé $n \in \mathbb{N}$, $n \geq 2$ platí $\mathbb{Z}_n = \langle 1 \rangle_{\mathbb{Z}_n}$

Platí $\mathbb{Z} = \langle 1 \rangle_{\mathbb{Z}}$

Def: Počet prvků grupy G označme $|G|$, nazýváme
řád grupy G . Pro $a \in G$ označme $|a|$ počet
prvků podgrupy $\langle a \rangle_G$, nazýváme řád prvku $a \in G$

Pozn: Pro konečnou G kladně: $\forall a \in G$ $|a| \leq |G| < +\infty$.

Platí: Pro libovolnou grupu G a prvek $a \in G$:

1) $|a|=1 \iff \langle a \rangle_G = \{e\} \iff a=e$

2) $|a|=2 \iff \langle a \rangle_G = \{e, a\} \iff a \neq e, a^{-1}=a$ tj. $a^2=e$.

Pro involutivní prvek

napr. $\left| \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right| = 2$, protože $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$.

$\in GL(2, \mathbb{R})$

dk: označme H množinu na PS .

- 1) $\langle X \rangle_G \subset H$: Pro každé $x \in X$ lze volit $m=1$, $a_1=x$, $k_1=1$.
 Odtud $H \neq \emptyset$ a navíc snadno vidíme, že
 H je podgrupa ($\forall a, b \in H$ je $a^{-1}b \in H$)
 Protože $\langle X \rangle_G$ je nejmenší podgrupa pbs. X ,
 tj. $\langle X \rangle_G \subset H$.
- 2) $H \subset \langle X \rangle_G$: Pro $m \in \mathbb{N}$, $a_1, \dots, a_m \in X$, $k_1, \dots, k_m \in \mathbb{Z}$ plyne,
 že $a_1^{k_1} \dots a_m^{k_m} \in \langle X \rangle_G$, protože $a_i \in X$ a
 $\langle X \rangle_G$ je podgrupa, tedy uzavřená na operaci.

Př: Pro každé $n \in \mathbb{N}$, $n \geq 2$ platí $\mathbb{Z}_n = \langle 1 \rangle_{\mathbb{Z}_n}$
 Platí $\mathbb{Z} = \langle 1 \rangle_{\mathbb{Z}}$

Def: Počet prvků grupy G označme $|G|$, nazýváme
řád grupy G . Pro $a \in G$ označme $|a|$ počet
 prvků podgrupy $\langle a \rangle_G$, nazýváme řád prvku a v G

Pozn: Pro konečnou G křijme: $\forall a \in G \quad |a| \leq |G| < +\infty$.

Platí: Pro libovolnou grupou G a prvek $a \in G$:

$$1) |a|=1 \Leftrightarrow \langle a \rangle_G = \{e\} \Leftrightarrow a=e$$

$$2) |a|=2 \Leftrightarrow \langle a \rangle_G = \{e, a\} \Leftrightarrow a \neq e, a^{-1}=a \text{ tj. } a^2=e, a \neq e$$

Pro involutivní prvek

např. $\left| \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right| = 2$, protože $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I_2$.

$\sim GL(2, \mathbb{R})$

Věta: Necht' G je grupa, $a \in G$. Pak nastane právě jedna z možností:

(1) $|a| = +\infty$, tj. $\forall m \in \mathbb{N}$ platí $a^m \neq e$.

Přitom zobrazení $f: \mathbb{Z} \rightarrow G: m \rightarrow a^m$ je monomorfismus.

tj. $\langle a \rangle_G = \{a^m \mid m \in \mathbb{Z}\} = \text{Im} f \simeq \mathbb{Z}$.

(2) $|a| = n \in \mathbb{N}$, kde n je nejmenší $\in \mathbb{N}$ tak, že $a^n = e$.

a $\forall m \in \mathbb{Z}$ platí $a^m = a^{m \bmod n}$.

Přitom zobrazení $\tilde{f}: \mathbb{Z}_n \rightarrow G: k \rightarrow a^k$ je monomorfismus.

tj. $\langle a \rangle_G = \{e = a^0, a^1, \dots, a^{n-1}\} = \text{Im} \tilde{f} \simeq \mathbb{Z}_n$

dk: Pro zobrazení $f: \mathbb{Z} \rightarrow G: m \rightarrow a^m$ nastane právě jedna z možností:

- $\text{Ker} f := \{m \in \mathbb{Z} \mid a^m = e\} = \{0\}$

Pak f je monomorfismus, tj. $\mathbb{Z} \simeq \text{Im} f = \langle a \rangle_G$.

Zřejmě $|a| = |\langle a \rangle_G| = +\infty$.

- $\text{Ker} f \neq \{0\}$. Označme $n = \min \{k \in \mathbb{N} \mid k \in \text{Ker} f\} = \min \{k \in \mathbb{N} \mid a^k = e\}$.

Takové n existuje, protože $\text{Ker} f$ je podgrupa $\mathbb{Z}$, tj. s každým $k \in \text{Ker} f$ je i $-k \in \text{Ker} f$.

Zkoumejme a^m . Vezmeme $m = k \cdot n + r$, $k \in \mathbb{Z}$, $r \in \{0, \dots, n-1\}$.

Pak $a^m = a^{kn+r} = (a^n)^k \cdot a^r = e^k \cdot a^r = a^r = a^{m \bmod n}$.

Zobrazení $\tilde{f}: \mathbb{Z}_n \rightarrow G: k \rightarrow a^k$ je monomorfismus.

homo: $\tilde{f}(k_1) \tilde{f}(k_2) = a^{k_1} a^{k_2} = a^{k_1+k_2} = a^{(k_1+k_2) \bmod n} = \tilde{f}(k_1+k_2)$.

mono: $\tilde{f}(k) := a^k = e \Leftrightarrow k = 0$ (z minimality n)

Proto $\text{Im} \tilde{f} = \langle a \rangle_G \simeq \mathbb{Z}_n$.

Pozn: Řád prvku a v grupě G :

$$|a| = |\langle a \rangle| = \min\{k \in \mathbb{N} \mid a^k = e\}$$

Plati: Je-li $|a| = m$, pak $a^k = e \Leftrightarrow m \mid k$.

Lemma: Necht' G je grupa. Potom

$$1) \forall a \in G: |\bar{a}^{-1}| = |a|$$

$$2) \forall a, b \in G: |ab| = |ba|$$

$$3) \forall a, b \in G: |ab\bar{a}^{-1}| = |b|$$

dk: ad1) Platí $(\bar{a}^{-1})^m = (\underbrace{a^m})^{-1} = e \Rightarrow |\bar{a}^{-1}| \leq |a|$
 naopak $a^m = (\underbrace{(\bar{a}^{-1})^m})^{-1} = e \Rightarrow |a| \leq |\bar{a}^{-1}| \Rightarrow |\bar{a}^{-1}| = |a|$

$$\text{ad2)} (ab)^n = e \Rightarrow (ba)^{n+1} = b \underbrace{(ab)^n} = e a = ba$$

$$\text{krácejším: } (ba)^n = e \Rightarrow |ab| \leq |ba|$$

ke symetrii $|ab| = |ba|$.

$$\text{ad3)} \text{ Dle 2) platí } |a(b\bar{a}^{-1})| = |b\bar{a}^{-1}a| = |b|.$$

Lemma: Necht' G je grupa. Potom mají-li $a, b \in G$ konečný řád a platí $ab = ba$, pak $|ab| \mid |a| \cdot |b|$.

dk: Označme $|a| = m, |b| = n$.

$$\text{Pak } (ab)^{m \cdot n} = \underbrace{(a^m)^n}_{\text{z komutace}} (b^n)^m = e^m \cdot e^m = e.$$

Př: Řád prvku $|1+2|$ v grupě $\mathbb{Z}_6$

$$|2+3|$$

$$\begin{array}{l|l} \underbrace{|1+2|}_{=2} = |3| & |1| \cdot |2| \\ & \frac{1}{6} \cdot \frac{1}{3} \\ \hline \underbrace{|2+3|}_{=6} = |5| & |2| \cdot |3| \\ & \frac{1}{3} \cdot \frac{1}{2} \end{array}$$

Cyklické' grupy

22

Def: Grupa G je cyklická, jistliže je generována' jedním prvkem, tedy $\exists a \in G$ tak, že $G = \langle a \rangle_G$.

Věta (klasifikace cyklických grup):

Nechť G je cyklická grupa. Potom platí' jedno z:

1) $G \cong \mathbb{Z}$ při $|G| = +\infty$

2) $G \cong \mathbb{Z}_n$ při $|G| = n \in \mathbb{N}$.

dk: viz věta výše.

Věta: Každá' podgrupa cyklické' grupy je cyklická'.

dk: Necht' $G = \langle a \rangle_G$, $H \subset G$ podgrupa.

Je-li $H = \{e\}$ nebo $H = G$, pak zřejmé'.

Necht' $\{e\} \neq H \neq G$. Nutně obsahuje prvek a^j .

Vezmu min j tak, že $a^j \in H$. Dokažeme $H = \langle a^j \rangle_G$.

Inkluze $\langle a^j \rangle \subset H$ je zřejmá'.

Naopak, vezmeme $b \in H$, tj. $b = a^m$ pro nějaké $m \in \mathbb{Z}$.

ozn. $m = sj + r$, takže $b = a^m = a^{sj+r} = (a^j)^s a^r$.

odtud $\underbrace{a^r}_{\in H} = \underbrace{(a^j)^{-s}}_{\in H} b \in H$.

Z minimality j nutně $r=0$,
proto $a^r = e$, čili $b = (a^j)^s$.

Tru. $H \subset \langle a^j \rangle$.

Pozn! $j \mid n$. Jinak $n = sj + r \Rightarrow a^n = e = (a^j)^s a^r \Rightarrow a^r = (a^j)^{-s} \in H$
spor

Věta: (popis generátorů): Necht' G je cyklická grupa,
 $G = \langle a \rangle$. Potom:

- 1) je-li G nekonečná, pak $G = \langle a \rangle = \langle a^{-1} \rangle$,
 ale $G \neq \langle a^k \rangle$ pro všechna $k \neq \pm 1$.
- 2) je-li G řádu n , pak $\langle a^k \rangle = G \Leftrightarrow k \perp n$.
 Speciálně G má $\varphi(n)$ různých generátorů.

dk: ad1) je-li $|G| = +\infty$, a $b \in G$ generátor $b = a^j$,
 nutně $\exists t \in \mathbb{Z}$ tak, že $a = (a^j)^t$.
 Odtud krátíme $e = a^{jt-1}$, spor s $\text{Ker} f = \{0\}$.

ad2) je-li $|G| = n \in \mathbb{N}$; $\langle a^k \rangle = G$. Pak

$a = (a^k)^x$ pro nějaké $x \in \mathbb{Z}$

Vydělíme $kx = y \cdot n + r$, $r \in \{0, \dots, n-1\}$,

takže $a = (\underbrace{a^n}_e)^y a^r$, tj. $e = a^{n-1}$.

Nutně $n-1/n \Rightarrow r=1$.

Protože $kx - ny = 1$, musí $k \perp n$.

Naopak je-li $k \perp n$, k Bézoutova lemma
 existují $x, y \in \mathbb{Z}$ tak, že $kx - ny = 1$.

Proto $(a^k)^x = (\underbrace{a^n}_e)^y a = a$, takže $\langle a^k \rangle = G$.

Def: Eulerova funkce $\varphi: \mathbb{N} \rightarrow \mathbb{N}$:

$$\varphi(n) = |\{k \in \mathbb{N} \mid k \leq n, k \perp n\}|$$

Pozn (viz D10.1): $\varphi(n) = n \prod_{\substack{p \text{ prvoč.} \\ p \perp n}} \left(1 - \frac{1}{p}\right)$

Př: $\varphi(28) = 28 \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{7}\right) = 12$

Pr: $\mathbb{Z}_{28} = \{0, 1, \dots, 27\}$

$$\{k \in \mathbb{Z}_{28} \mid k \perp 28\} = \{1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27\}$$

generators $\mathbb{Z}_{28}$ $\nearrow$

Pr: Grupa $C_n = (\underbrace{\{e^{\frac{2\pi i}{n}k}\}_{k \in \{0, \dots, n-1\}}}_{\omega^k}, \cdot)$

Generators C_n jsou $e^{\frac{2\pi i}{n}k}$, $k \perp n$.

... stav. primitivních n -tých kořenů z 1.

Věta: C_m je podgrupa $C_n \iff m \mid n$.

dlk: $\Leftarrow C_m = \{\omega^0=1, \omega, \omega^2, \dots, \omega^{m-1}\}$ pro $\omega = e^{\frac{2\pi i}{n}}$

$C_m = \{\eta^0=1, \eta, \dots, \eta^{m-1}\}$ pro $\eta = e^{\frac{2\pi i}{m}}$

$m \mid n \Rightarrow \eta = e^{\frac{2\pi i}{m}} = e^{\frac{2\pi i}{n} \cdot \frac{n}{m}} = \omega^{\frac{n}{m}} \in C_n$

$\Rightarrow C_m = \langle \omega^{\frac{n}{m}} \rangle_{C_n}$ podgrupa C_n .

$\Rightarrow$ z něj vyše každá podgrupa C_m je cyklická, přičemž je generována prvky ω^j , kde $j \mid m$.

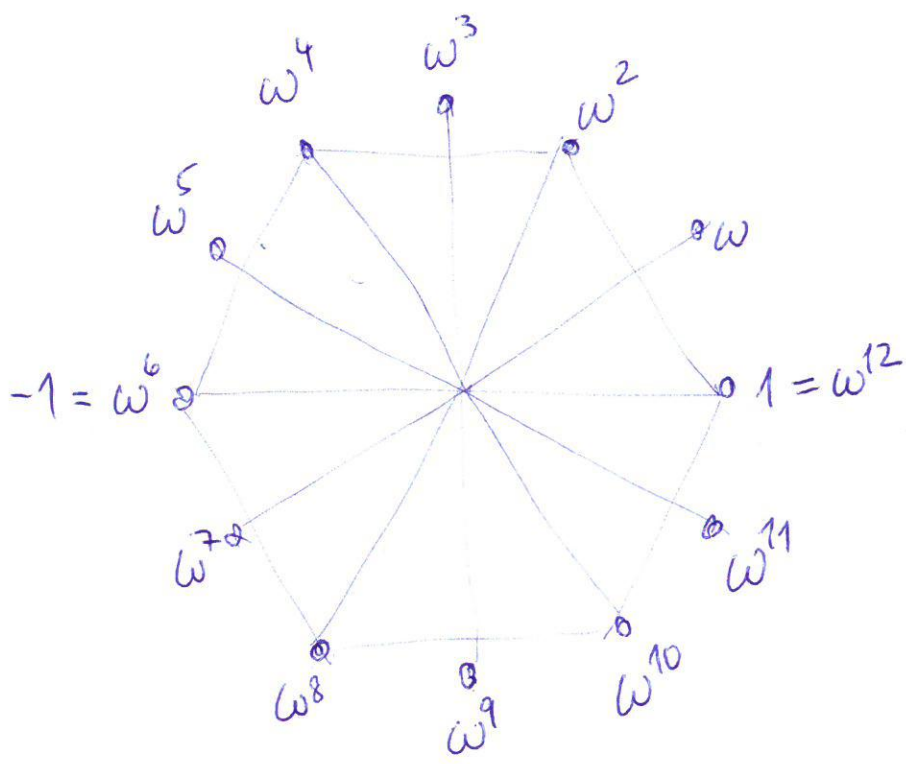
$\eta = \omega^j = e^{\frac{2\pi i}{n}j} = e^{\frac{2\pi i}{m}}$, kde $m = \frac{n}{j} \mid n$.

Důsledek: $n = \sum_{m \mid n} \varphi(m)$

dlk: Pro každé $m \mid n$ je právě $\varphi(m)$ primitivních m -tých kořenů z 1.

- Pr: $\mathbb{C}_{12}$ primitivní 12-té kořeny ω^k pro $k=1,5,7,11$
- $\mathbb{C}_6$ primitivní 6-té kořeny ω^k pro $k=2,10$ tj. $(\omega^2)^1, (\omega^2)^5$
- $\mathbb{C}_4$ primitivní 4-té kořeny ω^k pro $k=3,9$ tj. $(\omega^3)^1, (\omega^3)^3$
- $\mathbb{C}_3$ primitivní 3-té kořeny ω^k pro $k=4,8$ tj. $(\omega^4)^1, (\omega^4)^2$
- $\mathbb{C}_2$ primitivní 2-té kořeny ω^k pro $k=6$ tj. $(\omega^6)^1$
- $\mathbb{C} \dots k=0 \quad \omega^0=1$
resp. $k=12$

$\omega = e^{\frac{2\pi i}{12}}$



Další (širší) třída grup jsou
konečně generované abelovské grupy.

jako přímé zobecnění cyklických grup,
kteří jsou zřejmě abelovské a 1-generované.

Pro klasifikaci potřebujeme pojem
direktního součinu grup.

Klasifikaci uvedeme bez plného důkazu.

Direktní součin grup

25

Def: jsou-li G_1, G_2 grupy, pak $G_1 \times G_2$ s operací $*$:

$$\forall g_1, h_1 \in G_1, \forall g_2, h_2 \in G_2: (g_1, g_2) * (h_1, h_2) = (g_1 h_1, g_2 h_2)$$

je grupou, kterou nazýváme direktní součin grup G_1, G_2 .

Pozn: Definici lze rozšířit na libovolný počet součinitelů

Př: $\mathbb{Z}_2 \times \mathbb{Z}_2$

sro. $\mathbb{Z}_4$

	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)	(1,0)	(1,1)
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)	(1,0)	(1,1)	(0,0)	(0,1)
(1,1)	(1,1)	(1,0)	(0,1)	(0,0)

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Pozn: • jednotka $\pi G_1 \times G_2$ je $e_{G_1 \times G_2} = (e_{G_1}, e_{G_2})$

Pro $(g_1, g_2) \in G_1 \times G_2$ je inverze $(g_1, g_2)^{-1} = (g_1^{-1}, g_2^{-1})$.

• Zřejmě pro každou grupu G platí

$$G \cong \{e\} \times G.$$

Značení: Pro podmnožiny $X, Y \subset G$ označme

$$XY := \{ab \mid a \in X, b \in Y\}$$

Pro $X = \{a\}$ píšeme aY místo $\{a\}Y$.

Plati': Necht G_1, G_2 jsou grupy. Potom

$$\begin{aligned} f_1: G_1 &\rightarrow G_1 \times G_2 : u \mapsto (u, e_{G_2}) \\ f_2: G_2 &\rightarrow G_1 \times G_2 : v \mapsto (e_{G_1}, v) \end{aligned}$$

jsou monomorfismy.

Ověřme-li $G_1' = \text{Im} f_1 = G_1 \times \{e_{G_2}\}$

$G_2' = \text{Im} f_2 = \{e_{G_1}\} \times G_2$.

Pak platí: i) $\forall u \in G_1', \forall v \in G_2' : uv = vu$

ii) $G_1' \cap G_2' = \{e_{G_1 \times G_2}\}$

iii) $G_1' G_2' = G_1 \times G_2 \leftarrow \text{věty}.$

Tvrzení': Necht G je grupa a $G_1, G_2 \subset G$ podgrupy takové, že platí:

i) $\forall u \in G_1, \forall v \in G_2 : uv = vu$

ii) $G_1 \cap G_2 = \{e\}$

iii) $G_1 G_2 = G$

Pak $G \cong G_1 \times G_2$.

dk: Bod (iii) implikuje, že $\forall g \in G \exists u \in G_1, \exists v \in G_2 : g = uv$.

Rozklad je jednoznačný, jinak by

$uv = ab$ pro $a \in G_1, b \in G_2$. Pak ale

$\underbrace{\bar{a}^{-1}u}_{\in G_1} = \underbrace{bv^{-1}}_{\in G_2}$ tj. $\bar{a}^{-1}u = bv^{-1} = e$ (podle (ii)).

Odtud $a = u, b = v$.

Definujme tedy zobrazení $\varphi: G \rightarrow G_1 \times G_2 : \varphi(g) = (u, v)$, kde $g = uv$.

Ověřme, že φ je izomorfismus.

$$\varphi \text{ homomorfismus: } \varphi(g_1 g_2) \stackrel{?}{=} \varphi(g_1) \cdot \varphi(g_2)$$

27

$$\text{vime: } \varphi(g_i) = (u_i, v_i)$$

Máme $g_1 g_2 = u_1 v_1 u_2 v_2$. Podle (i) platí

$$\begin{aligned} g_1 g_2 &= u_1 u_2 v_1 v_2, \text{ tj. } \varphi(g_1 g_2) = (u_1 u_2, v_1 v_2) = \\ &= (u_1, v_1) (u_2, v_2) = \\ &= \varphi(g_1) \cdot \varphi(g_2) \text{ ok.} \end{aligned}$$

φ surjektivní: $\forall (u, v) \in G_1 \times G_2$ je $g = uv$ tak, že $\varphi(g) = (u, v)$.

φ injektivní: Je-li $\varphi(g) = (e, e)$, pak $g \stackrel{\uparrow}{=} ee = e$.

Odtud $\text{Ker } \varphi = \{e\}$, takže monomorf. ctd. z definice φ

Aplikace = ilustrace

Lemma (čínské o klytčích): Jsou-li $m_1, \dots, m_k \in \mathbb{N}$ po dvou nesoudělná pro $k \in \mathbb{N}$, pak $M = m_1 m_2 \dots m_k$.

Potom zobrazení $\varphi: \mathbb{Z}_M \rightarrow \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_k}$
 $n \mapsto (n \bmod m_1, \dots, n \bmod m_k)$

je izomorfismus grup.

Proto $\mathbb{Z}_M \cong \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$.

Pozn: Z DMT1 známe řešení:

Necht $m_1, \dots, m_k$ po dvou nesoudělná.

Pro libovolná $r_1, \dots, r_k \in \mathbb{Z}$ existuje řešení $n \in \mathbb{Z}$

soustavy $n = r_i \bmod m_i, i = 1, \dots, k$.

Je dáno jednoznačně mod $M (= m_1 \dots m_k)$.

dk: nutno ověřit, že $\varphi: \mathbb{Z}_M \rightarrow \mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}$
 je homomorfismus, tj. $\forall n, \tilde{n} \in \mathbb{Z}_M$:

$$\varphi(n + \tilde{n}) = (n \bmod m_1, \dots, n \bmod m_k) * (\tilde{n} \bmod m_1, \dots, \tilde{n} \bmod m_k)$$

$$= ((n + \tilde{n}) \bmod m_1, \dots, (n + \tilde{n}) \bmod m_k)$$

Plyne z vlastností kongruence a
 definice direktního součinu.

monomorf. ? $\text{Ker } \varphi = \{0\}$?

$$n \in \text{Ker } \varphi \Leftrightarrow \varphi(n) = (0, \dots, 0) \Leftrightarrow n \equiv 0 \bmod m_i \quad \forall i$$

$$\Leftrightarrow m_i \mid n \quad \forall i$$

$$\Leftrightarrow M \mid n \Leftrightarrow n = 0 \text{ v } \mathbb{Z}_M$$

$\uparrow$
 z nesoudělnosti m_i

$\Rightarrow \varphi$ je prosté!

epimorf. ? Ano, protože

$$|\mathbb{Z}_M| = M = m_1 \dots m_k = |\mathbb{Z}_{m_1} \times \dots \times \mathbb{Z}_{m_k}|$$

$\Rightarrow \varphi$ je izomorfismus.

Pozn: • Speciální případ $m_i = p_i^{l_i}$, p_i prvočíslo, $l_i \in \mathbb{N}$.
 Pak $\mathbb{Z}_M = \mathbb{Z}_{p_1^{l_1}} \times \dots \times \mathbb{Z}_{p_k^{l_k}}$, kde $M = p_1^{l_1} \dots p_k^{l_k}$.
 • Využívá se k paralelizaci výpočtů
 s velkými čísly.

Lemma: Necht G je abelovská grupa.

Označme $H = \{a \in G \mid |a| < +\infty\}$.

Pak H je podgrupa grupy G .

dk: z vlastnosti $ab = ba$ plyne $|ab| \mid |a| \cdot |b|$ (viz sh. 21,5)

Proto $|a|, |b| < +\infty \Rightarrow |ab| \mid |a| \cdot |b| \Rightarrow |ab| < +\infty$.

$\Rightarrow ab^{-1} \in H$ a tedy H je podgrupa. ($H \ni e$).

Def: Necht G je konečně generovaná abelovská grupa.

• Podgrupu $G_{\text{tor}} = \{a \in G \mid |a| < +\infty\}$ nazveme Torrem část grupy G .

• Je-li $G_{\text{tor}} = \{e\}$, říkáme, že G je bez torze.

• Je-li $G = G_{\text{tor}}$, říkáme, že G je Torrem grupa.

• Je-li $G \cong \mathbb{Z} \times \dots \times \mathbb{Z} = \mathbb{Z}^n$ pro nějaké $n \in \mathbb{N}_0$, říkáme, že G je volná abelovská grupa.

Pozn: Značíme $\mathbb{Z}^n = \{e\}$ pro $n = 0$.

Lemma: Necht G je konečně generovaná abelovská grupa.

Pak: 1) G je volná abelovská $\Leftrightarrow G$ je bez torze.

2) Každá podgrupa volné abelovské grupy je volná abelovská grupa.

3) $\forall G$ existuje volná abelovská podgrupa H
Pak, že $G \cong H \times G_{\text{tor}}$.

4) G_{tor} je konečně generovaná, tj. konečná.

Tvrzení: Necht' G je konečná abelovská grupa
a necht' p je prvočíslo takové, že $p \mid |G|$.
Pak $H = \{a \in G \mid |a| = p^k \text{ pro nějaké } k \in \mathbb{N}_0\}$
je podgrupa grupy G .

dk: $H \neq \emptyset$, protože $|e| = 1 = p^0$, tj. $e \in H$.

Pro $a, b \in H$, máme $|a| = p^j$, $|b| = p^k = |b^{-1}|$.

Pak $|ab^{-1}| \mid |a| \cdot |b^{-1}| = p^{j+k} \Rightarrow ab^{-1} \in H$.

Def: Necht' G je konečná abelovská grupa.
Podgrupu $G(p) := H$ k tvrzení nazveme
 p -prímární komponenta grupy G .

Tvrzení: Bud' G konečná abelovská grupa.

Pak $G \cong \prod_{\substack{p \in \mathbb{P} \\ p \mid |G|}} G(p) := G(p_1) \times \dots \times G(p_k)$.

Navíc $\forall p \in \mathbb{P}, p \mid |G|$ platí

$G(p) \cong \mathbb{Z}_{p^{i_1}} \times \dots \times \mathbb{Z}_{p^{i_k}}$ pro nějaké $j_1, \dots, j_k \in \mathbb{N}$.

Věta (Klasifikace konečně generovaných
abelovských grup):

Neht' G je konečně gen. abelovská grupa. Potom

$G \cong \mathbb{Z}^m \times \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_n^{k_n}}$, kde

$m, n \in \mathbb{N}_0$ jsou určeny jednoznačně,

$p_1, \dots, p_n \in \mathbb{P}$, $k_1, \dots, k_n \in \mathbb{N}$, přičemž soubor

$p_1^{k_1}, \dots, p_n^{k_n}$ je jednoznačný až na pořadí,

Př: $\mathbb{Z}[\omega] = \{a + b\omega + c\omega^2 + d\omega^3 \mid a, b, c, d \in \mathbb{Z}\}$

$\omega = e^{\frac{2\pi i}{8}} = \frac{\sqrt{2}}{2}(1+i)$ $\uparrow$ monoid vzhledem k $\cdot$,
protože $\omega^4 = -1$.

Lze ukázat, že grupa $(\mathbb{Z}[\omega])^\times$ invertibilních
prvků v $\mathbb{Z}[\omega]$ je tvaru:

$$(\mathbb{Z}[\omega])^\times = \{ \omega^j (1+\sqrt{2})^k \mid j, k \in \mathbb{Z} \} \simeq \mathbb{Z}_8 \times \mathbb{Z},$$

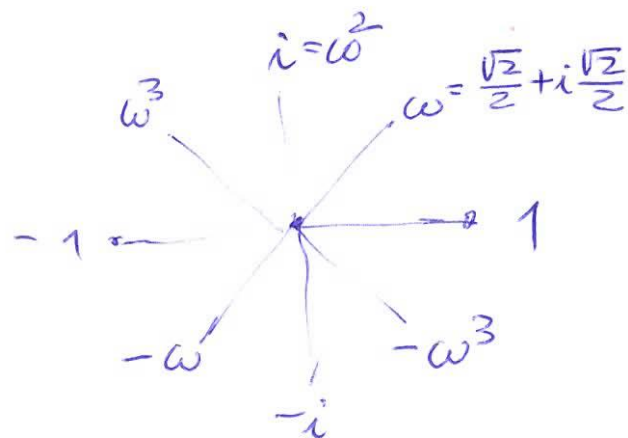
tj. 2-generovaná abelovská grupa,
která není ani torzem, ani volnou,
je tzv. smíšená.

Ověříme $1+\sqrt{2} \in \mathbb{Z}[\omega]$

$$1+\sqrt{2} = 1 + \omega - \omega^3 \in \mathbb{Z}[\omega]$$

podobně

$$-1+\sqrt{2} = -1 + \omega - \omega^3 \in \mathbb{Z}[\omega]$$



Přitom $(1+\sqrt{2})(-1+\sqrt{2}) = 1$,

tj. $1+\sqrt{2}, -1+\sqrt{2}$ jsou invertibilní v $\mathbb{Z}[\omega]$

$$(1+\sqrt{2})^{-1} = -1+\sqrt{2}.$$

Translace v grupě, Lagrangeova věta

29

Def: Necht G je grupa, $a \in G$. Potom

$$L_a: G \rightarrow G: x \rightarrow ax$$

$$R_a: G \rightarrow G: x \rightarrow xa$$

se nazývají levá, resp. prava translace o prvku a .

Twzení:

1) Zobrazení L_a, R_a jsou bijekce G na sebe.

$$2) L_a \circ R_b = R_b \circ L_a, \forall a, b \in G.$$

$$3) \text{ Zobrazení } G \rightarrow S_G: a \rightarrow L_a$$

$$G \rightarrow S_G^{\text{op}}: a \rightarrow R_a$$

jsou monomorfismy.

Pozn: S_G symetrická grupa = (bijekce na G , skládání)
 S_G^{op} = (bijekce na G , skládání v opačném pořadí)

dk: Vlastnosti L_a, R_a :

$$\bullet L_e = R_e = 1_G$$

$$\bullet (L_a \circ R_b)x = L_a(R_b x) = L_a(xb) = axb = a \cdot (xb) > \text{komutují}$$

$$(R_b \circ L_a)x = R_b(L_a x) = R_b(ax) = axb = a \cdot (xb)$$

$$\bullet L_a \circ L_b = L_{ab}, \text{ protože}$$

$$(L_a \circ L_b)x = L_a(L_b x) = L_a(bx) = abx = L_{ab}x$$

$$\bullet R_a \circ R_b = R_{ba}$$

$$(R_a \circ R_b)x = R_a(R_b x) = R_a(xb) = xba = R_{ba}x$$

$$\circ L_a \circ L_{a^{-1}} = L_{aa^{-1}} = L_e = 1_G = L_{a^{-1}a} = L_{a^{-1}} \circ L_a$$

$$\Rightarrow L_{a^{-1}} = (L_a)^{-1}$$

$$\circ R_a \circ R_{a^{-1}} = R_e = 1_G = R_{a^{-1}} \circ R_a$$

$$\Rightarrow R_{a^{-1}} = (R_a)^{-1}$$

• Zobrazení L_a, R_a mají inverze na G
 $\Rightarrow$ jsou to bijekce

• Zobrazení $a \rightarrow L_a$ je homomorfismus $G \rightarrow S_G$
 $a \rightarrow R_a$ je homomorfismus $G \rightarrow S_G^{\text{op}}$

$$\circ L_a = 1_G \Leftrightarrow \forall x \in G : L_a x = ax = x \Leftrightarrow a = e$$

tj. v jádru zobrazení $a \rightarrow L_a$ je jen e .

$\Rightarrow$ zobrazení je monomorfismus $G \rightarrow S_G$

• Stejně pro $a \rightarrow R_a$, monomorfismus $G \rightarrow S_G^{\text{op}}$.

Def: Necht G je grupa, $H \subset G$ podgrupa.

Na G definujeme relaci $\sim$:

$$\forall a, b \in G: a \sim_L b \Leftrightarrow ab^{-1} \in H \Leftrightarrow \exists h \in H: a = L_h b = hb$$

Poru: obdobně pro pravou translaci

$$a \sim_R b \Leftrightarrow b^{-1}a \in H \Leftrightarrow \exists h \in H: a = R_h b = bh$$

Lemma: Relace $\sim$ je ekvivalence.

dk:

- Reflexivita $a \sim a \Leftrightarrow aa^{-1} = e \in H$ ano
- Symetrie $a \sim b \Leftrightarrow ab^{-1} \in H \Rightarrow (ab^{-1})^{-1} = ba^{-1} \in H \Rightarrow b \sim a$
- Transitivita $\left. \begin{array}{l} a \sim b \Leftrightarrow ab^{-1} \in H \\ b \sim c \Leftrightarrow bc^{-1} \in H \end{array} \right\} \xRightarrow{?} ac^{-1} \in H$

$\underbrace{ab^{-1}}_{\in H} \underbrace{bc^{-1}}_{\in H} \xrightarrow{?} ac^{-1}$

ok.

Def:

Tridy ekvivalence $\sim_L$, resp. $\sim_R$ se nazývají
levé, resp. pravé tridy rozkladu G při H .

$$[a]_{\sim_L} = [a]_L = \{ha \mid h \in H\} = Ha = R_a(H)$$

$$[a]_{\sim_R} = [a]_R = \{ah \mid h \in H\} = aH = L_a(H)$$

Plati: V libovolné grupě G s podgrupou H platí:

- 1) $\forall a \in G$ je $|Ha| = |aH| = |H|$
- 2) Pro $[a], [b]$ platí $[a] \cap [b] = \emptyset$ nebo $[a] = [b]$.

dk: 2) z vlastností ekvivalence

1) R_a, L_a jsou bijekce (j. prostá zobr., proto $|H| = |R_a(H)| = |Ha| = |aH|$)

ok.

Známění: Pro grupu G a podgrupu H : 31

$$H \backslash G = \{ Ha \mid a \in G \} \text{ levý faktorprostor } G \text{ podle } H$$

$$G/H = \{ aH \mid a \in G \} \text{ pravý faktorprostor } G \text{ podle } H$$

Věta: (Lagrange): Je-li G konečná grupa,
 H její podgrupa, pak platí:

$$|G/H| = |H \backslash G| = \frac{|G|}{|H|}.$$

Speciálně platí $|H| \mid |G|$.

dk: Provedeme rozklad G podle ekvivalence $\sim$

$$G = \bigcup_{a \in G} [a] = \bigcup_{A \in H \backslash G} A$$

Množiny $A \in H \backslash G$ jsou disjunktní a všechny
stejně velké, $|A| = |H|$, proto

$$|G| = |H| \cdot |H \backslash G|.$$

Důsledek: Pro každý prvek $a \in G$ platí $|a| \mid |G|$.

dk: $|a| = |\langle a \rangle|$.

Důsledek: Je-li $|G| \in \mathbb{P}$, pak G je cyklická

dk: $a \in G, a \neq e$, musí mít řád $|a| = |G| \Rightarrow G = \langle a \rangle$

Def: Počet prvků v množině G/H resp. $H \backslash G$
se nazývá index podgrupy H v grupě G .

Věta (malá Fermatova):

Nechť $p \in \mathbb{P}$, $a \in \mathbb{N}$, $a \not\equiv 0 \pmod{p}$. Pak $a^{p-1} \equiv 1 \pmod{p}$.

dk: důsledek Lagrangeovy věty:

$G = (\mathbb{Z}_p^*, \cdot \pmod{p})$ má podgrupu $\langle a \rangle \neq \{e\}$.

Proto $\underbrace{|a|}_r = |\langle a \rangle| \mid |G| = p-1$.

$$a^{p-1} = (a^r)^{\frac{p-1}{r}} = 1 \quad r \in \mathbb{Z}_p^*.$$

Věta (Eulerova):

Nechť $a, n \in \mathbb{N}$, $a \not\equiv 0 \pmod{n}$. Potom $a^{\varphi(n)} \equiv 1 \pmod{n}$.

dk: V grupě $\mathbb{Z}_n^* = (\{1 \leq k \leq n \mid k \not\equiv 0 \pmod{n}\}, \cdot \pmod{n})$

řád prvku a opět: $r = |a| \mid |\mathbb{Z}_n^*| = \varphi(n)$.

$$a^{\varphi(n)} = (a^r)^{\frac{\varphi(n)}{r}} = 1 \quad r \in \mathbb{Z}_n^*.$$

Poznámka:

Normální podgrupy

32

Chceme, aby faktorprostor G/H , resp. $H \backslash G$ byla také grupa, tj. třídy $\sim_L$, resp. $\sim_R$ aby splňovaly $(aH)(bH) = (ab)H$

a nezáviselo to na výběru a, b (j. reprezentanta)

Podmínka se dá zapsat: $\forall a, b, c, d \in G$

$$\left. \begin{matrix} a \sim c \\ b \sim d \end{matrix} \right\} \Rightarrow ab \sim cd.$$

Def: Ekvivalence na groupoidu (v našem případě grupě) G splňující podmínku $(*)$ se nazývá kongruence na G .

Tvrzení: Necht G je grupa, $\equiv$ je na ní def. kongruence.

Pak $G/\equiv$ vybavený operací $[a]_{\equiv} \cdot [b]_{\equiv} = [ab]_{\equiv}$ je

faktorprostor grupa.

Jestli G abelova, $G/\equiv$ je abelova

Def: $G/\equiv$ nazýváme faktorgrupa grupy G podle $\equiv$.

dl: Operace je dobře def. a samozřejmě asociativní:

$$[a][b][c] = [ab][c] = [ab]c = [a][bc] = [a][b][c].$$

- neut. prvek $[e]$, protože $[a] = [ae] = [a][e]$ ok.
 $= [ea] = [e][a]$

- inverzní prvek: $[a]^{-1} = [a^{-1}]$, tj. $([a])^{-1} = [a]$.

- komutace $[a][b] = [ab] = [ba] = [b][a]$ ok.

Př: $\forall (\mathbb{Z}, +)$ je kongruence $\equiv_m \bmod m$ pro $m \in \mathbb{N}$ (odtud jméno!)

$$\mathbb{Z}/\equiv_m = \mathbb{Z}_m. \text{ Promyslet, že } \mathbb{Z}/\equiv_m = \mathbb{Z}/_m \mathbb{Z}.$$

$$a \equiv b \bmod m \quad a - b \in m\mathbb{Z}$$

Pozn. Chceme, aby G/H i $H \backslash G$ byly grupy,
 tj. aby $\sim_L, \sim_R$ byly kongruence.

Def. Podgrupa H grupy G je normální, pokud
 splývá s levo a pravo faktorprostor G podle H .
 Značíme $H \triangleleft G$.

Platí: H je normální $\Leftrightarrow \forall a \in G: aH = Ha$
 $[a]_L = [a]_R$

Pozor! ne nutně $ah = ha \ \forall h$!

Lemem:

- $G \triangleleft G, \{e\} \triangleleft G$
- Libovolná podgrupa abelské grupy je normální.

Věta: Faktorprostor $G/\equiv$, kde $\equiv$ je ekvivalence
 je faktorprostorem dle kongruence, právě když
 je faktorprostorem dle normální podgrupy grupy G .

důl: $\Rightarrow$ Necht $\equiv$ je kongruence. Dokažeme, že $[e] \triangleleft G$.

$$G/\equiv = \{[a] \mid a \in G\}$$

$\forall a, b \in [e]$ tj. $a \equiv e$ i $b \equiv e$ máme $a \equiv e, e = b^{-1}$,
 proto $ab^{-1} \equiv e$, tj. $ab^{-1} \in [e]$. ok.

$$\begin{aligned} \text{Přitom } x \in [a] &\Leftrightarrow x \equiv a \Leftrightarrow a^{-1}x \equiv e \Leftrightarrow x \sim a \Leftrightarrow x \in aH \\ &\Leftrightarrow x a^{-1} \equiv e \Leftrightarrow x \sim a \Leftrightarrow x \in Ha \end{aligned}$$

Proto $[a] = aH = Ha$ tj. $H = [e] \triangleleft G$.

$\Leftarrow$ Necht H je normální, čili $\sim_R = \sim_L = \equiv$ kongruence.

$a \sim b \Rightarrow a^{-1}b \in H$
 $c \sim d \Rightarrow c^{-1}d \in H$
 $\Rightarrow ac(bd)^{-1} = acd^{-1}b^{-1} = a \underset{\in H}{\tilde{c}} \underset{\in H}{\tilde{d}^{-1}} b^{-1} = a \underset{\in H}{\tilde{c}} \underset{\in H}{\tilde{d}^{-1}} \underset{\in H}{b^{-1}} \in H$ ok
 čili $ac \sim bd$ tj. $(ac)(bd)^{-1} \in H$
 $\uparrow$
 $ah = ha$
 $\times$ normality

Pozn: Vlastnost $aH = Ha$ nede na $aH\bar{a}^{-1} = H$.

34

Věta: Necht' G je grupa. Pro $a \in G$ položíme

$$\alpha_a: G \rightarrow G: \alpha_a(x) = ax\bar{a}^{-1}$$

$$\text{tj. } \alpha_a = L_a \circ R_{\bar{a}^{-1}}$$

Potom α_a je automorfismus, tj. $\alpha_a \in \text{Aut}(G)$

a zobrazení $\alpha: G \rightarrow \text{Aut}(G): \alpha(a) = \alpha_a$ je homomorfismus.

Def: Automorfismus α_a pro $a \in G$ se nazývá
vnitřní automorfismus grupy G

$$\text{Množina } \{\varphi \in \text{Aut}(G) \mid \exists a \in G: \varphi = \alpha_a\} = \text{Inn}(G)$$

je podgrupa $\text{Aut}(G)$ vnitřních automorfismů.

Pozn: (Plyne z toho, že $\text{Inn}(G) = \alpha(G) \stackrel{\text{Im } \alpha}{=} \text{obraz homomorfismu}$).

Pozn: • Libovolná abelská grupa má jediný (identický) vnitřní automorfismus $\rightarrow$ všechny podgrupy normální.

• Existují grupy, které nemají vnější automorf.
(např. S_3)

dk: Uvědomme si, že $\forall x, y \in G$ je $L_x \circ R_y = R_y \circ L_x$.

Postupně:

$$1) \alpha_e = 1_G$$

$$2) \alpha_a \circ \alpha_b = \alpha_{ab} \quad \forall a, b \in G, \text{ protože}$$

$$\alpha_a \alpha_b = L_a R_{\bar{a}^{-1}} L_b R_{\bar{b}^{-1}} = L_a L_b R_{\bar{a}^{-1}} R_{\bar{b}^{-1}} = L_{ab} R_{\bar{b}^{-1} \bar{a}^{-1}} = L_{ab} R_{(\bar{ab})^{-1}} = \alpha_{ab}$$

$$3) \text{ z 1 a 2 plyne } \alpha_a \alpha_{\bar{a}^{-1}} = \alpha_{a\bar{a}^{-1}} = \alpha_e = 1_G = \alpha_{\bar{a}^{-1}a} = \alpha_{\bar{a}^{-1}} \alpha_a,$$

tj. $(\alpha_a)^{-1} = \alpha_{\bar{a}^{-1}}$, tzn. α_a je bijekce

$$4) \alpha_a(xy) = axy\bar{a}^{-1} = ax\bar{a}^{-1}ay\bar{a}^{-1} = \alpha_a(x) \alpha_a(y)$$

tj. α_a je automorfismus.

5) Podle 2 je zobrazení $\alpha: G \rightarrow \text{Aut}(G)$ homomorfismus.

Věta: Podgrupa H grupy G je normální, právě když je uzavřena vůči všem vnitřním automorfizmům grupy G .

dk: $\Rightarrow$: K prvků $a \in G$ vezmu α_a .

Pak $\forall x \in H$ je $\alpha_a(x) = \underbrace{axa^{-1}}_{\in aH = Ha} = ha\bar{a}^{-1} = h \in H$.

$\Leftarrow$: chcí $aH = Ha$.

Vezmu $x \in aH$, tj. $x = ah = ah\bar{a}^{-1}a = \underbrace{\alpha_a(h)}_{=h \in H} a \in Ha$

$\Rightarrow aH \subset Ha$. Stejně naopak.

Lemma: Necht G je grupa. Pak $\text{Inn}(G) \triangleleft \text{Aut}(G)$.

dk: Ukažeme, že $\text{Inn}(G)$ je uzavřena vůči vnitřním automorfizmům grupy $\text{Aut}(G)$.

Tj. $\forall \varphi \in \text{Aut}(G), \forall a \in G$ chceme $\varphi \circ \alpha_a \circ \varphi^{-1} \in \text{Inn}(G)$.

To platí, protože

$$\begin{aligned} (\varphi \circ \alpha_a \circ \varphi^{-1})(x) &= \varphi(a \varphi^{-1}(x) \bar{a}^{-1}) = \varphi(a) x (\varphi(a))^{-1} = \\ &= \alpha_{\varphi(a)}(x) \quad \text{ok.} \end{aligned}$$

Def: Faktorgrupa $\text{Aut}(G) / \text{Inn}(G) =: \text{Out}(G)$

se nazývá grupa vnějších automorfizmů grupy G .

Věta: Podgrupa H grupy G je normální,
právě když je jádrem nějakého
homomorfismu $\varphi: G \rightarrow K$, kde K je grupa.

dk: $\Leftarrow$ Necht' $\varphi: G \rightarrow K$ je homomorfismus.

Ukažme, že $\text{Ker } \varphi \trianglelefteq G$, tj. chceme

$$\forall a \in G, \forall x \in \text{Ker } \varphi: \alpha_a(x) \in \text{Ker } \varphi.$$

$$\varphi(\alpha_a(x)) = \varphi(axa^{-1}) = \varphi(a) \underbrace{\varphi(x)}_{=e_K} \varphi(a^{-1}) = \varphi(a)(\varphi(a))^{-1} = e_K$$

$$\Rightarrow \alpha_a(x) \in \text{Ker } \varphi.$$

$\Rightarrow$ Projekce $\pi: G \rightarrow G/H$ je homomorfismus
(protože $[ab] = [a][b]$), přičemž $\text{Ker } \pi = H$.

Platí: Je-li $H \trianglelefteq G$, $N \trianglelefteq G$ a $H \subset N$, pak $H \trianglelefteq N$.

dk: H uzavřena vůči automorfismům
 α_a pro $a \in G$, takže i vůči α_a pro $a \in N$.

Lemma: Je-li $\varphi: G \rightarrow \tilde{G}$ homomorfismus grup
a $H \trianglelefteq G$ taková, že $H \subset \text{Ker } \varphi$, pak zobrazení

$$\tilde{\varphi}: G/H \rightarrow \tilde{G}: [a] \rightarrow \varphi(a)$$

je dobře definováno, je to homomorfismus

$$\text{a platí } \text{Im } \tilde{\varphi} = \text{Im } \varphi$$

$$\text{Ker } \tilde{\varphi} = \text{Ker } \varphi / H := \{ [a] \mid a \in \text{Ker } \varphi \}$$

Pozn: Zřejmě $H \trianglelefteq \text{Ker } \varphi$, takže má smysl.

Věta: Podgrupa H grupy G je normální,
právě když je jádrem nějakého
homomorfismu $\varphi: G \rightarrow K$, kde K je grupa.

dk: $\Leftarrow$ Necht' $\varphi: G \rightarrow K$ je homomorfismus.

Ukažme, že $\text{Ker } \varphi \trianglelefteq G$, tj. chceme

$$\forall a \in G, \forall x \in \text{Ker } \varphi: \alpha_a(x) \in \text{Ker } \varphi.$$

$$\varphi(\alpha_a(x)) = \varphi(axa^{-1}) = \varphi(a) \underbrace{\varphi(x)}_{=e_K} \varphi(a^{-1}) = \varphi(a)(\varphi(a))^{-1} = e_K$$

$$\Rightarrow \alpha_a(x) \in \text{Ker } \varphi.$$

$\Rightarrow$ Projekce $\pi: G \rightarrow G/H$ je homomorfismus
(protože $[ab] = [a][b]$), přičemž $\text{Ker } \pi = H$.

Platí: Je-li $H \trianglelefteq G$, $N \trianglelefteq G$ a $H \subset N$, pak $H \trianglelefteq N$.

dk: H uzavřena vůči automorfismům
 α_a pro $a \in G$, takže i vůči α_a pro $a \in N$.

Lemma: Je-li $\varphi: G \rightarrow \tilde{G}$ homomorfismus grup
a $H \trianglelefteq G$ taková, že $H \subset \text{Ker } \varphi$, pak zobrazení

$$\tilde{\varphi}: G/H \rightarrow \tilde{G}: [a] \rightarrow \varphi(a)$$

je dobře definováno, je to homomorfismus

$$\text{a platí } \text{Im } \tilde{\varphi} = \text{Im } \varphi$$

$$\text{Ker } \tilde{\varphi} = \text{Ker } \varphi / H := \{ [a] \mid a \in \text{Ker } \varphi \}$$

Pozn: Zřejmě $H \trianglelefteq \text{Ker } \varphi$, takže má smysl.

dk: • Je $\tilde{\varphi}$ dobře def.?

Pro $a, b \in G$, $a \sim b$, čili $\varphi(a) = \varphi(b) \cdot \underbrace{h \in H}_{\text{Ker } \varphi}$

$$a \sim b \Rightarrow \exists h \in H: a = bh \Rightarrow \varphi(a) = \varphi(b) \varphi(h) = \varphi(b) e_G = \varphi(b) \text{ ok.}$$

• Odtud $\tilde{\varphi}([a]) = \varphi(a) = \varphi(b)$ nezávisí na volbě reprezentanta třídy.

• Je $\tilde{\varphi}$ homomorfismus?

$$\tilde{\varphi}([a][b]) = \tilde{\varphi}([ab]) = \varphi(ab) = \varphi(a)\varphi(b) = \tilde{\varphi}([a])\tilde{\varphi}([b]) \text{ ok}$$

• $\text{Im } \varphi = \text{Im } \tilde{\varphi}$ zřejme k definici $\tilde{\varphi}$.

• Co je $\text{Ker } \tilde{\varphi}$?

$$\text{Pro } a \in G \text{ je } [a] \in \text{Ker } \tilde{\varphi} \Leftrightarrow \tilde{\varphi}([a]) = \varphi(a) = e_G \Leftrightarrow a \in \text{Ker } \varphi$$

$$\text{tj. } \text{Ker } \tilde{\varphi} = \{ [a] \mid a \in \text{Ker } \varphi \} = \text{Ker } \varphi / H$$

tj. můžeme rozkladu G/H na $\text{Ker } \varphi / H$.

Věta: (1. věta o izomorfismu): Necht' $G, \tilde{G}$ jsou grupy a $\varphi: G \rightarrow \tilde{G}$ homomorfismus.

$$\text{Pak } \varphi(G) = \text{Im } \varphi \cong G / \text{Ker } \varphi.$$

dk: Do lemmatu položíme $H = \text{Ker } \varphi$.

Zobrazení $\tilde{\varphi}: G / \text{Ker } \varphi \rightarrow \varphi(G) \subset \tilde{G}$ je homomorfismus.

Navíc je prostý, protože $\text{Ker } \tilde{\varphi} = \text{Ker } \varphi / \text{Ker } \varphi = \{e\}$.

a je surjektivní na $\text{Im } \varphi = \varphi(G)$.

Je to tedy izomorfismus $G / \text{Ker } \varphi$ a $\text{Im } \varphi$.

První:

$$\begin{array}{ccc}
 G & \xrightarrow{\varphi} & \tilde{G} \\
 \text{projekce } \pi \downarrow & \nearrow \tilde{\varphi} & \\
 G/H & &
 \end{array}
 \quad \varphi = \tilde{\varphi} \circ \pi$$

První: $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_n: k \rightarrow k \bmod n$
 $\text{Ker } \varphi = n\mathbb{Z}$. Proto $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$

První: $G = (\mathbb{R}^*, \cdot)$, $\tilde{G} = (\mathbb{R}^+, \cdot)$
 $\varphi: G \rightarrow \tilde{G}: x \rightarrow |x|$
 je homomorfismus: $\varphi(xy) = |xy| = |x| \cdot |y| = \varphi(x)\varphi(y)$
 je epimorfismus ($\text{Im } \varphi = \mathbb{R}^+$).
 $\text{Ker } \varphi = \{\pm 1\}$
 $\mathbb{Z} \text{ 1.VOI } \mathbb{R}^+ \cong \mathbb{R}^*/\{\pm 1\}$

První: $G = (\mathbb{R}, +)$, $\tilde{G} = (\mathbb{C}_1, \cdot)$ $\xleftarrow{\text{jednotková kružnice v } \mathbb{C}}$
 $\varphi(x) = e^{2\pi i x}$
 $\text{Ker } \varphi = \mathbb{Z}$, $\text{Im } \varphi = \mathbb{C}_1$.
 $\mathbb{Z} \text{ 1.VOI } \mathbb{C} \cong \mathbb{R}/\mathbb{Z} \text{ Aorus. } , \quad \mathbb{Z} \triangleleft \mathbb{R}$

První: $G = GL(n, \mathbb{R})$, $\tilde{G} = (\mathbb{R}^*, \cdot)$
 $\varphi = \det$, $\text{Ker } \varphi = SL(n, \mathbb{R})$
 $\mathbb{Z} \text{ 1.VOI } GL(n, \mathbb{R})/SL(n, \mathbb{R}) \cong \mathbb{R}^*$,

$$SL(n, \mathbb{R}) \triangleleft GL(n, \mathbb{R})$$

Věta (2. věta o izomorfismu):

Nechť G je grupa, $H, K \trianglelefteq G$ takové, že $H \subset K$.
Potom $H \trianglelefteq K$, $K/H \trianglelefteq G/H$ a platí:

$$\frac{(G/H)}{(K/H)} \cong G/K.$$

dk: • Větu lze $H \trianglelefteq K$ přejmout z uzavřenosti na násobení aut.

• Ukažme $K/H \trianglelefteq G/H$. Vezmeme projekci

$$\pi: G \rightarrow G/K: a \rightarrow [a]$$

$H \subset K = \text{Ker } \pi$, do lemmatu položíme

$$\varphi = \pi, G = G, \tilde{G} = G/K, H = H.$$

Z lemmatu: $\text{Ker } \pi/H = K/H = \text{Ker } \tilde{\pi}$, kde

$$\tilde{\pi}: G/H \rightarrow G/K: gH \rightarrow \pi(g) = [g]$$

je homomorfismus.

Jádro každého homomorfismu, tj. i $\text{Ker } \tilde{\pi} = K/H$ je podgrupa.

• Z lemmatu dále $\text{Im } \tilde{\pi} = \text{Im } \pi = G/K$.

Z 1. VOI na $\tilde{\pi}$: $\text{Im } \tilde{\pi} \cong (G/H)/\text{Ker } \tilde{\pi}$

$$\cong \frac{(G/H)}{(K/H)}.$$

Př: Zjistíme počet tříd rozkladu
 $n\mathbb{Z}/m\mathbb{Z}$ pro $n, m \in \mathbb{N}$ takové, že $n|m$.

Postup: Pro $n|m$ je $m\mathbb{Z}$ podgrupa $n\mathbb{Z}$ a
 je určitě normální, z abelovskosti.

Do 2.VOI zvolíme: $G = \mathbb{Z}$, $K = n\mathbb{Z}$, $H = m\mathbb{Z}$. Pak

$$(\mathbb{Z}/m\mathbb{Z}) / (n\mathbb{Z}/m\mathbb{Z}) \simeq \mathbb{Z}/n\mathbb{Z}$$

z Lagrangeovy věty:

$$|n\mathbb{Z}/m\mathbb{Z}| = \frac{|\mathbb{Z}/m\mathbb{Z}|}{|(n\mathbb{Z}/m\mathbb{Z})|} = \frac{|\mathbb{Z}_m|}{|\mathbb{Z}/n\mathbb{Z}|} = \frac{|\mathbb{Z}_m|}{|\mathbb{Z}_n|} = \frac{m}{n}.$$

40

Tvrzení: Necht G je grupa, $H \triangleleft G$, $K \subset G$ libv. podgrupa.
 Potom $HK = KH$ je podgrupa grupy G .

dl: Protože $H \triangleleft G$, je $Ha = aH \quad \forall a \in G$, tj.

$$HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH \quad \checkmark$$

• Neuvěnost na operace:

• $e \in HK$ ok

• $h \in H, k \in K : (hk)^{-1} = k^{-1}h^{-1} \in KH = HK$ ok.

• $h_1, h_2 \in H, k_1, k_2 \in K : (h_1 k_1)(h_2 k_2) = h_1 \underbrace{(k_1 h_2)}_{\substack{h_3 \in H \\ k_3 \in K}} k_2 \in HK$ ok.

Věta: (3. věta o izomorfismu):

Necht G je grupa, $H \triangleleft G$, $K \subset G$ libv. podgrupa.

Potom $H_n K \triangleleft K$ a platí $HK/H \cong K/H_n K$

Př: Aplikujme na $G = \mathbb{Z}$. Položíme $H = a\mathbb{Z}$, $K = b\mathbb{Z}$.

Potom $H_n K = \text{lcm}(a, b)\mathbb{Z}$, H/K (symmetrie, je aditivní, takže $H+K$)
 $\text{"gcd}(a, b)\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$

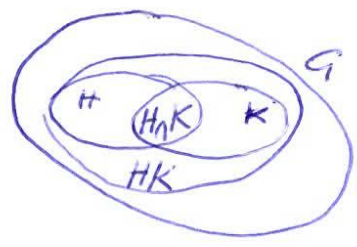
Proto máme $\text{gcd}(a, b)\mathbb{Z} / a\mathbb{Z} \cong b\mathbb{Z} / \text{lcm}(a, b)\mathbb{Z}$

Použijme, že $|\mathbb{Z}/m\mathbb{Z}| = \frac{n}{m}$, proto $\left(\frac{\text{gcd}(a, b)}{a}\right)^{-1} = \left(\frac{b}{\text{lcm}(a, b)}\right)^{-1}$

Aj. známé: $a \cdot b = \text{gcd}(a, b) \text{lcm}(a, b)$

dlí: HK je podgrupa G
 $H \cap K$ je podgrupa K , normalita vyplývá.

Zavedeme homomorfismus φ , na který aplikujeme 1. větu o izomorfismu



$$\varphi: K \longrightarrow G/H \xrightarrow{1.\text{VOT}} \frac{K/\text{Ker } \varphi}{H \cap K} \simeq \frac{\text{Im } \varphi}{HK/H}$$

Jak zavedeme? φ je důležitá projekce $\pi: G \rightarrow G/H$ na K .

Ověřme:

• $\text{Im } \varphi = HK/H$: z definice $\text{Im } \varphi = \{[k]_H / k \in K\} = \{kH / k \in K\}$.
 Ale $HK/H = \{k \cdot \underbrace{h}_H / k \in K, h \in H\} = \{kH / k \in K\}$.

• $\text{Ker } \varphi = H \cap K$: Pro $k \in K$ platí $\varphi(k) = e_{G/H} = [e] = H \iff k \in H$
 tj. $k \in \text{Ker } \varphi \iff k \in H \cap K$. důkaz.

Akce grupy na množině

41

Def: Necht G je grupa, X množina. Zobrazení

$$G \times X \rightarrow X :$$

$$(g, x) \mapsto gx$$

se nazývá akce grupy G na množině X , pokud

1) $\forall x \in X$ platí $ex = x$

2) $\forall a, b \in G \quad \forall x \in X \quad a.(b.x) = (ab).x$

Pozn: Značení. zatím jen symbol, zatím na konkrétních příkladech.

Př: $G = S_n$, $X = \{1, 2, \dots, n\}$, $g.x = g(x)$. Je to akce: $e.x = \text{id}(x) = x$
 $\sigma(\pi(x)) = (\sigma \circ \pi)x$

Def: Necht G je akce G na množině X

Pevný bod proku $g \in G$ je takové $x \in X$, že $g.x = x$.

Stabilizátor proku $x \in X$ je množina proků $g \in G$ taková, že x je jejich pevným bodem

$$G_x = \{g \in G \mid g.x = x\}$$

Orbita proku $x \in X$ při G je množina $y \in X$ tak, že $g.x = y$ pro nějaké $g \in G$.

$$O_x := G.x = \{g.x \mid g \in G\}$$

Platí: G_x je podgrupa grupy G .

dle: • $e \in G_x$ triv

• $a, b \in G_x \implies a^{-1}b \in G_x$

$$\begin{aligned} (a^{-1}b).x &= a^{-1}(b.x) = a^{-1}.x = a^{-1}(a.x) = \\ &= (a^{-1}a).x = e.x = x \quad \text{OK.} \end{aligned}$$

Příklady akce grupy:

4,5

Př: $(\mathbb{R}^n, +)$ má akci na $\mathbb{R}^n$ translace:

Pro $\vec{r} \in \mathbb{R}^n$ je $T_{\vec{r}}: \mathbb{R}^n \rightarrow \mathbb{R}^n: T_{\vec{r}}(\vec{w}) = \vec{w} + \vec{r} \quad \forall \vec{w} \in \mathbb{R}^n$.

Potřebujeme ověřit 1) $T_{\vec{0}}(\vec{w}) = \vec{w} + \vec{0} = \vec{w} \quad \checkmark$

$$\begin{aligned} 2) T_{\vec{r}}(T_{\vec{u}}(\vec{w})) &= (\vec{w} + \vec{u}) + \vec{r} = \\ &= \vec{w} + (\vec{u} + \vec{r}) = T_{\vec{u} + \vec{r}}(\vec{w}) \quad \checkmark \end{aligned}$$

Pro $\vec{w} \in \mathbb{R}^n$ je $\mathcal{O}_{\vec{w}} = \{\vec{w} + \vec{r} \mid \vec{r} \in \mathbb{R}^n\} = \mathbb{R}^n$
 $\mathcal{G}_{\vec{w}} = \{\vec{r} \mid \vec{w} + \vec{r} = \vec{w}\} = \{\vec{0}\}$.

Př: Grupa $GL(n, \mathbb{R})$ má akci na $\mathbb{R}^n$:

$A \cdot \vec{r} = A\vec{r}$.. násobení vektoru maticí

Ověřme 1) $I_n \vec{r} = \vec{r} \quad \checkmark$

$$2) A(B\vec{r}) = (AB)\vec{r} \quad \checkmark$$

Pro $\vec{0}$ je $\mathcal{O}_{\vec{0}} = \{A\vec{0} \mid A \in GL(n, \mathbb{R})\} = \{\vec{0}\}$.

$$\mathcal{G}_{\vec{0}} = \{A \in GL(n, \mathbb{R}) \mid A\vec{0} = \vec{0}\} = GL(n, \mathbb{R}).$$

Pro $\vec{r} \neq \vec{0}$ je $\mathcal{O}_{\vec{r}} = \{A\vec{r} \mid A \in GL(n, \mathbb{R})\}$
 $\mathcal{G}_{\vec{r}} = \{A \in GL(n, \mathbb{R}) \mid A\vec{r} = \vec{r}\}$

Pr: Akce grupy G sama na sobě: $X = g$ 41,75

i) $g \cdot x = gx = L_g x \quad \forall x \in G$

ii) $g \cdot x = xg^{-1} = R_{g^{-1}} x \quad \forall x \in G$

iii) $g \cdot x = gxg^{-1} \quad \forall x \in G$ konjugace

ověření: $g_1 \cdot (g_2 \cdot x) = g_1 \cdot (g_2 x g_2^{-1}) =$
 $= g_1 g_2 x g_2^{-1} g_1^{-1} = (g_1 g_2) x (g_1 g_2)^{-1} =$
 $= (g_1 g_2) \cdot x \quad \checkmark$

samočřejmě také $e \cdot x = ex e^{-1} = x \quad \checkmark$

V bodě i) $\forall x \in G \quad \sigma_x = \{gx \mid g \in G\} = G$

protože $\forall x \in G$ je $x = (xx^{-1})x$

$$G_x = \{g \in G \mid gx = x\} = \{e\}$$

Stejně v bodě ii)

Pro iii) $\forall x \in G \quad \sigma_x = \{gxg^{-1} \mid g \in G\}$ všude konjugace
prvků x

$$G_x = \{g \in G \mid gxg^{-1} = x\} =$$

$$= \{g \in G \mid gx = xg\}$$

centralizátor
prvků x

Věta: Necht G je grupa, $x \in X$. Pak je-li G konečné, 142
platí: $|O_x| = \frac{|G|}{|G_x|}$.

dh: Protože G_x je podgrupa, lze G/G_x .

Vzimeš $f: G/G_x \rightarrow O_x$:
pro každé $x \in X$
 $[g]_{G_x} \mapsto g \cdot x$

Ověřme vlastnosti f :

- f je dobře definované, tj. $f([g])$ nezávisí na volbě reprezentanta g třídy ekvivalence:

$$g_1 \sim g_2 \Leftrightarrow \exists h \in G_x \text{ tak, že } g_2 = g_1 h \Rightarrow \\ \Rightarrow g_2 \cdot x = g_1 h \cdot x = g_1 (h \cdot x) = g_1 x$$

- f je surjektivní - přímo z def.

- f je prostý:

$$f([g_1]) = f([g_2]) \Leftrightarrow g_1 x = g_2 x \Rightarrow g_1^{-1} g_2 x = g_1^{-1} (g_2 x) = \\ = g_1^{-1} (g_1 x) = (g_1^{-1} g_1) x = x$$

$$\Rightarrow g_1^{-1} g_2 = h \in G_x \Rightarrow g_1 \sim g_2 \Rightarrow [g_1] = [g_2]$$

Zobrazení f je tedy bijekce konečných množin,

proto $|O_x| = |G/G_x|$. Výsledek plyne

z Lagrangeovy věty, protože $|G/G_x| = \frac{|G|}{|G_x|}$.

Př: Grupa $D_3 = \{ \overset{\text{rotace}}{\underset{\text{id}}{k_0}}, \overset{\text{rotace}}{k_1}, \overset{\text{rotace}}{k_2}, \overset{\text{zrcadlení}}{s_0}, \overset{\text{zrcadlení}}{s_1}, \overset{\text{zrcadlení}}{s_2} \}$

Pozn: nejmenší neabelovská grupa

$$k_0 = \text{id}, k_1 \text{ rotace o } \frac{2\pi}{3}, k_2 \text{ rotace o } \frac{4\pi}{3} \rightarrow k_i^3 = \text{id}$$

$$k_i^2 = \text{id. zrcadlení}$$

nema' element řádu 6, není cyklická
je generována $D_3 = \langle k_1, k_0 k_1 \rangle$

Akce na $X = \mathbb{R}^2$:

- Bod x může mít ka stabilizátor nějakou podgrupu grupy D_3

- Podgrupy D_3 : $\{k_0, k_1, k_2\} \cong \mathbb{Z}_3$

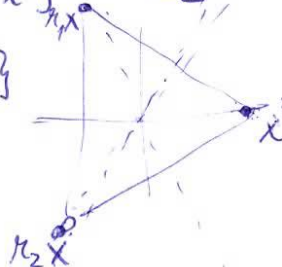
$$\{k_0, k_i\} \cong \mathbb{Z}_2$$

→ Vezmeme x stabilizované $\{k_0, k_1\}$
jeho orbita σ_x :

$$k_1 x = k_3 x$$

$$k_2 x = k_2 x$$

} → Pravo. Δ



$$|\sigma_x| = 3 = \frac{|G|}{|G_x|} = \frac{6}{2}$$

→ Vezmeme x stabilizované $\{k_0, k_1, k_2\}$
→ neexistuje

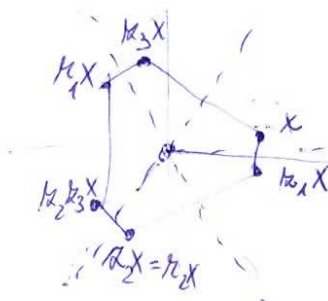
Pozor! Nemusí být každá podgrupa stabilizátorem.

→ Vezmeme x stabilizované celým G
 $x = 0$

$$|\sigma_x| = 1 = \frac{|G|}{|G|} = \frac{6}{6}$$

→ Vezmeme x stabilizované jen $\{\text{id}\}$

$$|\sigma_x| = 6 = \frac{|G|}{|e|} = \frac{6}{1}$$



Věta: Uvažujme akci grupy G na množině X 44

Pak X je disjunktivním sjednocením různých orbit při této akci.

Speciálně, je-li X konečná a $x_1, \dots, x_s$ jsou reprezentanti různých orbit, pak

$$|X| = \sum_{i=1}^s |\sigma_{x_i}| = \sum_{i=1}^s \frac{|G|}{|G_{x_i}|}.$$

dk: Ukážeme, že orbity dvou prvků $x, y \in X$ jsou shodné nebo disjunktivní:

Předpokládejme $\sigma_x \cap \sigma_y \neq \emptyset$, tj.

$x = g_1 \cdot x = g_2 \cdot y$ pro nějaké $g_1, g_2 \in G$.

Dokážeme $\sigma_x \subset \sigma_y$:

$\forall u \in \sigma_x \exists g \in G : u = g \cdot x$, ale $x = g_1 \cdot y$
 $g_1^{-1} \cdot x = (g_1^{-1} g_1) \cdot y = y$

proto $u = g \cdot x = g \cdot (g_1^{-1} \cdot x) = (g g_1^{-1}) \cdot x = (g g_1^{-1}) \cdot (g_2 \cdot y) =$
 $= (g g_1^{-1} g_2) \cdot y \in \sigma_y.$

Ze symetrie $\sigma_y \subset \sigma_x$, tj. $\sigma_x = \sigma_y$.

Pro X konečnou proto $|X| = \sum_{i=1}^s |\sigma_{x_i}| = \sum_{i=1}^s \frac{|G|}{|G_{x_i}|}$
poslední rovnost je předchozí věty.

/45

Def: Centrum grupy G je množina

$$Z(G) = \{g \in G \mid \forall x \in G: gx = xg\}$$

Důsledek: Necht G má řád $|G| = p^k$,
kde p je prvočíslo, $k \in \mathbb{N}$. Pak
 $Z(G)$ je netriviální, tj. $Z(G) \neq \{e\}$.

dk: Použijeme akci G na sobě konjugací.

$$\text{Víme } |G| = \sum_{i=1}^k |\sigma_{x_i}|$$

" p^k

Jedna z orbit je jednoprotekova:

$$\sigma_e = \{g e g^{-1} \mid g \in G\} = \{e\}$$

Resty protů jednotlivých orbit jsou
jedině $1, p, p^2, \dots, p^k$, protože $|\sigma_x| \mid |G|$.

Ze vzorce $\uparrow$ musí být alespoň
 p jednoprotekových orbit.

Je-li $|\sigma_x| = 1$, tj. $\sigma_x = \{x\}$, tj. $g^{-1} x g = x \quad \forall g$
 $xg = gx \quad \forall g$

$$\Rightarrow x \in Z(G).$$

Důsledek: Má-li grupa G řád $|G| = p^2$,
je abelovská. Dk. na cv.

Věta: Necht $\sim$ je kongruence na grupě G .

Pak existuje normální podgrupa H grupy G
tak, že $G/H = G/\sim$.

dk: Označím $G/\sim = \{[a] \mid a \in G\}$.

Ukažeme, že $H = [e] \trianglelefteq G$ a že $\sim_H = \sim$.

• $H \neq \emptyset$, protože $e \in [e] = H$.

• Vezmeme $a, b \in H$, chci $ab^{-1} \in H$.

$$a \in H \Rightarrow a \equiv e$$

$$b \in H \Rightarrow b \equiv e \rightarrow \text{toto vynásobím } b^{-1} \Rightarrow b^{-1} \equiv e$$

(le, protože kongruence je reflexivní)

$$e \equiv bb^{-1} = b^{-1}$$

$$\text{Vynásobíme } a \equiv e \text{ a } b^{-1} \equiv e \Rightarrow ab^{-1} \equiv e \Rightarrow ab^{-1} \in H.$$

• Zkoumáme $\sim_H$.

$$\text{z definice } a \sim_H b \Leftrightarrow ab^{-1} \in H = [e] \Leftrightarrow ab^{-1} \equiv e$$

$\equiv$ je kongruence, le vynásobit $b \equiv b^{-1} \Rightarrow a \equiv b$

• Proto rozklad $G/H = G/\sim_H = G/\sim$,

$$\text{ale obdobně } G/H = G/\sim_H = G/\sim$$

Akce rozkladu stejné a podgrupa H
je normální.

Okrulky

1

Def: Okrulka R je množina vybavená dvěma binárními operacemi $+$, $\cdot$, unární operací $a \rightarrow -a$, a dvěma nulárními operacemi $0, 1 \in R$ taková, že:

1) $(R, +, -, 0)$ je abelovská grupa

2) $(R, \cdot, 1)$ je monoid

3) platí distributivní zákony:

$$\forall a, b, c \in R: a \cdot (b + c) = a \cdot b + a \cdot c$$

$$(a + b) \cdot c = a \cdot c + b \cdot c$$

Okrulka R je komutativní, je-li operace $\cdot$ komutativní.

Pozn: Často se v definici okruhu u 2) požaduje pouze pologrupa. Jestliže v ní existuje neutrální prvek, říká se, že je to okruh s jednotkou.

Pozn: Z pravidel počítání v grupě platí:

$$a) a + c = b + c \Rightarrow a = b$$

$$b) -(-a) = a$$

$$c) -(a + b) = -a + (-b).$$

Další pravidla pro počítání v okruhu:

Trvzení 1: Necht' R je okruh. Potom

$$1) \forall a \in R \text{ je } a \cdot 0 = 0 \cdot a = 0 \quad (0 \text{ je absorbujucí v } R)$$

$$2) \forall a, b \in R \text{ je } -(a \cdot b) = (-a) \cdot b = a \cdot (-b)$$

$$3) \forall m \in \mathbb{Z}, \forall a, b \in R \text{ je}$$

$$m \times (a \cdot b) = (m \times a) \cdot b = a \cdot (m \times b).$$

dk: ad1) $a \cdot 0 + 0 = a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$

krácením $a \cdot 0 = 0$.

Podobně klva.

$$\text{ad 2)} \quad a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0$$

$$\Rightarrow -(a \cdot b) = (-a) \cdot b$$

$$a \cdot b + a \cdot (-b) = a \cdot (b + (-b)) = a \cdot 0 = 0$$

$$\Rightarrow -(a \cdot b) = a \cdot (-b)$$

ad3) Provedeme indukci na $m \in \mathbb{N}_0$:

$$m=0 \quad 0 \times (a \cdot b) = 0 = 0 \cdot b = (0 \times a) \cdot b$$

$$m \rightarrow m+1 \quad (m+1) \times (a \cdot b) = m \times (a \cdot b) + a \cdot b \stackrel{\uparrow \text{IP}}{=} (m \times a) \cdot b + a \cdot b =$$

$$\stackrel{\uparrow \text{distr.}}{=} (m \times a + a) \cdot b = ((m+1) \times a) \cdot b$$

$$\text{Pro } m < 0: \quad m \times (a \cdot b) = (-m) \times (-a \cdot b) \stackrel{\uparrow}{=} (-m) \times ((-a) \cdot b) =$$

$$\stackrel{\uparrow \text{ad 2)}}{=} ((-m) \times (-a)) \cdot b \stackrel{\uparrow \text{ad 2)}}{=} (m \times a) \cdot b$$

Podobně pro $m \times (a \cdot b) = a \cdot (m \times b)$.

Pozn: Pokud $\alpha \in R$ platí $0=1$, pak $R=\{0\}$
 Ano. nulový okruh .

2,5

je totiž $\forall a \in R: a = a \cdot 1 = a \cdot 0 = 0$.

Příklady:

- 1) $\mathbb{Z}$ s běžnými operacemi
- 2) $\mathbb{Z}_m$ s operacemi $+ \bmod m, \cdot \bmod m$.
- 3) Každé těleso T je okruh, např. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. (viz LAL)
- 4) Je-li R okruh a $n \in \mathbb{N}$, pak $R^{n \times n}$ s maticovým sčítáním a násobením je okruh.
- 5) Je-li G abelovská grupa, pak $\text{End}(G)$, tj. množina všech endomorfismů na G , je okruh, přičemž 0 je nulové zobrazení $0(g) = e \quad \forall g \in G$
 1 je identické zobrazení $1(g) = g \quad \forall g \in G$
operace $+$ je po prvích $(f+g)(a) := f(a) + g(a)$
 $\uparrow$ nové $\uparrow$ grupová $\in G$
kavedeno
operace $\cdot$ je skládání zobrazení $(f \cdot g)(a) = (f \circ g)(a)$.
Ověřte, že to je okruh! $(f+g, f \cdot g \in \text{End}(G),$
platí axiomy okruhu)
- 6) R okruh, $X \neq \emptyset$ množina. Pak R^X (množina
 $f: X \rightarrow R$ je okruh s operacemi $0(x) = 0; 1(x) = 1$
 $(f+g)(x) := f(x) + g(x); (f \cdot g)(x) := f(x) \cdot g(x)$,
 $\nwarrow \nearrow$
operace $\in R$.

Okruh polynomů

13

Def: Necht R je komutativní okruh,
značíme x formální proměnnou.

Okruh polynomů nad R v proměnné x
je komutativní okruh

$$R[x] := \left\{ \sum_{k=0}^n f_k x^k \mid n \in \mathbb{N}_0, f_k \in R \text{ pro } k=0, \dots, n \right\},$$

přičemž operace jsou standardní:

$$\sum f_k x^k + \sum g_k x^k := \sum (f_k + g_k) x^k$$

$$\left(\sum f_k x^k \right) \cdot \left(\sum g_k x^k \right) := \sum h_k x^k,$$

$$\text{kde } h_k = \sum f_i g_{k-i}.$$

Pozn: Operace lze vyvodit pomocí distrib. zákonů
a těchto: $\forall a, b \in R, \forall k, l \in \mathbb{N}_0$:

$$a \cdot x^k + b \cdot x^k = (a+b) x^k$$

$$0 \cdot x^k = 0$$

$$(a x^k) \cdot (b x^l) = (a \cdot b) \cdot x^{k+l}$$

$$x^0 = 1$$

Pozn: Platí $R \subset R[x]$, protože $a = a \cdot 1 = a \cdot x^0 \in R[x]$ $\forall a \in R$.
 $0, 1$ jsou nulový, resp. jednotkový prvek v $R[x]$.

Def: Stupeň polynomu $f = \sum_{k=0}^n f_k x^k$, $f_n \neq 0$,
je roven $\deg f := n \in \mathbb{N}_0$.

Stupeň nulového polynomu $\deg 0 := -1$.

Pozn: x je formální proměnná, tedy ne $x \in \mathbb{R}$ ani $x \in \mathbb{C}$. 4

Polynomiální funkce $f: \mathbb{R} \rightarrow \mathbb{R}$
 $x \rightarrow f(x)$

nemí nutně se vzájemně jednoznačně vztahují
a polynomech.

(Dva různé polynomy odpovídají někdy
stejně funkci – uvidíme později).

Okrus formálních mocninových řad

Def: Necht R je komutativní okrus, x form. proměnná

Označme

$$R[[x]] := \left\{ \sum_{k=0}^{\infty} f_k x^k \mid f_k \in R, k \in \mathbb{N}_0 \right\},$$

přičemž operace provádíme:

$$\sum_{k=0}^{\infty} f_k x^k + \sum_{k=0}^{\infty} g_k x^k := \sum_{k=0}^{\infty} (f_k + g_k) x^k$$

$$\sum_{k=0}^{\infty} f_k x^k \cdot \sum_{k=0}^{\infty} g_k x^k := \sum_{k=0}^{\infty} \left(\sum_{i=0}^{\infty} f_i g_{k-i} \right) x^k = \sum_{k=0}^{\infty} \left(\sum_{i+j=k} f_i g_j \right) x^k$$

Platí: $R[[x]]$ s operacemi $+$, $\cdot$ je okrus.

•) asociativita: $+$ a $\cdot$ je ověřeno

$$\begin{aligned} \sum_{k=0}^{\infty} f_k x^k \cdot \left(\sum_{k=0}^{\infty} g_k x^k \cdot \sum_{k=0}^{\infty} h_k x^k \right) &= \left(\sum_{k=0}^{\infty} f_k x^k \cdot \sum_{k=0}^{\infty} g_k x^k \right) \cdot \sum_{k=0}^{\infty} h_k x^k \\ &\quad \parallel \parallel \\ &= \sum_{k=0}^{\infty} \left(\sum_{i+j+l=k} f_i g_j h_l \right) x^k \end{aligned}$$

•) distributivita přímochaře

-) $0 \in R[x]$ je $\sum_{k=0}^{\infty} f_k x^k$ kde $f_k = 0 \ \forall k \in \mathbb{N}_0$ 5
-) $1 \in R[x]$ je $\sum_{k=0}^{\infty} f_k x^k$ kde $f_0 = 1, f_k = 0 \ \forall k \in \mathbb{N}$.

Pozn: Ztotožňujeme:

$$R[x] \simeq \left\{ (f_k)_{k=0}^{\infty} \mid f_k \in R \text{ pro } k \in \mathbb{N}_0 \right\}$$

A operacemi:

$$(f_k)_{k \in \mathbb{N}_0} + (g_k)_{k \in \mathbb{N}_0} := (f_k + g_k)_{k \in \mathbb{N}_0}$$

$$(f_k)_{k \in \mathbb{N}_0} \cdot (g_k)_{k \in \mathbb{N}_0} := \left(\sum_{i=0}^k f_i g_{k-i} \right)_{k \in \mathbb{N}_0}$$

$R[x] \subset R[[x]]$ odpovídá posloupnostem s konečnou mnohou nenulovými členy.

Def: Necht R je okruh, $S \subset R$. Řekneme, že S je podokruh R , pokud

- 1) S je podgrupa R vzhledem k +
 - 2) $1 \in S$
 - 3) $\forall a, b \in S$ je $a \cdot b \in S$.
- Říkáme také, že R je nadokruh S .

Př: Okruhy $\mathbb{Z}$ a $\mathbb{Z}_n$ nemají vlastní podokruhy, protože $1 \in S \Rightarrow \langle 1 \rangle = R \subset S$.

Pozn: Při definici bez jednotky jsou $n\mathbb{Z}$ podokruhy $n\mathbb{Z}$ pro $n \in \mathbb{N}_0$.

Pozn: Definici podokruhu S lze přepsat.

6

- 1) $S - S \subset S$ 2) $1 \in S$ 3) $S \cdot S \subset S$.

Pozn: Každý podokruh je sám okruhem.

Tvzení: Necht R je komutativní okruh. Pak

-) R je podokruh $R[x]$;
-) je-li $S \subset R$ podokruh, pak $S[x]$ je podokruh $R[x]$;
-) $R[x]$ je podokruh $R[[x]]$.

Def: Necht $R, \tilde{R}$ jsou okruhy s jednotkami $1, \tilde{1}$.
Zobrazení $\varphi: R \rightarrow \tilde{R}$ je homomorfismus okruhů,
jestliže:

- 1) $\forall a, b \in R$ je $\varphi(a+b) = \varphi(a) + \varphi(b)$
... φ je homomorfismus aditivních grup
- 2) $\varphi(1) = \tilde{1}$
- 3) $\forall a, b \in R$ je $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$
... φ je homomorfismus multiplikativních monoidů.

Standardně nazývá

monomorfismus, epimorfismus,
izomorfismus, endomorfismus, automorfismus.

Je-li φ izomorfismus $\varphi: R \rightarrow \tilde{R}$, píšeme $R \cong \tilde{R}$.

Pozn: Je-li $R \cong \tilde{R}$ a R komutativní, pak $\tilde{R}$ komut.

Def: Je-li R komutativní okruh, $n \in \mathbb{N}$,
 $x_1, \dots, x_n$ formální proměnné, označíme
 $\alpha := (\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n$ multiindex a

$$x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$$

Okruh formálních mocninových řad nad R
v n proměnných $x_1, \dots, x_n$ je množina

$$R[[x_1, \dots, x_n]] := \left\{ \sum_{\alpha \in \mathbb{N}_0^n} f_\alpha x^\alpha \mid f_\alpha \in R \text{ pro } \alpha \in \mathbb{N}_0^n \right\}$$

s operacemi $+$ a $\cdot$:

$$\sum_{\alpha \in \mathbb{N}_0^n} f_\alpha x^\alpha + \sum_{\alpha \in \mathbb{N}_0^n} g_\alpha x^\alpha := \sum_{\alpha \in \mathbb{N}_0^n} (f_\alpha + g_\alpha) x^\alpha$$

$$\sum_{\alpha \in \mathbb{N}_0^n} f_\alpha x^\alpha \cdot \sum_{\alpha \in \mathbb{N}_0^n} g_\alpha x^\alpha := \sum_{\alpha \in \mathbb{N}_0^n} \left(\sum_{\substack{\beta, \gamma \in \mathbb{N}_0^n \\ \beta + \gamma = \alpha}} f_\beta g_\gamma \right) x^\alpha$$

Okruh polynomů v n proměnných nad R je

$$R[x_1, \dots, x_n] := \left\{ \sum_{\alpha \in \mathbb{N}_0^n} f_\alpha x^\alpha \mid f_\alpha = 0 \text{ až na konečně mnoho } \alpha \in \mathbb{N}_0^n \right\}$$

s stejnými operacemi.

Platí: 1) $R[x_1, \dots, x_n]$ je okruh.

2) $R[x_1, \dots, x_n]$ je podokruh $R[[x_1, \dots, x_n]]$.

$$3) R[x_1, \dots, x_n] \cong (R[x_1, \dots, x_{n-1}])[x_n]$$

$$4) R[[x_1, \dots, x_n]] \cong (R[[x_1, \dots, x_{n-1}]])[[x_n]].$$

dk: ad1) ověřit axiomy okruhu.

ad2) křijme!

ad3) vyplývá ze 4)

ad4) najdeme izomorfismus, pro $n=2$:

Pro $f \in (R[x])[y]$ je $f = \sum_{k=0}^{\infty} f_k y^k$, kde $f_k = \sum_{j=0}^{\infty} f_{kj} x^j \in R[x]$

Přiradíme $f \rightarrow \tilde{f} = \sum_{j,k=0}^{\infty} f_{kj} x^j y^k \in R[x,y]$.

Ověřit, že to je izomorfismus.

Zobrazení φ pro polynomy získáme
kázáním f na moc. řady s konečným
počtem nemul.

tvrzení: Průnik libovolného systému
podokruhů okruhu R je podokruh.

dk: přímočaré.

Def: Necht' R je okruh, $0 \neq X \subset R$. Podokruh

$$\langle X \rangle_R := \bigcap \{ S \subset R \mid S \text{ podokruh } R, X \subset S \}$$

je podokruh generovaný množinou X .

Pr: $R[x] = \langle \{x\} \cup R \rangle_R$, je-li S nadokruh R a $x \in S \subset R$.

Tvrzení: Je-li R okruh, $0 \neq X \subset R$, pak

$$\langle X \rangle_R = \left\{ k_1 x_{m_1} + \dots + k_m x_{m_m} \cdot a_{m,m_m} \mid m, m_i \in \mathbb{N}_0, k_i \in \mathbb{Z}, a_{ij} \in X \right\}$$

dk jako u grup.

7

Def: Necht $R, \tilde{R}$ jsou okruhy. Direktní součin okruhů $R, \tilde{R}$ je kartézský součin $R \times \tilde{R}$ s operacemi $+$ a $\cdot$ po složkách, tj.

$$\forall g, h \in R, \forall \tilde{g}, \tilde{h} \in \tilde{R} \text{ je}$$

$$(g, \tilde{g}) + (h, \tilde{h}) := (g + h, \tilde{g} + \tilde{h})$$

$$(g, \tilde{g}) \cdot (h, \tilde{h}) := (g \cdot h, \tilde{g} \cdot \tilde{h})$$

Platí: Direktní součin okruhů je okruh.

Pozn: Definice lze rozšířit na libovolný počet součinitelů.

Př: $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$

izomorfismus okruhů $f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$

$$n \bmod 6 \rightarrow (n \bmod 2, n \bmod 3)$$

$$0 \rightarrow (0, 0)$$

$$1 \rightarrow (1, 1)$$

$$2 \rightarrow (0, 2)$$

$$3 \rightarrow (1, 0)$$

$$4 \rightarrow (0, 1)$$

$$5 \rightarrow (1, 2)$$

Pro aditivní grupy $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$ (viz číselná řada)

pro multiplikační monoidy plyne z toho,

že $f(1) = (1, 1)$... jednotka v $\mathbb{Z}_2 \times \mathbb{Z}_3$

a vlastnosti kongruencí.

Pr: Gaussova celá čísla: $\{a+bi \mid a, b \in \mathbb{Z}\} =: \mathbb{Z}[i]$ 7.5

jako aditivní grupa $\mathbb{Z}[i] \simeq \mathbb{Z} \times \mathbb{Z}$

jako okruh $\mathbb{Z}[i] \not\simeq \mathbb{Z} \times \mathbb{Z}$

násobení na $\mathbb{Z} \times \mathbb{Z}$: $(m, n) \cdot (\tilde{m}, \tilde{n}) = (m \cdot \tilde{m}, n \cdot \tilde{n})$

na $\mathbb{Z}[i]$: $(m+ni)(\tilde{m}+\tilde{n}i) =$
 $m\tilde{m} - n\tilde{n} + i(m\tilde{n} + n\tilde{m})$