Zbývají poslední dvě přednášky, včetně té, kterou právě čtete!

V nich už částečně půjde o opakování některých pojmů, několik věcí ještě bude nových.

Začneme vysokoškolským pohledem na přirozená čísla: Co jsou to přirozená čísla?

Jaké jsou axiomy struktury přirozených čísel?

Bude to trochu jiný pohled než jen říci, že $(N, +, \cdot)$ je polookruh.

Jedná se o ještě trochu elementárnější pohled, na kterém je ta struktura polookruhu vybudována.

Věta: N je až na izomorfismus jediným modelem struktury zvané Peanova množina

Co to je Peanova množina P?

Na této množině platí čtyři axiomy:

1) $\forall x \in P\ \exists$ tzv. následník prvku x, který označíme jako $x' \in P$

2) $\exists\, e \in P$: e není následníkem žádného prvku množiny P

3) $\forall x, y \in P$: $x \neq y \Rightarrow x' \neq y'$ (následníci různých prvků jsou různí)

4) Jestliže pro podmnožinu $M \subseteq P$ platí
   a) $e \in M$
   b) $\forall x \in P: x \in M \Rightarrow x' \in M$

   tak $\Rightarrow M = P$

Tyto čtyři axiomy platí na množině přirozených čísel **N**:

ad 1) $\forall n \in N$ víme, že jeho následník n' se rovná $n' = n+1$

ad 2) 1 není následníkem žádného přirozeného čísla

ad 3) $(m \neq n \Rightarrow m+1 \neq n+1)$ platí $\forall m, n \in N$

ad 4) pokud procházíme prvky množiny N tak, že
   a) začneme prvkem 1
   b) pro $n \in N$ víme, že i $n+1 \in N$

   tak tímto způsobem projdeme celou množinu N

Poznámka: 1) axiom 4: kdybychom krokově procházení množiny N u každého přirozeného čísla ještě ověřili nějakou vlastnost, která pro ně platí, tak vlastně provádíme důkaz matematickou indukcí – struktura axiomu 4 je tedy hodně podobná struktuře důkazu matematické indukce.

2) Ještě je důležité říci, že N je jediným modelem Peanovy množiny, až na izomorfismus: Tj. kdyby nějaká množina S také splňovala Peanovy axiomy, tak existuje bijekce $b: N \to S$ která
   1) zachovává všechny následníky
   2) zobrazí 1 na e_S
   3) zachovává různost následníků pro různé prvky
   4) z axiomu 4) už bijekce b nemusí splňovat žádnou další vlastnost

Význam Peanových axiomů – díky jedinečnosti (až na izomorfismus) charakterizují tyto čtyři axiomy právě jen množinu N a žádnou jinou – jedná se tedy o jakési vnitřní či charakteristické axiomy množiny N.

Co je velice zajímavé, je to, že na základě Peanových axiomů lze na množině P už dále definovat všechny další vlastnosti, které na známé množině N existují – relaci uspořádání $\leq$

– operaci +

– operaci $\cdot$

Například relaci $\leq$ definujeme na P následovně:

– lze dokázat, že na Peanově množině, pokud $x \neq e$, existuje $u \in P : u' = x$

(tj. všechny prvky kromě e mají nějaký prvek, jehož jsou následníkem ... tento prvek nazveme **předchůdcem** prvku x a označíme $'x = u$

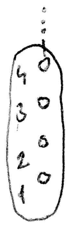
svislá čárka je před prvkem x

– lze definovat $U(a)$ = úsek Peanovy množiny příslušný prvku $a \in P$ takto:

1) $a \in U(a)$

2) $x \in U(a) \Rightarrow {'x} \in U(a)$, pokud tedy $'x$ existuje

například



$U(4) = \{1, 2, 3, 4\}$

$U(2) = \{1, 2\}$

(zkrátka $U(a)$ vytvoříme pomocí prvku a a všech možných předchůdců, které lze najít)

– pomocí pojmu předchůdce a úsek Peanovy množiny lze nyní definovat relaci uspořádání $\leq$ takto: $\boxed{a \leq b, \text{ když } a \in U(b)}$

Tímto způsobem jsme definovali uspořádání jen pomocí pojmu následník/předchůdce a pomocí pojmu podmnožina. Dále lze pomocí Peanových axiomů a pomocí právě definovaného uspořádání jejich prvků definovat operace sčítání i násobení tak, že $(P_0, +, \cdot)$ je komutativní polookruh

(stejně jako $(N_0, +, \cdot)$ je komutativní polookruh).

to už tady v této chvíli nebudeme dělat ani dokazovat,

cílem těchto prvních dvou stran bylo naznačit, že Peanovy axiomy tvoří jakousi minimální množinu axiomů, pomocí nichž lze definovat všechny pojmy, pro které platí všechny vlastnosti struktury $(N, +, \cdot)$, ~~za~~ které dodáním 0 vzhledem ke sčítání vznikne komutativní polookruh $(N_0, +, \cdot)$.

Abych řekl pravdu, to, co bude nyní následovat, bude pokusem o podobnou elementární „konstrukci" množin Z, Q, R, a nakonec možná i C. Intuitivně ovšem budete snad vědět, jaké vlastnosti daná struktura, kterou vytváříte chceme, má mít, protože jsme je procházeli v první polovině tohoto předmětu.

Intuitivně řečeno:

a) $(\mathbb{Z},+,\cdot)$ vytvoříme ze struktury $(\mathbb{N},+,\cdot)$ dodáním – 0 jako neutrálního prvku vzhledem ke sčítání
– záporných čísel jako inverzních prvků vzhledem ke sčítání

(dostaneme tak strukturu $(\mathbb{Z},+,\cdot)$, která je komutativní obor integrity, tj.

- $(\mathbb{Z},+)$ je komutativní grupa
- $(\mathbb{Z}^*,\cdot)$ je komutativní monoid → $\mathbb{Z}^*=\mathbb{Z}\setminus\{0\}$
- platí distributivní zákon $a\cdot(b+c)=ab+ac \quad \forall a,b,c\in\mathbb{Z}$
- $a\cdot b=0$ platí pouze pro $a=0$ nebo $b=0$)

b) $(\mathbb{Q},+,\cdot)$ vytvoříme ze struktury $(\mathbb{Z},+,\cdot)$ dodáním inverzních prvků vzhledem k násobení
(až na inverzní prvek k 0, který nedodáváme a spokojíme se s tím, že neexistuje – ani matematika nemůže reálně vytvářet to, co neexistuje v běžném životě)

dostaneme tak strukturu $(\mathbb{Q},+,\cdot)$, která je tělesem, tj.

- $(\mathbb{Q},+)$ je komut. grupa
- $(\mathbb{Q}^*,\cdot)$ je komut. grupa
- platí distributivní zákon $a\cdot(b+c)=ab+ac \quad \forall a,b,c\in\mathbb{Q}$

(nenuloví dělitelé nuly zde taky neexistují, ale to se u tělesa myslí automaticky, jak jsme zjistili v přednášce 6)

c) $(\mathbb{R},+,\cdot)$ vytvoříme ze struktury $(\mathbb{Q},+,\cdot)$ dodáním tzv. iracionálních čísel, což se pokusím vysvětlit za chvíli, vznikne struktura $(\mathbb{R},+,\cdot)$, která je také tělesem

d) $(\mathbb{C},+,\cdot)$ vytvoříme ze struktury $(\mathbb{R},+,\cdot)$ dodáním tzv. imaginární jednotky i, pro kterou platí $i^2=-1$, to už jsme si zhruba říkali, vznikne struktura $(\mathbb{C},+,\cdot)$, která je také tělesem.

Tedy z intuitivního popisu je vidět, že množiny $\mathbb{R}$, $\mathbb{C}$ už neznamenají algebraicky nový skok v pojmu, stále se jedná o tělesa jako u množiny $\mathbb{Q}$; tedy vzhledem k operacím $+,\cdot$ jsou množiny $\mathbb{Q},\mathbb{R},\mathbb{C}$ struktury stejného typu, pouze přibývají vlastnosti množin $\mathbb{R},\mathbb{C}$, které přímo nesouvisí s danými dvěma operacemi: u $\mathbb{R}$ je touto vlastností „iracionalita" některých čísel, u $\mathbb{C}$ je novou vlastností „imaginarita" některých čísel.

<u>Další poznámka</u>: Už jsem to asi říkal, ale ještě jednou připomenu, že odčítání a dělení nepovažujeme na této úrovni za DALŠÍ operace na dané množině, nýbrž

odčítání prvku/čísla je vlastně jen přičtení „opačného čísla" = inverze vzhledem k $+$

dělení nenulovým prvkem/číslem je vlastně jen násobení „inverzí" vzhledem ke $\cdot$

Ve zbytku této přednášky a v celé následující přednášce se podíváme na čtyři konstrukce uvedené na této stránce trochu přesněji.

Věta 2: Z komutativní pologrupy $(G,*)$ lze vždy vytvořit grupu

Jakým způsobem? Popišme si tuto konstrukci podrobněji:

(i) Vytvořme kartézský součin $G\times G$, na němž můžeme přirozeně definovat operaci „po složkách":

$$[a,b]*[c,d] = [a*c,\, b*d]$$

operace $*$ ze „staré" pologrupy

(ii) Definujme na $G\times G$ relaci ekvivalence $\sim$ takto:

$$[a,b]\sim[c,d], \text{ když } a*d = b*c$$

(iii) Vytvořme faktormnožinu $G\times G/_\sim$, tj. rozklad množiny $G\times G$ vzhledem k ekvivalenci $\sim$ na navzájem disjunktní podmnožiny, a tyto podmnožiny budeme chápat jako PRVKY množiny $G\times G/_\sim$.

(iv) Na množině $G\times G/_\sim$ definujme operaci $\circledast$ mezi jejími prvky takto:

$$\underbrace{\{[a,b]\}}_{\text{podmnožina obsahující prvek } [a,b]} \circledast \underbrace{\{[c,d]\}}_{\text{podmnožina obsahující prvek } [c,d]} := \underbrace{\{[a*c,\, b*d]\}}_{\text{podmnožina obsahující prvek } [a*c,\, b*d]}$$

operace ze „staré" pologrupy

Struktura $(G\times G/_\sim, \circledast)$ je grupa, protože operace mezi množinami splňuje vlastnosti ①, ②, ③, ④:

① plyne ze staré struktury – stará operace $*$ nám po složkách vytvoří prvek $[a*c, b*d]$, a ten zase leží v nějaké podmnožině množiny $G\times G/_\sim$

② asociativita nové operace $\circledast$ plyne z asociativity staré operace $*$

x je libovolný prvek staré pologrupy $(G,*)$ ⟶ ③ $\{[x,x]\}$ ... je neutrálním prvkem vzhledem k operaci $\circledast$, protože $\forall \{[a,b]\}\in G\times G/_\sim$ platí: $\{[a,b]\}\circledast\{[x,x]\} = \{[a*x,\, b*x]\} =$

a podle definice $\sim$ máme $[a,b]\sim[a*x,\, b*x]$, protože $a*b*x = b*a*x$ (plyne z komutativity staré operace $*$)

tedy prvky $[a,b]$, $[a*x,\, b*x]$ leží ve stejné podmnožině rozkladu, tj. $\{[a,b]\} = \{[a*x,\, b*x]\}$

(podmnožina obsah. $[a,b]$ je tatáž podmnožina, která obsahuje i prvek $[a*x,\, b*x]$)

$= \{[a,b]\}$ výsledek se nezměnil, ③ platí

④ $\forall \{[a,b]\}$ najdeme prvek inverzní, tím bude prvek $\{[b,a]\}$:

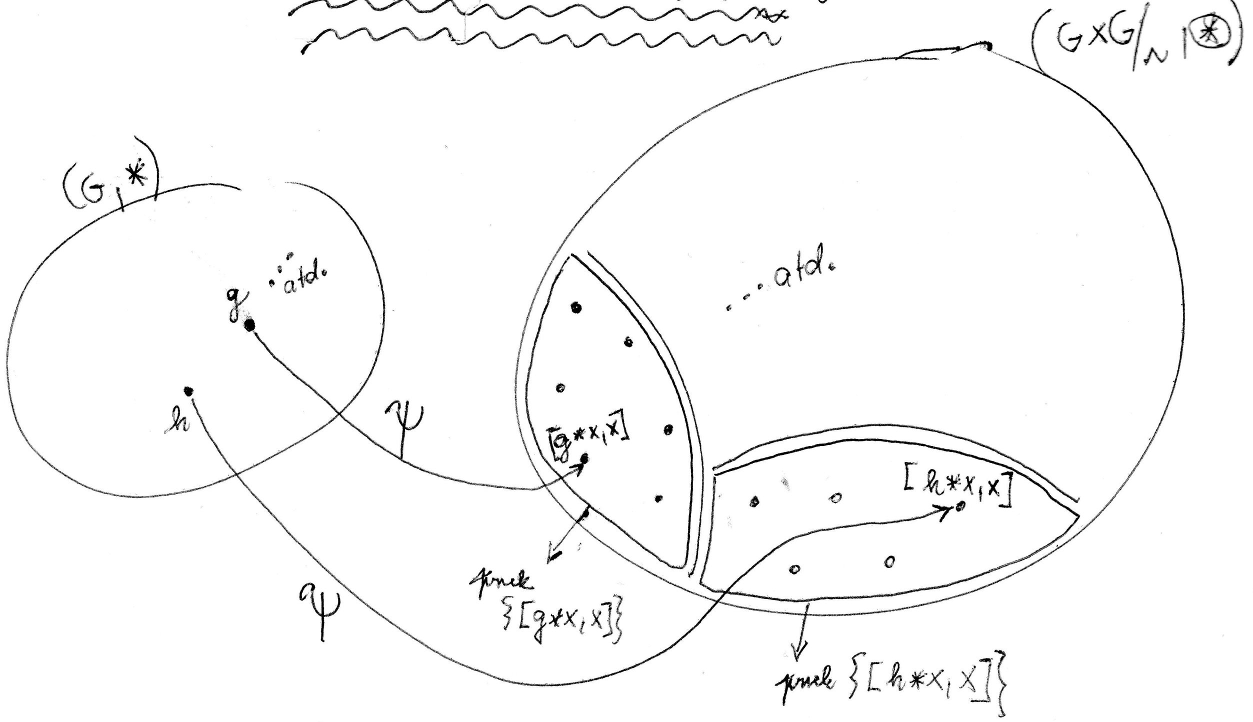
$$\{[a,b]\}\circledast\{[b,a]\} = \{[a*b,\, b*a]\} = \{[a*b,\, a*b]\} = \{[x,x]\}$$

platí komutativita staré operace $*$

Jsme hotovi, zkonstruovali jsme z pologrupy grupu!!!

Jsme dokonce schopni ještě tvrdit něco víc, a sice že existuje injektivní homomorfismus komutativní pologrupy $(G,*)$ do grupy $(G\times G/_\sim, \circledast)$, tj. pologrupu $(G,*)$ lze injektivně vnořit do grupy $(G\times G/_\sim, \circledast)$

Co tím mám na mysli? Definujme zobrazení $\psi(g)=\{[g*x,x]\}$



zobrazení $\psi : G \to G\times G/_\sim$ přiřadí prvku $g\in G$ tu podmnožinu z $G\times G/_\sim$, které obsahuje prvek $[g*x,X]$

Zobrazení ψ

1) je injektivní:

pro $g\neq h$: $[g*x,x]$ není v ekvivalenci s prvkem $[h*x,x]$, tedy prvky $[g*x,x]$, $[h*x,x]$ neleží ve stejné podmnožině rozkladu, ale v různých podmnožinách: $\{[g*x,x]\}\neq\{[h*x,x]\}$

2) zachovává výsledky operace:

označme $k := g*h$, $\psi(g)=\{[g*x,x]\}$

$\psi(h)=\{[h*x,x]\}$

$\psi(k)=\{[k*x,x]\}$

dokažme $\boxed{\psi(g*h)=\psi(g)\circledast\psi(h)}$ (podmínka zachování výsledků operace)

a) $\psi(g*h)=\{[\underbrace{g*h}_{k}*x,x]\}=\{[k*x,x]\}=L$

b) $\psi(g)\circledast\psi(h)=\{[g*x,x]\}\circledast\{[h*x,x]\}=\{[g*x*h*x,x*x]\}=$

$\underset{\text{komutativita}}{=}\{[g*h*x^2,x^2]\}=\{[g*h*x,x]\}=\{[k*x,x]\}=P$

protože $[g*h*x^2,x^2]\sim[g*h*x,x]$

dohromady: ψ je injektivní homomorfismus, pologrupu G „vnořuje" do grupy

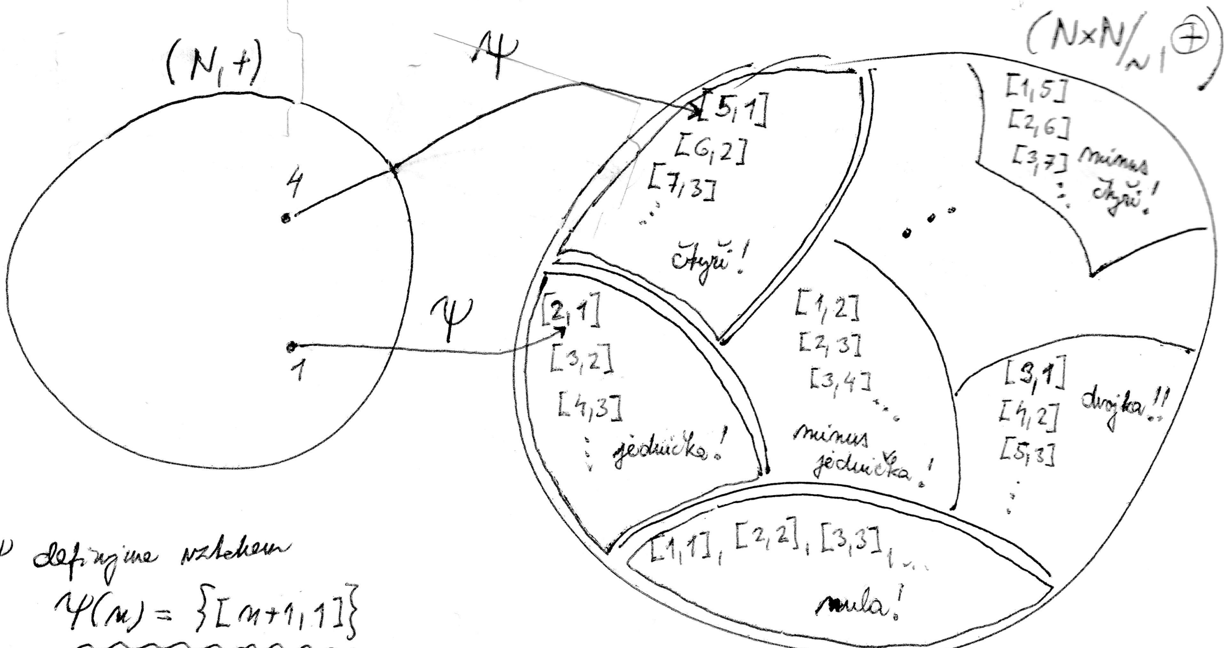
injektivní vnoření vlastně znamená, že množina G je izomorfní s nějakou podmnožinou prvků z $G\times G/_\sim$, tedy s podmnožinou podmnožin množiny $G\times G/_\sim$

<u>Reformulace věty 2</u>: Každou komutativní pologrupu $(G,*)$ lze injektivně vnořit do grupy $(G\times G/_\sim, \circledast)$, neboli každou komutativní pologrupu $(G,*)$ lze rozšířit na grupu $(G\times G/_\sim, \circledast)$

(této větě se říká věta o vnoření pologrupy do grupy, nebo: věta o rozšíření pologrupy na grupu.

Věta 3.: S využitím věty 2 lze komutativní pologrupu $(N,+)$ injektivně vnořit do grupy (= rozšířit na grupu) $Z := (N\times N/_{\sim}, \oplus)$

Věta 3 je tedy formálně naprosto přesný algebraický postup rozšíření přirozených čísel na celá čísla.



Zobrazení Ψ definujme vztahem

$$\Psi(n) = \{[n+1,1]\}$$

i) na $N\times N$ vytvořme operaci po složkách, jako sčítání vektorů

ii) na $N\times N$ definujme relaci ekvivalence: $[a,b]\sim[c,d]$, když $a+d=b+c$

iii) vytvořme faktormnožinu $N\times N/_{\sim}$, jejímiž prvky jsou podmnožiny určené danou ekvivalencí

iv) na množině podmnožin definujme operaci $\oplus$ takto: vybereme reprezentanty tříd = nějaké prvky těch tříd neboli podmnožin, sečteme je a výsledek určuje výslednou třídu (tím, že v ní leží)

$$\{[a,b]\}\oplus\{[c,d]\} := \{[a+c,b+d]\}$$

Tato operace $\oplus$ splňuje na množině $N\times N/_{\sim}$ vlastnosti

1 ... uzavřenost plyne z uzavřenosti „staré operace" + v jednotlivých souřadnicích = složkách

2 ... asociativita $\oplus$ plyne ze staré „asociativity operace + v jednotlivých souřadnicích = složkách

3 ... neutrálním prvkem je třída $\{[1,1]\}$, což je třída obsahující prvky $[1,1],[2,2],[3,3],\ldots$

4 ... například pro $\{[6,2]\}$ je inverzí $\{[2,6]\}$

tedy $(N\times N/_{\sim}, \oplus)$ je grupa!

Zobrazení $\Psi: N \to N\times N/_{\sim}$ je injektivní homomorfismus, tedy vnoření $(N,+)$ do struktury $(N\times N/_{\sim}, \oplus)$.

Závěrem:

Tímto způsobem jsme algebraicky přesně vytvořili jen pomocí přirozených čísel

– číslo 0 jako $\{[1,1],[2,2],[3,3],[4,4],\ldots\}$

– číslo (-4) jako $\{[1,5],[2,6],[3,7],[4,8],\ldots\}$

atd.

a přitom výsledky sčítání původních přirozených čísel zůstaly v nové struktuře zachovány!

to je zajištěno tím homomorfismem Ψ.