

4. ZÁKLADNÍ ALGEBRAICKÉ METODY

Universální algebra

$$A = (M, (w_i)_{i \in I})$$

M je normální množina

w_i jsou m-ární operace určené na normální množinu M

$$\text{Např.: } (\mathbb{Z}, +)$$

I je množina indexů

Podalgebra a podgrupa

Podalgebra algebry $A = (M, (w_i)_{i \in I})$ je nějaká algeba $(T, (w_i^*)_{i \in I})$ pro kterou platí, že $T \subseteq A$ a pro všechna $x_1, x_2, \dots, x_m \in T$ platí, že $w_i^* x_1, x_2, \dots, x_m \in T$ a rovnost $w_i^* x_1, x_2, \dots, x_m = w_i x_1, x_2, \dots, x_m$

— podgrupa je podalgebra splňující vlastnosti grupy

Generování podalgeber

— podalgebra vzniká z algebry tak, že si budeť prostě vybrat podmnožinu S libovolného "pluhu", že jí pak na množinu všechny operace původní algebry určené a nebo si vznut podmnožinu původní množiny křebsa S a nazvat ji systém generátorů podalgebry $\langle S \rangle$. Tedy $\langle S \rangle$ je podalgebra algebry A generovaná množinou S ($S \subseteq A$).

— máme křebs algebry $(M, \circ, e, -1)$ a z původní množiny M si vybereme funkci x a množinu z její jednoznačnou množinou $S = \{x\} \rightarrow$ nasledující množina X aplikující binární operaci \circ , kdy $x \circ x$ je nový výsledek, přes doplnění spolu s x do nové množiny křebsa $W \rightarrow$ tato funkce je množina W spolu s x do nové množiny křebsa $W \rightarrow$ tato funkce je množina W a tedy se prvním krokom $x \circ$ nový výsledek a nový x a sice principem de DeMorganova ...

— zde uvedeným "zádušním provozem" $\langle S \rangle = \langle x \rangle = (W, \circ, e, -1)$ je podalgebra původní algebry generovaná množinou z jediným prvkem x

— ! Když binární operaci aplikujeme množinu $\{-1\}$ a množinu $\{e\}$, pakže i inversní provoz jen funguje normálně množinu a stejně tak množinu funk

Př.: grupa $A = (R, \cdot, 1, a^{-1})$ — množinu množinách čísel

— všechny množiny funkci $2 \in R$ a všechny podalgebry (podgrupy)

$$\langle S \rangle = \langle 2 \rangle = (\{2^k \mid k \in \mathbb{Z}\}, \cdot, 1, a^{-1}) \quad - \text{blízkost a rozdílnost množiny}$$

(toto je iště označeno jinou množinou množinou, protože je operace množiny rovnoběžná s množinou 1 (neutral. pr.)

2. větší 1 (neutral. pr.)

Cyklická grupa

— grupa (R, \cdot, e, a^{-1}) je cyklická jestliže platí

$$\exists x \in R : R = \langle x \rangle$$

takže $\langle S \rangle = \langle S \rangle = \{x^k \mid k \in \mathbb{Z}\}$

Zobrazení

$y = f(x)$ může být $f: X \rightarrow Y$

- funkce je zobrazení

- mapuje funkce & množiny nejsou na funkci & množiny obecně

Př.: + souborné funkčních čísel N
je zobrazení (bijectivum)

+ $: N \times N \rightarrow N$

$\forall a, b \in N, \exists c \in N : + (a, b) = c$

(ani množina něčeho
A nejde jinak
než kdežto a množinám
je zobrazení funkce
definovat)

! nem',
zobrazení

$f: A \rightarrow B$

Typy zobrazení (podle počtu výchozích a cílových množin)

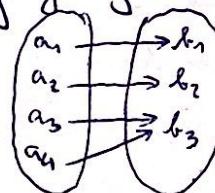
1) Zobrazení v množině

$f: A \rightarrow A$ - pouze se počtem funkce nějaké množiny

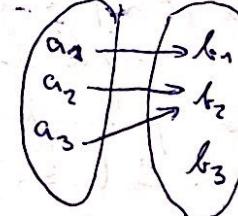
2) Surjektivní zobrazení

$f: A \rightarrow B$ kde platí že $\forall b \in B, \exists a \in A : f(a) = b$

- tedy každý výchozí obraz má alespoň jeden obraz množiny



✓



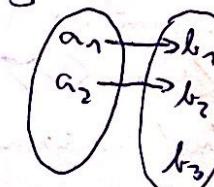
X

nem' surjektivní
- $b_4, b_5 \in B$ nem'
záčetné a. c.
stejný plátek
 $f(a) = b_3$

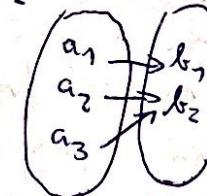
3) Injektivní zobrazení $f: A \rightarrow B$

- každou obraz množinu lze vymezit jednou až všechny obrazy neboli každý obraz množiny má vlastnou obraz množinu

$\forall a_1, a_2 \in A : f(a_1) = f(a_2) \rightarrow a_1 = a_2$



✓

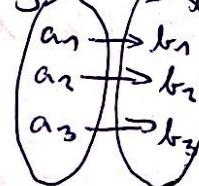
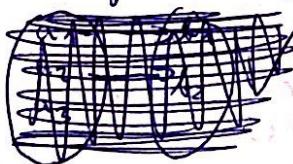


X b_2 má dva obrazy

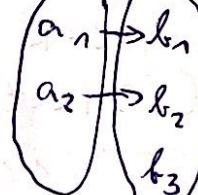
4) Bijectivní zobrazení $f: A \rightarrow B$

- injektivní a surjektivní zobrazení

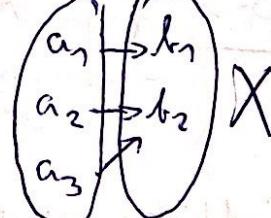
- každý obraz je rozdílný a rádce obraz nemá dva obrazy



✓



X



X

5) Inverzní zobrazení $f: A \rightarrow B$ $f': B \rightarrow A$

- je to zobrazení inverzní k injektivnímu zobrazení f

a tedy pokud $f: A \rightarrow B$ je $f': B \rightarrow A$

pomíjí surjektivní
 b_3 nem' obraz

pomíjí injektivní
 b_2 nem' obraz

Homomorfismus

- jedna se o zobrazení f jedné algebry do druhé algebry
 - obě algebry musí být stejných typů, ale jejich operace mohou být různé
 - např. $A = (\mathcal{M}, (w_i)_{i \in I})$ a $B = (\mathcal{M}^*, (w_i^*)_{i \in I})$ jsou algebry stejného typu, když mají obě grupy druhého řádu a $f: \mathcal{M} \rightarrow \mathcal{M}^*$ je homomorfismus algebry A do algebry B (takže $f(a_1, a_2, \dots, a_m) = w_i^*(f(a_1), f(a_2), \dots, f(a_m))$)
 - pro operaci w_i s aritikou $n > 0$
 - pro operaci w_i s aritikou $n = 0$
 - $f(w_i) = w_i^*$
- Pr.: máme algebry ~~\mathbb{Z}~~ $(\mathbb{Z}_1, +, 0, -)$ a algebry $(\mathbb{Z}^*, \circ, 1, \alpha^{-1})$ kde $\alpha \neq 0$ a $\alpha \circ \beta = \alpha + \beta + 1$.
 Potom zobrazení $f: \mathbb{Z} \rightarrow \mathbb{Z}^*$ dle' je f(x) = x-1 je homomorfismus \mathbb{Z} do \mathbb{Z}^* (homomorfismus prvej algebry do druhé) protože platí
 $f(x+y) = f(x) \circ f(y)$
 $f(x+y) = x+y-1$
 $f(x) \circ f(y) = (x-1) \circ (y-1) = x-1 + y-1 + 1 = x+y-1$

Typy homomorfismu (podle vlastností homomorfismu)

- máme homomorfismus $f: A \rightarrow A^*$ (platí keď pro všechny $a, b \in A$ že $f(a \circ b) = f(a) \circ f(b)$)
- Monomorfismus - je f injektivní
- Epimorfismus - je f surjektivní
- Isomorfismus - je f bijektivní
- Endomorfismus - normálním je stejná $A = A^*$ - f je zobrazení na vlastní
- Automorfismus - je izomorfismus a všechni Endomorfismus
- m/hoje homomorfismus se nazývají funkce f které jsou fiktivní
- ! - keď u homomorfismu $\{ \dots, -1, 0, 1, 2, \dots \}$ a $\{ \dots, -2, -1, 0, 1, \dots \}$ platí $f(0) = -1$

Jádro homomorfismu

- pokud se některé funkce f na stejném množině M^* (třeba $0 \neq 5$ nebo $1 \neq 2$) funkce f jsou jádro homomorfismu a keď u homomorfismu $Ker f = \{0, 5\}$
- Pr.: $f: \mathbb{Z}_6 \rightarrow \mathbb{Z}_6$ kde \mathbb{Z}_6 je cyklická skupina $\{0, 1, 2, 3, 4, 5\}$ a f je dle $f(x) = 2 \cdot x \bmod 6$ tak $Ker f = \{0, 3\}$ protože se daným fungem na 0

Relace ekvivalence

- je li relace ekvivalence:

- reflexivní $\forall x \in A : xRx$

- symetrická $\forall x, y \in A : xRy \rightarrow yRx$ — když je odlišný od relace (čárkou)

- transitivní $\forall x, y, z \in A : xRy \wedge yRz \rightarrow xRz$

například

$(xRy \wedge yRx \rightarrow x=y)$

↳ komutativnost je vlastnost relace ekvivalence

Pří:

máme děleno množinu $A = P(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$
A je tedy polenojednotková množina $\{1, 2, 3\}$

- je dělená relace R ekvivalence ji nasledující a $R \subseteq \{a | a \in A\}$

- je komutativní, protože dle pravidla množiny A jsou v relaci pořadí jenom ke množině se stejnou

- habíce plati $\emptyset R \emptyset$, $\{1\} R \{1\}$, $\{1\} R \{2\}$, $\{1\} R \{3\}$ atd... mohou být

- například $\{1\} \sim \{1, 2\}$ a $\{1, 2\} \sim \{1, 3\}$, $\{1, 2\} R \{1, 3\}$ atd...

- je li R relace ekvivalence?

reflexivní - $\{1\} R \{1\}$, $\{2\} R \{2\}$, $\{3\} R \{3\}$, $\emptyset R \emptyset$, $\{1, 2\} R \{1, 2\}$,
 ANO $\{1, 2\} R \{1, 2\}$, $\{2, 3\} R \{2, 3\}$, $\{1, 2, 3\} R \{1, 2, 3\}$

symetrická - $\{1\} R \{2\} \wedge \{2\} R \{1\}$...
 ANO

transitivní - $\{1\} R \{2\} \wedge \{2\} R \{3\} \wedge \{1\} R \{3\}$
 ANO a množina $\{1\}$ je vlastně $\{1, 2\}$ a $\{1, 2\}$ je vlastně $\{1, 2, 3\}$ až
 plati' atd... pro další...

ANO

- dleží máme nějakou množinu M a na ní definovanou relaci R (viz téma předchozího příkladu) a náleží řešit, že je relaci ekvivalence tak množin rozděluje na množiny M na trojice ekvivalence — v našem případě $T_1 = \{\emptyset\}$, $T_2 = \{\{1\}, \{2\}, \{3\}\}$

- relace ekvivalence rozdělá množinu na tři třídy ekvivalence $T_3 = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$

$T_4 = \{\{1, 2, 3\}\}$

- všechny množiny $f(M)$ rozdělenné množině množině ekvivalence R mohou být rozděleny podle množiny $f(M)$ (množina $f(M)$ je jedna všechny množiny $f(M)$ podle množiny $f(M)$)

- T_3 je rozdělení jeho třídy $\{1, 2\}$ ekvivalence R množině $\{1, 2\}$ množině $R[\{1, 2\}]$ což znamená, že množina $\{1, 2\}$ je rozdělena na dva podmnožiny $\{1\}$ a $\{2\}$ podle rel. ekvivalence R je reflexivní

TRÍDA EKVIVALENCE

- množina A relaci ekv. R je $A \setminus R = \{[a]_R \mid a \in A\}$

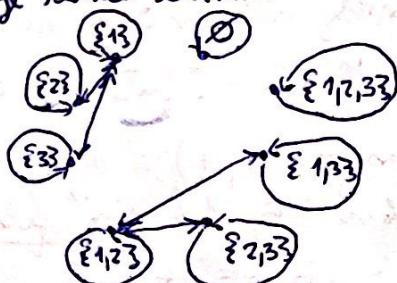
$\bullet [\emptyset]_R = \{\emptyset\}$ $\bullet [\{1\}]_R = \{\{1\}, \{2\}, \{3\}\}$ $\bullet [\{1, 2\}]_R = \{\{1, 2\}, \{1, 3\}, \{2, 3\}\}$

$\bullet [\{1, 2, 3\}]_R = \{\{1, 2, 3\}\}$ $= [\{1, 2\}]_R = [\{2, 3\}]_R$

$A \setminus R = \{[\{1\}]_R, [\emptyset]_R, [\{1, 2\}]_R, [\{1, 2, 3\}]_R\}$

Kongruence

- je speciální relace ekvivalence
- pokud máme množinu M a na ní dáme relaci R a tím relace je relace ekvivalence (je reflexivní, symetrická a transitivní) tak máme na M rovník do kříd ekvivalence
- Pr.: $M = \{\{1\}, \{2\}, \{3\}, \emptyset, \{1,2\}, \{1,3\}, \{2,3\}, \{1,2,3\}\}$ a R je dána a $R b \Leftrightarrow |a| = |b|$ možnost množiny
tak R je relace ekvivalence znázorňující na množinách jenom obrušky



Tak mám relace ekvivalence R rozdělila množinu M do kříd ekvivalence. Jde plati' že všechny párův z jedné kříd jsou ekvivalentní - tedy jsou každé char spolu rovnocenni.

- pokud mám dřívější algebraickou strukturu s mnoha množinami M a na ní definovanou relaci ekvivalence R a tím struktura má binární operaci \circ a máme pár $a_1, a_2 \in M$ blízce jen ekvivalentní (jsou ne stejně kříd) a pár pár $b_1, b_2 \in M$ blízce jen způsobem také ekvivalentní (jsou ne stejně kříd ale i jiné než a_1, a_2) a potom $a_1 \circ b_1 = c_1$ a $a_2 \circ b_2 = c_2$ (nebo $a_1 \circ b_2 = \dots$) tak by c_1 a c_2 množinou byly ekvivalentní (množina způsobem b_1 nezáleží) a někdo chybí možnou různou relaci R je homogenec

$$A = (M, (w_i)_{i \in I})$$

Jde $\# i \in I$ jen index a algebu ji lze písať $(n_i)_{i \in I}$
 když operace jen mimořádné, když $n_i > 0$ pro každou operaci $a_{i,1}, a_{i,2}, \dots, a_{i,n_i}$
 a R je relace ekvivalence na M $b_1, b_2, \dots, b_{n_i} \in M$

$$a_1 R b_1 \wedge a_2 R b_2 \wedge \dots \wedge a_{n_i} R b_{n_i}$$

$$\rightarrow w_i; a_1, a_2, \dots, a_{n_i} R w_i; b_1, b_2, \dots, b_{n_i}$$

Pr.: algebra $(N, +)$ kde N jen fiktivní čísla

redukuje se k definici jeho $a R b \Leftrightarrow a \bmod 5 = b \bmod 5$

- je reflexivní $\forall a \in N : a R a$ když $a \bmod 5 = a \bmod 5$

- je symetrická $\forall a, b \in N : a R b \rightarrow b R a$ když $a \bmod 5 = b \bmod 5 \rightarrow b \bmod 5 = a \bmod 5$

- je i transitivní $\dots \Rightarrow$ je to relace ekvivalence - normálně je komutativní

- rovník N do kříd $\{0\}_R, \{1\}_R, \{2\}_R, \{3\}_R$ a $\{4\}_R$ kde

$$\{3\}_R = \{3, 8, 13, 18, 23, 28, \dots\}$$

- je to R homogenec?

- je komutativní, když to málo' vypadá a je to jistě

$$13 R 18 \wedge 1 R 11 \rightarrow 13 + 1 R 18 + 11$$

$$- když množina vypadá 13+1 \bmod 5 = 4 \\ 18+1 \bmod 5 = 4$$

$$a_1 R b_1 \wedge \dots \wedge a_n R b_n \rightarrow (a_1 + a_2) R (b_1 + b_2)$$

\Rightarrow ANO je to homogenec k R

Faktorova' algebra

- testimoni main grup G a jijah
pada grup H alih-alih normalisasi ke grup G.
maka fungsi pada $H \times GL(H)$ yang memenuhi

- vnitřní relace ekvivalence R uvnitř množiny M je tedy ekvivalence. Sledováním tichého je reprezentovaná libobolná významná reprezentantka r/r' , když např. $\{1\}_R$
 - těžka ~~relativní~~ ekvivalence může být $\{a\}_R = \{b \in M \mid bRa\}$
 - a tedy doslouží tiché ekvivalentních a množin M
 - rozšíření množiny M pomocí relace R může tiché ekvivalence se řídit faktorovou množinou množiny M a tedy může $M/R = \{\{a\}_R \mid a \in M\}$
 - pokud máme algebra A s představou struktury $A = (N, +)$ a má může relaci ekvivalence R dle následujícího $a R b \Leftrightarrow a \text{ mod } 5 = b \text{ mod } 5$ tedy jde o faktorovou pole homomorfismu algebra $B = (N \setminus R, +)$ tedy $B = (\{\{0\}_R, \{1\}_R, \{2\}_R, \{3\}_R, \{4\}_R\}, +)$
 - v faktorové algebra B poskytuje pouze 5 reprezentantů tedy $0, 1, 2, 3, 4$ primitivní a může mít různé vlastnosti (základní vlastnosti) podle následujícího:
 - tedy v faktorové algebra B může mít třeba R relaci ekvivalence ale může mít i jinou homomorfismu proti kterému dojde rovněž k operaci $+$
 - pokud si jednáme o tiché pole faktorové množiny množiny M tedy dostaneme možnost $\bigcup_{a \in M} a = M$
 - základní charakteristiky faktorové množiny množiny M

Ideal okruhu

- Teoretyční výkaz

 - maximální obor R ledy $(Z_1 + |O_1 - a_1| \cdot)$ a jeho rozšířením je podobor I takový že je množinou na I: $\bullet \forall a, b \in I : a - b \in I$ (1.PODM)
 - $\bullet \forall a \in I, t \in R : a \cdot t \in I \quad$ (2.PODM)
 - Lavičkový obor R má maximální obor R a $\{0\}$ jej množinou prok
 - Pv: R je obor celých čísel $(Z_1 + |O_1 - a_1| \cdot)$ a I je jeho podobor všechny možné čísel ledy $I = (Z \% 2_1 + |O_1 - a_1| \cdot)$ - je to ideal?
 - pokud od jakehokoli nenechte číslu $a \in I$ ledy $a \in Z \% 2$ oddělme nenechte číslu $R \setminus I$ neb může mít pouze dve různé čísla
 - pokud jakehokoli nenechte číslu nejméně jednomu jakehokoli celému číslu z let rozdíru mezi různými čísly ledy
 - \Rightarrow daný je to ideal
 - maximální ideal by byl i $I_1 = (Z_1 + |O_1 - a_1| \cdot)$
a $I_2 = (\{0\}, + |O_1 - a_1| \cdot)$

Normalní podgrupa

- máme grupu (G, \cdot) a její normalní podgrupa je gruha (P, \cdot) kdežto splňuje vlastnost: $g \in G \cdot g \cdot P = P \cdot g$ a méně

~~$$g \in G \cdot g \cdot P = P \cdot g$$~~

$$P \cdot g = \{ p \cdot g \mid p \in P \}$$

$$g \cdot P = \{ g \cdot p \mid p \in P \}$$

- postřek ať provedeme operaci • nad jehožméněm problemem P a jehožméněm problemem G kde následkem té operace je $\cong P$
- aži třetí rada G jen reálně říká a P jen soudí kde • kdežto následně

Prvňe' součiny algebra

- ide ocelat prvňi' součin m algebra stejného typu (třeba $(2,0,1)$) a k nim
- množina množina algebra je kardinalitou součinem prvních množin množin a je tedy množinou m-tic

$$M_0 = M_1 \times M_2 \times M_3 \times \dots \times M_n \quad M_0 = M^m \quad - m je kód algebra m množin$$

- pro součin dvou algebra je množina množina množina dvojice kde první' je dvojice získaná z první' aleg. a druhý' z druhé'

$$M_1 = \{0,1\} \quad M_2 = \{2,3\} \quad M_0 = \{(0,2), (0,3), (1,2), (1,3)\}$$

- množina operace O je pak definována nad m-ticí' kde máte prvňi' pro kde operaci první' algebra (nad druhým) součin' albo..

$$U_1 = (A_1, +) \quad U_2 = (B_1, *)$$

$$U_1 \times U_2 = (A \times B, O) \quad \text{kde } (a_1, b_1) O (a_2, b_2) = (a_1 + a_2, b_1 * b_2)$$

Kongruence

Modulařní aritmetika

$$a \equiv b \pmod{n} \iff n \mid (a-b), \quad a, b \in \mathbb{Z}, \quad n \in \mathbb{N}$$

- proky a a b jsou kongruentní modulo n jestliže platí ře n dělí jejich rozdíl
- proky a a b když některý lze ještě (nemnoží se) ale pak je stejná čísla
- a a b jsou kongruentní vzhledem k operaci modulo n

$$a \pmod{n} = b \pmod{n}$$

- kongruence má násobky množinu (\sim kongruence $\pmod{2}$) na čísla které leží v tomto případě řídíme slabkové čísla ($\mathbb{Z}_5, \mathbb{Z}_7, \dots, \mathbb{Z}_m, m \in \mathbb{N}$)
- proky v jichne slabkové číidle mají stejné vlastnosti

Pr.: $7 \equiv 22 \pmod{5}$ $5 \mid 7-22 \dots 5 \mid -15 \checkmark$
 $5 \mid 22-7 \dots 5 \mid 15 \checkmark$

- křížka $\mathbb{Z}_5 = \{[0]_5, [1]_5, [2]_5, [3]_5, [4]_5\}$
 a $7 \sim 22$ patná' do $[2]_5$ protože $[2]_5$ je křížka obsahující všechny proky jejichž sbytek po dílení číslem 5 je 2 když $\mathbb{Z}_5 = \{2, 7, 12, 17, 22, 27, 3\}$
- sčítání slabkových čísel: $[a]_m \oplus [b]_m = [a+b]_m$

- násobení slabkových čísel: $[a]_m \otimes [b]_m = [a \cdot b]_m$ (s ohledem je slabkové číida součtu reprezentantů)
- a a b jsou libovolnými reprezentanty svého křížku $[0]_5$ množiny $\{1, 2, 3, 4\}$ a $[25]_5$

Pr.: $156 \cdot 231 \pmod{5} \iff [156]_5 \otimes [231]_5 \oplus [-5]_5$

- relaci kongruence můžeme zapsat $aRb \iff n \mid (a-b)$
- relace kongruence dělá rozklad množiny do křížků - fallorovou množinu
 $\mathbb{Z} \setminus R$ kde R je kongruence
- relace ekvivalence je relace na nejdále množině
- relace kongruence je relace na nejdále množině ohludem k nejdále operaci

Abstraktní algebra

Máme nějakou grupu (G, \circ) a její podgrupu (H, \circ) a máme dále
honguenci na grupě (G, \circ) podle podgrupy (H, \circ) , tedy $ha, b \in G$
platí, že a je ekvivalentní s b ($a \equiv_h b$) pokud $a^{-1}b \in H$
a a je správná honguenci s b ($a \equiv_p b$) pokud $a \circ b^{-1} \in H$.

Relace \equiv_h a \equiv_p jsou lzeva' a prava' honguence na grupě G podle
podgrupy H . honguence je typ. případ relace ekvivalence

— honguence je relace ekvivalence a rozhodnou' tedy grupu na křídlo
takže je chybějící pouze křídlo z jeho správné honguenci

$$\begin{aligned} ha \in G \text{ je lzeva' křídla } a \circ H &= \{a \circ h \mid h \in H\} \\ \text{je prava' křídla } H \circ a &= \{h \circ a \mid h \in H\} \end{aligned}$$

Př.: pro grupu $(\mathbb{Z}, +)$ — mámeže je komutativní, takže je jedna sloučená
 $(\mathbb{Z}, +)$ a $H = 5\mathbb{Z}$ — všechna celá čísla končí 5

$$13 \equiv 28 \dots -13 + 28 = 15 \in H$$

$$7 \equiv 22 \dots -7 + 22 = 15 \in H \text{ a tedy i } 7 + (-22) = -15 \in H$$

$\Rightarrow \equiv$ je tedy ~~ne~~ honguence na grupě $(\mathbb{Z}, +)$ podle grupy $5\mathbb{Z}$

Křídlo rozkladu je:

$$0+H = H+0 = \{h+0 \mid h \in H\} = \{-10, -5, 0, 5, 10, 15, \dots\}$$

$$1+H = H+1 = \{h+1 \mid h \in H\} = \{-11, -6, -1, 1, 6, 11, 16, 21, \dots\}$$

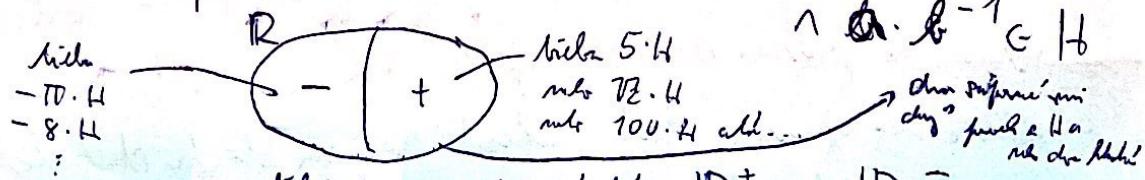
$$2+H = H+2 = \dots$$

$$3+H = H+3 = \dots$$

$$4+H = H+4 = \dots$$

— jednoduše křídlo je i v podgrupě H samou

$$\text{např. } (\mathbb{R} \setminus \{0\}, \cdot) \text{ a } H = \mathbb{R}^+ \quad a \equiv b \Leftrightarrow a^{-1}b \in H$$



— rozdělí se množina křídlo \mathbb{R}^+ a \mathbb{R}^-

Jinak lze rozdělit i pouze 'vlevo' nebo 'vpravo' pro honguenci na grupě G podle podgrupy H

$$\forall a, b \in G : a \equiv_h b \Leftrightarrow a^{-1}b \in H$$

$$\text{— } a \equiv_p b \Leftrightarrow a \circ b^{-1} \in H$$

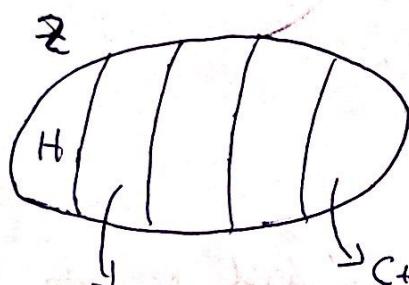
Faktorová algebra a Normální podgrupa

- máme nějakou algebrou $(Z, +)$ kde je definována relace kongruence na této algebře (\equiv) podle její podalgebry $(H, +)$
- když kongruence rovní množinu Z na jednotlivé tridy (tj. všechny jednotlivé tridy jsou rozdílné) je ekvivalentní k tomu když každá trida je:

$$[a]_R = \{a + h \mid h \in H\} \quad \text{kde } R \text{ je kongruence}$$

- množinu těchto trid se říká faktorová množina:

Faktorová algebra
 $\mathfrak{f}^*(Z|R, +)$
někdy nazývaná



$$a + H = b + H$$

a, b jsou v téže tridě
tj. jsou ekvivalentní

- každou tridu můžeme reprezentovat jako $c + H$ kde c je rámčí trida
- někdy $c + H$ kde c je rámčí trida - je jedno co zvolíme

Chceme dležit aby platilo i toto:

$$(a + H) + (c + H) = (a + c) + H$$

$$(b + H) + (d + H) = (b + d) + H$$

nesmí se stát že jsou součet (operační)

nebože ještě

je stejná trida

tedy nebože

kongruenční

to máme zavřený řetězec
podalgebra H bude normální podgrupa grupy G

Normální podgrupa

- pro normální podgrupu H grupy G platí všecky

$$\forall h \in H \quad \forall a \in G \quad a \cdot h \cdot a^{-1} \in H$$

- pokud je řetězec H normální podgrupa tak $(G|R, +)$ je faktorová algebra a $G|R$ je faktorová množina

tedy i řetězec
 $a \cdot H = H \cdot a$
je všechny tridy kongruenční

normální podgrupy
součinitelové grupy ne

→ tedy tedy máme komutativní grupu (Abelovou) a všechno nějakou způsobem patří do podgrup. Takže podgrupa je normální a tedy tedy když mi grupu rozdělím na podgrupy tak získáme faktorovou grupu.



— Mormon' podgrupa miss-lerí húdž základn rovny pravým
húdžom základn hí'prvoden' ~~podgrupa~~ grupy podle hí' podgrupy
(mormon') dne' konverzí'

Def $H_a \in G : a \cdot H = H \cdot a$