Algebra 1 – přednáška 5 (přednáška 4 se nekonala)

Na 1. přednášce jsme se zabývali různými vlastnostmi operace na množině – většinou dosti základními vlastnostmi, které platí pro běžné operace sčítání či násobení reálných čísel

(1) uzavřenost operace = neomezená definovanost operace na dané množině

(2) asociativita operace

(3) existence neutrálního prvku dané množiny vzhledem k této operaci

(4) existence inverzních prvků (každý prvek má jakýsi „protipól", se kterým když vstoupí do operace, výsledkem je neutrální prvek

(5) komutativita operace

Na některých množinách se definuje více operací, přichází zde do hry souhra těchto operací, ale tomu bude věnována samostatná přednáška (přednáška 6).

Jednotlivé vlastnosti operace lze dobře studovat v tzv. tabulce operace, až snad na asociativitu (2), kterou hned tak neodhalíme že platí, ale stejně ji mezi základní vlastnosti počítáme, protože axiom asociativity platí pro sčítání i násobení přirozených i reálných čísel a asociativitu lze lehce dokázat pro skládání zobrazení i skládání geometrických transformací, tj. velká řada běžných operací asociativitu splňuje.

Na 2. přednášce jsme pokračovali ve studiu těchto tabulek operace, ať už množin konečných nebo nekonečných – operace na nekonečné množině je dosti zdlouhavé do tabulky kreslit, ale přesto se o to pokusíme aspoň u několika prvků dané množiny, protože se tímto schématem vyjasní, které dva prvky do operace vstupují a který prvek je výsledkem.

Zjistili jsme, že $(H_6,+)$ je komutativní grupa

$(\mathbb{Z},+)$ je komutativní grupa

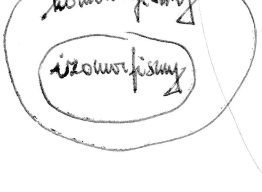
$(CF,\circ)$ je nekomutativní monoid

množina spojitých reálných funkcí

$(S_3,\circ)$ je nekomutativní grupa

$(\mathbb{Z}_6,\cdot)$ je komutativní monoid – zde si nejsem jistý, zda jsem neřekl pouze komutativní pologrupu, ale ona tam ta 1 je skutečně i neutrálním prvkem, jak jsme četli, tedy platí vlastnosti (1), (2), (3), (5). Říkali jsme si, že na $\mathbb{Z}_6$ vzhledem k násobení nemůžeme krátit, protože např. $2\cdot 2 = 5\cdot 2$, ale odtud neplyne, že $2=5$.

Na 3. přednášce jsme zavedli pojmy homomorfismu a izomorfismu mezi algebraickými strukturami, minimálně mezi grupoidy, protože oba tyto typy zobrazení zachovávají výsledky operace, a to všechny (tzv. vlastnost ZVO)



Každý izomorfismus je současně homomorfismem, ale nikoli naopak, protože na rozdíl od homomorfismu je izomorfismus ještě navíc bijekce.

Pokud zjistíme, že jsou dvě algebraické struktury izomorfní, znamená to nejen, že mají „stejný počet prvků" (u nekonečných množin říkáme, že mají stejnou mohutnost), ale operace ∇ na množině M_1 se chová zcela stejně jako operace $*$ na té druhé množině M_2 ... každý výsledek operace se zobrazí na příslušný výsledek operace

$$(ZVO) \quad f(a \nabla b) = f(a) * f(b)$$

Př. 3.1/str. 31: $(R,+)$ a $(R^+,\cdot)$ jsou izomorfní komutativní grupy; izomorfismus lze definovat vztahem $f:(R,+) \to (R^+,\cdot)$ tak, že $f(x)=e^x$. Jedná se skutečně o bijekci – každému reálnému x (i tomu zápornému) se přiřadí číslo e^x, které je vždy kladné (i když x je záporné). Naopak ke každému kladnému reálnému číslu y lze inverzní funkcí $\ln y$ (ZÁKLADY MATEMATIKY už jsou potřeba) přiřadit reálné číslo x tak, že $e^x = y$.

Navíc platí ZVO: $f(a+b) = f(a) \cdot f(b)$

operace ve 2. množině

operace v 1. množině

$$\checkmark \quad e^{a+b} = e^a \cdot e^b$$ .... známá vlastnost exponenty

Důležité je, že izomorfismus zachovává přesně stejné algebraické vlastnosti. Tam, kde jsou při zobrazení mezi algebraickými strukturami zachovány jen některé vlastnosti, mluvíme o homomorfismu. Zmiňovali jsme příklad homomorfismu $h: (Z,+) \to (Z_6,+)$, který zobrazuje nekonečnou množinu na množinu konečnou – „ztrácí" informaci o daném celém čísle, zachovává pouze informaci o tom, jaký je zbytek daného celého čísla po dělení šesti.

Říkal jsem vám, že matematik a chemik Cayley dokázal větu: každá grupa je izomorfní nějaké podgrupě grupy permutací $(S_n, \circ)$... tato věta v podstatě říká, že studium jakékoli množiny a jakékoli operace na ní lze převést na studium operace SKLÁDÁNÍ PERMUTACÍ na nějaké podmnožině množiny S_n, což je z matematického úhlu pohledu hodně zajímavé.

Běžný uživatel matematiky se s Cayleyho větou setká v tom smyslu, že pomocí ní bylo dokázáno (Gauss, Galois), že neexistuje vzorec analogický vzorci $x_{1,2} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ pro algebraické rovnice stupně 5 a více – což je sice negativní skutečnost, ale je to skutečnost.

(např. lze pomocí S_5 dokázat, že pro rovnici $x^5 - 5x - 2 = 0$ neexistuje vzorec $x_{1,2,3,4,5} = \ldots$, do kterého bychom mohli dosadit a řešení rovnice prostě vypočítat (tyto vzorce sice existují pro rovnice, kde maximální mocnina x je třetí nebo čtvrtá, ale už i tak jsou tak složité, že se nepoužívají – aspoň si myslíme, jako i v mnoha jiných věcech: myslet si jen s tím, co jsme se naučili na ZŠ. Ale vážně – v přednáškách 7 a 8 si o řešení těchto polynomických rovnic řekneme více).

Přednáška 4 – nekoná se, odpadá, protože se nekoná ani prověrka-a. Nyní v 5. přednášce: už jenom shrneme to, co bylo až dosud řečeno k algebraickým strukturám s jednou operací, na několika příkladech; v přednášce 6 se už začneme věnovat studiu algebraických struktur (množin), na kterých jsou definovány dvě operace.

Ještě jedna věc ohledně k homomorfismu – říkali jsme si (A DOKÁZALI), že homomorfismus musí zobrazovat neutrální prvek na neutrální prvek – když už jsme si to dokázali, budu vás z toho důkazu zkoušet. (skripta – věta 22, str. 45). Musíme ovšem předp., že (G_1, ∇), $(G_2, *)$ jsou grupy.

Dokažme ještě vztah mezi homomorfismem h a inverzními prvky a, a^{-1}: $h(a^{-1}) = (h(a))^{-1}$

(jinými slovy: h zobrazí prvky $a \longmapsto h(a)$

$a^{-1} \longmapsto h(a^{-1})$) a tyto prvky jsou mezi sebou opět ve vztahu inverze!!!

[Důkaz: Všimneme si, co se děje se „součinem" prvků $a \nabla a^{-1}$ před zobrazením:

změní se v neutrální prvek – toho v důkazu využijeme

– využijeme též toho, co jsme dokázali už minule, že neutrální prvek $e_1 \in (G_1, \nabla)$ se homomorfismem h zobrazí VŽDY na neutrální prvek $e_2 \in (G_2, *)$

dokázáno minule

$$e_2 = h(e_1) \overset{(4)}{=} h(a \nabla a^{-1}) \overset{ZVO}{=} h(a) * h(a^{-1})$$

a protože se nacházíme v grupě, víme, že takto přesně se definuje inverzní prvek k prvku $h(a)$, tj. $(h(a))^{-1} = h(a^{-1})$; důkaz je hotov, našli jsme inverzní prvek k prvku $h(a)$]

Př. 4.2/str. 42 Uvažujme dihedrální grupu D_5. Vypište všechny její podgrupy – využijte přitom poznatku z Lagrangeovy věty: počet prvků podgrupy konečné grupy je dělitelem počtu prvků této grupy

Nejprve k té Lagrangeově větě: její důkaz po vás chtít nebudu, ve skriptech je uveden jako pokračování vět 16, 17, 18, 19 – ale musíte si pamatovat, co Lagrangeova věta říká. U konečných grup nám usnadňuje práci při hledání podgrup.

Například u grupy S_3 (permutací 3-prvkové množiny), která má šest prvků, jsme kromě triviálních podgrup (jednoprvkové a šestiprvkové) našli ještě jednu podgrupu 3-prvkovou a tři podgrupy dvojprvkové. To není náhoda – počty prvků 1, 2, 3, 6 jsou dělitelé počtu 6 prvků celé grupy, a tak je to u konečných podgrup konečné grupy vždy.

Teď k té dihedrální grupě – název je hrozný, ale dihedrální grupu už jsme měli, jen jsme jí tak neříkali – je to šestiprvková grupa D_3 všech pootočení a osových souměrností, které zobrazí trojúhelník na sebe sama (skripta, str. 36)

– dihedrální grupa D_4 je vlastně grupa symetrií čtverce, čtyř otočení a čtyř osových souměrností (str. 21 až 24)

– no a dihedrální grupa D_5 se bude týkat geometrických transformací pravidelného pětiúhelníku a bude mít 5 otočení (včetně identity, což je otočení o úhel 0°) a 5 osových souměrností (osa vždy prochází vrcholem pětiúhelníku a středem protější strany)

Zkrátka, dihedrální grupu lze definovat pro každý do kružnice vepsaný pravidelný n-úhelník, D_n

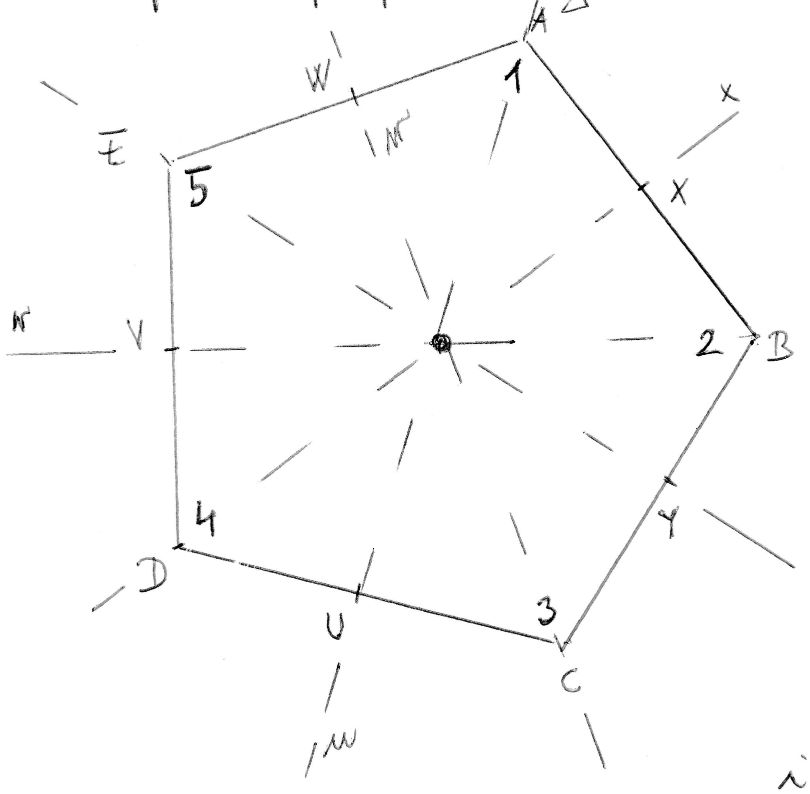
tato grupa má vždy $2n$ prvků – n otočení a n osových souměrností. A skládáním těchto geometrických transformací nám vždy dostaneme jednu z těchto transformací.

Teď mne prosím nezdržujte otázkami, k čemu vám řešení tohoto úkolu bude při výuce na ZŠ, a pokuste se sledovat tento VŠ popis základoškolských transformací pětiúhelníku:

<u>řešení:</u> $|D_5| = 10$, tj. kromě triviálních podgrup $P_1 = \{id\}$

$P_2 = D_5$ budou existovat jen podgrupy, jejichž počet prvků je dělitelem čísla 10,

tj. podgrupy <u>dvouprvkové</u> a <u>pětiprvkové</u>. Pokusme se je všechny najít pomocí označení permutacemi pětiprvkové množiny:



Klíčem je označit si vrcholy čísly 1 až 5

nyní vzhledem k zadání na str. 42 můžeme vypsat jednotlivé prvky:

$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \underline{\underline{id}}$

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

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

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

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

RADA: při zápisu cyklu začínejte vždy nejnižším číslem, které se zobrazí na jiné číslo (tj. zrovna 1, jen když se zobrazí na sebe sama, jinak jedničkou vždy začínejte)

$u = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 4 & 3 & 2 \end{pmatrix}$ ... vzhledem k ose u ... 1 zůstává na místě, $2 \leftrightarrow 5$ si změní místo, $3 \leftrightarrow 4$ si změní místo
$= (2,5) \circ (3,4)$

$v = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 1 & 5 & 4 \end{pmatrix}$ ... vzhledem k ose v ... 2 zůstává na místě, $1 \leftrightarrow 3$, $4 \leftrightarrow 5$ si změní místo
$= (1,3) \circ (4,5)$

$w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ ... vzhledem k ose w ... 3 zůstává na místě, $1 \leftrightarrow 5$, $2 \leftrightarrow 4$ si změní místo
$= (1,5) \circ (2,4)$

$x = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$ ... vzhledem k ose x ... 4 zůstává na místě, $1 \leftrightarrow 2$, $3 \leftrightarrow 5$ si změní místo
$= (1,2) \circ (3,5)$

$y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 1 & 5 \end{pmatrix}$ ... vzhledem k ose y ... 5 zůstává na místě, $1 \leftrightarrow 4$, $2 \leftrightarrow 3$ si změní místo
$= (1,4) \circ (2,3)$

Nyní vzhledem k Lagrangeově větě hledejme pouze
– pětiprvkové podgrupy
– dvouprvkové podgrupy

DŮLEŽITÉ JE, ŽE PŘÍKLAD JSME VYŘEŠILI I BEZ TABULKY OPERACÍ JEN POMOCÍ GEOMETRICKÉHO VÝZNAMU DANÝCH TRANSFORMACÍ A LAGRANGEOVY VĚTY

- Je vidět, že pětiprvková podmnožina všech pootočení tvoří podgrupu $\{e, f, g, h, i\} = P_3$

— obsahuje vždy inverze $e \longleftrightarrow e$ (obsahuje jednotkový prvek)

$f \longleftrightarrow i$ ... složením pool. o 72° a 288° dostaneme id

$g \longleftrightarrow h$ ... složením pool. o 144° a 216° dostaneme id

- podobně jako tomu bylo i v D_3 a D_4, osové souměrnosti jsou inverzemi sebe sama, tj. jejich připojením k neutrálnímu prvku dostaneme dvojprvkové podgrupy $\{e, u\} = P_4$, $\{e, v\} = P_5$, $\{e, w\} = P_6$, $\{e, x\} = P_7$, $\{e, y\} = P_8$

- žádné další netriviální podgrupy, než těchto šest (a dvou triviálních, P_1 a P_2), už neexistují

— když vezmeme jakékoli pootočení kromě identity, už pomocí něho VYGENERUJEME všechna další pootočení — a protože podgrupa musí být uzavřená na výsledek operace (= na složení transformací), musíme ty další pootočení přidat do téže podgrupy — tj. ať vezmeme jakékoli dvě různá pootočení, musíme už do stejné podgrupy přidat i tři další pootočení.

TOTO TAKÉ NENÍ UŽ NUTNÉ, PROTOŽE Z LAGRANGEOVY VĚTY (5 je prvočíslo) PLYNE, ŽE JEDINÁ PODGRUPA TÉTO GRUPY P_3 je jednoprvková

Například
$$f^1 = f$$
$$f^2 = f \circ f = g$$
$$f^3 = f \circ f \circ f = h$$
$$f^4 = f \circ f \circ f \circ f = i$$
$$f^5 = f \circ f \circ f \circ f \circ f = id = e$$

Takové podgrupě, která je GENEROVÁNA jedním prvkem, říkáme cyklická: $P_3 = \langle f \rangle$ ... je generovaná = „vytvořená" prvkem f

— kdybychom k některé ze podgrup P_4, P_5, P_6, P_7, P_8 přidali jediný další prvek, už by nutně (aby platila uzavřenost operace) vygeneroval celou množinu D_5

TOTO JE SPÍŠE TAKOVÁ ZKOUŠKA, ABYCHOM OVĚŘILI, ŽE ŽÁDNÁ DALŠÍ 5-i prvková podgrupa grupy D_5 UŽ NEEXISTUJE

Například přidáním v k množině $P_4 = \{e, u\}$
BY UŽ NUTNĚ DÍKY UZAVŘENOSTI PODGRUPY NA OPERACI

- $v \circ u = (1,5)\circ(2,4)\circ(2,5)\circ(3,4) = (1,5,4,3,2) = \underline{\underline{i}}$ muselo ležet v naší podgrupě
- $i^2 = h$ muselo ležet v naší podgrupě
- $i^3 = g$ — " —
- $i^4 = f$ — " —
- $i \circ u = (1,5,4,3,2)\circ(2,5)\circ(3,4) = (1,5)\circ(2,4) = v$
- $h \circ u = (1,4,2,5,3)\circ(2,5)\circ(3,4) = (1,4)\circ(2,3) = y$ muselo ležet v naší podgrupě
- $g \circ u = (1,3,5,2,4)\circ(2,5)\circ(3,4) = (1,3)\circ(4,5) = w$ — " —
- $f \circ u = (1,2,3,4,5)\circ(2,5)\circ(3,4) = (1,2)\circ(3,5) = x$ — " —

(tímto generováním už NUTNĚ dostaneme celou desetiprvkovou množinu D_5)

Pojem řádu prvku grupy: (def. str. 50) – cvičení číslo 5 mělo být věnováno řádu prvku, ale protože pravděpodobně odpadne, musím ten pojem připomenout, protože je užitečný:

řád ~~prvku~~ a grupy $(G, \triangledown)$ je nejmenší přirozené číslo k takové, že $a^k =$ neutrální prvek.

Pokud takové přirozené číslo neexistuje, říkáme, že řád prvku je ∞.

Př. a) ad příklad na předchozí straně: řád prvku f je roven 5, protože $f^5 = id = e$ a 5 je nejmenší přirozené číslo s touto vlastností

b) řád neutrálního prvku je vždy roven 1

c) $(\mathbb{Z}, +)$ … řád každého prvku mimo 0 je ∞, protože sčítáním stejného nenulového čísla nikdy nedostaneme nulu

Pojem řádu prvku je někdy užitečný při rozeznání, zda jsou dvě struktury izomorfní, nebo jen homomorfní: izomorfismus mezi grupami musí přesně zachovat řád prvku: řád vzoru = řád obrazu.

U homomorfismu nemusí striktně nastat rovnost, ale platí zde vztah:

řád obrazu | řád vzoru (řád obrazu je dělitelem řádu vzoru)

↑ dělí (viz základy matematiky)

Cvičení v rámci přípravy na závěrečnou zkoušku:

1) vypište všechny možné podgrupy dihedrální grupy D_6 (transformací pravidelného 6-úhelníku)

2) př. D2, str. 56 ve skriptu

př. N1, str. 57

př. N2, str. 57

př. D3, str. 58

př. N3, str. 59

u těchto příkladů nejsou výsledky na konci skript, zkuste je nějak dát dohromady společně, popřípadě se k nim vrátíme, pokud bude možnost

3) N4, str. 56 – výsledek příkladu viz str. 92

4) Definujte nějaký homomorfismus $(\mathbb{Z}_8, +) \to (\mathbb{Z}_4, +)$

↳ (str. 91, ad Například N.4 uprostřed stránky … jsou zde popsány všechny čtyři homomorfismy, které existují; na informace o jádru se vykašlete, to dělat nebudeme) Ale mohlo by vám pomoci, co to je jádro: jádro je množina prvků, které se homomorfismem zobrazí na neutrální prvek v té druhé grupě