Algebra 1 (MA 0003)

RNDr. Břetislav Fajmon, Ph.D.

Katedra matematiky Pedagogické fakulty Masarykovy univerzity v Brně – verze 2021

Obsah

Úvod

Tato skripta jsou napsána jako doplňující text do předmětu Algebra 1 pro 2. semestr bakalářského studia budoucích učitelů matematiky na 2.stupni ZŠ. Předmět svým charakterem navazuje na témata předmětu MA0001 (Základy matematiky) a předpokládá, že studenti si budou pamatovat pojmy: **množina, kartézský součin, relace, uspořádání, ekvivalence, zobrazení, operace, posloupnost, reálná funkce, a některé základní vlastnosti relace, viz cvičení 1 tohoto textu**.

V předmětu Základy matematiky jsme studovali zejména relace a jejich vlastnosti. Nyní v předmětu Algebra 1 budeme studovat zejména pojem operace.

Tento text by nemohl vzniknout bez knihy (Pinter 2010), ze které jsem podstatně čerpal jak pro přednášku, tak pro cvičení. I když tento předmět se studentům nutně bude zdát teoretický, Charles Pinter napsal svou knihu s přesvědčením, že algebra je pro matematiku potřebná – stejně potřebná jako geometrie.

V roce 2020 proběhla rekonstrukce osnovy, pro kterou budou v průběhu roku 2021 skripta průběžně doplňována. Pravděpodobně bude ve výuce použit i text kolegyně dr. Budínové o polynomech, pro část „komplexní čísla“ bude obohacením i středoškolská učebnice (Robová, Hála, Calda 2013).

Břetislav Fajmon,
verze textu leden 2021

1 Týden 01: Základní vlastnosti operace na množině M

1.1 Cvičení 1: Vlastnosti číselných operací

Podívejme se na tzv. Axiomy euklidovské geometrie:

1. Každé dva různé body lze spojit úsečkou.
2. Úsečku lze libovolně daleko prodloužit v přímku.
3. Pro dva různé body S, A lze sestrojit kružnici se středem v S, která prochází bodem A .
4. Přímý úhel lze kolmicí rozdělit na dva pravé úhly.
5. Bodem A, který neleží na přímce p, lze vést právě jednu přímku q rovnoběžnou s přímkou p.

Tyto axiomy si budete ještě procházet v předmětu geometrie. Nyní si pouze všimněme toho, že axiomy udávají vztahy mezi jednotlivými geometrickými pojmy (ty jsou podtrženy), nebo vlastnosti některých pojmů (např. přímý úhel je speciální úhel, který lze rozdělit kolmicí na dva shodné pravé úhly ... vlastnost 4).

Úkol cca na 10 min ve dvojicích. Přemýšlejte nad vlastnostmi známých operací sčítání, odčítání, násobení a dělení reálných čísel a pokuste se sestavit pět axiomů, které tyto operace splňují. Máte na to deset minut a poraďte se se sousedem (ve skupinkách o třech lidech).

Axiomy pro počítání s čísly (které studenti znají ze střední školy) zhruba daly základ pro definice následujících vlastností, jež budou hrát klíčovou roli:

Vlastnost (1) Uzavřenost množiny M vzhledem k operaci $*$:

$$\forall x, y \in M : \quad x * y \in M.$$

Vlastnost (1) je přirozená – chceme, aby operace na množině byly definované takovým způsobem, aby výsledek operace zase byl prvkem dané množiny.

Vlastnost (2) Asociativita operace $*$:

$$\forall x, y, z \in M : \quad (x * y) * z = x * (y * z).$$

Vlastnost (2) platí pro většinu operací, o kterých bude za chvíli řeč – jednoduše řečeno, několikanásobné použití jedné operace nezávisí na uzávorkování. Snad jen operace $-$ a : nejsou asociativní.

Vlastnost (3) Existence jednotkového prvku vzhledem k operaci $*$:

$$\exists e \in M : x * e = e * x = x \ \ \forall x \in M.$$

Příklad pro vlastnost (3): jednotkový prvek vzhledem k operaci sčítání je 0 (někdy nazýván též nulový prvek, aby nedošlo k záměně s prvkem 1), jednotkový prvek vzhledem k operaci násobení je 1.

Vlastnost (4) Existence inverzních prvků vzhledem k operaci $*$:

$$\forall x \in M \ \ \exists\, x^{-1} \in M : x * x^{-1} = x^{-1} * x = e.$$

Příklad pro vlastnost (4): Pro číslo 2 je inverzním prvkem vzhledem k operaci sčítání číslo -2, vzhledem k operaci násobení číslo $\frac{1}{2}$.

Uveďme nyní základní definice některých struktur, které splňují dané vlastnosti:

Definice 1 *Grupoid* $(M, *)$ *... množina* M*, na které operace* $*$ *splňuje vlastnost (1);*

Definice 2 *Pologrupa* $(M, *)$ *... množina* M*, na které operace* $*$ *splňuje vlastnosti (1),(2);*

Definice 3 *Monoid* $(M, *)$ *... množina* M*, na které operace* $*$ *splňuje vlastnosti (1),(2),(3) (někdy též podle starší terminologie: pologrupa s jednotkou, pologrupa s jednotkovým prvkem);*

Definice 4 *Grupa* $(M, *)$*... množina* M *s operací* $*$*, která splňuje na množině* M *vlastnosti (1), (2), (3), (4).*

Kromě těchto čtyř základních struktur, které byly právě definovány, ještě řada operací splňuje vlastnost (5) – viz následující definice. Tato vlastnost (5) už do samotné definice stěžejního pojmu grupy není zahrnuta, protože jak uvidíme v následujících dvou kapitolách, existují význačné příklady grup, které ji nesplňují. Proto slovo „komutativní“ musíme k právě definovaným strukturám zvlášť dodat jako novou vlastnost.

Vlastnost (5) Operace $*$ se nazývá komutativní na množině M, pokud platí vlastnost (5):

$$\forall x, y \in M \ \ : \ \ x * y = y * x.$$

Definice 5 $(M, *)$ *se nazývá komutativní grupoid, pokud je grupoid a operace* $*$ *splňuje vlastnost (5), tj. je komutativní na množině* M*.*

Definice 6 $(M, *)$ *se nazývá komutativní pologrupa, pokud je pologrupa a operace* $*$ *splňuje vlastnost (5), tj. je komutativní na množině* M*.*

Definice 7 $(M, *)$ *se nazývá komutativní monoid, pokud je monoid (tj. pokud je pologrupa s jednotkou) a operace* $*$ *splňuje vlastnost (5), tj. je komutativní na množině* M*.*

Definice 8 *$(M, *)$ se nazývá komutativní grupa, pokud je grupa a operace $*$ splňuje vlastnost (5), tj. je komutativní na množině M.*

Při přemýšlení nad základními vlastnostmi operací sčítání a násobení lze ještě najít často axiom, který si všímá „interakce“ = vzájemného vztahu mezi těmito dvěma operacemi: interakce operací + a · splňuje tzv. distributivní zákon = vlastnost (6):

$$\forall\ x, y, z \in M : x \cdot (y + z) = x \cdot y + x \cdot z,\ \ (y + z) \cdot x = y \cdot x + z \cdot x.$$

Název „distributivní“ lingvisticky odpovídá tomu, že po odstranění závorek se prvek x rozdělí = distribuuje k oběma členům součtu. Matematicky se jedná o pravidlo násobení závorky, ve které se nachází „součet“ prvků, kde „součet“ je operace s nižší prioritou než násobení. Například známá operace sčítání reálných čísel má nižší prioritu než násobení reálných čísel:

$$8 + 2 \cdot 3 = 14,$$

tj. operace · váže jednotlivá celá čísla s větší prioritou než je tomu u sčítání a odčítání (a pokud bychom chtěli nejprve sečíst čísla 8 a 2, a teprve pak výsledek vynásobit třemi, musíme díky větší prioritě násobení užít pro sčítání závorky).

Axiom (6) lze formulovat pro různé dvojice operací, tj. obecně bychom měli psát, že distributivní zákon mezi operacemi $*$ a $\bigtriangledown$ je

$$\forall\ x, y, z \in M : x * (y \bigtriangledown z) = (x * y) \bigtriangledown (x * z),\ \ (y \bigtriangledown z) * x = (y * x) \bigtriangledown (z * x).$$

To, že rovnice distributivity jsou dvě, musíme mít na mysli tam, kde operace $*$ není komutativní, tj. nesplňuje vlastnost (5).

Určitě si zopakujte ty nejdůležitější pojmy předmětu Základy matematiky:

Úloha 1.1 *Uveďte definice následujících základních pojmů z předmětu Základy matematiky a u každé uveďte příklad:*

a) *množina;*

b) *kartézský součin;*

c) *relace*

d) *ekvivalence;*

e) *uspořádání;*

f) *zobrazení;*

g) *operace;*

h) *(reálná) posloupnost;*

i) *(reálná) funkce.*

Úloha 1.2 *Uveďte následující definice vlastností relací a u každé z nich uveďte příklad:*

- *Relace ρ na množině M je reflexivní , když ...*
- *Relace ρ na množině M je symetrická, když ...*
- *Relace ρ na množině M je tranzitivní, když ...*
- *Relace ρ na množině M je úplná, když ...*
- *Zobrazení f z X do Y je taková relace na $X \times Y$, že platí ...*

Definice z obou úloh najdete v textu Základy matematiky.

1.2 Cvičení 2: Určování vlastností různých operací

Úloha 1.3 *Zjistěte, jaké struktury vzhledem k uvedené známé operaci (běžné označení) jsou následující množiny:*

a) $(N, +)$.

b) $(Z, +)$.

c) $(Z, \cdot)$.

d) $(Q, \cdot)$, $(R, \cdot)$.

e) $(Q - \{0\}, \cdot)$, $(R - \{0\}, \cdot)$.

f) $(2^A, \cup)$, *kde* $A = \{a, b, c, d, e\}$ *je pětiprvková množina.*

g) $(2^A, \cap)$, *kde* $A = \{a, b, c, d, e\}$ *je pětiprvková množina.*

h) $(Z, -)$, $(Z, :)$.

i) $(M, +)$, *kde* $M = \{-100, -99, -98, \ldots, -1, 0, 1, 2, \ldots, 99, 100\}$.

Úloha 1.4 *Opakování definic a práce s nimi*

a) *Nadiktujte sousedovi v lavici definici grupy a on ji zapíše zkráceným matematickým zápisem, ve kterém se nevyskytuje ani jedno české slovo, kromě slova „grupa“.*

b) *Co to znamená, že $(M, *)$ není grupoid, tj. není splněna vlastnost (1)? Negujte vlastnost (1).*

c) *Co to znamená že není splněna vlastnost (4) z definice grupy? Negujte vlastnost (4).*

Úloha 1.5 a) *Uveďte definici vlastnosti (4) pro operaci $\bigtriangledown$ na množině M ve stručném matematickém zápisu.*

b) *Uveďte příklad struktury $(M, \bigtriangledown)$, která splňuje vlastnost (4).*

c) *Uveďte příklad struktury $(M, \bigtriangledown)$, která NEsplňuje vlastnost (4).*

Úloha 1.6 *Dokažte, že množina všech podmnožin tříprvkové množiny s operací symetrického rozdílu $\div$ je grupa (viz Pinter 2010, str. 30, oddíl C).*

Výsledky některých cvičení najdete v závěru textu v oddílu 13.2.

1.3 Přednáška 1

Algebra je nauka o řešení rovnic[1]. Proto bychom mohli zmínit, co je to rovnice s neznámou x na množině M, na níž je definována operace $\bigtriangledown$:

- **Rovnost** je relace ekvivalence na množině výrazů, ve kterých vystupují prvky množiny M a operace $\bigtriangledown$. Příklad: běžně rovnost na množině reálných čísel chápeme jako relaci ekvivalence na množině výrazů, v nichž vystupují reálná čísla, reálné funkce a známé operace s reálnými čísly.
- **Rovnítko** je symbol relace rovnosti.
- **Rovnice** s neznámou x na množině M je výroková funkce, ve které vystupuje neznámý prvek x, symbol rovnosti (rovnítko), prvky množiny M nebo výrazy na množině M. Jak víme, výroková funkce není výrokem, protože bychom museli dosadit za x, abychom dostali výrok pravdivý či nepravdivý.
- **Řešit rovnici s neznámou x na množině** M znamená najít obor pravdivosti[3] K všech prvků z množiny M, pro které se stává daná rovnice pravdivým výrokem.

Podívejme se na některé jednoduché příklady:

a) Specifikace množiny M je také pro řešení rovnice důležitá. Například rovnice

$$7 + x = 2$$

nemá řešení na množině přirozených čísel (tedy tato rovnice nemá řešení na monoidu $(N_0, +)$)!! Nebo rovnice

$$7 \cdot x = 2$$

nemá řešení na množině celých čísel (tj. na monoidu $(Z, \cdot)$). Tj. vidíme, že už na monoidech (strukturách s jednou operací) některé rovnice nemají řešení!! Nebo rovnice

$$x^2 - 2 = 0$$

nemá řešení na množině racionálních čísel (v této rovnici uvažujeme současně výrazy s operací sčítání (odčítání) i násobení, hledáme tedy řešení na tělese $(Q, +, \cdot)$).

[1] Arabské „'al gebr“ znamenalo „složit“ rovnici, tj. vyřešit ji = nalézt její řešení[2]. Zejména se jedná o polynomické rovnice, kterými se budeme zabývat ve druhé polovině semestru.

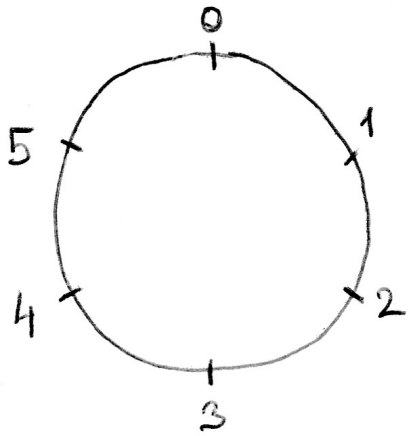
[3] K označuje tzv. množinu kořenů dané rovnice na množině M.

b) Ve většině tohoto textu se budeme zabývat rovnicemi s výrazy, ve kterých vystupuje jediná operace, a množina, na které budeme řešení rovnice hledat, bude zpravidla grupa nebo monoid vzhledem k této operaci. Oběma operacemi současně (tedy algebraickými strukturami se dvěma operacemi) se budeme zabývat až v kapitole 5.

Až dosud (v prvním týdnu) byly uvedeny různé axiomy operací, se kterými se v matematice setkáváme (operací sčítání, násobení čísel, operace průniku a sjednocení množin). Zkusme se nyní odpoutat od konkrétních operací, které známe. Podobně jako v předmětu Základu matematiky jsme se odpoutali od relací „menší nebo rovno“, „je dělitelem“ a „je podmnožinou“ a studovali obecně vlastnosti uspořádaných množin, tj. množin, na nichž je definována relace reflexivní, antisymetrická a tranzitivní, nyní se na chvíli odpoutáme od konkrétních operací a budeme studovat obecně vlastnosti grupy – tj. vlastnosti množiny, na níž je definována operace $*$, jež splňuje vlastnosti (1), (2), (3), (4).

Začněme ovšem jedním příkladem konečné, šestiprvkové grupy:

Příklad 1 *Grupa pootočení hodinové ručičky. Uvažujme čísla* 0 *až* 5 *rozmístěna po obvodu kružnice (např. obvodu ciferníku hodin) tímto způsobem (viz obrázek):*



Číslo 0 *se nachází tam, kde se obyčejně na hodinách vyskytuje číslo* 12. *Dále čísla* 1 *až* 5 *jsou společně s nulou rozmístěna rovnoměrně po obvodu kružnice tak, že úhel určený středem kružnice a rameny procházejícími dvěma sousedními čísly je* $60°$ *neboli* $\frac{\pi}{3}$.

Dále se budeme zabývat množinou pootočení jedné ručičky s osou otáčení ve středu kružnice:

- *prvek* 0 *představuje nulové pootočení ručičky – s ručičkou se nic nestane;*
- *prvek* 1 *představuje pootočení o jednu jednotku, tj. o* $60°$*;*
- *prvek* 2 *představuje pootočení ručičky o dvě jednotky, tj. o* $120°$*;*
- *prvek* 3 *přestavuje pootočení o* $180°$*;*
- *prvek* 4 *přestavuje pootočení o* $240°$*;*

- *prvek* 5 *přestavuje pootočení o* 300°.

Pokud ručička začíná svůj pohyb nasměrována na nulu, tak otáčením o uvedené úhly ji dostaneme opět do polohy nasměrované na některý z prvků – tj. množina otočení splňuje vlastnost (1), protože složením dvou otočení ručičky dostaneme zase nějaký ze základních šesti prvků.

Dále operace skládání otáčení je asociativní (splňuje (2)), když totiž při počátečním nastavení ručičky do nulové polohy složíme otočení $(1+2)+4$[4], dostaneme prvek 1 stejně jako při postupu $1+(2+4)$ – složením těchto tří pootočení dostaneme vždy úhel 420°, po jehož aplikaci ručička ukazuje na prvek 1. Tedy skládání pootočení nezávisí na jejich uzávorkování[5].

Pootočení 0 je neutrálním prvkem vzhledem ke skládání pootočení (platí vlastnost (3)) – když např. ručičku namířenou na prvek 4 pootočíme o 0, ručička je stále namířena na prvek 4.

A konečně, každý prvek má svůj inverzní prvek v této šestiprvkové množině (platí vlastnost (4)), se který když jej složíme, dostaneme ručičku zase do polohy 0:

- inverzí k 0 je opět 0;
- inverzí k 1 je 5 – a naopak, inverzí k 5 je 1;
- inverzí k 2 je 4 – a naopak, inverzí k 4 je 2;
- inverzí k 3 je opět 3.

Tedy celkem naše množina pootočení (označme ji $H_6 = \{0,1,2,3,4,5\}$) vzhledem k operaci skládání pootočení je grupa = operace + na ní definovaná splňuje vlastnosti (1) až (4).

Protože H_6 je konečná množina, lze si výsledky operace + napsat do tabulky:

Danou tabulku operace $*$ konstruujeme tak, že na průsečíku řádku prvku x a sloupce prvku y se vyskytuje výsledek operace $x * y$ (a této logiky konstrukce tabulek operací se budeme držet v celém textu):

$*$	...	y	...
...		...	
x	...	$x * y$	...
...		...	

Máme-li k dispozici úplnou tabulku operace $*$ na množině M, máme při zjišťování vlastností operace vyhráno. Jak lze nahlédnout v tabulce 1.1, vlastnosti (1), (2), (3), (4) operace + na Množině H_6 lze všechny z této)tabulky vyčíst (viz výklad ... elicit from

[4]Operaci označíme jako + – i když se nejedná o klasické sčítání čísel, toto skládání otočení má velmi příbuzné vlastnosti se sčítáním.

[5]Dokonce skládání tří pootočení nezávisí na jejich pořadí, protože operace skládání pootočení splňuje i vlastnost (5) = komutativitu; tou se ovšem nyní nechceme příliš zabývat.

Tabulka 1.1: Tabulka operace + na množině H_6.

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

the students).⋆ (tento znak znamená konec daného příkladu)

Je jasné, že lze obecně definovat grupu $(H_n, +)$ pootočení hodinové ručičky o násobky úhlu $\frac{2\pi}{n}$ s operací skládání pootočení – tato grupa má n prvků.

– při přepisu doplňte: všechny možné podmnožiny, na kterých je operace skládání pootočení uzavřená (tabulka pro operaci na podmnožině $\{0, 2, 4, \}$, ostatní jen zmiňte);
– poslední řádek příkladu zakončete takovou velkou tečkou za tečkou ve větě, která naznačuje konec příkladu. □.

Příklad 2 *Prozkoumejte vlastnosti operace sčítání na množině celých čísel.*

– při přepisu doplňte ... tabulku operace sčítání na množině Z

– při přepisu doplňte ... 0 je neutrální prvek vzhledem ke sčítání

– při přepisu doplňte ... inverze

– při přepisu doplňte ... podmnožiny uzavřené na operaci

Definice 9 Triviální podgrupy (= nevlastní podgrupy) *grupy $(G, \bigtriangledown)$ se nazývají dvě podgrupy: a) $S_1 = \{n\}$ je podgrupou vzhledem k $\bigtriangledown$, která obsahuje pouze neutrální prvek (je neprázdná a splňuje (1) a (4)), b) $S_2 = G$ (samotná celá grupa je též podgrupou sama sebe). Každou jinou podgrupu nazveme* **vlastní podgrupou** *grupy $(G, \bigtriangledown)$.*

Příklad 3 *Označme $(F(R), +)$ množinu všech funkcí (= zobrazení $R \to R$, viz předmět Základy matematiky) s operací sčítání funkcí.*

– při přepisu doplňte ... náznak tabulky operace, nějaké ukázky skládání funkcí, skutečnost, že skládání funkcí není komutativní, stručný důkaz, že skládání funkcí je asociativní (je vlastně vložen, jen ho okomentujte), co je neutrálním prvkem.

Skládání funkcí, potažmo jakýchkoli zobrazení, je asociativní operace:

$$(f \circ g) \circ h(x) = (f \circ g)(h(x)) = f(g(h(x))) = f \circ (g(h(x))) = f \circ (g \circ h)(x).$$

Příklad 4 *Důležitým příkladem grupy, na kterou se nyní zaměříme blíže, je grupa bijekcí n-prvkové množiny na sebe sama, kde operací je skládání zobrazení*[6]*. Často se jí též říká grupa permutací – označení opravdu má blízko ke středoškolskému pojmu permutace, kdy např. permutace* 5*-prvkové množiny* $\{1, 2, 3, 4, 5\}$ *byla chápána jako určité pořadí všech jejích prvků, např. pořadí* 51324*. Nyní budeme na tyto permutace pohlížet jako na zobrazení, které základní vzestupné pořadí* 12345 *přemění na pořadí např.* 51324*.*

Permutace $n-$prvkové množiny je bijekce množiny $\{1, 2, \ldots, n\}$ na sebe sama. S_n je množina všech permutací tohoto typu. Například permutace $f : M \to M$ pro $M = \{1, 2, 3, 4, 5\}$ definovaná

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$$

je bijektivní, takže existuje permutace f^{-1} k ní inverzní

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$$

Důležité úsporné označení permutace

V dalším textu budeme permutace zadávat úspornějším způsobem, který napíše každé číslo jen jednou, nikoli dvakrát. V tomto úsporném označení budeme permutaci

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} \quad \text{označovat jako} \quad f = (1, 5, 4, 2)$$

(v tomto označení se jedná o uzavřený cyklus zobrazení: 1 se zobrazí na následující zapsané číslo, tj. 5, číslo 5 se zobrazí na 4, číslo 4 na 2 a poslední zapsané číslo v závorce se zobrazí na první číslo 1, a tím se cyklus uzavře!!). Číslo 3 není v zápise uvedeno, protože se zobrazením f nemění. tj. $f(3) = 3$.

Podobně permutaci

$$f^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} \quad \text{budeme vyjadřovat jako} \quad f^{-1} = (1, 2, 4, 5)$$

[6] Až do konce této přednášky se všechny informace týkají tohoto příkladu.

(tj. změnil se změr cyklu, veškeré zobrazování otočilo směr; mohli bychom zapsat i $f^{-1} = (2, 4, 5, 1)$, protože nezáleží na tom, které číslo je v uzavřeném cyklu jako první; stále se jedná o stejný prvek:

$$f^{-1} = (1, 2, 4, 5) = (2, 4, 5, 1) = (4, 5, 1, 2) = (5, 1, 2, 4);$$

a protože nezáleží na pořadí prvků v cyklu, zavedeme další úmluvu, a sice první prvek každého cyklu napíšeme to nejmenší možné číslo).

Operace skládání permutací

Protože permutace je zvláštní případ zobrazení a zobrazení $M \to M$ lze skládat za sebou, můžeme mluvit o operaci „skládání zobrazení“, respektive „skládání permutací“.

- označení: $\circ$ ... (čti „po“) operace skládání zobrazení, ve které je nejdříve aplikováno druhé zobrazení v pořadí, a pak první – proto i čtení tohoto symbolu pomocí předložky „po“ je zcela instruktivní;

Ilustrujeme situaci pro $n = 3$: Uvažujme množinu permutací tříprvkové množiny $\{1, 2, 3\}$ do sebe – označme ji S_3. Množina S_3 má šest prvků:

$e := id$ (tímto symbolem budeme označovat identické zobrazení, jež zobrazí všechny prvky na sebe sama, tj. 1 na 1, 2 na 2 a 3 na 3), $s := (1, 2, 3)$ (pozor, neplést s identitou, u této permutace v souladu s úsporným označením platí $s(1) = 2$, $s(2) = 3$, $s(3) = 1$), $t := (1, 3, 2)$ (pozor, $(3, 2, 1)$ a $(2, 1, 3)$ je pořád stejný prvek t, ve kterém $t(1) = 3$, $t(3) = 2$, $t(2) = 1$), $u := (2, 3)$ ($u(2) = 3$, $u(3) = 2$, $u(1 = 1)$), a nakonec $v := (1, 3)$, $w := (1, 2)$. Permutací tříprvkové množiny je tedy šest.

Tyto permutace lze skládat, výsledkem složení je zase permutace tříprvkové množiny: například

$$s \circ e = (1, 2, 3) \circ id = (1, 2, 3) = s$$

nebo

$$u \circ v = (2, 3) \circ (1, 3) = (1, 2, 3) = s$$

(všimněte si, že zobrazování skládáme ZPRAVA DOLEVA, tj. 1 se zobrazí na 3, pak v levé permutaci 3 na 2, tj. celkem 1 na 2; dvojka v permutaci psané napravo není, tj. zobrazí se na sebe sama, složením s permutací vlevo se zobrazí na 3, celkem tedy 2 se zobrazí na 3; a konečně 3 se v permutaci napravo zobrazí na 1, v levé permutaci se 1 zobrazí na sebe sama, tj. celkem 3 na 1) nebo

$$v \circ u = (1, 3) \circ (2, 3) = (1, 3, 2) = t.$$

Čili z posledních dvou příkladů je vidět, že $v \circ u \neq u \circ v$, tj. operace $\circ$ je nekomutativní (neplatí vlastnost (5))! Propočítáním všech možných 36 kombinací dostaneme přehlednou tabulku výsledků operace $\circ$:

Nejprve je potřeba říci, že u každé tabulky operace $*$ na konečné množině prvků je prvek x v levém sloupcovém záhlaví vybrán jako první a prvek y v horním řádkovém záhlaví jako druhý[7].

Tabulka 1.2: Tabulka operace $\circ$ na množině S_3.

$\circ$	id	$(1,2,3)$	$(1,3,2)$	$(2,3)$	$(1,3)$	$(1,2)$
id	id	$(1,2,3)$	$(1,3,2)$	$(2,3)$	$(1,3)$	$(1,2)$
$(1,2,3)$	$(1,2,3)$	$(1,3,2)$	id	$(1,2)$	$(2,3)$	$(1,3)$
$(1,3,2)$	$(1,3,2)$	id	$(1,2,3)$	$(1,3)$	$(1,2)$	$(2,3)$
$(2,3)$	$(2,3)$	$(1,3)$	$(1,2)$	id	$(1,2,3)$	$(1,3,2)$
$(1,3)$	$(1,3)$	$(1,2)$	$(2,3)$	$(1,3,2)$	id	$(1,2,3)$
$(1,2)$	$(1,2)$	$(2,3)$	$(1,3)$	$(1,2,3)$	$(1,32,)$	id

Tedy konkrétně u operace $\circ$ na množině S_3 dostaneme tabulku operace:

Z tabulky je vidět, že operace je uzavřená na množině S_3, tj. platí vlastnost (1). Asociativita (2) platí pro skládání jakýchkoli zobrazení, viz příklad 3. A nakonec, je splněna i vlastnost (4), protože: jednotkový prvek id je (jako každý jednotkový prvek v grupě) inverzní sám k sobě; z tabulky dále vidíme, že $(1,2,3)^{-1} = (1,3,2)$, $(1,3,2)^{-1} = (1,2,3)$, a prvky $(2,3)$, $(1,3)$, $(1,2)$ jsou inverzemi sebe sama!

Dále existuje šest podgrup grupy $(S_3, \circ)$: tzv. triviální podgrupa, která obsahuje pouze jednotkový prvek id, s tabulkou operace

$\circ$	id
id	id

,

další podgrupou je celá šestiprvková grupa $(S_3, \circ)$ samotná. Kromě těchto dvou extrémně malých nebo velkých podgrup existují též tři dvouprvkové podgrupy

$\circ$	id	$(2,3)$
id	id	$(2,3)$
$(2,3)$	$(2,3)$	id

,

$\circ$	id	$(1,3)$
id	id	$(1,3)$
$(1,3)$	$(1,3)$	id

,

$\circ$	id	$(1,2)$
id	id	$(1,2)$
$(1,2)$	$(1,2)$	id

a jedna tříprvková podgrupa s tabulkou operace

$\circ$	id	$(1,2,3)$	$(1,3,2)$
id	id	$(1,2,3)$	$(1,3,2)$
$(1,2,3)$	$(1,3,2)$	$(1,2,3)$	id
$(1,3,2)$	$(1,3,2)$	id	$(1,2,3)$

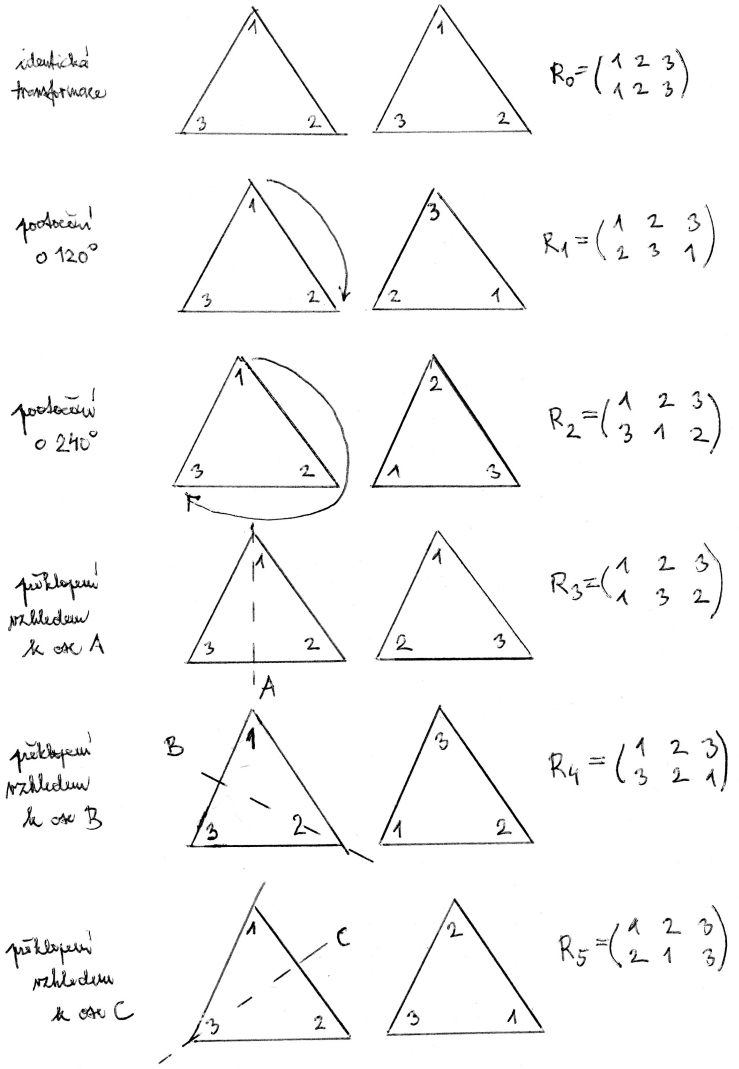
.

K čemu je dobrá grupa permutací S_3? Má i svůj geometrický význam, tj. lze ji použít při popisu některých základních geometrických zobrazení, například bijektivních zobrazení

[7] Toto je klíčově důležitá domluva, řečená už výše. Pořadí hraje roli právě u tohoto příkladu, kdy se jedná o operaci nekomutativní, tj. na pořadí prvků do operace vstupujících záleží.

trojúhelníku na sebe sama (tzv. symetrií trojúhelníku, odtud i původ písmene S v označení množiny), kterých je také šest, stejně jako prvků množiny S_3 – jedná se o tři otočení a tři osové souměrnosti. Každé z těchto geometrických proměn (= transformací) trojúhelníku lze přiřadit jednu permutaci jeho tří vrcholů.

– zde by se hodil obrázek s přiřazením permutací v krátkém zápisu jednotlivým transformacím trojúhelníku, s mírným vysvětlením. zkuste použít tento obrázek (vlastně jej můžete překreslit stejně, jen v posledním sloupečku bude to zjednodušené označení permutací pomocí cyklů = označení uvedené v té tabulce grupy S_3):



Obrázek 1.1: Množina D_3 permutací odpovídajících symetriím trojúhelníku.

1.4 Dodatky 1

V této části jsou uloženy součásti textu, které možná nebudou probrány – některé obecné důkazy, některé teoretické věci jsou zde „matematicky přesněji vyloženy“. Studenti by měli z těchto dodatkových částí vědět definice, a pak jen to, co jim speciálně zdůrazní vyučující, respektive co se probere na přednášce.

Základní vlastnosti grup

Studujme nyní tedy obecně vlastnosti grupy $(G, \bigtriangledown)$. Co v této obecné poloze lze říci o množině G a operaci $\bigtriangledown$? Pokud abstrahujeme od konkrétních situací a budeme studovat pouze vlastnosti (1) až (4) na množině G, dojdeme k poznatkům, které platí pro každou strukturu, která je vzhledem k nějaké operaci grupa.

První otázku si položme ohledně axiomu (3): pokud existuje neutrální prvek grupy, musí být jeden, nebo v jedné grupě může existovat více neutrálních prvků?[8]

Věta 1 *(o jednoznačnosti neutrálního prvku) V každé grupě $(G, \bigtriangledown)$ existuje jediný neutrální prvek.*

Důkaz: Sporem: předpokládejme, že v grupě existují dva různé neutrální prvky n_1 a n_2 takové, že $n_1 \neq n_2$. Jaké z toho plynou vlastnosti těchto dvou prvků?

Klíčová myšlenka: pokud je prvek neutrální, tak nemění výsledek operace $\bigtriangledown$ vůči jakémukoli dalšímu prvku, tj. např. $g \bigtriangledown n_1 = g$. Mohlo by tedy být zajímavé, co se stane, když aplikujeme operaci na dané dva neutrální prvky n_1, n_2[9]:

$$n_1 \overset{(3)_2}{=} n_1 \bigtriangledown n_2 \overset{(3)_1}{=} n_2,$$

což je spor s tím, že oba neutrální prvky jsou navzájem různé[10]. □

Tak to je zajímavé, neutrální prvek grupy může být pouze jeden jediný. A jak je to s inverzními prvky grupy? Víme, že v grupě existuje inverze ke každému prvku vzhledem k operaci $\bigtriangledown$ – musí také ke každému prvku existovat jediná inverze? Mohli bychom najít v grupě nějaký prvek, ke kterému existují inverze dvě?

Věta 2 *(o jednoznačnosti inverzních prvků) V každé grupě $(G, \bigtriangledown)$ existuje ke každému prvku x jediný inverzní prvek x^{-1} vzhledem k operaci $\bigtriangledown$.*

[8] Víme, že např. na množině $Q - \{0\}$ existuje vzhledem k násobení jediný neutrální prvek 1 – ale musí tomu tak být v každé grupě? Co když existují grupy se dvěma nebo třemi neutrálními prvky?

[9] Vlastnost $(3)_1$ znamená, že využíváme vlastnosti (3) pro prvek n_1, vlastnost $(3)_2$ platí pro neutrální prvek n_2.

[10] Celý důkaz je možné formulovat i jako přímý důkaz typu 2: předpokládáme, že prvky n_1, n_2 oba se chovají jako neutrální, tj. uvedené odvození by o nich dokázalo, že se musí nutně rovnat – tj. z toho plyne přímo, že prvek neutrální je pouze jeden.

Důkaz: Předpokládejme opět, že k nějakému prvku $a \in G$ vykazují dva prvky a_1^{-1}, a_2^{-1} vlastnost inverze, tj. platí

$$a \bigtriangledown a_1^{-1} = n, \quad \wedge \quad a_1^{-1} \bigtriangledown a = n$$

(musí platit oba vztahy, protože o operaci $\bigtriangledown$ zatím nevíme, zda je komutativní) a současně

$$a \bigtriangledown a_2^{-1} = n, \quad \wedge \quad a_2^{-1} \bigtriangledown a = n.$$

Klíčová myšlenka: vynásobením[11] $a_1^{-1} \bigtriangledown a_2^{-1}$ pravděpodobně nic nezískáme. Prvky a_1^{-1}, a_2^{-1} vystupují ve vlastnosti (4), tj. měli bychom studovat něco jako rovnice ve vlastnosti (4). VYUŽIJEME TOHO, ŽE VE VLASTNOSTI (4) SE VYSKYTUJÍ DVĚ ROVNOSTI, A JEDNU APLIKUJEME NA PRVEK a ZLEVA, DRUHOU ZPRAVA:

$$a_2^{-1} \overset{(3)}{=} n \bigtriangledown a_2^{-1} \overset{(4)_1}{=} (a_1^{-1} \bigtriangledown a) \bigtriangledown a_2^{-1} \overset{(2)}{=} a_1^{-1} \bigtriangledown (a \bigtriangledown a_2^{-1}) \overset{(4)_2}{=} a_1^{-1} \bigtriangledown n \overset{(3)}{=} a_1^{-1}.$$

Využili jsme platnosti asociativního zákona (2) pro kaskádu tří prvků uprostřed spojených operací $\bigtriangledown$. Z uvedené kaskády rovností je vidět, že prvky a_1^{-1} a a_2^{-1} musí nutně být stejné. Důkaz je hotov – inverzní prvek k prvku a existuje v grupě právě jeden. □

Věta 3 *(můžeme „krátit“[12] v rovnostech, ve kterých se vyskytují prvky grupy G a operace $\bigtriangledown$?) V každé grupě $(G, \bigtriangledown)$ platí zákony o krácení (7), tj.*

$$\forall a, b, c \in G: \quad (a \bigtriangledown b = a \bigtriangledown c \Rightarrow b = c) \quad \wedge \quad (b \bigtriangledown a = c \bigtriangledown a \Rightarrow b = c).$$

Důkaz: Provedeme například pro první z implikací: Vztah

$$a \bigtriangledown b = a \bigtriangledown c$$

rozšíříme zleva aplikací inverzního prvku na obě strany rovnice (to je vlastně vlastnost anti-(7), která ovšem plyne z vlastnosti (1): „vynásobením“ téhož prvku grupy G (který je na obou stranách rovnice) dostaneme opět prvek grupy G:

$$a^{-1} \bigtriangledown a \bigtriangledown b = a^{-1} \cdot a \bigtriangledown c,$$

a s využitím asociativity (2) (v grupě nezáleží na uzávorkování „součinu“ tří prvků vzhledem k operaci $\bigtriangledown$), vlastnosti inverzí (4) a vlastnosti neutrálního prvku (3) dostaneme

$$b = c.$$

Důkaz druhé nerovnosti bychom museli provádět vynásobením obou stran rovnice zprava, abychom mohli aplikovat vlastnost inverzí (4). □

[11] Všimněte si, že říkám „vynásobením“, ikdyž nyní nestudujeme operaci násobení, ale operaci $\bigtriangledown$ ... tak moc jsou operace sčítání a násobení v nás zakódovány, že používáme terminologii, která odpovídá těmto operacím – správně bychom měli říci: aplikací operace $\bigtriangledown$ na dané prvky v daném pořadí, tj. na uspořádanou dvojici prvků ...

[12] Opět terminologie: i když mluvíme obecně o operaci $\bigtriangledown$, pro vlastnost (7) se vžil termín „zákony o krácení“, třebaže krácení je termín vzatý z rovností, ve kterých se vyskytuje běžná operace násobení.

Věta 4 *(o vzájemně inverzních prvích) V každé grupě* $(G, \bigtriangledown)$ *z rovnosti* $a \bigtriangledown b = n$ *(kde* n *je neutrální prvek) plyne, že platí*

$$a^{-1} = b, \quad \text{a současně} \quad b^{-1} = a$$

(tedy prvek b *je inverzní k prvku* a*, a současně prvek* a *je inverzním prvkem k prvku* b*).*

Důkaz: je prostý, neboť plyne z věty 2: pokud b vykazuje vlastnosti inverze (4), tak musí být inverzní k prvku a, protože více inverzních prvků k danému prvku v grupě být nemůže. Další možnost důkazu: pokud rozšíříme rovnost $a \bigtriangledown b = n$ prvkem a^{-1} zleva, dostaneme

$$a^{-1} \bigtriangledown a \bigtriangledown b = a^{-1} \bigtriangledown n \overset{(3)}{=} a^{-1},$$

po aplikaci vlastnosti (4) na první výraz dostaneme $b = a^{-1}$. □

Věta 5 *(o výpočtech inverzních prvků) V každé grupě* $(G, \bigtriangledown)$ *platí:*

i) $(a \bigtriangledown b)^{-1} = b^{-1} \bigtriangledown a^{-1}$ *(inverze součinu dvou prvků je součin jejich inverzí, ale v opačném pořadí!!!);*

ii) $(a^{-1})^{-1} = a$ *(inverzí k inverzi je původní prvek).*

Důkaz: ad i) Přímo ověřením vlastnosti (4) pro prvky $a \bigtriangledown b$ a $b^{-1} \bigtriangledown a^{-1}$:

$$a \bigtriangledown b \bigtriangledown (b^{-1} \bigtriangledown a^{-1}) \overset{(2)}{=} a \bigtriangledown (b \bigtriangledown b^{-1}) \bigtriangledown a^{-1} \overset{(4)}{=} a \bigtriangledown n \bigtriangledown a^{-1} \overset{(3)}{=} a \bigtriangledown a^{-1} \overset{(4)}{=} n.$$

Protože nevíme, zda operace $\bigtriangledown$ je komutativní, měli bychom ověřit i druhý za zákonů (4), tj. upravovat výraz

$$(b^{-1} \bigtriangledown a^{-1}) \bigtriangledown a \bigtriangledown b$$

analogickým způsobem se v něm „vyruší“ nejprve $a^{-1} \bigtriangledown a$, a pak$b^{-1} \bigtriangledown b$ a dostaneme opět pouze n.

ad ii) Z rovnosti $a \bigtriangledown a^{-1} = n$ a věty 4 o vzájemné inverzi máme $(a^{-1})^{-1} = a$. □

Definice 10 Řád konečné grupy *se nazývá počet jejích prvků, označujeme* $|G|$.

Označení počtu prvků je standardní, nazývat tento počet prvků řádem je poněkud bizarní, ale má jakési opodstatnění u cyklických grup.

Rozšíření vlastnosti (2) na k prvků

Ve větě 5 se vyskytuje „součin“ čtyř prvků za sebou – přesně pracující matematik by měl prozkoumat, zda se nedopouští při důkazu něčeho, co není definováno. Pokud

definujeme součin čtyř prvků vzhledem k operaci $\bigtriangledown$jako součin prvního prvku se součinem následujících tří prvků, tj.

$$a \bigtriangledown (b \bigtriangledown c \bigtriangledown d),$$

postupným užitím vlastnosti (2) pro tři prvky dostaneme

$$a \bigtriangledown (b \bigtriangledown c) \bigtriangledown d = a \bigtriangledown b \bigtriangledown (c \bigtriangledown d) = (a \bigtriangledown b) \bigtriangledown (c \bigtriangledown d) = (a \bigtriangledown b) \bigtriangledown c \bigtriangledown d$$

a jedná se stále o týž výsledek. „Součin“ čtyř prvků je tedy definován korektně a platí pro něj vlastnost (2)' ... v sekvenci třikrát za sebou použité operaci $\bigtriangledown$ nezáleží na uzávorkování.

S takto rozšířeným zákonem asociativity můžeme pak vyslovit a dokázat některé věty pro větší počet operací $\bigtriangledown$ v řetězci za sebou, například analogii části (a) věty 5:

$$(a_1 \bigtriangledown a_2 \bigtriangledown \cdots \bigtriangledown a_k)^{-1} == a_k^{-1} \bigtriangledown a_{k-1}^{-1} \bigtriangledown \cdots \bigtriangledown a_2^{-1} \bigtriangledown a_1^{-1}.$$

Dále pro nás bude užitečná například definici n-té mocniny vzhledem k operaci $\bigtriangledown$:

Definice 11 n-tá mocnina prvku *a grupy $(G, \bigtriangledown)$ se definuje jako prvek získaný v řetězci operací*

$$a^n := \underbrace{a \bigtriangledown a \bigtriangledown \cdots \bigtriangledown a}_{n-krát}.$$

A pokud už máme definovanou mocninu, má smysl ptát se, zda existují odmocniny, a sice v následujícím smyslu:

Definice 12 n-tá odmocnina prvku *a grupy $(G, \bigtriangledown)$ je takový prvek $x \in G$ (pokud tedy existuje), že $a = x^n$.*

Definice 13 zápornou odmocninu *a^{-5} grupy $(G, \bigtriangledown)$ definujeme jako pátou mocninu jejího inverzního prvku, tj. $a^{-5} := (a^{-1})^5$.*

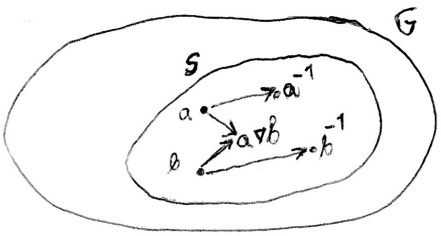
2 Týden 02 – další vlastnosti operace na množině

2.1 Přednáška 2

Podgrupa $(S, \bigtriangledown)$ grupy $(G, \bigtriangledown)$

Zabývejme se nyní otázkou: kdy je neprázdná podmnožina S grupy $(G, \bigtriangledown)$ také grupou?

Definice 14 Podgrupa $(S, \bigtriangledown)$ **grupy** $(G, \bigtriangledown)$ *je taková neprázdná podmnožina S množiny G, která je uzavřená vzhledem k operaci $\bigtriangledown$ (vlastnost 1) a s každým prvkem a obsahuje i jeho inverzi a^{-1} (vlastnost 4).*



Kupodivu se ukazuje, že dané dvě vlastnosti (1), (4) neprázdné[13] podmnožině S grupy $(G, \bigtriangledown)$ stačí na to, aby byla grupou vzhledem k téže operaci $\bigtriangledown$:

Věta 6 *(co stačí podmnožině grupy, aby byla sama grupou) Pokud neprázdná podmnožina S grupy $(G, \bigtriangledown)$ splňuje vlastnosti (1), (4), už je sama grupou vzhledem k téže operaci $\bigtriangledown$.*

Důkaz: $(S, \bigtriangledown)$ splňuje asociativitu (2) díky tomu, že je podmnožinou grupy, kde vlastnost (2) platí. Vlastnost (3), = existence neutrálního prvku, plyne z vlastnosti (4):

Díky tomu, že S je neprázdná, obsahuje aspoň jeden prvek, označme jej a.

$$a \in S \overset{(4)}{\Rightarrow} a^{-1} \in S \overset{(1)}{\Rightarrow} a \bigtriangledown a^{-1} = n \in S,$$

tedy neutrální prvek n patří i do množiny S a pro $(S, \bigtriangledown)$ platí (3). □

Označení 01 ... hvězdička znamená, že z dané množiny Z, Q, R vyloučíme nulu, značíme tedy symbolem Z^*, Q^*, R^*.

Příklad 5 *Podmnožina Q^* všech zlomků kromě nuly je podgrupou grupy $(R^*, \cdot)$: vynásobením dvou nenulových zlomků dostaneme nenulový zlomek (platí (1)), inverzí k nenulovému zlomku vzhledem k násobení je jeho převrácená hodnota (platí (4)) a Q^* je neprázdná.*

[13] Ve skutečnosti podmínka neprázdnosti je třetí podmínkou, která musí platit – uvidíme v důkazu, že z neprázdnosti a vlastnosti (4) už plyne vlastnost (3) o neutrálním prvku.

Generátory podgrupy

Uvažujme množinu $S = \{a, b, c\}$, která je podmnožinou grupy $(G, \bigtriangledown)$. Na to, abychom našli nejmenší možnou podgrupu, která obsahuje prvky a, b, c, musíme vyrobit všechny možné součiny těchto tří prvků a jejich inverzí[14], a nejen to: musíme brát všechny možné konečné sekvence prvků spojených operací $\bigtriangledown$, ve kterých se vyskytují (i opakovaně) prvky a, b, c a jejich inverze.

Typickými takto vytvářenými prvky jsou například

$$a \bigtriangledown b \bigtriangledown a \bigtriangledown c^{-1} \quad \text{nebo} \quad c^{-1} \bigtriangledown a^{-1} \bigtriangledown b \bigtriangledown b \bigtriangledown c.$$

Je jasné že součinem dvou prvků tohoto typu je zase prvek tohoto typu (tj. platí (1)): Například „součinem“ prvku $a \bigtriangledown b \bigtriangledown a$ a prvku $c \bigtriangledown b^{-1} \bigtriangledown a \bigtriangledown c$ je prvek

$$a \bigtriangledown b \bigtriangledown a \bigtriangledown c \bigtriangledown b^{-1} \bigtriangledown a \bigtriangledown c.$$

Dále jsou prvky tohoto typu uzavřené vzhledem k inverzi, tj. k prvku $a \bigtriangledown b^{-1} \bigtriangledown c^{-1} \bigtriangledown a$ je inverzí (podle věty 5.a bereme součin dílčích inverzních prvků v opačném pořadí) prvek

$$a^{-1} \bigtriangledown c \bigtriangledown b \bigtriangledown a^{-1}$$

(tedy platí i (4)). Dokázali jsme celkem, že množina prvků tohoto typu tvoří podgrupu grupy $(G, \bigtriangledown)$. Nazývá se

Definice 15 podgrupa grupy G **generovaná množinou** S, *prvky množiny* S *nazýváme* **generátory** *podgrupy* $< S >$.

Podgrupu generovanou podmnožinou S označujeme jako (označení 02) $< S >$. A ještě jedna definice, která s tím souvisí:

Definice 16 *Pokud podgrupa* $< S >$ *je celá generována některým svým prvkem* a, *nazývá se* **cyklická podgrupa** *grupy* G.

Cyklickou podgrupu generovanou prvkem a někdy označujeme (označení 03) $< a >$ a je jasné, že obsahuje prvky

$$a, \quad a^2 := a \bigtriangledown a, \quad a^3 := a \bigtriangledown a \bigtriangledown a, \ldots,$$

a také prvky

$$a^{-1}, \quad a^{-1} \bigtriangledown a^{-1}, \quad a^{-1} \bigtriangledown a^{-1} \bigtriangledown a^{-1}, \ldots,$$

a také prvek $n = a \bigtriangledown a^{-1}$.

Ad Příklad 1: Grupa $(H_6, +)$ s operací pootočení hodinové ručičky je příkladem cyklické grupy, generované jediným prvkem – kterým? □

[14] V této chvíli už se v daných součinech vyskytuje neutrální prvek $n \in G$, protože $a \bigtriangledown a^{-1} = n$.

Ad příklad 4: Ohledně generátorů grupy S_3 lze říci, že $(S_3, \circ)$ je generována dvěma svými prvky, a sice $(1,3)$ a $(1,2)$, protože všechny další čtyři prvky grupy lze vyjádřit pomocí operace $\circ$ a prvků $(1,3)$, $(1,2)$:

$$\begin{aligned} id &= (1,3)\circ(1,3); \\ (1,2,3) &= (1,3)\circ(1,2); \\ (1,3,2) &= (1,2,3)\circ(1,2,3) = ((1,3)\circ(1,2))^2 = ((1,3)\circ(1,2))\circ((1,3)\circ(1,2)); \\ (2,3) &= (1,2)\circ(1,2,3) = (1,2)\circ((1,3)\circ(1,2)). \end{aligned}$$

Podle označení množiny generátorů lze psát

$$(S_3, \circ) =< (1,3), (1,2) > .$$

Tato grupa tedy není cyklická, protože naše množina generátorů je dvouprvková a žádnou jednoprvkovou množinu generátorů v ní nelze najít. □

Věta 7 *$(S_n, \circ)$, množina permutací*[15] *$M \to M$ pro $M = \{1, 2, \ldots, n\}$ vzhledem k operaci skládání permutací je pro $n \geq 3$ nekomutativní grupa.*

Důkaz pro obecné n: Operace $\circ$ je na množině S_n uzavřená, tj. platí vlastnost (1), protože složení dvou permutací je opět permutace. Asociativita (2) platí pro skládání jakýchkoli zobrazení, viz příklad 3. Identické zobrazení id definované $\forall a \in \{1, 2, \ldots, n\}$ vztahem $id(a) = a$ je neutrálním prvkem na množině permutací, tj. platí (3): Pro obecnou permutaci $p : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$ totiž máme pro každné $a \in \{1, 2, \ldots, n\}$:

$$p \circ id(a) = p(a) \quad \wedge \quad id \circ p(a) = id(p(a)) = p(a).$$

Zbývá důkaz vlastnosti (4): V obecném případě $(S_n, \circ)$ permutací na n-prvkové množině $M = \{1, \ldots, n\}$ najdeme pro libovolnou permutaci $p \in S_n$ její inverzní prvek p^{-1} následujícím způsobem. Jelikož $p : M \to M$ je bijektivní zobrazení, podle věty 17 ze základů matematiky (inverzní relace k prostému zobrazení je také zobrazení) víme, že inverzní relace p^{-1} je zobrazením. Dále p je surjekce, tj. p^{-1} je definováno pro každé $a \in \{1, 2, \ldots, n\}$. Tedy pro bijekci p je p^{-1} také bijekce (v grafické reprezentaci relace pouze zaměníme směr všech šipek), a tedy permutace $\{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\}$.

A konečně pro $n \geq 4$ stačí najít jednu dvojici, pro kterou operace $\circ$ nekomutuje, a to je např. cyklus $(1, 2)$ a cyklus $(1, 2, \ldots, n)$:

$$(1,2)\circ(1,2,\ldots,n) = (2,3,n-1,n) \neq (1,2,\ldots,n)\circ(1,2) = (1,3,4,n-1,n).$$

Důkaz je hotov. □

Operace na cyklické podgrupě je vždy komutativní

[15] Pozor, prvky množiny S_n nejsou podmnožiny či jednotlivé prvky množiny M, ale zobrazení množiny M do sebe!! Jedná se už o složitější strukturu.

Navzdory patáliím nekomutativních operací existuje i v tabulkách nekomutativních operací jedna jistota a elegantní věc: Operace na cyklické podgrupě (= podgrupě generované jediným prvkem) H grupy G je komutativní, třebaže na celé grupě G tato operace komutativní být nemusí.

Například podgrupa $\{id, (1,2,3), (1,3,2)\}$ grupy $(S_3, \circ)$ je generovaná prvkem $(1,2,3)$, a tedy je to cyklická podgrupa, tj. cyklická grupa. Je vidět, že tabulka operace na $\{id, (1,2,3), (1,3,2)\}$ je symetrická, tj. operace je na ní komutativní.

Důkaz faktu, že operace na každé cyklické grupě je komutativní, je lehký – pokuste se o něj v rámci cvičení.

Názvy a vla stnosti algebraických struktur – příklady

Příklad 6 *Zopakujte vlastnosti (1) až (5) a přiřaďte názvy algebraických struktur k příkladům z minulé přednášky podle definic 1 až 8.*

Zmíněna vlastnost (6) = distributivita souhry dvou operací, na kterou se lze odkazovat jako na stranu 6.

Příklad 7 *Určete algebraické vlastnosti struktury* $(Z_6, \cdot)$.

– ještě před tímto příkladem uveďte větu o krácení v grupě, a pak upozorněte na neplatnost této věty o krácení v tomto příkladu (může k tomu dojít, protože se nejedná o grupu);

– ten systém rovnic x na druhou =b, x na pátou = é raději neopisujte, tuto část z přednášky vyřadím

3 Týden 03

3.1 Cvičení 03: Vlastnosti grup, podgrupy a generátory grupy

Úloha 3.1 *Příklady z Pinter 2010, str. 39, oddíl B:*

Například B.1: Dokažte, že v každé grupě platí následující implikace (e je neutrální prvek grupy), nebo uveďte protipříklad, že neplatí:

$$x^2 = e \quad \Rightarrow \quad x = e.$$

Například B.2: Dokažte, že v každé grupě platí následující implikace, nebo uveďte protipříklad, že neplatí:

$$x^2 = a^2 \quad \Rightarrow \quad x = a.$$

Například B.4: Dokažte, že v grupě platí následující implikace, nebo uveďte protipříklad, že neplatí (e je neutrální prvek grupy):

$$x^2 = x \quad \Rightarrow \quad x = e.$$

Například B.5: Dokažte, že v grupě platí následující fakt, nebo uveďte protipříklad, že neplatí:

$$\forall x \in G \ \exists \ y \in G \ : \ x = y^2$$

(tj. každý prvek x má v grupě svou „odmocninu“ y).

Úloha 3.2 *Příklady z Pinter 2010, str. 40, oddíl E: počet prvků a jejich inverzí – výborné příklady.*

Úloha 3.3 *Příklady z Pinter 2010, str. 41, oddíl F: vytváření tabulky operace pro grupy s malým počtem prvků – např.:*

Například F.2: Může v grupě $(G, \star)$ nastat situace, že v tabulce její operace se dvakrát opakuje stejný prvek na jednom řádku?

$\star$	...	x_1	...	x_2	...
...		...		...	
a	...	y	...	y	...
...		...		...	

Zdůvodněte, proč ano - proč ne.

Například F.3: $M = \{e, a, b\}$. Doplňte tabulku operace $\star$

$\star$	e	a	b
e	e	a	b
a	a		
b	b		

tak, aby $(M, \star)$ byla grupa.

Například F.4: Čtyřprvková grupa $G = \{e, a, b, c, \}$ splňuje $\forall x \in G : \quad x^2 = e$ (kde e je její neutrální prvek). Sestavte tabulku operace $*$ této grupy:

$*$	e	a	b	c
e				
a				
b				
c				

Například F.5: Čtyřprvková grupa $G = \{e, a, b, c, \}$ splňuje $a^2 = e$, $b^2 \neq e$ (kde e je její neutrální prvek). Sestavte tabulku operace $*$ této grupy:

$*$	e	a	b	c
e				
a				
b				
c				

Úloha 3.4 *(text Pinter 2010, str. 42, oddíl G): Dokažte, že kartézský součin grup* $(G, \bigtriangledown)$ *a* $(H, *)$ *je grupa* $(G \times H, \square)$ *– jak definovat operaci* $\square$*?*

Úloha 3.5 *Příklady z Pinter 2010, str. 43, oddíl H: mocniny a odmocniny v grupě – výborné příklady.*

Například H.0: a) zopakujte si definici n-té mocniny a n-té odmocniny v grupě. b) Jak byste definovali v grupě zápornou mocninu a^{-5} *pro nějaký prvek a?*

Úloha 3.6 *Příklady z Pinter 2010, str. 48, oddíl A: rozeznání podgrupy – výborné příklady.*

Například A.1: $G = (R, +)$ je grupa vzhledem k běžné operaci sčítání. Je $H = \{\log a; a \in Q, a > 0\}$ podgrupou grupy G vzhledem ke stejné operaci? Zdůvodněte.

Například A.5: $G = (R \times R, +)$ je grupa vzhledem k běžné operaci sčítání vektorů. Je $H = \{(x, y); y = 2x\}$ podgrupou grupy G vzhledem ke stejné operaci? Zdůvodněte.

Například D.5 na str. 50: $(G, \star)$ je konečná grupa, H její neprázdná podmnožina uzavřená vzhledem k operaci $\star$, a navíc $e \in H$, kde e je jednotkový prvek grupy G. Dokažte, že pro $a \in H$ také $a^{-1} \in H$ (tj. H je uzavřená vzhledem k inverzím).

Nápověda k důkazu : $H = \{a_1, a_2, \ldots, a_n\}$ a vyberme si libovolné $a_i \in H$. Uvažujme nyní navzájem RŮZNÉ prvky $a_i \star a_1$, $a_i \star a_2$, $\ldots$, $a_i \star a_n$: atd.

Úloha 3.7 *Příklady z Pinter 2010, str. 50, oddíl E: generátory grupy – výborné příklady.*

Například N.1 (není v textu Pinter 2010): Vypište všechny prvky podgrupy $< 6 >$ grupy $(H_{16}, +)$ = grupy všech pootočení ručičky o jednu šestnáctinu plného úhlu.

Například E.1: Vypište všechny cyklické podgrupy grupy $(H_{10}, +)$ skládání otáčení hodinové ručičky o násobky desetiny plného úhlu.

Například E.3: Vypište všechny prvky podgrupy $< 6, 9 >$ grupy $(H_{12}, +)$.

Například E.7 – modifikace[16]: V grupě $H_2 \times H_4$ je operace sčítání po složkách zadaná tabulkou

Tabulka 3.3: Tabulka operace $+$ na množině $H_2 \times H_4$.

$+$	$[0;0]$	$[0;1]$	$[0;2]$	$[0;3]$	$[1;0]$	$[1;1]$	$[1;2]$	$[1;3]$
$[0;0]$	$[0;0]$	$[0;1]$	$[0;2]$	$[0;3]$	$[1;0]$	$[1;1]$	$[1;2]$	$[1;3]$
$[0;1]$	$[0;1]$	$[0;2]$	$[0;3]$	$[0;0]$	$[1;1]$	$[1;2]$	$[1;3]$	$[1;0]$
$[0;2]$	$[0;2]$	$[0;3]$	$[0;0]$	$[0;1]$	$[1;2]$	$[1;3]$	$[1;0]$	$[1;1]$
$[0;3]$	$[0;3]$	$[0;0]$	$[0;1]$	$[0;2]$	$[1;3]$	$[1;0]$	$[1;1]$	$[1;2]$
$[1;0]$	$[1;0]$	$[1;1]$	$[1;2]$	$[1;3]$	$[0;0]$	$[0;1]$	$[0;2]$	$[0;3]$
$[1;1]$	$[1;1]$	$[1;2]$	$[1;3]$	$[1;0]$	$[0;1]$	$[0;2]$	$[0;3]$	$[0;0]$
$[1;2]$	$[1;2]$	$[1;3]$	$[1;0]$	$[1;1]$	$[0;2]$	$[0;3]$	$[0;0]$	$[0;1]$
$[1;3]$	$[1;3]$	$[1;0]$	$[1;1]$	$[1;2]$	$[0;3]$	$[0;0]$	$[0;1]$	$[0;2]$

Určete, jakou podgrupu generuje prvek $[1;1]$.

Například E.6: Sestavte tabulku operace grupy $(H_2 \times H_3)$ vzhledem k operaci sčítání po složkách. A druhý úkol: dokažte o této grupě, že je cyklická.

Například N.3: Zjistěte, zda je grupa z příkladu E.7 cyklická, a pokud ne, tak najděte nějakou minimální množinu jejích generátorů (existuje nějaké dva prvky, které už generují celou tuto grupu?).

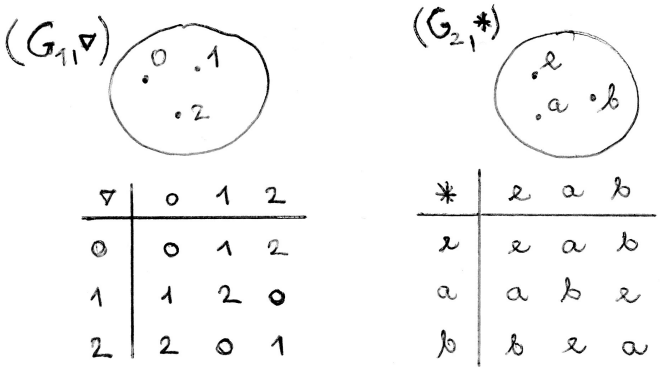
Výsledky některých cvičení najdete v závěru textu v oddílu 13.3.

[16] Jediný důvod, proč je příklad E.7 před příkladem E.6 je historický – E.7 byl nejprve podrobně napsán na písemce. U příkladu E.6 se pak očekává, že si čtenář sestaví při řešení tabulku operace na součinu grup sám.

3.2 Přednáška 3: Izomorfismus, Calyeho věta

V 18. a 19. století, když se formovaly termíny českého překladu předmětu algebra, byl jedním z návrhů českého překladu slova algebra termín „stejnostka“ neboli nauka o stejnostech[17]. I když se tento český překlad neujal, vystihuje snahy moderní algebry všímat si shodných či podobných vlastností různých objektů.

Ve shodě s navrhovaným starým překladem názvu tohoto předmětu nyní budeme zkoumat pojem izomorfismu. Lapidárně řečeno, dva objekty jsou izomorfní, když mají tutéž strukturu. I řecké slovo izomorfismus je podobného obsahu (isos = stejný, morfé = tvar, tj. izomorfní budou objekty, které mají možná jinou podstatu, ale v jistém smyslu stejný tvar).



$\triangledown$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$*$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Obrázek 3.2: Dvě izomorfní grupy.

V této kapitolce se budeme zejména zabývat „stejností“ vzhledem k pojmu binární operace – protože operace je něco dynamického, kdy dvěma prvkům podle jistého předpisu přiřazujeme třetí prvek, tedy stejnost (či podobnost), která nás bude zajímat, je dána tabulkou výsledků operace na dané množině[18]. Na obrázku 3.2 vidíme tabulky operace dvou tříprvkových grup, které jsou izomorfní – existuje mezi nimi totiž bijekce

$$\begin{pmatrix} 0 & 1 & 2 \\ \downarrow & \downarrow & \downarrow \\ e & a & b \end{pmatrix},$$

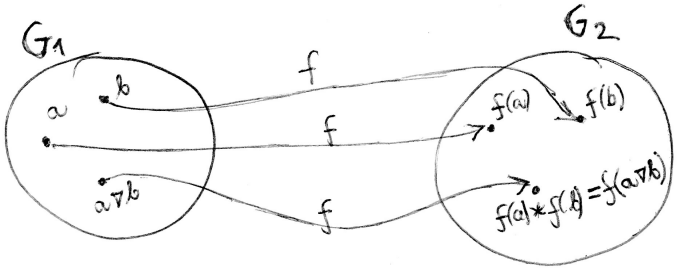
ale nejen to – tato bijekce v jistém smyslu „zachovává výsledky operace“, tj. např. prvek $1 \triangledown 2$ z grupy G_1, což lze v tabulce operace $\triangledown$ grupy G_1 najít, že je roven 0, odpovídá v navrhované bijekci prvku e v grupě G_2, který je výsledkem operace $a * b$, kde a je obraz prvku 1 a b je obraz prvku 2, TEDY platí $a * b = e$. Toto zachování výsledků operace musí platit pro každou dvojici prvků z G_1 (v daném pořadí).

[17] Viz Alena Šolcová, přednáška o Cestách k české terminologii v některých partiích matematiky, Katedra matematiky Pdf, 14. března 2018.

[18] Tedy izomorfismus je v případě zachování výsledků operace vlastností poněkud skrytou – poznáme ji až podrobnějším studiem tabulky operace na obou strukturách.

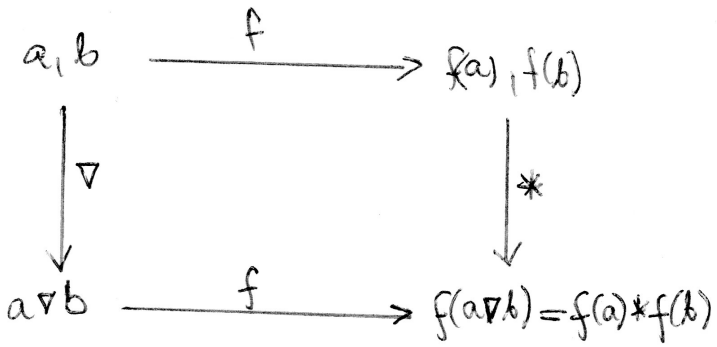
Definice 17 *Izomorfismus grupy* $(G_1, \triangledown)$ *na grupu* $(G_2, *)$ *je bijekce* $f : G_1 \to G_2$, *která splňuje vlastnost*

$$\forall a, b \in G_1 : \quad f(a \triangledown b) = f(a) * f(b).$$



Obrázek 3.3: Podmínka zachování výsledků operace při zobrazení f.

Jinými slovy (viz obrázek 3.3, izomorfismus mezi grupami je taková bijekce $f : G_1 \to G_2$, při které jsou $f(a \triangledown b)$ a $f(a) * f(b)$ tytéž prvky, pro jakoukoli dvojici prvků a, b.



Obrázek 3.4: Komutativní diagram pro podmínku zachování výsledků operace.

A nebo ještě jinak, říkáme, že izomorfismus f mezi grupami je bijekce, pro kterou diagram na obrázku 3.4 komutuje, neboli když vypustíme na prvky a, b z „ohrady“ G_1 operaci $\triangledown$, a pak výsledek přeneseme (zobrazením f) do „ohrady“ G_2, dosáhneme stejného výsledku, jako když bychom nejprve přenesli oddělené prvky a, b zobrazením f do „ohrady“ G_2 a tam na ně vypustili operaci $*$[19].

Příklad 8 $(R, +)$ *a* $(R^+, \cdot)$ *jsou izomorfní grupy, pokud definujeme zobrazení* $R \to R^+$ *vztahem* $f(x) = e^x$. *Snadno se vidí, že zobrazení* f *je injekce, protože nenabývá dvou*

[19]Diagram komutuje = nezáleží na pořadí: operace následovaná zobrazením dává tentýž výsledek jako zobrazení následované operací, pokud vždy mluvíme o binární operaci na té množině, ve které se dané dva prvky vyskytují.

stejných hodnot pro dvě různá $x_1, x_2 \in R$. Dále je f surjekce R na R^+ – pro každé $y \in R^+$ existuje $x \in R$ tak, že $e^x = y$. Celkem tedy f je bijekce. Dále podmínka zachování výsledků operace nyní má vzhledem k zadaným operacím tvar

$$f(a+b) = f(a) \cdot f(b).$$

Tato podmínka také platí, protože

$$e^{a+b} = e^a \cdot e^b.$$

Celkem f je grupovým izomorfismem.$\star$

Při hledání odpovědi na otázku, zda jsou dvě různé grupy izomorfní, musíme tedy projít tři kroky: a) definovat zobrazení $f : G_1 \to G_2$; b) dokázat o tomto zobrazení, že je injektivní a surjektivní, a tedy bijekce; c) dokázat, že platí vlastnost zachování výsledků operace.

Pokud jsou dvě grupy izomorfní, tak chování operace na té druhé je přesnou kopií chování operace na první grupě. Tedy pokud první grupa $(G_1, \bigtriangledown)$ má vlastnost, kterou grupa $(G_2, *)$ nemá, nemohou být tyto grupy izomorfní. Například

- G_1 je komutativní, ale G_2 ne.
- G_1 má nějaký prvek, který je inverzí sebe sama, ale G_2 takový prvek nemá.
- G_1 je generována dvěma svými prvky, ale G_2 není generována žádnou dvojicí svých prvků.
- Atd., možná více viz cvičení.

Před více než 100 lety dokázal Arhur Cayley větu, kterou se nyní budeme zabývat: *Každá grupa* (libovolná, konečná i nekonečná, komutativní i nekomutativní) *je izomorfní nějaké podgrupě grupy permutací* (ty byly představeny v minulé kapitole). Tento výsledek je revolučním ve studiu grup, protože vlastně tvrdí, že žádné jiné grupy (až na přeznačení prvků) než grupy permutací vlastně neexistují!!! A o to více je tento výsledek revoluční ve studiu operací – tvrdí totiž, že na grupách neexistuje žádná jiná operace než operace skládání permutací!!!! Jinými slovy, pomocí operace SKLÁDÁNÍ PERMUTACÍ lze reprezentovat jakékoli další operace na grupách, tj. sčítání, násobení, atd.

Věta 8 *(Cayley) Každá grupa $(G, \bigtriangledown)$ je izomorfní nějaké grupě permutací.*

Důkaz: dokážeme ve třech krocích:

1. Ke každému prvku $a \in G$ vytvoříme permutaci $\pi_a : G \to G$ (a dokážeme, že se jedná o permutaci G, tedy o bijekci).

2. O množině těchto permutací

$$G^* := \{\pi_a; a \in G\}$$

dokážeme, že je podgrupa grupy S_G všech permutací množiny G (= grupy všech bijekcí $G \to G$).

3. Definujeme zobrazení $f : G \to G^*$ a dokážeme o něm, že je izomorfismus mezi grupami.

Tak pojďme na to!!

Důkaz podrobněji:

1. **Ke každému prvku $a \in G$ vytvoříme permutaci $\pi_a : G \to G$ (a dokážeme, že se jedná o permutaci G, tedy o bijekci).**

Definujme pro libovolný prvek $a \in G$ zobrazení π_a definované vztahem

$$\forall x \in G : \pi_a(x) := a \bigtriangledown x$$

(zobrazení π_a zobrazí každé $x \in G$ na prvek $a \bigtriangledown x \in G$). Dokažme o π_a, že se jedná o bijekci:

- π_a je injekce $G \to G$: Předpokládejme, že $\pi_a(x_1) = \pi_a(x_2)$ – to by znamenalo podle definice zobrazení π_a, že

$$a \bigtriangledown x_1 = a \bigtriangledown x_2,$$

a protože v grupě platí vlastnost (7), můžeme vykrátit po vynásobení rovnosti prvkem a^{-1} zleva a dostaneme $x_1 = x_2$ ... tedy rovnost hodnot zobrazení π_a může nastat jen pro tentýž prvek $x_1 = x_2$, a tedy f je injekce.

- π_a je surjekce G na G: Pro libovolný prvek $y \in G$ musíme najít jeho vzor vzhledem k zobrazení π_a – jakmile najdeme aspoň jeden vzor, budeme vědět, že jedná se o surjekci, protože všechny prvky $y \in G$ by pak byly pokryty nějakými vzory vzhledem k zobrazení f. Odpověď: hledaný vzor z G je prvek $a^{-1} \bigtriangledown y$, pak totiž

$$\pi_a(a^{-1} \bigtriangledown y) = a \bigtriangledown a^{-1} \bigtriangledown y = y.$$

- Celkem π_a je bijekce.

2. **O množině těchto permutací**

$$G^* := \{\pi_a; a \in G\}$$

dokážeme, že je podgrupa grupy S_G všech permutací množiny G (= grupy všech bijekcí $G \to G$).

G^* je podmnožinou grupy S_G všech permutací na $G \to G$. Dokážeme o G^*, že je podgrupa:

- $G*$ je neprázdná, nejmenší možná grupa G je totiž minimálně jednoprvková (obsahuje neutrální prvek e), a tedy minimálně $\pi_e(x) := e \bigtriangledown x$ je identická permutace, která náleží do G^*.
- $(G^*, \circ)$ splňuje vlastnost (1), tedy pro dvě různé permutace π_a, π_b musíme najít prvek $c \in G$, že $\pi_c = pi_a \circ \pi_b$. Skutečně to platí – pokud vezmeme $c := a \bigtriangledown b$, potom

  $$\pi_{a \bigtriangledown b} = \pi_a \circ \pi_b.$$

  Podrobněji rozepsáno,

  $$\forall x \in G: \quad \pi_{a \bigtriangledown b}(x) = (a \bigtriangledown b) \bigtriangledown x = a \bigtriangledown (b \bigtriangledown x) = a \bigtriangledown \pi_b(x) = \pi_a(\pi_b(x)) = (\pi_a \circ \pi_b)(x).$$

  Tedy složením dvou prvků π_a a π_b z G^* je zase prvek z G^*, tj. množina G^* je uzavřená vzhledem k operaci $\circ$.
- $(G^*, \circ)$ splňuje vlastnost (4): Stačí dokázat, že ke každému $\pi_a \in G^*$ existuje inverzní permutace vzhledem ke skládání permutací: A to opravdu existuje, je to totiž permutace $\pi_{a^{-1}}$ odpovídající prvku $a^{-1} \in G$ – pak platí (podle vlastnosti (1) je složením permutací permutace odpovídající „násobku“ obou dílčích prvků)

  $$\pi_a \circ \pi_{a^{-1}} = \pi_{a \bigtriangledown a^{-1}} = \pi_e.$$

- Tedy celkem G^* je neprázdná a splňuje vlastnosti (1) a (4) – podle věty 6 je G^* podgrupa grupy S_G, a tedy hlavně sama $(G^*, \circ)$ je grupou.

3. **Definujeme zobrazení $f : G \to G^*$ a dokážeme o něm, že je izomorfismus mezi grupami.**

   - Jako zobrazení f se nabízí přiřazení, o kterém už dlouho mluvíme: prvku $a \in G$ přiřadíme jím definovanou permutaci $\pi_a \in G^*$, neboli

     $$f(a) = \pi_a.$$

   - f je injekce: Pokud $f(a) = f(b)$, znamená to, že $\pi_a = \pi_b$, tedy

     $$\forall x \in G: \quad \pi_a(x) = \pi_b(x);$$

     a tak i speciálně pro jednotku $e \in G$ platí $\pi_a(e) = \pi_b(e)$, což znamená

     $$a \bigtriangledown e = b \bigtriangledown e,$$

     to ale znamená, že $a = b$. Rovnost obrazů si vynucuje rovnost vzorů, tedy f je injekce.
   - f je surjekce: Tato vlastnost je zaručena už tím, jak je množina G^* vytvořena: jsou do ní vybírány jen ty permutace π_a, které odpovídají prvku $a \in G$, tj. každá permutace π_a má svůj vzor $a \in G$ vzhledem k zobrazení f.

- f zachovává výsledky operace: chceme dokázat podmínku

$$\forall a, b \in G: \quad f(a \bigtriangledown b) = f(a) \circ f(b),$$

a tu snadno dokážeme rozepsáním podle definice zobrazení f a vlastnosti (1) pro skládání permutací:

$$f(a \bigtriangledown b) = \pi_{a \bigtriangledown b} \overset{(1)}{=} \pi_a \circ \pi_b = f(a) \circ f(b).$$

- Celkem f je izomorfismus grupy $(G, \bigtriangledown)$ na grupu $(G^*, \circ)$.

Příklad 9 *Kniha Pinter 2010, str. 97-102, opět poskytuje řadu cvičení na pojem izomorfismu:*

Například C.3: Zjistěte, zda je grupa $2^{\{a,b\}}$ s operací symetrického rozdílu $\div$ (stejná operace jako v úloze 1.6) izomorfní s grupou $(V, \cdot)$, kde $V = \{1, -1, i, -i\}$ a $\cdot$ je operace násobení komplexních čísel. Své zjištění zdůvodněte.

Například D.1: Prozkoumejte grupy a) $(H_4, +)$; b) $(H_2 \times H_2, +)$ (sčítání definováno po složkách po složkách); c) grupu komplexních jednotek $(V, \cdot)$, kde $V = \{1, -1, i, -i\}$ a $\cdot$ je operace násobení komplexních čísel. Které dvě z nich jsou izomorfní, a proč ta třetí s nimi není izomorfní?

Například D.2: Viz cvičení 05, kde budou zhruba probrány grupy zbytkových tříd.

(cvičení sady G): Izomorfní grupy na množině reálných čísel.

(cvičení sady J): Regulární reprezentace grupy – rychlá konstrukce podgrupy grupy S_n, která je s grupou G izomorfní!!

4 Týden 04

4.1 Cvičení 04: Nekomutativní grupy

Úloha 4.1 *Jsou dány permutace*

$$P = (1, 5, 6, 2, 3), \quad R = (1, 7, 5, 4, 3, 6, 2).$$

Vypočtěte $P \circ R^2$ (výsledek najdete na konci tohoto textu).

Úloha 4.2 *Kniha Pinter 2010, str. 75, oddíl B, příklady na grupy permutací.*

Například B.2: Vypište prvky cyklické podgrupy grupy $(S_6, \circ)$ generované prvkem

$$f = (1, 2, 3, 4) \circ (5, 6).$$

Například B.3: Najděte čtyřprvkovou komutativní podgrupu grupy $(S_5, \circ)$ a napište její tabulku operace.

Například B.4: Podgrupa grupy $(S_5, \circ)$ generovaná prvky

$$f = (1, 2), \quad g = (3, 4, 5)$$

má šest prvků. Vypište tyto prvky, označte je e, f, g, h, i, j a sestavte tabulku operace $\circ$.

Například N.1: Podgrupa grupy $(S_4, \circ)$ generovaná prvky

$$f = (1, 3) \circ (2, 4), \quad g = (3, 4)$$

má osm prvků. Najděte je všechny. Může vám pomoci vytváření tabulky operace $\circ$, ale nemusíte ji dělat celou.

Například N.2: Vypište všechny prvky cyklické podgrupy grupy $(S_7, \circ)$ generované prvkem

$$f = (1, 3) \circ (4, 5, 7).$$

Například N.3: Grupa $(S_4, \circ)$ má 24 prvků. Najděte nějakou její osmiprvkovou podgrupu – vypište podrobně zbylých sedm prvků kromě neutrálního prvku. Může vám pomoci vytváření tabulky operace $\circ$, ale nemusíte ji dělat celou.

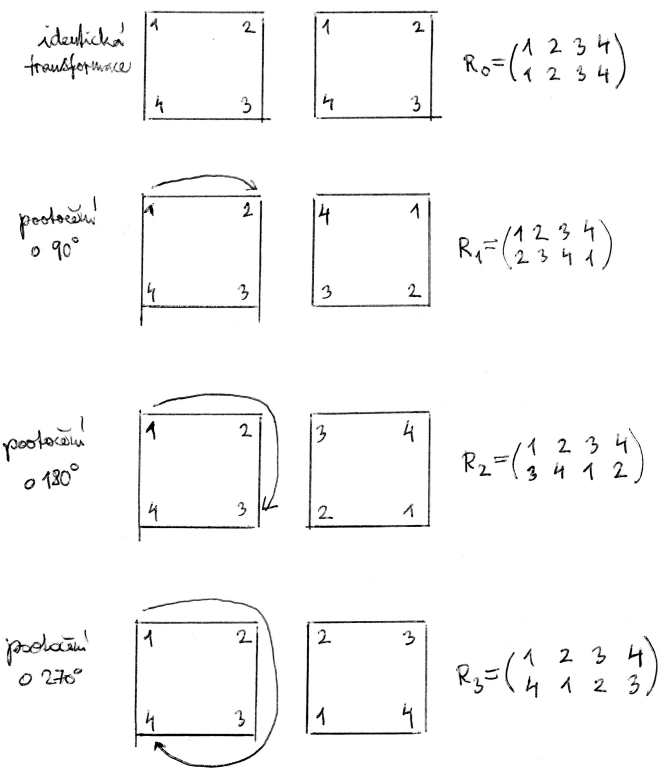
Úloha 4.3 *(ad Pinter 2010, str. 77, sada F) na grupu symetrií pravidelného n-úhelníka: Grupa symetrií čtverce (příklad je zde podrobně rozebrán, ale možná, že bude třeba se studenty projít ještě příklad na symetrie trojúhelníka z přednášky 1 a připomenout celou problematiku).*

Uvažujme čtverec a takové jeho transformace, že po jejich provedení dostaneme zase čtverec se stranami rovnoběžnými s vertikálním a horizontálním směrem. Mám na mysli pootočení čtverce (se středem otáčení ve středu čtverce) o násobky $90°$ (ty jsou čtyři, a sice pootočení o $0°$, o $90°$, o $180°$ a o $270°$), a ještě překlopení čtverce v osové souměrnosti

podle navzájem symetrických os (ty jsou též čtyři pro osy otáčení v obou úhlopříčkách čtverce a ve dvou osách procházejících středy protějších stran čtverce). Použitím některé z těchto osmi transformací na čtverec dostaneme zase nějakou pozici čterce, která vznikne ze základní polohy uplatněním jedné dílčí transformace, tj. množina těchto osmi transformací (= přeměn ve smyslu osového překlopení či ve smyslu pootočení čtverce) tvoří grupu.

Jak nyní dojdeme k permutaci přirozených čísel? Například tak, že do rohů základní polohy čtverce umístíme čísla $1, 2, 3, 4$. A po provedení dané transformace zapíšeme permutaci těchto čtyř čísel vzhledem k základní poloze. Pak identické transformaci (při které se neděje nic) odpovídá permutace $R_0 = id$, pootočení o 90° odpovídá permutace $R_1 = (1, 2, 3, 4)$ (v tom smyslu, že číslo 1 se pootočením dostalo na pozici čísla 2, číslo 2 se na pozici čísla 3, číslo 3 na 4 a číslo 4 na pozici 1). Podobně pootočení o 180° odpovídá permutace $R_2 = (1, 3) \circ (2, 4)$[20] a pootočení o 270° permutace $R_3 = (1, 4, 3, 2)$[21].

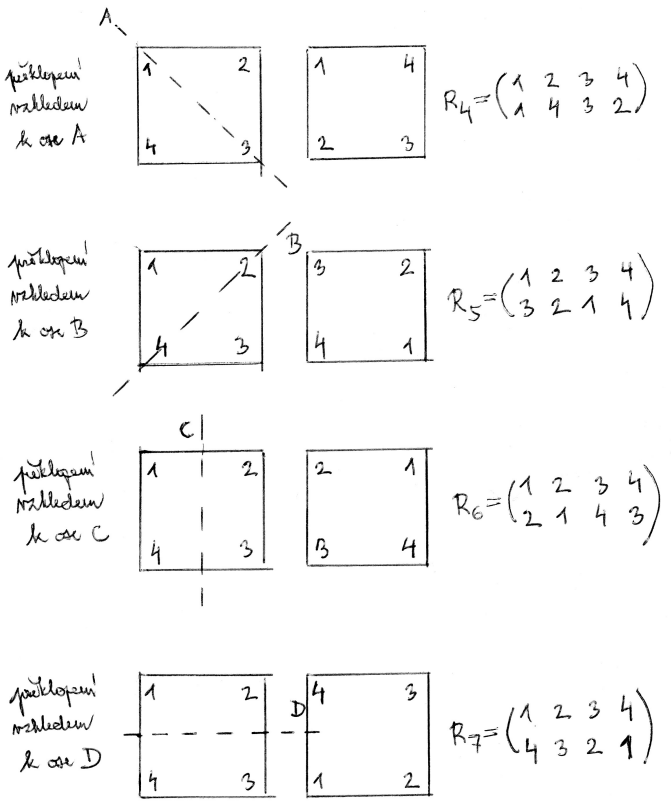
(podrobněji viz obrázek 4.5).



Obrázek 4.5: Permutace odpovídající pootočení čtverce.

[20]Pozor, tuto permutaci nelze lépe označit než spojením dvou disjunktních cyklů délky 2, protože dochází ke dvěma nezávislým prohozením během jedné permutace.

[21]Což je totéž jako $(4, 3, 2, 1)$, ale začínáme při zápisu nejmenším možným číslem, abychom se vyznali ve výsledcích operací a podle pozice nejmenšího čísla poznali jednoznačně daný prvek.



Obrázek 4.6: Permutace odpovídající osové symetrii čtverce.

Podobně dostaneme permutace odpovídající přeměně čísel ve vrcholech čtverce při osové souměrnosti vzhledem ke čtyřem hlavním osám souměrnosti, viz obrázek 4.6.

Skládáním $R_1 \circ R_4$ například dostaneme

$$R_1 \circ R_4 = (1,2,3,4) \circ (2,4) = (1,2) \circ (3,4) = R_6,$$

atd. Vyplněním operace pro každou dvojici prvků v obou pořadích (operace je opět nekomutativní, protože např. $R_4 \circ R_1 = R_7$) dostaneme tabulku grupy $(D_4, \circ)$ symetrií čtverce, která odpovídá podgrupě grupy permutací s osmi prvky (viz tabulka 4.4). Všech permutací čtyřprvkové množiny je 24; tedy naše osmiprvková množina je podgrupou grupy S_4.

Pro každé přirozené $n \geq 3$ lze sestrojit grupu symetrií pravidelného n-úhelníku a označit ji D_n vzhledem k operaci skládání zobrazení. Například D_5 označuje grupu symetrií pětiúhelníku, atd. Každému rovinnému útvaru, který je pravidelný vzhledem k otáčení nebo osové souměrnosti, lze přiřadit jistou grupu symetrií. Grupy symetrií se široce používají v teorii elektronové struktury a molekulárních vibrací. V elementární částicové fyzice byly tyto grupy symetrii využity k předpovězení existence částic, které ještě ani nebyly experimentálně zjištěny! Proto i studium nekomutativních grup má svoje

místo v algebře.

Tabulka 4.4: Tabulka operace $\circ$ na množině D_4 symetrií čtverce.

$\circ$	R_0	R_1	R_2	R_3	R_4	R_5	R_6	R_7
R_0	R_0	R_1	R_2	R_3	R_4	R_5	R_6	R_7
R_1	R_1	R_2	R_3	id	R_6	R_7	R_5	R_4
R_2	R_2	R_3	R_0	R_1	R_5	R_4	R_7	R_6
R_3	R_3	R_0	R_1	R_2	R_7	R_6	R_4	R_5
R_4	R_4	R_7	R_5	R_6	R_0	R_2	R_3	R_1
R_5	R_5	R_6	R_4	R_7	R_2	R_0	R_1	R_3
R_6	R_6	R_4	R_7	R_5	R_1	R_3	R_0	R_2
R_7	R_7	R_5	R_6	R_4	R_3	R_1	R_2	R_0

Úkol: Najděte všechny inverzní prvky a všechny podgrupy v grupě D_4.

Úloha 4.4 *Dva úkoly pro grupu permutací $(S_3, \circ)$ (použijte prosím označení prvků a tabulku operace $\circ$ v příkladu 4): a) dokažte, že $(S_3, \circ)$ není cyklická grupa;*
b) najděte dvouprvkovou podmnožinu grupy, která generuje celou grupu $(S_3, \circ)$.

Úloha 4.5 *Pokud bude čas, je možné se zabývat některými dalšími vlastnostmi permutací (ad Pinter 2010, kapitola 8): Každou permutaci lze rozložit na součin cyklů, každý cyklus lze rozložit na součin transpozic. Sudá a lichá permutace podle počtu transpozic. Ale to spíše až do předmětu Algebra 2 (lineární algebra).*

Výsledky některých cvičení najdete v závěru textu v oddílu 13.4.

4.2 Přednáška 04: Lagrangeova věta, homomorfismus grup, faktorgrupa

V dnešním oddílu budeme potřebovat znalosti o pojmu ekvivalence (relace reflexivní, symetrická a tranzitivní) a pojmu rozklad určený ekvivalencí (v jedné třídě rozkladu jsou právě ty prvky množiny M, které jsou navzájem v relaci příslušné ekvivalence) – viz předmět Základy matematiky. Jen zde připomeňme, že rozklad množiny M na systém podmnožin $M_1, M_2, \ldots, M_k$ je takový systém podmnožin, které jsou a) neprázdné, b) po dvou disjunktní (každé dvě různé množiny mají prázdný průnik) a c) jejich sjednocením je celá množina M – někdy se takovému systému podmnožin říká též disjunktní pokrytí,

tj. je to systém po dvou disjunktních podmnožin, který pokrývá celou množinu M v tom smyslu, že $\bigcup M_i = M$.

Přidejme nyní navíc k předmětu Základy matematiky:

- Pro důkaz jednoho zajímavého tvrzení (věty 17) nám bude stačit si uvědomit, že pokud dvě třídy rozkladu M_i, M_j mají neprázdný průnik, pak se musí rovnat, čili $M_i = M_j$ a jedná se o tutéž třídu. Lze tedy rozklad množiny M na podmnožiny M_i definovat i následovně:
  - $\forall i \in \{1, 2, \ldots, k\} : \quad M_i \neq \emptyset$;
  - $a \in M_i \cup M_j \Rightarrow M_i = M_j$;
  - každý prvek $a \in M$ leží v jedné třídě rozkladu.
- Označení 04: Znak $\sim$ bude značit relaci ekvivalence určenou daným rozkladem, tj. $a \sim b$ právě tehdy, když $a, b \in M_i$ pro nějaké i.
- Označení 05: Označme dále $[a]$ tu třídu rozkladu, která obsahuje prvek a, tedy podmínku z označení 07 budeme psát ve tvaru

$$a \sim b \quad \Leftrightarrow \quad [a] = [b].$$

Někdy se matematické výsledky dostavují zajímavým a překvapujícím způsobem. Při studiu pojmu grupa, tj. pojmu binární operace $\bigtriangledown$, která na množině M splňuje čtyři axiomy známé z operací sčítání a násobení racionálních čísel, jsme se zatím dostali ke Cayleyho větě, která je svým způsobem šokující: každou operaci v grupě lze reprezentovat operací skládání permutací na nějaké grupě permutací. K dalšímu zajímavému, a snad i nečekanému výsledku dojdeme nyní, když budeme přemýšlet o pojmu tzv. třídy prvku vzhledem k podgrupě.

Definice 18 *$\forall a$ z grupy $(G, \bigtriangledown)$ a její podgrupu $(H, \bigtriangledown)$ lze definovat:*

levá třída prvku $a \in G$ vzhledem k podgrupě H je množina

$$a \bigtriangledown H := \{a \bigtriangledown h \in G : h \in H\}$$

(množina výsledků operace $a \bigtriangledown h$, kde prvek $a \in G$ je pevné a prvek h probíhá podgrupu H);

podobně pravá třída prvku $a \in G$ vzhledem k podgrupě H je množina

$$H \bigtriangledown a := \{h \bigtriangledown a \in G : h \in H\}$$

(množina výsledků operace $h \bigtriangledown a$, kde prvek $a \in G$ je pevné a prvek h probíhá podgrupu H).

Pojmy levá a pravá třída prvku splývají jen tehdy, pokud $\bigtriangledown$ je komutativní operace, jinak ne. Dříve, než půjdeme dále, musíme se podívat na nějaký příklad tříd prvku vzhledem k podgrupě:

Příklad 10 *Pro grupu* $G = (H_4, +) = (Z_4, +) = (\{0, 1, 2, 3, \}, +)$ *a podgrupu* $H = (\{0, 2\})$ *dostáváme následující levé třídy prvků podle podgrupy:*

- *levá třída prvku* 0 *vzhledem k* H *je* $0 + H = \{0, 2\} = H = H + 0$ *(tedy levá třída prvku* 0 *je rovná pravé třídě prvku* 0*);*
- *levá třída prvku* 2 *vzhledem k* H *je* $2 + H = \{0, 2\} = H = H + 2$ *(tedy levá třída prvku* 2 *je rovná pravé třídě prvku* 2*);*
- *levá třída prvku* 1 *vzhledem k* H *je* $1 + H = \{1, 3\} = H + 1$ *(tedy levá třída prvku* 1 *je rovná pravé třídě prvku* 1*);*
- *levá třída prvku* 3 *vzhledem k* H *je* $3 + H = \{1, 3\} = H + 3$ *(tedy levá třída prvku* 3 *je rovná pravé třídě prvku* 3*);*

Příklad 11 *Pro grupu* $G = (S_3, \circ)$ *permutací z příkladu 4 a podgrupu* $H = (\{id, (1, 2, 3), (1, 3, 2)\})$ *dostáváme následující levé třídy prvků podle podgrupy (viz tabulka operace* $\circ$ *u příkladu 4):*

- *levá třída prvku* id *vzhledem k* H *je* $id \circ H = \{id, (1, 2, 3), (1, 3, 2)\} = H = H \circ id$ *(tedy levá třída prvku* id *je rovná pravé třídě prvku* id *vzhledem k operaci* $\circ$*);*
- *levá třída prvku* $(1, 2, 3)$ *vzhledem k* H *je* $(1, 2, 3) \circ H = \{id, (1, 2, 3), (1, 3, 2)\} = H = H \circ (1, 2, 3)$ *(tedy levá třída prvku* $(1, 2, 3)$ *je rovná pravé třídě prvku* $(1, 2, 3)$*);*
- *levá třída prvku* $(1, 3, 2)$ *vzhledem k* H *je* $(1, 3, 2) \circ H = \{id, (1, 2, 3), (1, 3, 2)\} = H \circ (1, 3, 2)$ *(tedy levá třída prvku* $(1, 3, 2)$ *je rovná pravé třídě prvku* $(1, 3, 2)$*);*
- *levá třída prvku* $(2, 3)$ *vzhledem k* H *je* $(2, 3) \circ H = \{(2, 3), (1, 3), (1, 2)\} = H \circ (2, 3)$ *(tedy levá třída prvku* $(2, 3)$ *je rovná pravé třídě prvku* $(2, 3)$*);*
- *levá třída prvku* $(1, 3)$ *vzhledem k* H *je* $(1, 3) \circ H = \{(2, 3), (1, 3), (1, 2)\} = H \circ (1, 3)$ *(tedy levá třída prvku* $(1, 3)$ *je rovná pravé třídě prvku* $(1, 3)$*);*
- *levá třída prvku* $(1, 2)$ *vzhledem k* H *je* $(1, 2) \circ H = \{(2, 3), (1, 3), (1, 2)\} = H \circ (1, 2)$ *(tedy levá třída prvku* $(1, 2)$ *je rovná pravé třídě prvku* $(1, 2)$*);*

Na příkladu 11 je vidět, že například množina $(2, 3) \circ H$ nemusí obsahovat žádný z původních prvků podgrupy H, a taky nemusí být podgrupa, protože neobsahuje neutrální prvek id, i když H podgrupa grupy G je (ze všech navzájem disjunktních tříd = podmnožin je podgrupou právě jedna – ta, která obsahuje neutrální prvek, a tedy třída $H \circ id$ neboli třída H).

Zabývejme se dále pouze pravými třídami prvků – všechny následující věty se budou týkat pravých tříd prvku vzhledem k podgrupě H, ikdyž bychom je mohli analogicky (či duálně?) formulovat i pro levé třídy prvku. Věta 9 je pouze pomocnou větou, která bude potřeba v důkazu věty 10 (věty 9 až 12 jsou řečeny za předpokladu označení z definice 18, tj. $(H, \bigtriangledown)$ je podgrupa grupy $(G, \bigtriangledown)$).

Věta 9 *$a \in H \bigtriangledown b$ právě tehdy, když $H \bigtriangledown a = H \bigtriangledown b$.*

Důkaz: „$\Leftarrow$“: tato část důkazu je triviální: protože $a = e \bigtriangledown a \in H \bigtriangledown a$ a také $b = e \bigtriangledown b \in H \bigtriangledown b$, z rovnosti množin plyne i $a \in H \bigtriangledown b$.

„$\Rightarrow$“: předpokládejme, že $a \in H \bigtriangledown b$, a tedy existuje $h \in H$ tak, že $a = h \bigtriangledown b$. Za tohoto předpokladu dokážeme množinovou rovnost z platnosti dvou inkluzí:

$H \bigtriangledown a \subseteq H \bigtriangledown b$: Pokud $x \in H \bigtriangledown a$, tak $x = h_1 \bigtriangledown a$ pro nějaké $h_1 \in H$. Z předpokladu věty dosaďme za a a dostaneme

$$x = h_1 \bigtriangledown a = h_1 \bigtriangledown (h \bigtriangledown b) = (h_1 \bigtriangledown h) \bigtriangledown b,$$

a protože součin v poslední závorce je prvkem H, dostáváme celkem, že $x \in H \bigtriangledown b$.

$H \bigtriangledown b \subseteq H \bigtriangledown a$: Pokud $x \in H \bigtriangledown b$, tak $x = h_2 \bigtriangledown b$ pro nějaké $h_2 \in H$. Z předpokladu věty ($a = h \bigtriangledown b$) si vyjádřeme b, konkrétně (protože jsme v grupě G, všechny inverze existují)

$$a = h \bigtriangledown b \quad \Rightarrow \quad h^{-1} \bigtriangledown a = b,$$

a po dosazení za b dostaneme

$$x = h_2 \bigtriangledown b = h_2 \bigtriangledown (h^{-1} \bigtriangledown a) = (h_2 \bigtriangledown h^{-1}) \bigtriangledown a,$$

a protože součin v poslední závorce je prvkem množiny H, dostáváme celkem, že $x \in H \bigtriangledown a$.

Věta 9 netvrdí nic světoborného, v podstatě jen to, že pokud prvky a, b jsou spojeny v operaci $\bigtriangledown$ „přes podgrupu H“, tak jejich pravé třídy jsou totožné. Následující věta 10 je prvním významným výsledkem této kapitoly.

Věta 10 *Pravé[22] třídy $H \bigtriangledown a$ pro všechny možné prvky a grupy $(G, \bigtriangledown)$ tvoří rozklad množiny G.*

Důkaz: Dokážeme ve dvou krocích: a) $H \bigtriangledown a$, $H \bigtriangledown b$ jsou buď disjunktní, nebo totožné; b) každý prvek grupy G leží v nějaké třídě takto vytvořeného rozkladu.

[22] Platí i analogická věta: Všechny levé třídy $a \bigtriangledown H$ ...

a) Pokud množiny $H \bigtriangledown a$, $H \bigtriangledown b$ mají prázdný společný průnik, neděláme nic, protože to je pozitivní situace, kterou jsme si přáli; zbývá projít situaci, kdy průnik obou těchto množin je neprázdný a obsahuje nějaký prvek x:

$$x \in (H \bigtriangledown a) \cap (H \bigtriangledown b) \Rightarrow (x = h_1 \bigtriangledown a) \quad \wedge \quad (x = h_2 \bigtriangledown b) \Rightarrow h_1 \bigtriangledown a = h_2 \bigtriangledown b;$$

vyjádřeme například prvek a z rovnosti, ke které jsme dospěli (jsme v grupě, tedy všechny inverze existují): $a = h_1^{-1} \bigtriangledown h_2 \bigtriangledown b$. To tedy znamená, že

$$a = (h_1^{-1} \bigtriangledown h_2) \bigtriangledown b \in H \bigtriangledown b,$$

a to podle věty 9 (tady právě ji potřebujeme!!) znamená, že $H \bigtriangledown a = H \bigtriangledown b$.

b) Zbývá ukázat, že libovolný prvek $c \in G$ leží v některé z pravých tříd vzhledem k podgrupě H: to je už celkem snadné, protože $c = e \bigtriangledown c$ (kde e je neutrální prvek), a tedy $c \in H \bigtriangledown c$. Našli jsme třídu rozkladu, ve které prvek c leží.

Než se dostaneme k větě 12 vedoucí k Lagrangeově větě, ještě jedno označení a jeden výsledek, věta 11: Označení 06. Označme množinu tříd $G/_H$ rozkladu grupy G podle její komutativní podgrupy H ... vzhledem k operaci $\underline{\bigtriangledown}$ definované pomocí vztahu

$$(H \bigtriangledown a) \underline{\bigtriangledown} (H \bigtriangledown b) := H \bigtriangledown (a \bigtriangledown b)$$

jako tzv. rozkladovou grupu nebo též při doslovném překladu faktorgrupu[23].

Věta 11 *Struktura $G/_H$ vytvořená z tříd podle nějaké své komutativní podgrupy H s operací $\underline{\bigtriangledown}$ je grupa.*

Důkaz věty 11 je technický a nebudeme ho uvádět. Raději zde zmíníme, že $G/_H$ v příkladech 10 a 11 jsou tedy grupy, jejímiž prvky jsou podmnožiny původní množiny G, a operace sčítání či skládání zobrazení je tak definována mezi množinami! Základním často použitým příkladem v tomto textu je právě příklad 10, kde Z_4 je tzv. množina zbytkových tříd. Zbytkovým třídám se budeme věnovat v příští kapitole, v této kapitole jsme pouze zmínili větu, v níž je klíčové zejména to, že operace „sčítání množin“ je definována korektně, tj. bez ohledu na to, jaký prvek vybereme z první množiny a ze druhé množiny, výsledek jejich operace stále padne též do stejné množiny jako všechny ostatní takto zkonstruované výsledky.

Věta 12 *Existuje bijekce mezi podgrupou $(H, \bigtriangledown)$ a každou pravou třídou $H \bigtriangledown a$.*

Důkaz: Bijekcí bude to nejpřirozenější zobrazení $f : H \to H \bigtriangledown a$, které bychom asi vytvořili:

$$f(h) = h \bigtriangledown a.$$

Takto definované f je injekce:

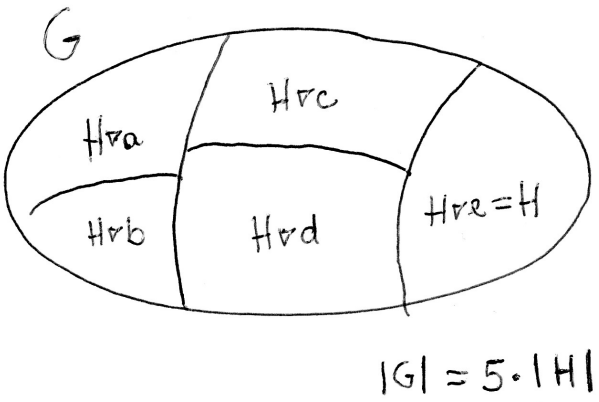
$$f(h_1) = f(h_2) \Rightarrow \quad h_1 \bigtriangledown a = h_2 \bigtriangledown a \Rightarrow \quad h_1 = h_2$$

[23] Anglicky FACTOR znamená, „rozložit“.

(a podmínka injekce o rovnosti vzorů při rovnosti obrazů je dokázána). Dále f je surjekce: každý prvek množiny $H \bigtriangledown a$ je tvaru $h \bigtriangledown a$ pro nějaké $h \in H$, a toto h je hledaným vzorem vzhledem k zobrazení f. Celkem f je tedy injekce i surjekce, a tedy bijekce. Důkaz je hotov. □

Důsledkem věty 12 pro konečné grupy G je: Všechny pravé třídy $H \bigtriangledown a$ mají tentýž počet prvků!!!!!

Čtenář si určitě říká, kdy už přijde ta slavná Lagrangeova věta z názvu této kapitoly – už se blíží, je to věta následující!!! Ale ty nejdůležitější věty, věta 10 a věta 12, už byly řečeny. Ta následující je pouze jejich důsledkem, tj. pan Lagrange je autorem souvislostí všech těchto vět. Podívejme se ovšem předtím na příklad ilustrující celou situaci:



Obrázek 4.7: Rozklad konečné grupy G na pět pravých tříd vzhledem k podgrupě H. Všechny třídy rozkladu mají stejný počet prvků.

Příklad 12 *Uvažujme situaci na obrázku 4.7: všech pravých tříd vzhledem k podgrupě H konečné grupy G je pět – jedna z nich je $H \bigtriangledown e = H$ a další čtyři jsou $H \bigtriangledown a$, $H \bigtriangledown b$, $H \bigtriangledown c$, $H \bigtriangledown d$. Existuje bijekce (podle věty 12) mezi těmito čtyřmi množinami a grupou H, tj. všech pět množin má stejný počet prvků. Při konečném počtu prvků grupy G by platil vztah*

$$|G| = 5 \cdot |H|.$$

Věta 13 Lagrangeova věta pro konečné grupy. *Počet prvků libovolné podgrupy H je dělitelem počtu prvků konečné grupy G (připomeneme-li si definici řádu grupy, tak: řád podgrupy H je dělitelem řádu grupy G).*

Důkaz Lagrangeovy věty je dalším důsledkem věty 12: pokud všechny pravé třídy mají stejný počet prvků, tak počet všech prvků je pouze nějakým násobkem počtu $|H|$.

Příklad 13 *Pokud G má 15 prvků, tak kromě nevlastních podgrup (jednoprvkové obsahující pouze neutrální prvek a celé grupy G) mohou mít jakékoli vlastní podgrupy jen tři prvky nebo pět prvků (což jsou vlastní dělitelé čísla 15).*

Příklad 14 *Pokud $|G|$ je prvočíslo, tak grupa G má pouze nevlastní podgrupy (sebe samotnou a jednoprvkovou triviální podgrupu).*

Věta 14 *Pokud $|G| = p$ je prvočíslo, tak grupa $(G, \bigtriangledown)$ je cyklická grupa a jakékoli $a \in G$ různé od neutrálního prvku e je jejím generátorem.*

Důkaz: Uvažujme $a \in G$, a dále platí $a \neq e$ (kde e je neutrální prvek). Řád prvku a je roven $m > 1$ (protože řádu 1 je pouze neutrální prvek grupy). Pak $< a >$ je cyklická podgrupa, která má m prvků (a současně z předchozího platí $m > 1$), tj. celkem

$$m|p \quad \wedge \quad m > 1 \quad \Rightarrow \quad m = p$$

(z neexistence vlastních dělitelů čísla p tedy plyne, že řád libovolného prvku a různého od e je roven p). □

Věta 14 je dalším důležitým faktem sama o sobě: existuje jediná grupa (až na izomorfismus) daného prvočíselného počtu prvků. Například $(Z_7, +)$ je jediná sedmiprvková grupa, $(Z_{11}, +)$ je jediná jedináctiprvková grupa, apod. Získali jsme tedy úplnou informaci o grupách o prvočíselném počtu prvků – jsou cyklické, až na izomorfismus jediné (co se týká počtu prvků) a lze je generovat libovolným jejich prvkem a různým od neutrálního prvku.

Věta 15 *Řád každého prvku $a \in G$ je dělitelem řádu konečné grupy G.*

Důkaz: pro prvek $c \in G$ řádu m je $< c >$ cyklickou podgrupou řádu m (libovolný prvek generuje cyklickou podgrupu grupy G), a tedy m je některý z dělitelů čísla $|G|$, což je řád grupy G.

Definice 19 *Protože přirozené číslo, které udává řád podgrupy $|H|$, je dělitelem řádu konečné grupy $|G|$, lze provést tuto operaci dělení přirozeným číslem a označit index podgrupy H v grupě G jako*

$$(G : H) = \frac{|G|}{|H|} = \text{ počet navzájem různých tříd rozkladu } \{H \bigtriangledown a; a \in G\}.$$

Homomorfismus grup

Izomorfismus grup je bijektivním zobrazením, které zachovává výsledky operace. Tato vlastnost (zachování výsledků operace) se objevuje i u jiných zobrazení než bijekcí – taková zobrazení nazveme homomorfismy[24].

Definice 20 *Grupový homomorfismus $f : G \to H$ je takové zobrazení mezi grupami $(G, \bigtriangledown)$ a $(H, *)$, které zachovává výsledky operace, tj. platí vlastnost*

$$\forall a, b \in G : \quad f(a \bigtriangledown b) = f(a) * f(b).$$

[24] Jazykově: izomorfismus = stejný tvar, totožný tvar; homomorfismus = podobný tvar, odvozený tvar (v jistém smyslu).

Příklad 15 *Zobrazení grupy $(Z, +)$ na grupu zbytkových tříd $(Z_6, +)$ definované vztahem „$f(z) =$ zbytek po dělení čísla z číslem 6“ je homomorfismus grup.*

Takto definované zobrazení opravdu splňuje podmínku zachování výsledků operace: například platí

$$f(5 + 53) = f(5) + f(53),$$

protože

$$[4] = [5] + [5]$$

(rovnost skutečně platí, protože v Z_6 platí $[5] + [5] = [10] = [4]$, neboli číslo 56 dává po dělení šesti zbytek 4, který určuje stejnou třídu rozkladu $[4]$, která obsahuje prvek 10, což je součet zbytku po dělení čísla 5 šesti a zbytku po dělení čísla 53 šesti).□

Význam homomorfismu: Pod homomorfismem lze v řadě případů (tehdy, když f je surjekce grupy G na grupu H) vidět jistou projekci, která některé vlastnosti původní grupy ztrácí, ale zachová jednu jistou vlastnost. Třeba v právě uvedeném příkladu se při zobrazení f jistým způsobem ztrácí nekonečnost množiny Z a zůstává jen informace, jaké zbytky po dělení šesti existovaly mezi celými čísly, a dále zůstává na Z_6 zachována vlastnost součtu zbytků, neboli součet dvou celých čísel dává po vydělení šesti zbytek, který je obsažen v té třídě rozkladu množiny Z_6, která obsahuje součet zbytků obou původních čísel po vydělení šesti.

Příklad 16 *Zobrazení $f : Z_6 \to Z_3$, přičemž na obou množinách uvažujeme operací sčítání, definované vztahem*

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 2 & 0 & 1 & 2 \end{pmatrix}$$

je také grupový homomorfismus, protože zbytek po dělení šesti v grupě $(Z_6, +)$ je zobrazen na zbytek tohoto zbytku po dělení třemi v grupě $(Z_3, +)$. V důsledku zobrazení f se ztrácí jisté informace z grupy Z_6, a sice celočíselná odchylka nejbližšího násobku šesti na číselné ose směrem vlevo od libovolného reprezentanta dané třídy rozkladu, ovšem zůstává zachována celočíselná odchylka nejbližšího násobku tří na číselné ose směrem vlevo od libovolného reprezentanta dané třídy rozkladu.□

Definice 21 *Pokud $f : G \to H$ je grupový homomorfismus a současně surjekce, označujeme $f(G) = H$ a grupa H se nazývá homomorfní obraz grupy G.*

Viz příklad 16: grupa $(Z_3, +)$ je homomorfním obrazem grupy $(Z_6, +)$ vzhledem k homomorfismu f.

Podívejme se tedy na některé vlastnosti každého grupového homomorfismu. Tyto vlastnosti platí i pro izomorfismus, protože homomorfismus je obecnější pojem (každý grupový izomorfismus je současně i grupovým homomorfismem):

Věta 16 *Pro grupový homomorfismus $f : G \to H$ grupy $(G, \bigtriangledown)$ do grupy $(H, *)$ platí:*

a) $f(e_G) = e_H$ *(grupový homomorfismus vždy zobrazuje jednotkový prvek grupy G na Jednotkový prvek grupy H);*

b) $(f(a))^{-1} = f(a^{-1})$ *(vzhledem ke grupovému homomorfismu platí: inverze obrazu = obraz inverze).*

Důkaz:

- ad a) Prvek e_G jistě můžeme psát jako $e_G \bigtriangledown e_G$, a po využití vlastnosti (h) homomorfismu (= vlastnosti zachování výsledků operace) dostaneme:

$$f(e_G) = F(e_G \bigtriangledown e_G) \overset{(h)}{=} f(e_G) * f(e_G),$$

dostali jsme tedy rovnost

$$f(e_G) = f(e_G) * f(e_G),$$

ze které po vynásobení rovnosti prvkem $(f(e_G))^{-1}$ (který existuje díky vlastnosti (4) v grupě $(H, *)$) zprava dostaneme

$$f(e_G) * (f(e_G))^{-1} = f(e_G) * f(e_G) * (f(e_G))^{-1},$$

a nyní použitím vlastnosti (3) grupy $(H, *)$ na levé i pravé straně poslední rovnosti máme neutrální prvek e_H grupy H a dostaneme

$$e_H = f(e_G) * e_H \overset{(3)_H}{=} f(e_G),$$

a to jsme chtěli dokázat (jednotkový prvek se zobrazí na jednotkový prvek).

- ad b) chceme dokázat vztah

$$f(a) * f(a^{-1}) = e_H,$$

pak totiž podle věty 4 v grupě oba prvky, jejichž součin je neutrální prvek, si jsou navzájem inverzní. No ale to není těžké, začneme upravovat levou stranu rovnosti, kterou chceme dokázat, a využijeme vlastnost homomorfismu grup:

$$f(a) * f(a^{-1}) \overset{(h)}{=} f(a \bigtriangledown a^{-1}) \overset{(4)_G}{=} f(e_G) \overset{(a)}{=} e_H,$$

takže podle věty 4 inverzní prvek k prvku $f(a)$ je prvek $f(a^{-1})$, neboli $(f(a))^{-1} = f(a^{-1})$. Důkaz je hotov. □

Definice 22 *Jádro grupového homomorfismu $f : G \to H$ se nazývá množina ker_f (označení 07)[25] těch prvků z grupy $(G, \bigtriangledown)$, které se zobrazí na neutrální prvek e_H grupy $(H, *)$.*

[25] Označení plyne z německého slova kernel – anglické core se z historických důvodů neprosadilo.

Příklad 17 *a) V grupovém izomorfismu je jádrem zobrazení f pouze jednoprvková množina $\{e_G\}$.*

b) V homomorfismu $f : Z_6 \to Z_3$ z příkladu 16 je jádrem množina těch prvků, které se zobrazí na nulu: $ker_f = \{0, 3\}$.

Věta 17 *Pro každý grupový homomorfismus platí tyto další vlastnosti:*

a) *ker_f je normální podgrupa v $(G, \bigtriangledown)$;*

b) *$f(G)$ je podgrupa v $(H, *)$.*

Důkaz: ad a) vezměme libovolný $a \in \ker_f$ a libovolný $x \in G$. Chceme ukázat, že $x \bigtriangledown a \bigtriangledown x^{-1} \in \ker_f$. Půjde to jednoduše, využijeme přitom předpokladu (p) věty ($f(a) = e_H$) a vlastnosti (h) homomorfismu:

$$f(x \bigtriangledown a \bigtriangledown x^{-1}) \overset{(h)}{=} f(x) * f(a) * f(x^{-1}) \overset{(p)}{=} f(x) * e_H * f(x^{-1}) \overset{(3)}{=} f(x) * f(x^{-1}) \overset{(4)}{=} e_H,$$

tj. protože se prvek $x \bigtriangledown a \bigtriangledown x^{-1}$ zobrazil na neutrální prvek, patří do jádra $\ker_f$, protože právě těmito prvky je jádro definováno.

ad b) i) $f(G)$ je neprázdná množina, protože obsahuje minimálně neutrální prvek $f(e_G) = e_H$; ii) $f(G)$ je uzavřená vzhledem k operaci $*$: pro $f(x)$ a $f(y)$ platí

$$f(x) * f(y) \overset{(h)}{=} f(x \bigtriangledown y),$$

tedy prvek $f(x) * f(y)$ je obrazem prvku $x \bigtriangledown y \in G$, a tedy $f(x) * f(y) \in f(G)$, platí (1); iii) $f(G)$ je uzavřená vzhledem k inverzím: pokud $f(a) \in f(G)$ také $f(a^{-1}) \in f(G)$ a díky větě 22(b) víme že tyto dva prvky jsou navzájem inverzní, tj. našli jsme inverzi k prvku $f(a)$, platí vlastnost (4). Celkem podle věty 6 je $f(G)$ podgrupa grupy $(H, *)$. □

5 Týden 05

5.1 Cvičení 05: Řád prvku, cyklické grupy, grupy zbytkových tříd

V prvním týdnu jsme už mluvili o n-té mocnině prvku. Jednoduše v každé grupě platí i zákonitosti, na které jsme zvyklí např. z operace násobení na množině všech zlomků:

- $a^m \bigtriangledown a^n = a^{m+n}$,
- $(a^m)^n = a^{m \cdot n}$,
- $a^{-n} = (a^{-1})^n$.

Při našem hloubavém přemýšlení o vlastnostech obecných grup se ukazuje důležitým jeden pojem, který je s otázkou mocniny přirozeně spjatý – pojem řádu prvku. Uvidíme, že tento pojem je důležitý zejména pro konečné grupy, a v nekonečných grupách hraje svou specifickou roli, která souvisí s nekonečnými množinami.

Definice 23 *Řád prvku a grupy $(G, \bigtriangledown)$ je roven nejmenšímu přirozenému číslu n, pro které $a^n = e$ (n-tá mocnina prvku $a \in G$ je rovna neutrálnímu prvku $e \in G$. Pokud takové přirozené číslo neexistuje, říkáme, že řád prvku a je nekonečný.*

Příklad 18 *Co se týká řádu jednotlivých prvků grupy $(S_3, \circ)$, platí:*

- $id^1 = id$, *tj. id je prvek řádu* 1;
- $(2,3)^2 = (1,3)^2 = (1,2)^2 = id$, *tj. prvky* $(2,3)$, $(1,3)$, $(1,2)$ *jsou řádu* 2;
- $(1,2,3)^3 = (1,3,2)^3 = id$, *tj. prvky* $(1,2,3)$, $(1,3,2)$ *jsou řádu* 3.

Z řádů jednotlivých prvků také vidíme, že existuje $k = 6$ (nejmenší společný násobek řádů jednotlivých prvků) tak, že libovolný z prvků umocněný na šestou se rovná jednotce id:

$$id^6 = id,\ (2,3)^6 = ((2,3)^2)^3 = id^3 = id,\ (1,3)^6 = id,\ (1,2)^6 = id,$$

$$(1,2,3)^6 = ((1,2,3)^3)^2 = id^2 = id,\ (1,3,2)^6 = id.$$

To je tedy zajímavá vlastnost, ke které jsme dospěli – v konečné grupě vždy po několikerém umocnění každého prvku dostaneme prvek jednotkový.

Příklad 19 *V grupě $(Z, +)$ je řád všech prvků nekonečný, kromě prvku* 0, *jehož řád (jako řád každého neutrálního prvku) je roven jedné.*

Při krátkém zkoumání pojmu řádu prvku (ať už je konečný, nebo nekonečný), matematici dospěli k následujícím dvěma větám, které vrhají světlo na celou situaci:

Věta 18 *Pro prvek a řádu n v grupě $(G, \bigtriangledown)$ platí: v této grupě existuje právě nrůzných hodnot $a^0 = e = a^n$ (e je neutrální prvek grupy), a^1, a^2, ..., a^{n-1}.*

Důkaz: Dokážeme ve dvou částích: a) každá mocnina a^m prvku a řádu n je rovna některé z mocnin a^0, a^1, ..., a^{n-1}; b) prvky a^0, a^1, ..., a^{n-1} jsou navzájem různé.

Důkaz části a): Uvažujme libovolnou mocninu a^m prvku $a \in G$, který je řádu n. Pak podle věty 21 z předmětu Základy matematiky (věta o dělení se zbytkem, která platí pro celá čísla – my ji nyní použijeme pouze pro čísla přirozená) vydělíme $m : n$ a dostaneme, že existují přirozená čísla q, r tak, že

$$m = n \cdot q + r, \quad 0 \leq r < n.$$

Pak lze upravit a^m na tvar

$$a^m = a^{n \cdot q + r} = (a^n)^q \bigtriangledown a^r = e^q \bigtriangledown a^r = a^r,$$

a protože r je přirozené číslo, pro které $0 \leq r < n$, musí být r rovno jednomu z čísel 0, 1, ..., $n - 1$.

Důkaz části b): Zbývá dokázat, že prvky a^0, a^1, ..., a^{n-1} jsou navzájem různé. Pokud se některé z těchto dvou prvků rovnají, platí $a^r = a^s$, kde r i s jsou dvě různá čísla z množiny $\{0, 1, 2, \ldots, n-1\}$, tj. $r \neq s$. BUNO[26] například $s < r$, tj. platí $0 \leq s < r < n$, a tedy $0 < r - s < n$. A protože $a^r = a^s$ (to je náš předpoklad (p)), lze psát

$$a^{r-s} = a^r \bigtriangledown (a^s)^{-1} \overset{(p)}{=} a^s \bigtriangledown (a^s)^{-1} = e.$$

To je ovšem spor s definicí řádu n jako nejmenšího přirozeného čísla takového, že $a^n = e$, protože $r - s < n$. Náš předpoklad $a^r = a^s$ byl nesprávný, je tedy dokázán opak, že se jedná o n navzájem různých hodnot. □

Pokud se nad větou 18 zamyslíme, plyne z ní, že poté, co dosáhneme umocňováním prvku a konečného řádu n prvku $a^n = e$, další mocniny už nevytváří nové prvky, ale začínají opakovat předchozí prvky: $a^{n+1} = a$, $a^{n+2} = a^2$, ..., $a^{2n-1} = a^{n-1}$, a pak začíná druhé kolo opakování $a^{2n} = e$, $a^{2n+1} = a$, atd.

Věta 19 *Pro prvek a nekonečného řádu v grupě $(G, \bigtriangledown)$ platí: v této grupě neexistují dvě mocniny tohoto prvku, které se rovnají, tj. pro dvě různá celá čísla r, s platí $a^r \neq a^s$.*

Důkaz: je prostý, použijeme tutéž úvahu jako v důkazu věty 18, část b): Pokud by platilo $a^r = a^s$, úpravou $a^r \bigtriangledown (a^s)^{-1}$ dostaneme

$$a^{r-s} = a^r \bigtriangledown (a^s)^{-1} = a^s \bigtriangledown (a^s)^{-1} = e,$$

a to je spor s tvrzením, že řád prvku a je nekonečný, protože by existovala konečná mocnina prvku a rovná neutrálnímu prvku. Tj. předpoklad $a^r = a^s$ je nesprávný a důkaz

[26] BUNO = Bez újmy na obecnosti.

sporem je hotov.□

To tedy znamená, že prvek nekonečného řádu „svým umocňováním“[27] vede na nekonečně mnoho navzájem různých prvků grupy.

A dodejme ještě větu, která upřesňuje situaci kolem konečného řádu prvku grupy:

Věta 20 *Pokud řád prvku a v grupě je n (označení 08 : označme $ord(a) = n$), pak platí pro celočíselné t:*

$$a^t = e \Leftrightarrow (n|t, \quad tj.\ t = n \bigtriangledown q, \quad pro\ nějaké\ q \in Z).$$

(mocnina prvku konečného řádu je rovna neutrálnímu prvku tehdy a jen tehdy[28], když mocnitel t je násobek řádu n daného prvku).

Důkaz: Dokážeme obě implikace: Ad „⇒“: Důkaz je podobný jako důkaz věty 18, část a): Pokud $a^t = e$, pak podle věty o dělení se zbytkem pro celá čísla platí $t = n \cdot q + r$, kde $0 \leq r < n$. Pak dosazením do naší rovnosti dostaneme

$$e = a^t = a^{n \cdot q + r} = (a^n)^q \bigtriangledown a^r = e \bigtriangledown a^r.$$

Ale protože n jako řád prvku a je nejmenší přirozené číslo takové, že $a^n = e$, Nemůže být $r > 0$, ale musí $r = 0$.

Důkaz opačné implikace „⇐“: je zřejmý ... pokud $t = n \cdot q$, pak

$$a^t = a^{n \cdot q} = (a^n)^q = e^q = e.$$

Cyklické grupy

Pojem cyklické grupy a jejího generátoru (jediného prvku) už byl vysvětlen dříve v dodatcích v kapitole 1. Nyní se podívejme na cyklické grupy ještě jednou poté, co známe pojmy izomorfismus grup a řád prvku grupy:

Je jasné, že pokud $< a >$ je cyklická grupa generovaná svým prvkem, který je řádu n, platí

$$< a >= \{e, a, a^2, \ldots, a^{n-1}\}.$$

Existuje tedy izomorfismus grupy $(H_n, +)$ pootočení hodinové ručičky s operací skládání pootočení na grupu $(< a >, \bigtriangledown)$ definovaný vztahem $f(k) = a^k$ pro $k = 0, 1, \ldots, n-1$. Hned vidíme, že podmínka zachování výsledků operace je skutečně splněna:

$$f(k + l) = a^{k+l} = a^k \bigtriangledown a^l = f(k) \bigtriangledown f(l).$$

Touto kratinkou úvahou jsme vlastně dokázali větu

[27] Umocňování = opakované použití operace $\bigtriangledown$ na týž prvek.

[28] Poznámka pro čtenáře v angličtině: anglické matematické vyjadřování vyjadřuje někdy logickou spojku ⇔ výrazem *iff*, což je zkráceně přesnějšího nematematického *if and only if* = tehdy a jen tehdy, když.

Věta 21 *Každá konečná cyklická grupa řádu n (= grupa generovaná jediným prvkem řádu n) je izomorfní grupě $(H_n, +)$. Speciálně, každé dvě konečné cyklické grupy řádu n*[29] *jsou navzájem izomorfní.*

A podobně pro cyklickou grupu generovanou prvkem nekonečného řádu: lze psát

$$< a >= \{\dots, a^{-2}, a^{-1}, e, a, a^2, a^3, \dots\},$$

a tedy můžeme definovat izomorfismus grupy $(Z, +)$ na grupu $(< a >, \bigtriangledown)$ definovaný vztahem $f(k) = a^k$ pro jakékoli celé číslo k, který opět splňuje podmínku zachování výsledků operace. Dostáváme tak větu

Věta 22 *Každá nekonečná cyklická grupa (= grupa generovaná jediným prvkem nekonečného řádu) je izomorfní grupě $(Z, +)$. Speciálně, každé dvě nekonečné cyklické grupy jsou navzájem izomorfní.*

Tedy věty 21 a 22 nám dávají nahlédnout do situace cyklických grup: všechny cyklické grupy jsou víceméně určeny grupami celých čísel – ať už nekonečné grupy jsou určeny a popsány grupou $(Z, +)$, tak konečné cyklické grupy jsou určeny a popsány (až na přeznačení prvků) grupou $(Z_n, +)$ (což je grupa zbytkových tříd modulo n, která je izomorfní grupě pootočení hodinové ručičky $(H_n, +)$)). Mohli bychom pracovat stále s grupou pootočení hodinové ručičky, ale protože studenti už grupy zbytkových tříd absolvovali na cvičení, lze pracovat přímo s nimi. Následuje oddílek opakující znalosti ze cvičení o grupách zbytkových tříd.

Grupy zbytkových tříd

Klíčovou strukturu představuje následující pojem:

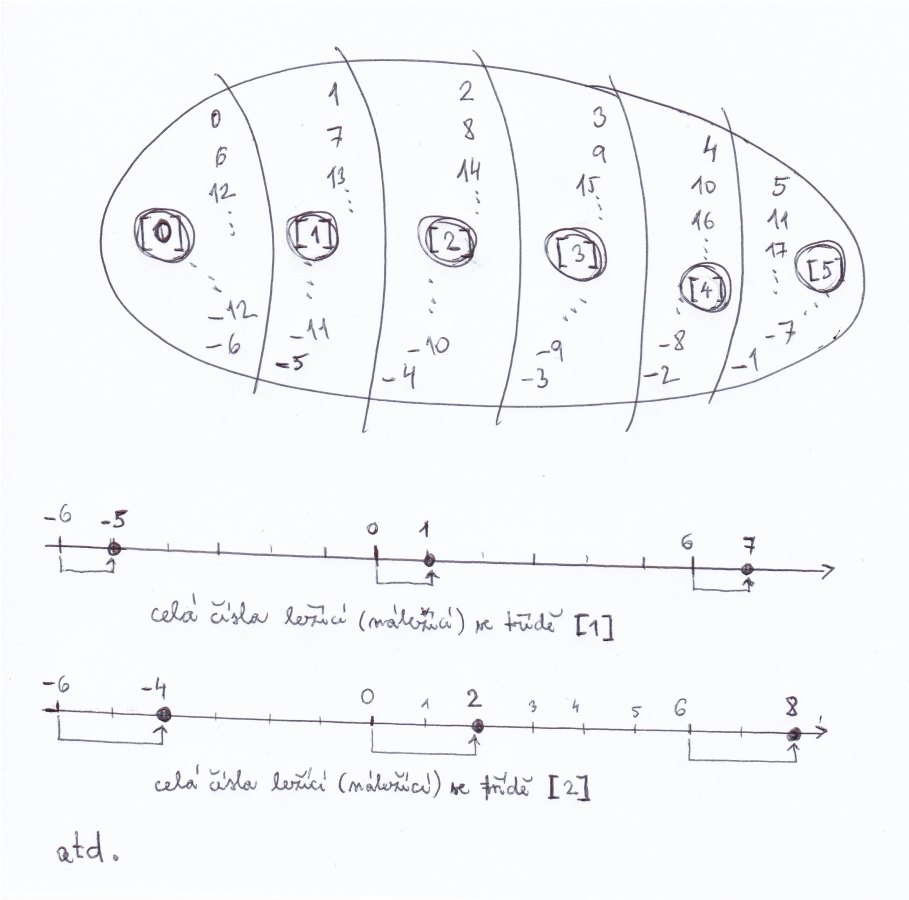
Definice 24 *množina zbytkových tříd modulo n ... popíšeme celou konstrukci této množiny například pro $n = 6$: Rozdělíme všechna celá čísla do šesti podmnožin podle toho, jak daleko je dané číslo na číselné ose vpravo od nejbližšího násobku čísla 6 (viz obrázek 5.8). Pak v každé třídě jsou právě ta celá čísla, která jsou mezi sebou kongruentní modulo 6, tj.*

$$a \equiv b, \text{ když } 6|(a - b).$$

O relaci kongruence lze dokázat, že je to ekvivalence (tj. relace reflexivní, symetrická, tranzitivní).

- Třída [1] obsahuje čísla 1, 7, 13, atd. ale také záporná čísla -5, -11, -17, atd., protože nejbližší násobek čísla 6 je od nich vzdálený o jednu jednotku vlevo.
- Třída [2] obsahuje čísla 2, 8, 14, atd. ale také záporná čísla -4, -10, -16, atd. a jsou to právě ta čísla, od nichž je vzdálen násobek šesti o dvě jednotky vlevo.

[29] Připomínka bizarní definice řádu grupy: řád grupy = počet prvků grupy.



Obrázek 5.8: Rozdělení celých čísel do šesti podmnožin.

- Třída [3] obsahuje čísla 3, 9, 15, atd. ale také záporná čísla -3, -9, -15, atd.
- Třída [4] obsahuje čísla 4, 10, 16, atd. ale také záporná čísla -2, -8, -14, atd.
- Třída [5] obsahuje čísla 5, 11, 17, atd. ale také záporná čísla -1, -7, -13, atd.
- A konečně třída [0] obsahuje všechna celá čísla dělitelná šesti, tj. 0, 6, 12, atd. ale také záporná čísla -6, -12, -18, atd.

V každé třídě takto vytvořené jsou právě ta celá čísla, která jsou mezi sebou kongruentní modulo 6. Každá z daných těchto šesti podmnožin je nekonečná, odtud tedy honosný název „třída“.

Nyní se budeme dále dívat na tyto třídy jako na prvky množiny Z_6 (tj. množina Z_6 je konečná a má jen šest prvků!!!) a definujeme na této množině operace $\oplus$, $\odot$ následovně:

$$[a] \oplus [b] := [a + b];$$

tj. součet tříd je třída, která obsahuje celé číslo $a + b$,

$$[a] \odot [b] := [a \cdot b];$$

tj. součin tříd je třída obsahující celé číslo $a \cdot b$. Lze ukázat, že tyto dvě operace nezávisí na výběru celých čísel a, b z daných nekonečných množin. Pro takto definovanou šestiprvkovou množinu a operace na ní nyní platí, že $(Z_6, \oplus)$ je grupa (zbytkových tříd modulo 6), $(Z_6*, \odot) = (Z_6 - \{[0]\}, \odot)$ je monoid (zbytkových tříd modulo 6).

Příklad 20 *a) Pomocí tabulky operace $\oplus$ dokažte, že $(Z_6, \oplus)$ je grupa:*

Tabulka 5.5: Tabulka operace $\oplus$ na množině Z_6.

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

b) Pomocí tabulky operace $\odot$ dokažte, že$(Z_6, \odot)$ je monoid:

Tabulka 5.6: Tabulka operace $\odot$ na množině Z_6.

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

- označení 09 : Z_n ... množina zbytkových tříd modulo n;
- označení 10 : Z_n^* ... množina zbytkových tříd modulo n mimo prvek [0], tj.

$$Z_n^* := Z_n - \{[0]\}.$$

Toto označení používáme i pro klasické množiny Q^* (racionální čísla mimo nuly), R^* (reálná čísla mimo nuly), protože se nám hodí, že $(Q^*, \cdot)$, $(R^*, \cdot)$ jsou grupy (nulu

z těchto množin musíme vyloučit, protože pro ni neexistuje inverzní prvek vzhledem k operaci násobení).

Zbytkové třídy lze sestavit nejen pro $n = 6$, ale pro jakékoli přirozené $n > 1$. Následující dvě věty studenti nemusí umět dokázat (ale je dobré si zapamatovat, co říkají):

Věta 23 *Ve struktuře $(Z_n^*, \odot)$ existuje k prvku $[k]$ inverzní prvek vzhledem k násobení $\odot$ právě tehdy, když k, n jsou nesoudělná.*

Například v $(Z_6, \odot)$ neexistují k prvkům [2], [3], [4] inverzní prvky, protože čísla 2, 3, 4 jsou soudělná s číslem 6.

Věta 24 *Důsledek předchozí věty: Pokud n je prvočíslo, tak k, n jsou nesoudělná čísla pro $k = 1, 2, \ldots, (n-1)$, tj. ke všem prvkům (kromě [0], kterou jsme vyloučili) existují inverzní prvky vzhledem k násobení $\odot$, a tedy $(Z_n^*, \odot)$ je grupa.*

Například $(Z_7^*, \odot)$ je grupa. Čtenář by se o tom mohl snadno přesvědčit z tabulky operace $\odot$ na množině Z_7^*:

$\odot$	[1]	[2]	[3]	[4]	[5]	[6]
[1]	[1]	[2]	[3]	[4]	[5]	[6]
[2]	[2]	[4]	[6]	[1]	[3]	[5]
[3]	[3]	[6]	[2]	[5]	[1]	[4]
[4]	[4]	[1]	[5]	[2]	[6]	[3]
[5]	[5]	[3]	[1]	[6]	[4]	[2]
[6]	[6]	[5]	[4]	[3]	[2]	[1]

Úloha 5.1 *Cvičení k pojmu řád prvku: Ad Pinter 2010, str. 107-110:*

- *Cvičení B (str. 108): Příklady řádu prvků.*

  Například N.4: Na grupě permutací $(S_7, \circ)$ jsou zadány prvky (formou součinu cyklů, který vypočtěte) $\alpha = (1,2,3,4) \circ (2,4,5)$, $\beta = (1,6,7) \circ (2,5,7)$. Vypočtěte prvek $(\alpha^3 \circ \beta^4)^5$ a určete jeho řád.

- *Cvičení F: řád mocnin prvku.*

- *Cvičení G: vztah mezi $ord(a)$ a $ord(a^k)$.*

Úloha 5.2 *Cvičení k pojmu cyklická grupa:*

- *Na přednášce už nezbyl čas na důkaz věty: každá podgrupa cyklické grupy je cyklická, tj. lze ji generovat jediným prvkem – kterým?? (viz Pinter 2010, str. 114-115).*

- *Cvičení A (str. 115): příklady cyklických grup.*

- *Cvičení B: elementární vlastnosti cyklických grup.*

- *Cvičení C: generátory cyklické grupy.*
- *Cvičení E: kartézský součin cyklických grup.*

Úloha 5.3 *Cvičení k pojmu grupy zbytkových tříd:*

Například D.2 z knihy Pinter 2010, str. 98: Všechny následující čtyři grupy jsou šestiprvkové. Vytvořte jejich rozklad do tříd tak, že v jedné třídě jsou grupy navzájem izomorfní. Najděte daný izomorfismus, popřípadě vysvětlete, proč grupy v různých třídách izomorfní nejsou.

Grupa $(S_3, \circ)$ *permutací tříprvkové množiny na sebe sama – tabulku operace najdete v přednášce o nekomutativních grupách.*

Grupa $(Z_7^*, \odot)$ *(je vyloučena třída* $[0]$*, ke které neexistuje inverze vzhledem k násobení):*

$\odot$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[2]$	$[2]$	$[4]$	$[6]$	$[1]$	$[3]$	$[5]$
$[3]$	$[3]$	$[6]$	$[2]$	$[5]$	$[1]$	$[4]$
$[4]$	$[4]$	$[1]$	$[5]$	$[2]$	$[6]$	$[3]$
$[5]$	$[5]$	$[3]$	$[1]$	$[6]$	$[4]$	$[2]$
$[6]$	$[6]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

$(Z_6, \oplus)$ *je grupa:*

$\oplus$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

Grupa $(H_3 \times H_2, +)$*:*

$+$	$[0;0]$	$[0;1]$	$[1;0]$	$[1;1]$	$[2;0]$	$[2;1]$
$[0;0]$	$[0;0]$	$[0;1]$	$[1;0]$	$[1;1]$	$[2;0]$	$[2;1]$
$[0;1]$	$[0;1]$	$[0;0]$	$[1;1]$	$[1;0]$	$[2;1]$	$[2;0]$
$[1;0]$	$[1;0]$	$[1;1]$	$[2;0]$	$[2;1]$	$[0;0]$	$[0;1]$
$[1;1]$	$[1;1]$	$[1;0]$	$[2;1]$	$[2;0]$	$[0;1]$	$[0;0]$
$[2;0]$	$[2;0]$	$[2;1]$	$[0;0]$	$[0;1]$	$[1;0]$	$[1;1]$
$[2;1]$	$[2;1]$	$[2;0]$	$[0;1]$	$[0;0]$	$[1;1]$	$[1;0]$

.

Například N.1: Jsou grupy $(Z_9, +)$ a $(Z_3 \times Z_3)$ izomorfní? Pokud ano, daný izomorfismus najděte. Pokud ne, vysvětlete, proč izomorfní být nemohou.

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[0]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]
[1]	[1]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]
[2]	[2]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]
[3]	[3]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]
[4]	[4]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]
[5]	[5]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]
[6]	[6]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]
[7]	[7]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]
[8]	[8]	[0]	[1]	[2]	[3]	[4]	[5]	[6]	[7]

$+$	[0;0]	[0;1]	[0;2]	[1;0]	[1;1]	[1;2]	[2;0]	[2;1]	[2;2]
[0;0]	[0;0]	[0;1]	[0;2]	[1;0]	[1;1]	[1;2]	[2;0]	[2;1]	[2;2]
[0;1]	[0;1]	[0;2]	[0;0]	[1;1]	[1;2]	[1;0]	[2;1]	[2;2]	[2;0]
[0;2]	[0;2]	[0;0]	[0;1]	[1;2]	[1;0]	[1;1]	[2;2]	[2;0]	[2;1]
[1;0]	[1;0]	[1;1]	[1;2]	[2;0]	[2;1]	[2;2]	[0;0]	[0;1]	[0;2]
[1;1]	[1;1]	[1;2]	[1;0]	[2;1]	[2;2]	[2;0]	[0;1]	[0;2]	[0;0]
[1;2]	[1;2]	[1;0]	[1;1]	[2;2]	[2;0]	[2;1]	[0;2]	[0;0]	[0;1]
[2;0]	[2;0]	[2;1]	[2;2]	[0;0]	[0;1]	[0;2]	[1;0]	[1;1]	[1;2]
[2;1]	[2;1]	[2;2]	[2;0]	[0;1]	[0;2]	[0;0]	[1;1]	[1;2]	[1;0]
[2;2]	[2;2]	[2;0]	[2;1]	[0;2]	[0;0]	[0;1]	[1;2]	[1;0]	[1;1]

.

Například N.2: Najděte minimální (vzhledem k počtu prvků) množinu generátorů grupy $(Z_2 \times Z_2 \times Z_2, \oplus)$:

$\oplus$	[0;0;0]	[0;0;1]	[0;1;0]	[1;0;0]	[0;1;1]	[1;0;1]	[1;1;0]	[1;1;1]
[0;0;0]	[0;0;0]	[0;0;1]	[0;1;0]	[1;0;0]	[0;1;1]	[1;0;1]	[1;1;0]	[1;1;1]
[0;0;1]	[0;0;1]	[0;0;0]	[0;1;1]	[1;0;1]	[0;1;0]	[1;0;0]	[1;1;1]	[1;1;0]
[0;1;0]	[0;1;0]	[0;1;1]	[0;0;0]	[1;1;0]	[0;0;1]	[1;1;1]	[1;0;0]	[1;0;1]
[1;0;0]	[1;0;0]	[1;0;1]	[1;1;0]	[0;0;0]	[1;1;1]	[0;0;1]	[0;1;0]	[0;1;1]
[0;1;1]	[0;1;1]	[0;1;0]	[0;0;1]	[1;1;1]	[0;0;0]	[1;1;0]	[1;0;1]	[1;0;0]
[1;0;1]	[1;0;1]	[1;0;0]	[1;1;1]	[0;0;1]	[1;1;0]	[0;0;0]	[0;1;1]	[0;1;0]
[1;1;0]	[1;1;0]	[1;1;1]	[1;0;0]	[0;1;0]	[1;0;1]	[0;1;1]	[0;0;0]	[0;0;1]
[1;1;1]	[1;1;1]	[1;1;0]	[1;0;1]	[0;1;1]	[1;0;0]	[0;1;0]	[0;0;1]	[0;0;0]

Například D.3: Všechny následující tři grupy jsou osmiprvkové. Zjistěte, zda některé z těchto grup jsou izomorfní, popřípadě vysvětlete, proč izomorfní nejsou: Grupa $(Z_8, \oplus)$*:*

$\oplus$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[6]$	$[7]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[6]$	$[7]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[6]$	$[7]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[6]$	$[6]$	$[7]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[7]$	$[7]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$

Grupa $(Z_2 \times Z_2 \times Z_2, \oplus)$*:*

$+$	$[0;0;0]$	$[0;0;1]$	$[0;1;0]$	$[1;0;0]$	$[0;1;1]$	$[1;0;1]$	$[1;1;0]$	$[1;1;1]$
$[0;0;0]$	$[0;0;0]$	$[0;0;1]$	$[0;1;0]$	$[1;0;0]$	$[0;1;1]$	$[1;0;1]$	$[1;1;0]$	$[1;1;1]$
$[0;0;1]$	$[0;0;1]$	$[0;0;0]$	$[0;1;1]$	$[1;0;1]$	$[0;1;0]$	$[1;0;0]$	$[1;1;1]$	$[1;1;0]$
$[0;1;0]$	$[0;1;0]$	$[0;1;1]$	$[0;0;0]$	$[1;1;0]$	$[0;0;1]$	$[1;1;1]$	$[1;0;0]$	$[1;0;1]$
$[1;0;0]$	$[1;0;0]$	$[1;0;1]$	$[1;1;0]$	$[0;0;0]$	$[1;1;1]$	$[0;0;1]$	$[0;1;0]$	$[0;1;1]$
$[0;1;1]$	$[0;1;1]$	$[0;1;0]$	$[0;0;1]$	$[1;1;1]$	$[0;0;0]$	$[1;1;0]$	$[1;0;1]$	$[1;0;0]$
$[1;0;1]$	$[1;0;1]$	$[1;0;0]$	$[1;1;1]$	$[0;0;1]$	$[1;1;0]$	$[0;0;0]$	$[0;1;1]$	$[0;1;0]$
$[1;1;0]$	$[1;1;0]$	$[1;1;1]$	$[1;0;0]$	$[0;1;0]$	$[1;0;1]$	$[0;1;1]$	$[0;0;0]$	$[0;0;1]$
$[1;1;1]$	$[1;1;1]$	$[1;1;0]$	$[1;0;1]$	$[0;1;1]$	$[1;0;0]$	$[0;1;0]$	$[0;0;1]$	$[0;0;0]$

.

Grupa $(D_4, \circ)$*: (*R_0*,* R_1*,* R_2*,* R_3 *jsou rotace čtverce o násobek pravého úhlu;* S_4*,* S_5 *osové souměrnosti vzhledem k úhlopříčkám čtverce;* S_6*,* S_7 *osové souměrnosti vzhledem ke spojnicím středů protějších stran čtverce)*

$\circ$	R_0	R_1	R_2	R_3	S_4	S_5	S_6	S_7
R_0	R_0	R_1	R_2	R_3	S_4	S_5	S_6	S_7
R_1	R_1	R_2	R_3	R_0	S_6	S_7	S_5	S_4
R_2	R_2	R_3	R_0	R_1	S_5	S_4	S_7	S_6
R_3	R_3	R_0	R_1	R_2	S_7	S_6	S_4	S_5
S_4	S_4	S_7	S_5	S_6	R_0	R_2	R_3	R_1
S_5	S_5	S_6	S_4	S_7	R_2	R_0	R_1	R_3
S_6	S_6	S_4	S_7	S_5	R_1	R_3	R_0	R_2
S_7	S_7	S_5	S_6	S_4	R_3	R_1	R_2	R_0

Například N.3: Definujte přesně izomorfismus $(Z_7^*, \odot)$ na $(Z_6, \oplus)$, který zachovává výsledky operace. Grupa $(Z_7^*, \odot)$ (je vyloučena třída $[0]$, ke které neexistuje inverze vzhledem k násobení):

$\odot$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[6]$
$[2]$	$[2]$	$[4]$	$[6]$	$[1]$	$[3]$	$[5]$
$[3]$	$[3]$	$[6]$	$[2]$	$[5]$	$[1]$	$[4]$
$[4]$	$[4]$	$[1]$	$[5]$	$[2]$	$[6]$	$[3]$
$[5]$	$[5]$	$[3]$	$[1]$	$[6]$	$[4]$	$[2]$
$[6]$	$[6]$	$[5]$	$[4]$	$[3]$	$[2]$	$[1]$

Grupa $(Z_6, \oplus)$:

$\oplus$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$
$[5]$	$[5]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$

Výsledky některých cvičení najdete v závěru textu v oddílu 13.5.

5.2 Přednáška 05

Tato přednáška nepřináší nové pojmy a zákonitosti, pouze procvičuje už dříve probrané – stejně na příkladech lze všechny pojmy vidět nejlépe.

Příklad 21 *Cvičení na podgrupy, které využívá poznatku Lagrangeovy věty: Pro grupu $(D_5, \circ)$, kde D_5 je desetiprvková množina transformací pravidelného pětiúhelníka na sebe sama a operace $\circ$ (=„po“) je skládání transformací,* **vypište všechny její podgrupy**. *Použijte přitom informace o jejích prvcích (zachovejte prosím označení):*

- *e ... identita (nedělá s pětiúhelníkem nic);*
- *f ... pootočení pětiúhelníka v jeho středu o $72°$ po směru hodinových ručiček;*
- *g ... pootočení pětiúhelníka v jeho středu o $144°$ po směru hodinových ručiček;*
- *h ... pootočení pětiúhelníka v jeho středu o $216°$ po směru hodinových ručiček;*
- *i ... pootočení pětiúhelníka v jeho středu o $288°$ po směru hodinových ručiček;*

- *u ... osová souměrnost vzhledem k ose AU, kde A je vrchol pětiúhelníka a U je střed strany CD;*
- *v ... osová souměrnost vzhledem k ose BV, kde B je vrchol pětiúhelníka a V je střed strany DE;*
- *w ... osová souměrnost vzhledem k ose CW, kde C je vrchol pětiúhelníka a W je střed strany EA;*
- *x ... osová souměrnost vzhledem k ose DX, kde D je vrchol pětiúhelníka a X je střed strany AB;*
- *y ... osová souměrnost vzhledem k ose EY, kde E je vrchol pětiúhelníka a Y je střed strany BC;*

a informace o vlastnostech, které platí:

- *Podle Lagrangeovy věty může mít podgrupa konečné grupy jen jistý počet prvků;*
- *uvažte také uzavřenost operace na podgrupě: některé prvky samy od sebe generují jiné prvky (a jejich zahrnutí v podgrupě tedy vyžaduje i zahrnutí dalších prvků);*
- *ještě musíte do každé podgrupy zahrnout i všechny příslušné inverzní prvky.*

Příklad 22 *Cvičení k pojmu levá a pravá třída prvku vzhledem k podgrupě (Pinter 2010, str. 130-135):*

- *A. Příklady tříd prvku vzhledem k podgrupě konečné grupy*
- *B. Příklady tříd prvku vzhledem k podgrupě nekonečné grupy:*

  Například N.1: $H =< 5 >$ je podgrupa grupy $(Z, +)$ generovaná prvkem 5. Vypište všechny pravé třídy prvků vzhledem k podgrupě H.
- *C. Důsledky Lagrangeovy věty*
- *D. Další důsledky Lagrangeovy věty*
- *E. Vlastnosti tříd prvku vzhledem k podgrupě.*

Příklad 23 *Lagrangeova věta (a její důsledek – věta 14) společně s větou 21 nám pomalu, ale jistě dává informace o všech konečných grupách o malém počtu prvků:*

- *Jednoprvková grupa je (až na izomorfismus) jediná a obsahuje pouze neutrální prvek.*
- *Grupa o prvočíselném počtu prvků 2, 3, 5, 7, atd. je cyklická (věta 14), a tedy až na izomorfismus stejná jako $(H_p, +)$ neboli $(Z_p, +)$ (věta 21), tedy grupa prvočíselného počtu prvků je až na izomorfismus jediná.*

- *Dále grupa o počtu prvků p^2, který je druhou mocninou prvočísla, je podle cvičení G (Pinter 2010, str.154-155) izomorfní buď $(Z_{p^2}, +)$, nebo $(Z_p \times Z_p)$, tedy existují pouze dvě navzájem neizomorfní grupy řádu p^2.*
- *Přehled všech šestiprvkových grup: cvičení F, str. 132.*
- *Přehled všech desetiprvkových grup: cvičení G, str. 132.*
- *Přehled všech osmiprvkových grup: cvičení H, str. 133.*

Následující příklady viz Pinter 2010, str. 141-146:

Příklad 24 *Například A.1.*

a) *Definujte nějaký (aspoň jeden) homomorfismus $f : (Z_8, +) \to (Z_4, +)$:*

$$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ & & & & & & & \end{pmatrix}.$$

b) *Určete jádro K homomorfismu z části (a).*

Příklad 25 *Například A.5: Každá z dvanácti transformací pravidelného šestiúhelníka v grupě $(D_6, \circ)$ (šest pootočení o násobek šedesáti stupňů, včetně identity = pootočení o úhel nulový; dalších šest jsou osové souměrnosti podle tří úhlopříček procházejících protějšími vrcholy (A,D a B,E a C,F) a podle tří spojnic středů protějších stran) nějak permutuje jeho tři úhlopříčky, které si označme čísly 1 (AD), 2 (BE) a 3 (CF), tj. tato současná permutace šesti vrcholů a permutace tří úhlopříček definuje homomorfismus $f : D_6 \to S_3$, v obou grupách uvažujeme operaci skládání permutací. Například*

$$f(id_6) = id_3, \quad f(1,2,3,4,5,6) = (1,2,3).$$

Napište, na jaké prvky se zobrazí tímto homomorfismem zbylých deset prvků grupy D_6. Grupa $(S_3, \circ)$ má prvky: id, $(1,2,3)$, $(1,3,2)$, $(2,3)$, $(1,3)$, $(1,2)$.

Příklad 26 *B. Příklady homomorfismu nekonečných grup:*

Například B.2: Zdůvodněte, proč zobrazení φ je grupovým homomorfismem, a najděte jeho jádro:

$$\varphi : (D(R), +) \to (F(R), +) \text{ je definované vztahem } \varphi(f) = f'$$

($D(R)$ je množina reálných funkcí, u kterých existuje jejich derivace f', a $F(R)$ je množina reálných funkcí).

Například B.3: Zdůvodněte, proč zobrazení f je grupovým homomorfismem, a najděte jeho jádro:

$$f : (R \times R, +) \to (R, +) \text{ je definované vztahem } f([x,y]) = x + y$$

($(R \times R, +)$ je množina je množina uspořádaných dvojic reálných čísel, které sčítáme po složkách).

Příklad 27 *F. Homomorfismus a řád prvku (postup a výsledky tohoto příkladu viz 13.5).*

Například F.1: Pro homomorfismus grup $f : (G, \bigtriangledown) \to (H, *)$ je $a \in G$ prvek řádu n. Vyzkoumejte na příkladech (např A.1), co lze říci o řádu prvku $f(a)$ – POZOR, nemusí být stejný jako řád prvku a.

Například N.3: Dokažte větičku: Grupový homomorfismus zobrazuje generátor cyklické podgrupy na generátor cyklické podgrupy.

Například N.4: Pomocí věty 16 a předchozích dvou větiček F.1, N.3 najděte všechny možné homomorfismy z příkladu A.1, tj. všechny možné homomorfismy grupy $(Z_8, \oplus)$ do grupy $(Z_4, \oplus)$ a určete jejich jádra.

Například N.2: Vypište všechny prvky grup $(Z_9, \oplus)$, $(S_3, \circ)$ a u každého prvku určete jeho řád. Potom popište všechny možné homomorfismy grupy $(Z_9, \oplus)$ do grupy $(S_3, \circ)$, které existují – musíte při každém z nich určit, kam se zobrazí každý prvek množiny Z_9. U každého z těchto homomorfismů určete jeho jádro.

Příklad 28 *Například N.1: Uvažujme homomorfismus φ grupy $(Z_8, \oplus)$ do grupy $(Z_4, \oplus)$ definovaný $\varphi(0) = 0$, $\varphi(1) = 1$, atd.*

a) *Určete jádro K tohoto homomorfismu;*

b) *Jaké prvky má faktorgrupa $Z_8/_K$ s operací rozšířenou na třídy? Je možné vyjádřit obrázkem, ale vyznačte zřetelně prvky faktorgrupy.*

Výsledky některých příkladů najdete v závěru textu v oddílu 13.5.

6 Týden 06

6.1 Cvičení 06: Rezerva, resty z minulých hodin, odpovědi na otázky

6.2 Přednáška 06: struktury se dvěma operacemi

Okruh je po grupě druhou základní definicí struktury v kursech moderní algebry. A je to definice naprosto přirozená. Když totiž zkoumáme množinu Z, nikdy o ní ne přemýšlíme jako o množině s jedinou operací, ale máme současně na mysli sčítání (odčítání je skryto v inverzních prvcích) a násobení (dělení je skryto v inverzních prvcích). Matematik se tedy snaží formulovat, jaké zákonitosti platí pro interakci operací + a $\cdot$. Tato interakce je popsána v definici algebraické struktury zvané okruh:

Definice 25 *okruh (anglicky: ring) je množina $(M, +, \cdot)$ s operacemi + a $\cdot$, které splňují vlastnosti:*

a) *Operace + splňuje vlastnosti (1), (2), (3), (4), (5), tj. $(M, +)$ je komutativní grupa;*

b) *operace $\cdot$ splňuje vlastnosti (1), (2), (3), tj. množina $(M, \cdot)$ je monoid (= pologrupa s jednotkou);*

c) *interakce operací + a $\cdot$ splňuje tzv. distributivní zákon = vlastnost (6):*

$$\forall\ x, y, z \in M : x \cdot (y + z) = x \cdot y + x \cdot z,\ \ (y + z) \cdot x = y \cdot x + z \cdot x$$

(rovnice jsou dvě díky tomu, že operace $\cdot$ není obecně komutativní).

Příklad 29

- *Příkladem konečného okruhu je struktura zbytkových tříd $(Z_n, \oplus, \odot)$.*
- *Příkladem nekonečného okruhu je $(Z, +, \cdot)$, tedy množina celých čísel s tradičními operacemi sčítání a násobení.*

Ovšem struktura $(Z_n, \cdot)$ vykazuje určité defekty, tj. obsahuje tzv, netriviální dělitele nuly:

Definice 26 *nenulový dělitelé nuly jsou takové prvky a, b množiny M, které se nerovnají nule (0 = neutrální prvek v grupě $(M, +)$), ale jejich součin (= výsledek operace násobení v pologrupě $(M, \cdot)$) je roven nule: $a \cdot b = 0$;*

Příklad 30 *Příkladem struktury s nenulovými dělitely nuly je množina Z_6 zbytkových tříd modulo 6: její prvky [2], [3] nebo [3], [4] jsou nenulový dělitelé nuly, protože platí*

$$[2] \odot [3] = [0], \quad [3] \odot [4] = [0].$$

Je vidět, že právě dělitelé nuly způsobují, že v některých pologrupách či monoidech (např. $(Z_6, \odot)$ je monoid vzhledem k operaci $\odot$) neplatí zákon o krácení (7): např. právě v $(Z_6, \oplus, \odot)$ vidíme, že

$$[2] \odot [2] = [2] \odot [5],$$

ale nemůžeme vykrátit z rovnosti třídu [2], protože $[2] \neq [5]$.

Netriviální dělitelé nuly jsou dosti překvapivým jevem, který například u celých čísel nenastane – a také nežádoucím jevem. Okamžitá otázka pro matematický popis vyvstává, kdy se taková situace vyskytne a jak zaručit, že k ní nedojde. Z tohoto důvodu definujeme obor integrity:

Definice 27 *obor integrity*[30] *(anglicky: integral domain) je množina*[31] $(M, +, \cdot)$ *s operacemi* $+$ *a* $\cdot$*, která je okruhem a navíc jsou splněny vlastnosti:*

ad a) *Operace* $+$ *nesplňuje nic navíc;*

ad b) *operace* $\cdot$ *splňuje navíc:*

- *M neobsahuje netriviální dělitele nuly (vzhledem k operaci* $\cdot$*);*
- *vlastnost (5), tj. operace* $\cdot$ *je komutativní na M;*

ad c) *díky komutativitě operace* $\cdot$ *lze distributivní zákon psát v jediné rovnici:*

$$\forall\ x, y, z \in M : x \cdot (y + z) = x \cdot y + x \cdot z = y \cdot x + z \cdot x = (y + z) \cdot x.$$

Příklad 31

- $(Z_7, \oplus, \odot)$ *je konečný obor integrity, protože* 7 *je prvočíslo, tj.* $(Z_7^*, \odot)$ *neobsahuje netriviální dělitele nuly.*
- $(Z, +, \cdot)$ *je nejen nekonečný okruh, ale i nekonečný obor integrity, protože neobsahuje netriviální dělitele nuly a násobení je komutativní, a tedy distributivní zákon lze psát v jedné rovnici.*

V klasické teorii operací se definuje ještě jeden pojem, který je dokonce ještě silnější než obor integrity, a sice těleso:

[30] Význam slova **integrita**: celistvost. Ve stejné rodině významů je i slovo integer = celek, celé číslo. Podobně i slovo „integrál“ vlastně znamená součet, spojení, sečtení. A fráze „is an integral part of ...“ = je nedílnou součástí, je zakomponovanou součástí. V Bibli je hebrejský výraz „:íš támím“ překládán do angličtiny jako „the man of integrity“, do češtiny jako „muž bezúhonný“, ale lepší by byl překlad „celistvý člověk“ ... to neznamená člověk naprosto dokonalý, ale člověk, který je ochoten pracovat na všech třech hlavních oblastech života: na svém vztahu k Bohu, na vztahu k lidem i na svém vztahu k práci. Tedy integrita je něco pozitivního, velmi žádoucího a charakterního. Podobně tomu bude i v matematice: obor integrity neobsahuje patologický jev výskytu netriviálních dělitelů nuly.

[31] Aby byla definice naprosto čistá, měli bychom dodat, že množina je minimálně dvouprvková, obsahuje totiž nulu jako jednotkový prvek vzhledem ke sčítání a jedničku jako jednotkový prvek vzhledem k násobení a $0 \neq 1$.

Definice 28 *Těleso (anglicky: field ... proto některé české učebnice používají též název „pole“) je množina $(M, +, \cdot)$, která je oborem integrity a navíc operace $\cdot$ splňuje vlastnost (4), tj.*

ad a) *Operace $+$ nesplňuje nic nového,*

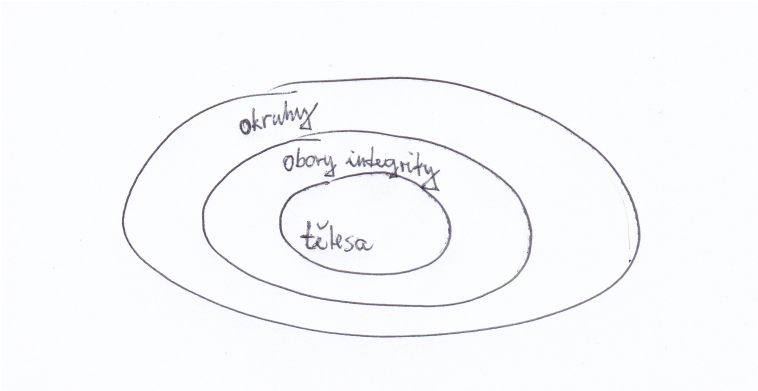
ad b) *operace $\cdot$ splňuje navíc vlastnost (4), tedy $(M - \{0\}, \cdot)$ je grupa*[32]*;*

ad c) *zde nic nového.*

Příklad 32

- *$(Z_7, \oplus, \odot)$ je konečný obor integrity, ale též i konečné těleso, protože v případě konečné množiny M pojmy obor integrity a těleso splývají.*
- *$(Q, +, \cdot)$ je nekonečné těleso, protože $(Q - \{0\}, \cdot)$ je grupa ... je splněna i vlastnost (4), že množina M obsahuje i inverzní prvky vzhledem k operaci násobení.*
- *$(Z, +, \cdot)$ je nekonečný obor integrity, který není tělesem, protože množina Z neobsahuje většinu inverzních prvků vzhledem k operaci násobení.*

Tedy pojmy okruh, obor integrity a těleso představují struktury stále silnějších vlastností:



Obrázek 6.9: Vztah mezi pojmy okruh, obor integrity, těleso.

Každé těleso je oborem integrity, každý obor integrity je i okruh (a z tranzitivity pojmů plyne, že i každé těleso je okruh). Ale naopak to neplatí: existují okruhy, které nejsou oborem integrity, např. $(Z_6, \oplus, \odot)$; a existují obory integrity, které nejsou tělesem, např. $(Z, +, \cdot)$.

Kromě termínů okruh, obor integrity, těleso se někdy v algebraické teorii vyskytují pojmy ideál a hlavní ideál, které bude asi dobré doplnit společně s příklady, a tím se semestr uzavře.

[32] Vlastnost (4) je silnější než vlastnost „neobsahuje netriviální dělitele nuly“, tj. u bodu b) je dostatečné uvést, že operace $\cdot$ u tělesa splňuje (1),(2),(3),(4),(5). Lze dokázat tvrzení, že každé těleso je i oborem integrity, tj. těleso „neobsahuje netriviální dělitele nuly“.

Definice 29 *Ideál je neprázdná podmnožina B okruhu $(M, +, \cdot)$ taková, že $(B, +)$ je podgrupa (tj. B vzhledem k operaci $+$ splňuje vlastnosti (1) a (4)) a navíc B absorbuje součiny na množině M, tj.*

$$\forall b \in B, \;\; m \in M : \;\; b \cdot m \in B$$

(vynásobíme-li prvek množiny B prvkem množiny M, výsledek padne do množiny B).

Příklad 33 *Nejpřirozenějším příkladem ideálu je podmnožina B sudých celých čísel okruhu $(Z, +, \cdot)$:*

$$B = \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

Je zřejmé, že $(B, +)$ je podgrupa grupy $(Z, +)$ a vynásobíme-li sudé číslo jakýmkoli celým číslem, výsledek je opět sudé číslo, tj. množina B absorbuje všechny násobky sebe sama s lichými čísly. Tedy B je ideál v $(Z, +, \cdot)$.

Definice 30 *V teorii ideálů hraje klíčové místo tzv. hlavní ideál okruhu, který definujeme jako takový ideál B, který vygenerujeme jediným prvkem b, jenž vynásobíme se všemi prvky množiny M.*

Příklad 34 *Pro $M = (Z, +, \cdot)$ jsou hlavními ideály tyto množiny:*

- $B_1 :=< 1 >$ *... ideál generovaný prvkem 1 a všemi součiny $1 \cdot z$ pro $z \in Z$, tj. $B_1 = Z$ (okruh $(Z, +, \cdot)$ je sám o sobě hlavním ideálem);*
- $B_2 :=< 2 >$ *... ideál generovaný prvkem 2 a všemi součiny $2 \cdot z$ pro $z \in Z$, tj. jedná se o ideál z příkladu 6.5:*

  $$B = \{\ldots, -4, -2, 0, 2, 4, \ldots\}.$$

- $B_3 :=< 3 >$ *... ideál generovaný prvkem 3 a všemi součiny $3 \cdot z$ pro $z \in Z$, tj.*

  $$B_3 = \{\ldots, -6, -3, 0, 3, 6, \ldots\}.$$

- *atd.*
- *Pokud v okruhu $(Z, +, \cdot)$ vezmeme ideál generovaný dvěma prvky, například $B =< \{3, 7\} >$, jeho prvky jsou například celá čísla dělitelná třemi nebo sedmi, ale POZOR, to nejsou všechny jeho prvky: B musí být grupou vzhledem k operaci sčítání, obsahuje tedy i číslo $7 - 3 = 4$, a pokud obsahuje čísla 3 i 4, obsahuje také jejich rozdíl $4 - 3 = 1$, a pokud obsahuje jedničku, obsahuje vlastně všechna celá čísla, protože jednička vzhledem ke sčítání vygeneruje celou množinu Z, a to je hlavní ideál vzhledem k prvku 1, tedy došli jsme k tomu, že*

  $$< \{3, 7\} >= Z =< 1 > .$$

  Takže není tak jednoduché najít ideál, který není hlavní, protože o množině Z víme, že je hlavním ideálem vzhledem ke generátoru 1. Ve skutečnosti je docela schůdné dokázat matematickou větu, že každý ideál okruhu $(Z, +, \cdot)$ je hlavním ideálem.

Čtenář tohoto textu či student předmětu Algebra 1 si určitě říká, nač je toto vše podrobné studium pojmů, vycházejících většinou z vlastností operací sčítání, násobení, průniku a sjednocení. Rád bych jej ubezpečil, že kromě toho, že zákonitosti jsou samy o sobě zajímavé, posloužily v historii právě v tom nejdůležitějším úkolu algebry, a tedy ke hledání řešení algebraických rovnic. Ve druhé polovině semestru se budeme právě řešením algebraických rovnic zabývat podrobně.

Procvičení pojmů okruh, obor integrity, těleso: např. viz Pinter 2010, kapitola 17 a cvičení na str. 174-178.

Například N.1:

a) Které z vlastností (1) až (10) splňuje struktura $(2^P, \cup, \cap)$ pro $P = \{a, b, c\}$?

b) Jak byste strukturu $(2^P, \cup, \cap)$ z části (a) nazvali (okruh, obor integrity, těleso, nebo něco jiného)?

c) Najděte netriviální dělitele nuly na struktuře $(2^P, \cup, \cap)$. Dejte pozor na to, že „nula“ je vždy prvek vzhledem k první uvedené operaci struktury, zatímco dělitelnost se zkoumá vzhledem ke druhé operaci struktury.

d) Najděte netriviální dělitele nuly na struktuře $(2^P, \cap, \cup)$. Dejte pozor na to, že „nula“ je vždy prvek vzhledem k první uvedené operaci struktury, zatímco dělitelnost se zkoumá vzhledem ke druhé operaci struktury.

Například N.2: Uveďte příklad nekonečného oboru integrity, který není tělesem.

Například D.1:

a) Uvažujme množinu 2^P všech podmnožin množiny $P = \{a, b, c\}$. Na této množině lze definovat operaci symetrického rozdílu $A \div B := (A - B) \cup (B - A)$ a klasickou operaci $\cap$ průniku. Sestavte tabulky operací $\div$ a $\cap$ na množině 2^P.

b) Jak byste strukturu $(2^P, \div, \cap)$ z části (a) algebraicky popsali (je to okruh, obor integrity, těleso, nebo něco jiného)?

Procvičení pojmů ideál, hlavní ideál, homomorfismus okruhů: viz Pinter 2010, kapitola 18 a cvičení na str. 185-189.

Například N.3: Ideál $(D, +, \cdot)$ okruhu celých čísel $(Z, +, \cdot)$ je takový jeho podokruh, který je uzavřený vzhledem k násobení celým číslem, tj.

$$d \cdot z \in D \ \ \forall\, d \in D,\ z \in Z.$$

Uveďte příklad ideálu D okruhu $(Z, +, \cdot)$, který obsahuje číslo 2 a neobsahuje číslo 3.

7 Týden 07

7.1 Cvičení 07: Polynomy 01

Rozklad polynomu na součin polynomů prvního stupně, kořen polynomu, Hornerovo schéma, největší společný dělitel polynomů.

Studenti měli Hornerovo schéma i Eukleidův algoritmus a dělení polynomů v předmětu Diskrétní matematika (MA0001), ale je potřeba zopakovat.

Doporučené materiály k využití:

- Označení: $(Z[x],+,\cdot)$, $(Q[x],+,\cdot)$, $(R[x],+,\cdot)$, ... po řadě okruhy polynomů s koeficienty z okruhu celých čísel, tělesa racionálních čísel a tělesa reálných čísel. Tyto okruhy neobsahují netriviální dělitele nuly, takže se jedná o obory integrity (Budínová 2013, str. 7, věta 1). Ideální definice okruhu $Z[x]$: jedná se o rozšíření okruhu $(Z,+,\cdot)$ o prvek x, kde nevíme, co je, může tam být cokoliv, třeba[33] číslo π. Množina polynomů tedy neobsahuje všechny inverze vzhledem k násobení polynomů.

- Budínová 2013, str.8-10: stupeň polynomu, dělení polynomů se zbytkem ... studenti znají, ale připomeňte.

- Hornerovo schéma (Budínová 2013, str. 10-12), základní věta algebry, vydělte polynom $6x^3+13x^2-1$ polynomem $(x-1)$ nebo $(x+2)$:

  $$a_n\cdot x^n + a_{n-1}\cdot x^{n-1} + \cdots + a_1\cdot x + a_0 = a_n\cdot(x-x_1)\cdot(x-x_2)\cdots(x-x_n),$$

  například

  $$6x^3+13x^2-4 = 6(x+2)(x-\frac{1}{2})(x+\frac{2}{3}).$$

- Budínová 2013, str. 18-21 po pojem ireducubilní polynom, objasnění, že v základní větě algebry se vyskytují ireducibilní polynomy. Dělitel polynomů, největší společný dělitel polynomů, Eukleidův algoritmus: znají, ale připomeňte (na příkladu). Normovaný největší společný dělitel.

- Nalezněte NSD polynomů: Eukleidovým algoritmem (Budínová 2013, str.20, př. 16), rozkladem na součin ireducibilních polynomů (př. 18,19, str. 23 ... upozorněte studenty, že rozklad lze realizovat substitucí (př.18) nebo postupným vytýkáním).

[33] Pinter, 2010, str. 241.

7.2 Přednáška 07: Struktury se dvěma operacemi II

Analogie Cayleyho věty, analogie Lagrangeovy věty, analogie věty o homomorfismu, analogie dobře definované operace na faktorgrupě. Věta o rozšíření těles: polynom s koeficienty z tělesa T nemusí mít kořeny přímo v tělese T, ale to lze rozšířit na těleso F_t, které už obsahuje kořeny původního polynomu.

8 Týden 08

8.1 Cvičení 08: Polynomy 02

Věta o racionálních kořenech polynomu v $(Z[x], +, \cdot)$. Odstranění násobných kořenů polynomu.

Využijte například následující materiál:

- Věta o racionálních kořenech polynomu z $(Z[x], +, \cdot)$ – Budínová 2013, str. 33, věta 24. Příklad. 21 na str. 28: Nalezněte kořeny polynomu $x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8$. Pojem násobnosti kořene, základní věta algebry v terminologii násobnosti kořene.
- Příklady na procvičení: str.34-př.29, str.35-př.30 ... je nutné dělat ty znaménkové změny? To rozhodne cvičící.
- Odstranění násobných kořenů: str.32 poznámka až str. 33 příklad 28. Pak ještě nějaký příklad s násobnými kořeny, např. polynom čtvrtého stupně se dvěma dvojnásobnými komplexně sdruženými kořeny.

8.2 Přednáška 08: Přehled algebraických metod hledání kořene polynomu

9 Týden 09

9.1 Cvičení 09: Polynomy 03

Dodělání osnovy na cvičení pro polynomy, viz plán cvičicího.

9.2 Přednáška 09: Přehled numerických metod hledání kořene polynomu

Hledání iracionálních a komplexních kořenů polynomu numerickými metodami – metoda půlení intervalu, Newtonova metoda.

Použijte např. následující materiál:

- Budínová, Př. 23-str.29: nalezněte řešení algebraické rovnice

$$2x^5 + 3x^4 - 7x^3 + 6x^2 - 11x + 5 = 0.$$

  Hornerovým schématem ověříme, že žádné racionální řešení neexistuje. Všechna řešení tedy jsou reálná iracionální, nebo komplexní.

- A) Hrubá detekce (Budínová, str.29, věta 16): všechny kořeny leží v komplexní rovnice uvnitř kružnice se středem v počátku a poloměrem

$$r = 1 + \frac{max\ \{|a_0|, |a_1|, \ldots, |a_{n-1}|\}}{|a_n|}.$$

  Dosazením do tohoto vzorce v našem příkladu máme

$$|x_i| \leq 1 + \frac{max\{3, 7, 6, 11, 5\}}{2} = 1 + \frac{11}{2} = 6{,}5.$$

  To znamená, že všechna řešení, imaginární i komplexní (a kdyby byla některá racionální, což v našem příkaldu nejsou, tak i ta) leží v Gaussově rovině v kruhu se středem v počátku a poloměrem 6,5.

- B) Jemnější detekce reálných řešení: Ad A ... stále stejný řešený příklad, $|x_i| \leq 6,5$: Víme, že $x_i \in \langle -6{,}5; 6{,}5\rangle$, řešíme rovnici $p(x) = 0$ pro

$$p(x) = 2x^5 + 3x^4 - 7x^3 + 6x^2 - 11x + 5.$$

  Protože $p(x)$ je spojitá funkce, tj. vypočteme $p(h_i)$ pro h_i postupně rovno $-6{,}5$, pak $-6{,}4$, pak $-6{,}3$, ..., pak 6,3, pak 6,4, pak 6,5.

  Pokud se stane pro nějaké i, že $p(h_i) \cdot p(h_{i-1}) < 0$, znamená to, že dvě po sobě jdoucí hodoty mají rozdílná znaménka, tedy objevíme, že na intervalu $\langle h_i; h_{i+1}\rangle$ leží nějaké řešení. Další možností je nakreslit si graf funkce $p(x)$ a intervaly s řešením upřesnit z grafu.

  Celý postup lze snadno předvést v jazyce R (lze volně stahnout a nainstalovat), což je takové lepší offline kalkulačka a kreslička. Napíšeme v tomto prostředí za zobáček

$$x < -seq(from = -6.5, to = 6.5, by = 0.5)$$

(a stiskneme ENTER ... vytvoří se vektor x našich hodnot h_i), pak napíšeme

$$p < -2 * x^5 + 3 * x^4 - 7 * x^3 + 6 * x^2 - 11 * x + 5$$

(a stiskneme ENTER). V paměti se vypočte vektor funkčních hodnot, musíme jej ještě zobrazit na obrazovce, když např. napíšeme pouze písmenko označující proměnnou „p“ a stiskneme ENTER.

Tímto způsobem jsme odhalili, že kořeny leží v intervalech $\langle -3{,}5; -3\rangle$, $\langle 0{,}5; 1\rangle$, $\langle 1; 1{,}5\rangle$. Pokud máme jistotu, že krok 0,5 byl zvolen dostatečně jemně, takže na žádném z těchto tří intervalů se nevyskytuje více řešení současně (to bychom mohli zpřesnit třeba volbou 0,1), znamená to, že zbývající dvě řešení jsou komplexní (a díky větě „pokud $a + ib$ je kořenem polynomu z $(R[x], +, \cdot)$, tak nutně i $a - ib$ je kořenem tohoto polynomu“) víme, že tato řešení jsou komplexně sdružená čísla.

Jiný způsob by zde spočíval v nakreslení grafu polynomu $p(x)$, lze též v jazyce R zadáním posloupnosti bodů, které se vykreslí (ENTER po každém řádku):

$$y < -seq(from = -3.5, to = 3.5, by = 0.01)$$
$$pp < -2 * y^5 + 3 * y^4 - 7 * y^3 + 6 * y^2 - 11 * y + 5$$
$$plot(y, pp)$$

(obrázek lze „zvětšit“ zadáním kratšího intervalu při definici vektoru y, například $from = 0$ a $to = 1.5$ nakreslí graf na sporném intervalu, na kterém existují dvě řešení).

- C) Finální dopočtení kořenů: Do proměnné *pol* v prostředí R si nadefinujeme polynom, jehož funkční hodnoty jsme počítali, jako funkci, která vypočte $pol(k)$ pro jakoukoli hodnotu k:

$$pol < -function(z)return(2 * z^5 + 3 * z^4 - 7 * z^3 + 6 * z^2 - 11 * z + 5)$$

a stiskneme ENTER. Poté zkusíme najít řešení rovnice na intervalu $\langle -3, 5; -3\rangle$ metodou půlení intervalu (vysvětlení viz BP (Trombiková, 2019, str. 28-30)). Celý algoritmus lze naprogramovat v R pomocí cyklu WHILE, například s tou přesností, že délka zkracujícího se intervalu bude menší než 0,00001:

$$a < - - 3.5$$

a ENTER (první minus je součástí přiřazovací šipky, druhé minus je součástí čísla),

$$b < - - 3$$

a ENTER, a dále celý cyklus WHILE napíšeme na jeden řádek (v prostředí R to bude možné, zde v textu to vyjde na více řádků) a stiskneme ENTER:

$$while(abs(a - b) > 0.00001)$$
$$\{if \ \ (pol((a + b)/2) * pol(b) < 0) \ \ \{a < -((a + b)/2); print((a + b)/2)\}$$
$$else \ \ \{b < -((a + b)/2); print((a + b)/2)\}\}$$

(na obrazovku se nyní vypíše posloupnost středů intervalů blížících se k řešení, které zhruba s přesností na pět desetinných míst je $z_1 = -3{,}12991$).

Pokud celý postup (posloupnost tří kroků ukončených ENTER) zopakujeme pouze pro volbu $a = 0{,}5$, $b = 1$, najdeme řešení $z_2 = 0{,}56489$. Toho lze dosáhnout velmi jednoduše, protože v prostředí R nemusíme už jednou napsané příkazy vypisovat znovu, ale volbou šipky nahoru se lze dostat na předchozí tři příkazy, ve kterých pozměníme pouze hodnoty a, b a celý cyklus while beze změny ještě jednou potom zobrazíme šipkou nahoru a stiskneme ENTER.

Poslední reálné iracionální řešení pro $a = 1$, $b = 1{,}5$ najdeme podobně s přesností na pět desetinných míst $z_3 = 1{,}22892$.

Výhoda metody půlení intervalu (metody bisekce): vždy najde řešení, pokud na počátku algoritmu víme, že na daném intervalu existuje řešení právě jedno. Teoreticky (pokud bychom hledali tímto způsobem i kořeny racionální) by mohla po jistém počtu kroků nastat situace, že střed intervalu bude přesně roven hledanému řešení – to ovšem u hledání iracionálního řešení nemůže nastat, protože půlení racionálních čísel a, b a středů z nich vzniklých nelze dostat číslo iracionální, tato posloupnost středů intervalů se pouze bude limitně blížit k řešení.

Metoda Newtonova = metoda tečen: obrázek a vysvětlení viz BP Trombiková, str. 34-38: zvolíme vhodně z_0 a počítáme posloupnost hodnot $z_1, z_2, \ldots$ užitím vzorce

$$z_{n+1} = z_n - \frac{p(z_n)}{p'(z_n)}.$$

Výpočet v prostředí R: Navíc k definici funkce $pol(k)$ z předchozího algoritmu, kterou máme stále v paměti prostředí nadefinovanou (a pokud jsme ukončili práci a při ukončování zvolili ANO na otázku, zda si má prostředí pamatovat uložená data, bude nadefinovaná i při opětovném spuštění prostředí R), budeme potřebovat ještě nadefinovat funkci pro výpočet derivace $p'(x)$ našeho polynomu:

$$der <- function(w)\{return(10 * w^4 + 12 * w^3 - 21 * w^2 + 12 * w - 11)\}$$

(a ENTER). Nyní podobným cyklem WHILE najdeme všechna tři řešení jako u metody půlení, nicméně nyní pomocí metody Newtonovy: rozdíl je zde v tom, že místo intervalu se zadává pouze jediný vstupní bod z:

$$z <- -3.5$$

a ENTER, a provedeme cyklus WHILE:

$$while(abs(pol(z)) > 0.00001)\{z <- z - \frac{pol(z)}{der(z)}; print(z)\}$$

(a ENTER) ... po několika krocích bude nalezeno řešení $z_1 = -3{,}12991$. Podobně pro vstupní $z = -1$ dostaneme $z_3 = 1{,}22892$ a pro vstupní $z = 0{,}5$ dostaneme $z_2 = 0{,}54689$. Slabina Newtonovy metody: díky konstrukci pomocí tečny může postup zcela zhavarovat, směřovat do nekonečna nebo najít řešení, které už známe z jiného intevalu (jak se to stalo při volbě $z = 1$).

Výhody Newtonovy metody ovšem jsou značné: a) najde řešení (pokud je tedy najde) mnohem rychleji než metoda půlení. b) najde i řešení komplexní!!!!!!!!!! Newtonově metodě (ani jazyku R) principiálně nevadí, když pracujeme s čísly komplexními. Jedinou podmínkou zde je, aby počáteční z bylo komplexní, nikoli reálné číslo – pro reálné vstupní z se totiž vzorec metody sám od sebe nikdy nedostane. Zkusme tedy najít zbývající řešení z_4, z_5, které podle základní věty algebry víme, že musí existovat. Newtonovou metodou:

- Volme vstupní $z = 1+1i$, najeďme šipkou na příkaz cyklu WHILE a stiskněme enter ... dospíváme k řešení $z_2 = 0{,}56489$ ... to se tedy může stát, že volbou komplexního vstupního z celá posloupnost konstruovaných čísel konverguje k řešení reálnému.
- Zkusme jiné vstupní $z = 1 + 3i$ z našeho kruhu v komplexní rovině $|z| \leq 6{,}5$: dojdeme k řešení $z_4 = -0{,}07295 + i \cdot 1{,}08773$ s přesností na pět desetinných míst, a díky teoretické větě o komplexně sdružených kořenech už nemusíme dále počítat, stačí psát $z_5 = -0{,}07295 - i \cdot 1{,}08773$.

- Našli jsme tedy podle numerických metod všechna řešení, která podle přesných algebraických postupů najít nelze – přesněji řečeno, nenašli jsme je zcela přesně, pouze s přesností na pět desetinných míst, to je ovšem přesnost dostatečná.

- Celkem jednoduchou metodou lze najít komplexní řešení speciální rovnice, tzv. binomické rovnice, protože je v této rovnici pouze binom = dvojčlen: mocnina neznámé z a nějaké komplexní číslo. Tento poslední rychlý způsob pro tuto speciální rovnici se studenti naučí v následujících čtrnácti dnech, které budou věnovány komplexním číslům.

10 Týden 10

10.1 Cvičení 10: Komplexní čísla 01

Operace s komplexními čísly, algebraický a goniometrický tvar komplexního čísla (argument a velikost komplexního čísla), geometrický význam násobení a dělení komplexních čísel.

Lze postupovat podle nejnovější učebnice pro střední školy (Robová, Hála, Calda 2013), ale vše se asi nestihne, tj. cvičící rozhodnou, co přesně ve cvičeních 10 a 11 stihne probrat.

10.2 Přednáška 10: Konstrukce číselných oborů

Peanova množina (= axiomy množiny N), konstrukce $N \rightarrow Z$, konstrukce $Z \rightarrow Q$, konstrukce $Q \rightarrow R$.

11 Týden 11

11.1 Cvičení 11: Komplexní čísla 02

n-tá mocnina a n-tá odmocnina z komplexního čísla, řešení binomických rovnic.

11.2 Přednáška 11: Konstrukce oboru C, o komplexních číslech

12 Týden 12

12.1 Cvičení 12: Prověrka-b na polynomy a komplexní čísla

12.2 Přednáška 12: Příprava a otázky ke zkoušce

Otázka 01. Struktury s jednou binární operací a jejich vlastnosti.

- Definice binární operace na množině.
- Vyberte si příklad jedné konečné množiny s jednou operací, a jedné nekonečné množiny s jednou operací (prosím volte jiné operace než operace průniku, sjednocení, rozdílu, symetrického rozdílu ... množinové operace budou tématem otázky 02) – vypište vlastnosti těchto operací a řekněte, o jaké algebraické struktury se vzhledem k této operaci jedná.
- Pokud je to možné či snadno proveditelné či to víte, zdůvodněte, proč vlastnosti platí: např. platí vlastnost neutrálního prvku, protože jím je ... ; platí vlastnost existence inverzí, protože například pro ... je inverzí ...

Otázka 02. Množinové operace a jejich vlastnosti. Uvažujte strukturu 2^A pro $A = \{1, 2, 3, 4, 5\}$, tj. množinu všech podmnožin množiny A.

- Co za algebraickou strukturu (viz přednáška 6: struktury se dvěma operacemi) je $(2^A, \div, \cap)$? Uveďte u každé z operací neutrální prvek a příklad, že existuje-neexistuje inverzní prvek.
- Jednotlivé vlastnosti těchto operací jsou vlastně vztahy mezi množinami. Dokažte některý z nich, ideálně například distributivní zákon (pomocí Vennových diagramů).
- Obsahuje tato struktura nenulové dělitele nuly? Uveďte příklad.
- Doplňující nedůležitá[34] otázka: Operace průniku, sjednocení a symetrického rozdílu jsou tzv. binární operace. Znáte nějaký příklad unární množinové operace – do operace vstupuje jen jedna množina, nikoli dvě? Odpověď: příkladem unární operace je operace doplňku – doplněk vždy hledáme jen pro jednu množinu. Zajímavou vlastností jsou tzv. de Morganova pravidla (Základy mat., přednáška 4), která vyjadřují vztah mezi binární operací sjednocení-průniku a unární operací doplňku. Dokazují se jak jinak, pomocí Vennových diagramů.
- Doplňující nedůležitá, ale zajímavá otázka: Mají operace průniku a sjednocení množin nějakou vlastnost, kterou nemají operace sčítání a násobení čísel? Odpověď: jednu zajímavost speciální pro sjednocení a průnik v kombinaci jsem říkal v přednášce číslo 6 (zaměnitelnost operací v distributivním zákonu). Ale existují i další vlastnosti např. samotného průniku či samotného sjednocení (tzv. idempotence[35]), nebo další vlastnosti interakce operací sjednocení a průniku (absorbce, modularita). Všechny se dokazují pomocí Vennových diagramů.

[34] Nedůležité otázky jsou zajímavé z hlediska matematiky, ale nerozhodnou o tom, zda zkoušku složíte nebo ne – věnujte se v prvé řadě otázkám, které jako nedůležité označeny nejsou; ty byste znát měli. Nedůležité otázky ovšem můžete dostat třeba u státnic, tj. je dobré se zamyslet nad odpovědí.

[35] Např. $X^2 = X \cup X = X$, nebo $X^3 = X \cup X \cup X = X$ ... tj. vzhledem k operaci sjednocení neexistují mocniny, „umocňováním“ dostaneme zase jen množinu X. Naprosto jiné než u čísel.

Otázka 03: Pojem homomorfismu a jeho význam.

- Uveďte definici homomorfismu mezi grupoidy.
- Řekněte, jak se přirozeně (jak jsme si říkali na přednášce 03) definuje homomorfismus grupy $(Z, +)$ do grupy $(Z_6, +)$. Tento homomorfismus není prostý, ale je surjektivním zobrazením. Co je pro pojem surjektivního homomorfismu charakteristické?

  Odpověď na část otázky: Surjektivní homomorfismus redukuje množinu Z na menší množinu Z_6, na které některé vlastnosti zůstaly zachovány (např. zbytek po dělení číslem 6 je stejný u vzoru i obrazu tohoto zobrazení), kdežto některé vlastnosti zachovány nebyly (ztratila se nekonečnost množiny Z, např. všech nekonečně mnoho násobků čísla 6 se zredukovalo do jednoho prvku $[0]$). Tedy pokud chceme pracovat pouze se zbytky po dělení šesti, vlastně ve svém přemýšlení-vyjadřování provádíme fiktivní homomorfismus množiny celých čísel na množinu zbytků.
- Co je charakteristické pro pojem injektivního homomorfismu?

  Odpověď: Pojem injektivního homomorfismu se objevuje například při konstrukci nebo koncepčním přechodu od množiny N na množinu Z. Formálně do množiny N „přidáváme“ další prvky, a přitom ovšem chceme, aby dosavadní pojetí přirozených čísel (včetně výsledků operací sčítání a násobení) zůstalo zachováno. To přesně „kontroluje“, dokazuje či „zaručuje“ homomorfismus $\psi : \ N \ \to \ N \times N/_{\sim}$. Mluvíme o VNOŘENÍ množiny N do množiny $N \times N/_{\sim}$, která má více prvků (nekonečně mnoho dalších prvků) – ty jsou „modelem“ nuly a záporných čísel. Tedy v tomto pohledu injektivní homomorfismus přesně matematicky ukazuje, že při přechodu od N k Z na ZŠ zachováváme dosavadní pojetí práce s čísly, pouze „rozšiřujeme“ toto pojetí čísla na nadmnožinu Z. (podobnou argumentaci lze provést při rozšíření Z na Q)
- Nějaké vlastnosti homomorfismu dokažte:
  - homomorfismus zobrazuje neutrální prvek na neutrální prvek,
  - homomorfismus „zachovává inverze“ v tom smyslu, že prvky $f(x^{-1}) = (f(x))^{-1}$,
  - $Ker(\varphi)$ je podgrupa grupy $(G_1, \bigtriangledown)$ při homomorfismu grupy $(G_1, \bigtriangledown)$ do grupy $(G_2, \star)$,
  - $Im(\varphi)$ je podgrupa grupy $(G_2, \star)$ při homomorfismu grupy $(G_1, \bigtriangledown)$ do grupy $(G_2, \star)$.
- U pojmu jádra homomorfismu se zkuste zamyslet nad příklady 24 a 26 na str. 58, nebo si přečtěte příklad 27 na str. 59 a jeho řešení na konci skript v oddílu 13.5.

Otázka 04: Pojem izomorfismu a jeho význam.

- Definice izomorfismu mezi grupoidy[36].
- Jaký je význam izomorfismu?

  Odpověď: Izomorfismus i homomorfismus v algebře slouží pro porovnávání různých algebraických struktur – pokud mezi dvěma strukturami lze zavést homomorfismus nebo izomorfismus, popíšeme tím dosti velkou příbuznost těchto struktur, protože při homomorfismu i izomorfismu jsou zachovány výsledky dané operace. Izomorfismus (= bijekce zachovávající výsledky operace) nám představuje velmi silné algebraické tvrzení: operace na obou množinách vykazuje naprosto stejné vlastnosti. Například

  – izomorfismus zobrazí podgrupu na podgrupu o stejném počtu prvků. Srovnání s homomorfismem: Homomorfismus též zobrazí podgrupu na podgrupu, ale počet prvků se může redukovat – uvažujte například homomorfismus $(Z_8, +)$ na $(Z_4, +)$. definovaný

  $$f = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 0 & 1 & 2 & 3 & 0 & 1 & 2 & 3 \end{pmatrix}.$$

  Podgrupa $\langle 2 \rangle := \{0, 2, 4, 6\}$ grupy Z_8 se zobrazí na podgrupu $\langle 2 \rangle := \{0, 2\}$ grupy Z_4.

  – izomorfismus zobrazí prvek řádu 3 na prvek řádu 3. Srovnání s homomorfismem: řád obrazu u homomorfismu může být nižší než řád vzoru – uvažujte například homomorfismus $(Z_8, +)$ na $(Z_4, +)$ (viz výše): řád prvku 2 v Z_8 je roven čtyřem, řád obrazu 2 v Z_4 je roven dvěma (řád obrazu u homomorfismu nemusí být stejný, ale je dělitelem řádu vzoru).

  – izomorfismus zobrazí cyklickou podgrupu na cyklickou podgrupu o stejném počtu prvků. Srovnání s homomorfismem, ad homomorfismus $(Z_8, +)$ na $(Z_4, +)$ (viz výše): Cyklická čtyřprvková podgrupa $\langle 2 \rangle$ grupy Z_8 se zobrazí na cyklickou dvouprvkovou podgrupu $\langle 2 \rangle$ grupy Z_4.

  – atd.

  Tedy pokud přeznačíme prvky první struktury příslušnými prvky druhé struktury určenými izomorfismem, daná tabulka operace první struktury (pokud prvky v záhlaví tabulky napíšeme ve stejném pořadí) bude naprosto totožná jako tabulka operace druhé struktury.

- Příklad: Rozhodněte, které z grup $(\{1, -1, i, -i\}, \cdot)$, $(Z_4, +)$, $(Z_2 \times Z_2, +)$ jsou mezi sebou izomorfní (= vykazují naprosto stejné vlastnosti dané operace, kromě toho, že se jedná o bijekci)a které ne.

[36] Grupoidy jsou struktury s nejmenším možným počtem podmínek (jedinou – uzavřeností operace na dané množině), mezi kterými lze homomorfismus nebo izomorfismus definovat. V realitě pak velmi často studujeme či popisujeme homomorfismus či izomorfismus grup, kde platí v každé struktuře už podmínky čtyři.

- Další příklady, které by se mohly objevit: Str. 52, příklad 5.1, například N.4; str. 53, příklad 5.2, různé například o izomorfismu.

Otázka 05: Grupa permutací a Cayleyho věta

- Vypište celou tabulku operace skládání permutací grupy S_3.
- Z tabulky vyčtěte základní informace o inverzních prvcích a podgrupách, neutrálním prvku.
- Co říká Cayleyho věta?
- Ilustrujte Cayleyho větu na konečné grupě $(Z_3, +)$ a nekonečné grupě $(Z, +)$.
- Mohl by se objevit např. příklad: Jakou osmiprvkovou podgrupu grupy $(S_4, \circ)$ vygenerují cykly $(1, 2, 3, 4)$ a $(1, 2)$ při operaci skládání permutací? Nápověda: nemusíte vypisovat celou tabulku operace, ale při vytváření tabulky operace se objevují různé prvky jako výsledky, tj. sestavit aspoň část této tabulky by vám pomohlo.

Otázka 06: Dihedrální grupy D_3 (grupa symetrií trojúhelníka), D_4 (grupa symetrií čtverce), D_5 (grupa symetrií pětiúhelníku pravidelného), D_6 (grupa symetrií šestiúhelníka pravidelného) a Lagrangeova věta.

- Vysvětlete prvky těchto grup geometricky i v jejich algebraickém tvaru.
- Zkonstruujte tabulky operace skládání zobrazení v těchto grupách, nebo v některých podgrupách.
- Co je tvrzením Lagrangeovy věty?
- Vypište na základě geometrického významu i Lagrangeovy věty všechny podgrupy těchto grup.
- Určete množinu generátorů dané grupy.
- Mohl by se třeba objevit příklad 25 ze str. 58.

Otázka 07: Struktury se dvěma operacemi. Viz přednáška 6:

- Definujte okruh; uveďte příklad okruhu zbytkových tříd, který není oborem integrity, včetně vysvětlení a příkladu nenulových dělitelů nuly.
- Definujte obor integrity; uveďte příklad a) okruhu zbytkových tříd, který je oborem integrity; b) oboru integrity, který není tělesem.

- Definujte těleso; uveďte příklad a) konečného, b) nekonečného tělesa.
- Dokažte větičku: Každý konečný obor integrity je už automaticky tělesem (důkaz viz video 12).
- Dokažte větičku (důkaz lépe viz video 12): V okruhu platí: Daný okruh $(M, +, \cdot)$ je obor integrity právě tehdy, když v něm platí vlastnost krácení (7∗) pro okruhy:

$$\forall a, b, c \in M, \quad a \neq 0, \quad : a \cdot b = a \cdot c \implies b = c.$$

Otázka 08: Polynomické rovnice – algebraické metody řešení. Viz přednáška 7 a kousek předn 8. U zkoušky z algebry 1 tato otázka nebude, ale bude opět u bakalářských zkoušek na konci třetího ročníku.

- Co je to množina všech polynomů $(R[x], +, \cdot)$ s reálnými koeficienty, s operacemi sčítání a násobení, z algebraického hlediska?
- Co je to polynom stupně n, vedoucí koeficient polynomu, kořen polynomu, násobnost kořene? Co říká základní věta algebry?
- Co říká věta o racionálních kořenech polynomu a jak je lze určit pomocí Hornerova schématu?
- Co říká „věta o odstranění násobných kořenů polynomu“? Popište postup, příklad uvádět nemusíte (přednáška 8, oddíl B).
- Co je zajímavé na komplexních kořenech polynomu z $R[x]$? Odpověď: věta z oddílu C přednášky 8.

Otázka 09: Polynomické rovnice – numerické metody řešení. Viz přednáška číslo 8, nebo i ve skriptech cvičení číslo 9.

- Jak lze zhruba vymezit všechny kořeny polynomu? Odpověď: Oddíly A ze cvičení 9 v tomto textu.
- Jak lze zhruba najít interval, na kterém existuje reálné řešení polynomu, který jsme zbavili násobných kořenů[37]? Odpověď: oddíl B ze cvičení 9 v tomto textu.

[37]Tento předpoklad jsem v přednášce 8 nezmínil a je důležitý: Kdybychom totiž zkoumali polynom $p(x)$, aniž bychom snížili stupeň polynomu při vícenásobných kořenech postupem popsaným na přednášce, mohlo by dojít k situaci, že některé reálné kořeny mají násobnost 2 nebo 4 atd. zkrátka násobnost sudou. Při zkoumání grafu funkce $p(x)$ pak neplatí skutečnost, že by funkce přecházela v bodě kořene se sudou násobností ze záporných funkčních hodnot na kladné (nebo z kladných funkčních hodnot na záporné), nýbrž graf funkce $p(x)$ se v blízkosti kořene blíží k ose x, v bodě kořene x_k se jí dotkne a „odrazí se na tutéž stranu“, tj. např. $p(x) < 0$ pro $x < x_k$, pak $p(x_k) = 0$, ale pak $p(x) < 0$ nastane i pro $x > x_k$, tj.

- Popište na příkladu, jak upřesníme iracionální kořen polynomu získaný z oddílu F, pomocí metody půlení intervalu a metody Newtonovy. Najděte řešení rovnice $x^5 - x^2 - 1 = 0$ na intervalu $\langle 1; 2\rangle$ oběma těmito numerickými metodami ... proveďte tři kroky u každé z metod. Je možné, že u zkoušky zde bude jiná rovnice, například rovnice $2x^3 + 5x - 1 = 0$, a interval délky 1, který obsahuje řešení, budete muset sami najít.

Otázka 10: Peanova množina P, množina N přirozených čísel. Viz předn. 9.

- Peanovy axiomy,
- vztah množin P a N,
- definice uspořádání na P,
- Z Peanových axiomů lze tedy zkostruovat algebraickou strukturu $(P_0, +, \cdot)$, resp. $(N_0, +, \cdot)$. Celý tento postup jsme si vlastně neříkali (ještě zbývá definovat operace sčítání a násobení na Peanově množině a dokázat, že splňují běžné vlastnosti), uveďte pouze pojem, který strukturu $(N_0, +, \cdot)$ vystihuje.

Otázka 11: Algebraický popis, jak z N zkonstruujeme Z. Viz přednáška 9, odkazy jsou vzhledem ke skenu přípravy.

- Popište konstrukci intuitivně (viz předn. 9, strana 3, oddíl (a)) a řekněte, jaké jsou algebraické vlastnosti výsledku $(Z, +, \cdot)$.
- Popište konstrukci přesně algebraicky – minimálně poslední strana z přednášky 9, mohl by stačit i dobře okomentovaný obrázek z té poslední strany (když se naučíte celou stranu, to je vlastně komentář k obrázku)[38].

Otázka 12: Algebraický popis, jak ze Z zkonstruujeme Q

neplatí, že by funkční hodnoty $p(x)$ při průchodu proměnné x bodem x_k měnily znaménko. To znamená, že postupné počítání funkčních hodnot z intervalu $(-r; r)$ takový kořen neodhalí. Tomuto problému se vyhneme, když provedeme postup odstranění násobných kořenů polynomu. Potom při výpočtu funkčních hodnot v intervalu $(-r; r)$ s dostatečně malým krokem odhalíme už všechny iracionální jednonásobné kořeny pomocí na přednášce popsané změny znaménka funkční hodnoty při procházení tohoto kořene.

[38] Poznámka k bodu (iii) této konstrukce: Faktormnožinu jsme mockrát nevytvářeli, ale jedná se o proces analogický vytvoření struktury zbytkových tříd, například Z_5 – přitom jsme také rozdělili množinu na podmnožiny a definovali sčítání a násobení mezi těmito podmnožinami pomocí tzv. „reprezentantů“ z těchto podmnožin, tj. jakýchkoli prvků z nich vybraných. Přesně stejný proces zde děláme, ale nikoli tedy s množinou Z, ale s množinou $N \times N$ – rozdělíme ji na podmnožiny, každá z podmnožin má nekonečně mnoho prvků, definujeme pak v kroku (iv) sčítání mezi těmito podmnožinami pomocí libovolných reprezentantů z podmnožin vybraných, a výsledkem sčítání není jen jedna uspořádaná dvojice, ale zase jedna celá podmnožina, která součet těch dvou vybraných reprezentantů obsahuje.

- Popište konstrukci intuitivně (viz předn. 9, strana 3, oddíl (b) vzhledem ke skenu přípravy) a řekněte, jaké jsou algebraické vlastnosti výsledku $(Q, +, \cdot)$.
- Popište konstrukci přesně algebraicky – minimálně první strana z přednášky 10, mohl by stačit i dobře okomentovaný obrázek z této strany (doporučuji se kroky a,b,c,d též naučit).

Otázka 13: Algebraický popis, jak z Q zkonstruujeme R pomocí řezů množiny Q.

Otázka 14: Algebraický popis, jak z R zkonstruujeme C.

Informace ke zkoušce v předmětu Algebra 1 v roce 2021: u zkoušky dostanete čtyři z předchozích otázek nebo jejich části, asi v následujícím složení:

1. jednu z otázek 1,2,7 ... základní definice vlastností operace, algebraických struktur;
2. jednu z otázek 3,4,5,6 ... něco o homomorfismu, izomorfismu, grupě permutací S_n nebo dihedrální grupě D_n;
3. otázku 8 nedostanete, ta byla prozkoušena na cvičení; ale všichni dostanete otázku 9, tj. přineste si kalkulačku a pro zadanou rovnici a interval a) najdete interval délky 1 obsahující řešení, b) zpřesníte řešení metodou půlení, c) zpřesníte řešení metodou Newtonovou;
4. jednu z otázek 10 až 14 nebo jejich části.

13 Výsledky některých příkladů

13.1 Výsledky ke cvičení 1.1 – zatím žádné nejsou uvedeny

13.2 Výsledky ke cvičení 1.2 – Určování vlastností různých operací

Ad úloha 1.3:

a) $(N,+)$ je komutativní pologrupa. Opravdu, operace sčítání je komutativní – platí (5). Sečtením dvou přirozených čísel je zase přirozené číslo – platí (1). Sečtení tří čísel z N nezáleží na uzávorkování – platí (2). Vlastnosti (1),(2) platí na struktuře, která se nazývá pologrupa. Vlastnost (3) neplatí, protože 0 = jednotkový prvek vzhledem ke sčítání, není přirozené číslo (eventuálně bychom mohli tvrdit, že $(N_0,+)$ je monoid). Vlastnost (4) na $(N,+)$ neplatí, protože např. inverzní prvek k 2 je -2, ale $-2 \notin N$. □

b) $(Z,+)$ je komutativní grupa.

c) $(Z,\cdot)$ je komutativní monoid. Opravdu, násobení je komutativní – platí (5). Vynásobením dvou celých čísel je zase celé číslo – platí (1). Násobení tří čísel nezávisí na uzávorkování – platí (2). Jednotkovým prvkem vzhledem k násobení je číslo 1, což je celé číslo – platí tedy (3), tedy $(Z,\cdot)$ je monoid. Ovšem inverzní prvky vzhledem k násobení nejsou celá čísla: např. inverzí k číslu 2 vzhledem k násobení je $\frac{1}{2}$, ale to není celé číslo, inverzí k 3 je $\frac{1}{3}$, ale $\frac{1}{3} \notin Z$, atd. □

d) $(Q,\cdot)$, $(R,\cdot)$ jsou komutativní monoidy. Opravdu, přece jen chybí ještě jeden inverzní prvek vzhledem k operaci násobení, a sice pro nulu: rovnice $0 \cdot x = 1$ nemá řešení na množině Q nebo R, tj. neplatí vlastnost (4), dané množiny nejsou grupami vzhledem k násobení. □

e) $(Q-\{0\},\cdot)$, $(R-\{0\},\cdot)$ jsou komutativní grupy. Někdy též značíme

$$Q^* := Q-\{0\}, \quad R^* := R-\{0\},$$

tj. $(Q^*,\cdot)$, $(R^*,\cdot)$ jsou komutativní grupy.

f),g) $(2^A,\cup)$, $(2^A,\cap)$ jsou komutativní monoidy. Opravdu, sjednocením či průnikem dvou podmnožin dané množiny A je zase nějaká podmnožina množiny A – platí (1). Operace $\cup$ a $\cap$ nezáleží na uzávorkování – platí (2). Jednotkovým prvkem vzhledem ke sjednocení je $\emptyset$, jednotkovým prvkem vzhledem k průniku je celá množina A ... platí (3) vzhledem k oběma operacím. Inverze ke mnoha prvkům této struktury neexistují – například pro operaci sjednocení a podmnožinu $\{a\}$ množiny $A = \{a,b,c,d,e\}$ by musela existovat podmnožina X množiny A, aby $\{a\} \cup X = \emptyset$, a to neexistuje.

h) $(Z,-)$ je jen grupoid, protože operace MINUS není asociativní, tj. záleží na uzávorkování; $(Z,:)$ není ani grupoid, protože výsledek dělení řady celých čísel není celé číslo.

i) $(M,+)$, kde $M = \{-100,-99,-98,\ldots,-1,0,1,2,\ldots,99,100\}$ není ani grupoid, protože součtem některých dvojic dostaneme číslo, které neleží v množině M.

13.3 Výsledky ke cvičení 3.1 – Vlastnosti grup, podgrupy a generátory grupy

Ad úloha 3.3 – F.2: Na jednom řádku operace v grupě nemohou být stejné dva prvky, protože v grupě platí zákon o krácení (7). Sporem: Na jednom řádku se vyskytují různé x_1 a x_2. Rovnici

$$a * x_1 = y = a * x_2$$

vynásobíme prvkem A^{-1} zleva a dostaneme po využití vlastnosti (3) na obou stranách rovnosti dostaneme $x_1 = x_2$, což je spor s tím, že x_1 a x_2 jsou různé prvky.

Ad F.3: Tabulku lze doplnit na:

$\star$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

.

Ad úloha 3.6 – A.1: H je podgrupou grupy G, protože (1) součet logaritmů je logaritmus součinu a součin kladných hodnot je zase kladná hodnota, tj. H je uzavřená vzhledem k součtu. Dále je neprázdná, obsahuje např. prvek $\log 1$, což je neutrální prvek vzhledem ke sčítání (platí (3)). Asociativita se sveze z asociativity grupy $(R,+)$, platí (2). A nakonec inverzní prvek k prvku $\log a$ je prvek $\log \frac{1}{a}$, protože platí (4): pro každé $\log a \in H$

$$\log a + \log \frac{1}{a} = \log 1 = 0.$$

Ad A.5:ano, jedná se o podgrupu, prvky grupy jsou body na přímce procházející počátkem, operace sčítání těchto prvků (funguje stejně jako operace sčítání vektorů s počátečním bodem v počátku a koncovým bodem v daném prvku) splňuje vlastnosti (1), (4 ... inverzní prvek k prvku $(x,2x)$ je prvek $(-x,-2x)$, který opět leží na dané přímce) a množina je jasně neprázdná.

Ad D.5: Pokud dané součiny jsou navzájem různé prvky (to plyne mimo jiné z úlohy F.2 z minulého cvičení, že na jednom řádku operace grupy nemohou být stejné prvky), jeden z těchto součinů musí být roven neutrálnímu prvku n, tj. nechť například $a_i * a_l = n$, pak podle věty 4 platí $a_i^{-1} = a_l$, našli jsme inverzi k prvku a_i, platí vlastnost (4).

Ad úloha 3.7 – ad N.1: $H = \{6,12,2,8,14,4,10,0\}$ a prvky jsou napsány v tom pořadí, jak je získáváme užitím prvku 6.

Ad E.1: podgrupy jsou čtyři: a) celá H_{10} generovaná prvkem 1 nebo prvkem 3 nebo prvkem 7 nebo prvkem 9;

b) druhá triviální podgrupa $(\{0\}, +)$ generovaná prvkem 0;
c) podgrupa $(\{0, 2, 4, 6, 8\}, +)$ generovaná prvkem 2 nebo prvkem 4 nebo prvkem 6 nebo prvkem 8;
d) podgrupa $(\{0, 5\}, +)$ generovaná prvkem 5;

Ad E.3: $< 6, 9 >= \{6, 0, 9, 3\}$ vzhledem k operaci skládání otáčení.

Ad E.7 modifikace: prvek $[1, 1]$ je generátorem podgrupy $\{[1; 1;], [0; 2], [1; 3], [0; 0]\}$ vzhledem ke sčítání.

Ad E.6: ano, prvek $[1, 1]$ je generátorem celé grupy vzhledem ke sčítání. Grupa má šest prvků a výsledek lze vyčíst z tabulky operace v této grupě.

13.4 Výsledky ke cvičení 4.1 – nekomutativní grupy

Ad úloha 4.1: Podle definice skládání zobrazení platí

$$P \circ R^2 = P \circ R \circ R = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 7 & 1 & 6 & 3 & 4 & 2 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 7 & 2 & 6 & 3 & 1 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 7 & 3 & 2 & 1 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 7 & 3 & 2 & 1 & 5 & 4 \end{pmatrix}.$$

Ad úloha 4.3: Zde je jen výsledek k první části příkladu, a sice tabulka operace $\circ$ na množině D_3 symetrií trojúhelníku:

Tabulka 13.7: Tabulka operace $\circ$ na množině D_3 symetrií trojúhelníku.

$\circ$	R_0	R_1	R_2	R_3	R_4	R_5
R_0	R_0	R_1	R_2	R_3	R_4	R_5
R_1	R_1	R_2	R_0	R_5	R_3	R_4
R_2	R_2	R_0	R_1	R_4	R_5	R_3
R_3	R_3	R_4	R_5	R_0	R_1	R_2
R_4	R_4	R_5	R_3	R_2	R_0	R_1
R_5	R_5	R_3	R_4	R_1	R_2	R_0

Pokud tuto tabulku porovnáme s tabulkou grupy $(S_3, \circ)$ v příkladu 4 je vidět, že mezi oběma grupami existuje izomorfismus, tj. příslušné tabulky operace se liší pouze

přeznačením prvků: $f(e) = R_0$, $f(s) = R_1$, $f(t) = R_2$, $f(u) = R_3$, $f(v) = R_4$, $f(w) = R_5$ (toto izomorfní přiřazení je vidět i na obrázku 1.1). Aby zobrazení f bylo izomorfismem, musíme z tabulky operace první grupy dostat přeznačením prvků vzhledem k zobrazení f přesně tutéž tabulku vzhledem k operaci v druhé grupě.

13.5 Výsledky ke cvičení 5.1 – řád prvku, cyklické grupy, grupy zbytkových tříd

ad Cvičení 5.1.

Například N.4: α i β vyjádříme jako součin navzájem nezávislých cyklů:

$$\alpha = (1,2) \circ (3,4,5), \quad \beta = (1,6,7,2,5).$$

Pak lze cykly zvlášť umocnit a spojit: $\alpha^3 = (1,2) \circ \mathrm{id} = (1,2)$, $\beta^4 = (1,5,2,7,6)$[39]. Spočteme „součin“ a rozložíme na dílčí „součin“ navzájem nezávislých cyklů:

$$\alpha^3 \circ \beta^4 = (1,5) \circ (2,7,6).$$

Při umocnění na pátou nyní opět umocníme každý cyklus zvlášť:

$$(\alpha^3 \circ \beta^4)^5 = (1,5) \circ (2,6,7).$$

Řád cyklu $(1,5)$ je 2, řád cyklu $(2,6,7)$ je 3, a tedy řád jejich složení je nejmenší společný násobek dílčích řádů, tedy 6.

Následují některé výsledky příkladů z přednášky **??** o homomorfismu a Lagrangeově větě:

Ad příklad 27 Ad Například F.1: Řád obrazu je dělitelem řádu vzoru. Lze i celkem jednoduše dokázat: Sporem ... předpokládejme, že prvek a řádu k se zobrazí na prvek řádu l, kde l není dělitelem k, tj. $k = l \cdot q + m$, kde $0 < m < l$. Označme ještě e_1 neutrální prvek v grupě $G_1 = (G, \bigtriangledown)$, e_2 je neutrální prvek v grupě $G_2 = (H, *)$. Celkem máme

$$e_2 = \varphi(e_1) = \varphi(a^k) = \varphi(a^{l \cdot q + m}) = \varphi(a)^{l \cdot q} * \varphi(a)^m = e_2 * \varphi(a)^m,$$

což je spor s tím, že řád prvku $\varphi(a)$ není m, ale větší číslo l.

Ad Například N.3: Nevím, jak přesně dokázat, ale nebude to težké – snad stačí říci, že to plyne z předchozí větičky N.1 a vlastnosti zachování operace u homomorfismu. Pokud zobrazíme generátor na generátor, obrazy všech ostatních prvků už jsou jednoznačně určeny. Důkaz: Když a je generátor cyklické podgrupy první grupy, $\varphi(a)$ jistě také vygeneruje nějaké prvky svými mocninami, a podle větičky N.1 jich bude tolik, že jejich

[39] Mimochodem: protože Podgrupa generovaná permutací β je cyklická a prvek β je řádu 5 (cyklus délky k je řádu k, platí $\beta^5 = \mathrm{id}$, a tedy $\beta^4 = \beta^{-1}$ ... inverzním prvkem k cyklu β je mocnina prvku β o jedničku nižší než řád prvku β.

počet dělí řád prvku a v první grupě.

Ad Například N.4: 0 se v každém homomorfismu zobrazí na 0. Dále $(Z_8, \oplus)$ je cyklická grupa generovaná např.prvkem 1. Tedy celý homomorfismus je jednoznačně určen, zadáme-li obraz generátoru 1.

hom 01: $0 \xrightarrow{\varphi} 0$, $1 \xrightarrow{\varphi} 0$ ... pokud se generátor zobrazí na nulu, aby byla splněna podmínka homomorfismu, všechny další prvky se zobrazí na nulu. Jádrem je tedy celá množina Z_8.

hom 02: $0 \xrightarrow{\varphi} 0$, $1 \xrightarrow{\varphi} 1$ ... podle podmínky homomorfismu nyní dopočteme, že musí nastat $2 = 1+1 \xrightarrow{\varphi} \varphi(1)+\varphi(1) = 2$, dále $3 = 2+1 \xrightarrow{\varphi} \varphi(2)+\varphi(1) = 2+1 = 3$, atd. Jádrem je množina $\{0, 4\}$

hom 03: $0 \xrightarrow{\varphi} 0$, $1 \xrightarrow{\varphi} 2$ ... prvek $2 \in Z_4$ generuje podgrupu $\{0, 2\}$, tj. podle podmínky homomorfismu se 0, 2, 4, 6 zobrazí na nulu, a 1, 3, 5, 7 na dvojku, tj. jádrem je $\{0, 2, 4, 6, \}$.

hom 04: $0 \xrightarrow{\varphi} 0$, $1 \xrightarrow{\varphi} 3$ ... prvek $3 \in Z_4$ generuje celou Z_4, a tedy 0, 1, 2, 3 se postupně zobrazí na 0, 3, 2, 1, a pak už se obrazy zopakují: $4 \to 0$, $5 \to 3$, $6 \to 2$, $7 \to 1$. Jádrem je množina $\{0, 4\}$ grupy Z_8.

Ad Například N.2: $(Z_9, \oplus)$ sestává z prvků: (operací „umocňování“ je sčítání prvků) [0] je řádu 1, [1] je řádu 9, [2] je řádu 9, [3] je řádu 3, [4] je řádu 9, [5] je řádu 9, [6] je řádu 3, [7] je řádu 9, *Pinter*2010 je řádu 9.

Dále $(S_3, \circ)$ sestává z prvků (ve zkráceném zápisu pomocí disjunktních cyklů): id je řádu 1, $(1, 2, 3)$ je řádu 3, $(1, 3, 2)$ je řádu 3, $(1, 2)$ je řádu 2, $(1, 3)$ je řádu 2, $(2, 3)$ je řádu 2.

Pojďme ke hledání všech různých homomorfismů: neutrální prvek se musí vždy zobrazit na neutrální prvek – tedy [0] se zobrazí na id. Vzhledem k předchozímu příkladu N.1 řád obrazu musí být dělitelem řádu vzoru, tj. žádný z dalších prvků 58du tři nebo devět se nemůže zobrazit na dvouprvkové cykly $(1, 2)$, $(1, 3)$ nebo $(2, 3)$, protože ty jsou řádu 2.

Dále si všimněme, že grupa Z_9 má řadu prvků řádu devět, je tedy cyklická, tj. stačí zobrazit jeden z generátorů celé grupy, například prvek [1], a všechny obrazy ostatních prvků jsou už jednoznačně určeny z podmínky homomorfismu (podmínky zachování výsledku operace. Díky těmto faktům lze dospět ke třem různým homomorfismům:

hom 01: $\varphi_1([0]) = \mathrm{id}$, $\varphi_1([1]) = (1, 2, 3)$, a nyní už

$$\begin{aligned}
\varphi_1([2]) &= \varphi_1([1]+[1]) = (1,2,3) \circ (1,2,3) = (1,3,2);\\
\varphi_1([3]) &= \varphi_1([2]+[1]) = (1,3,2) \circ (1,2,3) = \mathrm{id};\\
\varphi_1([4]) &= \varphi_1([3]+[1]) = \mathrm{id} \circ (1,2,3) = (1,2,3);\\
\varphi_1([5]) &= \varphi_1([4]+[1]) = (1,2,3) \circ (1,2,3) = (1,3,2);\\
&\text{atd.}
\end{aligned}$$

Je vidět, že jádrem homomorfismu jsou prvky id, [3], [6], protože ty se zobrazí na neutrální prvek druhé grupy.

hom 02: $\varphi_1([0])$ =id, $\varphi_1([1]) = (1,3,2)$, a nyní už

$$\begin{aligned}
\varphi_2([2]) &= \varphi_2([1]+[1]) = (1,3,2)\circ(1,3,2) = (1,2,3);\\
\varphi_2([3]) &= \varphi_2([2]+[1]) = (1,2,3)\circ(1,3,2) = \mathrm{id};\\
\varphi_2([4]) &= \varphi_2([3]+[1]) = \mathrm{id}\circ(1,3,2) = (1,3,2);\\
\varphi_2([5]) &= \varphi_2([4]+[1]) = (1,3,2)\circ(1,3,2) = (1,2,3);\\
&\text{atd.}
\end{aligned}$$

Je vidět, že jádrem homomorfismu jsou prvky id, [3], [6], protože ty se zobrazí na neutrální prvek druhé grupy.

hom 03: $\varphi_3([0])$ =id, $\varphi_3([1])$ =id, a nyní už

$$\begin{aligned}
\varphi_3([2]) &= \varphi_3([1]+[1]) = \mathrm{id}\circ\mathrm{id} = \mathrm{id};\\
\varphi_3([3]) &= \varphi_3([2]+[1]) = \mathrm{id}\circ\mathrm{id} = \mathrm{id};\\
&\text{atd.}
\end{aligned}$$

Je vidět, že jádrem homomorfismu je celá grupa Z_9, protože všechny její prvky se zobrazí na neutrální prvek.

Seznam literatury:

Beránek, 2011 Jaroslav Beránek: Vybrané kapitoly z algebry. Skriptum Pdf, počet stran 70. Doplnění obsahu předmětů Algebra 1 a Algebra 3 na PdF pro budoucí učitele 2.stupně. Brno 2011.

Budínová, I., 2013 Irena Budínová: Polynomy. Text určený studentům učitelství matematiky, Brno 2013. Počet stran 56.

Drozd, 2008 P. Drozd – základy práce se softwarem R. Manuál ke stažení z internetu o některých základních funkcích jazyka R, který lze v 1.ročníku VŠ doporučit jako lepší kalkulačku zvládající běžné matematické funkce, a současně jednoduché kreslení obrázků, které lze stáhnout v různých formátech. I jednoduché programy lze v tomto prostředí realizovat. Prostředí po instalaci funguje offline.

Horák, 2002 P. Horák: Cvičení z algebry a teoretické aritmetiky I, Brno 2002. Sbírka příkladů na Přírodovědecké fakultě MU. Cvičení pokrývá zhruba látku v předmětech Základy matematiky, Algebra 1, Algebra 2 vyučovaných na Pedagogické fakultě.

Horák, 2013 P. Horák: Základy matematiky. Přednáškový text na Přírodovědecké fakultě MU.

Fajmon, 2019 B.Fajmon: Základy matematiky – verze 2019. Doplnění přednášek v předmětu MA0001, počet stran 144.

Jordan, Smith, 2008 D.Jordan, P.Smith: Mathematical techniques. Oxford 2008, 4th Edition.

Koláček J. Koláček: Výuka jazyka R. Rovněž úvod do jazyka R, nyní od vysokoškolského učitele matematiky, což je vhodným doplněním textu (Drozd, 2008).

Komprsová 2018 Komprsová, T.: Řešení rovnic v algebře. Bakalářská práce na Pdf MUNI, Brno 2018.

Kopka, J., 1991 Jan Kopka: Svazy a Booleovy algebry (Ústí nad Labem 1991, zejména str. 19-82). Pan profesor Kopka napsal svůj text z té pozice, že by rád přehledně a srozumitelně podal přehled pojmů algebry a diskrétní matematiky, aby byla vidět její krása. Kniha je hlubším rozvedením pojmu uspořádaná množina uvedeným v předmětu Základy matematiky.

Pinter, 2010 Charles Pinter: A book of Abstract Algebra, 2010. Jedná se o reprint druhého vydání z roku 1990. Neobyčejně čtivý text, napsaný z té pozice, že algebra je důležitá a má důležitá uplatnění.

Robová, Hála, Calda 2013 Robová, J., Hála, M., Calda, E.: Komplexní čísla, kombinatorika, pravděpodobnost a statistika. Prometheus 2013, v sérii Matematika pro střední školy. Velmi dobrý úvod do daných čtyř oborů na středoškolské úrovni, kromě výkladu kombinací s opakováním, který je málo srozumitelný.

Rosický, J., 2000 Jiří Rosický: Algebra – grupy a okruhy 2000, reprint textu z roku 1985. Tento text se hodně shoduje s osnovou předmětu Algebra 1 na PdF, nicméně jen až jako doplnění čtivější knihy (Pinter, 2010).

Trombiková, 2019 Trombiková, I: Numerické metody pro řešení polynomických rovnic. Bakalářská práce Pdf MUNI, Brno 2019.