Algebra 1 (MA-0003)

verze červen 2019

Břetislav Fajmon

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**. Znalost těchto pojmů bude prověřena i v předmětu Algebra 1.

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 [8], ze které jsem podstatně čerpal jak pro přednášku, tak pro cvičení. I když tento předmět se studentům nutně bude zdát teoretický, Charles Pinter napsal knihu [8] s přesvědčením, že algebra je pro matematiku potřebná – stejně potřebná jako geometrie.

V roce 2019 proběhne rekonstrukce textu, některé partie první poloviny budou vyhozeny, naopak druhá polovina bude doplněna o polynomy a komplexní čísla.

Břetislav Fajmon,
verze textu červen 2019

1 Axiomy operací, vlastnosti (1) až (5)

1.1 Warmup

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. 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).

1.2 Přednáška

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

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

$$\forall x, y \in M : \quad x * y \in M. \tag{1}$$

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 $*$:

$$\forall x, y, z \in M : \quad (x * y) * z = x * (y * z). \tag{2}$$

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 $*$:

$$\exists e \in M : x * e = e * x = x \;\; \forall x \in M. \tag{3}$$

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 $*$:

$$\forall x \in M \ \ \exists\, x^{-1} \in M : x * x^{-1} = x^{-1} * x = e. \tag{4}$$

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 1.1. Grupoid $(M,*)$ ... množina M, na které operace $*$ splňuje vlastnost (1);
- Definice 1.2. Pologrupa $(M,*)$ ... množina M, na které operace $*$ splňuje vlastnosti (1),(2);
- Definice 1.3. 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 1.4. 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):

$$\forall x, y \in M \quad : \quad x * y = y * x. \tag{5}$$

- Definice 1.5. $(M,*)$ se nazývá komutativní grupoid, pokud je grupoid a operace $*$ splňuje vlastnost (5), tj. je komutativní na množině M.
- Definice 1.6. $(M,*)$ se nazývá komutativní pologrupa, pokud je pologrupa a operace $*$ splňuje vlastnost (5), tj. je komutativní na množině M.
- Definice 1.7. $(M,*)$ 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 1.8. $(M,*)$ 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 $\cdot$ splňuje tzv. distributivní zákon = vlastnost (6):

$$\forall \ \ x, y, z \in M : x \cdot (y+z) = x \cdot y + x \cdot z, \ \ (y+z) \cdot x = y \cdot x + z \cdot x. \tag{6}$$

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 se stejnou nebo nižší prioritou než násobení. Například známá operace sčítání reálných čísel má nižší prioritu než násobení reálných čísel:

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

tj. operace $\cdot$ 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

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

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

1.3 Cvičení

Cvičení 1.1. 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 $M = \{-100, -99, -98, \dots, -1, 0, 1, 2, \dots, 99, 100\}$.

Cvičení 1.2. 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).

Cvičení 1.3. 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.

Cvičení 1.4.

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).

Cvičení 1.5. Dokažte, že množina všech podmnožin tříprvkové množiny s operací symetrického rozdílu $\div$ je grupa (viz [8], str. 30, oddíl C).

Cvičení 1.6. Uveďte definice vlastností relací (11) až (18) a u každé z nich uveďte příklad:

- Relace ρ na množině M je reflexivní (11), když ...
- Relace ρ na množině M je symetrická (12), když ...
- Relace ρ na množině M je tranzitivní (13), když ...
- Relace ρ na množině M je úplná (14), když ...
- Uspořádaná množina (poset) P s relací uspořádání $\trianglelefteq$ je dobře uspořádaná (15), když ...
- Prvek $x \sqcap y$ je největší (16b) dolní závorou (16a) prvků x, y, když ...
- Prvek $x \sqcup y$ je nejmenší (17b) horní závorou (17a) prvků x, y, když ...
- Zobrazení f z X do Y je taková relace na $X \times Y$, že platí

Výsledky některých cvičení najdete v závěru textu v oddílu 11.1.

2 Další vlastnosti grup

2.1 Warm-up

Algebra je nauka o řešení rovnic. 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 K[1] všech prvků z množiny M, pro které se stává daná rovnice pravdivým výrokem.

Příklad 3.0 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 $(N, +)$)!! 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 $(Q, +, \cdot)$).

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 se budeme zabývat ve druhé části textu.

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

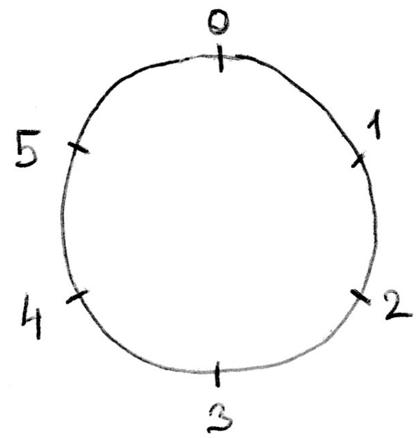
2.2 Přednáška

Až dosud (v prvních dvou přednáškách) 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 (11), antisymetrická (anti-(12)) a tranzitivní (13), nyní se 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 nějakým příkladem grupy:

Příklad 3.1.: 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 $(1+2)+4$[2], 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[3].

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:

Tabulka 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

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

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

Danou tabulku operace $*$ konstruujeme tak, že na průsečíku řádku prvku x a sloupce prvku y se vyskytuje výsledek operace $x * y$:

$$\begin{array}{c|ccc} * & \dots & y & \dots \\ \hline \dots & & \dots & \\ x & \dots & x * y & \dots \\ \dots & & \dots & \end{array}$$

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

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?[4]

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[5]:

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

což je spor s tím, že oba neutrální prvky jsou navzájem různé[6].$\square$

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

[4] 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?

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

[6] 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.

grupě nějaký prvek, ke kterému existují inverze dvě?

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

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

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

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

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

Klíčová myšlenka: vynásobením[7] $a_1^{-1} \triangledown a_2^{-1}$ 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:

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

Využili jsme platnosti asociativního zákona (2) pro kaskádu tří prvků uprostřed spojených operací $\triangledown$. 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“[8] v rovnostech, ve kterých se vyskytují prvky grupy G a operace $\triangledown$?) V každé grupě $(G, \triangledown)$ platí zákony o krácení (7), tj.

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

Důkaz: Provedeme například pro první z implikací: Vztah

$$a \triangledown b = a \triangledown c$$

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:

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

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

$$b = c.$$

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

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

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

Věta 4. (o vzájemně inverzních prvích) V každé grupě $(G, \triangledown)$ z rovnosti $a \triangledown b = n$ (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 $a \triangledown b = n$ prvkem a^{-1} zleva, dostaneme

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

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

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

i) $(a \triangledown b)^{-1} = b^{-1} \triangledown a^{-1}$ (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 $a \triangledown b$ a $b^{-1} \triangledown a^{-1}$:

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

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

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

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

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

Definice 3.1. **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 (viz kapitola 5).

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 $\triangledown$jako součin prvního prvku se součinem následujících tří prvků, tj.

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

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 věty 5a):

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

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

Definice 3.2. **n-tá mocnina prvku** a grupy $(G, \bigtriangledown)$ se definuje jako prvek získaný v řetězci operací

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

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

Definice 3.3. **n-tá odmocnina prvku** a grupy $(G, \bigtriangledown)$ je takový prvek $x \in G$ (pokud tedy existuje), že $a = x^n$.

Definice 3.4. **zápornou odmocninu** a^{-5} grupy $(G, \bigtriangledown)$ definujeme jako pátou mocninu jejího inverzního prvku, tj. $a^{-5} := (a^{-1})^5$.

2.3 Cvičení

Z následujících doporučení většinou jde o jednoduché otázky, ty složitější mají na konci textu [8] návod k řešení. Některé z těchto doporučených příkladů, které se vyskytly u zkoušky, zde jsou výslovně napsány se zadáním i výsledkem.

Cvičení 3.1. Příklady z [8], str. 39, oddíl A: řešení rovnic v grupách – výborné příklady, je zde vidět nutnost přidávat prvek na té správné straně výrazu při nekomutativní operaci a to, že obecně nemůžeme odmocňovat.

Například A.0: Vyřešte v grupě $(G, *)$ systém rovnic (e je neutrální prvek; dospějte ke vztahu $x = \ldots$ na pravé straně bude výraz obsahující prvek b a žádné x ani x^{-1}):

$$\begin{aligned} x^2 &= b, \\ x^5 &= e. \end{aligned}$$

Například A.1, A.2: viz warm-up v této kapitole.

Například A.3: Vyřešte v grupě $(G, *)$ systém rovnic (vyjádřete prvek x v závislosti na prvcích a, b, c (a jejich inverzích), tj. dospějte ke vztahu $x = \ldots$). POZOR, v grupě obecně neplatí komutativní zákon pro všechny dvojice prvků:

$$\begin{aligned} x^2 * a &= b * x * c^{-1}, \\ a * c * x &= x * a * c. \end{aligned}$$

Například A.4: Vyřešte v grupě $(G, *)$ systém rovnic (vyjádřete prvek x v závislosti na prvcích a, b (a jejich inverzích), tj. dospějte ke vztahu $x = \ldots$). :

$$\begin{aligned} a * x^2 &= b, \\ x^3 &= e. \end{aligned}$$

Například A.5: Vyřešte v grupě $(G, *)$ systém rovnic (e je neutrální prvek; dospějte ke vztahu $x = \ldots$ na pravé straně bude výraz obsahující prvek a a neobsahující x):

$$\begin{aligned} x^2 &= a^2, \\ x^5 &= e. \end{aligned}$$

Například A.6: Vyřešte v grupě $(G, *)$ systém rovnic (nepředpokládejte, že obecně platí vlastnost (5) = komutativní zákon; dospějte ke vztahu $x = \ldots$ na pravé straně bude výraz obsahující prvky a, b a žádné x):

$$\begin{aligned} (x * a * x)^3 &= b * x, \\ x^2 * a = (x * a)^{-1} &= \ldots . \end{aligned}$$

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:

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

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

Cvičení 3.2. Příklady z [8], str. 40, oddíl E: počet prvků a jejich inverzí – výborné příklady.

Cvičení 3.3. Příklady z [8], str. 41, oddíl F: vytváření tabulky operace pro grupy s malým počtem prvků – výborné příklady.

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

$$\begin{array}{c|ccccc} \star & \dots & x_1 & \dots & x_2 & \dots \\ \hline \cdots & & \cdots & & \cdots & \\ a & \cdots & y & \cdots & y & \cdots \\ \cdots & & \cdots & & \cdots & \end{array}$$

Zdůvodněte, proč ano - proč ne.

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

$$\begin{array}{c|ccc} \star & e & a & b \\ \hline e & e & a & b \\ a & a & & \\ b & b & & \end{array}$$

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:

$$\begin{array}{c|cccc} * & e & a & b & c \\ \hline e & & & & \\ a & & & & \\ b & & & & \\ c & & & & \end{array}$$

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:

$$\begin{array}{c|cccc} * & e & a & b & c \\ \hline e & & & & \\ a & & & & \\ b & & & & \\ c & & & & \end{array}$$

Cvičení 3.4. (text [8], str. 42, oddíl G): Dokažte, že kartézský součin grup $(G, \bigtriangledown)$ a $(H, *)$ je grupa $(G \times H, \Box)$ – jak definovat operaci $\Box$?

Cvičení 3.5. Příklady z [8], 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?

Výsledky některých cvičení najdete v závěru textu v oddílu 11.3.

3 Podgrupy a generátory grupy

3.1 Warmup

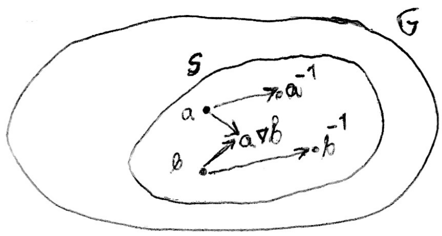
Týden 04: Teorie prověrka-a na obsah týdnů 1 až 3. Do otázek bude zahrnuto i vše ze cvičení 1, tedy i základní pojmy a vlastnosti (11) až (18) z předmětu Základy matematiky. V jedné otázce bude i důkaz některé z vět 1 až 5.

3.2 Přednáška

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

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

Definice 4.1. **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[9] 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).□

Příklad 4.1.

[9]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.

- Podmnožina $S = \{\dots, -4, -2, 0, 2, 4, \dots\}$ všech sudých celých čísel je podgrupou grupy $(Z, +)$: opravdu, je neprázdná, uzavřená vzhledem ke sčítání ((1) ... součtem dvou sudých celých čísel je opět sudé celé číslo) a obsahuje všechny inverze ((4) ... nula je inverzí sama k sobě vzhledem ke sčítání, inverzí čísla 2 vzhledem ke sčítání je číslo -2, atd.).

- Podmnožina Q^* (označení 01) 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.

Jedna z aplikací pojmu podgrupa je v tom, když dokazujeme o nějaké neprázdné množině, že je grupa: pokud víme, že tato množina S je podmnožinou množiny G, o které víme, že je grupa, stačí nám ukázat platnost (1) a (4) na množině S a jsme s důkazem, že S je grupa vzhledem k téže operaci, hotovi.

Příklad 4.2.

- Označme $(F(R), +)$ množinu všech funkcí (= zobrazení $R \to R$, viz předmět Základy matematiky) s operací sčítání funkcí. Zřejmě tato množina je grupa, protože součtem dvou funkcí je zase funkce (platí (1)), toto sčítání funkcí je asociativní (platí (2)), existuje nulová funkce jako neutrální prvek (platí (3)), ke každé funkci $f(x)$ existuje její inverze $-f(x)$, takže součet obou těchto funkcí je nulová funkce.

  Na základě věty 6 nyní snadno uzavřeme, že neprázdná množina $C(R)$ všech spojitých funkcí je grupa vzhledem ke sčítání funkcí, protože je neprázdnou podmnožinou grupy $(F(R), +)$, splňuje vlastnosti (1) i (4) (součtem dvou spojitých funkcí je spojitá funkce, inverzí ke spojité funkci $f(x)$ je spojitá $-f(x)$.

  Podobně neprázdná množina všech diferencovatelných funkcí $D(R)$, tedy funkcí, které mají derivaci v každém bodě, je podmnožinou grupy $(F(R), +)$ a splňuje (1) i (4) z podobných důvodů jako $C(R)$, je tedy grupou vzhledem ke sčítání funkcí.

Definice 4.2. **Triviální podgrupy (= nevlastní podgrupy)** grupy $(G, \triangledown)$ se nazývají dvě podgrupy: a) $S_1 = \{n\}$ je podgrupou vzhledem k $\triangledown$, 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 $(G, \triangledown)$.

Generátory podgrupy

Uvažujme množinu $S = \{a, b, c\}$, která je podmnožinou grupy $(G, \triangledown)$. Na to, abychom našli nejmenší možnou podgrupu, která obsahuje prvky a, b, c, musíme vyrobit všechny možné součiny těchto tří prvků a jejich inverzí[10], a nejen to: musíme brát všechny možné konečné sekvence prvků spojených operací $\triangledown$, ve kterých se vyskytují (i opakovaně) prvky a, b, c a jejich inverze.

Typickými takto vytvářenými prvky jsou například

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

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

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 4.3) **podgrupa grupy** G **generovaná množinou** S a označujeme ji (označení 02) $< S >$. Prvky množiny S nazýváme **generátory** podgrupy $< S >$.

A ještě jedna definice, která s tí souvisí (definice 4.4): 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 $n = a \bigtriangledown a^{-1}$.

Příklad 4.3. Grupa $(H_6, +)$ z příkladu 3.2 je příkladem cyklické grupy, generované jediným prvkem – kterým???

3.3 Cvičení

Cvičení 4.1. Příklady z [8], 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 $a_i \star a_1$, $a_i \star a_2$, …, $a_i \star a_n$: atd.

Cvičení 4.2. Příklady z [8], str. 50, oddíl E: generátory grupy – výborné příklady.

Například N.1 (není v textu [8]): 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[11]: V grupě $(H_2 \times H_4)$ je operace sčítání po složkách zadaná tabulkou

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

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.

[11] 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.

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 11.4.

4 Nekomutativní grupy

4.1 Přednáška

Příklad 5.1. Grupy netvoří jen číselné množiny a operace na nich. **Zajímavým příkladem grupy je množina $FI(R)$ všech funkcí z R do R, ke kterým existuje inverzní funkce, společně s operací $\circ =$ „po“, neboli operací skládání zobrazení**. Při tomto vymezení množiny a operace na ní je struktura $(FI(R), \circ)$ grupa, neboť

1. složením dvou těchto funkcí je opět funkce z R do R, ke které existuje inverze – podle věty 5 o výpočtu inverzí platí

$$(f \circ g)^{-1} = g^{-1} \circ f^{-1}$$

   (inverze ke složení funkcí je složení dílčích inverzí v opačném pořadí).

2. Skládání funkcí, potažmo jakýchkoli zobrazení, je asociativní operace:

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

3. Jednotkou vzhledem ke skládání funkcí je identita $f_{id}(x) = x \ \ \forall x \in R$.

4. Vlastnost (4) je požadavkem, podle kterého jsou funkce vybírány, tj. platí.

Právě uvedený příklad je důležitý v tom, že je příkladem nekomutativní grupy. Například pro funkce $f(x) = \sin x$, $g(x) = \frac{1}{x}$ je funkce $f \circ g = \sin \frac{1}{x}$ odlišná od funkce $g \circ f = \frac{1}{\sin x}$.

Příklad 5.2. Grupa permutací Důležitým příkladem grupy, na kterou se nyní zaměříme blíže, je grupa bijekcí n-prvkové množiny na sebe sama, kde operací je skládání zobrazení. 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 na vysoké škole budeme na tyto permutace pohlížet jako na zobrazení, které základní vzestupné pořadí 12345 přemění na pořadí např. 51324:

Definice 5.1. <u>Permutace</u> $n-$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

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

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 označení „po“ je zcela instruktivní;

Věta 7. $(S_n, \circ)$, množina permutací[12] $M \to M$ pro $M = \{1, 2, \ldots, n\}$ vzhledem k operaci skládání permutací je pro $n \geq 3$ nekomutativní grupa.

Ilustrace důkazu: Pro lepší pochopení důkazu situaci nejprve ilustrujeme na příkladě permutací na tříprvkové množině: Uvažujme množinu permutací tříprvkové množiny $\{1, 2, 3\}$ do sebe – označme ji S_3. Množina S_3 má šest prvků:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix},$$

$$u = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix}, \quad v = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{pmatrix}, \quad w = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{pmatrix}.$$

Prvek e je jednotkový (tj. platí zde vlastnost (3)), neprovede žádnou změnu v pořadí, například

$$s \circ e = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} = s.$$

Všimněme si, že nejprve je prováděno přiřazení e, a až poté ($\circ$ = „po“) je provedeno přiřazení s. Dále například

$$u \circ v = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix} = s,$$

$$v \circ u = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix} = t.$$

Čili 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 $\circ$.

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

Nejprve je potřeba říci, že u každé tabulky operace $*$ na konečné množině prvků je levý prvek x vybrán[13] z levého sloupce záhlaví a pravý prvek y z horního řádku záhlaví; výsledek operace pak je znázorněn na průsečíku „řádku x“ a „sloupce y“:

$$\begin{array}{c|ccc} * & \dots & y & \dots \\ \hline \dots & & \dots & \\ x & \dots & x*y & \dots \\ \dots & & \dots & \end{array}$$

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

$\circ$	e	s	t	u	v	w
e	e	s	t	u	v	w
s	s	t	e	w	u	v
t	t	e	s	v	w	u
u	u	v	w	e	s	t
v	v	w	u	t	e	s
w	w	u	v	s	t	e

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 5.1. A nakonec, je splněna i vlastnost (4), protože: jednotkový prvek e je (jako každý jednotkový prvek v grupě) inverzní sám k sobě; z tabulky dále vidíme, že $s^{-1} = t$, $t^{-1} = s$, a prvky u, v, w jsou inverzemi sebe sama!

Důkaz pro obecné n: Operace $\circ$ je na množine S_n uzavřená, tj. platí vlastnost (1), protože složení dvou permutací je opět permutace. Asociativita (2) platí pro skládání jakýchkoli zobrazení, viz příklad 5.1. Identické zobrazení f_{id} definované $\forall a \in \{1, 2, \dots, n\}$ vztahem $f_{id}(a) = a$ je neutrálním prvkem na množině permutací, tj. platí (3): Pro obecnou permutaci $p : \{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$ totiž máme pro každné $a \in \{1, 2, \dots, n\}$:

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

Důkaz vlastnosti (4): V obecném případě $(S_n, \circ)$ permutací na n-prvkové množině $M = \{1, \dots, n\}$ 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 $a \in \{1, 2, \dots, n\}$. Tedy pro bijekci p je p^{-1} také bijekce (v grafické reprezentaci relace pouze zaměníme směr všech šipek), a tedy permutace $\{1, 2, \dots, n\} \to \{1, 2, \dots, n\}$.

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

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

[13] Toto je klíčově důležitá domluva, řečená už v předchozí kapitole. Většina operací je komutativních, a tam je pořadí prvků vstupujících do operace zaměnitelné, ale u nekomutativních operací tomu tak není a u tabulky operace se musíme jednoznačně domluvit na pořadí první prvek – druhý prvek pro danou operaci.

Důkaz je hotov. $\square$

Ad příklad 5.2. Uveďme nyní některé další vlastnosti této grupy, které vyplývají z kapitoly 3: Za prvé, existuje šest podgrup grupy $(S_3, \circ)$: tzv. triviální podgrupa, která obsahuje pouze jednotkový prvek e, s tabulkou operace

$$\begin{array}{c|c} \circ & e \\ \hline e & e \end{array},$$

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

$$\begin{array}{c|cc} \circ & e & u \\ \hline e & e & u \\ u & u & e \end{array}, \qquad \begin{array}{c|cc} \circ & e & v \\ \hline e & e & v \\ v & v & e \end{array}, \qquad \begin{array}{c|cc} \circ & e & w \\ \hline e & e & w \\ w & w & e \end{array}$$

a jedna tříprvková podgrupa s tabulkou operace

$$\begin{array}{c|ccc} \circ & e & s & t \\ \hline e & e & s & t \\ s & s & t & e \\ t & t & e & s \end{array}.$$

Dále, ohledně generátorů grupy S_3 lze říci, že $(S_3, \circ)$ je generována dvěma svými prvky, a sice v a w, protože všechny další čtyři prvky grupy lze vyjádřit pomocí operace $\circ$ a prvků v, w:

$$\begin{aligned} e &= v \circ v; \\ s &= v \circ w; \\ t &= s \circ s = (v \circ w)^2 = (v \circ w) \circ (v \circ w); \\ u &= w \circ s = w \circ (v \circ w). \end{aligned}$$

Podle označení množiny generátorů lze psát

$$(S_3, \circ) = < v, w > .$$

Písmeno S v označení množiny S_n pravděpodobně pochází z toho faktu, že tyto permutace představují jakési jistým způsobem symetrické útvary, nebo modelují struktury, kterým se říká symetrie. Ukažme si, jak tyto grupy permutací vznikají ze grup symetrií, například na grupě symetrií čtverce.

Příklad 5.3: grupa symetrií čtverce: 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

$$R_0 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 4 \end{pmatrix},$$

pootočení o 90° odpovídá permutace

$$R_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

(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 a pootočení o 270° permutace R_3:

$$R_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad R_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

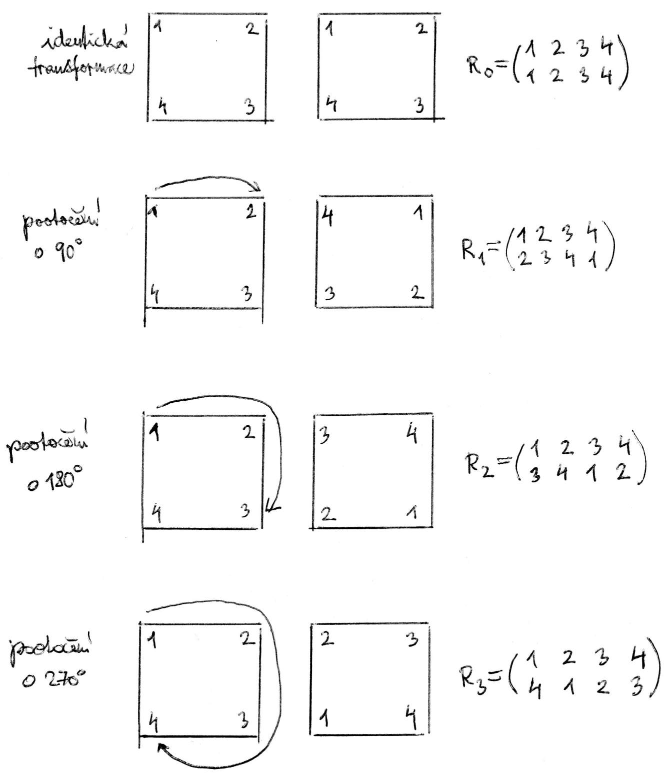
(podrobněji viz obrázek 1).

Podobně dostaneme permutace odpovídající přeměně čísel ve vrcholech čtverce při osové souměrnosti vzhledem ke čtyřem hlavním osám souměrnosti, viz obrázek 2. Skládáním $R_1 \circ R_4$ například dostaneme

$$R_1 \circ R_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 4 & 3 & 2 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 4 & 3 \end{pmatrix} = R_6,$$

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 2). 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-úhelníka a označit ji D_n vzhledem k operaci skládání zobrazení. Například D_5 označuje grupu symetrií pětiúhelníka, 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.

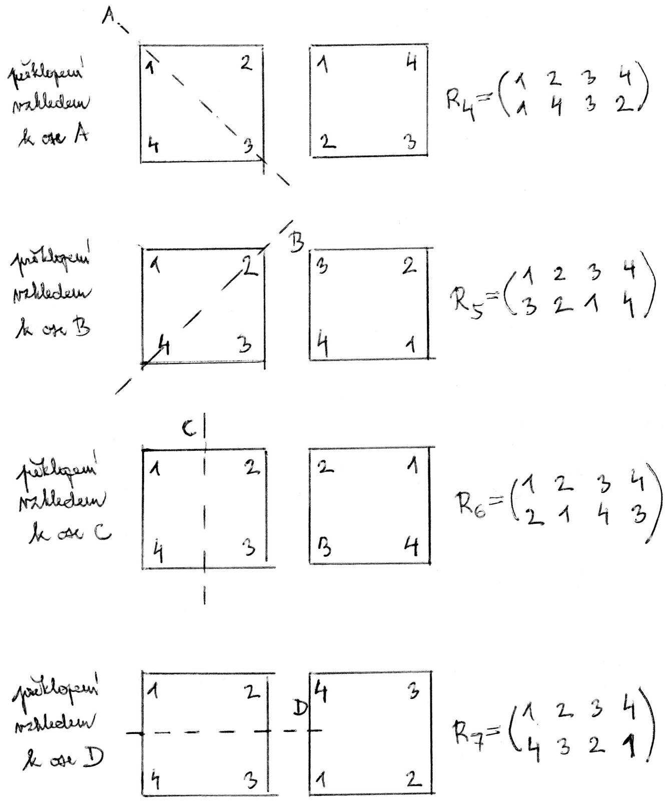


Obrázek 1: Permutace odpovídající pootočení čtverce.

Tabulka 2: 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	R_0	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

Příklad 5.4. Posledním důležitým příkladem nekomutativní grupy, se kterou se studenti budou v budoucnu setkávat, je množina všech čtvercových matic, ke kterým existuje inverze vzhledem k násobení matic, společně s operací násobení matic. Tento příklad bude podrobně rozebrán v předmětu Algebra 2 – násobení matic, jak uvidíme,



Obrázek 2: Permutace odpovídající osové symetrii čtverce.

je nekomutativní operací. Pro zájemce je tento typ operace uveden jako příklad důležité nekomutativní operace už v úvodu knihy [8], str.7-8.

Operace na cyklické podgrupě je vždy komutativní

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 $\{e, s, t\}$ grupy $(S_3, \circ)$ je generovaná prvkem s, a tedy je to cyklická podgrupa, tj. cyklická grupa. Je vidět, že tabulka operace na $\{e, s, t\}$ je symetrická, tj. operace je na ní komutativní.

Další příklad: Grupa symetrií čtverce (příklad 5.3) je vzhledem ke skládání těchto symetrií nekomutativní grupou, ale například podgrupa $\{R_0, R_1, R_2, R_3\}$ pootočení čtverce je generována prvkem R_1, odpovídajícím pootočení čtverce o 90°, tj. je cyklická. I z tabulky symetrií je též vidět, že příslušná část odpovídající podgrupě pootočení je symetrická, tj. operace je na této podgrupě cyklická. Nekomutativita je způsobena až osovými souměrnostmi.

Důkaz faktu, že operace na každé cyklické grupě je komutativní, připomeňte cvičícímu ve cvičení za kapitolou 6.

4.2 Cvičení

Cvičení 5.1. Jsou dány permutace

$$P = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 3 & 1 & 4 & 6 & 2 & 7 \end{pmatrix}, \quad R = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 7 & 1 & 6 & 3 & 4 & 2 & 5 \end{pmatrix}.$$

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

Cvičení 5.2. Kniha [8], str. 75, oddíl B, příklady na grupy permutací.
Například B.2: Vypište prvky cyklické podgrupy grupy $(S_6, \circ)$ generované prvkem

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

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

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix} \quad \text{a} \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 4 & 5 & 3 \end{pmatrix}$$

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

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \text{a} \quad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

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

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

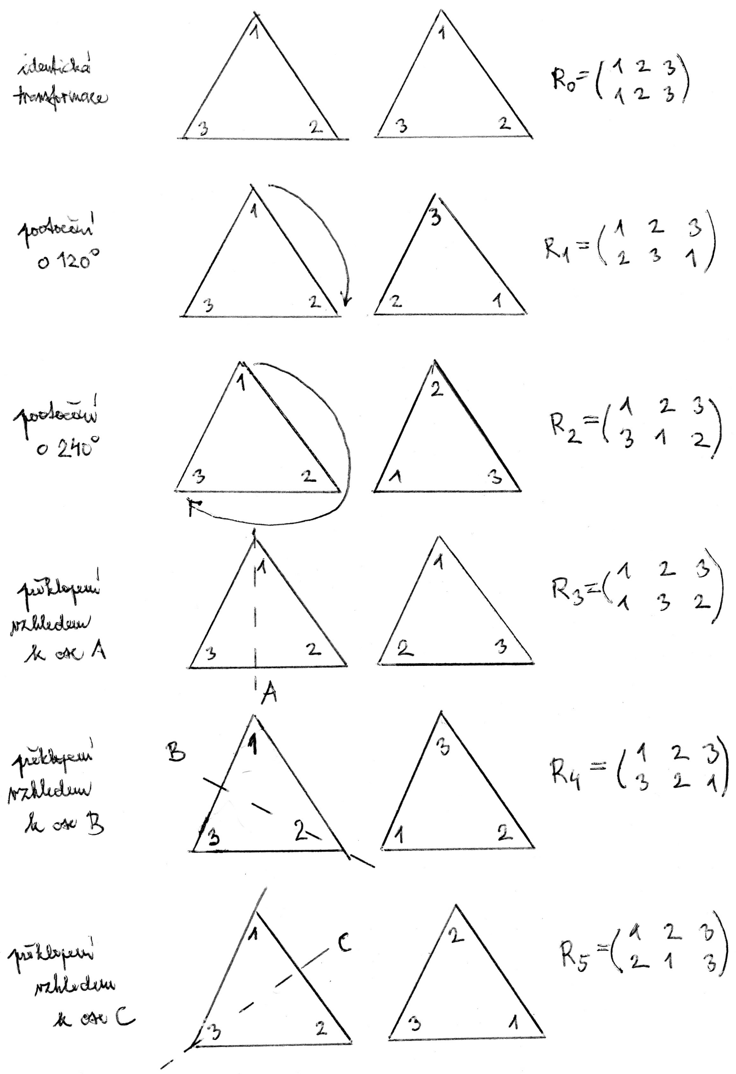
Například N.3: Grupa $(S_4, \circ)$ má 24 prvků a neutrálním prvkem je

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

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.

Cvičení 5.3. Příklady [8], str. 77, sada F na grupu symetrií pravidelného n-úhelníka.

Například F.0: Sestavte tabulku grupy D_3 symetrií rovnostranného trojúhelníka vzhledem k operaci skládání zobrazení (množina D_3 má šest prvků – tři rotace: o nula stupňů (R_1), o 120 stupňů (R_2), o 240 stupňů (R_3); a tři osové souměrnosti vzhledem osám jednotlivých úhlů (R_4, R_5, R_6)). Těmto geometrickým transformacím lze přiřadit permutace tříprvkové množiny podle toho, jak se změní pozice čísel 1, 2, 3 přiřazeným jednotlivým vrcholům trojúhelníku vůči základní poloze – viz obrázek 3.



Obrázek 3: Permutace D_3 odpovídající symetriím trojúhelníku.

Cvičení 5.4. Dva úkoly pro grupu permutací $(S_3, \circ)$ (použijte prosím označení prvků a tabulku operace $\circ$ ve větě 7): a) dokažte, že $(S_3, \circ)$ není cyklická grupa;
b) najděte dvouprvkovou podmnožinu grupy, která generuje celou grupu $(S_3, \circ)$.

Cvičení 5.5. Pokud bude čas, je možné se zabývat některými dalšími vlastnostmi permutací (ad [8], kapitola 8): Každou permutaci lze rozložit na součin cyklů, každý cyklus lze rozložit na součin transpozic. Sudá a lichá permutace podle počtu transpozic.

Výsledky některých cvičení najdete v závěru textu v oddílu 11.5.

5 Izomorfismus, Calyeho věta

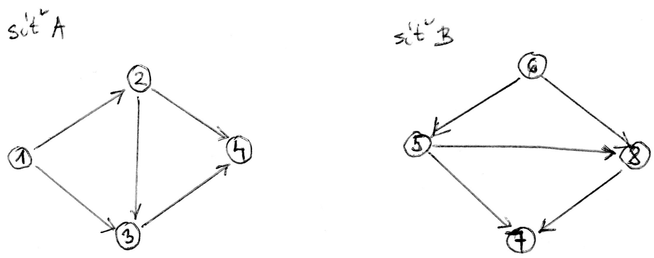
5.1 Warmup

Oslava dne učitelů.

5.2 Přednáška

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[14]. 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 izimorfní, 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).



Obrázek 4: Dvě izomorfní struktury toku v sítích.

Například na obrázku 4 jsou nakresleny dva příklady toku v sítích[15] – může se jednat o tok informací ve spravodajské síti, tok financí v ekonomické síti, tok proudu elektrickým obvodem, apod. Matematické grafy reprezentující tyto toky jsou příkladem diskrétních grafů (na rozdíl od spojitých grafů funkce v matematické analýze). Když studujeme síť A a síť B na obrázku, vidíme, že tyto dvě sítě jsou izomorfní, tj. mají stejnou vnitřní strukturu: existuje totiž bijekce

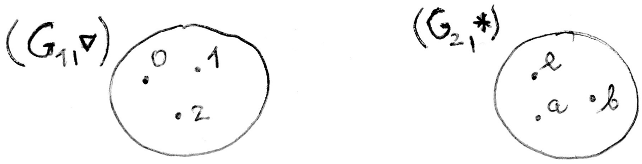
$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 6 & 5 & 8 & 7 \end{pmatrix},$$

která zobrazuje prvky sítě A na odpovídající prvky sítě B v tom smyslu, že prvek 1, ze kterého vycházejí dvě orientované hranu do dvou dalších uzlů sítě A, odpovídá prvku 6 sítě B, ze kterého rovněž vycházejí dvě orientované hrany. Podobně prvek 2 v síti A odpovídá prvku 5 v síti B, protože tyto dva uzly mají tutéž vlastnost (každý ve své síti), že do nich jedna hrana grafu vstupuje a dvě hrany z nich vycházejí, atd. Tj. izomorfismus

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

[15] Pozor, obrázek 4 se neučte, jedná se jen o příklad „stejnosti“ z teorie grafů, ovšem na uvedených strukturách není definována (binární) operace. Skutečná definice izomorfismu grup se týká obrázku 5 nebo 6, kde máme na obou strukturách definovanou operaci – jeden z nich se můžete naučit.

těchto grafů je nejen bijekcí, ale navíc ještě zobrazuje prvek jedné sítě na prvek stejného strukturálního charakteru v jiné síti.



$\triangledown$	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 5: Dvě izomorfní grupy.

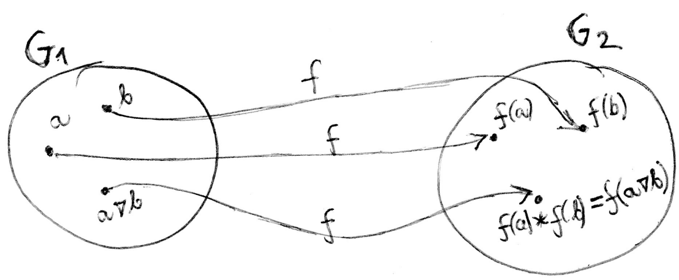
Podobně na obrázku 5 vidíme dvě izomorfní grupy. Obě jsou tříprvkové a existuje mezi nimi bijekce

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

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 0, odpovídá v navrhované bijekci prvku e v grupě G_2, který je výsledkem operace $*$ mezi obrazy prvků 1 a 2, tj. mezi a a b, tedy platí $a * b = e$. Toto zachování výsledků operace musí platit pro každou dvojici prvků z G_1.

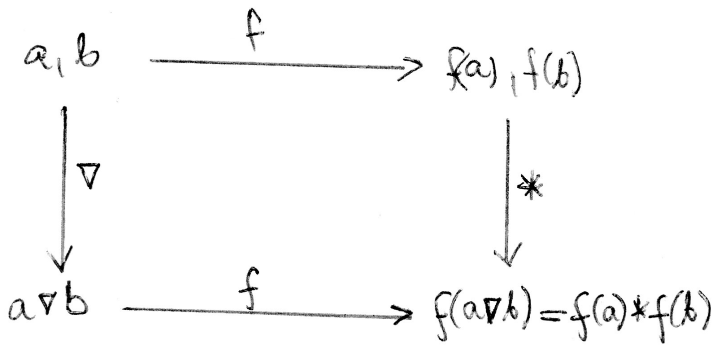
Definice 6.1. Izomorfismus grupy $(G_1, \triangledown)$ na grupu $(G_2, *)$ je bijekce $f: G_1 \to G_2$, která splňuje vlastnost

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



Obrázek 6: Podmínka zachování výsledků operace při zobrazení f.

Jinými slovy (viz obrázek 6, 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 7: Komutativní diagram pro podmínku zachování výsledků operace.

A nebo ještě jinak, říkáme, že izomorfismus f mezi grupami je bijekce, pro kterou diagram na obrázku 7 komutuje, neboli když vypustíme na prvky a, b z „ohrady“ G_1 operaci $\bigtriangledown$, 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 $*$[16].

Příklad 6.1. $(R, +)$ 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 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.

[16] 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.

- 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 $(G^*, \circ)$.

5.3 Cvičení

Kniha [8] opět poskytuje řadu cvičení, doporučuji provést aspoň některá cvičení ze str. 97-102:

Cvičení 6.1. (sady C,D): Jsou dané grupy izomorfní?

Například C.3: Zjistěte, zda je grupa $2^{\{a,b,c\}}$ ze cvičení 1.5 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 za kapitolou 7, kde budou zhruba probrány grupy zbytkových tříd.

Cvičení 6.2. (sada G): Izomorfní grupy na množině reálných čísel.

Cvičení 6.3. (sada J): Regulární reprezentace grupy – rychlá konstrukce podgrupy grupy S_n, která je s grupou G izomorfní!!

Výsledky některých cvičení najdete v závěru textu v oddílu 11.6.

6 Řád prvku, cyklické grupy

6.1 Přednáška

V kapitole **??** 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 7.1. 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 7.1. Co se týká řádu jednotlivých prvků grupy $(S_3, \circ)$, platí (viz tabulka operace příkladu 5.2):

- $e^1 = e$, tj. e je prvek řádu 1;
- $u^2 = v^2 = w^2 = e$, tj. prvky u, v, w jsou řádu 2;
- $s^3 = t^3 = e$, tj. prvky s, t 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 e:

$$e^6 = e,\ u^6 = (u^2)^3 = e^3 = e,\ v^6 = e,\ w^6 = e,\ s^6 = (s^3)^2 = e^2 = e,\ t^6 = e.$$

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

Příklad 7.2. 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 9. 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 12 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 $\{0, 1, 2, \dots, n-1\}$, tj. $r \neq s$. BUNO[17] 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 9 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 10. 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 9b): 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 sporem je hotov.□

To tedy znamená, že prvek nekonečného řádu „svým umocňováním“[18] vede na nekonečně mnoho navzájem různých prvků grupy.

A dodejme ještě větu 11, která upřesňuje situaci kolem konečného řádu prvku grupy:

[17] BUNO = Bez újmy na obecnosti.

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

Věta 11. Pokud řád prvku a v grupě je n (označení 04: označme $ord(a) = n$), pak platí pro celočíselné t:

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

(mocnina prvku konečného řádu je rovna neutrálnímu prvku tehdy a jen tehdy[19], když mocnitel t je násobek řádu n daného prvku).

Důkaz: Dokážeme obě implikace: Ad „⇒“: Důkaz je podobný jako důkaz 9a): 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 v kapitolách ?? a 3. 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 12:

Věta 12. 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[20] jsou navzájem izomorfní.

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

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

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

[19] 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.

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

výsledků operace. Dostáváme tak větu

Věta 13. 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 12 a 13 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 definice 7.2.: 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 8). Pak v každé třídě jsou právě ta celá čísla, která jsou mezi sebou kongruentní modulo 6, tj.

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

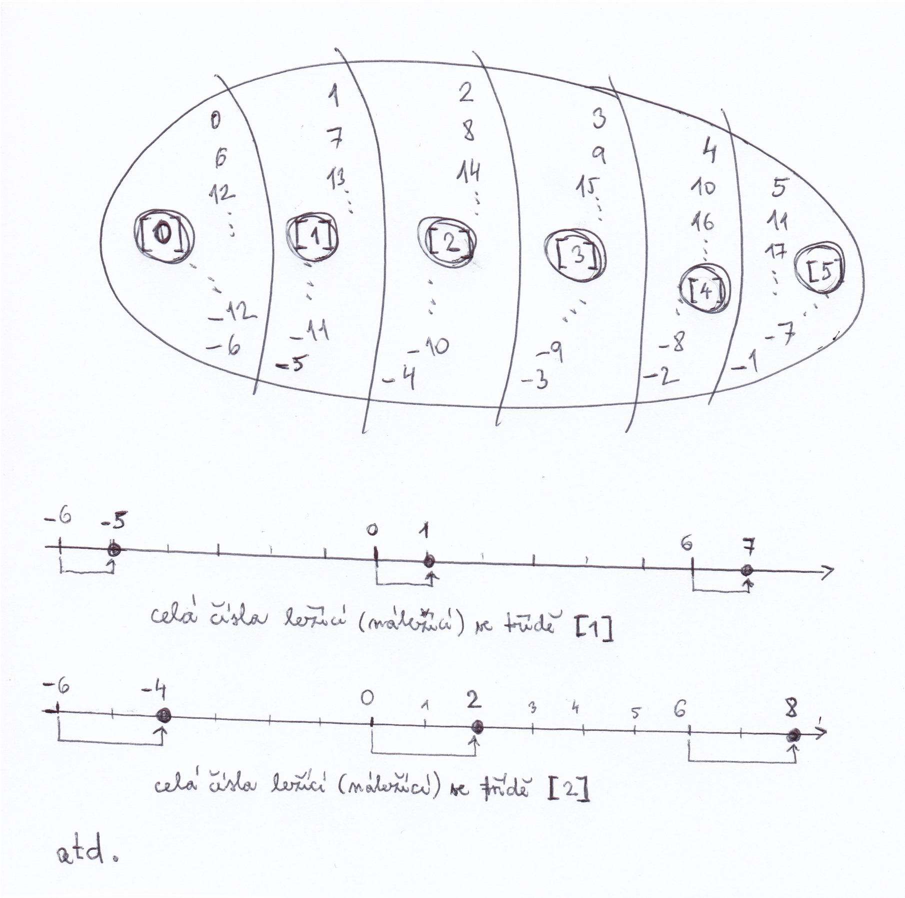
O relaci kongruence lze dokázat, že je to ekvivalence (tj. relace reflexivní, symetrická, tranzitivní).

- Třída [1] obsahuje čísla 1, 7, 13, atd. ale také záporná čísla -5, -11, -17, atd., protože nejbliží 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.
- 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:

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



Obrázek 8: Rozdělení celých čísel do šesti podmnožin.

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 7.3. a) Pomocí tabulky operace $\oplus$ dokažte, že $(Z_6,\oplus)$ je grupa:
b) Pomocí tabulky operace $\odot$ dokažte, že$(Z_6,\odot)$ je monoid:

- označení 05: Z_n ... množina zbytkových tříd modulo n;
- označení 06: 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).

Tabulka 3: 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]

Tabulka 4: 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]

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 14. 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 15. 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]

6.2 Cvičení

Cvičení 7.1. Cvičení k pojmu řád prvku: Ad [8], 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 $ord(a^k)$.

Cvičení 7.2. 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 [8], 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.

Cvičení 7.3 Cvičení k pojmu grupy zbytkových tříd:

Například D.2 z knihy [8], 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 $(S_3, \circ)$:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix},$$
$$u = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix}, \quad v = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{pmatrix}, \quad w = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{pmatrix}.$$

$\circ$	e	s	t	u	v	w
e	e	s	t	u	v	w
s	s	t	e	w	u	v
t	t	e	s	v	w	u
u	u	v	w	e	s	t
v	v	w	u	t	e	s
w	w	u	v	s	t	e

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

⊕	[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 $(Z_8, \oplus)$:

⊕	[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 11.7.

7 Lagrangeova věta

7.1 Warmup

Prověrka b – z týdnů 01 až 07.

7.2 Přednáška

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, ..., 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 07: 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 08: 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 $\triangledown$, 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 8.1. $\forall a$ z grupy $(G, \triangledown)$ a její podgrupu $(H, \triangledown)$ lze definovat:

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

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

(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 8.1. 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 8.2. Pro grupu $G = (S_3, \circ)$ permutací z věty 7 a podgrupu $H = (\{e, s, t\})$ dostáváme následující levé třídy prvků podle podgrupy (viz tabulka operace $\circ$ u věty 7):

- levá třída prvku e vzhledem k H je $e \circ H = \{e, s, t\} = H = H \circ e$ (tedy levá třída prvku e je rovná pravé třídě prvku e vzhledem k operaci $\circ$);
- levá třída prvku s vzhledem k H je $s \circ H = \{e, s, t\} = H = H \circ s$ (tedy levá třída prvku s je rovná pravé třídě prvku s);
- levá třída prvku t vzhledem k H je $t \circ H = \{e, s, t\} = H \circ t$ (tedy levá třída prvku t je rovná pravé třídě prvku t);
- levá třída prvku u vzhledem k H je $u \circ H = \{u, v, w\} = H \circ u$ (tedy levá třída prvku u je rovná pravé třídě prvku u);
- levá třída prvku v vzhledem k H je $v \circ H = \{u, v, w\} = H \circ v$ (tedy levá třída prvku v je rovná pravé třídě prvku v);
- levá třída prvku w vzhledem k H je $w \circ H = \{u, v, w\} = H \circ w$ (tedy levá třída prvku w je rovná pravé třídě prvku w);

Na příkladu 8.2 je vidět, že například množina $u \circ H$ nemusí obsahovat žádný z původních prvků podgrupy H, a taky nemusí být podgrupa, protože neobsahuje neutrální prvek e, i když H podgrupa grupy G je.

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 16 je pouze pomocnou větou, která bude potřeba v důkazu věty 17 (věty 16 až 18 jsou řečeny za předpokladu označení z definice 8.1, tj. $(H, \triangledown)$ je podgrupa grupy $(G, \triangledown)$).

Věta 16. $a \in H \triangledown b$ právě tehdy, když $H \triangledown a = H \triangledown b$.

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

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

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

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

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

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

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

a po dosazení za b dostaneme

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

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

Věta 16 netvrdí nic světoborného, v podstatě jen to, že pokud prvky a, b jsou spojeny v operaci $\triangledown$ „přes podgrupu H“, tak jejich pravé třídy jsou totožné. Následující věta 17 je prvním významným výsledkem této kapitoly.

Věta 17. Pravé[21] třídy $H \triangledown a$ pro všechny možné prvky a grupy $(G, \triangledown)$ tvoří rozklad množiny G.

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

[21] Platí i analogická věta: Všechny levé třídy $a \triangledown H$ ...

a) Pokud množiny $H \triangledown a$, $H \triangledown b$ 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:

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

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

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

a to podle věty 16 (tady právě ji potřebujeme!!) znamená, že $H \triangledown a = H \triangledown b$.

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 $c = e \triangledown c$ (kde e je neutrální prvek), a tedy $c \in H \triangledown c$. Našli jsme třídu rozkladu, ve které prvek c leží.

Věta 18. Existuje bijekce mezi podgrupou $(H, \triangledown)$ a každou pravou třídou $H \triangledown a$.

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

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

Takto definované f je injekce:

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

(a podmínka injekce o rovnosti vzorů při rovnosti obrazů je dokázána). Dále f je surjekce: každý prvek množiny $H \triangledown a$ je tvaru $h \triangledown a$ 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.

Důsledek věty 18 pro konečné grupy G: Všechny pravé třídy $H \triangledown a$ mají tentýž počet prvků!!!!!

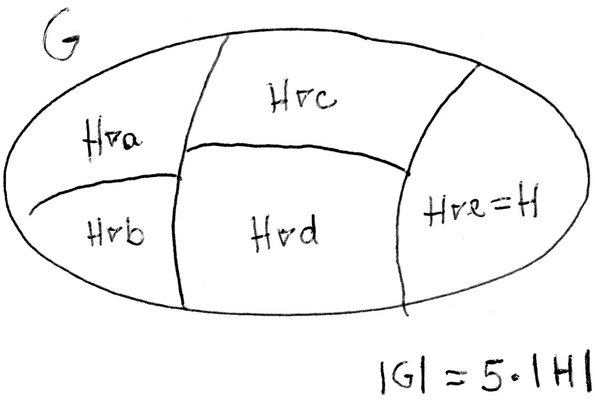
Čtenář si určitě říká, kdy už přijde ta slavná Lagrangeova věta z názvu této kapitoly – už se blíží, je to věta 19!!! Ale ty nejdůležitější věty, věta 17 a věta 18, už byly řečeny. Věta 19 je pouze jejich důsledkem, tj. pan Lagrange je autorem souvislostí všech těchto vět. Podívejme se ovšem předtím na příklad ilustrující celou situaci:

Příklad 8.3. Uvažujme situaci na obrázku 9: všech pravých tříd vzhledem k podgrupě H konečné grupy G je pět – jedna z nich je $H \triangledown e = H$ a další čtyři jsou $H \triangledown a$, $H \triangledown b$, $H \triangledown c$, $H \triangledown d$. Existuje bijekce (podle věty 18) 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 19 – Lagrangeova pro konečné grupy. Počet prvků libovolné podgrupy H je dělitelem počtu prvků konečné grupy G[22].

[22]Připomeneme-li si definici 3.1 řádu grupy, tak: řád podgrupy H je dělitelem řádu grupy G.



Obrázek 9: Rozklad konečné grupy G na pět pravých tříd vzhledem k podgrupě H. Všechny třídy rozkladu mají stejný počet prvků.

Důkaz Lagrangeovy věty je dalším důsledkem věty 18: pokud všechny pravé třídy mají stejný počet prvků, tak počet všech prvků je pouze nějakým násobkem počtu $|H|$.

Příklad 8.4. 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 8.5. Pokud $|G|$ je prvočíslo, tak grupa G má pouze nevlastní podgrupy.

Věta 20. Pokud $|G| = p$ je prvočíslo, tak grupa $(G, \triangledown)$ 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 20 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 21. 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 8.2. 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

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

7.3 Cvičení

Cvičení 8.1. Cvičení k pojmu ekvivalence a rozklady – snad byl procvičeno dost v předmětu Základy matematiky, více viz [8]. str. 123-125 ... ovšem v naší situaci by bylo zajímavé cvičeníčko D na str. 124 – relace ekvivalence na grupě.

Například D.0: Uvažujme grupu $G = (Z_6, \oplus)$ a její podgrupu $H = \langle 2 \rangle$. Definujme na G relaci $a \sim b$, když $a + b^{-1} \in H$. Dokažte, že relace $\sim$ je ekvivalence.

Cvičení D.1: Pro grupu $(G, \cdot)$ a její podgrupu H zkuste obecně dokázat, že relace $\sim := \{[a, b] \in G \times G : ab^{-1} \in H\}$ je ekvivalence.

Cvičení D.2: Pro grupu $(G, \cdot)$ a její podgrupu H zkuste obecně dokázat, že relace $\sim := \{[a, b] \in G \times G : a^{-1}b \in H\}$ je ekvivalence, popřípadě najděte konkrétní příklad, který tento fakt vyvrací.

Cvičení D.3: Pro grupu $(G, \cdot)$ a její podgrupu H zkuste obecně dokázat, že relace $\sim := \{[a, b] \in G \times G : \exists x \in G : a = xbx^{-1}\}$ je ekvivalence.

Cvičení 8.2. 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.

Cvičení 8.3. Cvičení k pojmu levá a pravá třída prvku vzhledem k podgrupě ([8], 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.

Důležitý dodatek, možno dělat na cvičení: Lagrangeova věta (a její důsledek – věta 20) společně s větou 12 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 20), a tedy až na izomorfismus stejná jako $(H_p, +)$ neboli $(Z_p, +)$ (věta 12), 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 ([8], 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.

Výsledky některých cvičení najdete v závěru textu v oddílu 11.8.

8 Homomorfismus, normální podgrupa

8.1 Přednáška

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[23].

Definice 9.1 Grupový homomorfismus $f : G \to H$ je takové zobrazení mezi grupami $(G, \bigtriangledown)$ a $(H, *)$, které zachovává výsledky operace, tj. platí vlastnost

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

Příklad 9.1. 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 9.2. 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

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

zůstává zachována celočíselná odchylka nejbližšího násobku tří na číselné ose směrem vlevo od libovolného reprezentanta dané třídy rozkladu.□

Definice 9.2. 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 9.2: 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, prtože homomorfismus je obecnější pojem (každý grupový izomorfismus je současně i grupovým homomorfismem):

Věta 22. 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.

Normální podgrupa grupy

K definici normální podgrupy se dostaneme přes definici konjugovaného prvku:

Definice 9.3. Pro grupu $(G, \bigtriangledown)$ a její prvek a definujeme konjugovaný prvek k prvku $a \in G$, pokud existuje $x \in G$ tak, že $x \bigtriangledown a \bigtriangledown x^{-1}$.

Věta 23. Než půjdeme dále, všimněme si dvou trivialit:

a) **Každý prvek** a **grupy** G **je konjugovaný se sebou samotným**, protože vždy platí $a = a \bigtriangledown a \bigtriangledown a^{-1}$ (pro $x = a$) nebo $a = e \bigtriangledown a \bigtriangledown e^{-1}$ (pro $x = e$, kde e je neutrální prvek grupy $(G, \bigtriangledown)$ a o neutrálním prvku víme, že je vždy inverzí k sobě samotnému).

b) Jistě k některým prvkům $a \in G$ bude existovat více navzájem různých konjugovaných prvků jinak by tento pojem vůbec neměl smysl, kdyby každý prvek byl konjugovaný jen sám se sebou. Nicméně určitě víme, že **k neutrálnímu prvku** $e \in G$ **neexistuje žádný jiný konjugovaný prvek než** e **samotný**, protože

$$\forall x \in G: \quad x \bigtriangledown e \bigtriangledown x^{-1} \overset{(3)}{=} x \bigtriangledown x^{-1} \overset{(4)}{=} e.$$

Příklad 9.3. Najděme v grupě $(Z_6, +)$ všechny konjugované prvky k prvku 2: budeme procházet všechna možná $x \in G$ a počítat konjugované prvky $x + 2 + x^{-1}$:

$$\begin{aligned} 0 + 2 + 0 &= 2, \\ 1 + 2 + 5 &= 2, \\ 2 + 2 + 4 &= 2, \\ 3 + 2 + 3 &= 2, \\ 4 + 2 + 2 &= 2, \\ 5 + 2 + 1 &= 2. \end{aligned}$$

Poslední dva řádky už byly zbytečné, protože daný součet prvku a jeho inverze byl proveden v jiném pořadí na řádcích druhém a třetím, ale díky tomu, že operace sčítání je komutativní, jsme mohli pořadí prvků zaměnit. Dospěli jsme k zjištění, že v našem příkladu je prvek [2] konjugovaný pouze se sebou samotným. A když si toto zjištění rozmyslíme podrobněji, poobný výsledek dostaneme v jakékoli komutativní grupě, protože prvky x a x^{-1} lze díky komutativitě seskupit vedle sebe a provést operaci s nimi jako první, výsledkem je jednotkový prvek, a tak vždy bude platit

$$x \bigtriangledown a \bigtriangledown x^{-1} \overset{(5)}{=} x \bigtriangledown x^{-1} \bigtriangledown a = e \bigtriangledown a = a.$$

Touto úvahou jsme dokázali tuto větičku:

Věta 24. V komutativní grupě je k prvku a konjugovaný pouze prvek a samotný.

Příklad 9.4. Zkusme najít všechny konjugované prvky v grupě permutací $(S_3, \circ)$ k prvku u (viz tabulka operace $\circ$ ve větě 7 kapitoly 4):

$$\begin{aligned} e \circ u \circ e^{-1} &= u, \\ u \circ u \circ u^{-1} &= u, \\ v \circ u \circ v^{-1} &= w, \\ w \circ u \circ w^{-1} &= t, \\ s \circ u \circ s^{-1} &= t, \\ t \circ u \circ t^{-1} &= w. \end{aligned}$$

K prvku u tedy existují tři konjugované prvky u, w, t.

Nyní jsme připraveni na definici normální podgrupy:

Definice 9.4. Podgrupa $(H, \bigtriangledown)$ grupy $(G, \bigtriangledown)$ se nazývá normální podgrupa, pokud je uzavřená vzhledem ke konjugovaným prvkům, tj. platí

$$a \in H, x \in G \quad \Rightarrow \quad x \bigtriangledown a \bigtriangledown x^{-1} \in H.$$

Díky větičce 24 platí věta 25:

Věta 25. V komutativní grupě je každá podgrupa normální.

Ad příklad 9.4. Z příkladu 9.4 je vidět, že v nekomutativních grupách obecně existuje více konjugovaných prvků k danému prvku, tj. například podgrupa $(\{e, u\}, \circ)$ grupy $(S_3, \circ)$ není normální, protože k prvku u kromě jeho samotného existují dva další konjugované prvky t, w, takže podgrupa $(\{e, u\}, \circ)$ není uzavřená na konjugované prvky.

Definice 9.5. Jádro grupového homomorfismu $f : G \to H$ se nazývá množina $\ker_f$ (označení 09)[24] těch prvků z grupy $(G, \bigtriangledown)$, které se zobrazí na neutrální prvek e_H grupy $(H, *)$.

Příklad 9.5. a)V grupovém izomorfismu je jádrem zobrazení f pouze jednoprvková množina $\{e_G\}$.

b) V homomorfismu $f : Z_6 \to Z_3$ z příkladu 9.3 je jádrem množina těch prvků, které se zobrazí na nulu: $\ker_f = \{0, 3\}$.

Věta 26. 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

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

($f(a) = e_H$) 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 $(H, *)$.

8.2 Cvičení

Viz [8], str. 141-146:

- A. Příklady homomorfismu konečných grup.

  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).

  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

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

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

$$e = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 2 & 3 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 3 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 1 & 2 \end{pmatrix},$$
$$u = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 1 & 3 & 2 \end{pmatrix}, \quad v = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 3 & 2 & 1 \end{pmatrix}, \quad w = \begin{pmatrix} 1 & 2 & 3 \\ \downarrow & \downarrow & \downarrow \\ 2 & 1 & 3 \end{pmatrix}.$$

- 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).

- C. Základní vlastnosti homomorfismu.
- D. Základní vlastnosti normální podgrupy.

Například D.0: Zjistěte, zda $\{e, s, t\}$ je normální podgrupa grupy permutací tříprvkové množiny $(S_3, \circ)$. Můžete použít tabulku operace $\circ$:

$\circ$	e	s	t	u	v	w
e	e	s	t	u	v	w
s	s	t	e	w	u	v
t	t	e	s	v	w	u
u	u	v	w	e	s	t
v	v	w	u	t	e	s
w	w	u	v	s	t	e

- F. Homomorfismus a řád prvku.

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 22 a předchozích dvou větiček N.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.

- G. Vlastnosti zachované homomorfismem.
- I. Konjugované podgrupy vzhledem k podgrupě.

Výsledky některých cvičení najdete v závěru textu v oddílu 11.9.

9 Faktorgrupa

9.1 Přednáška

V minulé přednášce jsme se naučili poznat. kdy je H homomorfním obrazem grupy G (tehdy, když existuje surjektivní homomorfismus G na H). Nyní uděláme velký skok a naučíme se zkonstruovat všechny možné homomorfní obrazy jakékoli grupy G. Nejdůležitejším pojmem při této konstrukci je právě pojem normální podgrupy (= podgrupy uzavřené vzhledem ke konjugovaným prvkům).

Začneme tím, že si všimneme vztahu mezi normální podgrupou a levou a pravou třídou prvku vzhledem k této podgrupě (věta 27 představuje jakousi formu „komutativity“ – sice díky ní nemáme zaručeno $a \bigtriangledown h_1 = h_1 \bigtriangledown a$ (to platí jen tehdy, je-li grupa G komutativní), ale máme s využitím dvou prvků $h_1, h_2 \in H$ zaručeno, že $a \bigtriangledown h_1 = h_2 \bigtriangledown a$; jinými slovy, v normální podgrupě můžeme i při nekomutativní operaci zaměnit pořadí prvků, pokud nahradíme $h_1 \in H$ obecně jiným prvkem $h_2 \in H$):

Věta 27. H je normální podgrupa grupy $(G, \bigtriangledown)$, tj. $a \bigtriangledown h \bigtriangledown a^{-1} \in H \quad \forall a \in G$. Pak $a \bigtriangledown H = H \bigtriangledown a$ (levá a pravá třída prvku jsou totožné).

Důkaz: „$\subseteq$“:

$$x \in a \bigtriangledown H \quad \Rightarrow \quad x = a \bigtriangledown h = a \bigtriangledown h \bigtriangledown (a^{-1} \bigtriangledown a) \overset{(2)}{=} \underbrace{(a \bigtriangledown h \bigtriangledown a^{-1})}_{\in H} \bigtriangledown a \quad \Rightarrow \quad x \in H \bigtriangledown a.$$

„$\supseteq$“:

$$x \in H \bigtriangledown a \quad \Rightarrow \quad x = h \bigtriangledown a = (a \bigtriangledown a^{-1}) \bigtriangledown h \bigtriangledown a \overset{(2)}{=} a \bigtriangledown \underbrace{(a^{-1} \bigtriangledown h \bigtriangledown a)}_{\in H} \quad \Rightarrow \quad x \in a \bigtriangledown H.$$

Důkaz je hotov. $\square$

Definice operace pro třídy prvků

Co kdybychom nyní na pravých třídách prvku (podle věty 17 se jedná o třídy rozkladu G) chtěli definovat operaci $\underline{\bigtriangledown}$ odvozenou od operace $\bigtriangledown$, jejímž výsledkem by byla nějaká (obecně další) třída rozkladu grupy G? Definiční vztah by mohl mít tvar

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

Problém je ten, že nevíme, zda tato operace je korektně definována – byla by korektně definována jen v případě, že při výběru jiného prvku $c \in H \bigtriangledown a$ (což můžeme udělat, protože pro $c \in H \bigtriangledown a$ platí podle věty 16, že $H \bigtriangledown a = H \bigtriangledown c$) a prvku $d \in H \bigtriangledown b$ (protože pak podle věty 16 platí $H \bigtriangledown b = H \bigtriangledown d$) by platilo

$$(H \bigtriangledown c)\underline{\bigtriangledown}(H \bigtriangledown d) = H \bigtriangledown (c \bigtriangledown d) \quad \wedge \quad H \bigtriangledown (a \bigtriangledown b) = H \bigtriangledown (c \bigtriangledown d).$$

Pak by totiž (a tak se této vlastnosti i říká) nově definované „násobení tříd“ (vzhledem k operaci $\underline{\bigtriangledown}$) **nezáviselo na výběru reprezentantů**: ať bychom ze třídy $H \bigtriangledown a = H \bigtriangledown c$

vybrali reprezentanta a nebo c, a ze třídy $H \bigtriangledown b = H \bigtriangledown d$ vybrali reprezentanta b nebo d, dostali bychom jednoznačně určenou třídu $H \bigtriangledown (a \bigtriangledown b) = H \bigtriangledown (c \bigtriangledown d)$.

Příklad 10.1. Obecně myšlenku právě navrženou nelze realizovat, například pro $G = (S_3, \circ)$ a $H = (\{e, u\}, \circ)$ pravé třídy jsou třídy

$$\begin{aligned} H \circ v &= \{v, s\} = H \circ s, \\ H \circ t &= \{t, w\} = H \circ w, \\ H \circ e &= H = H \circ u. \end{aligned}$$

Všechny pravé třídy prvků vzhledem k téže podgrupě H tedy tvoří podle věty 17 rozklad grupy $G = (S_3, \circ)$, to samozřejmě platí pro libovolnou grupu, tedy i pro tu v tomto příkladu. Ovšem pokud bychom nyní chtěli definovat spojení tříd $H \circ v$ a $H \circ t$ způsobem

$$(H \circ v)\underline{\circ}(H \circ t) := H \circ (v \circ t) = H \circ u = H,$$

toto spojení tříd by záviselo na výběru reprezentanta, protože výběrem druhých možných prvků z daných tříd bychom dostali

$$(H \circ s)\underline{\circ}(H \circ w) := H \circ (s \circ w) = H \circ v = \{v, s\} \neq H,$$

tedy výběrem různých reprezentantů z těchto tříd dostáváme různé třídy – celý proces tedy není korektně definován, operace se třídami nefunguje jako zobrazení, kdy je každé dvojici tříd (v daném pořadí) jednoznačně přiřazen výsledek operace. Na třídách rozkladu podle podgrupy $H = \{e, u\}$ nelze toto spojení tříd korektně definovat.

Pokud ovšem H je normální podgrupa, násobení tříd lze definovat korektně:

Věta 28. Pokud H je normální podgrupa grupy $(G, \bigtriangledown)$ a platí

$$\begin{aligned} H \bigtriangledown a &= H \bigtriangledown c, \\ H \bigtriangledown b &= H \bigtriangledown d, \end{aligned}$$

tak operace $\bigtriangledown$ použitá na třídy prvků nezávisí na výběru reprezentantů, tj.

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

Důkaz: i)

$$H \bigtriangledown a = H \bigtriangledown c \quad \Rightarrow a \in H \bigtriangledown c,$$

protože $a \in H \bigtriangledown a$ (neboť $a = e \bigtriangledown a \in H \bigtriangledown a$, kde $e \in H$ je neutrální prvek), tak podle předpokladu věty také $a \in H \bigtriangledown c$. Tedy $a = h_1 \bigtriangledown c$ pro nějaké $h_1 \in H$.

ii)

$$H \bigtriangledown b = H \bigtriangledown d \quad \Rightarrow b \in H \bigtriangledown d,$$

protože $b \in H \bigtriangledown b$ (neboť $b = e \bigtriangledown b \in H \bigtriangledown b$, kde $e \in H$ je neutrální prvek), tak podle předpokladu věty také $b \in H \bigtriangledown d$. Tedy $b = h_2 \bigtriangledown d$ pro nějaké $h_2 \in H$.

Dohromady z i) a ii) plyne:

$$a \triangledown b = h_1 \triangledown c \triangledown h_2 \triangledown d.$$

Nyní využijeme předpokladu, že H je normální podgrupa, tj. podle věty 27 platí $c \triangledown H = H \triangledown c$, tedy $c \triangledown h_2$ lze upravit

$$c \triangledown h_2 = h_3 \triangledown c$$

pro nějaké $h_3 \in H$. Pokračujme v úpravě $a \triangledown b$ a dostaneme

$$a \triangledown b = h_1 \triangledown (c \triangledown h_2) \triangledown d = \underbrace{h_1 \triangledown h_3}_{\in H} \triangledown c \triangledown d \in H \triangledown (c \triangledown d).$$

Celkem protože $a \triangledown b \in H \triangledown (c \triangledown d)$, tak podle věty 16 platí

$$H \triangledown (a \triangledown b) = H \triangledown (c \triangledown d).$$

Důkaz je hotov!!□

Označení 10. Označme množinu tříd $G/_H$ rozkladu podle normální podgrupy H ... vzhledem k operaci $\underline{\triangledown}$ definované pomocí vztahu

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

jako tzv. rozkladovou grupu nebo též při doslovném překladu faktorgrupu[25].

Věta 29. Struktura $G/_H$ vytvořená z tříd podle normální podgrupy H s operací $\underline{\triangledown}$ je grupa.

Důkaz. Vlastnost (1): korektní definice operace $\underline{\triangledown}$ pro třídy rozkladu a uzavřenost této operace plyne z věty 28.

Vlastnost (2): Asociativita plyne z asociativity operace $\triangledown$ na $(G, \triangledown)$ a korektní definice operace mezi třídami (věta 28):

$$\begin{aligned}&((H \triangledown a)\underline{\triangledown}(H \triangledown b))\underline{\triangledown}(H \triangledown c) = (H \triangledown (a \triangledown b))\underline{\triangledown}(H \triangledown c) = H \triangledown ((a \triangledown b) \triangledown c) = \\ &= H \triangledown (a \triangledown (b \triangledown c)) = (H \triangledown a)\underline{\triangledown}(H \triangledown (b \triangledown c)) = (H \triangledown a)\underline{\triangledown}((H \triangledown b)\underline{\triangledown}(H \triangledown c)).\end{aligned}$$

Vlastnost (3): Neutrálním prvkem je třída $H \triangledown e$, protože platí (e je neutrální prvek v $(G, \triangledown)$):

$$(H \triangledown a)\underline{\triangledown}(H \triangledown e) = H \triangledown a,$$
$$(H \triangledown e)\underline{\triangledown}(H \triangledown a) = H \triangledown a.$$

Vlastnost (4): Inverzním prvkem ke třídě $H \triangledown a$ je třída $H \triangledown a^{-1}$:

$$(H \triangledown a)\underline{\triangledown}(H \triangledown a^{-1}) = H \triangledown e,$$
$$(H \triangledown a^{-1})\underline{\triangledown}(H \triangledown a) = H \triangledown e.$$

[25] Anglicky FACTOR znamená, „rozložit“.

Věta 30. Rozkladová grupa $(G/_H, \triangledown)$ je homomorfním obrazem grupy $(G, \triangledown)$, neboli přirozeně definované zobrazení f, které přiřadí prvku $a \in G$ třídu $H \triangledown a \in G/_H$, je surjektivní grupový homomorfismus.

Důkaz. Zobrazení f je a) surjekce, což plyne z konstrukce zobrazení f: pro libovolnou třídu $H \triangledown c$ je vzorem prvek $c \in G$;

b) je splněna vlastnost zachování výsledků operace:

$$f(x \triangledown y) \overset{def.}{=} H \triangledown (x \triangledown y) \overset{v.28}{=} (H \triangledown x)\underline{\triangledown}(H \triangledown y) \overset{def.}{=} f(x)\underline{\triangledown}f(y).$$

Jedná se tedy o surjektivní homomorfismus, tedy grupa obrazů je homomorfním obrazem grupy vzorů.□

Tímto způsobem (= podle věty 30), jak brzy uvidíme (viz příklad 10.3), lze zkonstruovat všechny homomorfní obrazy grupy $(G, \triangledown)$.

Příklad 10.2. Pokud $G = (Z, +)$ a $H =< 6 >= \{\ldots, -12, -6, 0, 6, 12, \ldots\}$ její cyklická podgrupa (která je současně normální podgrupou, protože $(Z, +)$ je komutativní grupa – věta 25), třídy prvku vzhledem k podgrupě $(H, +)$ jsou

$$\begin{aligned}
< 6 > +0 &= \{\ldots, -12, -6, 0, 6, 12, \ldots\} =< 6 > +6,\\
< 6 > +1 &= \{\ldots, -11, -5, 1, 7, 13, \ldots\} =< 6 > +7,\\
< 6 > +2 &= \{\ldots, -10, -4, 2, 8, 14, \ldots\} =< 6 > +8,\\
< 6 > +3 &= \{\ldots, -9, -3, 3, 9, 15, \ldots\} =< 6 > +9,\\
< 6 > +4 &= \{\ldots, -8, -2, 4, 10, 16, \ldots\} =< 6 > +10,\\
< 6 > +5 &= \{\ldots, -7, -1, 5, 11, 17, \ldots\} =< 6 > +11, \text{ atd.}
\end{aligned}$$

Zkrátka všech různých tříd prvků vzhledem k podgrupě $< 6 >$ je pouze šest, a těchto šest tříd (věta 17) tvoří rozklad množiny Z. Podle věty 25 je $< 6 >$ normální podgrupa, tj. podle věty 28 sčítání těchto tříd nezávisí na výběru reprezentanta, tj. struktura $Z_6 := (Z/_{<6>}, +)$ je faktorgrupa (rozkladová grupa) grupy $(Z, +)$. V této kapitole 10 jsme tedy dopodrobna popsali konstrukci grupy zbytkových tříd $(Z_6, +)$. Tato grupa je homomorfním obrazem grupy $(Z, +)$, pokud definujeme zobrazení f přirozeně tím způsobem, že prvku $z \in Z$ je přiřazena třída $[z]$ grupy $(Z/_{<6>}, +)$.

Věta 31. Vraťme se ještě k základním vlastnostem podgrup a dokažme jednu vlastnost (a), kterou budeme potřebovat ve zbytku kapitoly, a druhou vlasnost (b), která platí triviálně a už jsme s ní pracovali, ale nyní bude vyslovena ve tvaru ekvivalence: **Pro každou grupu $(G, \triangledown)$ a její podgrupu H platí**

a) $H \triangledown a = H \triangledown b \quad \Leftrightarrow \quad a \triangledown b^{-1} \in H.$

b) $H \triangledown a = H \quad \Leftrightarrow \quad a \in H.$

Důkaz.ad a) „⇒“: Pokud $H \triangledown a = H \triangledown b$, kde $e \in H$ je neutrální prvek vzhledem k operaci $\triangledown$, tak protože $a = e \triangledown a \in H \triangledown a$, musí $a \in H \triangledown b$. Tedy

$$a = h \triangledown b$$

pro nějaké $h \in H$ a vynásobením této poslední rovnosti prvkem b^{-1} zprava dostaneme

$$a \triangledown b^{-1} = h, \text{ tedy } a \triangledown b^{-1} \in H.$$

„$\Leftarrow$“:

$$a \triangledown b^{-1} \in H \quad \Rightarrow \quad a \triangledown b^{-1} = h \quad \Rightarrow \quad a = h \triangledown b \quad \Rightarrow \quad a \in H \triangledown b \quad \overset{v.16}{\Rightarrow} \quad H \triangledown a = H \triangledown b.$$

ad b) lze dokázat přímo (pomocí dvou implikací), ale tvrzení i důkaz je speciálním případem čísti (a) pro $b = e$ (kde pro neutrální prvek $e \in H$ platí $H \triangledown e = H$ a $e^{-1} = e$). Důkaz je hotov. $\square$

Příklad 10.3. V tomto příkladu naznačíme, jak lze zkonstruovat homomorfní obraz grupy, ve kterém je zachována vlastnost, kterou jsme si zvolili jako pozitivní a kladnou, zatímco vlastnost, kterou chápeme jako nežádoucí, je v homomorfním obrazu „vyloučena“: Dejme tomu, že se nám líbí vlastnost (5) = komutativita, ale grupa G je nekomutativní, tj. obsahuje dvojice prvků a, b, pro které $a \triangledown b \neq b \triangledown a$. Rádi bychom nekomutativní prvky „vyloučili“ z této grupy, ale všechny ostatní prvky zachovali. Uděláme to následujícím způsobem:

Uvažujme podmnožinu H všech komutátorů v G, neboli všech součinů tvaru

$$a \triangledown b \triangledown a^{-1} \triangledown b^{-1}.$$

Důvod, proč se tyto prvky nazývají komutátory, je platnost podmínky

$$a \triangledown b \triangledown a^{-1} \triangledown b^{-1} = e \quad \Leftrightarrow \quad a \triangledown b = b \triangledown a$$

(tedy pro komutativní dvojici prvků je komutátor z ní vytvořený (bez ohledu na jejich pořadí) roven neutrálnímu prvku, a právě ve všech ostatních případech nekomutativních dvojic prvků je komutátor z nich vytvořený jiný prvek než e). Tedy v komutativní grupě jsou všechny komutátory rovny neutrálnímu prvku e. V nekomutativní grupě G je počet všech komutátorů jakýmsi měřítkem toho, jak dalece se G odchyluje od vlastnosti (5).

Pokud množina všech komutátorů H je normální podgrupou grupy G, pak tedy faktorgrupa G/H bude obsahovat jen jediný komutátor, a sice třídu $H \triangledown e = H$, tedy triviální komutátor, který v grupě existuje vždy – ale žádné jiné!! Tedy grupa G/H je komutativní – faktorizací neboli konstrukcí rozkladové grupy jsme „odstranili“ nekomutativní prvky a „zachovali“ pouze ty komutativní.

To vskutku platí, ověřme podmínku komutativity operace $\triangledown$ v podílové grupě G/H:

$$(H \triangledown x)\underline{\triangledown}(H \triangledown y) = (H \triangledown y)\underline{\triangledown}(H \triangledown x)$$

lze upravit vzhledem ke korektně definované operaci (věta 28) na tvar

$$H \triangledown (x \triangledown y) = H \triangledown (y \triangledown x),$$

a to podle věty 31a) platí právě tehdy, když $x \triangledown y \triangledown (y \triangledown x)^{-1} \in H$. To je ovšem splněno, protože podle věty 5 o výpočtu inverze součinu $(y \triangledown x)^{-1} = x^{-1} \triangledown y^{-1}$, a tedy

$$x \triangledown y \triangledown (y \triangledown x)^{-1} = x \triangledown y \triangledown x^{-1} \triangledown y^{-1},$$

a to je právě prvek typu komutátor, který patří do H.

Fundamentální věta o homomorfismu

Ve větě 30 jsme viděli, že každá podílová grupa je homomorfním obrazem (vzhledem k surjektivnímu homomorfismu) grupy G. Nyní naopak dospějeme k větě 33, že každý homomorfní obraz grupy G je její rozkladovou grupou. Všimneme si totiž, že platí podmínka věty 32:

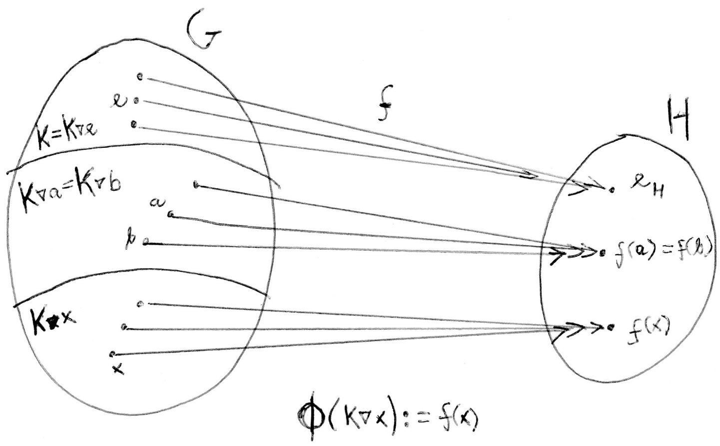
Věta 32. Pro grupový homomorfismus $f : (G, \triangledown) \to (H, *)$ s jádrem $K := \ker_f$ (které podle věty 26-(a) je normální podgrupou grupy G) platí

$$K \triangledown a = K \triangledown b \quad \Leftrightarrow \quad f(a) = f(b).$$

Důkaz: Využívá věty 31a), viz též obrázek 10 (každá třída $K \triangledown x$ se zobrazí na jediný prvek):

$$K \triangledown a = K \triangledown b \quad \overset{v.31a)}{\Leftrightarrow} \quad a \triangledown b^{-1} \in K \quad \Leftrightarrow \quad f(a \triangledown b^{-1}) = e_H \quad \overset{(hom)}{\Leftrightarrow} \quad f(a) * [f(b)]^{-1} = e_H,$$

a poslední uvedenou rovnost lze ekvivalentně (pracujeme v grupě) upravit vynásobením $f(b)$ zprava na rovnost $f(a) = f(b)$, čímž dostaneme podmínku věty.



Obrázek 10: Definice izomorfismu Φ na základě homomorfismu f.

Věta 33. Pro surjektivní grupový homomorfismus $f : (G, \triangledown) \to (H, *)$ s jádrem K lze zkonstruovat podílovou grupu $G/_K$ a zobrazení $\Phi : G/_K \to H$, které je grupovým izomorfismem.

Důkaz: Definujeme-li zobrazení Φ předpisem

$$\Phi(K \triangledown x) := f(x)$$

(zobrazení Φ přiřadí třídě $K \triangledown x$ ten prvek v H, který je obrazem prvku x vzhledem k homomorfismu f), toto zobrazení je podle věty 32 korektně definováno a dokonce z věty

32 plyne, že se jedná o injekci:

$$\Phi(K \bigtriangledown a) = \Phi(K \bigtriangledown b) \quad \Rightarrow \quad f(a) = f(b) \overset{v32}{\Rightarrow} K \bigtriangledown a = K \bigtriangledown b.$$

Surjektivita Φ plyne ze surjektivity zobrazení f: každý prvek grupy $(H, *)$ je tedy tvaru $f(x) = \phi(K \bigtriangledown x)$. A nakonec platí i podmínka zachování výsledků operace:

$$\Phi(K \bigtriangledown a \underline{\bigtriangledown} K \bigtriangledown b) = \Phi(K \bigtriangledown a \bigtriangledown b) = f(a \bigtriangledown b) = f(a) * f(b) = \phi(K \bigtriangledown a) * \phi(K \bigtriangledown b).$$

Příklad 10.4. Homomorfismus $f : (Z_6, +) \to (Z_3, +)$ z příkladu 9.2 definovaný vztahem

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

má jádro $K = \{0, 3\}$. Podílová grupa podle tohoto jádra musí být (věta 33) izomorfní grupě $(Z_3, +)$:

$$Z_6/\{0, 3\} \cong Z_3$$

(s operací sčítání v obou grupách).

9.2 Cvičení 10

Vhodná cvičení v knize [8]: za kapitolami 15 a 16.

A. Příklady konečných faktorgrup:

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.

B. Příklady nekonečných faktorgrup

Výsledky některých cvičení najdete v závěru textu v oddílu 11.10.

10 Struktury se dvěma operacemi

10.1 Přednáška

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 11.1. podruhé 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):

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

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

Příklad 11.1.

- 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 11.2. netriviální 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 11.2. Příkladem struktury s netriviálními dělitely nuly je množina Z_6 zbytkových tříd modulo 6: její prvky [2], [3] nebo [3], [4] jsou netriviální 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 11.3. obor integrity[26] (anglicky: integral domain) je množina[27] $(M, +, \cdot)$ 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 11.3.

- $(Z_7, \oplus, \odot)$ 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:

Definice 11.4. podruhé 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[28];

---

[26] 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.

[27] 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 $0 \neq 1$.

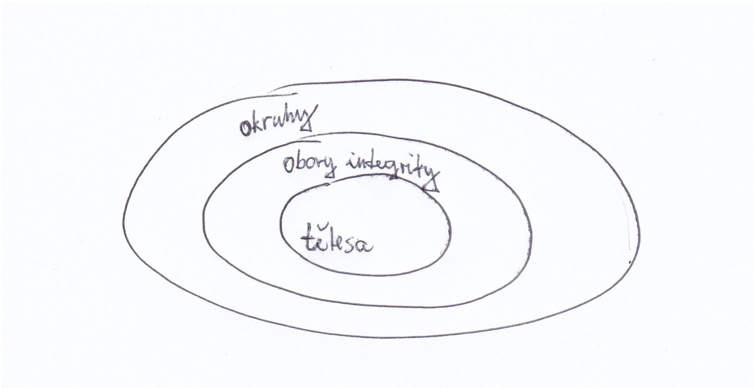
[28] Vlastnost (4) je silnější než vlastnost „neobsahuje netriviální dělitele nuly“, tj. u bodu b) je dostatečné uvést, že operace $\cdot$ u tělesa splňuje (1),(2),(3),(4),(5). Lze dokázat tvrzení, že každé těleso je i oborem integrity, tj. těleso „neobsahuje netriviální dělitele nuly“.

ad c) zde nic nového.

Příklad 11.4.

- $(Z_7, \oplus, \odot)$ 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 11: 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.

Definice 11.5. 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 11.5. Nejpřirozenějším příkladem ideálu je podmnožina B sudých celých čísel okruhu $(Z, +, \cdot)$:

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

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 $(Z, +, \cdot)$.

V teorii ideálů hraje klíčové místo tzv. hlavní ideál okruhu, který definujeme (definice 11.6.) jako takový ideál B, který vygenerujeme jediným prvkem b, jenž vynásobíme se všemi prvky množiny M.

Příklad 11.6. 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 9.5:

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

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

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

- 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.

Věta 34. Zde nyní je snad vhodné upozornit na matematickou větu, kterou zakončíme tento semestr (jejíž důkaz je nechán pro cvičení), že ideál je v okruhu analogie toho, co v grupě je normální podgrupa: **Uvažujeme-li homomorfismus okruhů (= homomorfismus, který zachovává výsledky obou operací $+$ i $\cdot$), tak jeho jádro $\ker_f$ (= množina všech prvků prvního okruhu, které se zobrazí na neutrální prvek vzhledem k $+$ ve druhém okruhu) je ideálem prvního okruhu** ... to je analogie věty 26a) pro homomorfismus okruhů, která říká, že jádro homomorfismu grup je normální podgrupa.

Poznámka na závěr semestru

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 probírané ve vlastnostech (1) až (10) jsou samy o sobě zajímavé, posloužily v historii právě v tom nejdůležitějším úkolu algebry, a tedy ke hledání řešení algebraických rovnic. Po jednosemestrové odbočce do předmětu Algebra 2, která se týká algebraického pohledu na geometrii a je zhruba řečeno jakýmsi metodickým úvodem do analytické geometrie, se k tématu řešení algebraických rovnic studenti vrátí v předmětu Algebra 3 a měli by se dozvědět, jakým způsobem lze na několika důležitých věcech zúročit studium třiceti čtyř vět a několika pojmů v tomto semestru.

10.2 Cvičení

Procvičení pojmů okruh, obor integrity, těleso: např. viz [8], 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 [8], 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.

Výsledky některých cvičení najdete v závěru textu v oddílu 11.11.

11 Výsledky některých příkladů

11.1 Výsledky ke cvičení 1.3 – Vlastnosti operací (1) až (5)

Ad cvičení 1.1:

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 $-2 \notin N$. $\square$

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. $\square$

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. $\square$

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.

11.2 Výsledky ke cvičení ?? – Vlastnosti operací (6) až (10)

K této kapitole dosud nejsou uvedeny žádné příklady s výsledkem.

11.3 Výsledky ke cvičení 2.3 – Základní vlastnosti grup

Ad cvičení 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 cvičení 3.3 – F.3: Tabulku lze doplnit na:

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

.

11.4 Výsledky ke cvičení 3.3 – Podgrupy a generátory grupy

Ad cvičení 4.1 – 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 cvičení 4.1 – 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 cvičení 4.2 – N.1: $H = \{6, 12, 2, 8, 14, 4, 10, 0\}$ a prvky jsou napsány v tom pořadí, jak je získáváme otočením o prvek 6.

Ad cvičení 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 cvičení 4.2 – E.1: 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 cvičení 4.2 – E.3: $< 6, 9 >= \{6, 0, 9, 3\}$ vzhledem k operaci skládání otáčení.
Ad cvičení 4.2 – E.7 modifikace: prvek $[1, 1]$ je generátorem podgrupy $\{[1; 1;], [0; 2], [1; 3], [0; 0]\}$ vzhledem ke sčítání.

Ad cvičení 4.2 – 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.

11.5 Výsledky ke cvičení 4.2 – nekomutativní grupy

Ad cvičení 5.1: 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 cvičení 5.3: Tabulka operace $\circ$ na množině D_3 symetrií trojúhelníku:

Tabulka 5: 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 $(S_3, \circ)$, 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 3). Izomorfismus bude precizně definován v následující kapitole, ale už teď můžeme říci, že 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.

11.6 Výsledky ke cvičení 5.3 – Izomorfismus, Cayleyho věta

K této kapitole dosud nejsou uvedeny žádné příklady s výsledkem.

11.7 Výsledky ke cvičení 6.2 – řád prvku, cyklické grupy

ad Cvičení 7.1.

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: $\alpha^3 = (1,2) \circ \mathrm{id} = (1,2)$, $\beta^4 = (1,5,2,7,6)$[29]. 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.

11.8 Výsledky ke cvičení 7.3 – Lagrangeova věta

K této kapitole dosud nejsou uvedeny žádné příklady s výsledkem.

11.9 Výsledky ke cvičení 8.2 – Homomorfismus, normální podgrupa

Ad cvičení F: Řád prvku a homomorfismus:

Ad Například N.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 $G_1 = (G, \triangledown)$, 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

[29] 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.

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 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: $0 \overset{\varphi}{\to} 0$, $1 \overset{\varphi}{\to} 0$ ... 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: $0 \overset{\varphi}{\to} 0$, $1 \overset{\varphi}{\to} 1$ ... podle podmínky homomorfismu nyní dopočteme, že musí nastat $2 = 1+1 \overset{\varphi}{\to} \varphi(1)+\varphi(1) = 2$, dále $3 = 2+1 \overset{\varphi}{\to} \varphi(2)+\varphi(1) = 2+1 = 3$, atd. Jádrem je množina $\{0, 4\}$

hom 03: $0 \overset{\varphi}{\to} 0$, $1 \overset{\varphi}{\to} 2$ ... 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: $0 \overset{\varphi}{\to} 0$, $1 \overset{\varphi}{\to} 3$ ... 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, [8] 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: $\varphi_1([0]) =$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.

11.10 Výsledky ke cvičení 9.2 – Podílová grupa

K této kapitole dosud nejsou uvedeny žádné příklady s výsledkem.

11.11 Výsledky ke cvičení 10.2 – Struktury se dvěma operacemi

K této kapitole dosud nejsou uvedeny žádné příklady s výsledkem.

Seznam literatury:

1 P. Horák: M 1125 Základy matematiky. Elektronický text do analogického předmětu na Přírodovědecké fakultě MU Brno. Počet stran 100 v roce 2013. Tento text pokrývá předmět M0001 Základy matematiky na Pedagogické fakultě asi z poloviny, ale i daná polovina se věnuje záležitostem odlišným od těch, na které je kladen důraz na Pedagogické fakultě.

2 Rediger Thiele: Matematické důkazy. SNTL Praha 1985. Počet stran 160. Představení zákonitostí logického usuzování a dokazování v matematice. Poněkud širší pokrytí tématu logika, kterému jsou v předmětu Základy matematiky věnovány první tři přednášky.

3 Raymond Smullyan: Jak se jmenuje tahle knížka? Zajímavé logické problémy od jednoduchých hádanek pro ZŠ až po složitější logické úlohy, které vyžadují důkladný vysokoškolský rozbor.

4 D.Jordan, P.Smith: Mathematical techniques. Oxford 2008, 4th Edition. V kontextu předmětu Základy matematiky nás z knihy zajímá zatím jen kapitolka 35 – sets (= množiny) na str. 791-800.

5 Eva Nováková: Analýza výsledků soutěže Matematický klokan, Brno 2016. Zajímavá kniha seznamující s mezinárodní soutěží Matematický klokan a rozborem výsledků této soutěže v ČR v kategorii pro 4.-5. třídy ZŠ. Tato kniha dobře uvádí do problematiky didaktiky matematiky na ZŠ: úlohy různého typu, dělení matematiky na různá odvětví, apod.

6 B.Fajmon: Základy matematiky – verze 2017. Doplnění přednášek v předmětu MA0001, počet stran 82.

7 Herman, Chrápavá, Jančovičová, Šimša: Matematika pro primy – úvodní opakování. Prometheus 1997, 2.přepracované vydání. Opakování učiva 1.stupně. Nultá kniha ze série sedmnácti knih pro 2.stupeň ZŠ a nižší ročníky osmiletých gymnázií.

8 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 (a tím i diskrétní matematika) je důležitá a má důležitá uplatnění.

9 O.Odvárko: Funkce, Prometheus 1993. Edice Matematika pro gymnázia, sešit 3, počet stran 160. Tento text je potřeba v závěru předmětu Základy matematiky a v úvodu navazujícího předmětu Matematická analýza 1 na Pedagogické fakultě MU.

10 O.Odvárko: Goniometrie, Prometheus 1994. Edice Matematika pro gymnázia, sešit 7, počet stran 127. Tento text je potřeba v závěru předmětu Základy matematiky a v úvodu navazujícího předmětu Matematická analýza 1 na Pedagogické fakultě MU.

11 S.Kowal: Matematika pro volné chvíle. Praha 1985, druhé vydání. Kniha, která na velkém množství úloh prochází celou historii matematiky v rámci zajímavých úloh, jejichž řešení uvádí buď v textu, nebo na konci každé kapitoly. Název láká širokou veřejnost, ale řada úloh je vysokoškolské obtížnosti, i když jejich řešení je často proveditelné i na SŠ.

12 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. Program po instalaci funguje offline.

13 J. Koláček: Výuka jazyka R. Rovněž úvod do jazyka R, nyní od vysokoškolského učitele matematiky, což je vhodným doplněním předchozího textu [12].

14 P. Horák: Cvičení z algebry a teoretické aritmetiky I, Brno 2002. Sbírka příkladů ke staršímu vydání textu [1] na Přírodovědecké fakultě MU.

15 Jiří Rosický: Algebra – grupy a okruhy 2000, reprint textu z roku 1985. Tento text je vhodný pro partie navazujícího předmětu Algebra 1 na PdF, nicméně jen až jako doplnění čtivější knihy [8].

16 Jan Kopka: Svazy a Booleovy algebry (Ústí nad Labem 1991, zejména str. 19-82). Kolega 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.

17 Jindřich pěnčík, Jarmila pěnčíková: Lámejte si hlavu. Sbírka úloh a hlavolamů pro základní školy, počet stran 382. Polovina knihy jsou zadání, druhá polovina řešení a výsledky. Dobrá kniha na doplnění hodin na ZŠ.

18 Ivan Bušek: Řešení maturitní úlohy z matematiky. SPN Praha 1985, kniha je k dostání v novějších vydáních stále ke koupi, možná i přepracovaná a doplněná. Dobrý pomocník k maturitě na gymnáziu, tj. dobrý pomocních k mnoha typům úloh v bakalářském pedagogickém studiu matematiky. Počet stran 530, novější vydání mají ještě větší počet stran.

19 Dag Hrubý, Josef Kubát: Matematika pro gymnázia 10 – diferenciální a integrální počet. Desátý sešit v edici pro gymnázia se zabývá zeména pojmy derivace a integrál. Prometheus 1997. Počet stran 195, stále sna nejlepší uvedení do diferenciálního a integrálního počtu, co na světě existuje. Doporučená literatura v předmětech Matem. analýza 1 a 2.

20 Milan Kočandrle,leo Boček: Matematika pro gymnázia 11 – analytická geometrie. Počet stran 186, Prometheus 1995. Uvedení do analytické geometrie se předpokládá, že studenti znají nebo si doplní, určitě znalost této knihy předpokládá předmět Analytická geometrie na PdF.

21 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.

22 Irena Budínová: Polynomy. Text určený studentům učitelství matematiky, Brno 2013. Počet stran 56.

23 B. Fajmon: Algebra 1. Text doplňující přednášku předmětu Algebra 1 – tento text, který právě čtete. Text vzniká v roce 2018.

24 Edice Nová škola 01, sešit Matematika – desetinná čísla. Brno 2012, první sešit ze série šestnácti učebnic, které vycházejí v letech 2012–2019 pro výuku na 2. stupni ZŠ. Počet stran 63, tato výkladová učebnice je doplněna ještě pracovním sešitem o 80 stranách, který ke každé kapitole výkladu v učebnici obsahuje příklady a) povinné pro vyplnění pracovního sešitu, b) procvičující, c) rozšiřující a náročnější pro zvídavější studenty.