Algebra 1 (MA 0003)

RNDr. Břetislav Fajmon, Ph.D.

Katedra matematiky Pedagogické fakulty Masarykovy univerzity v Brně – verze únor 2025

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 některé základní pojmy předmětu, které jsou shrnuty v otázkách 1 až 5 ke zkoušce ke konci tohoto textu.

V předmětu Základy matematiky jsme studovali zejména relace a jejich vlastnosti. Nyní v předmětu Algebra 1 budeme studovat zejména pojem operace. Tento text by nemohl vzniknout bez knihy (Pinter 2010), ze které jsem podstatně čerpal jak pro přednášku, tak pro cvičení. I když tento předmět se studentům nutně bude zdát teoretický, Charles Pinter napsal svou knihu s přesvědčením, že algebra je pro matematiku potřebná – stejně potřebná jako geometrie.

Rád bych zde vyjádřil díky za to, že studentka Andrea Danešová přepsala asi 50 stran tohoto textu z mého rukopisu do počítače v prostředí sazby textu TEX – jedná se o velmi pečlivý přepis, kde kromě velmi heslovitých poznámek z mé strany u některých přednášek se dobře zorientovala v tomto prostředí sazby tabulek a textů.

Text není úplně samonosný, odkazuje se i na učební pdf text kolegyně dr. Budínové o polynomech, pro část „komplexní čísla“ bude důležitou součástí i středoškolská učebnice (Robová, Hála, Calda 2013).

Břetislav Fajmon,
verze textu únor 2025

1 Týden 01

1.1 Cvičení 1: Vlastnosti číselných operací

Podívejme se na tzv. Axiomy euklidovské geometrie:

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

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

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

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

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

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

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

Vlastnost (2) Asociativita operace $*$:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Jestliže se to nestihne na prvním cvičení, měli byste si zopakovat ty nejdůležitější pojmy předmětu Základy matematiky:

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

a) *množina;*

b) *kartézský součin;*

c) *relace*

d) *ekvivalence;*

e) *uspořádání;*

f) *zobrazení;*

g) *operace;*

h) *(reálná) posloupnost;*

i) *(reálná) funkce.*

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

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

Definice z obou úloh najdete v textu Základy matematiky.

Úloha 1.3 *V množině celých čísel je definována operace $\circ$ předpisem $x \circ y = x + y - xy$. Zjistěte, zda operace $\circ$ je:*

a) neomezeně definovaná,

b) komutativní,

c) asociativní.

Dále zjistěte, zda množina Z vzhledem k operaci $\circ$ obsahuje prvek neutrální a případně, ke kterým celým číslům existují prvky inverzní.

Úloha 1.4 *V množině $M = \{0, 2, 3, 4\}$ je definována operace $\circ$ vztahem $x \circ y = (x - 1) \cdot (y - 1)$, který využívá známé oprace odčítání a násobení, jak jsme na ně zvyklí z práce s reálnými čísly. Zjistěte, zda je operace neomezeně definovaná (tj. uzavřená) na množině M. Sestavte operační tabulku.*

Úloha 1.5 *V množině $A = \{x, y\}$ jsou dány operace $\triangle, \square$ tabulkami. Určete všechny vlastnosti uvedených operací.*

$\triangle$	x	y
x	x	x
y	x	y

$\square$	x	y
x	x	y
y	y	x

Úloha 1.6 *Na množině $K = \{1, 2, 3\}$ je definovaná operace $\star$. Určete její vlastnosti.*

$\star$	1	2	3
1	3	1	2
2	1	2	3
3	1	3	1

Úloha 1.7 *Na množině Z je definována operace odčítání. Určete její vlastnosti, tj. určete, jakou algebraickou strukturou je $(Z, -)$.*

Úloha 1.8 *V množině Q je definována operace $\circ$ takto: $a \circ b = 2a + 2b - 5$. Pro operaci určete neomezenou definovanost, komutativnost, asociativnost, neutrální prvek, a ke kterým prvkům množiny existují prvky inverzní.*

Úloha 1.9 *V množině R je definována operace $\circ$ takto: $x \circ y = \sqrt{x^2 + y^2}$. Pro operaci určete neomezenou definovanost, komutativnost, asociativnost, neutrální prvek, a ke kterým prvkům množiny existují prvky inverzní.*

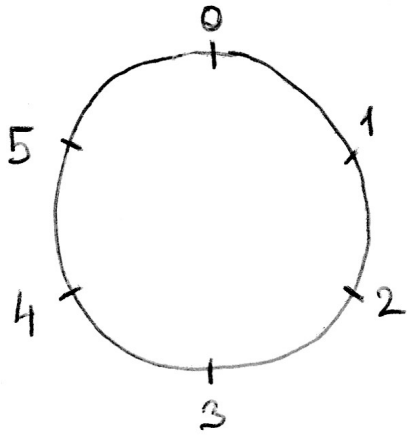
Výsledky některých cvičení najdete v závěru textu v oddílu 14.1.

1.2 Přednáška 1: Základní vlastnosti operace – příklady

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

Začněme ovšem jedním příkladem konečné, šestiprvkové grupy:

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



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

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

- *prvek* 0 *představuje nulové pootočení ručičky – s ručičkou se nic nestane;*
- *prvek* 1 *představuje pootočení o jednu jednotku, tj. o* 60°*;*
- *prvek* 2 *představuje pootočení ručičky o dvě jednotky, tj. o* 120°*;*
- *prvek* 3 *přestavuje pootočení o* 180°*;*
- *prvek* 4 *přestavuje pootočení o* 240°*;*
- *prvek* 5 *přestavuje pootočení o* 300°.

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

Dále operace skládání otáčení je asociativní (splňuje (2)), když totiž při počátečním nastavení ručičky do nulové polohy složíme otočení $(1+2)+4$[1], 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[2].

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 kterým když jej složíme, dostaneme ručičku zase do polohy 0:

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

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

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

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

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

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

Dále nás může zajímat, zda existují nějaké podmnožiny množiny H_6 uzavřené vzhledem k operaci skládání pootočení. Vlastnost (1) je splněna na následujících podmnožinách:

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

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

Tabulka 1.1: Tabulka operace + na množině H_6.

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

- $P_1 = \{0\}$ - triviální podmnožina množiny H_6 - podmnožina obsahující pouze neutrální prvek je vždy uzavřená na výsledek operace;
- $P_2 = H_6$ - triviální podmnožina množiny H_6 - tato podmnožina je také vždy uzavřená na výsledek operace;
- $P_3 = \{0, 3\}$;
- $P_4 = \{0, 2, 4\}$ - výsledky operace sčítání na této podmnožině znázorňuje tabulka 1.2.

Tabulka 1.2: Tabulka operace + na podmnožině $\{0, 2, 4\}$.

+	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

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. •

Definice 9 Triviální podgrupy (= nevlastní podgrupy) *grupy $(G, \bigtriangledown)$ se nazývají dvě podgrupy: a) $S_1 = \{n_0\}$ je podgrupou vzhledem k $\bigtriangledown$, která obsahuje pouze neutrální prvek, b) $S_2 = G$ (samotná celá grupa je též podgrupou sama sebe). Každou jinou podgrupu nazveme* **vlastní podgrupou** *grupy $(G, \bigtriangledown)$.*

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

Z je nekonečná množina, proto by tabulka výsledků operace + obsahovala nekonečně mnoho výsledků. Můžeme ji však naznačit alespoň pro několik prvků množiny:

Tabulka 1.3: Tabulka operace + na množině Z.

$+$	$\ldots$	-2	-1	0	1	2	$\ldots$
$\ldots$		$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	
-2	$\ldots$	-4	-3	-2	-1	0	$\ldots$
-1	$\ldots$	-3	-2	-1	0	1	$\ldots$
0	$\ldots$	-2	-1	0	1	2	$\ldots$
1	$\ldots$	-1	0	1	2	3	$\ldots$
2	$\ldots$	0	1	2	3	4	$\ldots$
$\ldots$		$\ldots$	$\ldots$	$\ldots$	$\ldots$	$\ldots$	

Vidíme, že všechny výsledky operace budou z množiny Z, jelikož sečtením dvou celých čísel získáváme opět číslo celé. Množina Z s operací sčítání tedy splňuje vlastnost (1). Splněna je rovněž vlastnost (2), jelikož operace sčítání je na množině celých čísel asociativní.

0 je neutrálním prvkem, platí tedy vlastnost (3).

Každý prvek množiny celých čísel má svůj inverzní prvek (platí vlastnosti (4)):

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

Vidíme, že na struktuře $(Z, +)$ jsou splněny vlastnosti (1) až (4).

Můžeme se opět podívat také na podmnožiny množiny celých čísel, které jsou uzavřené na výsledky operace sčítání:

- $P_1 = \{0\}$ je triviální podmnožina obsahující pouze neutrální prvek;
- $P_2 = Z$ je triviální podmnožina množiny celých čísel.

- existují i netriviální podmnožiny uzavřené na výsledky operace sčítání, ale jsou nekonečné:
  - $P_3 = \{\ldots -9, -6, -3, 0, 3, 6, 9, 12, \ldots\}$;
  - $P_4 = \{\ldots -2, 0, 2, 4, \ldots\}$;
  - atd.

Podmnožin množiny Z uzavřených na operaci sčítání je tedy nekonečně mnoho. •

Příklad 3 *Označme $(F(R), \circ)$ množinu všech funkcí (= zobrazení z R do R, viz předmět Základy matematiky) s operací skládání funkcí. Prozkoumejte vlastnosti této operace na množině všech funkcí.*

Operace skládání funkcí $\circ$ čteme jako „po“, což nám napovídá, jak získáme výsledky dané operace:

$$e^{x+3} \circ sinx = e^{sinx+3}$$
$$sinx \circ e^{x+3} = sin(e^{x+3})$$
$$e^{x+3} \circ e^{x+3} = e^{e^{x+3}+3}$$
$$x^5 \circ x^5 = x^{25}$$
$$\ldots$$

Můžeme vidět, že když zaměníme pořadí funkcí, se kterými provádíme operaci skládání, dostáváme různé výsledky. Skládání funkcí tedy není komutativní.

Stejně jako v předchozím příkladě, i tentokrát se jedná o nekonečnou množinu. Můžeme tedy opět naznačit tabulku výsledků operace skládání pouze pro část prvků dané množiny.

Tabulka 1.4: Tabulka operace $\circ$ na množině $F(R)$.

$\circ$	$\ldots$	e^{x+3}	$sinx$	x^5	$\ldots$
$\ldots$		$\ldots$	$\ldots$	$\ldots$	
e^{x+3}	$\ldots$	$e^{e^{x+3}+3}$	$e^{e^{sinx+3}}$	e^{x^5+3}	$\ldots$
$sinx$	$\ldots$	$sin(e^{x+3})$	$sin(sinx)$	$sin(x^5)$	$\ldots$
x^5	$\ldots$	$(e^{x+3})^5$	$(sinx)^5$	x^{25}	$\ldots$
$\ldots$		$\ldots$	$\ldots$	$\ldots$	

Neutrálním prvkem vzhledem ke skládání funkcí je funkce $f(x) = x$, kterou můžeme označit $id(x)$. Platí:

$$sinx \circ id(x) = sinx$$

$$id(x) \circ sinx = sinx$$
$$id(x) \circ id(x) = id(x)$$
$$atd.$$

Skládání funkcí, potažmo jakýchkoli zobrazení, je asociativní operace:

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

Jsou tedy splněny vlastnosti (2) a (3). Složením dvou reálných funkcí získáme opět reálnou funkci, takže vlastnost (1) platí také. Naopak vlastnost (4) platit nebude, protože aby platila, musela by ke každé reálné funkci existovat funkce inverzí. Stačí najít nějaký protipříklad, kterým je např. funkce $f(x) = x^2$. •

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

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

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

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

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

Důležité úsporné označení permutace

Pořád pokračujeme v příkladu 4: V dalším textu budeme permutace zadávat úspornějším způsobem, který napíše každé číslo jen jednou, nikoli dvakrát. V tomto úsporném označení budeme permutaci

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

(v tomto označení se jedná o uzavřený cyklus zobrazení: 1 se zobrazí na následující zapsané číslo, tj. 5, číslo 5 se zobrazí na 4, číslo 4 na 2 a poslední zapsané číslo v závorce se zobrazí

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

na první číslo 1, a tím se cyklus uzavře!!). Číslo 3 není v zápise uvedeno, protože se zobrazením f nemění. tj. $f(3) = 3$.

Podobně permutaci

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

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

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

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

Operace skládání permutací

Pořád pokračujeme v příkladu 4, teprve se dostáváme k operaci definované na množině permutací: Protože permutace je zvláštní případ zobrazení a zobrazení $M \to M$ lze skládat za sebou, můžeme mluvit o operaci „skládání zobrazení“, respektive „skládání permutací“.

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

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

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

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

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

nebo

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

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

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

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

Nejprve je potřeba říci, že u každé tabulky operace $*$ na konečné množině prvků je prvek x v levém sloupcovém záhlaví vybrán jako první a prvek y v horním řádkovém záhlaví jako druhý[4].

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

Tabulka 1.5: Tabulka operace $\circ$ na množině S_3.

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

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

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

$\circ$	id
id	id

,

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

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

,

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

,

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

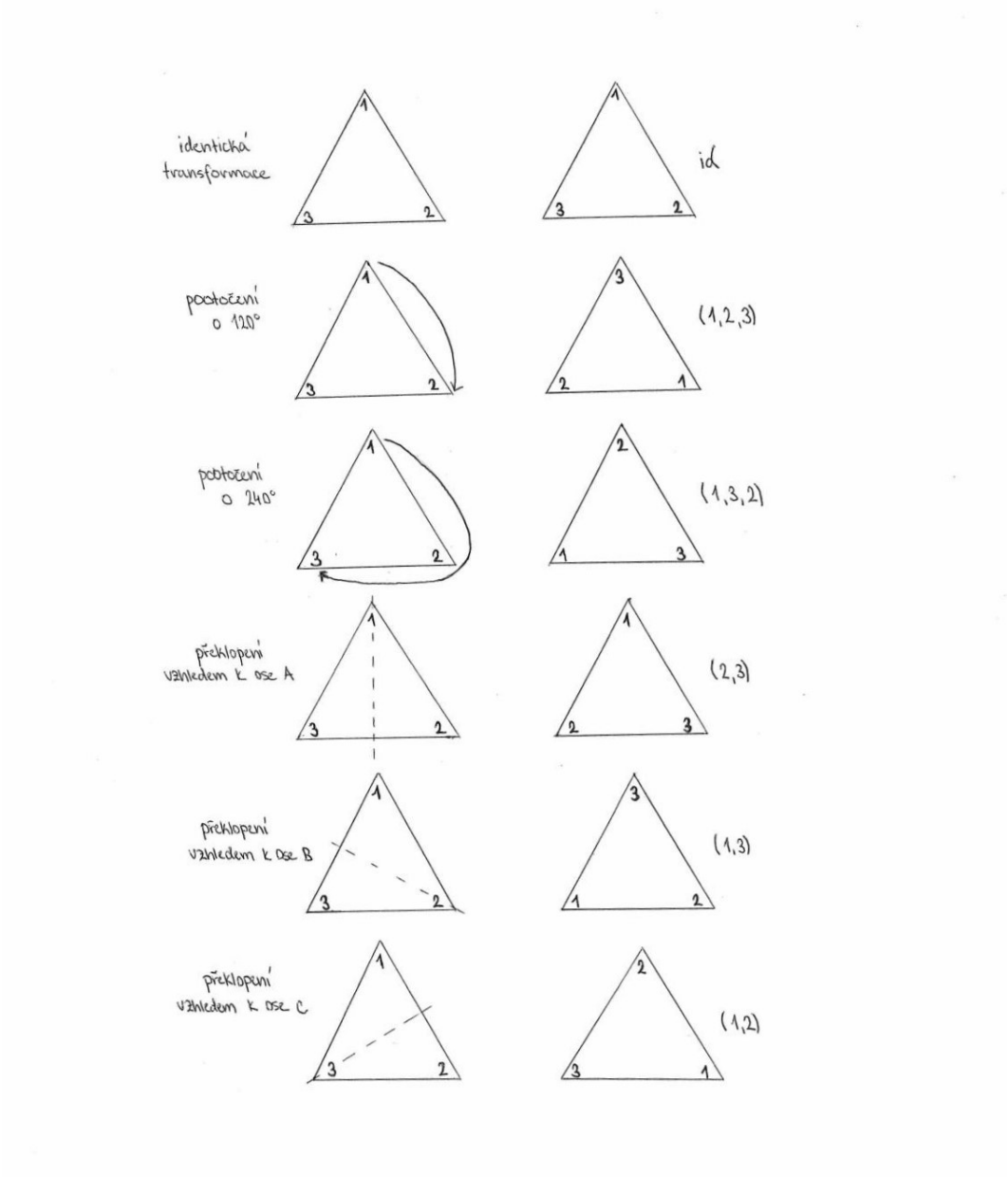
[4]Toto je klíčově důležitá domluva, řečená už výše. Pořadí hraje roli právě u tohoto příkladu, kdy se jedná o operaci nekomutativní, tj. na pořadí prvků do operace vstupujících záleží.

a jedna tříprvková podgrupa s tabulkou operace

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

.

K čemu je dobrá grupa permutací S_3? Má i svůj geometrický význam, tj. lze ji použít při popisu některých základních geometrických zobrazení, například bijektivních zobrazení trojúhelníku na sebe sama (tzv. symetrií trojúhelníku, odtud i původ písmene S v označení množiny), kterých je také šest, stejně jako prvků množiny S_3 – jedná se o tři otočení a tři osové souměrnosti. Každé z těchto geometrických proměn (= transformací) trojúhelníku lze přiřadit jednu permutaci jeho tří vrcholů:



A poslední věc na závěr příkladu 4: v grupě permutací $(S_3, \circ)$ lze řešit i rovnice, jako v jakékoli jiné grupě: Najděte neznámou permutaci z rovnice $(1,2) \circ x = (1,2,3)$.

Řešení této rovnice: $(S_3, \circ)$ je nekomutativní grupa. Provedeme krácení zleva pomocí inverzního prvku k permutaci $(1,2)$, kterým je opět prvek $(1,2)$.

$$(1,2) \circ x = (1,2,3) \qquad / \circ (1,2)(zleva)$$

$$(1,2) \circ (1,2) \circ x = (1,2) \circ (1,2,3)$$

$$x = (1,2) \circ (1,2,3)$$

$$x = (2,3)$$

Řešením dané rovnice je tedy permutace $(2,3)$. Je důležité, že při „násobení“ obou stran rovnice jsem překládali prvek $(1,2)$ zleva, a pak při řešení dostali složení $(1,2) \circ (1,2,3)$. Kdybychom nesprávně skládali prvky v jiném pořadí, a sice $(1,2,3) \circ (1,2)$, dostali bychom jiný výsledek, a sice $(1,3)$ (viz tabulka operace). •

Naše čtyři příklady v řeči pojmů ze cvičení 1

Množině M s operací $*$ se pak podle toho, kolik splňuje vlastností říká:

- Grupoid $(M, *)$ - operace $*$ splňuje na množině M vlastnost (1);
- Pologrupa $(M, *)$ - operace $*$ splňuje na množině M vlastnosti (1), (2);
- Monoid $(M, *)$ - operace $*$ splňuje na množině M vlastnost (1), (2), (3);
- Grupa $(M, *)$ - operace $*$ splňuje na množině M vlastnost (1), (2), (3), (4).

Pokud množina M s operací $*$ splňuje navíc vlastnost (5), pak do jejího označení přidáváme slovo komutativní. $(M, *)$ tedy může být komutativní grupoid/pologrupa/monoid/grupa.

Nyní můžeme přiřadit názvy algebraických struktur příkladům z první přednášky:

- Struktura $(H_6, +)$ z příkladu 1 splňuje vlastnosti (1), (2), (3), (4) a navíc je i komutativní, tedy je splněna vlastost (5). Dohromady je tedy $(H_6, +)$ komutativní grupa.
- Struktura $(Z, +)$ z příkladu 2 také splňuje všechny vlastnosti (1), (2), (3), (4) i (5). $(Z, +)$ je také komutativní grupa.
- Struktura $(F(R), \circ)$ z příkladu 3 splňuje pouze vlastnosti (1), (2), (3). Dohromady je tedy $(F(R), \circ)$ monoid.
- Struktura $(S_3, \circ)$ z příkladu 4 splňuje vlastnosti (1), (2), (3), (4), ovšem nikoliv vlastnost (5). $(S_3, \circ)$ je tedy grupa, která ale není komutativní. •

2 Týden 02

2.1 Cvičení 2: Určování vlastností různých operací

Úloha 2.1 *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* $M = \{-100, -99, -98, \ldots, -1, 0, 1, 2, \ldots, 99, 100\}$.

Úloha 2.2 *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).*

Úloha 2.3 a) *Uveďte definici vlastnosti (4) pro operaci* $\bigtriangledown$ *na množině* M *ve stručném matematickém zápisu.*

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

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

Úloha 2.4 *Dokažte, že množina všech podmnožin tříprvkové množiny s operací symetrického rozdílu* $\div$ *je grupa (viz Pinter 2010, str. 30, oddíl C).*

Úloha 2.5 *V množině* $M = \{1, 2\}$ *je operace* ∇ *tabulkou:*

∇	1	2
1	1	1
2	1	2

Určete typ algebraické struktury (M, ∇).

Úloha 2.6 *V množině* $M = \{a, b, c\}$ *je operace* $\triangle$ *tabulkou:*

$\triangle$	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

Určete typ algebraické struktury $(M, \triangle)$.

Úloha 2.7 *Určete typ algebraické struktury:* $(N - \{0\}, *)$, *kde* $x * y = x^y$.

Úloha 2.8 *Určete typ algebraické struktury:* $(R^+, \circ)$, *kde* $x \circ y = \sqrt{xy}$.

Výsledky některých cvičení najdete v závěru textu v oddílu 14.2.

2.2 Přednáška 2: Základní vlastnosti operace – věty

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?[5]

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[6]:

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

což je spor s tím, že oba neutrální prvky jsou navzájem různé[7]. □

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

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

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

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

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

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

[5] 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?

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

[7] 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.

Klíčová myšlenka: vynásobením[8] $a_1^{-1} \bigtriangledown a_2^{-1}$ pravděpodobně nic nezískáme. Prvky a_1^{-1}, a_2^{-1} vystupují ve vlastnosti (4), tj. měli bychom studovat něco jako rovnice ve vlastnosti (4). VYUŽIJEME TOHO, ŽE VE VLASTNOSTI (4) SE VYSKYTUJÍ DVĚ ROVNOSTI, A JEDNU APLIKUJEME NA PRVEK a ZLEVA, DRUHOU ZPRAVA:

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

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

Věta 3 *(můžeme „krátit“[9] v rovnostech, ve kterých se vyskytují prvky grupy G a operace $\bigtriangledown$?) V každé grupě $(G, \bigtriangledown)$ platí zákony o krácení (7), tj.*

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

Důkaz: Provedeme například pro první z implikací: Vztah

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

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

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

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

$$b = c.$$

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

Příklad 5 *Určete algebraické vlastnosti struktury $(Z_6, \cdot)$.*

Začneme tím, že si sestavíme tabulku výsledků operace:

Když máme nyní sestavenou tabulku výsledků operace $\cdot$ na množině Z_6, můžeme s její pomocí určit vlastnosti dané struktury:
V tabulce jsou pouze prvky množiny Z_6, je tedy splněna vlastnost (1).

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

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

Tabulka 2.6: Tabulka operace $\cdot$ na množině Z_6.

$\cdot$	[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]

Z tabulky sice nepoznáme, zda je operace $\cdot$ asociativní, ovšem obecně platí, že tato operace asociativní je, takže vlastnost (2) platí také. Neutrálním prvkem je [1], je tedy splněna i vlastnost (3).
Vlastnost (4) však splněna není, jelikož prvky [0], [2], [3] a [4] nemají inverzní prvek.
Vlastnost (5) platí, což vidíme z tabulky, jelikož je souměrná podle hlavní diagonály.

Dohromady je tedy $(Z_6, \cdot)$ komutativní monoid.

Můžeme si všimnout, že v této struktuře nemůžeme provádět krácení podle věty 3. Např. z tabulky vidíme, že $[2] \cdot [2] = [2] \cdot [5]$, ovšem $[2] \neq [5]$. Uvedená struktura totiž nesplňuje vlastnost (4), není tedy grupa.•

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Nazývat tento počet prvků grupy řádem grupy je poněkud bizarní, ale má jakési opodstatnění u cyklických grup,, kde souvisí s pojmem řádu prvku (viz přednáška 5 nebo 6).

Rozšíření vlastnosti (2) na k prvků

Ve větě 5 se vyskytuje „součin“ čtyř prvků za sebou – přesně pracující matematik by měl prozkoumat, zda se nedopouští při důkazu něčeho, co není definováno. Pokud definujeme součin čtyř prvků vzhledem k operaci $\bigtriangledown$jako součin prvního prvku se součinem následujících tří prvků, tj.

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

postupným užitím vlastnosti (2) pro tři prvky dostaneme

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

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

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

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

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

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

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

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

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

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

3 Týden 03

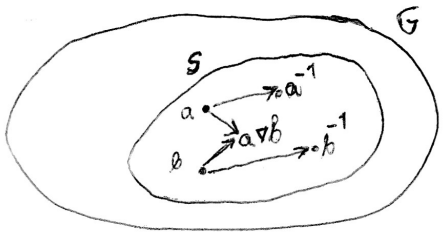
3.1 Přednáška 3: Podgrupa grupy – příklady i věty

Příklad 6 *Na strukturách $(H_7, +)$ a $(H_7, \cdot)$ ilustrujme pojmy zavedené na konci druhé přednášky, tj. n-tá mocnina, odmocnina a záporná mocnina v grupě.*

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

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

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



Kupodivu se ukazuje, že dané dvě vlastnosti (1), (4) neprázdné[10] 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. A dále vlastnost (3), existenci neutrálního prvku, dokážeme z vlastnosti (4):

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

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

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

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

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

Generátory podgrupy

Uvažujme množinu $S = \{a, b, c\}$, která je podmnožinou grupy $(G, \bigtriangledown)$. Na to, abychom našli nejmenší možnou podgrupu, která obsahuje prvky a, b, c, musíme vyrobit všechny možné součiny těchto tří prvků a jejich inverzí[11], a nejen to: musíme brát všechny možné konečné sekvence prvků spojených operací $\bigtriangledown$, ve kterých se vyskytují (i opakovaně) prvky a, b, c a jejich inverze.

Typickými takto vytvářenými prvky jsou například

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

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

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

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

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

(tedy platí i (4)). Dokázali jsme celkem, že množina prvků tohoto typu tvoří podgrupu grupy $(G, \bigtriangledown)$. Formulujme nyní tento fakt jako větu sedmou:

Věta 7 *Pro neprázdnou podmnožinu M grupy $(G, \bigtriangledown)$ lze nejmenší (co do počtu prvků či mohutnosti) možnou podgrupu $< M >$ grupy $(G, \bigtriangledown)$, která obsahuje množinu M, sestrojit takto přidáváním prvků:*

krok 0) *K přidávaným prvkům dáme samotné prvky množiny M;*

krok 1) *Pro a, b už přidané dříve přidáme prvek $a \bigtriangledown b$ (zaručujeme tím vlastnost (1), uzavřenost na výsledky operace);*

krok 2) *Pro a, b už přidané dříve přidáme prvky a^1, a^2, $a^3 \ldots$, b^1, b^2, $b^3 \ldots$, (zaručujeme tím vlastnost (1), uzavřenost na výsledky operace);*

krok 3) *pro c už přidané dříve přidáme prvky c^{-1}, c^{-2}, $c^{-3} \ldots$ (zaručujeme tím vlastnost (4), uzavřenost na inverze, a taky přidáním všech další záporných mocnin (definovaných řádně jako kladnou mocninu inverzního prvku) uzavřenost na práci s inverzním prvkem;*

krok 4) *Kroky 1, 2, 3 opakujeme tak dlouho, až už nelze nic přidat.*

Důkaz: plyne z předchozích úvah i ze tvrzení věty, které je konstrukčním důkazem pro konečné množiny. Pro nekonečné množiny bychom museli důkaz doplnit indukcí. □

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

Definice 15 *Podgrupu generovanou podmnožinou M vzniklou přidáváním prvků popsaným ve větě 7 označujeme (označení 02) $< M >$.*

Definice 16 *Pokud podgrupa $< M >$ 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 7 *Pro grupu $(H_{10}, +)$ a množinu $M = \{2\}$ máme $< 2 >= \ldots$;*

pro množinu $T = \{2; 3\}$ máme $< 2; 3 >= \ldots$

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

Příklad 8 *Ad příklad 4: Ohledně generátorů grupy S_3 lze říci, že $(S_3, \circ)$ je generována dvěma svými prvky, a sice $(1,3)$ a $(1,2)$, protože všechny další čtyři prvky grupy lze vyjádřit pomocí operace $\circ$ a prvků $(1,3)$, $(1,2)$:*

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

Podle označení množiny generátorů lze psát

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

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

Pokračujme ještě v příkladu 8 a v rámci tohoto příkladu si připomeneme jednou drobnou věc: Navzdory patáliím nekomutativních operací existuje i v tabulkách nekomutativních operací jedna jistota a elegantní věc: Operace na cyklické podgrupě (= podgrupě generované jediným prvkem) H grupy G je komutativní, třebaže na celé grupě G tato operace komutativní být nemusí.

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

$\{id, (1,2,3), (1,3,2)\}$ je symetrická, tj. operace je na ní komutativní. Důkaz faktu, že operace na každé cyklické grupě je komutativní, je lehký – pokuste se o něj v rámci cvičení.

A na závěr jeden příklad na větu 12, která je uvedena v náslených dodatcích, ale její použití je důležité a studenti jej musí znát: Je to skutečnost o rozdílu mezi grupou permutací $(S_n, \circ)$, která má $n!$ prvků, a její podgrupou $(D_n, \circ)$, tzv. dihedrální podgrupou, která má $2n$ prvků – vysvětlíme pro $n = 4$: Grupa všech bijekcí (permutací) $(S_4, \circ)$na čtyřprvkové množině má 24 prvků, její dihedrální podgrupa $(D_4, \circ)$ shodných zobrazení čtverce na sebe sama má 8 prvků. Podle Lagrangeovy věty počet prvků podgrupy (8 prvků) je dělitelem počtu prvků celé konečné grupy bijekcí čtyřprvkové množiny na sebe sama (24 prvků).

Podrobněji: (ad Pinter 2010, str. 77, sada F) Dihedrální podgrupa $(D_4, \circ)$ grupy $(S_4, \circ)$:

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 čtverce, která vznikne ze základní polohy uplatněním jedné dílčí transformace, tj. množina těchto osmi transformací (= přeměn ve smyslu osového překlopení či ve smyslu pootočení čtverce) tvoří grupu.

Jak nyní dojdeme k permutaci přirozených čísel? Například tak, že do rohů základní polohy čtverce umístíme čísla $1, 2, 3, 4$. A po provedení dané transformace zapíšeme permutaci těchto čtyř čísel vzhledem k základní poloze. Pak identické transformaci (při které se neděje nic) odpovídá permutace $R_0 = id$, pootočení o 90° odpovídá permutace $R_1 = (1,2,3,4)$ (v tom smyslu, že číslo 1 se pootočením dostalo na pozici čísla 2, číslo 2 se na pozici čísla 3, číslo 3 na 4 a číslo 4 na pozici 1). Podobně pootočení o 180° odpovídá permutace $R_2 = (1,3) \circ (2,4)$[12] a pootočení o 270° permutace $R_3 = (1,4,3,2)$[13].

(podrobněji viz obrázek 3.1).

Podobně dostaneme permutace odpovídající přeměně čísel ve vrcholech čtverce při osové souměrnosti vzhledem ke čtyřem hlavním osám souměrnosti, viz obrázek 3.2.

Skládáním $R_1 \circ R_5$ například dostaneme

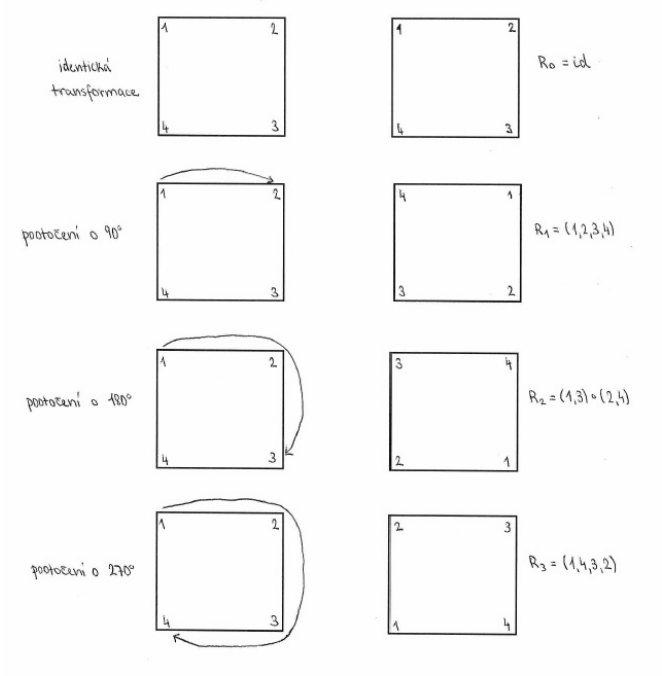
$$R_1 \circ R_5 = (1,2,3,4) \circ (2,4) = (1,2) \circ (3,4) = R_6,$$

atd. Vyplněním operace pro každou dvojici prvků v obou pořadích (operace je opět nekomutativní, protože např. $R_5 \circ R_1 = R_7$) dostaneme tabulku grupy $(D_4, \circ)$ symetrií čtverce, která odpovídá podgrupě grupy permutací s osmi prvky (viz tabulka 3.3). Všech

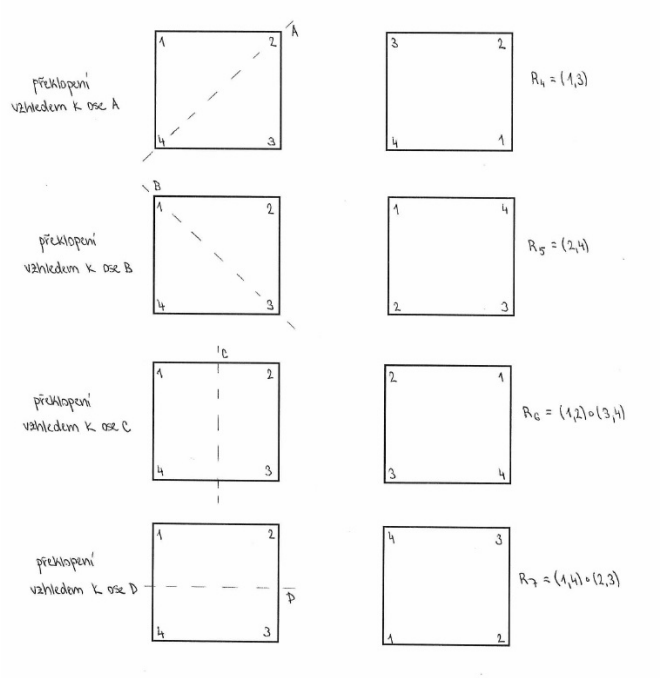
[12] Pozor, tuto permutaci nelze lépe označit než spojením dvou disjunktních cyklů délky 2, protože dochází ke dvěma nezávislým prohozením během jedné permutace.

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

permutací čtyřprvkové množiny je 24; tedy naše osmiprvková množina je podgrupou grupy S_4.



Obrázek 3.1: Permutace odpovídající pootočení čtverce.



Obrázek 3.2: Permutace odpovídající osové symetrii čtverce.

∘	id	(1,2,3,4)	(1,3) ∘ (2,4)	(1,4,3,2)	(1,3)	(2,4)	(1,2) ∘ (3,4)	(1,4) ∘ (2,3)
id	id	(1,2,3,4)	(1,3) ∘ (2,4)	(1,4,3,2)	(1,3)	(2,4)	(1,2) ∘ (3,4)	(1,4) ∘ (2,3)
(1,2,3,4)	(1,2,3,4)	(1,3) ∘ (2,4)	(1,4,3,2)	id	(1,4) ∘ (2,3)	(1,2) ∘ (3,4)	(1,3)	(2,4)
(1,3) ∘ (2,4)	(1,3) ∘ (2,4)	(1,4,3,2)	id	(1,2,3,4)	(2,4)	(1,3)	(1,4) ∘ (2,3)	(1,2) ∘ (3,4)
(1,4,3,2)	(1,4,3,2)	id	(1,2,3,4)	(1,3) ∘ (2,4)	(1,2) ∘ (3,4)	(1,4) ∘ (2,3)	(2,4)	(1,3)
(1,3)	(1,3)	(1,2) ∘ (3,4)	(2,4)	(1,4) ∘ (2,3)	id	(1,3) ∘ (2,4)	(1,2,3,4)	(1,4,3,2)
(2,4)	(2,4)	(1,4) ∘ (2,3)	(1,3)	(1,2) ∘ (3,4)	(1,3) ∘ (2,4)	id	(1,4,3,2)	(1,2,3,4)
(1,2) ∘ (3,4)	(1,2) ∘ (3,4)	(2,4)	(1,4) ∘ (2,3)	(1,3)	(1,4,3,2)	(1,2,3,4)	id	(1,3) ∘ (2,4)
(1,4) ∘ (2,3)	(1,4) ∘ (2,3)	(1,3)	(1,2) ∘ (3,4)	(2,4)	(1,2,3,4)	(1,4,3,2)	(1,3) ∘ (2,4)	id

Obrázek 3.3: Tabulka operace ∘ na množině D_4 symetrií čtverce

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

ještě ani nebyly experimentálně zjištěny! Proto i studium nekomutativních grup má svoje místo v algebře.

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

Začneme tedy vypsáním inverzních prvků. K tomu nám pomůže jednak tabulka, ale také uvědomění si geometrických významů daných permutací:
$id \leftrightarrow id$
$(1,2,3,4) \leftrightarrow (1,4,3,2)$
$(1,3)\circ(2,4) \leftrightarrow (1,3)\circ(2,4)$
$(1,3) \leftrightarrow (1,3)$
$(2,4) \leftrightarrow (2,4)$
$(1,2)\circ(3,4) \leftrightarrow (1,2)\circ(3,4)$
$(1,4)\circ(2,3) \leftrightarrow (1,4)\circ(2,3)$

Nyní k podgrupám grupy D_4:

Dvě z nich jsou triviální $P_1 = \{id\}$ a $P_2 = D_4$.

Zkusme se teď podívat na dvouprvkové podgrupy. K tomu můžeme využít geometrického významu - všechny osové souměrnosti s identitou tvoří dvouprvkovou podgrupu, jelikož osová souměrnost je inverzní prvek sama k sobě: $P_3 = \{id,(1,3)\}, P_4 = \{id,(2,4)\}, P_5 = \{id,(1,2)\circ(3,4)\}, P_6 = \{id,(1,4)\circ(2,3)\}$. Otočení o 180° je také samo sobě inverzí, takže jeho spojením s identitou získáme podgrupu $P_7 = \{id,(1,3)\circ(2,4)\}$.

Můžeme přejít k čtyřprvkovým podgrupám. První je množina čtyř pootočení $P_8 = \{id,(1,2,3,4),(1,3)\circ(2,4),(1,4,3,2)\}$, další jsou $P_9 = \{id,(1,3)\circ(2,4),(1,3),(2,4)\}$ a $P_{10} = \{id,(1,3)\circ(2,4),(1,2)\circ(3,4),(1,4)\circ(2,3)\}$. Tím jsme našli všechny podgrupy grupy D_4.

Vidíme, že Lagrangeova věta 12 platí i pro podgrupy grupy $(D_4,\circ)$: počet prvků libovolné její podgrupy je děliteme čísla 8.

3.2 Dodatky, na které nebude čas 01

Z těchto dodatků by bylo možné sestavit jednu zajímavou obecnou přednášku, která ve svém vyvrcholení dospívá v tzv Lagrangeově větě – 12. Na všechno zajímavé zkoumání není čas, z tohoto dodatku si prosím pamatujte jen znění Lagrangeovy věty bez důkazu a žlutá označení 04, 05, 06.[14]

Začneme zopakováním znalostí o pojmu ekvivalence (relace reflexivní, symetrická a tranzitivní) a pojmu rozkladu určeného 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 9) nám bude stačit si uvědomit, že pokud dvě třídy rozkladu M_i, M_j mají neprázdný průnik, pak se musí rovnat, čili $M_i = M_j$ a jedná se o tutéž třídu. Lze tedy rozklad množiny M na podmnožiny M_i definovat i následovně:
  - $\forall i \in \{1, 2, \ldots, k\} : \quad M_i \neq \emptyset$;
  - $a \in M_i \cup M_j \Rightarrow M_i = M_j$;
  - každý prvek $a \in M$ leží v jedné třídě rozkladu.
- Označení 04: Znak $\sim$ bude značit relaci ekvivalence určenou daným rozkladem, tj. $a \sim b$ právě tehdy, když $a, b \in M_i$ pro nějaké i.
- Označení 05: Označme dále $[a]$ tu třídu rozkladu, která obsahuje prvek a, tedy podmínku z označení 07 budeme psát ve tvaru

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

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

[14] V jednom důkazu je též použit pojem homomorfismu a izomorfismu, který vysvětlíme v dalších čtrnácti dnech – ovšem protože důkazy v dodatku přeskakujeme, není potřeba přímá chronologie všech pojmů, běžný student, který nečte nepovinné dodatky, to ani nezjistí.

Definice 17 *$\forall a$ z grupy $(G, \bigtriangledown)$ a její podgrupu $(H, \bigtriangledown)$ lze definovat:*

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

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

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

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

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

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

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

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

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

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

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

Zabývejme se dále pouze pravými třídami prvků – všechny následující věty se budou týkat pravých tříd prvku vzhledem k podgrupě H, ikdyž bychom je mohli analogicky (či duálně?) formulovat i pro levé třídy prvku. Věta 8 je pouze pomocnou větou, která bude potřeba v důkazu věty 9 (věty 8 až 11 jsou řečeny za předpokladu označení z definice 17, tj. $(H, \bigtriangledown)$ je podgrupa grupy $(G, \bigtriangledown)$).

Věta 8 *$a \in H \bigtriangledown b$ právě tehdy, když $H \bigtriangledown a = H \bigtriangledown b$.*

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

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

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

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

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

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

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

a po dosazení za b dostaneme

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

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

Věta 8 netvrdí nic světoborného, v podstatě jen to, že pokud prvky a, b jsou spojeny v operaci $\bigtriangledown$ „přes podgrupu H“, tak jejich pravé třídy jsou totožné. Následující věta 9 je prvním významným výsledkem této kapitoly.

Věta 9 *Pravé*[15] *třídy* $H \bigtriangledown a$ *pro všechny možné prvky* a *grupy* $(G, \bigtriangledown)$ *tvoří rozklad množiny* G.

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

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

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

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

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

a to podle věty 8 (tady právě ji potřebujeme!!) znamená, že $H \bigtriangledown a = H \bigtriangledown b$.

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

Než se dostaneme k větě 11 vedoucí k Lagrangeově větě, ještě jedno označení a jeden výsledek, věta 10: Označení 06. Označme množinu tříd $G/_H$ rozkladu grupy G podle její komutativní podgrupy H ... vzhledem k operaci $\underline{\bigtriangledown}$ definované pomocí vztahu

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

dostáváme tzv. rozkladovou grupu nebo též při doslovném překladu faktorgrupu[16].

Věta 10 *Struktura* $G/_H$ *vytvořená z tříd podle nějaké své komutativní podgrupy* H *s operací* $\underline{\bigtriangledown}$ *je grupa.*

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

Věta 11 *Existuje bijekce mezi podgrupou* $(H, \bigtriangledown)$ *a každou pravou třídou* $H \bigtriangledown a$.

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

[16] Anglicky FACTOR znamená, „rozložit“.

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

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

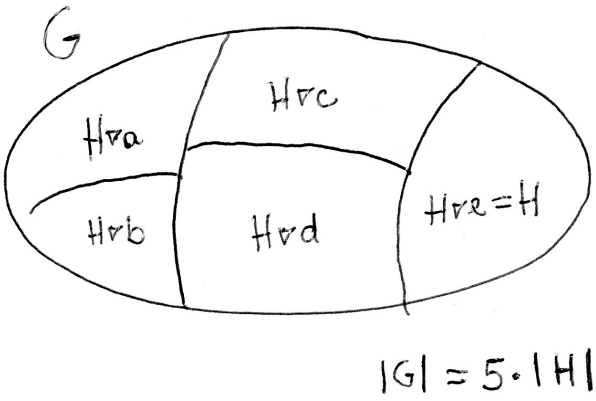
Takto definované f je injekce:

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

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

Důsledkem věty 11 pro konečné grupy G je: Všechny pravé třídy $H \bigtriangledown a$ mají tentýž počet prvků!!!!!

Čtenář si určitě říká, kdy už přijde ta slavná Lagrangeova věta z názvu této kapitoly – už se blíží, je to věta následující!!! Ale ty nejdůležitější věty, věta 9 a věta 11, už byly řečeny. Ta následující je pouze jejich důsledkem, tj. pan Lagrange je autorem souvislostí všech těchto vět. Podívejme se ovšem předtím na příklad ilustrující celou situaci:



Obrázek 3.4: Rozklad konečné grupy G na pět pravých tříd vzhledem k podgrupě H. Všechny třídy rozkladu mají stejný počet prvků.

(příkad z dodatku 3-3) Uvažujme situaci na obrázku 3.4: všech pravých tříd vzhledem k podgrupě H konečné grupy G je pět – jedna z nich je $H \bigtriangledown e = H$ a další čtyři jsou $H \bigtriangledown a$, $H \bigtriangledown b$, $H \bigtriangledown c$, $H \bigtriangledown d$. Existuje bijekce (podle věty 11) 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 12 Lagrangeova věta pro konečné grupy. *Počet prvků libovolné podgrupy H je dělitelem počtu prvků konečné grupy G*

(připomeneme-li si definici řádu grupy, tak: řád podgrupy H je dělitelem řádu grupy G).

Důkaz Lagrangeovy věty je dalším důsledkem věty 11: pokud všechny pravé třídy mají stejný počet prvků, tak počet všech prvků je pouze nějakým násobkem počtu $|H|$.

(příklad dodatku 3-4) 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 dodatku 3-5) Pokud $|G|$ je prvočíslo, tak grupa G má pouze nevlastní podgrupy (sebe samotnou a jednoprvkovou triviální podgrupu).

Věta 13 *Pokud $|G| = p$ je prvočíslo, tak grupa $(G, \bigtriangledown)$ je cyklická grupa a jakékoli $a \in G$ různé od neutrálního prvku e je jejím generátorem.*

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

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

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

Věta 13 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 14 *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 18 *Protože přirozené číslo, které udává řád podgrupy $|H|$, je dělitelem řádu konečné grupy $|G|$ (věta 12 Lagrangeova), lze provést tuto operaci dělení přirozeným číslem a označit index podgrupy H v grupě G jako*

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

3.3 Cvičení 03: Vlastnosti grup, podgrupy a generátory grupy

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

$*$	e	a	b	c
e				
a				
b				
c				

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

$*$	e	a	b	c
e				
a				
b				
c				

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

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

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

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

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

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

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

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

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

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

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

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

Například E.7 – modifikace[17]: V grupě $H_2 \times H_4$ je operace sčítání po složkách zadaná tabulkou – určete, jakou podgrupu generuje prvek $[1; 1]$:

[17] 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.

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

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

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

Úloha 3.8 *Pro následující grupy nalezněte podgrupy:*

a) $(Z, +)$

b) $(R - \{0\}, \cdot)$

c) $(F(R), +)$

Úloha 3.9 *Určete tabulku pro grupu všech symetrií rovnostranného trojúhelníka s operací skládání* $(D_3, \circ)$.

Úloha 3.10 *Vypište všechny cyklické podgrupy grupy* $(H_{10}, +)$ *skládání otáčení hodinové ručičky o násobky desetiny plného úhlu.*

Úloha 3.11 *Vypište všechny cyklické podgrupy grupy* $(H_{12}, +)$ *skládání otáčení hodinové ručičky o násobky dvanáctiny plného úhlu.*

Výsledky některých cvičení najdete v závěru textu v oddílu 14.3.

4 Týden 04

4.1 Přednáška 4: Izomorfismus a homomorfismus – příklady

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[18]. I když se tento český překlad neujal, vystihuje snahu moderní algebry všímat si shodných či podobných vlastností různých objektů.

V této kapitolce se budeme zejména zabývat „stejností“ či „podobností“ algebraických struktur vzhledem k pojmu binární operace – protože operace je něco dynamického, kdy dvěma prvkům podle jistého předpisu přiřazujeme třetí prvek, tedy stejnost (či podobnost), která nás bude zajímat, je dána tabulkou výsledků operace na dané množině. Jestliže najdeme mezi dvěma algebraickými strukturami zobrazení, které je homomorfismus, bude to znamenat podobnost daných dvou algebraických struktur, jestliže izomorfismus, bude to znamenat totožnost daných dvou struktur, až na přeznačení (bijekci) prvků jedné struktury na prvky druhé struktury.

Definice 19 *Izomorfismus grupy $(G_1, \bigtriangledown)$ na grupu $(G_2, *)$ je bijekce $f : G_1 \to G_2$, která splňuje vlastnost zachování výsledků operace (ZVO)*

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

homomorfismus $f : G \to H$ je takové zobrazení mezi algebrickými strukturami $(G, \bigtriangledown)$ a $(H, *)$, které zachovává výsledky operace (ZVO) podobně jako izomorfismus, ale na rozdíl od izomorfismu nemusí být bijektivní.

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

Příklad 9 *Zobrazení grupy $(Z, +)$ na grupu zbytkových tříd $(Z_6, +)$ definované vztahem „$f(z) =$ zbytek po dělení čísla z číslem 6“ je surjektivní homomorfismus grup.*

Grupa $(Z, +)$:

$+$	$\dots$	-2	-1	0	$\dots$
$\dots$		$\dots$	$\dots$	$\dots$	
-2	$\dots$	-4	-3	-2	$\dots$
-1	$\dots$	-3	-2	-1	$\dots$
0	$\dots$	-2	-1	0	$\dots$
$\dots$		$\dots$	$\dots$	$\dots$	

Grupa $(Z_6, +)$:

$+$	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

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

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).

Obecně platí: Celá čísla $6k+m$ a $6l+n$ se mezi sebou sečtou na $6(k+l)+m+n = 6p+r$. Tato celá čísla se zobrazí na jejich zbytky: $6k+m \to m$, $6l+n \to m$ a $6p+r \to r$. Musí platit, že součet zbytků m a n je roven r, což skutečně platí (součet zbytků po dělení šesti je zase zbytek po dělení šesti), tedy je splněna podmínka zachování výsledků operace. □

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 10 *Podobně jiný příklad: Zobrazení struktury $(Z, \cdot)$ (komutativní monoid) na strukturu $(Z_5, \cdot)$ (komutativní monoid) je sice zobrazením mezi dvěma strukturami stejného typu – je to sice surjektivní homomorfismus, ale nejedná se o izomorfismus, protože vzhledem k násobení jen jeden prvek nemá inverzi, a sice $[0]$, kdežto na struktuře $(Z, \cdot)$ nemají inverzi vzhledem k násobení také prvky, které e zobrazí na jiný prvek než $[0]$.*

Příklad 11 *Hopomorfismus, který je injekcí, jestliže definujeme zobrazení $\varphi : Z \to Q$ vztahem $\varphi(z) = z$. Trochu jiné pojetí, viz video.*

Příklad 12 *Zobrazení množiny $(H_6, +)$ na množinu $(Z_6, +)$ je izomorfismus.*

Příklad 13 *$(R, +)$ 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.⋆

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 (ZVO).

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 následující dvojice struktur není izomorfní, jestliže

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

Příklad 14 *Zjistěte, které ze čtyřprvkových struktur a)* $2^{\{a,b\}}$ *s operací symetrického rozdílu* $\div$ *(stejná operace jako v úloze 2.4); b)* $(V, \cdot)$*, kde* $V = \{1, -1, i, -i\}$ *a* $\cdot$ *je operace násobení komplexních čísel; c) struktura* $(H_4, +)$*; d) struktura* $(H_2 \times H_2, +)$ *jsou navzájem izomorfní a které ne, své zjištění zdůvodněte.*

Nejprve si opět sestavíme tabulky operací na daných množinách.

Grupa $(2^{\{a,b\}}, \div)$:

$\div$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\emptyset$	$\emptyset$	$\{a\}$	$\{b\}$	$\{a,b\}$
$\{a\}$	$\{a\}$	$\emptyset$	$\{a,b\}$	$\{b\}$
$\{b\}$	$\{b\}$	$\{a,b\}$	$\emptyset$	$\{a\}$
$\{a,b\}$	$\{a,b\}$	$\{b\}$	$\{a\}$	$\emptyset$

Grupa $(V, \cdot)$:

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	1	-1
$-i$	$-i$	i	1	-1

Při pohledu na tabulky není na první pohled vidět, zda se jedná o bijekci zachovávající výsledky operace. Proto se zvlášť podíváme na vlastnosti obou grup.
Zkusme se podívat na inverze. Pro grupu $(2^{\{a,b\}}, \div)$ platí:

$$\emptyset \leftrightarrow \emptyset$$

$$\{a\} \leftrightarrow \{a\}$$
$$\{b\} \leftrightarrow \{b\}$$
$$\{a,b\} \leftrightarrow \{a,b\}$$

Pro grupu $(V,\cdot)$ platí:

$$1 \leftrightarrow 1$$
$$-1 \leftrightarrow -1$$
$$i \leftrightarrow -i$$

Aby platila vlastnost zachování výsledků operace, musely by se dvojice inverzních prvků zobrazit opět na dvojice inverzních prvků, což v tomto případě neplatí. Grupy $(2^{\{a,b\}}, \div)$ a $(V,\cdot)$ tedy nejsou izomorfní. •

Grupa $(H_4,+)$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

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

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

Ani v tomto příkladě nejsme na základě tabulek schopni na první pohled říci, zda jsou dané struktury izomorfní. Zkusme tedy zjistit, zda izomorfismus existuje, pomocí inverzních prvků:

$(H_4,+)$: $0 \leftrightarrow 0$, $1 \leftrightarrow 3$, $2 \leftrightarrow 2$
$(V,\cdot)$: $1 \leftrightarrow 1$, $-1 \leftrightarrow -1$, $i \leftrightarrow -i$
$(H_2 \times H_2, +)$: $[0;0] \leftrightarrow [0;0]$, $[0;1] \leftrightarrow [0;1]$, $[1;0] \leftrightarrow [1;0]$, $[1;1] \leftrightarrow [1;1]$

Můžeme vidět, že struktura $(H_2 \times H_2, +)$ není izomorfní ani s jednou ze zbývajících dvou, jelikož izomorfismus musí zachovávat inverze.
$(H_4,+)$ i $(V,\cdot)$ obsahují dva prvky, které jsou inverzní k sobě samému. Struktura inverzí je u obou struktur stejná.
Na základě inverzí by tedy zobrazení mohlo vypadat takto: $0 \to 1$, $1 \to i$, $2 \to -1$, $3 \to -i$. Vypišme si nyní tabulku $(V,\cdot)$ s přehozenými prvky. Dostaneme:

$\cdot$	1	i	-1	$-i$
1	1	i	-1	$-i$
i	i	-1	$-i$	1
-1	-1	$-i$	1	i
$-i$	$-i$	1	i	-1

Tabulky jsou nyní zcela stejné až na přeznačení prvků. Grupy $(H_4, +)$ a $(V, \cdot)$ jsou tedy izomorfní.

Příklad 15 *a) Zjistěte, zda existuje izomorfismus mezi následujícími třemi strukturami:* $(Z_6, +)$, $(Z_7^*, \cdot)$, $(Z_2 \times Z_3)$. *Využijte tabulky jednotlivých operací:*

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

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

.

b) Definujte přesně izomorfismus $(Z_7^*, \cdot)$ na $(Z_6, +)$, který zachovává výsledky operace.

Příklad 16 *a) 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]

.

b) Všechny následující tři grupy jsou osmiprvkové. Zjistěte, zda některé z těchto grup jsou izomorfní, popřípadě vysvětlete, proč izomorfní nejsou:

Grupa $(Z_8, \oplus)$:

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

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

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

.

Grupa $(D_4, \circ)$*:*

$\circ$	id	(1,2,3,4)	(1,3) ∘ (2,4)	(1,4,3,2)	(1,3)	(2,4)	(1,2) ∘ (3,4)	(1,4) ∘ (2,3)
id	id	(1,2,3,4)	(1,3) ∘ (2,4)	(1,4,3,2)	(1,3)	(2,4)	(1,2) ∘ (3,4)	(1,4) ∘ (2,3)
(1,2,3,4)	(1,2,3,4)	(1,3) ∘ (2,4)	(1,4,3,2)	id	(1,4) ∘ (2,3)	(1,2) ∘ (3,4)	(1,3)	(2,4)
(1,3) ∘ (2,4)	(1,3) ∘ (2,4)	(1,4,3,2)	id	(1,2,3,4)	(2,4)	(1,3)	(1,4) ∘ (2,3)	(1,2) ∘ (3,4)
(1,4,3,2)	(1,4,3,2)	id	(1,2,3,4)	(1,3) ∘ (2,4)	(1,2) ∘ (3,4)	(1,4) ∘ (2,3)	(2,4)	(1,3)
(1,3)	(1,3)	(1,2) ∘ (3,4)	(2,4)	(1,4) ∘ (2,3)	id	(1,3) ∘ (2,4)	(1,2,3,4)	(1,4,3,2)
(2,4)	(2,4)	(1,4) ∘ (2,3)	(1,3)	(1,2) ∘ (3,4)	(1,3) ∘ (2,4)	id	(1,4,3,2)	(1,2,3,4)
(1,2) ∘ (3,4)	(1,2) ∘ (3,4)	(2,4)	(1,4) ∘ (2,3)	(1,3)	(1,4,3,2)	(1,2,3,4)	id	(1,3) ∘ (2,4)
(1,4) ∘ (2,3)	(1,4) ∘ (2,3)	(1,3)	(1,2) ∘ (3,4)	(2,4)	(1,2,3,4)	(1,4,3,2)	(1,3) ∘ (2,4)	id

4.2 Cvičení 04: Nekomutativní grupy

Úloha 4.1 *Jsou dány permutace*

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Úloha 4.3 *Dva úkoly pro grupu permutací* $(S_3, \circ)$ *(použijte prosím označení prvků a tabulku operace* $\circ$ *v příkladu 4): a) dokažte, že* $(S_3, \circ)$ *není cyklická grupa;*
b) najděte dvouprvkovou podmnožinu grupy, která generuje celou grupu $(S_3, \circ)$*.*

Úloha 4.4 *Pokud bude čas, je možné se zabývat některými dalšími vlastnostmi permutací (ad Pinter 2010, kapitola 8): Každou permutaci lze rozložit na součin cyklů, každý cyklus lze rozložit na součin transpozic. Sudá a lichá permutace podle počtu transpozic. Ale to spíše až do předmětu Algebra 2 (lineární algebra).*

Výsledky některých cvičení najdete v závěru textu v oddílu 14.4.

5 Týden 05

5.1 Přednáška 05: izomorfismus – věty

Věta 15 *Může v grupě $(G, \star)$ nastat situace, že v tabulce její operace se dvakrát opakuje stejný prvek na jednom řádku?*

$\star$	$\ldots$	x_1	$\ldots$	x_2	$\ldots$
$\ldots$		$\ldots$		$\ldots$	
a	$\ldots$	y	$\ldots$	y	$\ldots$
$\ldots$		$\ldots$		$\ldots$	

Zdůvodněte, proč ano - proč ne.

Věta 16 *(Cayley) Každá grupa $(G, \bigtriangledown)$ je izomorfní nějaké grupě permutací.*

Důkaz: Lze najít v knize Pinter. Namísto důkazu si uvedeme tři příklady, a třetí z nich je konstrukční a obsahuje hlavní myšlenku důkazu pro konečné grupy. Pinter ovšem dokazuje i pro nekonečné grupy. □

Příklad 17 *Tříprvková grupa pootočení $(H_3, +)$ je izomorfní s podgrupou grupy permutací $(S_3, \circ)$ obsahující tři prvky id, $(1,2,3)$ a $(1,3,2)$.*

Grupa $(H_3, +)$:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	1	0

Grupa $(S_3, \circ)$:

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

$(H_3, +)$ se izomorfně zobrazila na podgrupu grupy $(S_3, \circ)$ se stejným počtem prvků, která je sama grupou (je uzavřená vzhledem k operaci skládání a obsahuje inverze ke všem svým prvkům). Z tabulek je vidět, že pokud se 0 zobrazí na id, 1 na $(1,2,3)$ a 2 na $(1,3,2)$, tak výsledky operace zůstávají v tabulce na přesně stejném místě (pokud tedy prvky v záhlaví tabulky napíšeme ve stejném pořadí). •

Příklad 18 *Grupu permutací, která je izomorfní k dané grupě je možné najít i v případě, kdy je původní grupa nekonečná.*
Pokusme se najít izomorfní grupu permutací k množině $(Z, +)$. Hledaná grupa existuje a bude to grupa bijekcí na množině, která má nekonečný počet prvků $(S_Z, \circ)$.

Grupa $(Z, +)$:

$+$	$\dots$	-2	-1	0	$\dots$
$\dots$		$\dots$	$\dots$	$\dots$	
-2	$\dots$	-4	-3	-2	$\dots$
-1	$\dots$	-3	-2	-1	$\dots$
0	$\dots$	-2	-1	0	$\dots$
$\dots$		$\dots$	$\dots$	$\dots$	

Grupa $(S_Z, \circ)$:

$\circ$	$\dots$	$\begin{pmatrix} \dots & -1 & 0 & 1 & \dots \\ & \downarrow & \downarrow & \downarrow & \\ \dots & -3 & -2 & -1 & \dots \end{pmatrix}$	$\begin{pmatrix} \dots & -1 & 0 & 1 & \dots \\ & \downarrow & \downarrow & \downarrow & \\ \dots & -2 & -1 & 0 & \dots \end{pmatrix}$	$\dots$
$\begin{pmatrix} \dots & -1 & 0 & 1 & \dots \\ & \downarrow & \downarrow & \downarrow & \\ \dots & -3 & -2 & -1 & \dots \end{pmatrix}$	$\dots$	$\begin{pmatrix} \dots & -1 & 0 & 1 & \dots \\ & \downarrow & \downarrow & \downarrow & \\ \dots & -5 & -4 & -3 & \dots \end{pmatrix}$	$\begin{pmatrix} \dots & -1 & 0 & 1 & \dots \\ & \downarrow & \downarrow & \downarrow & \\ \dots & -4 & -3 & -2 & \dots \end{pmatrix}$	$\dots$

Prvek -2 z grupy celých čísel se zobrazí na bijekci Z do Z, která posouvá všechna čísla na čísla o -2 nižší, prvek -1 se zobrazí na bijekci, která všechna čísla posouvá na čísla o -1 nižší atd. Výsledek operace zůstane zachován. Grupy $(Z, +)$ a $(S_Z, \circ)$ jsou tedy skutečně izomorfní. •

Příklad 19 *Grupu $(Z_2 \times Z_4, +)$ lze injektivně vnořit do grupy $(S_8, \circ)$, takže grupa $(Z_2 \times Z_4)$ je izomorfní podgrupě $(P, \circ)$ grupy $(S_8, \circ)$: pokusme se podgrupu P najít.*

Tabulka operace viz strana 43. Konstrukce permutací a jejich geometrický význam viz video, přednáška 05. Příklad musíte umět.

5.2 Cvičení 05: Algebraické struktury se 2 operacemi zadané tabulkou i předpisem, zbytkové třídy.

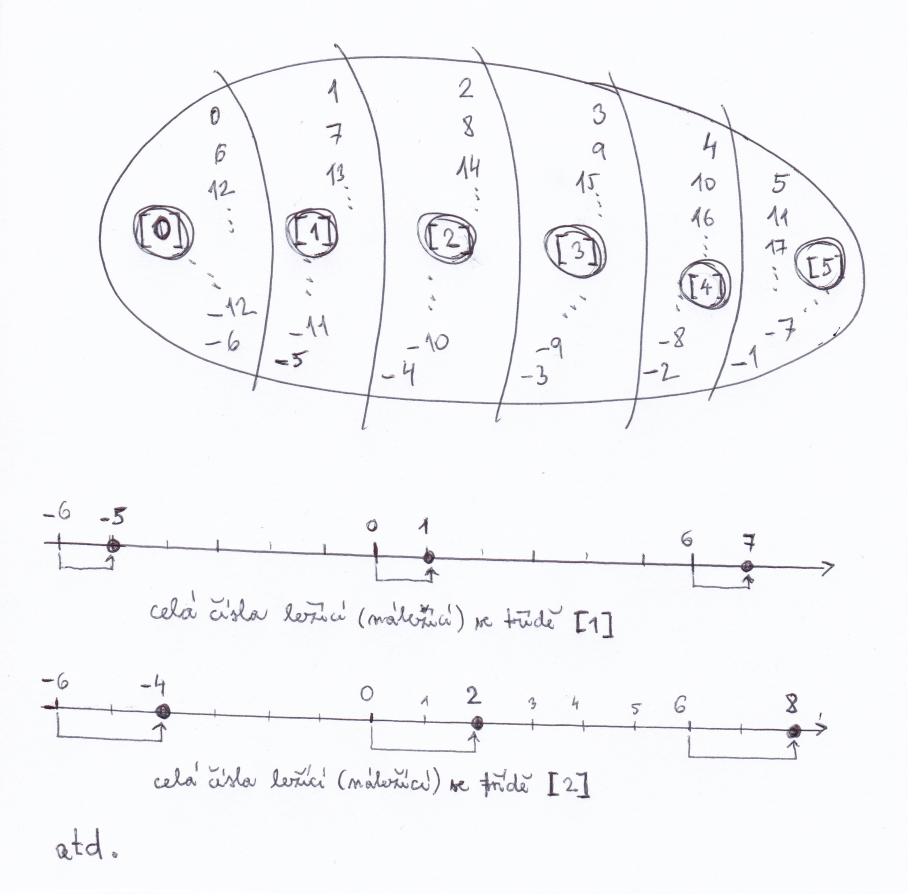
Grupy zbytkových tříd

Toto je jen uvedení do zbytkových tříd a skutečností, že zbytkové třídy můžeme sčítat a násobit, a tak množiny zbytkových tříd tvoří algebraické struktury.

Definice 20 *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). 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:

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

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).

Z tabulky operace je snad jasné, že $(Z_6, \oplus)$ 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]

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

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

- označení 07: Z_n ... množina zbytkových tříd modulo n;
- označení 08: Z_n^* ... množina zbytkových tříd modulo n mimo prvek [0], tj.

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

Toto označení používáme i pro klasické množiny Q^* (racionální čísla mimo nuly), R^* (reálná čísla mimo nuly), protože se nám hodí, že $(Q^*, \cdot)$, $(R^*, \cdot)$ jsou grupy (nulu z těchto množin musíme vyloučit, protože pro ni neexistuje inverzní prvek vzhledem k operaci násobení).

Zbytkové třídy lze sestavit nejen pro $n = 6$, ale pro jakékoli přirozené $n > 1$. Přitom platí následující skutečnosti:

Skutečnost první (věta 24): 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.

Skutečnost druhá (věta 25): Důsledek předchozí skutečnosti: 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]

Generování kartézského součinu grup zbytkových tříd

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

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

Obecné cvičení na struktury se dvěma operacemi

Následující příklady se týkají cvičení po přednášce číslo 7, takže pokud některé věci nebudou vysvětleny na cvičení, snad je najdete na přednášce 7. Pojem ideálu není povinný.

Úloha 5.1 *V množině Q jsou definovány operace $\oplus$ a $\odot$ předpisy: $x \oplus y = x + y, x \odot y = \frac{1}{2}xy$. Ověřte, zda $(Q, \oplus, \odot)$ je těleso.*

Úloha 5.2 *V množině Z jsou definovány operace $\oplus$ a $\odot$ předpisy: $a \oplus b = a+b+1, a \odot b = a + b + ab$. Určete typ algebraické struktury.*

Úloha 5.3 *V množině R jsou definovány operace $\oplus$ a $\odot$. Zjistěte, zda $(R, \oplus, \odot)$ je těleso.*

a) $x \oplus y = x^2 + y^2, x \odot y = xy$

b) $x \oplus y = x + y, x \odot y = \frac{1}{3}xy$

Úloha 5.4 *V množině $(Z_6, \oplus, \odot)$ sestavte operační tabulku pro operace $\oplus$ a $\odot$. Určete typ struktury $(Z_6, \oplus, \odot)$.*

Úloha 5.5 *Výpočtem určete typ algebraické struktury $(Z_5, \oplus, \odot)$.*

Úloha 5.6 *Určete všechny dělitele nuly v následujících komutativních okruzích:*

a) $(Z_{12}, \oplus, \odot)$

b) $(Z_{15}, \oplus, \odot)$

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

Například N.1:

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

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

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

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

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

Například D.1:

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

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

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

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

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

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

6 týden 06

6.1 přednáška 06: homomorfismus – věty

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

Věta 17 *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).*

c) *f zobrazí podgrupu $(S, \bigtriangledown)$ na podgrupu $(f(S), *)$.*

Důkaz:

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

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

  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 (ZVO) a právě dokázanou vlastnost (a):

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

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. □

ad c) i) $f(S)$ je neprázdná množina, protože obsahuje minimálně neutrální prvek $f(e_G) = e_H$;

ii) $f(S)$ je uzavřená vzhledem k operaci $*$: pro $f(x)$ a $f(y)$ platí

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

tedy prvek $f(x) * f(y)$ je obrazem prvku $x \bigtriangledown y \in G$, a tedy $f(x) * f(y) \in f(S)$, platí uzavřenost operace $*$ na množině $f(S)$;

iii) $f(S)$ je uzavřená vzhledem k inverzím: pokud $f(a) \in f(S)$, tak podle výše dokázané vlastnosti (b) víme, že $f(a)^{-1} = f(a^{-1})$, a protože S je podgrupa uzavřená na inverze a $a \in S$, tak také $a^{-1} \in S$, tedy $f(a^{-1}) \in f(S)$ ... a protože $f(a^{-1})$ je inverzní prvek k prvku $f(a)$, je $f(S)$ uzavřená na inverze.

Celkem podle věty 6 je $f(G)$ podgrupa grupy $(H, *)$. □

Definice 21 *Jádro grupového homomorfismu $f : G \to H$ se nazývá množina ker_f (označení 09a)*[19] *těch prvků z grupy $(G, \bigtriangledown)$, které se zobrazí na neutrální prvek e_H grupy $(H, *)$.*

Obor hodnot grupového homomorfismu $f : G \to H$ se nazývá množina všech obrazů vzhledem k tomuto zobrazení – označujeme $Im(\varphi)$ (označení 09b).

Příklad 20 *a) V grupovém izomorfismu je jádrem zobrazení f vždy pouze jednoprvková množina $\{e_G\}$.*

b) V homomorfismu $f : (Z_6, +) \to (Z_3, +)$ je jádrem množina těch prvků, které se zobrazí na nulu: $Ker(f) = \{0, 3\}$ $Im(f) = \ldots$.

c) V homomorfismu $\varphi : (Z, +) \to (Z_5, +)$ definovaném $\varphi(z) = [z \mod 5]$ je $Ker(f) = \ldots$, $Im(f) = \ldots$

Věta 18 *Pro grupový homomorfismus $f : G \to H$ grupy $(G, \bigtriangledown)$ do grupy $(H, *)$ platí:*

a) Jádro $Ker\varphi$ grupového homomorfismu je podgrupou grupy $(G, \bigtriangledown)$.

b) Homomorfní obraz $Im(\varphi)$ vstupní grupy je podgrupou grupy $(H, *)$.

[19] Označení plyne z německého slova kernel.

Důkaz: viz video, přednáška 06.

Na závěr tématu ještě drobnůstka, která spíše už měla být řečena, o řádu prvku v grupě:

Definice 22 *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 21 a) *V grupě $(Z_5, +)$ je řád neutrálního prvku roven jedné a řád ostatních prvků je roven pěti.*

b) *V grupě $(S_3, \circ)$ platí pro řády prvků:*

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

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

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

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

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

Příklad 22 *V grupě permutací $(S_7, \circ)$ určete řád prvku*

- $(1,2,3,4) \circ (2,4,5)$;
- $\{[(1,2,3,4) \circ (2,4,5)]^3 \circ [(1,6,7) \circ (2,5)]^4\}^5$

Řešení druhého z úkolů: Označme $\alpha = (1,2,3,4) \circ (2,4,5)$, $\beta = (1,6,7) \circ (2,5,7)$. Nyní vlastně máme určit řád prvku $(\alpha^3 \circ \beta^4)^5$ Začněme tím, že si prvky α, β zjednodušíme tak, že vypočteme spojení bijekcí, které představují:

$$\alpha = (1,2) \circ (3,4,5), \quad \beta = (1,6,7,2,5).$$

Pak lze cykly zvlášť umocnit a spojit: $\alpha^3 = (1,2) \circ \mathrm{id} = (1,2)$, $\beta^4 = (1,5,2,7,6)$ po umocnění[20]. Spočteme „součin“ a rozložíme na dílčí „součin“ navzájem nezávislých cyklů:

$$\alpha^3 \circ \beta^4 = (1,5) \circ (2,7,6).$$

[20]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.

Při umocnění na pátou nyní opět umocníme každý cyklus zvlášť, a dostaneme paradoxně tentýž prvek:

$$(\alpha^3 \circ \beta^4)^5 = (1,5) \circ (2,6,7).$$

Nyní si výpočet řádu tohoto prvku můžeme hodně zjednodušit následující úvahou: 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.

Příklad 23 *Pro grupu $(D_5, \circ)$, kde D_5 je desetiprvková množina transformací pravidelného pětiúhelníka na sebe sama a operace $\circ$ (=„po“) je skládání transformací,*

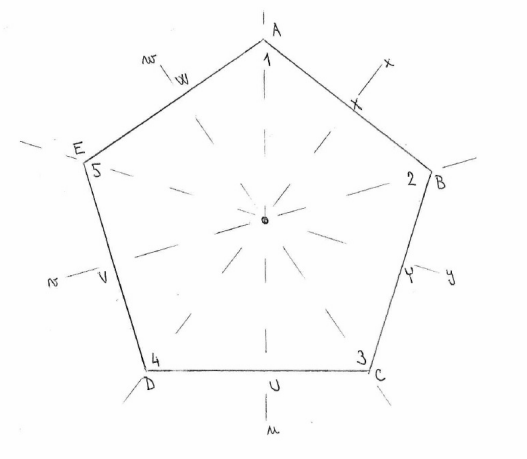
a) vypište všechny prvky a určete jejich řád;

b) vypište všechny její podgrupy.

Řešení: *ad a) všechny prvky jsou v dalším vypsány, jejich řád ne, ale čtenář si jej určí jako cvičení; ad b) Podgrupy jsou všechny vypsány.*

Použijeme následující 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.*

$|D_5| = 10$, tj. kromě triviálních podgrup $P_1 = \{id\}, P_2 = D_5$ budou existovat ještě podgrupy, jejichž počet prvků je dělitelem čísla 10, tj. podgrupy dvouprvkové a pětiprvkové. Pokusme se všechny najít pomocí označení permutacemi pětiprvkové množiny: Klíčem je označit si vrcholy čísly 1 až 5, pak:

- $e = id$; $f = (1,2,3,4,5)$; $g = (1,3,5,2,4)$; $h = (1,4,2,5,3)$; $i = (1,5,4,3,2)$; $u = (2,5) \circ (3,4)$; $v = (1,3) \circ (4,5)$; $w = (1,5) \circ (2,4)$; $x = (1,2) \circ (3,5)$; $y = (1,4) \circ (2,3)$.

Je vidět, že pětiprvková podmnožina všech pootočení tvoří podgrupu $P_3 = \{e, f, g, h, i\}$. Obsahuje všechny inverze: $e \leftrightarrow e, f \leftrightarrow i, g \leftrightarrow h$.

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

Žádné další netriviální podgrupy, než těchto šest, už neexistují. Celkem má tedy D_5 osm podgrup.

- Když vezmeme jakékoliv pootočení kromě identity, už pomocí něho vygenerujeme všechna další pootočení - a protože podgrupa musí být uzavřená na výsledek operace (= na složení transformací), musíme ty další pootočení přidat do téže podgrupy - tj. až vezmeme jakákoli dvě různá pootočení, musíme už do stejné podgrupy přidat i tři další pootočení.

  Např. $f^1 = f$

  $f^2 = f \circ f = g$

$f^3 = f \circ f \circ f = h$

$f^4 = f \circ f \circ f \circ f = i$

$f^5 = f \circ f \circ f \circ f \circ f = e$

Takové podgrupě, který je generována jediným prvkem, říkáme cyklická: $P_3 = \langle f \rangle$ ...je generovaná („vytvořená“) prvkem f.

- Kdybychom k některé z podgrup P_4, P_5, P_6, P_7, P_8 přidali jediný další prvek, už by nutně (aby platila uzavřenost operace) vygeneroval celou množinu D_5.

  Např. přidáním w k množině $P_4 = \{e, u\}$:

  $w \circ u = (1,5) \circ (2,4) \circ (2,5) \circ (3,4) = (1,5,4,3,2) = i$ díky uzavřenosti podgrupy na operaci by už i muselo nutně ležet v naší podgrupě

  $i^2 = h$ díky uzavřenosti podgrupy na operaci by už h muselo nutně ležet v naší podgrupě

  $i^3 = g$ díky uzavřenosti podgrupy na operaci by už g muselo nutně ležet v naší podgrupě

  $i^4 = f$ díky uzavřenosti podgrupy na operaci by už f muselo nutně ležet v naší podgrupě

  $i \circ u = (1,5,4,3,2) \circ (2,5) \circ (3,4) = (1,5) \circ (2,4) = w$ díky uzavřenosti podgrupy na operaci by už w muselo nutně ležet v naší podgrupě

  $h \circ u = (1,4,2,5,3) \circ (2,5) \circ (3,4) = (1,4) \circ (2,3) = y$ díky uzavřenosti podgrupy na operaci by už y muselo nutně ležet v naší podgrupě

  $g \circ u = (1,3,5,2,4) \circ (2,5) \circ (3,4) = (1,3) \circ (4,5) = v$ díky uzavřenosti podgrupy na operaci by už v muselo nutně ležet v naší podgrupě

  $f \circ u = (1,2,3,4,5) \circ (2,5) \circ (3,4) = (1,2) \circ (3,5) = x$ díky uzavřenosti podgrupy na operaci by už x muselo nutně ležet v naší podgrupě

  Tímto generováním už nutně dostaneme celou desetiprvkovou množinu D_5.

6.2 Dodatky, na které nebude čas 02

O řádu prvku v grupě

Věta 19 *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 částech: 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 o dělení celých čísel se zbytkem vždy nezáporným (viz Základy matematiky – my ji nyní použijeme pouze pro čísla přirozená) vydělíme $m : n$ a dostaneme, že existují přirozená čísla q, r tak, že

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

Pak lze upravit a^m na tvar

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

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

Důkaz části b): Zbývá dokázat, že prvky a^0, a^1, …, a^{n-1} jsou navzájem různé. Pokud se některé z těchto dvou prvků rovnají, platí $a^r = a^s$, kde r i s jsou dvě různá čísla z množiny $\{0, 1, 2, \ldots, n-1\}$, tj. $r \neq s$. BUNO[21] 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 19 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 20 *Pro prvek a nekonečného řádu v grupě $(G, \bigtriangledown)$ platí: v této grupě neexistují dvě mocniny tohoto prvku, které se rovnají, tj. pro dvě různá celá čísla r, s platí $a^r \neq a^s$.*

Důkaz: je prostý, použijeme tutéž úvahu jako v důkazu věty 19, část b): Pokud by platilo $a^r = a^s$, úpravou $a^r \bigtriangledown (a^s)^{-1}$ dostaneme

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

[21] BUNO = Bez újmy na obecnosti.

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“[22] vede na nekonečně mnoho navzájem různých prvků grupy.

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

Věta 21 *Pokud řád prvku a v grupě $(G, \bigtriangledown)$ je n (označení 10 : označme $ord(a) = n$), pak platí pro celočíselné t:*

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

(mocnina prvku konečného řádu je rovna neutrálnímu prvku tehdy a jen tehdy[23], když mocnitel t je násobek řádu n daného prvku).

Důkaz: Dokážeme obě implikace: Ad „⇒“: Důkaz je podobný jako důkaz věty 19, část a): Pokud $a^t = e$, pak podle věty o dělení se zbytkem pro celá čísla platí $t = n \cdot q + r$, kde $0 \leq r < n$. Pak dosazením do naší rovnosti dostaneme

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

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

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

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

Cyklické grupy

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

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

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

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

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

Touto kratinkou úvahou jsme vlastně dokázali větu

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

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

Věta 22 *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*[24] *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 výsledků operace. Dostáváme tak větu

Věta 23 *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 22 a 23 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.

Následující dvě věty lze dokázat pomocí pojmu řád prvku (přednáška 6), ale studenti na jejich platnost intuitivně přijdou z příkladů tabulky operace, a tak jim skutečnost ve větách 24, 25 nebude cizí, i když ji formálně nebudou umět dokázat:

Věta 24 *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 25 *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]

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

6.3 Cvičení 06: První cvičení na polynomy – Dělení polynomů (Hornerovo schéma při dělení polynomů a zjišťování funkční hodnoty), Eukleidův algoritmus.

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

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

Doporučené materiály k využití:

- Označení: $(Z[x],+,\cdot)$, $(Q[x],+,\cdot)$, $(R[x],+,\cdot)$, ... po řadě okruhy polynomů s koeficienty z okruhu celých čísel, tělesa racionálních čísel a tělesa reálných čísel. Tyto okruhy neobsahují netriviální dělitele nuly, takže se jedná o obory integrity (Budínová 2013, str. 7, věta 1). Ideální definice okruhu $Z[x]$: jedná se o rozšíření okruhu $(Z,+,\cdot)$ o prvek x, kde nevíme, co je, může tam být cokoliv, třeba[25] číslo π. Množina polynomů tedy neobsahuje všechny inverze vzhledem k násobení polynomů.

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

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

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

  například

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

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

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

[25] Pinter, 2010, str. 241.

7 Týden 07

7.1 Přednáška 07: struktury se dvěma operacemi

Základní definice

Okruh je po grupě druhou základní strukturou 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 souhrnně pro obě operace. Tato interakce je popsána v následujících čtyřech definicích:

Definice 23 *polookruh (anglicky: semiring) je množina $(M, \bigtriangledown, \star)$ s vlastnostmi:*

a) *Operace $\bigtriangledown$ splňuje vlastnosti (1), (2), (3), (5), tj. $(M, \bigtriangledown)$ je komutativní monoid;*

b) *operace $\star$ splňuje vlastnosti (1), (2), (3), tj. množina $(M, \star)$ je monoid;*

c) *interakce operací $\bigtriangledown$ a $\star$ splňuje tzv. distributivní zákon = vlastnosti (6a), (6b):*

$$\forall\ x, y, z \in M : x \star (y \bigtriangledown z) = (x \star y) \bigtriangledown (x \star z), \qquad (6a)$$
$$\forall\ x, y, z \in M : (y \bigtriangledown z) \star x = (y \star x) \bigtriangledown (z \star x). \qquad (6b)$$

(rovnice (6a), (6b) jsou dvě díky tomu, že operace $\star$ není obecně komutativní; počítáme-li rovnice (6a), (6b) za dvě vlastnosti, celkově je vlastností v polookruhu devět; platí-li navíc komutativita druhé operace $\star$, vlastností je opět devět, protože sice přibude vlastnost (5) pro operaci $\star$, ale vlastnost (6b) ubude díky komutativitě operace $\star$).

Typickým příkladem polookruhu je množina přirozených čísel obohacena o nulu, s operacemi sčítání a násobení: $(N_0, +, \cdot)$ je komutativní polookruh, neobsahuje inverze vzhledem k žádné z operací.

Definice 24 *okruh (anglicky: ring) je množina $(M, \bigtriangledown, \star)$ s vlastnostmi:*

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

b) *operace $\star$ splňuje vlastnosti (1), (2), (3), tj. množina $(M, \star)$ je monoid;*

c) *interakce operací $\bigtriangledown$ a $\star$ splňuje tzv. distributivní zákon = vlastnosti (6a), (6b):*

$$\forall\ x, y, z \in M : x \star (y \bigtriangledown z) = (x \star y) \bigtriangledown (x \star z), \qquad (6a)$$
$$\forall\ x, y, z \in M : (y \bigtriangledown z) \star x = (y \star x) \bigtriangledown (z \star x). \qquad (6b)$$

(**Na rozdíl od polookruhu v okruhu přibývá jediná vlastnost, a sice vlastnost (4), existence inverzí u operace $\bigtriangledown$; protože inverzní prvky budou ve strukturách se dvěma operacemi existovat vzhledem ke dvěma operacem, musíme**

použít dvojí označení inverzního prvku: inverzi prvku a vzhledem ke $\bigtriangledown$ budeme označovat jako $-a$, tedy znakem minus před daným prvkem;

rovnice (6a), (6b) jsou dvě díky tomu, že operace $\star$ není obecně komutativní; počítáme-li rovnice (6a), (6b) za dvě vlastnosti, celkově je vlastností v okruhu deset; platí-li navíc komutativita druhé operace $\star$, vlastností je opět deset, protože sice přibude vlastnost (5) pro operaci $\star$, ale vlastnost (6b) ubude díky komutativitě operace $\star$).

Typickým příkladem okruhu je množina $(Z_6, +, \cdot)$ – komutativní okruh, který není oborem integrity (obor integrity definujeme jako další z algebraických struktur, viz níže). Podrobnějším prozkoumání Cayleyho tabulek struktury $(Z_6, +, \cdot)$ zjistíme:

$+$	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

$\cdot$	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

a) Operace sčítání splňuje vlastnosti $(1), (2), (3), (4), (5)$;

b) Oprace násobení splňuje vlastnosti $(1), (2), (3), (5)$, nesplňuje vlastnost (4), protože neexistují inverze vzhledem k násobení pro prvky 0, 2, 3, 4.;

c) Interakce obou operací splňuje distributivní zákony $(6a), (6b)$.

Tedy celkem $(Z_6, +, \cdot)$ je komutativní okruh. Ovšem struktura $(Z_6, \cdot)$ vykazuje určité defekty, tj. obsahuje tzv. nenulové dělitele nuly:

Definice 25 *nenuloví dělitelé nuly jsou takové prvky a, b algebraické struktury $(M, \bigtriangledown, \star)$, které se nerovnají nule $0_\bigtriangledown$ (neutrální prvek v grupě $(M, \bigtriangledown)$, tj. vzhledem k první operaci), ale výsledek druhé operace s těmito prvky $a \star b$ je roven nule: $a \star b = 0_\bigtriangledown$;*

Množina Z_6 zbytkových tříd modulo 6 je příkladem struktury s nenulovými děliteli nuly: její prvky [2], [3] nebo [3], [4] jsou nenuloví dělitelé nuly, protože platí

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

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

$$[2] \cdot [2] = [2] \cdot [5], \quad \text{ale } [2] \neq [5].$$

Nenulové dělitele 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. Ale než se dostaneme k odpovědím, definujme obor integrity – algebraickou strukturu, která nenulové dělitele nuly neobsahuje:

Definice 26 *obor integrity*[26] *(anglicky: integral domain) je množina*[27] $(M, \bigtriangledown, \star)$ *s vlastnostmi:*

ad a) *Operace* $\bigtriangledown$ *splňuje vlastnosti* (1), (2), (3), (4), (5)*;*

ad b) *operace* $\star$ *splňuje vlastnosti* (1), (2), (3), ($\nexists\, NDN$), (5)*;*

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

$$\forall\ x, y, z \in M : x \star (y \bigtriangledown z) = (x \star y) \bigtriangledown (x \star z), \qquad (6)$$

Na rozdíl od okruhu v oboru integrity je už zaručena komutativita obou operací, tj. přibude vlastnost (5) pro operaci $\star$ jako nedílná součást každého oboru integrity, ale namísto distributivních zákonů (6a), (6b) máme jen jeden distributivní zákon (6). Přesto je v oboru integrity splněno více vlastností, a sice jedenáct, protože navíc přibývá vlastnost neexistence nenulových dělitelů nuly ($\nexists\, NDN$).

Typickým příkladem oboru integrity je algebraická struktura $(Z, +, \cdot)$ celých čísel s operacemi sčítání a násobení.

Definice 27 *Těleso (anglicky: field ... proto některé (starší) české učebnice používají též název „pole“) je množina* $(M, \bigtriangledown, \star)$ *s vlastnostmi:*

ad a) *Operace* $\bigtriangledown$ *splňuje vlastnosti* (1), (2), (3), (4), (5) *na množině* M*, tedy* $(M, \bigtriangledown)$ *je komutativní grupa;*

[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 neutrální prvek vzhledem k první operaci a neutrální prvek vzhledem ke druhé operaci, a navíc jsou tyto dva prvky navzájem odlišné, nerovnají se.

ad b) *Operace* $\star$ *splňuje vlastnosti* (1), (2), (3), (4), (5) **na množině** $M \setminus \{0_\triangledown\}$, *tedy* $(M \setminus \{0_\triangledown\}, \star)$ *je komutativní grupa;*

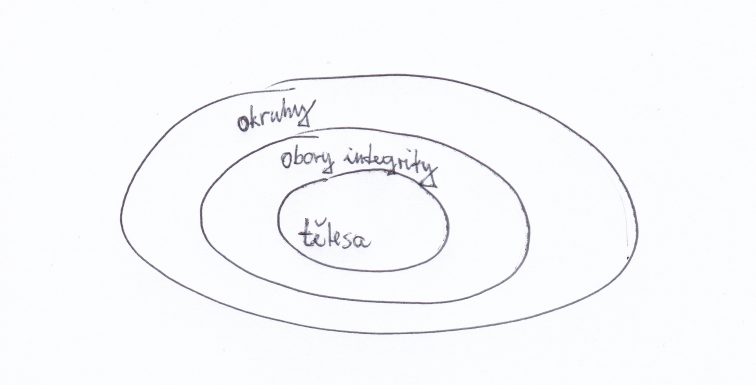
ad c) *díky komutativitě operace* $\cdot$ *lze distributivní zákon psát v jediné rovnici:*

$$\forall\ x, y, z \in M : x \star (y \triangledown z) = (x \star y) \triangledown (x \star z), \qquad (6)$$

Na rozdíl od oboru integrity v tělese platí pro operaci $\star$ vlastnost (4) namísto vlastnosti $(\not\exists\ NDN)$ – v tělese je tedy splněno jedenáct vlastností, stejně jako v oboru integrity. **Ale pozor, vlastnosti** $(1), (2), (3), (4), (5)$ **operace** $\star$ **neplatí v tělese na množině** M**, ale na množině** $M \setminus \{0_\triangledown\}$ **... vypuštění neutrálního prvku** $0_\triangledown$ **potřebujeme zejména k zajištění vlastností inverzí, k prvku** $0_\triangledown$ **totiž neexistuje inverze vzhledem k operaci** $\star$**.** Ovšem všechny z vlastností $(1), (2), (3), (4), (5)$ pak platí na množině $M \setminus \{0_\triangledown\}$: operace $\star$ je uzavřená na množině $M \setminus \{0_\triangledown\}$, asociativní a komutativní na množině $M \setminus \{0_\triangledown\}$, neutrální prvek $1_\star$ existuje na množině $M \setminus \{0_\triangledown\}$, všechny inverze vzhledem k operaci $\star$ existují na množině $M \setminus \{0_\triangledown\}$.

Typickým příkladem těles jsou známé množiny $(Q, +, \cdot)$, $(R, +, \cdot)$.

Na základě věty 27 uvidíme, že vlastnost (4) na množině $(M \setminus \{0_\triangledown\}, \star)$ je silnější než vlastnost $(\not\exists\ NDN)$, tedy v tělese automaticky z definice vyplývá, že v něm neexistují nenulové dělitele nuly. Tedy pojmy polookruh, okruh, obor integrity a těleso představují struktury stále silnějších vlastností (na obrázku chybí zakreslit polookruhy, který by zahrnovaly ještě větší část roviny než jen množinu všech okruhů):



Zákon krácení v okruhu

Dříve než se ovšem pustíme do rozdílů mezi algebraickými strukturami dvou operací, podívejme se ještě na jednu vlastnost, která byla zmíněna v grupě (vlastnost krácení (7)) a je důležitá i ve strukturách se dvěma operacemi: označíme ji v okruhu stejným číslem $(7)^\star$, jen symbol $\star$ označuje určitou odlišnost typickou pro okruhy:

$$\forall a, b, c \in (M, \triangledown, *), a \neq 0_\triangledown : a * b = a * c \Rightarrow b = c \quad (7)^*$$

(tedy jestliže prvek $a \in (M, \bigtriangledown, \star)$ není neutrálním prvkem vzhledem k operaci $\bigtriangledown$, pak jím lze v rovnici krátit – tento požadavek je rozumný, víme přece, že z rovnosti $0 \cdot 6 = 0 \cdot 7$ neplyne, že $6 = 7$, tedy nulou krátit nelze). Označení $(7)^\star$ je také rozumné, protože pomáhá si zapamatovat, že zákon krácení se týká operace $\star$ v okruhu.

Následující věta ukazuje na překvapivý a velice užitečný výsledek, který vnese jasno do vztahu mezi nenulovými děliteli nuly a ostatními vlastnostmi:

Věta 26 *V každém okruhu* $(M, \bigtriangledown, \star)$ *platí:* $(7)^\star \Leftrightarrow \nexists$ *NDN.*

Důkaz: "⇒" Předpokládejme, že $(M, \bigtriangledown, \star)$ je okruh splňující vlastnost $(7)^\star$, a chceme dokázat, že neexistují nenulové dělitele nuly.

Prozkoumáme rovnici $a \star b = 0_\bigtriangledown$:

1) pokud $a = 0_\bigtriangledown$, jsme hotovi, protože b je nulový (triviální) dělitel nuly.

2) pokud $a \neq 0_\bigtriangledown$, můžeme psát:
$a \star b = 0_\bigtriangledown = a \star 0_\bigtriangledown$ (umělá finta, nulu jsme vyjádřili jako $a \star 0_\bigtriangledown$!!!!!), tedy:

$a \star b = a \star 0_\bigtriangledown \Rightarrow$ podle (7)* platí $b = 0_\bigtriangledown$, tedy a je triviální (nulový) dělitel nuly, což nám právě nevadí, my jsme hledali netriviální (nenulové) dělitele nuly, a ty jsme nenašli.

Celkem aspoň jedno z čísel a, b je nula $\Rightarrow$, tj. nenašli jsme žádné nenulové dělitele nuly ... tedy žádní neexistují, a to jsme chtěli dokázat.

"⇐" Předpokládejme, že $(M, +, \cdot)$ je okruh neobsahující nenulové dělitele nuly, ukážeme, že splňuje (7)*.
Pokud $a \neq 0_\bigtriangledown$, uvažujme rovnost $a \star b = a \star c$. Obecně prvek a^{-1} nemusí existovat, ale nyní využijeme druhé operace, tj. existence opačného prvku $(-a \star c)$ k prvku $(a \star c)$:

$a \star b - a \star c = 0_\bigtriangledown$ ... využijeme distributivní zákon (6a), dostaneme:

$a \star (b - c) = 0_\bigtriangledown$ ... Víme, že okruh neobsahuje nenulové dělitele nuly $\Rightarrow$ musí nastat $b - c = 0_\bigtriangledown$, a tedy $b = c$, dokázali jsme (7)*. □.

Například ve struktuře $(Z_6, +, \cdot)$ víme, že existují nenulové dělitele nuly – na základě předchozí věty tedy hned můžeme uzavřít, že v této algebraické struktuře nelze krátit. Ve struktuře $(Z_7^{star}, \cdot)$, kde hvězdička označuje, že z množiny Z_7 jsme vyloučili nulu (struktura $Z_7^\star$ má tedy šest prvků), tabulka operace neobsahuje prvek nula jako výsledek, tedy odtud víme, že nenulové dělitele se zde nevyskytují – odtud hned víme, že ve struktuře $(Z_7, +, \cdot)$ lze krátit všechny nenulové prvky, tj. platí zde $(7)^\star$.

Dále z věty 26 plyne, že vlastnost ($\nexists NDN$) v definici oboru integrity lze ekvivalentně nahradit vlastností $(7)^\star$.

Doplnění obrazu o vztahu mezi strukturami se dvěma operacemi

Věta 27 *V každém tělese* $(M, \bigtriangledown, *)$ *platí: Z existence inverzí* (4) *vzhledem k operaci* $*$ *plyne, že je splněna vlastnost* $(7)^*$.

(Důkaz jednoduše: Z existence inverzí (4) vzhledem k operaci $*$ plyne, že pro libovolné $x \in (M - \{0_\bigtriangledown\}, *)$ lze rovnost

$$x * y = x * z$$

vynásobit zleva inverzním prvkem x^{-1}:

$$y = 1 * y = x^{-1} * x * y = x^{-1} * x * z = 1 * z = z \quad \Rightarrow \quad y = z.$$

To ovšem znamená, že pro nenulové x lze v rovnosti $x * y = x * z$ krátit, a tedy platí $(7)^*$. Důkaz je hotov. $\square$.)

Věta 27, doplněna větou 26, dokazuje, že každé těleso je současně oborem integrity, tedy neobsahuje nenulové dělitele nuly – teprve nyní jsme obecně ukázali, že obrázek na straně 73 je oprávněný. Každé těleso je oborem integrity, ale naopak existují obory integrity, které nejsou tělesem, například $(Z, +, \cdot)$ je obor integrity, který není tělesem.

Příklad struktury $(Z, +, \cdot)$ dokazuje, ž existují obory integrity, které nejsou tělesem. Následující větička dokazuje, že u konečných oborů to neplatí – neexistuje konečný obor integrity, který by nebyl tělesem:

Věta 28 *Každý konečný obor integrity* $(M, \bigtriangledown, *)$ *je už tělesem.*

(Důkaz: Přímý – předpokládejme, že $(M, \bigtriangledown, *)$ je konečný obor integrity, dokážeme, že je tělesem, tj. to bude objasněno, jestliže najdeme v M inverze vzhledem k operaci $*$ pro všechny prvky mimo prvek $0_\bigtriangledown$. Pojďme na to: už na začátku víme, že neutrální prvek 1_* je inverzní sám k sobě. Najděme inverze vzhledem k operaci $*$ pro prvky zbývající: protože předpokládáme, že $M = \{0_\bigtriangledown, 1_*, x_1, x_2, \ldots, x_{n-2}\}$ je konečná množina, stačí najít inverze pro prvky $x_1, x_2, \ldots, x_{n-2}$ (nulu vzhledem k první operaci z hledání inverzí vzhledem ke druhé operaci vylučujeme, protože víme, že bychom ji nenašli, neexistuje totiž – i tak ukážeme, že struktura $(M \setminus \{0_\bigtriangledown\}, \star)$ je grupa uzavřená na výsledky operace). Najděme bez újmy na obecnosti inverzi pro prvek x_1 ... ten označuje libovolný prvek množiny $M \setminus \{0_\bigtriangledown\}$ mimo neutrálního prvku $1_\star$.

Jestliže prvek x_1 násobíme všemi možnými nenulovými prvky, dostáváme součiny $x_1 * 1_*$, $x_1 * x_1$, $x_1 * x_2$, $x_1 * x_3$, ..., $x_1 * x_{n-2}$. Jedná se o $(n-1)$ součinů, z nichž každé dva dávají různý výsledek – kdybychom totiž dostali dva stejné výsledky, mohli bychom v oboru integrity provést krácení, a dospěli k tomu, že v záhlaví tabulky operace $*$ se vyskytují dva stejné prvky, což není možné (označení jsme od začátku konstruovali tak, že 1_*, x_1, x_2, ..., x_{n-2} označují různé nenulové prvky našeho oboru integrity). Protože M je konečná množina, některý z $(n-1)$ výsledků součinu musí být číslo 1_*, tedy pro nějaké $s \in \{1, 2, \ldots, n-2\}$ platí

$$x_1 * x_s = 1_*.$$

Našli jsme tedy inverzi x_s prvku x_1 vzhledem k operaci $*$. Protože úvahu lze provést nejen pro x_1, ale pro libovolný prvek různý od neutrálního, je tím prokázána existence všech inverzních prvků na množině $M \setminus \{0_\triangledown\}$. Důkaz je hotov. $\square$.)

Příklad 24 *$(Z_6, +, \cdot)$ je komutativní okruh, který obsahuje nenulové dělitele nuly; $(Z_7, +, \cdot)$ neobsahuje nenulové dělitele nuly, a tedy je oborem integrity, ale jako konečný obor integrity je podle věty 28 dokonce tělesem. To není náhoda, ale pravidlo: jestliže n je prvočíslo, tak $(Z_n, +, \cdot)$ je těleso. Jestliže n je číslo složené, $(Z_n, +, \cdot)$ obsahuje dělitele nuly a je tedy jen komutativním okruhem.*

Příklad 25 *Struktura $(2^A, \cup, \cap)$ je komutativní polookruh, který obsahuje nenulové dělitele nuly.*

Příklad 26 *Struktura $(2^A, \div, \cap)$ je komutativní okruh, který obsahuje nenulové dělitele nuly.*

Pojem ideálu je nepovinný

Kromě termínů polookruh, okruh, obor integrity, těleso se někdy v algebraické teorii vyskytují pojmy ideál a hlavní ideál, které bude asi dobré doplnit společně s příklady pojem ideálu a příklad už ovšem nebude zkoušeno, na rozdíl ode všeho ostatního v této přednášce.

Definice 28 *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).

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

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

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

Definice 29 *V teorii ideálů hraje klíčové místo tzv. hlavní ideál okruhu, který definujeme jako takový ideál B, který vygenerujeme jediným prvkem b, jenž vynásobíme se všemi prvky množiny M.*

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

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

- $B_2 :=< 2 >$ ... ideál generovaný prvkem 2 a všemi součiny $2 \cdot z$ pro $z \in Z$, tj. jedná se o ideál z příkladu 6.5:

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

- $B_3 :=< 3 >$ ... 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. Ve skutečnosti je docela schůdné dokázat matematickou větu, že každý ideál okruhu $(Z, +, \cdot)$ je hlavním ideálem.

S teoretickým výkladem a uvedením několika důležitých výsledků celé teorie budeme pokračovat v předmětu Algebra 3, v rozsahu asi dvou přednášek. Nyní už se pustíme do hledání kořenů polynomu, tedy řešení polynomických rovnic.

7.2 Cvičení 07: Polynomy 02

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

Využijte například následující materiál:

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

8 Týden 08

8.1 Přednáška 08: Polynomické rovnice – algebraické metody

Označme

$Z[x] := \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0; a_i \in Z, n \in N\}$ množinu polynomů s celočíselnými koeficienty, x je proměnná

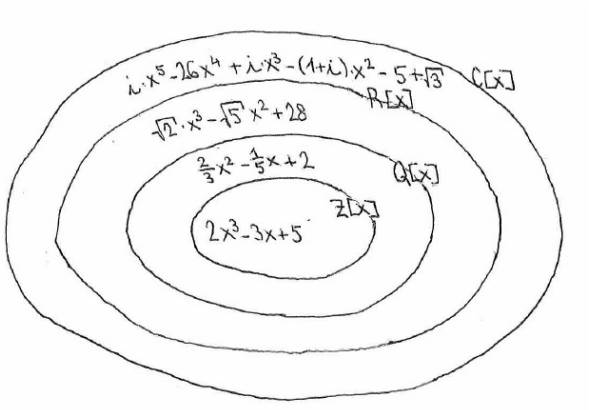
$Q[x] := \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0; a_i \in Q, n \in N\}$ množinu polynomů s racionálními koeficienty, x je proměnná

$R[x] := \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0; a_i \in R, n \in N\}$ množinu polynomů s reálnými koeficienty, x je proměnná

$C[x] := \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0; a_i \in C, n \in N\}$ množinu polynomů s komplexními koeficienty, x je proměnná

Nyní se dostáváme k jádru předmětu algebra - k řešení polynomických rovnic typu $p(x) = 0$, kde $p(x)$ je právě nekterá z množin $Z[x], Q[x], R[x], C[x]$, tzn. polynom. Co se týká množinového porovnání těchto množin, platí $Z[x] \subseteq Q[x] \subseteq R[x] \subseteq C[x]$:

- polynom s celočíselnými koeficienty je současně i polynomem s koeficienty racionálními, reálnými i komplexními
- polynom s racionálními koeficienty (tj. koeficienty ve tvaru zlomku) je současně i polynomem s koeficienty reálnými i komplexními
- polynom s reálnými koeficienty je současně i polynomem s koeficienty komplexními



Většinou nám bude v této přednášce stačit zabývat se polynomu z množin $Z[x]$ nebo $Q[x]$, ale několik věcí, které budou řečeny, bude platit i pro polynomy z množin $R[x]$ a $C[x]$.

Už v samotném tvaru polynomu se používají dvě operace, sčítání a násobení, pomocí těchto stejných operací můžeme sčítat a násobit i samotné polynomy, tj. máme struktury

se dvěma operacemi $(Z[x],+,\cdot),(Q[x],+,\cdot),(R[x],+,\cdot),(C[x],+,\cdot)$. První otázka matematického zkoumání zní, o jaké struktury se jedná z algebraického hlediska?

operace $+$: pro $p(x)=2x^3-5x^2+4, q(x)=3x^2-2x+5 \Rightarrow p(x)+q(x)=2x^3-2x^2-2x+9$
(1) platí, výsledek je opět polynom, tj. operace je uzavřená
(2) platí, což plyne z asociativity sčítání čísel
(3) platí, neutrálním prvkem je polynom $n(x)=0$ ... velmi jednoduchý polynom
(4) platí, např. pro polynom $p(x)=2x^3-5x^2+4$ je inverzí vzhledem ke sčítání polynom $-p(x)=-2x^3+5x^2-4$
(5) platí, $p(x)+q(x)=q(x)+p(x)$

operace $\cdot$: pro $p(x)=2x^3-5x^2+4, q(x)=3x^2-2x+5 \Rightarrow p(x)\cdot q(x)=(2x^3-5x^2+4)\cdot(3x^2-2x+5)=6x^5-19x^4+20x^3-13x^2-8x+20$
(1) platí, výsledek je opět polynom
(2) platí, což plyne z asociativity násobení čísel
(3) platí, neutrálním prvkem je polynom $j(x)=1$ ... tedy celkem jednoduchý polynom
(4) neplatí, polynom $p(x)$ nemá inverzi: $(2x^3-5x^2+4)\cdot\frac{1}{2x^3-5x^2+4}=1$, jenže $\frac{1}{2x^3-5x^2+4}$ není polynom (nemá tvar ax^3+bx^2+cx+d)
Inverzní funkce u mnoha polynomů sice existuje, ale neleží v naší množině $Z[x],Q[x],R[x],C[x]$. (5) platí, $p(x)\cdot q(x)=q(x)\cdot p(x)$

interakce operací $+,\cdot$: lze ověřit, že $p(x)\cdot(q(x)+r(x))=p(x)\cdot q(x)+p(x)\cdot r(x)$ ... $\forall p(x),q(x),r(x)$

Tedy celkem všechny ze struktur $(Z[x],+,\cdot),(Q[x],+,\cdot),(R[x],+,\cdot),(C[x],+,\cdot)$ jsou okruhy - a když si uvědomíme, že se v nich vlastně jedná o běžné sčítání a násobení čísel, zjistíme, že se zde nevyskytují nenuloví dělitelé nuly, tj. všechny tyto okruhy jsou současně i obory integrity.

Pozor na záměnu označení: struktury $(Q,+,\cdot),(R,+,\cdot),(C,+,\cdot)$ samozřejmě tělesa jsou, jak již bylo dříve řečeno, ovšem nyní uvažujeme složitější objekty, které v sobě zahrnují neznámou hodnotu x, a dohromady tyto objekty vytvářejí pouze obory integrity.

Definice 30 *$p(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ ... prvek množiny $Z[x],Q[x],R[x]$ nebo $C[x]$ se nazývá polynom stupně n. Koeficienty a_i náleží do množiny Z (nebo Q nebo R nebo C), symbol x se nazývá proměnná a označuje cokoli, zpravidla číslo, které za objekt x lze dosadit.*

Při tomto označení už předpokládáme, že $a_n\neq 0$ (a_n je tzv. vedoucí koeficient polynomu $p(x)$), jinak bychom a_n nepsali - s jedinou výjimkou, když $p(x)=0$, tam je $a_0=0$ vedoucí koeficient, který se nule rovnat musí.

Kořen c polynomu $p(x)$ je n

Definice 31 *Říkáme, že číslo c je kořen polynomu $p(x)$, respektive že c je řešení polynomické rovnice $p(x)=0$, jestliže $p(c)=0$, tj. po dosazení $x=c$*

- *dostaneme hodnotu 0 ... v případě polynomu $p(x)$*
- *dostaneme pravdivou rovnost ... v případě rovnice $p(x)=0$*

Tedy řešení polynomické rovnice souvisí s pojmem kořen polynomu. Někdy tyto dva pojmy bývají nepřesně spojovány, například v učebnicích pro ZŠ mluvíme o kořenech rovnice, což není přesné. VŠ terminologie zde rozlišuje pojmy „kořen polynomu“ a „řešení rovnice“. Nejprve si řekneme něco o vzorcích:

a) $a \cdot x + b = 0$ ... to je tzv. lineární rovnice

Pozor, vzhledem k počtu řešení zde mohou nastat tři situace, např.

$0 \cdot x + 5 = 0$ ... nemá řešení

$2 \cdot x + 5 = 0$ ... nemá řešení v Z, ale v Q, R, C ano: $x_1 = \frac{-5}{2}$

$0 \cdot x + 2 = 2$ ... má řešení nekonečně mnoho: každé číslo z množiny, které nás zajímá, je řešením rovnice po dosazení za x.

b) $a \cdot x^2 + b \cdot x + c = 0$ ... to je tzv. kvadratická rovnice

Existují vzorce pro její řešení: všimněme si, že vzorce automaticky předpokládají, že $a \neq 0$ jinak bychom ji zapsali jako rovnici lineární, viz výše.

$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$ ... dosadíme a vypočteme řešení. Pozor, už u kvadratických rovnic někdy dochází k tomu, že $b^2 - 4ac$ je záporné číslo. Má smysl počítat odmocninu ze záporného čísla? Jinými slovy, existuje řešení kvadratické rovnice $x^2 + 1 = 0$?

Na množině R jistě takové řešení neexistuje, jelikož žádné číslo x se po umocnění na druhou a přičtení k 1 nerovná 0.

Zde někde vzniká pojem komplexního čísla. Stejně jako se matematika stovky let zdráhala pracovat se zápornými čísly, nejprve se zdráhala pracovat s komplexními čísly.

$$C := \{\ a + bi, \text{ kde } a, b \in R,\ i \text{ je imaginární číslo: } i^2 = -1\ \}$$

Lze ověřit, že komplexní čísla tvaru $a + bi$ lze mezi sebou násobit i sčítat, dokonce existují i inverze vzhledem k oběma operacím, zkrátka $(C, +, \cdot)$ je těleso, tj. struktura s hezkými algebraickými vlastnostmi k oběma operacím. Blíže ke komplexním číslům aspoň v jedné přednášce v desátém týdnu.

c) $ax^3 + bx^2 + cx + d = 0$, $a \neq 0$ ... to je tzv. kubická rovnice

Pro tuto rovnici a její řešení existují obecné vzorce pro $a, b, c, d \in R$ (tzv. Cardanovy vzorce - viz BP Ivety Trombikové, najdete v IS tohoto předmětu, str. $22 - 23$). Tyto vzorce se příliš neužívají, i když z algebraického hlediska se jedná o totální vzorce. I při dosazování do těchto vzorců se opět velmi snadno mohou vyskytnout komplexní čísla - a to i v případě, že výsledné řešení je pouze reálné!

d) $ax^4 + bx^3 + cx^2 + dx + e = 0$, $a \neq 0$ ... to je tzv. kvartická rovnice, ovšem toto označení se příliš nepoužívá, mnohem názornější je říci algebraická rovnice 4. stupně nebo polynomická rovnice 4. stupně

Opět k jejich řešení existují vzorce obecné, totální a kupodivu jednodušší než vzorce u kubické rovnice, protože po substituci $x^2 = y$ a „doplnění části polynomu na čtverec“ dostaneme rovnici kvadratickou proměnné y. Tyto vzorce je možné užít častěji než u rovnice kubické.

e) Obecné vzorce pro rovnice řádu 5 a výše neexistují, což bylo dokázáno pány Gauss a Galois (a blíže možná viz Algebra 3). Matematika tedy běžnému uživateli, kterého by zajímalo řešení těchto rovnic, vzorce většinou nenabídne. Přesto existuje několik algebraických postupů, jak některá řešení najít:

A) Hornerovo schéma: Zjistí, zda je polynom $p(x)$ dělitelný polynomem $(x - c)$ stupně 1. Hornerovo schéma má ovšem funkce minimálně tři, a to ještě další funkce najdete ve skriptu kolegyně Budínové Polynomy (viz knihovna):

- **a)** Hornerovo schéma najde fukční hodnotu polynomu $p(x)$ v čísle c ... poslední hodnota na řádku Hornerova schématu; když to není nula, i tak je to funkční hodnota $p(c)$.
- **b)** Hornerovo schéma najde kořen k, jestliže funkční hodnota $p(k)$ je rovna nule.
- **c)** Hornerovo schéma provede dělení polynomu $p(x)$ lineárním polynomem $(x - k)$, kde k je kořen – jestliže neuvažujeme nulu na poslední pozici Hornerova schématu, zbylá čísla jsou koeficienty podílu.

Například

$$(6x^3 + 13x^2 - 4) : (x + 2) = 6x^2 + x - 2$$
$$x - (-2)$$

	6	13	0	−4
−2	6	1	−2	0

Hornerovu schématu jste se věnovali v diskrétní matematice, ovšem vedoucí koeficient byl většinou roven jedné. Nyní budeme pracovat s obecným vedoucím koeficientem.

Pokud se poslední hodnota na řádku Hornerova schématu rovná 0, víme, že $c = -2$ je kořenem polynomu $6x^3 + 13x^2 - 4$, a tedy řešením polynomické rovnice $6x^3 + 13x^2 - 4 = 0$. Navíc koeficienty $6, 1, -2$ určují polynom, který vzniká jako podíl. Můžeme tedy dopočítat zbylé řešení:

$6x^3 + 13x^2 - 4 = 0$
$(x + 2) \cdot (6x^2 + x - 2) = 0$

$x_1 = -2 \qquad x_{2,3} = \frac{-1 \pm \sqrt{1+4\cdot 6\cdot 2}}{12} \qquad x_2 = \frac{1}{2} \qquad x_3 = \frac{-2}{3}$

Pomocí Hornerova schématu jsme tedy snížili stupeň zkoumaného polynomu a užitím vzorce $x_{2,3} = \frac{-b \pm \sqrt{b^2-4ac}}{2a}$ našli ostatní kořeny. Našli jsme tři řešení rovnice: $x_1 = -2; x_2 = \frac{1}{2}; x_3 = \frac{-2}{3}$. ⋆

Otázkou je, zda tento rozklad polynomu na součin lineárních polynomů existuje vždy. Na ni odpověděl pan Gauss v roce 1797 a dnes se tato odpověď jmenuje Základní věta algebry:

Věta 29 *Základní věta algebry: Každý polynom* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in C[x]$ *lze rozložit na součin vedoucího koeficientu a lineárních polynomů* $x - x_i$, *kde* $x_i \in C$, *jsou jeho kořeny:*

$$a_n \cdot (x - x_1) \cdot (x - x_2) \ldots (x - x_n).$$

Náš polynom $6x^3+13x^2-4$ z předchozí strany lze psát jako $6\cdot(x+2)\cdot(x-\frac{1}{2})\cdot(x+\frac{2}{3})$ tedy rovnici $6x^3+13x^2-4 = 0$ při rozkladu polynomu na součin polynomů lineárních $6 \cdot (x + 2) \cdot (x - \frac{1}{2}) \cdot (x + \frac{2}{3}) = 0$ lze snadno řešit. Řešením jsou přesně ty hodnoty, které po dosazení za x vynulují některou ze závorek.

Základní věta algebry nám vlastně říká, že stejně jako každé přirozené číslo lze rozložit na součin prvočísel, i každý polynom stupně n lze rozložit na součin vedoucího koeficientu a jednoduchých lineárních polynomů typu $(x - x_i)$.

Definice 32 *Kořen* c *polynomu* $p(x)$ *se nazývá k-násobný, jestliže v rozkladu* $p(x)$ *na součin lineárních polynomů podle základní věty algebry se vyskytuje* $(x - c)^k$ *(závorka* $(x - c)$ *je umocněna právě na mocninu* k*).*

Příklad 27 *Polynom* $2x^9 + 14x^8 - 4x^7 - 92x^6 + 130x^5 - 50x^4$ *lze rozložit na tvar*

$$2 \cdot (x - 0)^4 \cdot (x - 1)^3 \cdot (x + 5)^2.$$

Věta 30 *Pro derivaci* $p'(x)$ *polynomu* $p(x)$ *platí, že jestliže kořen* k *je kořenem násobnosti* 4 *polynomu* $p(x)$*, tak je kořen* k *kořenem násobnosti* 3 *(o jednu jednotku menším) polynomu* $p'(x)$*. Jestliže kořen* l *polynomu* $p(x)$ *je násobnosti* 1*, tak* l *není kořenem polynomu* $p'(x)$ *(násobnost nula u kořene znamená, že dané číslo není vůbec kořenem daného polynomu).*

Ad příklad 27: Derivací polynomu $p(x)$ z příkladu 27 dostaneme

$$p'(x) = 2 \cdot x^3 \cdot (x - 1)^2 \cdot (x + 5) \cdot (9x^2 + 29x - 20).$$

V polynomu p' jsou oproti polynomu p dva nové kořeny, jejichž přesnou hodnotu dostaneme z poslední závorky – ale u kořenů, které má p' stejné jako p, se násobnost snížila u všech o jednu jednotku.

Klíčovou otázkou zůstává, jakým způsobem zjišťujeme, jaká čísla máme dosadit do Hornerova schématu. Docela dobrou odpověď na tuto otázku dává:

Věta 31 *Věta o racionálních kořenech polynomu: Jestliže polynom* $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in Z[x]$ *má nějaké kořeny ve tvaru zlomku* $\frac{k}{l}$*, tak* $k|a_0 \wedge l|a_n$.

Tato věta nám pomůže najít všechny racionální kořeny:
Vypíšeme si všechny dělitele čísla a_0, všechny dělitele čísla a_n a vytvoříme z nich zlomky. Tyto zlomky zkusíme užít jako vstupy do Hornerova schématu - tyto zlomky mohou i nemusí být kořenem polynomu, ale máme jistotu, že žádná další racionální čísla zkoušet nemusíme.

Pozor na to, že postup funguje jen tehdy, když všechny koeficienty a_i, nejen první a poslední, jsou celočíselné.

Příklad 28 *Řešte rovnici* $2x^5 + x^4 - 12x^3 - 20x^2 - 19x - 6 = 0$

6 má dělitele $\pm 1, \pm 2, \pm 3, \pm 6$
2 má dělitele $\pm 1, \pm 2$
$\Rightarrow$ Pokud existuje kořen ve tvaru zlomku, musí být obsažen v množině $\{\pm 1, \pm\frac{1}{2}, \pm 2, \pm 3 \pm \frac{3}{2}, \pm 6\}$

Zkusme postupně některé z nich:

	2	1	−12	−20	−19	−6	
$\frac{1}{2}$	2	2	−11	...	...	...	zde se nezdá, že by na konci řádku vyšla 0
$\frac{-1}{2}$	2	0	−12	−14	−12	$\underline{0}$	

Jakmile jsme našli jedno řešení, díváme se už dál na polynom vzniklý jako podíl a vidíme, že všechny koeficienty jsou sudé, takže vytýkáme 2:

$2x^5 + x^4 - 12x^3 - 20x^2 - 19x - 6 = 0$

$(x + \frac{1}{2}) \cdot (2x^4 - 12x^2 - 14x - 12) = 0$

$2 \cdot (x + \frac{1}{2}) \cdot (x^4 - 6x^2 - 7x - 6) = 0$

A dále už pracuji s polynomem $x^4 - 6x^2 - 7x - 6$. Opět proto použiji postup pro racionální kořeny polynomu a získávám, že další potenciální kořen musí být, pokud je racionální, z množiny $\{\pm 1, \pm 2, \pm 3, \pm 6\}$:

	1	0	−6	−7	−6	
3	1	3	3	2	$\underline{0}$	znovu přepočítáme a zjistíme, že potenciální kořeny jsou $\pm 1, \pm 2$
1	...	...	...	...		není kořen
−1	...	...	...	...		není kořen
2	...	...	...	...		není kořen
−2	1	1	1	$\underline{0}$		

Zase si vše napišme jako součin závorek: $2 \cdot (x + \frac{1}{2}) \cdot (x - 3) \cdot (x + 2) \cdot (x^2 + x + 1) = 0$. Dílčí polynom $x^2 + x + 1$ má komplexní kořeny, jak lze snadno zjistit, a všechny

kořeny lze tedy přehledně zapsat při úpravě ponynomu do tvaru užitého v základní větě algebry:

$$2 \cdot (x + \frac{1}{2}) \cdot (x - 3) \cdot (x + 2) \cdot (x + (\frac{1}{2} + i\frac{\sqrt{3}}{2})) \cdot (x + (\frac{1}{2} - i\frac{\sqrt{3}}{2})) = 0.$$

Poznámka: Možnost nalezení kořene s vyšší násobností nám napovídá, abychom např. při užití Hornerova schématu nezapomněli na možnost užít znovu stejné číslo. Například při řešení rovnice $x^5 - 15x^3 + 10x^2 + 60x - 72 = 0$ zkoušíme marně ± 1, ale při dosazení $c = 2$ dostaneme:

	1	0	−15	10	60	−72	
2	1	2	−11	−12	36	0	a hned dosadíme 2 ještě jednou
2	1	4	−3	−18	0		
2	1	6	9	0			všechny koeficienty jsou kladné, tj. eventuální
−3	1	3	0				další řešení musí být záporné
−3	1	0					

Tedy po rozkladu získáváme $(x - 2)^3 \cdot (x + 3)^2 = 0$.

B) Odstranění násobných kořenů polynomu: Tento postup využívá derivace $p'(x)$ a toho, že zderivováním se násobnost každého kořene sníží o 1.

Věta 32 *Vydělíme-li polynom $p(x)$ polynomem $d(x) = NSD(p, p') =$ největší společný dělitel polynomů p, p', dostaneme polynom $v(x)$, který má přesně stejné kořeny jako $p(x)$, ale jsou všechny pouze jednonásobné. Tedy postup $p(x) \to v(x)$ umožňuje snížit stupeň polynomu dříve, než začneme hledat jeho kořeny.*

Pokud $p(x)$ žádné vícenásobné kořeny nemá, $d(x) = NSD(p, p') = 1$, takže $v(x) = p(x)$, polynom $p(x)$ se při převodu na $v(x)$ vůbec nezmění.

Příklad 29 *Při řešení rovnice $16x^4 + 32x^3 + 40x^2 + 24x + 9 = 0$ bychom pomocí Hornerova schématu zjistili, že žádné racionální řešení neexistuje. Zkusme tedy algoritmus odstranění násobných kořenů:*

$p(x) = 16x^4 + 32x^3 + 40x^2 + 24x + 9$
$p'(x) = 64x^3 + 96x^2 + 80x + 24$

Hledejme NSD těchto polynomů Euklidovým algoritmem (rozepsán v Základech matematiky pro přirozená čísla, ale funguje stejně dobře i pro polynomy a jejich rozklad na součin lineárních polynomů do tvaru uvedeného v základní větě algebry):

$(16x^4 + 32x^3 + 40x^2 + 24x + 9) : (64x^3 + 96x^2 + 80x + 24) = \frac{1}{4}x + \frac{1}{8}$
$-(16x^4 + 24x^3 + 20x^2 + 6x)$
$8x^3 + 20x^2 + 18x + 9$
$-(8x^3 + 12x^2 + 10x + 3)$
$8x^2 + 8x + 6$

$$(64x^3+96x^2+80x+24):(8x^2+8x+6)=8x+4$$
$$\underline{-(64x^3+64x^2+48x)}$$
$$32x^2+32x+24$$
$$\underline{-(32x^2+32x+24)}$$
$$0$$

Tedy $d(x) = NSD =$ *poslední nenulový zbytek tohoto procesu* $= 8x^2+8x+6$. *Pak:*

$$v(x)=p(x):d(x)=(16x^4+32x^3+40x^2+24x+9):(8x^2+8x+6)=2x^2+2x+\tfrac{3}{2}$$
$$\underline{-(16x^4+16x^3+12x^2)}$$
$$16x^3+28x^2+24x+9$$
$$\underline{-(16x^3+16x^2+12x)}$$
$$12x^2+12x+9$$
$$\underline{-(12x^2+12x+9)}$$
$$0$$

Tedy rovnici lze psát ve tvaru $(8x^2+8x+6)\cdot(2x^2+2x+\frac{3}{2})=0$

$$(4x^2+4x+3)\cdot(4x^2+4x+3)=0$$
$$(4x^2+4x+3)^2=0$$

$x_{1,2}=\frac{-4\pm\sqrt{16-48}}{8}$
$x_1=\frac{-1}{2}+i\frac{\sqrt{2}}{2}$ *... kořen násobnosti* 2 $\quad x_2=\frac{-1}{2}-i\frac{\sqrt{2}}{2}$ *... kořen násobnosti* 2
Celkem lze tedy náš polynom $16x^4+32x^3+40x^2+24x+9$ *rozložit a řešit rovnici ve tvaru:* $16\cdot(x+\frac{1}{2}+i\frac{\sqrt{2}}{2})^2\cdot(x+\frac{1}{2}-i\frac{\sqrt{2}}{2})^2=0$ *... algebraický rozklad dané rovnice v komplexním oboru.* $\star$

C) Polynom $p(x)\in R[x]$ musí mít komplexní kořeny „po dvojicích“ ve tvaru $a\pm i\cdot b$:

Věta 33 *Pokud* $c_1=a+i\cdot b$ *je kořenem polynomu* $p(x)\in R[x]$ *(tj. polynomu s reálnými koeficienty), nutně z toho plyne, že i komplexní číslo* $c_2=a-i\cdot b$ *je kořenem téhož polynomu. Čísla* $a\pm i\cdot b$ *se nazývají komplexně sdružená.*

Důkaz této skutečnosti budu po vás chtít – viz video.

Příklad 30 *Při řešení polynomické rovnice* $x^6+x^5+x^4+x^3+x^2+x+1=0$ *projdeme právě popsané kroky A,B,C a zjistíme:*

A) žádné racionální kořeny tohoto polynomu neexistují; B) násobné kořeny tento polynom nemá, všechny jeho kořeny jsou navzájem různé; C) jestliže má polynom komplexní kořeny, budou se u polynomu vyskytovat ve dvojicích komplexně sdružených čísel.

Tuto rovnici vyřešíme jako vedlejší produkt jistých úvah za 14 dní (za dvě přednášky).

Příklad 31 *Věta 33 neplatí pro polynomy, jejichž koeficienty jsou komplexní, tedy polynomy* $p(x)$*, které napatří do množiny* $R[x]$*: příklad viz video.*

8.2 Cvičení 08: Polynomy 03

Dodělání osnovy na cvičení pro polynomy, viz plán cvičícího.

9 Týden 09

9.1 Přednáška 09: Polynomické rovnice – numerické metody

Příklad 32

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

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

Ad A) Hornerovým schématem lze ověřit, že žádné racionální řešení neexistuje. Ad B) Proces odstranění násobných kořenů polynomu na levé straně rovnice nenajde žádný kořen násobnosti větší než 1. Všechna řešení tedy jsou reálná iracionální, nebo komplexní. Ad C) Polynom má reálné koeficienty – tedy při existenci komplexního kořene víme, že i komplexně sdružené číslo je kořenem, tj. komplexní kořeny se zde budou vyskytovat ve „zpřízněných dvojicích".

Jaké další možnosti máme pro řešení této rovnice? Jaké metody? Pokračujme v označení metod z minulé přednášky, tj. následuje metoda či úvaha D:

D) Geometrický názor v komplexní rovině: (Budínová, str. 29, věta 16): Všechny kořeny polynomu $p(x)$ leží v komplexní rovině uvnitř kružnice se středem v počátku a poloměrem

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

Dosazením do uvedeného vzorce v našem příkladu máme

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

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

E) Geometrický názor pro $p(x) \in R[x]$: Nakreslíme graf funkce $p(x)$ a sledujeme, kde graf protne osu x, v takovém průsečíků c totiž platí $p(c) = 0$, tj. reálné číslo c je řešením rovnice $p(x) = 0$. Z předcházejícího bodu D navíc víme, že jestliže reálné řešení c existuje, tak $c \in \langle -6{,}5; 6{,}5\rangle$. Když si v grafickém kalkulátoru nakreslíme graf funkce $p(x)$ zjistíme, že se jedná o spojitou křivku, která třikrát protne osu x na daném intervalu. Tyto průsečíky s osou x jsou právě tři různá reálná řešení x_1, x_2, x_3.

Z faktu, že průsečíky jsou jen 3 dále plyne, že čtvrté a páté řešení jsou komplexně sdružená čísla $x_{4,5} = a \pm ib$, kde a, b zatím neznáme.

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

$p(-6)$, $p(-5)$, $p(-4), \ldots, p(0), \ldots, p(4)$, $p(5)$, $p(6)$.

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

Zkusme tedy postupně za x dosazovat hodnoty z intervalu $\langle -6{,}5; 6{,}5 \rangle$ s krokem $0,5$ a počítat funkční hodnoty: $p(-6,5) = -15598,25$; $p(-6) = -9865$; $p(-5,5) = -5908,875$; $p(-5) = -3290$; $p(-4,5) = -1646,5$; $p(-4) = -687$; $p(-3,5) = \underline{-183,125}$; $p(-3) = \underline{38}$; $p(-2,5) = 101,25$; $p(-2) = 91$; $p(-1,5) = \overline{58,625}$; $p(-1) = 30$; $p(-0,5) = 13$; $p(0) = 5$; $p(0,5) = \underline{0,375}$; $p(1) = \underline{-2}$; $p(1,5) = \underline{8,75}$; $p(2) = 63$ ... další funkční hodnoty jsou už všechny kladné.

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

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

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

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

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

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

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

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

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

Příklad 33 *Pozor ovšem na polynom s násobnými kořeny: Jestliže bychom řešili rovnici*

$$x^4 - (2\sqrt{2} + 2\sqrt{3})x^3 + (5 + 4\sqrt{6})x^2 - (4\sqrt{3} + 6\sqrt{2})x + 6 = 0$$

tak, že bychom se snažili počítat funkční hodnoty $p(0)$, $p(1)$, $p(2)$, tak by všechny byly kladné, protože graf polynomu v kořenu sudé násobnosti $x_{1,2} = \sqrt{2} \doteq 1{,}41$ nebo $x_{3,4} = \sqrt{3} \doteq 1{,}73$ se od osy x „odrazí“ na tutéž stranu, opět do kladných hodnot (obrázek viz video) a právě popsaná metoda E intervaly obsahující řešení nenajde.

Tedy je důležité nejprve z polynomu odstranit případné násobné kořeny a řešit rovnici $q(x) = 0$, kde polynom $q(x)$ má tytéž kořeny jako $p(x)$, ale jednonásobné (viz oddíl B).

F1) Dohledání řešení metodou půlení intervalu: Vycházíme ze situace, kdy rovnice $p(x) = 0$ má na intervalu $\langle a; b\rangle$ právě jedno řešení a $p(x)$ je spojitá funkce a platí $p(a) < 0; p(b) > 0$ nebo $p(a) > 0; p(b) < 0$. (a toto řešení je kořenem polynomu na levé straně rovnice, jehož násobnost je lichá – viz právě uvedený příklad 33)

a) Najdeme střed intervalu $\langle -3{,}5; -3\rangle$ podle vzorce $x_1 = \frac{a+b}{2}$, tj. $x_1 = -3,25$.

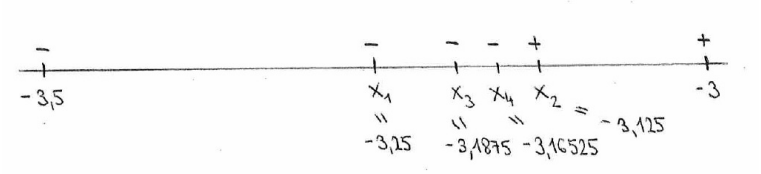
b) V tomto bodě $x_1 = -3,25$ spočteme funkční hodnotu $p(-3,25) = -46,06055$ - důležité je to, že je záporná. V další fázi z intervalů $\langle -3{,}5; -3{,}25\rangle$, $\langle -3{,}25; -3\rangle$ vybereme jako $\langle a_1; b_1\rangle$ interval $\langle -3{,}25; -3\rangle$, protože v krajních bodech jsou rozdílná znaménka funkčních hodnot, záporné a kladné, tj. řešení leží na tomto intervalu.

c) Najdeme střed $x_2 = \frac{a_1+b_1}{2} = \frac{-3,25-3}{2} = -3,125$, pak $p(-3,125) > 0$. Tedy jako $\langle a_2; b_2\rangle$ volíme $\langle -3{,}25; -3{,}125\rangle$, protože $p(-3,25) < 0, p(-3,125) > 0$, tj, řešení leží v tomto intervalu.

d) Najdeme střed $x_3 = \frac{a_2+b_2}{2} = \frac{-3,25-3,125}{2} = -3,1875$, pak $p(-3,1875) < 0$. Tedy jako $\langle a_3; b_3\rangle$ volíme $\langle -3{,}1875; -3{,}125\rangle$.

e) Najdeme střed $x_4 = \frac{a_3+b_3}{2} = \frac{-3,1875-3,125}{2} = -3,16525$, pak $p(-3,16525) < 0$. Tedy jako $\langle a_4; b_4\rangle$ volíme $\langle -3{,}16525; -3{,}125\rangle$.

f) Atd. po dalších deseti krocích $x_15 \doteq -3,12991$. A to je bod, který pokládáme za řešení $z_1 \doteq -3,12991$.



Metoda půlení intervalu tedy spočívá v tom, že výchozí interval dělíme na poloviny, vybranou polovinu zase na poloviny atd. a pro další dělení vybíráme vždy tu

polovinu, v jejíž krajních bodech má polynom $p(x)$ opačná znaménka funkčních hodnot, což znamená, že tato polovina obsahuje řešení.

Celý algoritmus jsme zastavili asi po 15 krocích, kdy už délka intervalu $\langle a_{14}; b_{14}\rangle$ byla menší než $0,00001$, tedy je jasné, že jeho střed x_{15} je spočítán zhruba s přesností na pět desetinných míst.

Tentýž algoritmus půlení intervalu použijeme i na další dva hrubě vymezené intervaly $\langle 0{,}5; 1\rangle$ a $\langle 1; 1{,}5\rangle$ a dostaneme další dvě řešení: $z_2 = 0,54689$ a $z_3 = 1,22892$.

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

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

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

$$a < - - 3.5$$

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

$$b < - - 3$$

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

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

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

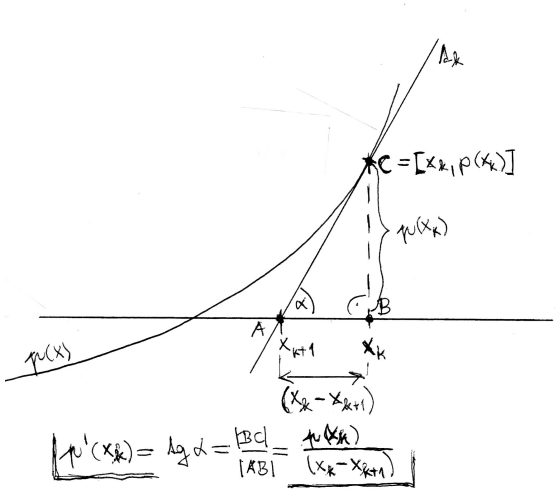
Pokud celý postup (posloupnost tří kroků ukončených ENTER) zopakujeme pouze pro volbu $a = 0{,}5$, $b = 1$, najdeme řešení $z_2 = 0{,}54689$. Toho lze dosáhnout velmi jednoduše, protože v prostředí R nemusíme už jednou napsané příkazy vypisovat znovu, ale volbou šipky nahoru se lze dostat na předchozí tři příkazy, ve kterých pozměníme pouze hodnoty a, b a celý cyklus while beze změny ještě jednou potom zobrazíme šipkou nahoru a stiskneme ENTER.

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

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

Nevýhoda metody půlení intervalu spočívá v tom, že je velmi pomalá, pokud nepoužijeme počítač - na zpřesnění o jedno desetinné číslo potřebujeme zhruba tři kroky. Hledáme-li metodu, která je i za použití pouze kalkulačky značně rychlejší, můžeme použít metodu Newtonovu.

F2) Dohledání řešení metodou Newtonovou = metodou tečen: S velmi rychlou metodou přišel Izák Newton: využil při tom pojem tečny ke grafu funkce:



a) Zvolíme bod x_0 vhodně blízko našeho řešení.

b) Sestavujeme posloupnost bodů $x_1, x_2, x_3, \ldots$ podle klíče: vedeme tečnu ke grafu $p(x)$ v bodě $[x_k, p(x_k)]$ a tam, kde tato tečna protne osu x, bude ležet x_{k+1}. Nyní dvojím vyjádřením tangenty úhlu α, jednou pomocí derivace a podruhé pomocí pravoúhlého trojúhelníka ABC, viz obrázek, dostaneme

$$p'(x_k) = \operatorname{tg} \alpha = \frac{p(x_k)}{x_k - x_{k+1}}$$

a když odtud vyjádříme x_{k+1}, dostaneme

$$x_{k+1} = x_k - \frac{p(x_k)}{p'(x_k)}.$$

V našem příkladu by měl vzorec tvar:

$$x_{k+1} = x_k - \frac{2x_k^5 + 3x_k^4 - 7x_k^3 + 6x_k^2 - 11x_k + 5}{10x_k^4 + 12x_k^3 - 21x_k^2 + 12x_k - 11}$$

Ukazuje se, že se zbavíme znaménka MINUS před zlomkem a ušetříme několik operací, když rozdíl na pravé straně převedeme na společného jmenovatele:

$$x_{k+1} = \frac{10x_k^5 + 12x_k^4 - 21x_k^3 + 12x_k^2 - 11x_k - (2x_k^5 + 3x_k^4 - 7x_k^3 + 6x_k^2 - 11x_k + 5)}{10x_k^4 + 12x_k^3 - 21x_k^2 + 12x_k - 11}.$$

$$x_{k+1} = \frac{8x_k^5 + 9x_k^4 + 28x_k^3 + 6x_k^2 - 5}{10x_k^4 + 12x_k^3 - 21x_k^2 + 12x_k - 11}$$

A tento vzorec použijeme v našem příkladu.

$z_1 \in \langle -3{,}5; -3\rangle$: Volme $x_0 = -3,5$:

$x_1 = \frac{8(-3,5)^5+9(-3,5)^4+28(-3,5)^3+6(-3,5)^2-5}{10(-3,5)^4+12(-3,5)^3-21(-3,5)^2+12(-3,5)-11} = -3,229055$

$x_2 = \frac{-8{\cdot}3,229055^5+9{\cdot}3,229055^4-28{\cdot}3,229055^3+6{\cdot}3,229055^2-5}{10{\cdot}3,229055^4-12{\cdot}3,229055^3-21{\cdot}3,229055^2-12{\cdot}3,229055-11} = -3,139302$

$x_3 = \frac{-8{\cdot}3,139302^5+9{\cdot}3,139302^4-28{\cdot}3,139302^3+6{\cdot}3,139302^2-5}{10{\cdot}3,139302^4-12{\cdot}3,139302^3-21{\cdot}3,139302^2-12{\cdot}3,139302-11} = -3,130003$

$x_4 = \frac{-8{\cdot}3,130003^5+9{\cdot}3,130003^4-28{\cdot}3,130003^3+6{\cdot}3,130003^2-5}{10{\cdot}3,130003^4-12{\cdot}3,130003^3-21{\cdot}3,130003^2-12{\cdot}3,130003-11} = -3,129909 \doteq \underline{\underline{-3,12991}}$

Téhož výsledku jsme Newtonovou metodou dosáhli již po čtyřech krocích!

$z_2 \in \langle 0{,}5; 1\rangle$: Volbou $x_0 = 0,5$ dostaneme už po dvou krocích $x_2 \doteq z_2 = \underline{\underline{0,54689}}$.

$z_3 \in \langle 1; 1{,}5\rangle$: Volbou $x_0 = 1,5$ dostaneme po čtyřech krocích $x_4 \doteq z_3 = \underline{\underline{1,22892}}$.

Slabina Newtonovy metody: Někdy sestrojená posloupnost bodů x_0, x_1, $x_2, \ldots$ nemusí se blížit k řešení – například když tečna v daném bodě x_k „vystřelí“ průsečík x_{k+1} dále od řešení, místo aby to bylo blízko ... nebo když tečna je rovnoběžná s osou x, bod x_{k+1} vůbec neexistuje! Oba tyto trable lze zpravidla vyřešit tím, že zvolíme bod x_0 jinak, aby byl dost blízko řešení ... zkoušením volby různých počátečních x_0 pro Newtonovu metodu se zpravidla ve většině případů lze dobrat k řešení, i když některé volby počátečního x_0 selhaly.

Silná stránka Newtonovy metody: jestliže konverguje, tak konverguje velmi rychle, jeden krok zpravidla vyspraví v hledaném řešení jedno až dvě desetinná místa.

Velkou předností Newtonovy metody je to, že najde i komplexní řešení! Musíme ovšem počáteční x_0 volit komplexní s nenulovou imaginární částí, jelikož metoda se sama od sebe do komplexních čísel nedostane.

Zkusme určit dvojici komplexně sdružených řešení v našem příkladu: $2x^5 + 3x^4 - 7x^3 + 6x^2 - 11x + 5 = 0$

Víme, že $|z_4| < 6,5$, $|z_5| < 6,5$, takže budeme volit jako x_0 různá komplexní čísla s velikostí menší, než $6,5$ a vložíme je do Newtonovy metody podle již známého vzorce:

- $x_0 = 1 + i$ ... Po pěti krocích $x_5 \doteq 0,54689$. Posloupnost se blíží k reálnému řešení, které už známe. Nenašli jsme nové řešení s nenulovou imaginární částí.
- $x_0 = 1 + 2i$ ... Po jedenácti krocích $x_{11} \doteq 0,54689$. Posloupnost se blíží k reálnému řešení, které už známe. Nenašli jsme nové řešení s nenulovou imaginární částí.
- $x_0 = 1+3i$ ... Po deseti krocích se dostaneme k $x_{10} \doteq \underline{\underline{-0,07295 + i \cdot 1,08773 \doteq z_4}}$. A protože víme, že druhé komplexní řešení je pouze komplexně sdružené k předchozímu, můžeme bez počítání psát $\underline{\underline{z_5 \doteq -0,07295 - i \cdot 1,08773}}$

Naše rovnice $2x^5 + 3x^4 - 7x^3 + 6x^2 - 11x + 5 = 0$ má tedy tři racionální řešení: $z_1 \doteq -3,12991; z_2 \doteq 0,54689; z_3 \doteq 1,22892$ a dvě komplexní řešení $z_4 \doteq -0,07295 + i \cdot 1,08773; z_5 \doteq -0,07295 - i \cdot 1,08773$.

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

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

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

$$z <- -3.5$$

a ENTER, a provedeme cyklus WHILE:

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

(a ENTER) ... po několika krocích bude nalezeno řešení $z_1 = -3,12991$. Podobně pro vstupní $z_0 = -1$ dostaneme $z_3 = 1,22892$ a pro vstupní $z_0 = 0,5$ dostaneme $z_2 = 0,54689$. Zkusme dále najít zbývající dvě komplexně sdružená řešení:

- Volme vstupní $z = 1+1i$, najeďme šipkou na příkaz cyklu WHILE a stiskněme enter ... dospíváme k řešení $z_2 = 0,54689$ ... to se tedy může stát, že volbou komplexního vstupního z celá posloupnost konstruovaných čísel konverguje k řešení reálnému.

- Zkusme jiné vstupní $z = 1 + 3i$ z našeho kruhu v komplexní rovině $|z| \leq 6{,}5$: dojdeme k řešení $z_4 = -0{,}07295 + i \cdot 1{,}08773$ s přesností na pět desetinných míst, a díky teoretické větě o komplexně sdružených kořenech už nemusíme dále počítat, stačí psát $z_5 = -0{,}07295 - i \cdot 1{,}08773$.

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

G) Řešení **reciproké rovnice**, například $8x^5 - 64x^4 + 100x^3 + 100x^2 - 64x + 8 = 0$:
Pokud polynom na levé straně rovnice je lichého stupně, víme, že jeho řešením bude číslo $x_1 = -1$ (to plyne právě z toho, že reciproké koeficienty jsou stejné, tj. po dosazení $x = -1$ dostaneme na levé straně hodnotu nulovou) – pomocí Hornerova schématu provedeme dělení polynomu polynomem $(x + 1)$, a dostaneme reciprokou rovnici sudého stupně. Tu řešíme pomocí speciální substituce $x + \frac{1}{x} = t$, vysvětlení viz video.

H) Řešení **binomické rovnice** – viz následující přednáška, ve druhé polovině, příklad 37.

9.2 Cvičení 09: Písemka

Písemka se odehraje v termínech určených cvičícím, podle jeho pokynů.

10 Týden 10

10.1 Přednáška 10: Operace s komplexními čísly, mocnina a odmocnina z komplexního čísla

Viz video, zde jen heslovitě: komplexní číslo bývá uváděno většinou v jednom ze tří tvarů: algebraickém tvaru $a+bi$, goniometrickém tvaru $r\cdot(\cos\varphi+i\cdot\sin\varphi)$ nebo exponenciálním tvaru $r\cdot e^{i\cdot\varphi}$.

Příklad 34 *Najděte goniometrický a exponenciální tvar komplexních čísel* $z_1=1+i$, $z_2=\frac{-1}{2}+i\cdot\frac{\sqrt{3}}{2}$.

Příklad 35 *Vypočtěte a znázorněte v komplexní rovině součet a součin komplexních čísel* $z_1=2-i$, $z_2=\frac{\sqrt{2}}{2}+i\cdot\frac{\sqrt{2}}{2}$.

- Sčítání komplexních čísel „se odehrává“ v Gaussově (komplexní) rovině podobně jako sčítání vektorů v reálné rovině R^2.
- Násobení vektorů skalárně – skalární součin vektorů a jeho geometrický význam. Výsledkem skalárního součinu vektorů je číslo!
- Násobení vektorů vektorově – vektorový součin vektorů a jeho geometrický význam (orientace podle pravidla pravé ruky, velikost vektorového součinu vyjadřuje obsah rovnoběžníku určeného oběma vstupními vektory). Výsledkem vektorového součinu vektorů je vektor kolmý na danou rovinu, ovšem vektorům v rovině je potřeba přidat třetí souřadnici, protože vektorový součin má dva vstupní vektory pouze v dimenzi 3.
- Geometrický význam násobení komplexních čísel v komplexní rovině: pro $z_1=r_1\cdot(\cos\varphi_1+i\cdot\sin\varphi_1)$ a $r_2\cdot(\cos\varphi_2+i\cdot\sin\varphi_2)$ jejich součin má tvar

  $$z_1\cdot z_2=r_1\cdot r_2\cdot(\cos(\varphi_1+\varphi_2)+i\cdot\sin(varphi i_1)+\varphi_2).$$

  (obraz součinu $z_1\cdot z_2$ leží na kružnici o poloměru $r_1\cdot r_2$ a jeho argument (určující úhel) je roven součtu obou dílčích argumentů).

Podobně součin čísel $z_1=1+i$, $z_2=\frac{\sqrt{3}}{2}+\frac{1}{2}\cdot i$.

Poznámka: Co je množina $(C,+,\cdot)$ algebraicky? Těleso, zdůvodnění viz video.

Věta 34 *Moivreho věta: viz video.*

Příklad 36 $(1+i)^8=\dots$,

$(1+i\cdot\sqrt{3})^5=\dots$

H) Řešení **binomické rovnice** – viz následující věta a příklad. Velmi speciální polynomická rovnice, kde na levé straně je binom = dvojčlen.

Věta 35 *n-tá odmocnina z komplexního čísla: viz video.*

Příklad 37 *Vyřešte rovnice:*

- *a) vyřešte binomickou rovnici* $z^4 + 1 = 0$.
- *b) vyřešte binomickou rovnici* $z^6 - 64 = 0$.
- *c) vyřešte rovnici* $z^6 + z^5 + z^4 + z^3 + z^2 + z + 1 = 0$.

10.2 Cvičení 10: Komplexní čísla 01

Odehraje se podle pokynů cvičícího.

11 Týden 11

11.1 Přednáška 11: Konstrukce číselných oborů

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

Zbývají poslední dvě přednášky, ve kterých se bude částečně jednat o opakování některých pojmů, ovšem některé informace budou ještě nové.

11.1.1 Peanova množina

Začneme vysokoškolským pohledem na přirozená čísla: Co jsou to přirozená čísla? Jaké jsou axiomy struktury přirozených čísel?

Půjde o trochu jiný pohled, než jen tvrzení, že $(N_0, +, \cdot)$ je polookruh. Jedná o ještě trochu elementárnější pohled, na kterém je struktura polookruh vybudována.

Co to je Peanova množina? Množina, na které platí

A) triviální čtyři axiomy o rovnosti (viz video);

B) netriviální čtyři až pět axiomů o pojmu následník:

1. $\forall x \in P \; \exists$ tzv. následník prvku x, který označujeme jako $x' \in P$.
2. $\exists \, e \in P$: e není následníkem žádného prvku množiny P.
3. $\forall x, y \in P : x \neq y \Rightarrow x' \neq y'$ (následníci různých prvků jsou různé).
4. Jestliže pro podmnožinu $M \subseteq P$ platí:
   a) $e \in M$
   b) $\forall x \in P : x \in M \Rightarrow x' \in M$
   tak $\Rightarrow M = P$.

Tyto čtyři axiomy platí na množině přirozených čísel N:

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

Ad 2) 1 není následníkem žádného přirozeného čísla.

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

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

tak tímto způsobem projdeme celou množinu N. Kdybychom kromě procházení množiny N u každého přirozeného čísla ještě ověřili nějakou vlastnost, která pro ně platí, tak vlastně provádíme důkaz matematickou indukcí - struktura axiomu 4 je tedy velmi

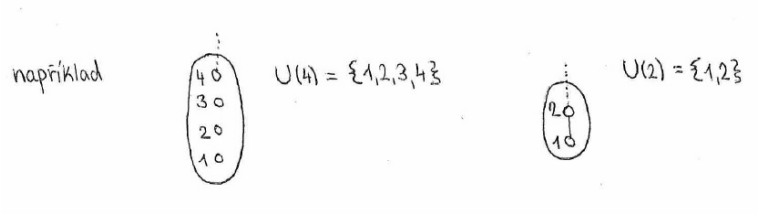
podobná struktuře důkazu matematickou indukcí.

Ještě je důležité říci, že:

Věta 36 *N je až na izomorfismus jediným modelem struktury zvané Peanova množina.*

C) Definujme na Peanově množině uspořádání: relaci $\leq$ definujeme na P následovně:

- Lze dokázat, že na Peanově množině, pokud $x \neq e$, existuje $u \in P : u' = x$. Tj. všechny prvky krome e mají nějaký prvek, jehož jsou následníkem. Tento prvek nazveme předchůdce prvku x a označíme $'x = u$.
- Lze definovat $U(a) =$ úsek Peanovy množiny příslušný prvku $a \in P$ takto:
  1) $a \in U(a)$
  2) $x \in U(a) \Rightarrow 'x \in U(a)$, pokud tedy $'x$ existuje



  (Zkrátka $U(a)$ vytvoříme pomocí prvku a a všech možných předchůdců, které lze najít.)
- Pomocí pojmů předchůdce a úsek Peanovy množiny lze nyní definovat relaci uspořádání $\leq$ takto: $a \leq b$, když $a \in U(b)$.

Tímto způsobem jsme jasně definovali uspořádání jen pomocí pojmů následník/předchůdce a pomocí pojmu podmnožina.

D) ještě krátce k operacím sčítání a násobení na Peanově množině:

Věta 37 *Dále lze pomocí Peanových axiomů a pomocí právě definovaného uspořádání jejích prvků definovat operace sčítání i násobení tak, že platí:*

a) $x + e = x'$;

b) $x + y' = (x + y)'$;

c) $x \cdot e = x$;

d) $x \cdot y' = xy + x$.

11.1.2 Nástin této a následující přednášky intuitivně

To, co bude nyní následovat, bude pokusem o podobnou elementární „konstrukci“ množin Z, Q, R a nakonec i C. Intuitivně ovšem budeme vědět, jaké vlastnosti daná struktura, kterou vytvářet chceme, má mít, protože jsme je procházeli v první polovině tohoto předmětu.

- a) $(Z, +, \cdot)$ vytvoříme ze struktury $(N, +, \cdot)$ dodáním:
  - 0 jako neutrálního prvku vzhledem ke sčítání,
  - záporných čísel jako inverzích prvků vzhledem ke sčítání.

  Dostaneme tak strukturu $(Z, +, \cdot)$, která je obor integrity, tj.
  - $(Z, +)$ je komutativní grupa
  - $(Z^*, \cdot)$ je komutativní monoid ($Z^* = Z - \{0\}$)
  - platí distributivní zákon $a \cdot (b + c) = ab + ac \quad \forall a, b, c \in Z$
  - $a \cdot b = 0$ platí pro $a = 0$ nebo $b = 0$

- b) $(Q, +, \cdot)$ vytvoříme ze struktury $(Z, +, \cdot)$ dodáním inverzních prvků vzhledem k násobení (až na inverzní prvek k 0, který nedodáváme a spokojíme se s tím, že neexistuje).

  Dostaneme tak strukturu $(Q, +, \cdot)$, která je tělesem, tj.
  - $(Q, +)$ je komutativní grupa
  - $(Q^*, \cdot)$ je komutativní grupa
  - platí distributivní zákon $a \cdot (b + c) = ab + ac \quad \forall a, b, c \in Q$

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

- c) $(R, +, \cdot)$ vytvoříme ze struktury $(Q, +, \cdot)$ dodáním tzv. iracionálních čísel. Vznikne struktura $(R, +, \cdot)$, která je také tělesem.

- d) $(C, +, \cdot)$ vytvoříme ze struktury $(R, +, \cdot)$ dodáním tzv. imaginární jednotky i, pro kterou platí $i^2 = -1$. Vznikne struktura $(C, +, \cdot)$, která je také tělesem.

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

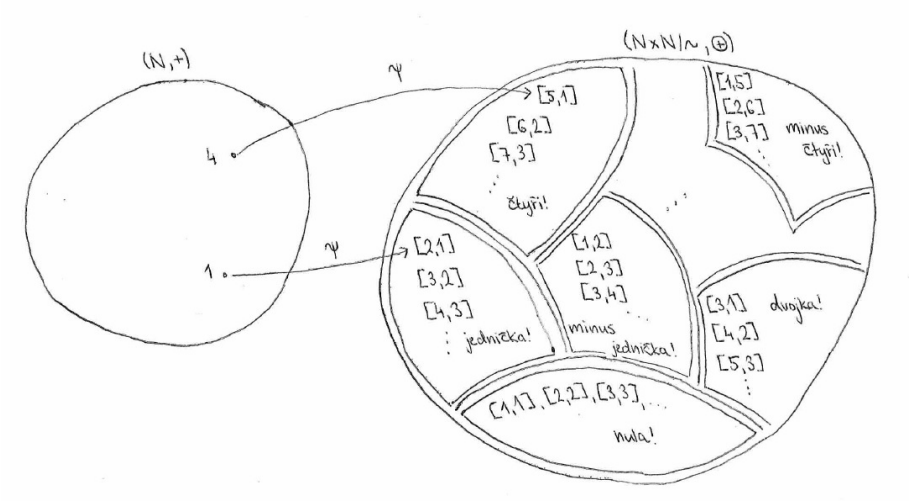
Další poznámka: Odčítání a dělení nepovažujeme na této úrovni za další operace na dané množiny, nýbrž odčítání prvku/čísla je vlastně jen přičtení „opačného čísla“ = inverze vzhledem k $+$, dělení nenulovým prvkem/číslem je vlastně jen násobení „inverzí“

vzhledem k $\cdot$.

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

11.1.3 Konstrukce $N \to Z$

Věta 38 *Komutativní pologrupu $(N, +)$ lze injektivně vnořit do komutativní grupy (= rozšířit na grupu) $Z := (N \times N/_\sim, \oplus)$.*



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

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

Zdůvodněme pořádně, že relace $\sim$ je reflexivní, symetrická, tranzitivní:

Relace $\sim$ je reflexivní: $[a; b] \sim [a; b]$ ... ano, protože $a + b = b + a$ ... plyne z komutativity sčítání v pologrupě $(N, +)$.

Relace $\sim$ je symetrická: $[a; b] \sim [c; d] \overset{?}{\Rightarrow} [c; d] \sim [a; b]$. Ano, implikace platí, důkaz přímý: jestliže $a + d = b + c$, pak i $c + b = d + a$ (pouze na základě komutativity sčítání na původní množině N), a to podle definice znamená, že $[c; d] \sim [a; b]$.

Relace $\sim$ je tranzitivní: $[a; b] \sim [c; d] \wedge [c; d] \sim [e; f] \overset{?}{\Rightarrow} [a; b] \sim [e; f]$. Ano, implikace platí, důkaz přímý: Z faktu $[a; b] \sim [c; d]$ plyne, že $a + d = b + c$; z faktu $[c; d] \sim [e; f]$ plyne, že $c + f = d + e$. Sečtením obou rovností dostaneme

$$a + (d + c) + f = b + (c + d) + e.$$

V závorce na každé straně přičítáme (s využitím komutativity sčítání) totéž přirozené číslo – kdybychom je nepřičetli, rovnost též platí, tj. $a + f = b + e$ ... a to podle definice relace $\sim$ znamená, že $[a; b] \sim [e; f]$, zdůvodnění implikace je hotovo.

iii) Vytvořme faktormnožinu $N \times N/_\sim$, jejímiž prvky jsou podmnožiny určené danou ekvivalencí.

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

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

O takto definované operaci sčítání podmnožin musíme nejprve ukázat, že nezávisí na výběru reprezentanta z dané podmnožiny: $M_1 := \{[a;b];[e;f];\dots\}$, $M_2 := \{[c;d];[g;h];\dots\}$ ... musíme dokázat, že $\{[a,b]\} \oplus \{[c,d]\} = \{[e,f]\} \oplus \{[g,h]\}$:

Využijeme toho, že $[a;b] \in M_1$; $[e;f] \in M_1$, tj. $a+f = b+e$ (rovnice 1); a toho, že $[c;d] \in M_2$; $[g;h] \in M_2$, tj. $c+h = d+g$ (rovnice 2): Pak

$$\{[a,b]\} \oplus \{[c,d]\} := \{[a+c, b+d]\}; \quad \{[e,f]\} \oplus \{[g,h]\} := \{[e+g, f+h]\}$$

Nyní potřebujeme ukázat, že tyto dva různé výsledky, $\{[a+c, b+d]\}$ i $\{[e+g, f+h]\}$ leží ve stejné podmnožině rozkladu, tj. že platí $a+c+f+h = b+d+e+g$ ... a to skutečně platí, protože tuto rovnost dostaneme sečtením rovnice 1 a rovnice 2, z jejichž platnosti jsme vyšli.

Tedy operace $\oplus$ je na množině $N \times N/_\sim$ korektně definovaná; má tedy smysl zkoumat její algebraické vlastnosti:

(1) Uzavřenost plyne z uzavřenosti „staré operace“ + v jednotlivých souřadnicích = složkách. (viz video)

(2) Asociativita $\oplus$ plyne ze „staré“ asociativity operace + v jednotlivých souřadnicích = složkách. (viz video)

(3) Neutrálním prvkem je třída $\{[1,1]\}$, což je třída obsahující prvky $[1,1], [2,2], [3,3], \dots$ (viz video)

(4) Např. pro $\{[6,2]\}$ je inverzí $\{[2,6]\}$. Obecně (viz video) pro $\{[a,b]\}$ je inverzí $\{[b,a]\}$

(5) Operace $\oplus$ je komutativní ... ukáže se lehce, podobně jako předchozí vlastnosti – a plyne vlastně z komutativity sčítání obyčejného na množině N.

$\Rightarrow$ Tedy $(N \times N/_\sim, \oplus)$ je komutativní grupa!

v) Zobrazení ψ definujeme vztahem $\psi(n) = \{[n+1, 1]\}$. Takto definované zobrazení $\psi : N \to N \times N/_\sim$ je injektivní homomorfismus, tedy vnoření $(N, +)$ do struktury $(N \times N/_\sim, \oplus)$.:

a) dokažme nejprve, že ψ je injekce: pro různé vzory $a \neq b$ jsou různé i obrazy $\psi(a) = \{[a+1, 1]\}$ a $\psi(b) = \{[b+1, 1]\}$.

b) a nyní dokažme, že platí vlastnost zachování výsledků operace, tj. $\psi(n_1 + n_2) = \psi(n_1) \oplus \psi(n_2)$: Ano, skutečně, dosaďme do levé a pravé strany rovnosti a zjistíme, že se tyto rovnají:

$L = \psi(n_1 + n_2) = \{[n_1 + n_2 + 1, 1]\};$

$P = \psi(n_1) \oplus \psi(n_2) = \{[n_1 + 1, 1]\} \oplus \{[n_2 + 1, 1]\} = \{[n_1 + n_2 + 2; 2]\}.$

Nyní vidíme, že L i P jsou určeny reprezentanty, které leží v téže podmnožině, tj. $\{[n_1 + n_2 + 1, 1]\} = \{[n_1 + n_1 + 2; 2]\}$, protože podle definice relace $\sim$ platí $n_1 + n_2 + 1 + 2 = n_1 + n_2 + 2 + 1$. Tedy jedná se o dva reprezentanty téže podmnožiny a platí $L = P$.

Celá konstrukce je tedy hotova. Tímto způsobem jsme algebraicky přesně vytvořili jen pomocí přirozených čísel:

- číslo 0 jako $\{[1, 1], [2, 2], [3, 3], [4, 4], \dots\}$

- číslo -4 jako $\{[1, 5], [2, 6], [3, 7], [4, 8], \dots\}$ atd.

a přitom výsledky sčítání přirozených čísel zůstaly v nové struktuře zachovány, to je zajištěno injektivním homomorfismem ψ.

11.2 Cvičení 11: Komplexní čísla 02

Odehraje se podle pokynů cvičícího.

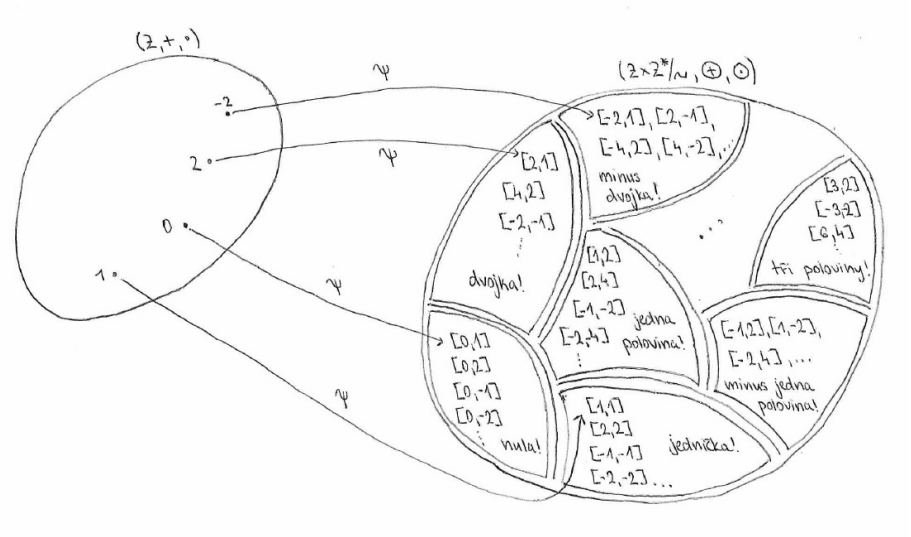
12 Týden 12

12.1 Přednáška 12: Konstrukce oborů Q, R, C

Na této přednášce budeme pokračovat v konstrukcích číselných oborů.

12.1.1 Konstrukce $Z \rightarrow Q$

Věta 39 *Obor integrity* $(Z, +, \cdot)$ *injektivně vnořit do tělesa (= rozšířit na těleso)* $Q := (Z \times Z^*/_\sim, \oplus, \odot)$.



a) Nejprve vytvoříme kartézský součin $Z \times Z^*$, kde $Z^* := Z \setminus \{0\}$.

b) Na $Z \times Z^*$ definujme relaci ekvivalence $\sim$ takto: $[a, b] \sim [c, d]$, když $a \cdot d = b \cdot c$, kde násobení v této rovnici je „starou“ operací násobení v $\cdot$ v $(Z, +, \cdot)$.

O relaci $\sim$ ukažme, že se jedná o relaci reflexivní, symetrickou a tranzitivní:

Relace $\sim$ je reflexivní: $[a; b] \sim [a; b]$ ... ano, protože $a \cdot b = b \cdot a$ ... plyne z komutativity násobení na množině Z.

Relace $\sim$ je symetrická: $[a; b] \sim [c; d] \overset{?}{\Rightarrow} [c; d] \sim [a; b]$. Ano, implikace platí, důkaz přímý: jestliže $a \cdot d = b \cdot c$, pak i $c \cdot b = d \cdot a$ (pouze na základě komutativity násobení na původní množině Z), a to podle definice znamená, že $[c; d] \sim [a; b]$.

Relace $\sim$ je tranzitivní: $[a; b] \sim [c; d] \wedge [c; d] \sim [e; f] \overset{?}{\Rightarrow} [a; b] \sim [e; f]$. Ano, implikace platí, důkaz přímý: Z faktu $[a; b] \sim [c; d]$ plyne, že $a \cdot d = b \cdot c$; z faktu $[c; d] \sim [e; f]$ plyne, že $c \cdot f = d \cdot e$. Vynásobením obou rovností dostaneme

$$a \cdot (d \cdot c) \cdot f = b \cdot (c \cdot d) \cdot e.$$

V závorce na každé straně (s využitím komutativity) násobíme tímtéž celým číslem – kdybychom to nedělali, rovnost též platí, tj. $a \cdot f = b \cdot e$ ... a to podle definice relace $\sim$ znamená, že $[a; b] \sim [e; f]$, zdůvodnění implikace je hotovo.

c) Vytvoříme faktormnožinu $Z \times Z^*/_\sim$, jejímiž prvky jsou podmnožiny rozkladu určeného ekvivalencí $\sim$.

d) Na $Z \times Z^*/_\sim$ definujeme operace $\oplus, \odot$ takto:

$$\{[a, b]\} \oplus \{[c, d]\} := \{[ad + bc, b \cdot d];$$

$$\{[a, b]\} \odot \{[c, d]\} := \{[a \cdot c, b \cdot d]\}.$$

O takto definovaných operacích musíme nejprve dokázat, že jsou definovány korektně, tj. že nezávisí na výběru reprezentanta v dané podmnožině rozkladu, a pak prozkoumáme jejich vlastnosti:

Operace sčítání: Sčítání nezávisí nezávisí na výběru reprezentanta z dané podmnožiny: $M_1 := \{[a; b]; [e; f]; \dots\}$, $M_2 := \{[c; d]; [g; h]; \dots\}$ ... musíme dokázat, že $\{[a, b]\} \oplus \{[c, d]\} = \{[e, f]\} \oplus \{[g, h]\}$:
Využijeme toho, že $[a; b] \in M_1$; $[e; f] \in M_1$, tj. $a \cdot f = b \cdot e$ (rovnice 1); a toho, že $[c; d] \in M_2$; $[g; h] \in M_2$, tj. $c \cdot h = d \cdot g$ (rovnice 2): Pak

$$\{[a, b]\} \oplus \{[c, d]\} := \{[ad + bc, bd]\}; \quad \{[e, f]\} \oplus \{[g, h]\} := \{[eh + fg, fh]\}$$

Nyní potřebujeme ukázat, že tyto dva různé výsledky, $\{[ad + bc, bd]\}$ i $\{[eh + fg, fh]\}$ leží ve stejné podmnožině rozkladu, tj. že platí $(ad + bc) \cdot fh = (eh + fg) \cdot bd$ ... a to skutečně platí, protože roznásobením závorek dostaneme

$$(af)dh + (hc)bf = (eb)dh + (gd)bf,$$

a nyní z rovnice (1) plyne, že první členy na obou stranách se rovnají (neboť součiny v závorce prvních členů se rovnají), a z rovnice (2) plyne, že druhé členy na obou stranách rovnice se rovnají, neboť součiny v závorce druhých členů se rovnají.

Tedy operace $\oplus$ je na množině $Z \times Z^*/_\sim$ korektně definovaná; má tedy smysl zkoumat její algebraické vlastnosti:

(1) Uzavřenost plyne z uzavřenosti „staré operace“ sčítání a násobení na množině Z – zde jen dodejme, že souřadnice bd součtu $[ad + bc, bd]$ je různá od nuly, protože b i d jsou různé od nuly, tj. druhá souřadnice zůstává nenulová.

(2) Asociativita $\oplus$ plyne ze „staré“ asociativity operace $+$ v jednotlivých souřadnicích = složkách. (viz video) ... tzv. nulový prvek.

(3) Neutrálním prvkem je třída $\{[0, 1]\}$, což je třída obsahující prvky $[0, 1], [0, 2], [0, 3], \dots$ (viz video)

(4) Např. pro $\{[6,2]\}$ je inverzí $\{[-6,-2]\}$. Obecně (viz video) pro $\{[a,b]\}$ je inverzí vzhledem ke sčítání $\{[-a,-b]\}$ ... tzv. opačný prvek.

(5) Operace $\oplus$ je komutativní ... ukáže se lehce, podobně jako předchozí vlastnosti – a plyne vlastně z komutativity sčítání a násobení obyčejného na množině Z.

$\Rightarrow$ Tedy $(Z \times Z^*/_\sim, \oplus)$ je komutativní grupa!

Operace násobení: Násobení nezávisí nezávisí na výběru reprezentanta z dané podmnožiny: $M_1 := \{[a;b];[e;f];\dots\}$, $M_2 := \{[c;d];[g;h];\dots\}$ ... musíme dokázat, že $\{[a,b]\} \odot \{[c,d]\} = \{[e,f]\} \odot \{[g,h]\}$:
Využijeme toho, že $[a;b] \in M_1$; $[e;f] \in M_1$, tj. $a \cdot f = b \cdot e$ (rovnice 1); a toho, že $[c;d] \in M_2$; $[g;h] \in M_2$, tj. $c \cdot h = d \cdot g$ (rovnice 2): Pak

$$\{[a,b]\} \odot \{[c,d]\} := \{[ac,bd]\}; \quad \{[e,f]\} \odot \{[g,h]\} := \{[eg,fh]\}$$

Nyní potřebujeme ukázat, že tyto dva různé výsledky, $\{[ac,bd]\}$ i $\{[eg,fh]\}$ leží ve stejné podmnožině rozkladu, tj. že platí $acfh = egbd$ ... a to skutečně platí, protože tuto rovnost získáme vynásobením levých stran rovnice (3) a rovnice (4) a vynásobením pravých stran rovnice (3) a rovnice (4).

Tedy operace $\odot$ je na množině $Z \times Z^*/_\sim$ korektně definovaná; má tedy smysl zkoumat její algebraické vlastnosti:

(1) Uzavřenost plyne z uzavřenosti „staré operace“ sčítání a násobení na množině Z – za navíc stále platí, že druhá souřadnice bd součinu $[ac,bd]$ zůstává nenulová.

(2) Asociativita $\odot$ plyne ze „staré“ asociativity operace násobení v jednotlivých souřadnicích = složkách. (viz video)

(3) Neutrálním prvkem je třída $\{[1,1]\}$, což je třída obsahující prvky $[1,1],[2,2],[3,3],\dots$ (viz video) ... tzv. jednotkový prvek.

(4) Např. pro $\{[6,2]\}$ je inverzí $\{[2,6]\}$. Obecně (viz video) pro $\{[a,b]\}$ je inverzí vzhledem k násobení $\{[b,a]\}$. A protože inverzi hledáme pouze pro prvky různé od nulového, tak předpokládáme, že $a \neq 0$, tedy i inverzní prvek $\{[b,a]\}$ leží ve množině $Z \times Z^*/_\sim$.

(5) Operace $\odot$ je komutativní ... ukáže se lehce, podobně jako předchozí vlastnosti – a plyne vlastně z komutativity sčítání a násobení obyčejného na množině Z.

$\Rightarrow$ Tedy $(Z \times Z^*/_\sim \setminus \{[0;1]\}, \oplus)$ je komutativní grupa!

(6) Navíc platí pro interakci obou operací komutativní zákon

$$(\{[a;b]\} \oplus \{[c;d]\}) \odot \{[e;f]\} = (\{[a;b]\} \odot \{[e;f]\}) \oplus (\{[c;d]\} \odot \{[e;f]\})$$

(důkaz poplyne opět rozepsáním pro levou a pravou stranu, a ověříme, že prvky vzniklé definičně na každé ze stran leží ve stejné podmnožině rozkladu, tj. jsou ve vazbě určené relací $\sim$). Tedy celá struktura $(Z \times Z^*/_\sim, \oplus, \odot)$ je těleso!!!

e) Zobrazení $\psi : Z \to Z \times Z^*/_\sim$ je definované vztahem $\psi(z) = \{[z \cdot 1, 1]\}$ je injektivním vnořením, tj. přenáší výsledky operací z množiny Z do nové struktury, kterou označíme jako Q.

i) dokažme nejprve, že ψ je injekce: pro různé vzory $a \neq b$ jsou různé i obrazy $\psi(a) = \{[a \cdot 1, 1]\}$ a $\psi(b) = \{[b \cdot 1, 1]\}$.

ii) a nyní dokažme, že platí vlastnost zachování výsledků operace SČÍTÁNÍ PODMNOŽIN, tj. $\psi(z_1 + z_2) = \psi(z_1) \oplus \psi(z_2)$: Ano, skutečně, dosaďme do levé a pravé strany rovnosti a zjistíme, že se tyto rovnají:

$L = \psi(z_1 + z_2) = \{[(z_1 + z_2) \cdot 1, 1]\} = \{[z_1 + z_2, 1]\}$;

$P = \psi(z_1) \oplus \psi(z_2) = \{[z_1 \cdot 1, 1]\} \oplus \{[z_2 \cdot 1, 1]\} = \{[z_1 + z_2; 1]\}$. Tedy $L = P$.

iii) a nyní dokažme, že platí vlastnost zachování výsledků operace NÁSOBENÍ PODMNOŽIN, tj. $\psi(z_1 + z_2) = \psi(z_1) \oplus \psi(z_2)$: Ano, skutečně, dosaďme do levé a pravé strany rovnosti a zjistíme, že se tyto rovnají:

$left = \psi(z_1 \cdot z_2) = \{[z_1 \cdot z_2 \cdot 1, 1]\} = \{[z_1 \cdot z_2, 1]\}$;

$right = \psi(z_1) \odot \psi(z_2) = \{[z_1 \cdot 1, 1]\} \odot \{[z_2 \cdot 1, 1]\} = \{[z_1 \cdot z_2; 1]\}$. Tedy $left = right$.

iv) Celkem tedy ψ je injektivním homomorfismem u obou operací, tj. výsledky operací sčítání a násobení celých čísel jsou přeneseny beze změny na výsledky sčítání a násobení odpovídajících objektů v nově vytvořené struktuře.

12.1.2 Konstrukce $Q \to R$

Jak již bylo řečeno na minulé přednášce, konstrukce $Q \to R, R \to C$ už jsou jiného charakteru, protože nevytváříme strukturu nového typu (R a C jsou už stále tělesa), pouze obohatíme množinu Q o nějaké další prvky.

Množina Q se skládá z racionálních čísel. Každé racionální číslo lze vyjádřit nekonečně mnoha zlomky a lze převést na číslo s desetinným rozvojem ukončeným nebo neukončeným periodickým. Přidáním iracionálních čísel z množiny I, jejichž desetinný rozvoj je neperiodický neukončený, dostaneme množinu R reálných čísel.

Věta 40 *Konstrukce $Q \to R$, první možný pohled: Doplníme-li množinu Q o limity všech možných posloupností prvků z Q, které v samotné množině Q neleží, dostaneme množinu R.*

Důkaz: iracionální čísla jsou právě ta čísla, která jsou limitami posloupností zlomků z množiny Q, a přitom nejsou prvky množiny Q. □

Věta 41 *Konstrukce $Q \to R$, druhý možný pohled: R je množina řezů (A, B) množiny Q, které jsou 1. druhu (ty odpovídají racionálním číslům) nebo 3. druhu (ty odpovídají iracionálním číslům).*

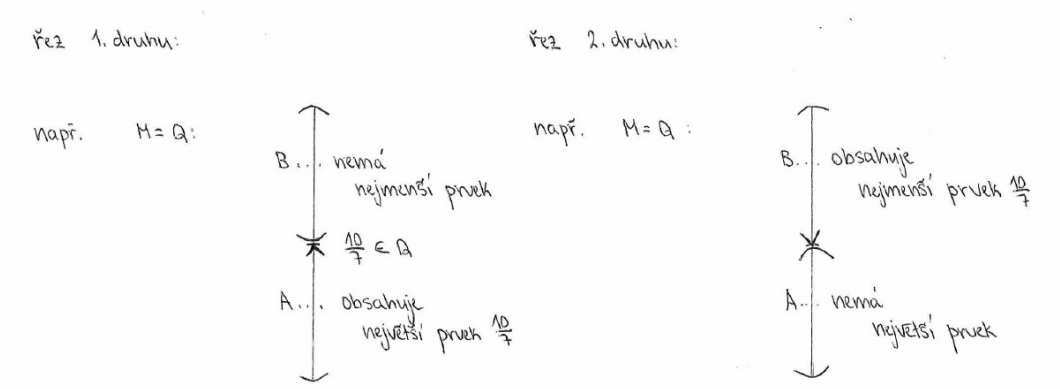
Důkaz či objasnění: Nejprve musíme definovat pojem řezu (A, B) lineárně uspořádané množiny M (tedy M je poset = částečně uspořádaná množina, ve které jsou každé dva prvky srovnatelné = tzv. řetězec).

Řez (A, B) řetězce M je rozklad množiny M na podmnožiny A, B ($A \cap B = \emptyset, A \cup B = M, A \neq \emptyset, B \neq \emptyset$ takový, že $\forall a \in A, \forall b \in B : a < b$.

Vzhledem k pojmům nejmenší prvek/největší prvek existují čtyři druhy řezů (vysvětleno na Hasseových diagramech množiny M):

Řez 1. druhu: A obsahuje svůj největší prvek, B nemá nejmenší prvek

Řez 2. druhu: A nemá největší prvek, B obsahuje svůj nejmenší prvek



Obrázek 12.5: Řez 1. druhu a řez 2. druhu

Racionálních čísel je právě tolik, kolik existuje řezů 1. druhu množiny Q, tj. existuje bijekce $Q \to$ řezy Q 1. druhu.

Podobně bychom mohli zlomek $\frac{10}{7}$ umístit namísto do množiny A do množiny B, a tím způsobem vznikne řez 2. druhu. Racionálních čísel je tedy právě tolik, kolik existuje řezů 2. druhu množiny Q, tj. existuje bijekce $Q \to$ řezy Q 2. druhu.

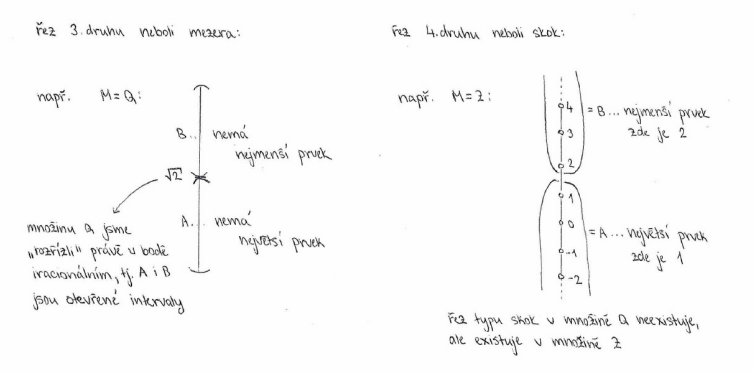
Podle toho, do které z množin A, B řezu „hraniční“ zlomek $\frac{10}{7}$ umístíme, vznikne řez 1. druhu nebo řez 2. druhu - můžeme si tedy vybrat, jak budeme racionální čísla (reprezentovaná zlomky) chápat, zda jako řezy 1. druhu nebo řezy 2. druhu množiny Q. Do tvrzení věty 41 jsme si vybrali racionální čísla reprezentovaná jako řezy množiny Q 1. druhu.

Řez 3. druhu neboli MEZERA: A nemá největší prvek, B nemá nejmenší prvek

Řez 4. druhu neboli SKOK: A má největší prvek, B má nejmenší prvek

Iracionálních čísel je právě tolik, kolik existuje MEZER (= řezů 3. druhu) v Q, tj. existuje bijekce $I \to$ mezery v Q. Například mezera na obrázku odpovídá iracionálnímu číslu $\sqrt{2}$.

Čili doplníme-li racionální čísla (= řezy 1. druhu) iracionálními čísly (= mezerami v Q = řezy 3. druhu), dostaneme R.



V obrázku mezery $\sqrt{2}$ v Q neexistuje největší prvek A, ani neexistuje nejmenší prvek množiny B - ovšem $\sqrt{2}$ je supremum množiny A, a současně $\sqrt{2}$ je infimum množiny B. Čili místo terminologie řezů lze kostrukci věty 41 formulovat i jinak: pomocí pojmu infimum nebo supremum - můžeme si vybrat, který z pojmů použijeme, protože $\sqrt{2}$ je současně $infB$ i $supA$, takže stačí použít jen jeden pojem, např. infimum:

Doplníme-li množinu Q o infima otevřených intervalů v Q, která neleží v Q, dostaneme R. Konec důkazu či objasnění.

Poznámka: Věty 40, 41 popisují tedy tutéž konstrukci $Q \to R$, pouze pomocí jiných pojmů: věta 40 pomocí pojmu limita posloupnosti, věta 41 pomocí pojmu řez. Konstukce pomocí pojmu řez je součástí bakalářské zkoušky ve 3. ročníku.

12.1.3 Konstrukce $R \to C$:

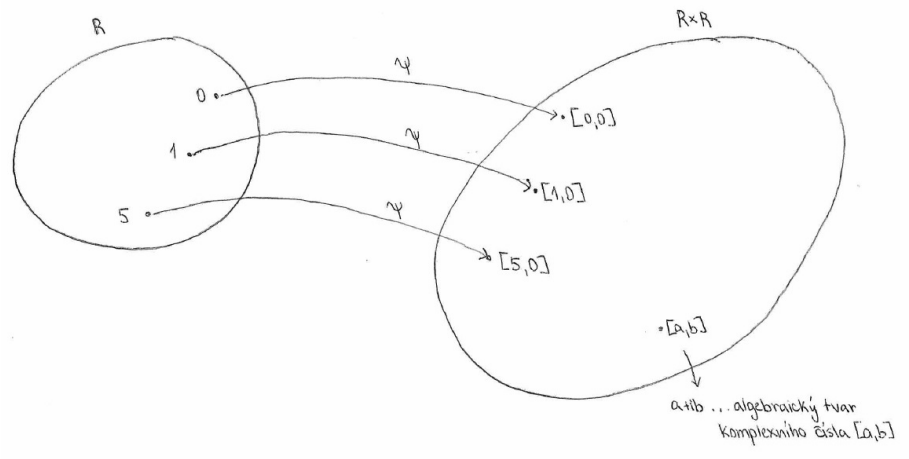
Věta 42 *Konstrukce $R \to C$: Těleso $(R, +, \cdot)$ lze vnořit do tělesa $C := R \times R$, ve kterém má rovnice $x^2 + 1 = 0$ řešení.*

a) Na $R \times R$ definujme operace $+, \cdot$ takto:

$$[a, b] + [c, d] := [a + c, b + d] \ldots a + ib + c + id = a + c + i(b + d)$$

$$[a, b] \cdot [c, d] := [ac - bd, ad + bc] \ldots (a+ib) \cdot (c+id) = ac + i^2bd + ibc + iad = ac - bd + i(ad + bc)$$

Pak struktura $(R \times R, +, \cdot)$ je těleso.



Obrázek 12.6: Vnoření tělesa $(R, +, \cdot)$ do tělesa $C := R \times R$

Opačný prvek k $[a, b]$ je $[-a, -b]$. Inverzní prvek k $[a, b]$ (mimo $[0, 0]$, ke kterému inverzi nehledáme) je $[\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}]$: $(a + ib) \cdot \frac{1}{(a+ib)} = 1$ ... vlastnost inverzního prvku.
$\frac{1}{a+ib}$ je inverzní prvek, upravme jej do tvaru „něco $+i$“:

$$\frac{1}{a+ib} = \frac{1}{a+ib} \cdot \frac{a-ib}{a-ib} = \frac{a-ib}{a^2-i^2b^2} = \frac{a-ib}{a^2+b^2} = \frac{a}{a^2+b^2} + i \cdot \frac{(-b)}{a^2+b^2}$$

A $\frac{a}{a^2+b^2} + i \cdot \frac{(-b)}{a^2+b^2}$ je algebraický tvar prvku $[\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}]$

b) Platí $[0, 1] \cdot [0, 1] = [-1, 0]$, algebraicky $i^2 = -1$, tj. $[0, 1]$, algebraicky i, je řešením rovnice $x^2 + 1 = 0$.

c) Zobrazení ψ definujeme vztahem $\psi(r) = [r, 0]$. Zobrazení $\psi : R \to R \times R$ je injektivní homomorfismus $R \to R \times R$ vzhledem k definovaným operacím, tj. původní výsledky sčítání a násobení reálných čísel jsou v nové struktuře zachovány.

12.2 Cvičení 12: Komplexní čísla 03

Odehraje se podle pokynů cvičícího.

13 Otázky ke zkoušce

Dejte prosím důraz na otázky 10-11, 12-13, 14-15, protože ty potřebujete zvládnout minimálně na 50 procent.

Otázka 01. Logika a množinové operace.

- Co je to výrok? Co je to kvantifikátor? U výroku $\forall n \in N: \quad 6|n \quad \Rightarrow \quad 2|n$ napište a) obrácení, b) obměnu, c) negaci, a to včetně kvantifikátorů.
- Proveďte negace výrokových forem (elementárně, tak aby nezůstal znak negace před žádnou závorkou):
  a) $A \Rightarrow (B \vee C)$;
  b) $(A \Leftrightarrow B) \wedge C$;
  c) $(A \wedge B) \vee C$.
- Které dvě důležité výrokové formy jsou jsou logicky ekvivalentní implikaci $A \Rightarrow B$?
- Ze symbolů $A \cup B$, $A \cap B$, $\overline{A}$, $A \setminus B$, $A \div B$, $A \times B$ jen čtyři jsou symboly označující binární operace, protože $\overline{A}$ je unární operace doplňku a $A \times B$ je kartézský součin, jehož výsledkem je množina uspořádaných dvojic, tj. struktura zcela jiného typu než vstupní množiny.
- Definujte symbolickým zápisem všech šest typů označení v předchozí odrážce.

Otázka 02. Relace a její vlastnosti.

- Definice (binární) relace na množině M.
- Definice šesti základních vlastností relace (a také schopnost provést negaci těchto vlastností).
- Co je to ekvivalence, uspořádání, řetězec?
- Co je to faktormnožina?
- Co je to relace kongruence na množině celých čísel? Uveďte příklad, znázorněte graficky.
- Co je to rozklad množiny? Jak se definuje rozklad množiny určený relací ekvivalence $\sim$?
- Jak se v Hasseho diagramu znázorňují jednotlivé vlastnosti relace uspořádání?
- Uveďte definici a příklad minimálního prvku množiny M, maximálního prvku množiny M, nejmenšího prvku množiny M, největšího prvku množiny M.
- M je podmnožina uspořádané množiny P; prvek $p \in P$ se nazývá a) dolní závora množiny M, b) horní závora množiny M, c) infimum množiny M, d) supremum množiny M, jestliže ...

Otázka 03. Zobrazení, funkce a jejich vlastnosti.

- f je zobrazení mezi množinami X a Y, jestliže ...
- posloupnost, funkce je ...
- a) f je zobrazení z X do Y, b) f je zobrazení X do Y, c) f je zobrazení z X na Y, d) f je zobrazení X na Y, e) f je prosté, f) f je injekce, g) f je „zobrazení na“ (neboli surjekce), h) f je bijekce, jestliže ...
- Vlastnosti reálných funkcí ... definice, příklady a negace u těchto vlastností.

Otázka 04. Struktury s jednou binární operací.

- Definice binární operace na množině. Různé vlastnosti operací napsané symbolickým zápisem.
- U operace definované na množině vypište vlastnosti (musíte znát jejich názvy i symbolickou definici) této operace a uveďte, o jaké algebraické struktury se vzhledem k této operaci jedná.
- Zdůvodněte, proč vlastnosti platí, zejména uvádějte neutrální prvek a stanovte inverzní prvky.
- Uveďte důkaz větiček (viz nejnovější verze skript): věta 1, věta 2, věta 3, věta 4, věta 5.
- Co je to řád grupy a řád prvku? Jak se tyto pojmy liší? Co je to cyklická grupa?
- Jak se definuje n-tá odmocnina prvku grupy a záporná mocnina prvku grupy?
- Co stačí ověřit u podmnožiny S grupy $(G, \bigtriangledown)$, abychom měli jistotu, že $(S, \bigtriangledown)$ je už také grupou? Věta 6 ... vyslovte ji a dokažte ji.
- Co říká věta 7 ohledně konstrukce podgrupy generované množinou M? Popište, jak se generování děje (bez důkazu).

Otázka 05: Struktury se dvěma operacemi.

- Definujte polookruh, uveďte příklad.
- Definujte okruh; uveďte příklad okruhu zbytkových tříd, který není oborem integrity, včetně vysvětlení a příkladu nenulových dělitelů nuly.
- Definujte nenulové dělitele nuly na struktuře $(M, \bigtriangledown, \star)$.
- Definujte obor integrity; uveďte příklad a) okruhu zbytkových tříd, který je oborem integrity; b) oboru integrity, který není tělesem.
- Definujte těleso; uveďte příklad a) konečného, b) nekonečného tělesa.

- Dokažte větičku 26, 27, 28.
- Uveďte zákon krácení (7)* v oboru integrity.
- Co za algebraickou strukturu se dvěma operacemi je $(2^A, \div, \cap)$? Uveďte u každé z operací neutrální prvek a příklad, že existuje-neexistuje inverzní prvek.
- Jednotlivé vlastnosti těchto operací jsou vlastně vztahy mezi množinami. Dokažte některý z nich, ideálně například distributivní zákon (pomocí Vennových diagramů).
- Obsahuje tato struktura nenulové dělitele nuly? Jaká rovnice by musela pro ně platit? Uveďte příklad těchto objektů sestavených do dané rovnice.
- Uveďte a dokažte tzv. de Morganova pravidla (Základy mat., přednáška 4), která vyjadřují vztah mezi binární operací sjednocení-průniku a unární operací doplňku. Dokazují se, jak jinak, pomocí Vennových diagramů.

Otázka 06: Nějaká větička na struktury s jednou-dvěma operacemi a její důkaz. Možné důkazy vět jsou vypsány v otázkách 04, 05, 07.

Otázka 07: Pojem homomorfismu a izomorfismu.

- Uveďte definici homomorfismu mezi grupoidy.
- Řekněte, jak se přirozeně (viz přednáška) definuje homomorfismus grupy $(Z, +)$ do grupy $(Z_6, +)$. Tento homomorfismus není prostý, ale je surjektivním zobrazením. Co je pro pojem surjektivního homomorfismu charakteristické?
- Věta 17a, věta 17b, věta 17c, 18a ... vlastnosti homomorfismu, dokažte tyto věty.
- Definice jádra $Ker\varphi$ homomorfismu φ, definice oboru hodnot homomorfismu φ, příklad.
- Co je charakteristické pro pojem injektivního homomorfismu? Viz kapitoly 11,12 (konstrukce číselných oborů).
- Definice izomorfismu mezi grupoidy-grupami.
- Jaký je význam izomorfismu grup?
- Jak lze poznat izomorfismus z tabulky operací obou struktur?

Otázka 08: Grupa permutací a Cayleyho věta

- Vypište celou tabulku operace skládání permutací grupy S_3.
- Uveďte Cayleyho větu a na jejím základě najděte pro zadanou grupu izomorfní podgrupu grupy permutací (viz příklad 19).
- Ilustrujte Cayleyho větu na konečné grupě $(Z_3, +)$ a nekonečné grupě $(Z, +)$.

- Mohl by se objevit příklad: Jakou osmiprvkovou podgrupu grupy $(S_4, \circ)$ vygenerují cykly $(1, 2, 3, 4)$ a $(1, 2)$ při operaci skládání permutací? Nápověda: Nemusíte vypisovat celou tabulku operace, ale při vytváření tabulky operace se postupně objevují různé prvky jako výsledky, tj. sestavit aspoň část této tabulky by vám pomohlo.
- Řešte v $(S_4, \circ)$ rovnici $(1, 2, 3) \circ x = (2, 3, 4)$.

Otázka 09: Dihedrální grupy D_3 (grupa symetrií trojúhelníku), D_4 (grupa symetrií čtverce), D_5 (grupa symetrií pravidelného pětiúhelníku), D_6 (grupa symetrií pravidelného šestiúhelníku) a Lagrangeova věta.

- Spojte geometrický význam jednotlivých shodných zobrazení s algebraickým zápisem dané permutace.
- Na druhé straně, pro daný algebraický tvar permutace vysvětlete její geometrický význam v dané dihedrální grupě, je-li jaký.
- Zkonstruujte tabulky operace skládání zobrazení v těchto grupách, nebo v některých podgrupách.
- Co je tvrzením Lagrangeovy věty?
- Vypište na základě geometrického významu i Lagrangeovy věty všechny podgrupy těchto grup (podívejte se na řešené příklady ve skriptech s těmito strukturami, najdete podle obrázků symetrie trojúhelníku, čtverce, pětiúhelníku a šestiúhelníku).
- Určete množinu generátorů dané grupy.

Otázka 10-11: Polynomické rovnice – algebraické metody řešení.

- **Co je to množina všech polynomů $(R[x], +, \cdot)$ s reálnými koeficienty, s operacemi sčítání a násobení, z algebraického hlediska?**
- **Co je to polynom stupně n, vedoucí koeficient polynomu, kořen polynomu, násobnost kořene? Co říká základní věta algebry?**
- **Jaký je trojí základní význam Hornerova schématu? (výpočet funkční hodnoty, nalezení kořene, provedení dělení polynomu lineárním polynomem)**
- **Co říká věta o racionálních kořenech polynomu a jak je lze určit pomocí Hornerova schématu?**
- **Co říká věta o odstranění násobných kořenů polynomu? Popište pomocí dobrého označení, příklad uvádět nemusíte.**
- **Co říká věta o komplexně sdružených kořenech polynomu? Vyslovte ji a dokažte ji. Lze najít také příklad polynomu, který nesplňuje větu o komplexně sdružených kořenech polynomu?**

- **(řešení reciproké rovnice): vysvětlete metodu při řešení rovnice**

$$x^6 - 3x^5 + 5x^4 - 7x^3 + 5x^2 - 3x + 1 = 0;$$

jen dokončete převod na rovnici třetího stupně, kterou už nemusíte řešit.

Otázka 12-13: Polynomické rovnice – numerické metody řešení.

- **U konkrétního polynomu nalezněte omezení pro velikost všech jeho kořenů, včetně kořenů komplexních.**
- **Najděte všechny intervaly délky 1, na kterých existuje kořen polynomu $p(x)$ s násobností 1.**
- **Najděte řešení rovnice $x^5 - x^2 - 1 = 0$ na intervalu $\langle 1; 2\rangle$ metodou půlení intervalu i metodou Newtonovou. Za pomoci kalkulačky proveďte tři kroky u každé z metod. Je možné, že u zkoušky zde bude jiná rovnice, například rovnice $2x^3 + 5x - 1 = 0$ a interval délky 1, který obsahuje řešení, budete muset sami najít.**
- **Uveďte přednosti a úskalí metody půlení intervalu. Za jakých předpokladů najde tato metoda kořen polynomu?**
- **Uveďte přednosti a úskalí Newtonovy metody.**
- **Odvoďte vzorec pro použití Newtonovy metody pro řešení rovnice $p(x) = 0$.**
- **Za jakých předpokladů najde Newtonova metoda i nereálný komplexní kořen polynomu?**

Otázka 14-15: Komplexní čísla – operace s komplexními čísly, mocnina a odmocnina z komplexního čísla:

- **komplexní číslo v algebraickém, goniometrickém a exponenciálním tvaru – vysvětlení každého tvaru, převody mezi tvary;**
- **geometrický význam sčítání a násobení komplexních čísel;**
- **výpočet n-té mocniny z komplexního čísla (Moivreho věta);**
- **vysvětlení skalárního součinu vektorů v rovině – geometrický význam;**
- **vysvětlení vektorového součinu vektorů v prostoru dimenze 3 – jaký geometrický význam má velikost a směr vektorového součinu?**
- **řešení binomické rovnice: řešte rovnici $x^4 + 1 = 0$ a znázorněte obrazy řešení v komplexní rovině ... vrcholy jakého obrazce jsou tato řešení? (výpočet n-té odmocniny z komplexního čísla; vyjádření výsledku v goniometrickém tvaru, a pak převedení na algebraický tvar, jestliže se jedná o násobek třiceti nebo pětačtyřiceti stupňů)**

Otázka 16: Peanova množina P, množina N přirozených čísel.

- Uveďte čtyři nedůležité Peanovy axiomy, které zná každý student pedagogické fakulty (viz video);
- uveďte důležitých čtyři až pět Peanových axiomů, které se týkají pojmu následníka;
- uveďte definici předchůdce, úseku a uspořádání na P;
- uveďte čtyři vlastnosti, které splňují operace sčítání a násobení, jež lze definovat na množině P;
- uveďte, jak lze strukturu $(N_0, +, \cdot)$ vystihnout algebraicky.

Otázka 17: Algebraický popis, jak z N zkonstruujeme Z. Studenti by měli umět nakreslit obrázek a celou konstrukci popsat. Bude též zkoušeno na následujících dílčích otázkách:

- Co provedeme s množinou N nejdříve? Vytvoříme kartézský součin $N \times N$.
- Jak definujeme relaci ekvivalence $\sim$? Dokažte o této relaci, že se skutečně jedná o ekvivalenci.
- Co je to $N \times N/_\sim$? Popište tuto strukturu – jaké jsou její prvky?
- Jak na struktuře $N \times N/_\sim$ definujeme operaci sčítání? Dokažte, že nově definovaná operac je korektně definovaná a nezávisí na výběru reprezentantů.
- Jaké má nově definovaná operace sčítání vlastnosti? Dokažte-zdůvodněte je.
- Jak se definuje zobrazení $N \to N \times N/_\sim$, jaké má vlastnosti (dokažte je) a co zaručuje (vysvětlete)?
- Jakým pojmem lze výslednou strukturu s operacemi sčítání a násobení vystihnout algebraicky?

Algebraický popis, jak ze Z zkonstruujeme Q. Studenti by měli umět nakreslit obrázek a celou konstrukci popsat. Bude též zkoušeno na následujících dílčích otázkách:

- Co provedeme s množinou Z nejdříve? Vytvoříme kartézský součin $Z \times Z^*$.
- Jak definujeme relaci ekvivalence $\sim$? Dokažte, že se skutečně jedná o ekvivalenci.
- Co je to $Z \times Z^*/_\sim$? Popište tuto strukturu – jaké jsou její prvky?
- Jak na struktuře $Z \times Z^*/_\sim$ definujeme operaci sčítání a operaci násobení? Dokažte, že jsou tyto operace korektně definovány a nezávisí na výběru reprezentanta.
- Jaké má nová operace sčítání podmnožin vlastnosti? Dokažte-zdůvodněte.
- Jaké má nová operace násobení podmnožin vlastnosti? Dokažte-zdůvodněte.

- Jak se definuje zobrazení $Z \to Z \times Z^*/_\sim$, jaké má vlastnosti (dokažte) a co zaručuje (vysvětlete)?
- Jakým pojmem lze výslednou strukturu s operacemi sčítání a násobení vystihnout algebraicky?

Otázka 18: Algebraický popis, jak z Q zkonstruujeme R pomocí řezů množiny Q.

- Co je to řez množiny M?
- Jaké čtyři typy řezů existují (a na jakých množinách)? Vysvětlete i graficky;
- Jak se „zkonstruuje“ R z množiny Q? Čemu odpovídají řezy Q prvního druhu, čemu odpovídají řezy Q třetího druhu?

Algebraický popis, jak z R zkonstruujeme C. Studenti by měli umět nakreslit obrázek a celou konstrukci popsat. Bude též zkoušeno na následujících dílčích otázkách:

- Co provedeme s množinou R nejdříve? Vytvoříme kartézský součin $R \times R$.
- Jak na struktuře $R \times R$ definujeme operaci sčítání a operaci násobení? Jaké má tato operace vlastnosti? Dokažte-zdůvodněte.
- Je inverzní prvek ke komplexnímu číslu $1 + 2i$ vzhledem k operaci násobení také komplexním číslem?
- Jak se definuje zobrazení $R \to R \times R$, jaké má vlastnosti (dokažte) a co zaručuje (zdůvodněte)?
- Jakým pojmem lze výslednou strukturu s operacemi sčítání a násobení vystihnout algebraicky?

14 Výsledky některých příkladů

14.1 Výsledky ke cvičení 1.1 – Vlastnosti binární operace

Ad úloha 1.1: Definice základních pojmů:

a) Množinou M rozumíme soubor navzájem rozlišitelných prvků, o kterých lze jednoznačně rozhodnout, že do něj patří.

b) Kartézský součin množin M, N je množina všech uspořádaných dvojic $[m, n]$, kde $m \in M$ a současně $n \in N$.

c) Relace na množině M je nějaká podmnožina kartézského součinu $M \times M$. Relace mezi množinami X a Y je nějaká podmnožina kartézského součinu $X \times Y$.

d) Relace ekvivalence na M je binární relace, která je reflexivní, symetrická a tranzitivní.

e) Relace uspořádání na M je relace, která je reflexivní, antisymetrická a tranzitivní.

f) Relace f na kartézském součinu $X \times Y$ se nazývá zobrazení z množiny X do množiny Y, jestliže pro ni platí podmínka: $[x, y] \in f \wedge [x, z] \in f \Rightarrow y = z$.

g) Binární operace ∇ na množině M je zobrazení $M \times M \to M$, tj. zobrazení, které přiřadí uspořádané dvojici $[a, b]$ z kartézského součinu $M \times M$ výsledek této operace, prvek $a \nabla b$.

h) Zobrazení $f : N \to R$) (tedy $D(f)$ je množina přirozených čísel, $H(f)$ množina reálných čísel) se nazývá posloupnost reálných čísel.

i) Zobrazení f z množiny reálných čísel R do množiny reálných čísel R se nazývá (reálná) funkce (jedné) reálné proměnné.

Ad úloha 1.2: Definice vlastností relací:

- Relace ρ na množině M je reflexivní, když $\forall x \in M : x \rho x$.
- Relace ρ na množině M je symetrická, když $\forall x, y \in M : x \rho y \Rightarrow y \rho x$.
- Relace ρ na množině M je tranzitivní, když $\forall x, y, z \in M : x \rho y \wedge y \rho z \Rightarrow x \rho z$.
- Relace ρ na množině M je úplná, když $\forall x, y \in M : x \rho y \vee y \rho x$.
- Zobrazení f z X do Y je taková relace $X \times Y$, že platí $[x, y] \in f \wedge [x, z] \in f \Rightarrow y = z$.

14.2 Výsledky ke cvičení 2.1 – Určování vlastností různých operací

Ad úloha 2.1:

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 $-2 \notin N$. □

b) $(Z, +)$ je komutativní grupa.

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

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

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

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

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

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

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

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

Ad úloha 2.5 (M, ∇) je komutativní monoid.

Ad úloha 2.6 $(M, \triangle)$ je komutativní grupa.

Ad úloha 2.7 $(N - \{0\}, *)$ je grupoid.

Ad úloha 2.8 $(R^+, \circ)$ je komutativní grupoid.

14.3 Výsledky ke cvičení 3.3 – Vlastnosti grup, podgrupy a generátory grupy

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

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

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

Ad F.3: Tabulku lze doplnit na:

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

.

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

$$\log a + \log \frac{1}{a} = \log 1 = 0.$$

Ad A.5:ano, jedná se o podgrupu, prvky grupy jsou body na přímce procházející počátkem, operace sčítání těchto prvků (funguje stejně jako operace sčítání vektorů s počátečním bodem v počátku a koncovým bodem v daném prvku) splňuje vlastnosti (1), (4 ... inverzní prvek k prvku $(x, 2x)$ je prvek $(-x, -2x)$, který opět leží na dané přímce) a množina je jasně neprázdná.

Ad D.5: Pokud dané součiny jsou navzájem různé prvky (to plyne mimo jiné z úlohy F.2 z minulého cvičení, že na jednom řádku operace grupy nemohou být stejné prvky), jeden z těchto součinů musí být roven neutrálnímu prvku n, tj. nechť například $a_i * a_l = n$, pak podle věty 4 platí $a_i^{-1} = a_l$, našli jsme inverzi k prvku a_i, platí vlastnost (4).

Ad úloha 3.7 – ad N.1: $H = \{6, 12, 2, 8, 14, 4, 10, 0\}$ a prvky jsou napsány v tom pořadí, jak je získáváme užitím prvku 6.

Ad E.1: podgrupy jsou čtyři: a) celá H_{10} generovaná prvkem 1 nebo prvkem 3 nebo prvkem 7 nebo prvkem 9;
b) druhá triviální podgrupa $(\{0\}, +)$ generovaná prvkem 0;
c) podgrupa $(\{0, 2, 4, 6, 8\}, +)$ generovaná prvkem 2 nebo prvkem 4 nebo prvkem 6 nebo prvkem 8;
d) podgrupa $(\{0, 5\}, +)$ generovaná prvkem 5;

Ad E.3: $< 6, 9 >= \{6, 0, 9, 3\}$ vzhledem k operaci skládání otáčení.

Ad E.7 modifikace: prvek $[1, 1]$ je generátorem podgrupy $\{[1; 1;], [0; 2], [1; 3], [0; 0]\}$ vzhledem ke sčítání.

Ad E.6: ano, prvek $[1, 1]$ je generátorem celé grupy vzhledem ke sčítání. Grupa má šest prvků a výsledek lze vyčíst z tabulky operace v této grupě.

Ad úloha **??**

a) $x = (b^2)^-1$

b) $x = b^{-1} * a$

c) $x = (a^4)^{-1}$

Ad úloha 3.9: Tabulka operace $\circ$ na množině D_3 symetrií trojúhelníku:

Tabulka 14.7: Tabulka operace $\circ$ na množině D_3 symetrií trojúhelníku.

$\circ$	R_0	R_1	R_2	R_3	R_4	R_5
R_0	R_0	R_1	R_2	R_3	R_4	R_5
R_1	R_1	R_2	R_0	R_5	R_3	R_4
R_2	R_2	R_0	R_1	R_4	R_5	R_3
R_3	R_3	R_4	R_5	R_0	R_1	R_2
R_4	R_4	R_5	R_3	R_2	R_0	R_1
R_5	R_5	R_3	R_4	R_1	R_2	R_0

Pokud tuto tabulku porovnáme s tabulkou grupy $(S_3, \circ)$ v příkladu 4 je vidět, že mezi oběma grupami existuje izomorfismus, tj. příslušné tabulky operace se liší pouze

přeznačením prvků: $f(e) = R_0$, $f(s) = R_1$, $f(t) = R_2$, $f(u) = R_3$, $f(v) = R_4$, $f(w) = R_5$ (toto izomorfní přiřazení je vidět i na obrázku **??**). 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.

Ad úloha 3.10 Cyklické podgrupy grupy $(H_{10}, +)$:

$(\{0\}, +), (\{0, 5\}, +), (\{0, 2, 4, 6, 8\}, +), (H_{10}, +)$.

Ad úloha 3.11 Cyklické podgrupy grupy $(H_{12}, +)$:

$(\{0\}, +), (\{0, 6\}, +), (\{0, 2, 4, 6, 8, 10\}, +), (\{0, 3, 6, 9\}, +), (\{0, 4, 8\}, +), (H_{12}, +)$.

14.4 Výsledky ke cvičení 4.2 – Nekomutativní grupy

Ad úloha 4.1: Podle definice skládání zobrazení platí

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

Seznam literatury:

Beránek, 2011 Jaroslav Beránek: Vybrané kapitoly z algebry. Skriptum Pdf, počet stran 70. Doplnění obsahu předmětů Algebra 1 a Algebra 3 na PdF pro budoucí učitele 2.stupně. Brno 2011.

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

Drozd, 2008 P. Drozd – základy práce se softwarem R. Manuál ke stažení z internetu o některých základních funkcích jazyka R, který lze v 1.ročníku VŠ doporučit jako lepší kalkulačku zvládající běžné matematické funkce, a současně jednoduché kreslení obrázků, které lze stáhnout v různých formátech. I jednoduché programy lze v tomto prostředí realizovat. Prostředí po instalaci funguje offline.

Horák, 2002 P. Horák: Cvičení z algebry a teoretické aritmetiky I, Brno 2002. Sbírka příkladů na Přírodovědecké fakultě MU. Cvičení pokrývá zhruba látku v předmětech Základy matematiky, Algebra 1, Algebra 2 vyučovaných na Pedagogické fakultě.

Horák, 2013 P. Horák: Základy matematiky. Přednáškový text na Přírodovědecké fakultě MU.

Fajmon, 2019 B.Fajmon: Základy matematiky – verze 2019. Doplnění přednášek v předmětu MA0001, počet stran 144.

Jordan, Smith, 2008 D.Jordan, P.Smith: Mathematical techniques. Oxford 2008, 4th Edition.

Koláček J. Koláček: Výuka jazyka R. Rovněž úvod do jazyka R, nyní od vysokoškolského učitele matematiky, což je vhodným doplněním textu (Drozd, 2008).

Komprsová 2018 Komprsová, T.: Řešení rovnic v algebře. Bakalářská práce na Pdf MUNI, Brno 2018.

Kopka, J., 1991 Jan Kopka: Svazy a Booleovy algebry (Ústí nad Labem 1991, zejména str. 19-82). Pan profesor Kopka napsal svůj text z té pozice, že by rád přehledně a srozumitelně podal přehled pojmů algebry a diskrétní matematiky, aby byla vidět její krása. Kniha je hlubším rozvedením pojmu uspořádaná množina uvedeným v předmětu Základy matematiky.

Pinter, 2010 Charles Pinter: A book of Abstract Algebra, 2010. Jedná se o reprint druhého vydání z roku 1990. Neobyčejně čtivý text, napsaný z té pozice, že algebra je důležitá a má důležitá uplatnění.

Robová, Hála, Calda 2013 Robová, J., Hála, M., Calda, E.: Komplexní čísla, kombinatorika, pravděpodobnost a statistika. Prometheus 2013, v sérii Matematika pro střední školy. Velmi dobrý úvod do daných čtyř oborů na středoškolské úrovni, kromě výkladu kombinací s opakováním, který je málo srozumitelný.

Rosický, J., 2000 Jiří Rosický: Algebra – grupy a okruhy 2000, reprint textu z roku 1985. Tento text se hodně shoduje s osnovou předmětu Algebra 1 na PdF, nicméně jen až jako doplnění čtivější knihy (Pinter, 2010).

Trombiková, 2019 Trombiková, I: Numerické metody pro řešení polynomických rovnic. Bakalářská práce Pdf MUNI, Brno 2019.