

Algebra 1 (MA 0003)

RNDr. Břetislav Fajmon, Ph.D.

Obsah

1	Týden 01: Základní vlastnosti operace na množině M	6
1.1	Cvičení 1: Vlastnosti číselných operací	6
1.2	Cvičení 2: Určování vlastností různých operací	11
1.3	Přednáška 1	13
1.4	Dodatky 1	23
2	Týden 02 – další vlastnosti operace na množině	27
2.1	Přednáška 2	27
3	Týden 03	33
3.1	Cvičení 03: Vlastnosti grup, podgrupy a generátory grupy	33
3.2	Přednáška 3: Izomorfismus, homomorfismus, Cayeho věta	37
4	Týden 04	49
4.1	Cvičení 04: Nekomutativní grupy	49
4.2	Přednáška 04: Grupa symetrií čtverce, Lagrangeova věta, faktorgrupa	50
4.3	Dodatky	54
5	Týden 05	60
5.1	Cvičení 05: Řád prvku, cyklické grupy, grupy zbytkových tříd	60
5.2	Přednáška 05	71
6	Týden 06	78
6.1	Přednáška 06: struktury se dvěma operacemi	78
6.2	Cvičení 06: Algebraické struktury se dvěma binárními operacemi	85
7	Týden 07	87
7.1	Cvičení 07: Polynomy 01	87
7.2	Přednáška 07: Přehled algebraických metod hledání kořene polynomu	88
8	Týden 08	97
8.1	Cvičení 08: Polynomy 02	97
8.2	Přednáška 08: Přehled numerických metod hledání kořene polynomu	98
9	Týden 09	105
9.1	Cvičení 09: Polynomy 03	105
9.2	Přednáška 09: Konstrukce číselných oborů	106
10	Týden 10	114
10.1	Cvičení 10: Komplexní čísla 01	114
10.2	Přednáška 10: Konstrukce oborů \mathbb{Q} , \mathbb{R} , \mathbb{C}	115

11 Týden 11	122
11.1 Cvičení 11: Komplexní čísla 02	122
11.2 Přednáška 11: Opakování a příprava ke zkoušce	122
12 Týden 12	123
12.1 Cvičení 12: Prověrka-b na polynomy a komplexní čísla	123
12.2 Přednáška 12: Příprava a otázky ke zkoušce	123
13 Výsledky některých příkladů	130
13.1 Výsledky ke cvičení 1.1 – Opakování definic z předmětu Základy matematiky	130
13.2 Výsledky ke cvičení 1.2 – Určování vlastností různých operací	131
13.3 Výsledky ke cvičení 3.1 – Vlastnosti grup, podgrupy a generátory grupy . .	132
13.4 Výsledky ke cvičení 4.1 – Nekomutativní grupy	134
13.5 Výsledky ke cvičení 5.1 – Řád prvku, cyklické grupy, grupy zbytkových tříd	134

Úvod

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

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

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

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 obohacením i středoškolská učebnice (Robová, Hála, Calda 2013).

Břetislav Fajmon,
verze textu září 2021

1 Týden 01: Základní vlastnosti operace na množině M

1.1 Cvičení 1: Vlastnosti číselných operací

Podívejme se na tzv. Axiomy euklidovské geometrie:

1. Každé dva různé body lze spojit úsečkou.
2. Úsečku lze libovolně daleko prodloužit v přímku.
3. Pro dva různé body S, A lze sestrojít 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 $*$:

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

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 $*$:

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

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 $*$:

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

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 $*$:

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

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 nespĺňují. Proto slovo „komutativní“ musíme k právě definovaným strukturám zvlášť dodat jako novou vlastnost.

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

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

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

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

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

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

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

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

Název „distributivní“ lingvisticky odpovídá tomu, že po odstranění závorek se prvek x rozdělí = distribuuje k oběma členům součtu. Matematicky se jedná o pravidlo násobení závorek, 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 \cdot váže jednotlivá celá čísla s větší prioritou než je tomu u sčítání a odčítání (a pokud bychom chtěli nejprve sečíst čísla 8 a 2, a teprve pak výsledek vynásobit třemi, musíme díky větší prioritě násobení užít pro sčítání závorek).

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

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

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

Určitě si zopakujte ty nejdůležitější pojmy předmětu Základy matematiky:

Úloha 1.1 Uved'te 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 Uved'te následující definice vlastností relací a u každé z nich uved'te 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 $x \circ y = (x - 1)(y - 1)$. Zjistěte, zda je operace neomezeně definovaná. Sestavte operační tabulku.

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

Δ	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 $-$. Určete její vlastnosti.

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 [13.1](#).

1.2 Cvičení 2: Určování vlastností různých operací

Úloha 1.10 Zjistěte, jaké struktury vzhledem k uvedené známé operaci (běžné označení) jsou následující množiny:

- a) $(\mathbb{N}, +)$.
- b) $(\mathbb{Z}, +)$.
- c) (\mathbb{Z}, \cdot) .
- d) $(\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$.
- e) $(\mathbb{Q} - \{0\}, \cdot), (\mathbb{R} - \{0\}, \cdot)$.
- 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) $(\mathbb{Z}, -), (\mathbb{Z}, :)$.
- i) $(M, +)$, kde $M = \{-100, -99, -98, \dots, -1, 0, 1, 2, \dots, 99, 100\}$.

Úloha 1.11 Opakování definic a práce s nimi

- a) Nadiktujte sousedovi v lavici definici grupy a on ji zapíše zkráceným matematickým zápisem, ve kterém se nevyskytuje ani jedno české slovo, kromě slova „grupa“.
- b) Co to znamená, že $(M, *)$ není grupoid, tj. není splněna vlastnost (1)? Negujte vlastnost (1).
- c) Co to znamená že není splněna vlastnost (4) z definice grupy? Negujte vlastnost (4).

Úloha 1.12 a) Uveďte definici vlastnosti (4) pro operaci ∇ na množině M ve stručném matematickém zápisu.

- b) Uveďte příklad struktury (M, ∇) , která splňuje vlastnost (4).
- c) Uveďte příklad struktury (M, ∇) , která NESplňuje vlastnost (4).

Úloha 1.13 Dokažte, že množina všech podmnožin tříprvkové množiny s operací symetrického rozdílu \div je grupa (viz Pinter 2010, str. 30, oddíl C).

Úloha 1.14 V množině $M = \{1, 2\}$ je operace ∇ tabulkou:

∇	1	2
1	1	1
2	1	2

Určete typ algebraické struktury (M, ∇) .

Úloha 1.15 V množině $M = \{a, b, c\}$ je operace Δ tabulkou:

Δ	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

Určete typ algebraické struktury (M, Δ) .

Úloha 1.16 Určete typ algebraické struktury: $(N - \{0\}, *)$, kde $x * y = x^y$.

Úloha 1.17 Určete typ algebraické struktury: (R^+, \circ) , kde $x \circ y = \sqrt{xy}$.

Výsledky některých cvičení najdete v závěru textu v oddílu [13.2](#).

1.3 Přednáška 1

Poznámka na úvod: První přednáška tohoto textu nepoužívá všechny pojmy a definice z prvního cvičení záměrně, protože je možné, že se bude konat před prvním cvičením. A pokud je použije, doporučuji je při prvním čtení ignorovat a vrátit se k nim až po absolvování příkladu 6 přednášky 2.

Vlastní text přednášky: Algebra je nauka o řešení rovnic¹. Proto bychom mohli zmínit, co je to rovnice s neznámou x na množině M , na níž je definována operace ∇ :

- **Rovnost** je relace ekvivalence na množině výrazů, ve kterých vystupují prvky množiny M a operace ∇ . Příklad: běžně rovnost na množině reálných čísel chápeme jako relaci ekvivalence na množině výrazů, v nichž vystupují reálná čísla, reálné funkce a známé operace s reálnými čísly.
- **Rovnítko** je symbol relace rovnosti.
- **Rovnice** s neznámou x na množině M je výroková funkce, ve které vystupuje neznámý prvek x , symbol rovnosti (rovnítko), prvky množiny M nebo výrazy na množině M . Jak víme, výroková funkce není výrokem, protože bychom museli dosadit za x , abychom dostali výrok pravdivý či nepravdivý.
- **Řešit rovnici s neznámou x na množině M** znamená najít obor pravdivosti² K všech prvků z množiny M , pro které se stává daná rovnice pravdivým výrokem.

Podívejme se na některé jednoduché příklady:

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

$$7 + x = 2$$

nemá řešení na množině přirozených čísel (tedy tato rovnice nemá řešení na monoidu $(\mathbb{N}_0, +)$)!! Nebo rovnice

$$7 \cdot x = 2$$

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

$$x^2 - 2 = 0$$

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

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

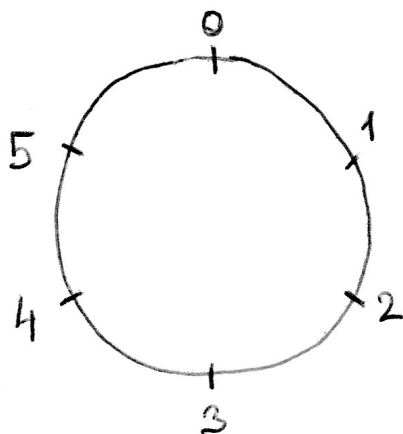
¹Arabské „al gebr“ znamenalo „složit“ rovnici, tj. vyřešit ji = nalézt její řešení – Viz úvod knihy Pinter 2010. Zejména se jedná o polynomické rovnice, kterými se budeme zabývat ve druhé polovině semestru.

² K označuje tzv. množinu kořenů dané rovnice na množině M .

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

Začneme ovšem jedním příkladem konečné, šestiprvkové grupy:

Příklad 1 *Grupa potočení 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 obvykle 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 potočení jedné ručičky s osou otáčení ve středu kružnice:

- prvek 0 představuje nulové potočení ručičky – s ručičkou se nic nestane;
- prvek 1 představuje potočení o jednu jednotku, tj. o 60° ;
- prvek 2 představuje potočení ručičky o dvě jednotky, tj. o 120° ;
- prvek 3 představuje potočení o 180° ;
- prvek 4 představuje potočení o 240° ;
- prvek 5 představuje potočení 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 $(1+2)+4^3$, 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 uzávorkování⁴.

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:

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

³Operaci označíme jako + – i když se nejedná o klasické sčítání čísel, toto skládání otáčení má velmi příbuzné vlastnosti se sčítáním.

⁴Dokonce skládání tří pootočení nezávisí na jejich pořadí, protože operace skládání pootočení splňuje i vlastnost (5) = komutativitu; tou se ovšem nyní nechceme příliš zabývat.

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

$*$	\dots	y	\dots
\dots	\dots		
x	\dots	$x * y$	\dots
\dots	\dots		

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:

- $P_1 = \{0\}$ - 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, ∇) se nazývají dvě podgrupy: a) $S_1 = \{n\}$ je podgrupou vzhledem k ∇ , která obsahuje pouze neutrální prvek (je neprázdná a splňuje (1) a (4)), b) $S_2 = G$ (samotná celá grupa je též podgrupou sama sebe). Každou jinou podgrupu nazveme **vlastní podgrupou** grupy (G, ∇) .

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 .

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

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:

$$- P_3 = \{ \dots - 9, -6, -3, 0, 3, 6, 9, 12, \dots \};$$

$$- P_4 = \{ \dots - 2, 0, 2, 4, \dots \};$$

- atd.

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

Příklad 3 Označme $(F(R), \circ)$ množinu všech funkcí (= zobrazení $R \rightarrow R$, 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:

$$e^{x+3} \circ \sin x = e^{\sin x + 3}$$

$$\sin x \circ e^{x+3} = \sin(e^{x+3})$$

$$e^{x+3} \circ e^{x+3} = e^{e^{x+3} + 3}$$

$$x^5 \circ x^5 = x^{25}$$

...

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	...	e^{x+3}	$\sin x$	x^5	...
...
e^{x+3}	...	$e^{e^{x+3}+3}$	$e^{e^{\sin x+3}}$	e^{x^5+3}	...
$\sin x$...	$\sin(e^{x+3})$	$\sin(\sin x)$	$\sin(x^5)$...
x^5	...	$(e^{x+3})^5$	$(\sin x)^5$	x^{25}	...
...

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

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

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

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

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 zobrazení⁵. 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 $\{1, 2, \dots, n\}$ na sebe sama. S_n je množina všech permutací tohoto typu. Například permutace $f : M \rightarrow M$ pro $M = \{1, 2, 3, 4, 5\}$ definovaná

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

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

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

Důležité úsporné označení permutace

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

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

(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

⁵Až 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

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

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

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

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

Operace skládání permutací

Protože permutace je zvláštní případ zobrazení a zobrazení $M \rightarrow M$ 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 pořad 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 druhý⁶.

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, 3, 2)	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

$$\frac{\circ}{id} \left| \begin{array}{c} id \\ id \end{array} \right.$$

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

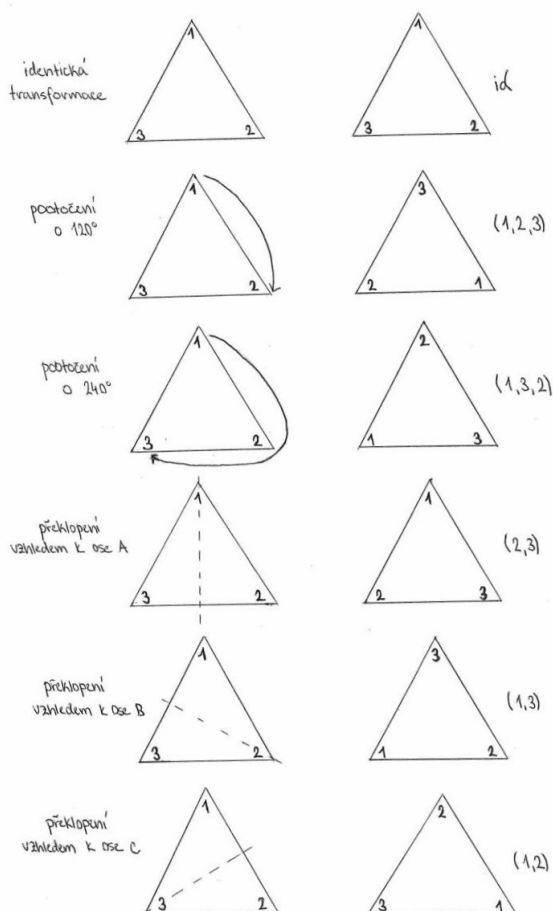
$$\frac{\circ}{(2,3)} \left| \begin{array}{cc} id & (2,3) \\ id & (2,3) \\ (2,3) & id \end{array} \right. , \quad \frac{\circ}{(1,3)} \left| \begin{array}{cc} id & (1,3) \\ id & (1,3) \\ (1,3) & id \end{array} \right. , \quad \frac{\circ}{(1,2)} \left| \begin{array}{cc} id & (1,2) \\ id & (1,2) \\ (1,2) & id \end{array} \right.$$

⁶Toto 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.



Obrázek 1.1: Množina D_3 permutací odpovídajících symetriím trojúhelníku.

1.4 Dodatky 1

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

Základní vlastnosti grup

Studujme nyní tedy obecně vlastnosti grupy (G, ∇) . Co v této obecné poloze lze říci o množině G a operaci ∇ ? 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?⁷

Věta 1 (o jednoznačnosti neutrálního prvku) *V každé grupě (G, ∇) 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 ∇ vůči jakémukoli dalšímu prvku, tj. např. $g \nabla n_1 = g$. Mohlo by tedy být zajímavé, co se stane, když aplikujeme operaci na dané dva neutrální prvky n_1, n_2 ⁸:

$$n_1 \stackrel{(3)_2}{=} n_1 \nabla n_2 \stackrel{(3)_1}{=} n_2,$$

což je spor s tím, že oba neutrální prvky jsou navzájem různé⁹. \square

Tak to je zajímavé, neutrální prvek grupy může být pouze jeden jediný. A jak je to s inverzními prvky grupy? Víme, že v grupě existuje inverze ke každému prvku vzhledem k operaci ∇ – 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, ∇) existuje ke každému prvku x jediný inverzní prvek x^{-1} vzhledem k operaci ∇ .*

⁷Víme, 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?

⁸Vlastnost $(3)_1$ znamená, že využíváme vlastnosti (3) pro prvek n_1 , vlastnost $(3)_2$ platí pro neutrální prvek n_2 .

⁹Celý důkaz je možné formulovat i jako přímý důkaz typu 2: předpokládáme, že prvky n_1, n_2 oba se chovají jako neutrální, tj. uvedené odvození by o nich dokázalo, že se musí nutně rovnat – tj. z toho plyne přímo, že prvek neutrální je pouze jeden.

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

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

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

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

Klíčová myšlenka: vynásobením¹⁰ $a_1^{-1} \nabla a_2^{-1}$ pravděpodobně nic nezískáme. Prvky a_1^{-1} , a_2^{-1} vystupují ve vlastnosti (4), tj. měli bychom studovat něco jako rovnice ve vlastnosti (4). VYUŽIJEME TOHO, ŽE VE VLASTNOSTI (4) SE VYSKYTUJÍ DVĚ ROVNOSTI, A JEDNU APLIKUJEME NA PRVEK a ZLEVA, DRUHOU ZPRAVA:

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

Využili jsme platnosti asociativního zákona (2) pro kaskádu tří prvků uprostřed spojených operací ∇ . 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. \square

Věta 3 (můžeme „krátit“¹¹ v rovnostech, ve kterých se vyskytují prvky grupy G a operace ∇ ?) V každé grupě (G, ∇) platí zákony o krácení (7), tj.

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

Důkaz: Provedeme například pro první z implikací: Vztah

$$a \nabla b = a \nabla c$$

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 :

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

a s využitím asociativity (2) (v grupě nezáleží na uzávorkování „součinu“ tří prvků vzhledem k operaci ∇), 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). \square

¹⁰Všimněte si, že říkám „vynásobením“, ikdyž nyní nestudujeme operaci násobení, ale operaci ∇ ... tak moc jsou operace sčítání a násobení v nás zakódovány, že používáme terminologii, která odpovídá těmto operacím – správně bychom měli říci: aplikací operace ∇ na dané prvky v daném pořadí, tj. na uspořádanou dvojici prvků ...

¹¹Opět terminologie: i když mluvíme obecně o operaci ∇ , pro vlastnost (7) se vžil termín „zákony o krácení“, třebaže krácení je termín vzatý z rovností, ve kterých se vyskytuje běžná operace násobení.

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

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

(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 $a \nabla b = n$ prvkem a^{-1} zleva, dostaneme

$$a^{-1} \nabla a \nabla b = a^{-1} \nabla n \stackrel{(3)}{=} a^{-1},$$

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

Věta 5 (o výpočtech inverzních prvků) V každé grupě (G, ∇) platí:

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

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

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

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

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

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

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

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

Rozšíření vlastnosti (2) na k prvků

Ve větě 8 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 ∇ jako součin prvního prvku se součinem následujících tří prvků, tj.

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

postupným užitím vlastnosti (2) pro tři prvky dostaneme

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

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 ∇ nezáleží na uzávorkování.

S takto rozšířeným zákonem asociativity můžeme pak vyslovit a dokázat některé věty pro větší počet operací ∇ v řetězci za sebou, například analogii části (a) věty 8:

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

Dále pro nás bude užitečná například definici n -té mocniny vzhledem k operaci ∇ :

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

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

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, ∇) je takový prvek $x \in G$ (pokud tedy existuje), že $a = x^n$.

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

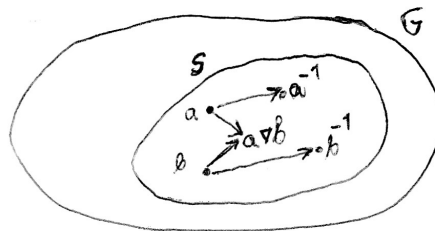
2 Týden 02 – další vlastnosti operace na množině

2.1 Přednáška 2

Podgrupa (S, ∇) grupy (G, ∇)

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

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



Kupodivu se ukazuje, že dané dvě vlastnosti (1), (4) neprázdné¹² podmnožině S grupy (G, ∇) stačí na to, aby byla grupou vzhledem k téže operaci ∇ :

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

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

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

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

tedy neutrální prvek n patří i do množiny S a pro (S, ∇) platí (3). \square

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

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

¹²Ve 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, ∇) . Na to, abychom našli nejmenší možnou podgrupu, která obsahuje prvky a, b, c , musíme vyrobit všechny možné součiny těchto tří prvků a jejich inverzí¹³, a nejen to: musíme brát všechny možné konečné sekvence prvků spojených operací ∇ , ve kterých se vyskytují (i opakovaně) prvky a, b, c a jejich inverze.

Typickými takto vytvářenými prvky jsou například

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

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

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

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

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

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

Definice 15 podgrupa grupy G generovaná množinou S , prvky množiny S nazýváme **generátory podgrupy** $\langle S \rangle$.

Podgrupu generovanou podmnožinou S označujeme jako (**označení 02**) $\langle S \rangle$. A ještě jedna definice, která s tím souvisí:

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

Cyklickou podgrupu generovanou prvkem a někdy označujeme (**označení 03**) $\langle a \rangle$ a je jasné, že obsahuje prvky

$$a, \quad a^2 := a \nabla a, \quad a^3 := a \nabla a \nabla a, \dots,$$

a také prvky

$$a^{-1}, \quad a^{-1} \nabla a^{-1}, \quad a^{-1} \nabla a^{-1} \nabla a^{-1}, \dots,$$

a také prvek $n = a \nabla a^{-1}$.

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

¹³V této chvíli už se v daných součinech vyskytuje neutrální prvek $n \in G$, protože $a \nabla a^{-1} = n$.

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

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

Podle označení množiny generátorů lze psát

$$(S_3, \circ) = \langle (1, 3), (1, 2) \rangle .$$

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

Věta 7 (S_n, \circ) , množina permutací¹⁴ $M \rightarrow M$ pro $M = \{1, 2, \dots, n\}$ vzhledem k operaci skládání permutací je pro $n \geq 3$ nekomutativní grupa.

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

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

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

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

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

Důkaz je hotov. \square

¹⁴Pozor, prvky množiny S_n nejsou podmnožiny či jednotlivé prvky množiny M , ale zobrazení množiny M do sebe!! Jedná se už o složitější strukturu.

Operace na cyklické podgrupě je vždy komutativní

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

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

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

Názvy a vlastnosti algebraických struktur – příklady

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

- Vlastnost (1): $\forall x, y \in M : x * y \in M$uzavřenost množiny M vzhledem k operaci $*$
- Vlastnost (2): $\forall x, y, z \in M : (x * y) * z = x * (y * z)$ asociativita operace $*$ na množině M
- Vlastnost (3): $\exists e \in M : x * e = e * x = x \quad \forall x \in M$ existence neutrálního prvku vzhledem k operaci $*$
- Vlastnost (4): $\forall x \in M \exists x^{-1} \in M : x * x^{-1} = x^{-1} * x = e$ existence inverzních prvků vzhledem k operaci $*$
- Vlastnost (5): $\forall x, y \in M : x * y = y * x$ komutativita operace $*$ na množině M

Pro dvojici operací $*$ a ∇ můžeme navíc definovat tzv. distributivní zákon 8:

- Vlastnost (6): $\forall x, y, z \in M : x*(y\nabla z) = (x*y)\nabla(x*z), (y\nabla z)*x = (y*x)\nabla(z*x)$.

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 vlastnosti (1), (2), (3);
- Grupa $(M, *)$ - operace $*$ splňuje na množině M vlastnosti (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 minulé 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. •

Věta 8 (o krácení v grupě) V každé grupě (G, \cdot) platí zákony o krácení (vlastnost (7)):

$$\begin{aligned} a * c = b * c & \quad / * c^{-1} \\ a * c * c^{-1} = b * c * c^{-1} \\ a = b \end{aligned}$$

Příklad 7 V grupě permutací (S_3, \circ) řešte rovnici $(1, 2) \circ x = (1, 2, 3)$, kde x označuje neznámou permutaci.

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

$$(1, 2) \circ x = (1, 2, 3) \quad / \circ (1, 2) \text{ (zleva)}$$

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

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

$$x = (2, 3)$$

Řešením dané rovnice je tedy permutace $(2, 3)$. •

Příklad 8 Určete algebraické vlastnosti struktury (Z_6, \cdot) .

Začneme tím, že si sestavíme tabulku výsledků operace:

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]

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).

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 8. Např. z tabulky vidíme, že $[2] \cdot [2] = [2] \cdot [5]$, ovšem $[2] \neq [5]$. Uvedená struktura totiž nespĺňuje vlastnost (4), není tedy grupa.●

3 Týden 03

3.1 Cvičení 03: Vlastnosti grup, podgrupy a generátory grupy

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Zdůvodněte, proč ano - proč ne.

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

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

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

Například F.4: Čtyřprvková grupa $G = \{e, a, b, c\}$ splňuje $\forall x \in G : x^2 = e$ (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, ∇) 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 : $H = \{a_1, a_2, \dots, a_n\}$ a vyberme si libovolné $a_i \in H$. Uvažujme nyní navzájem RŮZNÉ prvky $a_i \star a_1, a_i \star a_2, \dots, a_i \star a_n$: 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 $\langle 6 \rangle$ 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 $\langle 6, 9 \rangle$ grupy $(H_{12}, +)$.

Například E.7 – modifikace¹⁵: V grupě $H_2 \times H_4$ je operace sčítání po složkách zadaná tabulkou

Tabulka 3.7: Tabulka operace $+$ na množině $H_2 \times H_4$.

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

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

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

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

Úloha 3.8 Vyřešte v grupě $(G, *)$ systém rovnic:

a) $x^2 = b, x^5 = e$

b) $ax^2 = b, x^3 = e$

¹⁵Jediný důvod, proč je příklad E.7 před příkladem E.6 je historický – E.7 byl nejprve podrobně napsán na písence. U příkladu E.6 se pak očekává, že si čtenář sestaví při řešení tabulku operace na součinu grup sám.

$$c) x^2 = a^2, x^5 = e$$

Úloha 3.9 Pro následující grupy najděte podgrupy:

$$a) (Z, +)$$

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

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

Úloha 3.10 Určete tabulku pro grupu všech symetrií rovnostranného trojúhelníka s operací skládání (D_3, \circ) .

Úloha 3.11 Vypište všechny cyklické podgrupy grupy $(H_{10}, +)$ skládání otáčení hodinové ručičky o násobky desetiny plného úhlu.

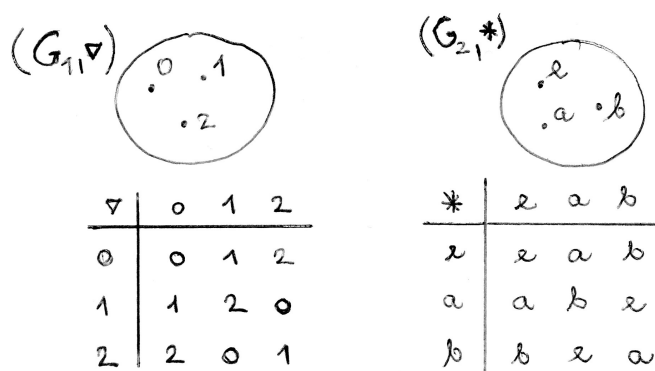
Úloha 3.12 Vypište všechny cyklické podgrupy grupy $(H_{12}, +)$ skládání otáčení hodinové ručičky o násobky dvanáctiny plného úhlu.

Výsledky některých cvičení najdete v závěru textu v oddílu [13.3](#).

3.2 Přednáška 3: Izomorfismus, homomorfismus, Cayeho věta

V 18. a 19. století, když se formovaly termíny českého překladu předmětu algebra, byl jedním z návrhů českého překladu slova algebra termín „stejnostka“ neboli nauka o stejnostech¹⁶. I když se tento český překlad neujal, vystihuje snahy moderní algebry všimnout si shodných či podobných vlastností různých objektů.

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



Obrázek 3.2: Dvě izomorfní grupy.

V této kapitole se budeme zejména zabývat „stejností“ vzhledem k pojmu binární operace – protože operace je něco dynamického, kdy dvěma prvkům podle jistého předpisu přiřazujeme třetí prvek, tedy stejnost (či podobnost), která nás bude zajímat, je dána tabulkou výsledků operace na dané množině¹⁷. Na obrázku 3.2 vidíme tabulky operace dvou tříprvkových grup, které jsou izomorfní – existuje mezi nimi totiž bijekce

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

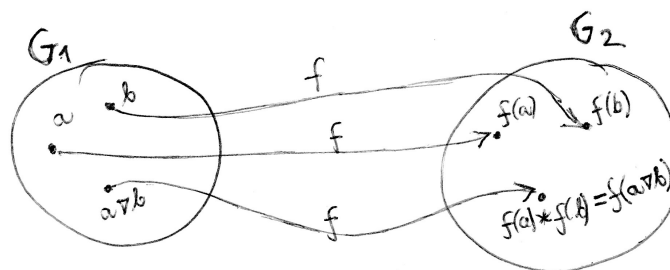
ale nejen to – tato bijekce v jistém smyslu „zachovává výsledky operace“, tj. např. prvek $1 \nabla 2$ z grupy G_1 , což lze v tabulce operace ∇ grupy G_1 najít, že je roven 0, odpovídá v navrhované bijekci prvku e v grupě G_2 , který je výsledkem operace $a * b$, kde a je obraz prvku 1 a b je obraz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

¹⁶Viz Alena Šolcová, přednáška o Cestách k české terminologii v některých partiích matematiky, Katedra matematiky PdF, 14. března 2018.

¹⁷Tedy izomorfismus je v případě zachování výsledků operace vlastností poněkud skrytou – poznáme ji až podrobnějším studiem tabulky operace na obou strukturách.

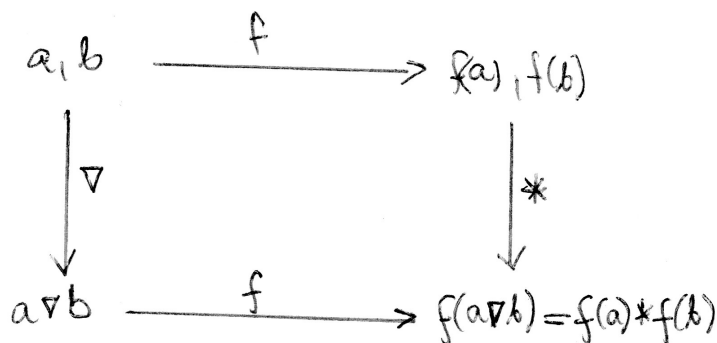
Definice 17 *Izomorfismus* grupy (G_1, ∇) na grupu $(G_2, *)$ je bijekce $f : G_1 \rightarrow G_2$, která splňuje vlastnost

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



Obrázek 3.3: Podmínka zachování výsledků operace při zobrazení f .

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



Obrázek 3.4: Komutativní diagram pro podmínku zachování výsledků operace.

A nebo ještě jinak, říkáme, že izomorfismus f mezi grupami je bijekce, pro kterou diagram na obrázku 3.4 komutuje, neboli když vypustíme na prvky a, b z „ohrady“ G_1 operaci ∇ , a pak výsledek přeneseme (zobrazením f) do „ohrady“ G_2 , dosáhneme stejného výsledku, jako když bychom nejprve přenesli oddělené prvky a, b zobrazením f do „ohrady“ G_2 a tam na ně vypustili operaci $*$ ¹⁸.

Příklad 9 $(R, +)$ a (R^+, \cdot) jsou izomorfní grupy, pokud definujeme zobrazení $R \rightarrow R^+$ vztahem $f(x) = e^x$. Snadno se vidí, že zobrazení f je injekce, protože nenabývá dvou

¹⁸Diagram komutuje = nezáleží na pořadí: operace následovaná zobrazením dává tentýž výsledek jako zobrazení následované operací, pokud vždy mluvíme o binární operaci na té množině, ve které se dané dva prvky vyskytují.

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

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

Tato podmínka také platí, protože

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

Celkem f je grupovým izomorfismem.★

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

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

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

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

Věta 9 (Cayley) *Každá grupa (G, ∇) je izomorfní nějaké grupě permutací.*

Důkaz: dokážeme ve třech krocích:

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

2. O množině těchto permutací

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

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

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

Tak pojďme na to!!

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

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

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

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

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

$$a \nabla x_1 = a \nabla x_2,$$

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

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

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

- Celkem π_a je bijekce.

2. **O množině těchto permutací**

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

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

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

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

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

Podrobněji rozepsáno,

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

Tedy složením dvou prvků π_a a π_b z G^* je zase prvek z G^* , tj. množina G^* je uzavřená vzhledem k operaci \circ .

- (G^*, \circ) splňuje vlastnost (4): Stačí dokázat, že ke každému $\pi_a \in G^*$ existuje inverzní permutace vzhledem ke skládání permutací: A to opravdu existuje, je to totiž permutace $\pi_{a^{-1}}$ odpovídající prvku $a^{-1} \in G$ – pak platí (podle vlastnosti (1) je složením permutací permutace odpovídající „násobku“ obou dílčích prvků)

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

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

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

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

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

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

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

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

$$a \nabla e = b \nabla e,$$

to ale znamená, že $a = b$. Rovnost obrazů si vynucuje rovnost vzorů, tedy f je injekce.

- f je surjekce: Tato vlastnost je zaručena už tím, jak je množina G^* vytvořena: jsou do ní vybírány jen ty permutace π_a , které odpovídají prvku $a \in G$, tj. každá permutace π_a má svůj vzor $a \in G$ vzhledem k zobrazení f .

- f zachovává výsledky operace: chceme dokázat podmínku

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

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

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

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

Příklad 10 *Tříprvková grupa potočení $(H_3, +)$ 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 11 *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 $(Z, +)$:

$+$...	-2	-1	0	...
...
-2	...	-4	-3	-2	...
-1	...	-3	-2	-1	...
0	...	-2	-1	0	...
...

Grupa (S_Z, \circ) :

\circ	\dots	$\left(\begin{array}{cccc} \dots & -1 & 0 & 1 & \dots \\ & \downarrow & \downarrow & \downarrow & \\ \dots & -3 & -2 & -1 & \dots \end{array} \right)$	$\left(\begin{array}{cccc} \dots & -1 & 0 & 1 & \dots \\ & \downarrow & \downarrow & \downarrow & \\ \dots & -2 & -1 & 0 & \dots \end{array} \right)$	\dots
$\left(\begin{array}{cccc} \dots & -1 & 0 & 1 & \dots \\ & \downarrow & \downarrow & \downarrow & \\ \dots & -3 & -2 & -1 & \dots \\ & \dots & & & \end{array} \right)$	\dots	$\left(\begin{array}{cccc} \dots & -1 & 0 & 1 & \dots \\ & \downarrow & \downarrow & \downarrow & \\ \dots & -5 & -4 & -3 & \dots \\ & & \dots & & \end{array} \right)$	$\left(\begin{array}{cccc} \dots & -1 & 0 & 1 & \dots \\ & \downarrow & \downarrow & \downarrow & \\ \dots & -4 & -3 & -2 & \dots \\ & & \dots & & \end{array} \right)$	\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. •

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

Příklad 12 *Například C.3: Zjistěte, zda je grupa $2^{\{a,b\}}$ s operací symetrického rozdílu \div (stejná operace jako v úloze 1.13) izomorfní s grupou (V, \cdot) , kde $V = \{1, -1, i, -i\}$ a \cdot je operace násobení komplexních čísel. Svě 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. •

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

Tabulku struktury (V, \cdot) máme sestavenou z předcházejícího příkladu. Sestavme tedy ještě tabulky zbylých dvou struktur.

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: $0 \rightarrow 1, 1 \rightarrow i, 2 \rightarrow -1, 3 \rightarrow -i$. 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.

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

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

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

Homomorfismus grup

Izomorfismus grup je bijektivním zobrazením, které zachovává výsledky operace. Tato vlastnost (zachování výsledků operace) se objevuje i u jiných zobrazení než bijekcí – taková zobrazení nazveme homomorfismy¹⁹.

Definice 18 *Grupový homomorfismus $f : G \rightarrow H$ je takové zobrazení mezi grupami (G, ∇) a $(H, *)$, které zachovává výsledky operace, tj. platí vlastnost*

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

Příklad 13 *Zobrazení grupy $(Z, +)$ na grupu zbytkových tříd $(Z_6, +)$ definované vztahem „ $f(z) =$ zbytek po dělení čísla z číslem 6“ je homomorfismus grup.*

Grupa $(Z, +)$:

+	...	-2	-1	0	...
...
-2	...	-4	-3	-2	...
-1	...	-3	-2	-1	...
0	...	-2	-1	0	...
...

¹⁹Jazykově: izomorfismus = stejný tvar, totožný tvar; homomorfismus = podobný tvar, odvozený tvar (v jistém smyslu).

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

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: $6k + m \rightarrow m$, $6l + n \rightarrow m$ a $6p + r \rightarrow r$. 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. \square

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 14 Zobrazení $f : Z_6 \rightarrow Z_3$, přičemž na obou množinách uvažujeme operaci sčítání, definované vztahem

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

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

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

Definice 19 Pokud $f : G \rightarrow H$ je grupový homomorfismus a současně surjekce, označujeme $f(G) = H$ a grupa H se nazývá homomorfní obraz grupy G .

Viz příklad 14: grupa $(Z_3, +)$ je homomorfním obrazem grupy $(Z_6, +)$ vzhledem k homomorfismu f .

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

Věta 10 Pro grupový homomorfismus $f : G \rightarrow H$ grupy (G, ∇) do grupy $(H, *)$ platí:

- a) $f(e_G) = e_H$ (grupový homomorfismus vždy zobrazuje jednotkový prvek grupy G na jednotkový prvek grupy H);
- b) $(f(a))^{-1} = f(a^{-1})$ (vzhledem ke grupovému homomorfismu platí: inverze obrazu = obraz inverze).

Důkaz:

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

$$f(e_G) = F(e_G \nabla e_G) \stackrel{(h)}{=} f(e_G) * f(e_G),$$

dostali jsme tedy rovnost

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

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

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

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

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

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

- ad b) chceme dokázat vztah

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

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

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

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. \square

Definice 20 *Jádro* grupového homomorfismu $f : G \rightarrow H$ se nazývá množina \ker_f (označení 04)²⁰ těch prvků z grupy (G, ∇) , které se zobrazí na neutrální prvek e_H grupy $(H, *)$.

Příklad 15 a) V grupovém izomorfismu je jádrem zobrazení f pouze jednoprvková množina $\{e_G\}$.

b) V homomorfismu $f : Z_6 \rightarrow Z_3$ z příkladu 21 je jádrem množina těch prvků, které se zobrazí na nulu: $\ker_f = \{0, 3\}$.

Věta 11 Pro každý grupový homomorfismus platí tyto další vlastnosti:

- \ker_f je normální podgrupa v (G, ∇) ;
- $f(G)$ je podgrupa v $(H, *)$.

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

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

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

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

$$f(x) * f(y) \stackrel{(h)}{=} f(x \nabla y),$$

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

²⁰Označení plyne z německého slova kernel – anglické core se z historických důvodů neprosadilo.

4 Týden 04

4.1 Cvičení 04: Nekomutativní grupy

Úloha 4.1 Jsou dány permutace

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Úloha 4.3 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 13.4.

4.2 Přednáška 04: Grupa symetrií čtverce, Lagrangeova věta, faktorgrupa

Na začátku této přednášky se vrátíme k příkladu na grupu permutací pravidelného n -úhelníka:

Příklad 16 (ad Pinter 2010, str. 77, sada F) Grupa symetrií čtverce:

Uvažujme čtverec a takové jeho transformace, že po jejich provedení dostaneme zase čtverec se stranami rovnoběžnými s vertikálním a horizontálním směrem. Mám na mysli pootočení čtverce (se středem otáčení ve středu čtverce) o násobky 90° (ty jsou čtyři, a sice pootočení o 0° , o 90° , o 180° a o 270°), a ještě překlopení čtverce v osové souměrnosti podle navzájem symetrických os (ty jsou též čtyři pro osy otáčení v obou úhlopříčkách čtverce a ve dvou osách procházejících středy protějších stran čtverce). Použitím některé z těchto osmi transformací na čtverec dostaneme zase nějakou pozici čtverce, která vznikne ze základní polohy uplatněním jedné důležitější 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 $R_2 = (1, 3) \circ (2, 4)$ ²¹ a pootočení o 270° permutace $R_3 = (1, 4, 3, 2)$ ²².

(podrobněji viz obrázek 4.5).

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

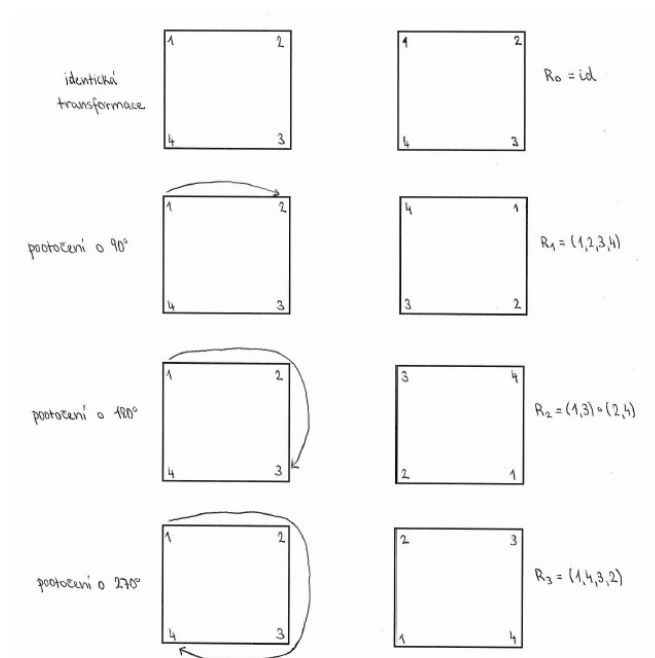
Skládáním $R_1 \circ R_5$ například dostaneme

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

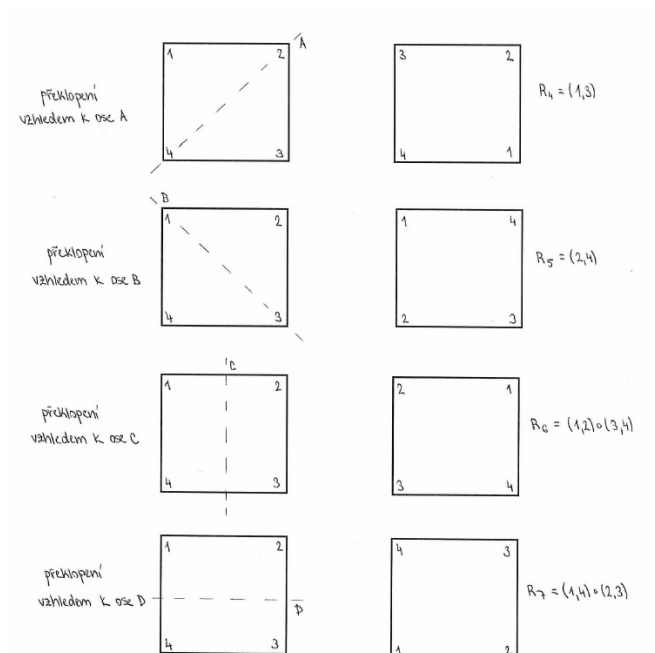
atd. Vyplněním operace pro každou dvojici prvků v obou pořadích (operace je opět nekomutativní, protože např. $R_5 \circ R_1 = R_7$) dostaneme tabulku grupy (D_4, \circ) symetrií čtverce, která odpovídá podgrupě grupy permutací s osmi prvky (viz tabulka 4.7). Všech permutací čtyřprvkové množiny je 24; tedy naše osmiprvková množina je podgrupou grupy S_4 .

²¹Pozor, tuto permutaci nelze lépe označit než spojením dvou disjunktních cyklů délky 2, protože dochází ke dvěma nezávislým prohozením během jedné permutace.

²²Což je totéž jako $(4, 3, 2, 1)$, ale začínáme při zápisu nejmenším možným číslem, abychom se vyznali ve výsledcích operací a podle pozice nejmenšího čísla poznali jednoznačně daný prvek.



Obrázek 4.5: Permutace odpovídající pootočení čtverce.



Obrázek 4.6: Permutace odpovídající osové symetrii čtverce.

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

Obrázek 4.7: Tabulka operace \circ na množině D_4 symetrií čtverce

Pro každé přirozené $n \geq 3$ lze sestavit 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 symetrií 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 .

V dalším následném textu dodatků v této kapitole (pokud vyučující nebude chtít vašich znalostí více) budete vyloženě potřebovat jen Lagrangeovu větu – větu [16](#), která bude procvičena v příkladech následující přednášky.

4.3 Dodatky

Z těchto dodatků možná vyučující probere jen část, na podrobné procházení není čas. Zejména věty 13, 15 a její důsledek jsou důležité, ale hlavně jsou tyto věty potřeba pro důkaz věty 16, kterou jedinou je určitě potřeba si pamatovat.

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, \dots, 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 13) 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:

- $\forall i \in \{1, 2, \dots, k\} : M_i \neq \emptyset$;
- $a \in M_i \cup M_j \Rightarrow M_i = M_j$;
- každý prvek $a \in M$ leží v jedné třídě rozkladu.

- **Označení 05:** 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 06:** Označme dále $[a]$ tu třídu rozkladu, která obsahuje prvek a , tedy podmínku z označení 07 budeme psát ve tvaru

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

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

Definice 21 $\forall a$ z grupy (G, ∇) a její podgrupu (H, ∇) lze definovat:

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

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

(množina výsledků operace $a \nabla h$, 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

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

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

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

Příklad 17 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 18 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 18 je vidět, že například množina $(2, 3) \circ H$ nemusí obsahovat žádný z původních prvků podgrupy H , a taky nemusí být podgrupa, protože neobsahuje neutrální prvek id , i když H podgrupa grupy G je (ze všech navzájem disjunktních tříd = podmnožin je podgrupou právě jedna – ta, která obsahuje neutrální prvek, a tedy třída $H \circ id$ neboli třída H).

Zabývejme se dále pouze pravými třídami prvků – všechny následující věty se budou týkat pravých tříd prvku vzhledem k podgrupě H , ikdyž bychom je mohli analogicky (či duálně?) formulovat i pro levé třídy prvku. Věta 12 je pouze pomocnou větou, která bude potřeba v důkazu věty 13 (věty 12 až 15 jsou řečeny za předpokladu označení z definice 21, tj. (H, ∇) je podgrupa grupy (G, ∇)).

Věta 12 $a \in H \nabla b$ právě tehdy, když $H \nabla a = H \nabla b$.

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

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

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

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

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

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

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

a po dosazení za b dostaneme

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

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

Věta 12 netvrdí nic světoborného, v podstatě jen to, že pokud prvky a, b jsou spojeny v operaci ∇ „přes podgrupu H “, tak jejich pravé třídy jsou totožné. Následující věta 13 je prvním významným výsledkem této kapitoly.

Věta 13 *Pravě²³ třídy $H \nabla a$ pro všechny možné prvky a grupy (G, ∇) tvoří rozklad množiny G .*

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

- a) Pokud množiny $H \nabla a, H \nabla b$ 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 :

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

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

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

a to podle věty 12 (tady právě ji potřebujeme!!) znamená, že $H \nabla a = H \nabla b$.

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

Než se dostaneme k větě 15 vedoucí k Lagrangeově větě, ještě jedno označení a jeden výsledek, věta 14: **Označení 07.** Označme množinu tříd G/H rozkladu grupy G podle její komutativní podgrupy H ... vzhledem k operaci $\underline{\nabla}$ definované pomocí vztahu

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

dostáváme tzv. rozkladovou grupu nebo též při doslovném překladu faktorgrupu²⁴.

Věta 14 *Struktura G/H vytvořená z tříd podle nějaké své komutativní podgrupy H s operací $\underline{\nabla}$ je grupa.*

Důkaz věty 14 je technický a nebudeme ho uvádět. Raději zde zmíníme, že G/H v příkladech 17 a 18 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 17, 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 15 *Existuje bijekce mezi podgrupou (H, ∇) a každou pravou třídou $H \nabla a$.*

²³Platí i analogická věta: Všechny levé třídy $a \nabla H$...

²⁴Anglicky FACTOR znamená, „rozložit“.

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

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

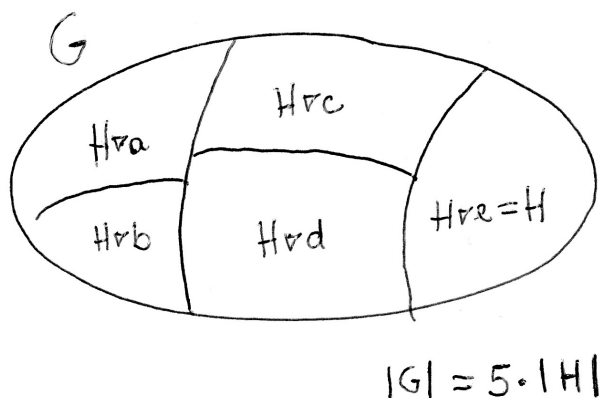
Takto definované f je injekce:

$$f(h_1) = f(h_2) \Rightarrow h_1 \triangleleft a = h_2 \triangleleft a \Rightarrow h_1 = h_2$$

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

Důsledkem věty 15 pro konečné grupy G je: Všechny pravé třídy $H \triangleleft a$ 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 13 a věta 15, už byly řečeny. Ta následující je pouze jejich důsledkem, tj. pan Lagrange je autorem souvislosti všech těchto vět. Podívejme se ovšem předtím na příklad ilustrující celou situaci:



Obrázek 4.8: Rozklad konečné grupy G na pět pravých tříd vzhledem k podgrupě H . Všechny třídy rozkladu mají stejný počet prvků.

Příklad 19 Uvažujme situaci na obrázku 4.8: všech pravých tříd vzhledem k podgrupě H konečné grupy G je pět – jedna z nich je $H \triangleleft e = H$ a další čtyři jsou $H \triangleleft a$, $H \triangleleft b$, $H \triangleleft c$, $H \triangleleft d$. Existuje bijekce (podle věty 15) 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 16 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 15: pokud všechny pravé třídy mají stejný počet prvků, tak počet všech prvků je pouze nějakým násobkem počtu $|H|$.

Příklad 20 *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 21 *Pokud $|G|$ je prvočíslo, tak grupa G má pouze nevlastní podgrupy (sebe samotnou a jednoprvkovou triviální podgrupu).*

Věta 17 *Pokud $|G| = p$ je prvočíslo, tak grupa (G, ∇) 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 $\langle a \rangle$ je cyklická podgrupa, která má m prvků (a současně z předchozího platí $m > 1$), tj. celkem

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

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

Věta 17 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 jedenáctiprvková 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 18 *Řád každého prvku $a \in G$ je dělitelem řádu konečné grupy G .*

Důkaz: pro prvek $c \in G$ řádu m je $\langle c \rangle$ 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 22 *Protože přirozené číslo, které udává řád podgrupy $|H|$, je dělitelem řádu konečné grupy $|G|$, lze provést tuto operaci dělení přirozeným číslem a označit index podgrupy H v grupě G jako*

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

5 Týden 05

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

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

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

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

Definice 23 *Řád prvku a grupy (G, ∇) 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 22 *Co se týká řádu jednotlivých prvků grupy (S_3, \circ) , platí:*

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

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

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

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

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

Příklad 23 *V grupě $(Z, +)$ je řád všech prvků nekonečný, kromě prvku 0, jehož řád (jako řád každého neutrálního prvku) je roven jedné.*

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

Věta 19 Pro prvek a řádu n v grupě (G, ∇) platí: v této grupě existuje právě n různých hodnot $a^0 = e = a^n$ (e je neutrální prvek grupy), a^1, a^2, \dots, a^{n-1} .

Důkaz: Dokážeme ve dvou částích: a) každá mocnina a^m prvku a řádu n je rovna některé z mocnin a^0, a^1, \dots, a^{n-1} ; b) prvky a^0, a^1, \dots, 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 22 z předmětu Základy matematiky (věta o dělení se zbytkem, která platí pro celá čísla – my ji nyní použijeme pouze pro čísla přirozená) vydělíme $m : n$ a dostaneme, že existují přirozená čísla q, r tak, že

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

Pak lze upravit a^m na tvar

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

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

Důkaz části b): Zbývá dokázat, že prvky a^0, a^1, \dots, a^{n-1} jsou navzájem různé. Pokud se některé z těchto dvou prvků rovnají, platí $a^r = a^s$, kde r i s jsou dvě různá čísla z množiny $\{0, 1, 2, \dots, n - 1\}$, tj. $r \neq s$. BUNO²⁵ 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

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

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. \square

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: $a^{n+1} = a$, $a^{n+2} = a^2$, \dots , $a^{2n-1} = a^{n-1}$, a pak začíná druhé kolo opakování $a^{2n} = e$, $a^{2n+1} = a$, atd.

Věta 20 Pro prvek a nekonečného řádu v grupě (G, ∇) 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 $a^r \nabla (a^s)^{-1}$ dostaneme

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

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

²⁵BUNO = Bez újmy na obecnosti.

sporem je hotov. \square

To tedy znamená, že prvek nekonečného řádu „svým umocňováním“²⁶ 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 je n (**označení 08**: označme $\text{ord}(a) = n$), pak platí pro celočíselné t :

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

(mocnina prvku konečného řádu je rovna neutrálnímu prvku tehdy a jen tehdy²⁷, když mocnitel t je násobek řádu n daného prvku).

Důkaz: Dokážeme obě implikace: Ad „ \Rightarrow “: 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

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

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 „ \Leftarrow “: 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 podíváme na cyklické grupy ještě jednou poté, co známe pojmy izomorfismus grup a řád prvku grupy:

Je jasné, že pokud $\langle a \rangle$ je cyklická grupa generovaná svým prvkem, který je řádu n , platí

$$\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}.$$

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

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

Touto kratinkou úvahou jsme vlastně dokázali větu

²⁶Umocňování = opakované použití operace ∇ na týž prvek.

²⁷Poznámka pro čtenáře v angličtině: anglické matematické vyjadřování vyjadřuje někdy logickou spojku \Leftrightarrow výrazem *iff*, což je zkráceně přesnějšího nematematického *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 ²⁸ jsou navzájem izomorfní.

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

$$\langle a \rangle = \{ \dots, a^{-2}, a^{-1}, e, a, a^2, a^3, \dots \},$$

a tedy můžeme definovat izomorfismus grupy $(Z, +)$ na grupu $(\langle a \rangle, \nabla)$ 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.

Grupy zbytkových tříd

Klíčovou strukturu představuje následující pojem:

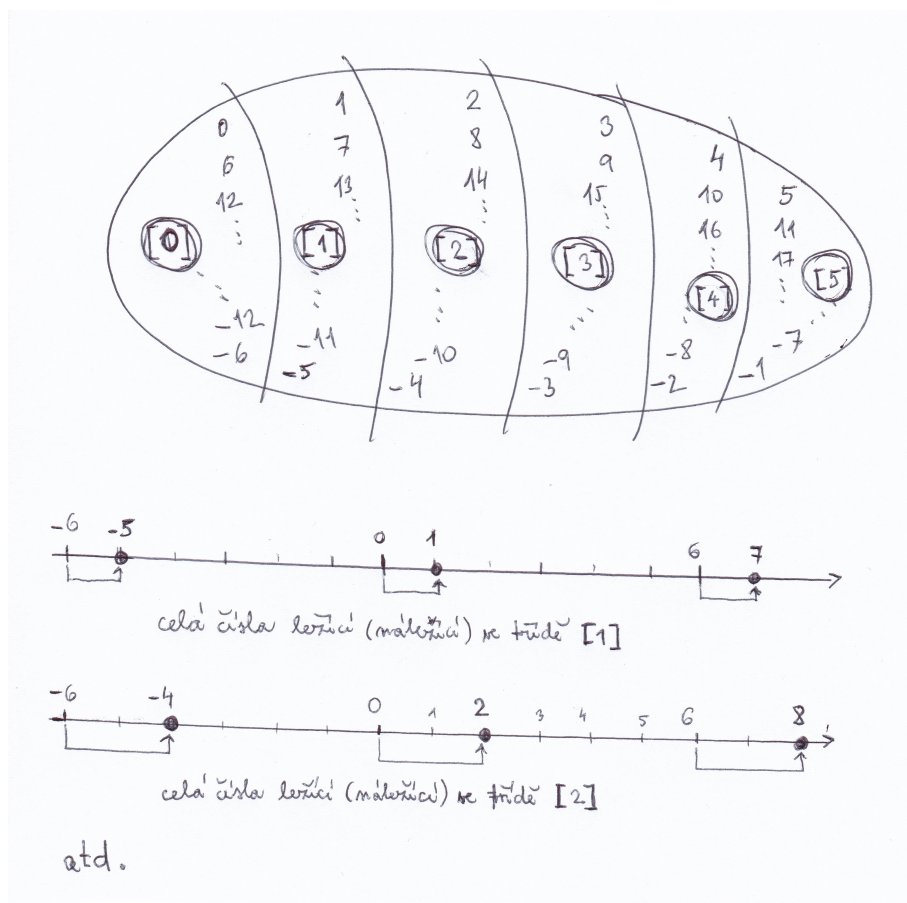
Definice 24 množina zbytkových tříd modulo n ... popíšeme celou konstrukci této množiny například pro $n = 6$: Rozdělíme všechna celá čísla do šesti podmnožin podle toho, jak daleko je dané číslo na číselné ose vpravo od nejbližšího násobku čísla 6 (viz obrázek 5.9). Pak v každé třídě jsou právě ta celá čísla, která jsou mezi sebou kongruentní modulo 6, tj.

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

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

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

²⁸Připomínka bizarní definice řádu grupy: řád grupy = počet prvků grupy.



Obrázek 5.9: Rozdělení celých čísel do šesti podmnožin.

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

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

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

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

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

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

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

Příklad 24 a) Pomocí tabulky operace \oplus dokažte, že (Z_6, \oplus) je grupa:

Tabulka 5.8: Tabulka operace \oplus na množině Z_6 .

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

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

Tabulka 5.9: Tabulka operace \odot na množině Z_6 .

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

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

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

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

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

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

Věta 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 $k = 1, 2, \dots, (n - 1)$, tj. ke všem prvkům (kromě $[0]$, kterou jsme vyloučili) existují inverzní prvky vzhledem k násobení \odot , a tedy (Z_n^*, \odot) je grupa.*

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

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

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

- Cvičení B (str. 108): Příklady řádu prvku.

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

- Cvičení F: řád mocnin prvku.
- Cvičení G: vztah mezi $\text{ord}(a)$ a $\text{ord}(a^k)$.

Úloha 5.2 *Cvičení k pojmu cyklická grupa:*

- Na přednášce už nezbyl čas na důkaz věty: každá podgrupa cyklické grupy je cyklická, tj. lze ji generovat jediným prvkem – kterým?? (viz Pinter 2010, str. 114-115).
- Cvičení A (str. 115): příklady cyklických grup.
- Cvičení B: elementární vlastnosti cyklických grup.

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

Úloha 5.3 Cvičení k pojmu grupy zbytkových tříd:

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

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

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

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

(Z_6, \oplus) je grupa:

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

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

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

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

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

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

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

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

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

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

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

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

Grupa (D_4, \circ) z příkladu 16:

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

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

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

Grupa (Z_6, \oplus) :

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

Výsledky některých cvičení najdete v závěru textu v oddílu [13.5](#).

5.2 Přednáška 05

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

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

- (1) uzavřenost operace = neomezená definovanost operace na dané množině
- (2) asociativita operace
- (3) existence neutrálního prvku dané množiny vzhledem k této operaci
- (4) existence inverzních prvků
- (5) komutativita operace

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

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

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

Zjistili jsme, že $(H_6, +)$ je komutativní grupa, $(Z, +)$ je komutativní grupa, (CF, \circ) je nekomutativní monoid, (S_3, \circ) je nekomutativní grupa, (Z_6, \cdot) je komutativní monoid.

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

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

Pokud zjistíme, že jsou dvě algebraické struktury izomorfní, znamená to nejen, že mají „stejný počet prvků“ (u nekonečných množin říkáme, že mají stejnou mohutnost), ale operace ∇ na množině M_1 se chová zcela stejně, jako operace $*$ na druhé množině M_2 . Každý výsledek operace se zobrazí na příslušný výsledek operace (ZVO): $f(a \nabla b) = f(a) * f(b)$.

Ad příklad 9: $(R, +)$ a (R^+, \cdot) jsou izomorfní komutativní grupy. Izomorfismus lze definovat vztahem $f : (R, +) \rightarrow (R^+, \cdot)$ tak, že $f(x) = e^x$. Jedná se skutečně o bijekci – každému reálnému x (i třeba zápornému) se přiřadí číslo e^x , které je vždy kladné (i když

x je záporné). Naopak ke každému reálnému číslu y lze inverzní funkcí $\ln y$ přiřadit reálné číslo x tak, že $e^x = y$. Navíc platí ZVO:

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

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

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

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

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

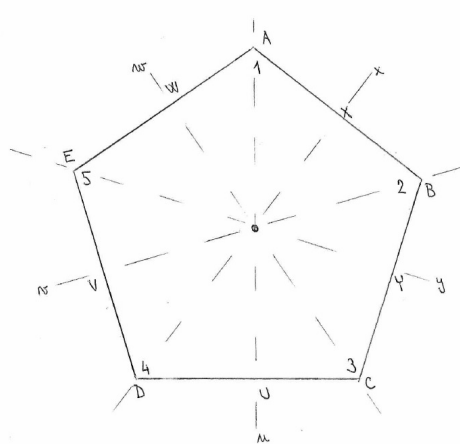
Nyní na 5. přednášce již jenom shrneme to, co bylo dosud řečeno k algebraickým strukturám s jednou operací, na několika příkladech. V přednášce 6 se už začneme věnovat studiu množin, na kterých jsou definovány dvě operace.

Příklad 25 *Cvičení na podgrupy, které využívá poznatku Lagrangeovy věty: Počet prvků podgrupy konečné grupy je dělitelem počtu prvků této grupy.*

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

- e ... identita (nedělá s pětiúhelníkem nic);
- f ... pootočení pětiúhelníka v jeho středu o 72° po směru hodinových ručiček;
- g ... pootočení pětiúhelníka v jeho středu o 144° po směru hodinových ručiček;
- h ... pootočení pětiúhelníka v jeho středu o 216° po směru hodinových ručiček;
- i ... pootočení pětiúhelníka v jeho středu o 288° po směru hodinových ručiček;
- u ... osová souměrnost vzhledem k ose AU , kde A je vrchol pětiúhelníka a U je střed strany CD ;
- v ... osová souměrnost vzhledem k ose BV , kde B je vrchol pětiúhelníka a V je střed strany DE ;

- w ... osová souměrnost vzhledem k ose CW , kde C je vrchol pětiúhelníka a W je střed strany EA ;
- x ... osová souměrnost vzhledem k ose DX , kde D je vrchol pětiúhelníka a X je střed strany AB ;
- y ... osová souměrnost vzhledem k ose EY , kde E je vrchol pětiúhelníka a Y je střed strany BC ;



a informace o vlastnostech, které platí:

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

$|D_5| = 10$, tj. kromě triviálních podgrup $P_1 = \{id\}$, $P_2 = D_5$ budou existovat ještě podgroupy, jejichž počet prvků je dělitelem čísla 10, tj. podgroupy dvouprvkové a pětiprvkové. Pokusme se všechny najít pomocí označení permutacemi pětiprvkové množiny: Klíčem je označit si vrcholy čísla 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 , osově souměrnosti jsou inverzemi sebe sama, tj. jejich připojením k neutrálnímu 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.

$$\text{Např. } f^1 = f$$

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

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

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

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

Takové podgrupě, který je generována jediným prvkem, říkáme cyklická:

$P_3 = \langle f \rangle \dots$ 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 . •

Příklad 26 Cvičení k pojmu levá a pravá třída prvku vzhledem k podgrupě (Pinter 2010, str. 130-135):

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

Například N.1: $H = \langle 5 \rangle$ je podgrupa grupy $(\mathbb{Z}, +)$ generovaná prvkem 5. Vypište všechny pravé třídy prvků vzhledem k podgrupě H .

- C. Důsledky Lagrangeovy věty
- D. Další důsledky Lagrangeovy věty
- E. Vlastnosti tříd prvku vzhledem k podgrupě.

Příklad 27 Lagrangeova věta (a její důsledek – věta 17) společně s větou 22 nám pomalu, ale jistě dává informace o všech konečných grupách o malém počtu prvků:

- Jednoprvková grupa je (až na izomorfismus) jediná a obsahuje pouze neutrální prvek.
- Grupa o prvočíselném počtu prvků 2, 3, 5, 7, atd. je cyklická (věta 17), a tedy až na izomorfismus stejná jako $(H_p, +)$ neboli $(\mathbb{Z}_p, +)$ (věta 22), tedy grupa prvočíselného počtu prvků je až na izomorfismus jediná.
- Dále grupa o počtu prvků p^2 , který je druhou mocninou prvočísla, je podle cvičení G (Pinter 2010, str.154-155) izomorfní buď $(\mathbb{Z}_{p^2}, +)$, nebo $(\mathbb{Z}_p \times \mathbb{Z}_p)$, tedy existují pouze dvě navzájem neizomorfní grupy řádu p^2 .
- Přehled všech šestiprvkových grup: cvičení F, str. 132.
- Přehled všech desetiprvkových grup: cvičení G, str. 132.
- Přehled všech osmiprvkových grup: cvičení H, str. 133.

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

Příklad 28 *Například A.1.*

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

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

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

Příklad 29 *Například A.5: Každá z dvanácti transformací pravidelného šestiúhelníka v grupě (D_6, \circ) (šest pootočení o násobek šedesáti stupňů, včetně identity = pootočení o úhel nulový; dalších šest jsou osové souměrnosti podle tří úhlopříček procházejících protějšími vrcholy (A,D) a (B,E) a (C,F) a podle tří spojnic středů protějších stran) nějak permutuje jeho tři úhlopříčky, které si označme čísly 1 (AD), 2 (BE) a 3 (CF), tj. tato současná permutace šesti vrcholů a permutace tří úhlopříček definuje homomorfismus $f : D_6 \rightarrow S_3$, v obou grupách uvažujeme operaci skládání permutací. Například*

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

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

Příklad 30 *B. Příklady homomorfismu nekonečných grup:*

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

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

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

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

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

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

Příklad 31 *F. Homomorfismus a řád prvku (postup a výsledky tohoto příkladu viz 13.5).*

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

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

Například N.4: Pomocí věty 10 a předchozích dvou větiček F.1, N.3 najděte všechny možné homomorfismy z příkladu A.1, tj. všechny možné homomorfismy grupy (Z_8, \oplus) do grupy (Z_4, \oplus) a určete jejich jádra.

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

Příklad 32 *Například N.1: Uvažujme homomorfismus φ grupy (Z_8, \oplus) do grupy (Z_4, \oplus) definovaný $\varphi(0) = 0$, $\varphi(1) = 1$, atd.*

- a) *Určete jádro K tohoto homomorfismu;*
- b) *Jaké prvky má faktorgrupa Z_8/K s operací rozšířenou na třídy? Je možné vyjádřit obrázkem, ale vyznačte zřetelně prvky faktorgrupy.*

Výsledky některých příkladů najdete v závěru textu v oddílu 13.5.

6 Týden 06

6.1 Přednáška 06: struktury se dvěma operacemi

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

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

- a) Operace $+$ splňuje vlastnosti (1), (2), (3), (4), (5), tj. $(M, +)$ je komutativní grupa;
- b) operace \cdot splňuje vlastnosti (1), (2), (3), tj. množina (M, \cdot) je monoid (= pologrupa s jednotkou);
- c) interakce operací $+$ a \cdot splňuje tzv. distributivní zákon = vlastnost (6):

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

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

Příklad 33 • Příkladem konečného okruhu je struktura zbytkových tříd (Z_n, \oplus, \odot) .

- Příkladem nekonečného okruhu je $(Z, +, \cdot)$, tedy množina celých čísel s tradičními operacemi sčítání a násobení.

Podívejme se např. na množinu Z_6 zbytkových tříd, kde jsou celá čísla rozdělena do 6 podmnožin podle toho, jaký zbytek dávají po dělení šesti. Pouze z pohodlnosti tyto zbytkové třídy označujeme stejně jako celá čísla 0, 1, 2, 3, 4, 5.

Na takto definovaných prvních lze zavést operace sčítání a násobení s následujícími tabulkami:

+	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

Když prozkoumáme vlastnosti těchto operací, tak zjistíme, že

- a) $+$ splňuje vlastnosti (0), (1), (2), (3), (4), (5)
- b) \cdot splňuje vlastnosti (0), (1), (2), (3), (5), nesplňuje vlastnost (4), protože neexistují inverze vzhledem k násobení pro prvky 0, 2, 3, 4.
- c) $+$, \cdot splňuje distributivní zákony (6a), (6b).

Tedy celkem $(Z_6, +, \cdot)$ je komutativní okruh.

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

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

Příklad 34 *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*

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

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

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

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

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

Definice 27 *obor integrity*²⁹ (anglicky: *integral domain*) je množina³⁰ $(M, +, \cdot)$ s operacemi $+$ a \cdot , která je okruhem a navíc jsou splněny vlastnosti:

ad a) Operace $+$ nesplňuje nic navíc;

ad b) operace \cdot splňuje navíc:

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

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

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

Příklad 35 • (Z_7, \oplus, \odot) je konečný obor integrity, protože 7 je prvočíslo, tj. (Z_7^*, \odot) neobsahuje netriviální dělitele nuly.

- $(Z, +, \cdot)$ je nejen nekonečný okruh, ale i nekonečný obor integrity, protože neobsahuje netriviální dělitele nuly a násobení je komutativní, a tedy distributivní zákon lze psát v jedné rovnici.

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

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

ad a) Operace $+$ nesplňuje nic nového,

ad b) operace \cdot splňuje navíc vlastnost (4), tedy $(M - \{0\}, \cdot)$ je grupa³¹;

ad c) zde nic nového.

²⁹Význam 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.

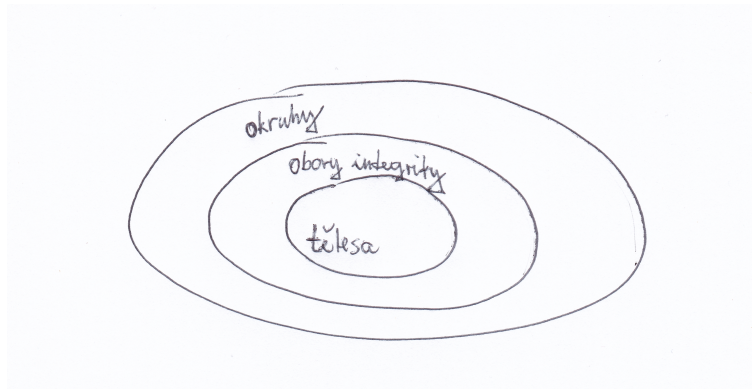
³⁰Aby byla definice naprosto čistá, měli bychom dodat, že množina je minimálně dvouprvková, obsahuje totiž nulu jako jednotkový prvek vzhledem ke sčítání a jedničku jako jednotkový prvek vzhledem k násobení a $0 \neq 1$.

³¹Vlastnost (4) je silnější než vlastnost „neobsahuje netriviální dělitele nuly“, tj. u bodu b) je dostatečné uvést, že operace \cdot u tělesa splňuje (1),(2),(3),(4),(5). Lze dokázat tvrzení, že každé těleso je i oborem integrity, tj. těleso „neobsahuje netriviální dělitele nuly“.

Příklad 36 • (Z_7, \oplus, \odot) je konečný obor integrity, ale též i konečné těleso, protože v případě konečné množiny M pojmy obor integrity a těleso splývají.

- $(Q, +, \cdot)$ je nekonečné těleso, protože $(Q - \{0\}, \cdot)$ je grupa ... je splněna i vlastnost (4), že množina M obsahuje i inverzní prvky vzhledem k operaci násobení.
- $(Z, +, \cdot)$ je nekonečný obor integrity, který není tělesem, protože množina Z neobsahuje většinu inverzních prvků vzhledem k operaci násobení.

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



Obrázek 6.10: Vztah mezi pojmy okruh, obor integrity, těleso.

Příklad 37 Zjistěte, co jsou z algebraického hlediska struktury a) $(2^A, \cup, \cap)$, b) $(2^A, \cap, \cup)$ (2^A ... množina všech podmnožin množiny A pro $A = \{1, 2, 3, 4, 5\}$).

a) $(2^A, \cup, \cap)$:

Vypišme si vlastnosti operací \cup : (1), (2), (3) („nula“ je \emptyset), (5). ((4) neplatí, protože $\{1\} \cup X = \emptyset$ pro žádnou podmnožinu X)

\cap : (1), (2), (3) („jednotka“ je A), (5). ((4) neplatí, protože $\{1\} \cap X = \{1, 2, 3, 4, 5\}$ pro žádnou podmnožinu X)

$\{1\} \cap \{2, 3\} = \emptyset$... existují zde nenulové dělitele nuly!

distributivní zákon (6): $X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$... lze dokázat Vennovými diagramy.

Tuto strukturu bychom snad mohli nazvat polookruh, který obsahuje nenulové dělitele nuly, protože množina podmnožin není grupou vzhledem k žádné z operací \cup, \cap .

b) $(2^A, \cap, \cup)$: Vlastně se jedná o tytéž operace, pouze vlastnost (6) je naopak (sjednocení ve významu „násobení“, průnik ve významu „sčítání“): $X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$

$\{1, 2\} \cap \{3, 4, 5\} = A$... existují zde nenulové dělitele nuly!

Opět $(2^A, \cap, \cup)$ je polookruh, který obsahuje nenulové dělitele nuly.

Co je na příkladech a), b) zajímavé, je to, že distributivní zákon zde platí, i když zaměníme pořadí obou operací!

$$X \cap (Y \cup Z) = (X \cap Y) \cup (X \cap Z)$$

$$X \cup (Y \cap Z) = (X \cup Y) \cap (X \cup Z)$$

To je z algebraického hlediska hodně zajímavé a vedlo to ke studiu množiny všech podmnožin, zavedení pojmu distributivní uspořádané množiny, atd.

Mohlo by vás zajímat, proč nadřazujeme vlastnost (4) v definici tělesa nad vlastnost NNDN v definici oboru integrity. To ještě nebylo vysvětleno.

Jednou z odpovědí, proč těleso je „více než“ obor integrity (v tom smyslu, že splňuje přísnější podmínky, tj. těleso je vlastně méně než oborů integrity) je existence $(Z, +, \cdot)$, to je obor integrity, který není tělesem.

Platí to však vždy, že obor integrity je „méně než“ těleso? Druhou možností odpovědi je větička, že každý konečný obor integrity je tělesem (jinými slovy, pokud M je konečná, tak pojem obor integrity a těleso je jedno a totéž).

Třetí odpověď jde přes vlastnost krácení, kterou jsme již dříve označovali číslem (7). Již bylo řečeno, že v grupě $(M, *)$ platí vlastnost krácení: (7) : $\forall x, y, z \in M : x * y = x * z \Rightarrow y = z$.

(Důkaz jednoduše: V grupě platí (4), tj. $\exists x^{-1}$: vynásobme předpoklad inverzí zleva:

$$x * y = x * z \quad / * x^{-1} \text{ zleva}$$

$$y = 1 * y = x^{-1} * x * y = x^{-1} * x * z = 1 * z = z$$

$$y = z$$

Důkaz je hotov. \square .)

Zkusme si položit otázku, která souvisí se zákonem o krácení: Lze krátit ve strukturách, ve kterých neexistuje inverze x^{-1} z předchozího důkazu - lze např. krátit v okruhu nebo v oboru integrity?

$(Z_6, +, \cdot)$ je okruh, víme, že zde krátit nelze.

$(Z, +, \cdot)$ je obor integrity a víme, že u celých čísel krátit lze. Platí to však vždy? Co když je to jen náhoda? Ukazuje se, že to platí vždy:

Věta 26 V každém okruhu $(M, +, \cdot)$ platí: Je splněna vlastnost (7)* \Leftrightarrow neexistují nenulové dělitelé nuly. ((7)* pro $a, b, c \in M, a \neq 0 : a \cdot b = a \cdot c \Rightarrow b = c$)

Důkaz: ” \Rightarrow ” Předpokládejme, že $(M, +, \cdot)$ je okruh splňující vlastnost (7)*, chceme dokázat, že neexistují nenulové dělitelé nuly.

$\forall a, b \in M$, pro které $a \cdot b = 0$

1) pokud $a = 0$, jsme hotovi, protože a, b nejsou nenulové dělitelé nuly

2) pokud $a \neq 0$, můžeme psát:

$$a \cdot b = 0 = a \cdot 0$$

$a \cdot b = a \cdot 0 \Rightarrow$ platí $(7)^* b = 0$, tedy opět a, b nejsou nenuloví dělitelé nuly. Celkem aspoň jedno z čísel a, b je nula \Rightarrow nejedná se o nenulové dělitele nuly, což jsme chtěli dokázat.

” \Leftarrow ” Předpokládejme, že $(M, +, \cdot)$ je okruh neobsahující nenulové dělitele nuly, ukážeme, že splňuje $(7)^*$.

Pokud $a \neq 0, a \cdot b = a \cdot c \dots a^{-1}$ nemusí existovat, ale nyní využijeme druhé operace, tj. existence prvku $(-a \cdot c)$

$$a \cdot b - a \cdot c = 0 \dots \text{využijeme distributivní zákon (6a)}$$

$$a \cdot (b - c) = 0$$

Víme, že okruh neobsahuje nenulové dělitele nuly \Rightarrow musí nastat $b - c = 0, b = c$, dokázali jsme $(7)^*$. \square .

Ted' už víme, že vlastnost $(7)^*$ je ekvivalentní s vlastností NNDN. Ale vlastnost $(7)^*$ se v každém tělese snadno dokáže vynásobením inverzí a^{-1} , která tam vždy existuje pro $a \neq 0$. Tedy ekvivalentně: žádné těleso neobsahuje nenulové dělitele nuly.

Každé těleso je oborem integrity, každý obor integrity je i okruh (a z tranzitivity pojmu plyne, že i každé těleso je okruh). Ale naopak to neplatí: existují okruhy, které nejsou oborem integrity, např. $(\mathbb{Z}_6, \oplus, \odot)$; a existují obory integrity, které nejsou tělesem, např. $(\mathbb{Z}, +, \cdot)$.

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

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

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

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

Příklad 38 *Nejpřirozenějším příkladem ideálu je podmnožina B sudých celých čísel okruhu $(\mathbb{Z}, +, \cdot)$:*

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

Je zřejmé, že $(B, +)$ je podgrupa grupy $(\mathbb{Z}, +)$ 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 $(\mathbb{Z}, +, \cdot)$.

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

Příklad 39 Pro $M = (Z, +, \cdot)$ jsou hlavními ideály tyto množiny:

- $B_1 := \langle 1 \rangle \dots$ 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);
- $B_2 := \langle 2 \rangle \dots$ ideál generovaný prvkem 2 a všemi součiny $2 \cdot z$ pro $z \in Z$, tj. jedná se o ideál z příkladu 6.5:

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

- $B_3 := \langle 3 \rangle \dots$ 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 $B = \langle 3, 7 \rangle$, 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

$$\langle \{3, 7\} \rangle = Z = \langle 1 \rangle.$$

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

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

6.2 Cvičení 06: Algebraické struktury se dvěma binárními operacemi

Je možné, že toto cvičení a pojmy související se strukturou se dvěma operacemi budete na cvičení probírat dříve než v šestém týdnu – sledujte rozvrh cvičícího.

Úloha 6.1 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 6.2 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 6.3 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 6.4 V množině (Z_6, \oplus, \odot) sestavte operační tabulku pro operace \oplus a \odot . Určete typ struktury (Z_6, \oplus, \odot) .

Úloha 6.5 Výpočtem určete typ algebraické struktury (Z_5, \oplus, \odot) .

Úloha 6.6 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:

- Které z vlastností (1) až (10) splňuje struktura $(2^P, \cup, \cap)$ pro $P = \{a, b, c\}$?
- Jak byste strukturu $(2^P, \cup, \cap)$ z části (a) nazvali (okruh, obor integrity, těleso, nebo něco jiného)?
- 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.
- 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 $A \dot{\div} B := (A - B) \cup (B - A)$ a klasickou operaci \cap průniku. Sestavte tabulky operací $\dot{\div}$ a \cap na množině 2^P .
- b) Jak byste strukturu $(2^P, \dot{\div}, \cap)$ 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.

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

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

7 Týden 07

7.1 Cvičení 07: Polynomy 01

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

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

Doporučené materiály k využití:

- Označení: $(Z[x], +, \cdot)$, $(Q[x], +, \cdot)$, $(R[x], +, \cdot)$, ... po řadě okruhy polynomů s koeficienty z okruhu celých čísel, tělesa racionálních čísel a tělesa reálných čísel. Tyto okruhy neobsahují netriviální dělitele nuly, takže se jedná o obory integrity (Budínová 2013, str. 7, věta 1). Ideální definice okruhu $Z[x]$: jedná se o rozšíření okruhu $(Z, +, \cdot)$ o prvek x , kde nevíme, co je, může tam být cokoliv, třeba³² 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 $(x + 2)$:

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

například

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

- Budínová 2013, str. 18-21 po pojem ireducibilní 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).

³²Pinter, 2010, str. 241.

7.2 Přednáška 07: Přehled algebraických metod hledání kořene polynomu

Označme

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

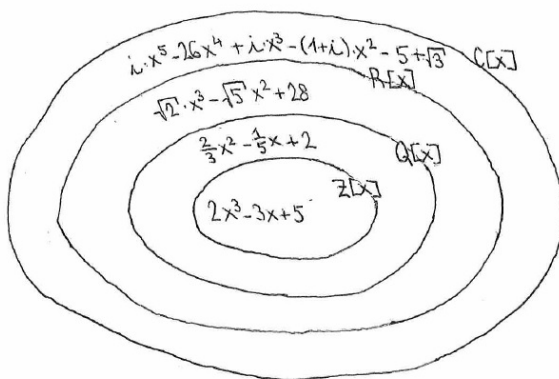
$Q[x] := \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0; a_i \in Q, n \in N\}$ množinu polynomů s racionálními koeficienty, x je proměnná

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

$C[x] := \{a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0; a_i \in C, n \in N\}$ 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 některá 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 polynomem 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 $n(x) = 0 \dots$ 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 $j(x) = 1 \dots$ 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 $p(x) \cdot (q(x) + r(x)) = p(x) \cdot q(x) + p(x) \cdot r(x) \dots \forall p(x), q(x), r(x)$

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 nenulové 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 31 $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \dots$ prvek množiny $Z[x], Q[x], R[x]$ nebo $C[x]$ se nazývá polynom stupně n .

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.

Definice 32 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 \dots v případě polynomu $p(x)$
- dostaneme pravdivou rovnost \dots 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) $a \cdot x + b = 0 \dots$ to je tzv. lineární rovnice

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

$0 \cdot x + 5 = 0 \dots$ nemá řešení

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

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

b) $a \cdot x^2 + b \cdot x + c = 0 \dots$ 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.

$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \dots$ 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.

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

Už jsme si říkali v ZÁKLADNÍCH MATEMATIKY, že komplexní čísla $a + bi$ lze mezi sebou násobit i sčítat, dokonce existují i inverze vzhledem k oběma operacím (tj. komplexní čísla můžeme odčítat i dělit - vyjma dělení nulou, kterou jsme ovšem nemohli dělit ani v Z, Q, R). Zkratka $(C, +, \cdot)$ je těleso, tj. struktura s hezkými algebraickými vlastnostmi k oběma operacím.

Matematický model komplexního čísla tedy sestrojít lze, otázkou je, k čemu je to dobré kromě základní věty algebry, kterou si řekneme za chvíli. Nakonec se ukázalo, že komplexní čísla jsou užitečná tam, kdekoliv chceme něco znázornit v rovině: komplexnímu číslu $a + bi$ totiž jednoznačně odpovídá bod $[a; b]$ v rovině. A jakmile se spojilo komplexní číslo s geometrickým významem, ukázalo se, že řadu úkolů, operací s body a vektory v rovině lze stejně dobře popsat či řešit pomocí komplexních čísel.

Příklad 40 V analytické geometrii lze přímku procházející bodem $[2; 1]$ se směrovým vektorem $(1, \frac{-1}{2})$ vyjádřit parametrickými rovnicemi

$$x = 2 + t \cdot 1$$

$$y = 1 + t \cdot \left(\frac{-1}{2}\right) \quad , t \in R$$

Tutéž přímku lze vyjádřit pomocí komplexních čísel jako

$$z = (2 + i) + t \cdot \left(1 - \frac{-1}{2}\right), \quad t \in \mathbb{R}$$

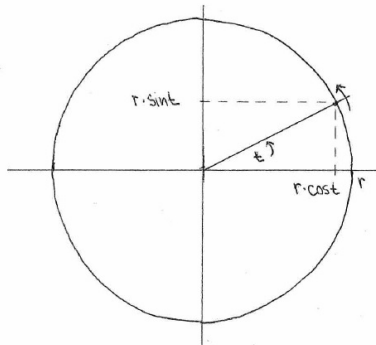
neboli dvourozměrné vektory „schováme“ do komplexních čísel, a pokud potřebujeme, k dílčím souřadnicím těchto čísel se dostaneme tak, že vezmeme/najdeme jejich reálnou část:

$x = \operatorname{Re} z =$ to, co není koeficientem u čísla i

$y = \operatorname{Im} z =$ to, co je koeficientem u čísla i

Tímto způsobem převedeme reálný případ na komplexní a naopak.

Příklad 41 Ještě zajímavější a užitečnější souvislosti najdeme při popisu pohybu bodu/objektu po kružnici o poloměru r : při popisu pomocí obloukové míry (proměnná t je rovna velikosti úhlu v radiánech) musíme užít funkcí \sin, \cos : souřadnice pohybujícího se objektu jsou $[r \cdot \cos t, r \cdot \sin t]$, dostáváme tedy rovnice $x = r \cdot \cos t, y = r \cdot \sin t$.



Při využití komplexních čísel se využívá starý Eulerův vzorec $e^{it} = \cos t + i \cdot \sin t$, takže rovnoměrný pohyb objektu po kružnici lze popsat rovnicí $z = r \cdot e^{it}$ (kde $z = x + iy$ je vztah mezi komplexním číslem z a vektorem (x, y)).

Protože pomocí vzorců pro okamžitý (či kmitavý) pohyb lze dobře popsat elektrický proud, komplexních čísel s oblibou využívají kolegové v elektrotechnice, místo aby pracovali s vektory v rovině.

Budeme tedy mírně pracovat i s imaginární jednotkou i s tou informací, že jedním z jejích využití je popis práce s body a vektory v rovině.

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

Pro tuto rovnici a její řešení existují obecné vzorce pro $a, b, c, d \in \mathbb{R}$ (tzv. Cardanovy vzorce - viz BP Ivety Trombikové, najdete v IS tohoto předmětu, str. 22 – 23). Tyto vzorce se příliš neuvžívají, 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) $ax^4 + bx^3 + cx^2 + dx + e = 0, a \neq 0 \dots$ 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. 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.

Příklad 42

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

$$x - (-2)$$

	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:

$$6x^3 + 13x^2 - 4 = 0$$

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

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

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

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

Ad Příklad 42: Náš polynom $6x^3 + 13x^2 - 4$ 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 $(x - x_i)$.

Příklad 43 Hodnoty x_i jsou obecně komplexní, což vidíme např. u polynomu $(x^2 + 1)$, který lze rozložit na součin $(x+i) \cdot (x-i)$ nebo u polynomu $(x^2 + x + 1)$ můžeme psát $(x + \frac{1}{2} + i\frac{\sqrt{3}}{2}) \cdot (x + \frac{1}{2} - i\frac{\sqrt{3}}{2})$ (při výpočtu jsme $\sqrt{-3}$ upravili na $i \cdot \sqrt{3}$ za využití označení, že $i = \sqrt{-1}$). Můžete si zkusit zpětným roznásobením závorek, že dostanete původní polynom.

Klíčovou otázkou zůstává, jakým způsobem jsme zjistili, že v příkladu 42 máme do Hornerova schématu dosadit zrovna číslo $c = -2$. Určitou odpověď na tuto otázku dává:

Věta 28 *Věta o racionálních kořenech polynomu:* Pokud polynom $p(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in Z[x]$ 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 44 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	<u>0</u>	

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	<u>0</u>	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	<u>0</u>		

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 víme z příkladu ???. Z tohoto zápisu již vidíme řešení: $2 \cdot (x + \frac{1}{2}) \cdot (x - 3) \cdot (x + 2) \cdot (x + (\frac{1}{2} + i\frac{\sqrt{3}}{2})) \cdot (x + (\frac{1}{2} - i\frac{\sqrt{3}}{2})) = 0$.

★

Definice 33 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 45 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	<u>0</u>	a hned dosadíme 2 ještě jednou
2	1	4	-3	-18	<u>0</u>		
2	1	6	9	<u>0</u>			všechny koeficienty jsou kladné, tj. eventuální další řešení musí být záporné
-3	1	3	<u>0</u>				
-3	1	<u>0</u>					

Tedy po rozkladu získáváme $(x - 2)^3 \cdot (x + 3)^2 = 0$. Řešení naší rovnice jsou tedy pouze dvě. ★

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

Věta 29 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 $p(x) \rightarrow v(x)$ umožňuje snížit stupeň polynomu dříve, než začneme hledat jeho kořeny.

Příklad 46 Pokud $p(x)$ žádné vícenásobné kořeny nemá, $d(x) = \text{NSD}(p, p') = 1$, takže $v(x) = p(x)$, polynom $p(x)$ se při převodu na $v(x)$ vůbec nezmění.

Příklad 47 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:

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

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

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

$$\begin{array}{r} v(x) = p(x) : d(x) = (16x^4 + 32x^3 + 40x^2 + 24x + 9) : (8x^2 + 8x + 6) = 2x^2 + 2x + \frac{3}{2} \\ -(16x^4 + 16x^3 + 12x^2) \\ \hline 16x^3 + 28x^2 + 24x + 9 \\ -(16x^3 + 16x^2 + 12x) \\ \hline 12x^2 + 12x + 9 \\ -(12x^2 + 12x + 9) \\ \hline 0 \end{array}$$

Tedy rovnici lze psát ve tvaru $(8x^2 + 8x + 6) \cdot (2x^2 + 2x + \frac{3}{2}) = 0$
 $(4x^2 + 4x + 3) \cdot (4x^2 + 4x + 3) = 0$
 $(4x^2 + 4x + 3)^2 = 0$

$$x_{1,2} = \frac{-4 \pm \sqrt{16-48}}{8}$$

$$x_1 = \frac{-1}{2} + i\frac{\sqrt{2}}{2} \dots \text{kořen násobnosti 2} \quad x_2 = \frac{-1}{2} - i\frac{\sqrt{2}}{2} \dots \text{kořen násobnosti 2}$$

Celkem lze tedy náš polynom $16x^4 + 32x^3 + 40x^2 + 24x + 9$ rozložit a řešit rovnici ve tvaru: $16 \cdot (x + \frac{1}{2} + i\frac{\sqrt{2}}{2})^2 \cdot (x + \frac{1}{2} - i\frac{\sqrt{2}}{2})^2 = 0 \dots$ algebraický rozklad dané rovnice v komplexním oboru. ★

- C) Polynom $p(x) \in R[x]$ musí mít komplexní kořeny „po dvojicích“ ve tvaru $a \pm i \cdot b$:
 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.
- D) (Budínová, str. 29, věta 16): Pro všechny kořeny polynomu $a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ platí:

$$|x_i| < 1 + \frac{\max\{|a_0|, |a_1|, \dots, |a_{n-1}|\}}{|a_n|}.$$

Označíme-li konstantu na pravé straně r , tak všechny kořeny polynomu, reálné i komplexní, musí ležet v komplexní rovině uvnitř kruhu se středem v 0 a poloměrem r , jelikož absolutní hodnota komplexního čísla $|x_i|$ znamená vzdálenost x_i od počátku. Jinými slovy, mezi kořeny a koeficienty dané algebraické rovnice existuje právě uvedený vztah: kořeny jsou blíže počátku než $\max\{|a_0|, |a_1|, \dots, |a_{n-1}|\}$ vydělené absolutní hodnotou $|a_n|$.

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

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

Dosazením do uvedeného vzorce v našem příkladu máme

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

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 6,5.

E) Hranice algebry:

Vysvětleno na příkladu: řešte rovnici $2x^5 + 3x^4 - 7x^3 + 6x^2 - 11x + 5 = 0$.

A) Pomocí Hornerova schématu a věty o racionálních kořenech ověříme, zda je některý ze zlomků $\pm 1, \pm 5, \pm \frac{1}{2}, \pm \frac{5}{2}$ kořenem polynomu na levé straně rovnice. Zjistíme, že polynom žádné racionální kořeny nemá.

B) Procesem odstranění násobných kořenů zjistíme, že polynom žádné vícenásobné kořeny nemá, tedy $v(x) = p(x)$. Tím jsme zjistili, že $p(x)$ má pět různých jednonásobných kořenů.

C) $p(x)$ má jen reálné koeficienty \Rightarrow pokud má $p(x)$ komplexní koeficienty, tak vždy po dvojicích, komplexně sdružené kořeny tvaru $a \pm i \cdot b$.

D) Pro každý z pěti kořenů platí $|x_i| \leq 1 + \frac{\max\{3, 7, 6, 11, 5\}}{2} = 1 + \frac{11}{2} = 6,5$. Všechny kořeny leží uvnitř kruhu se středem v 0 a poloměrem 6,5.

Tím končí možnosti algebry a nastupují numerické metody, kterým se budeme věnovat na následující přednášce.

8 Týden 08

8.1 Cvičení 08: Polynomy 02

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

Využijte například následující materiál:

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

8.2 Přednáška 08: Přehled numerických metod hledání kořene polynomu

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

Vraťme se např. k následujícímu příkladu:

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

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

Hornerovým schématem jsme ověřili, že žádné racionální řešení neexistuje. Všechna řešení tedy jsou reálná iracionální, nebo komplexní. Víme také, že polynom nemá žádné vícenásobné kořeny, takže má pět různých jednonásobných kořenů.

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

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

Dosazením do uvedeného vzorce v našem příkladu máme

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

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 6,5.

- B) Jemnější detekce reálných řešení: Z předcházejícího bodu víme, že $x \in \langle -6,5; 6,5 \rangle$. 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 $-6,3, \dots$, pak $6,3$, pak $6,4$, pak $6,5$.

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

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

Celý postup lze snadno předvést v jazyce R (lze volně stáhnout 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):

$$\begin{aligned} y &< -seq(from = -3.5, to = 3.5, by = 0.01) \\ pp &< -2 * y^5 + 3 * y^4 - 7 * y^3 + 6 * y^2 - 11 * y + 5 \\ plot(y, pp) \end{aligned}$$

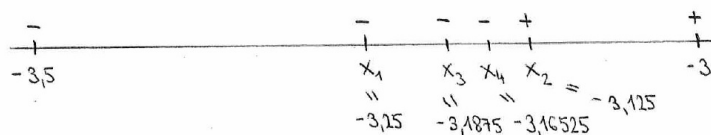
(obrázek lze „zvětšit“ zadáním kratšího intervalu při definici vektoru y , například $from = 0$ a $to = 1.5$ nakreslí graf na sporném intervalu, na kterém existují dvě řešení).

- C) Finální dopočtení kořenů: Víme, že řešení z_1, z_2, z_3 jsou iracionální, tj. jejich rozvoj je neperiodický neukončený, proto je nemůžeme přesně vyčíslit. Ovšem pokud se spokojíme s přesností třeba 5 platných číslic, počítat tuto přesnost najde velmi rychle. Podívejme se na dvě metody, jakými k řešení můžeme dospět:

Metoda půlení intervalu při řešení rovnice $p(x) = 0$ (vysvětlení viz BP (Trombiková, 2019, str. 28-30))

Vycházíme ze situace $p(-3,5) < 0$; $p(-3) > 0$

- 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 $z_1 \doteq -3,12991$.



Obrázek 8.11: Metoda půlení intervalu

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 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:

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

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

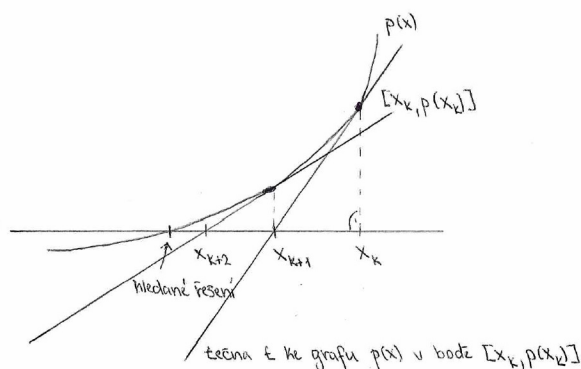
Pokud celý postup (posloupnost tří kroků ukončených ENTER) zopakujeme pouze pro volbu $a = 0,5$, $b = 1$, najdeme řešení $z_2 = 0,54689$. Toho lze dosáhnout velmi jednoduše, protože v prostředí R nemusíme už jednou napsané příkazy vypisovat znovu, ale volbou šipky nahoru se lze dostat na předchozí tři 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.

Metoda Newtonova = metoda tečen: obrázek a vysvětlení viz BP Trombiková, str. 34-38: S velmi rychlou metodou přišel Izák Newton: využil při tom pojem tečny ke grafu funkce:



Obrázek 8.12: Newtonova metoda = metoda tečen

- a) Zvolíme bod x_0 vhodně blízko našeho řešení.
 b) Sestavujeme posloupnost bodů x_1, x_2, x_3, \dots 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} :

$$x_{k+1} = x_k - \frac{p(x_k)}{p'(x_k)}.$$

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 $x_2 \doteq z_2 = \underline{0,54689}$.
 $z_3 \in \langle 1; 1,5 \rangle$: Volbou $x_0 = 1,5$ dostaneme po čtyřech krocích $x_4 \doteq z_3 = \underline{\underline{1,22892}}$.

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:

- $x_0 = 1 + i \dots$ 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.
- $x_0 = 1 + 2i \dots$ 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.
- $x_0 = 1 + 3i \dots$ 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 $z_5 \doteq \underline{\underline{-0,07295 - i \cdot 1,08773}}$

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 $z_4 \doteq -0,07295 + i \cdot 1,08773$; $z_5 \doteq -0,07295 - i \cdot 1,08773$

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

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

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

$$z < - - 3.5$$

a ENTER, a provedeme cyklus WHILE:

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

(a ENTER) ... po několika krocích bude nalezeno řešení $z_1 = -3,12991$. Podobně pro vstupní $z = -1$ dostaneme $z_3 = 1,22892$ a pro vstupní $z = 0,5$ dostaneme $z_2 =$

0,54689. Slabina Newtonovy metody: díky konstrukci pomocí tečny může postup zcela zhavarovat, směřovat do nekonečna nebo najít řešení, které už známe z jiného intervalu (jak se to stalo při volbě $z = 1$).

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

- Volme vstupní $z = 1 + 1i$, najedme šipkou na příkaz cyklu WHILE a stiskneme 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.
- Celkem jednoduchou metodou lze najít komplexní řešení speciální rovnice, tzv. binomické rovnice, protože je v této rovnici pouze binom = dvojčlen: mocnina neznámé z a nějaké komplexní číslo. Tento poslední rychlý způsob pro tuto speciální rovnici se studenti naučí v následujících čtrnácti dnech, které budou věnovány komplexním číslům.

9 Týden 09

9.1 Cvičení 09: Polynomy 03

Dodělání osnovy na cvičení pro polynomy, viz plán cvičícího.

9.2 Přednáška 09: 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.

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.

Věta 30 N je až na izomorfismus jediným modelem struktury zvané Peanova množina.

Co to je Peanova množina?

Na této množině platí čtyři axiomy:

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 .

Poznámka:

1. axiom 4: 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.

2. Ještě je důležité říci, že N je jediným modelem Peanovy množiny až na izomorfismus, tj. kdyby nějaká množina S také splňovala Peanovy axiomy, tak existuje bijekce $b: N \rightarrow S$, která

- 1) zachovává všechny následníky,
- 2) zobrazí 1 na e_s ,
- 3) zachovává různost následníků pro různé prvky,
- 4) z axiomu 4) už bijekce b nemusí splňovat žádnou další vlastnost.

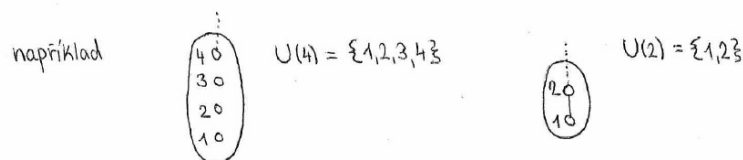
Význam Peanových axiomů: Díky jedinečnosti (až na izomorfismus) charakterizují tyto čtyři axiomy právě množinu N a žádnou jinou. Jedná se tedy o jakési vnitřní či charakteristické axiomy množiny N .

Velice zajímavé je to, že na základě Peanových axiomů lze na množině P už dále definovat všechny další vlastnosti, které na známé množině N existují:

- relaci uspořádání \leq
- operaci $+$
- operaci \cdot

Například 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 kromě 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. Dále lze pomocí Peanových axiomů a pomocí právě definovaného uspořádání jejích prvků definovat operace sčítání i násobení³³ tak, že $(P_0, +, \cdot)$ je komutativní polookruh (stejně jako $(N_0, +, \cdot)$ je komutativní polookruh).

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.

Intuitivně řečeno:

- 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 komutativní 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 $a \cdot (b + c) = ab + ac \quad \forall a, b, c \in Q$

(nenulové 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.

³³Definovat operace sčítání a násobení už tady v této chvíli nebudeme, cílem těchto dvou stran bylo naznačit, že Peanovy axiomy tvoří jakousi minimální množinu axiomů, pomocí nichž lze definovat všechny pojmy, pro které platí všechny vlastnosti struktury $(N, +, \cdot)$, ze které dodáním 0 vzhledem ke sčítání vznikne komutativní polookruh $(N_0, +, \cdot)$

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 množině, 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.

Věta 31 *Z komutativní pologrupy $(G, *)$ lze vždy vytvořit grupu.*

Jakým způsobem? Popišme si tuto konstrukci podrobněji:

- i) Vytvoříme kartézský součin $G \times G$, na němž máme přirozeně definovanou operaci „po složkách“: $[a, b] * [c, d] = [a * c, b * d]$ ³⁴
- ii) Definujme na $G \times G$ relaci ekvivalence \sim takto: $[a, b] \sim [c, d]$, když $a * d = b * c$
- iii) Vytvořme faktormnožinu $G \times G / \sim$, tj. rozklad množiny $G \times G$ vzhledem k ekvivalenci \sim na navzájem disjunktní podmnožiny, a tyto podmnožiny budeme chápat jako prvky množiny $G \times G / \sim$.
- iv) Na množině $G \times G / \sim$ definujme operace \otimes mezi jejími prvky takto:

$$\{[a, b]\}^{35} \otimes \{[c, d]\} := \{[a * c, b * d]\}$$

Struktura $(G \times G / \sim)$ je grupa, protože operace mezi množinami splňuje vlastnosti (1), (2), (3), (4):

- (1) Uzavřenost plyne ze staré struktury - stará operace $*$ nám po složkách vytvoří prvek $[a * c, b * d]$, a ten zase leží v nějaké podmnožině množiny $G \times G / \sim$.
- (2) Asociativita nové operace \otimes plyne z asociativity staré operace $*$.
- (3) $\{[x, x]\}^{36}$ je neutrálním prvkem vzhledem k operaci \otimes , protože $\forall \{[a, b]\} \in G \times G / \sim$ platí:

$$\{[a, b]\} \otimes \{[x, x]\} = \{[a * x, b * x]\}$$

a podle definice \sim máme $[a, b] \sim [a * x, b * x]$, protože $a * b * x = b * a * x$, což plyne z komutativity staré operace $*$.

³⁴operace $*$ ze „staré“ pologrupy

³⁵podmnožina obsahující prvek $[a, b]$

³⁶ x je libovolný prvek staré pologrupy $(G, *)$

Tedy prvky $[a, b]$, $[a * x, b * x]$ leží ve stejné podmnožině rozkladu, tj. $\{[a, b]\} = \{[a * x, b * x]\}$ (podmnožina obsahující $[a, b]$ je tatáž podmnožina, která obsahuje i prvek $\{[a * x, b * x]\}$).

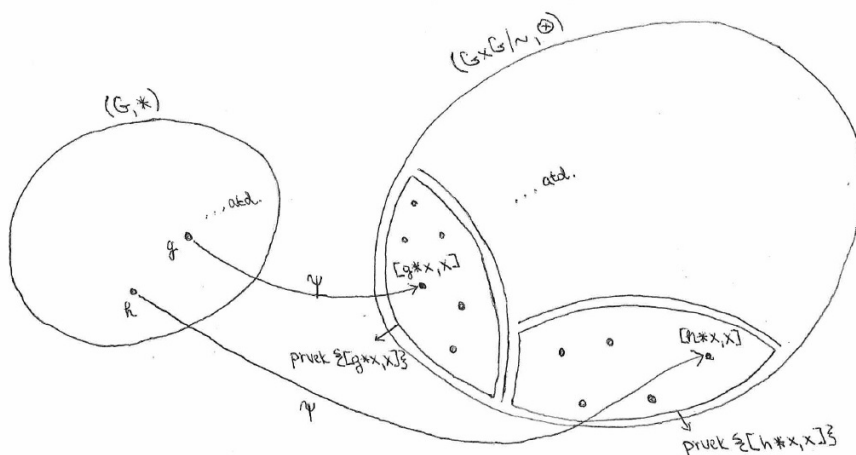
(4) $\forall \{[a, b]\}$ najdeme prvek inverzní, tím bude prvek $\{[b, a]\}$:

$$\{[a, b]\} \otimes \{[b, a]\} = \{[a * b, b * a]\} = {}^{37} \{[x, x]\}.$$

Jsme hotovi, zkonstruovali jsme z pologrupy grupu!

Dokonce jsme schopni tvrdit něco víc, a sice že existuje injektivní homomorfismus komutativní pologrupy $(G, *)$ do grupy $(G \times G/\sim, \otimes)$, tj. pologrupu $(G, *)$ lze injektivně vnořit do grupy $(G \times G/\sim, \otimes)$:

Definujme zobrazení $\psi(g) = \{[g * x, x]\}$.



Obrázek 9.13: Injektivní vnoření pologrupy $(G, *)$ do grupy $(G \times G/\sim, \otimes)$

Zobrazení $\psi : G \rightarrow G \times G/\sim$ přiřadí prvku $g \in G$ tu podmnožinu z $G \times G/\sim$, která obsahuje prvek $[g * x, x]$.

Zobrazení ψ :

1. je injektivní: pro $g \neq h$: $[g * x, x]$ není v ekvivalenci s prvkem $[h * x, x]$, tedy prvky $[g * x, x]$, $[h * x, x]$ neleží ve stejné podmnožině rozkladu, ale v různých podmnožinách: $\{[g * x, x]\} \neq \{[h * x, x]\}$
2. zachovává výsledky operace: označme $k := g * h$, $\psi(g) = \{[g * x, x]\}$
 $\psi(h) = \{[h * x, x]\}$

³⁷platí komutativita staré operace $*$

$$\psi(k) = \{[k * x, x]\}$$

Dokažme $\psi(g * h) = \psi(g) \otimes \psi(h)$ (podmínka zachování výsledků operace):

$$\text{a) } \psi(g * h) = \underbrace{\{g * h * x, x\}}_k = \{[k * x, x]\} = L$$

$$\text{b) } \psi(g) \otimes \psi(h) = \{[g * x, x]\} \otimes \{[h * x, x]\} = \{[g * x * h * x, x * x]\} =^{38} \\ \{[g * h * x^2, x^2]\} =^{39} \{[g * h * x, x]\} = \{[k * x, x]\} = P$$

\Rightarrow Dohromady: ψ je injektivní homomorfismus, pologrupu G „vnořuje“ do grupy.

Injektivní vnoření vlastně znamená, že množina G je izomorfní s nějakou podmnožinou prvků z $G \times G/\sim$, tedy s podmnožinou podmnožin množiny $G \times G/\sim$.

Reformulace věty 31: Každou komutativní pologrupu $(G, *)$ lze injektivně vnořit do grupy $(G \times G/\sim, \otimes)$, neboli každou komutativní pologrupu $(G, *)$ lze rozšířit na grupu $(G \times G/\sim, \otimes)$.

Této větě se říká věta o vnoření pologrupy do grupy, nebo věta o rozšíření pologrupy na grupu.

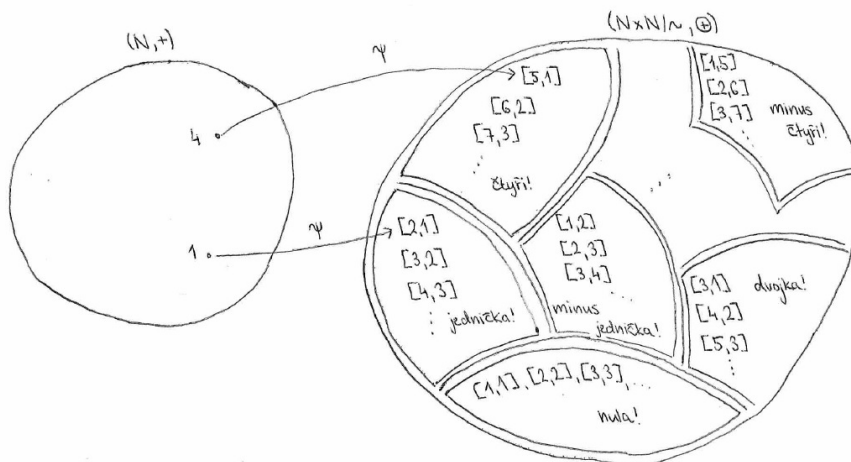
Konstrukce $N \rightarrow Z$:

Věta 32 S využitím věty 31 lze komutativní pologrupu $(N, +)$ injektivně vnořit do grupy (= rozšířit na grupu) $Z := (N \times N/\sim, \oplus)$.

Věta 32 je tedy formálně naprosto přesný algebraický postup rozšíření přirozených čísel na celá čísla.

³⁸Nyní potřebujeme komutativitu operace, abychom mohli pořadí prvků měnit, tj. prvky x v první složce sloučit do mocniny.

³⁹protože $[g * h * x^2, x^2] \sim [g * h * x, x]$



Obrázek 9.14: Injektivní vnoření komutativní pologrupy $(N, +)$ do grupy $Z := (N \times N / \sim, \oplus)$

Zobrazení ψ definujeme vztahem $\psi(n) = \{[n + 1, 1]\}$.

- 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 $a + d = b + c$.
- 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):

$$\{[a, b]\} \oplus \{[c, d]\} := \{[a + c, b + d]\}$$

Tato operace \oplus splňuje na množině $N \times N / \sim$ vlastnosti:

(1) Uzavřenost plyne z uzavřenosti „staré operace“ $+$ v jednotlivých souřadnicích = složkách.

(2) Asociativita \oplus plyne ze „staré“ asociativity operace $+$ v jednotlivých souřadnicích = složkách.

(3) Neutrálním prvkem je třída $\{[1, 1]\}$, což je třída obsahující prvky $[1, 1], [2, 2], [3, 3], \dots$

(4) Např. pro $\{[6, 2]\}$ je inverzí $\{[2, 6]\}$.

\Rightarrow Tedy $(N \times N / \sim, \oplus)$ je grupa!

Zobrazení $\psi : N \rightarrow N \times N/\sim$ je injektivní homomorfismus, tedy vnoření $(N, +)$ do struktury $(N \times N/\sim, \oplus)$.

Vysvětlení: 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 homomorfismem ψ .

10 Týden 10

10.1 Cvičení 10: Komplexní čísla 01

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

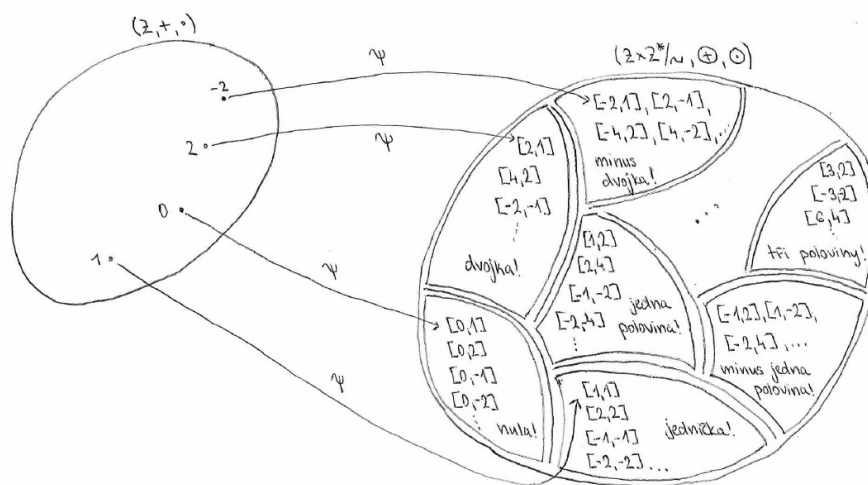
Lze postupovat podle nejnovější učebnice pro střední školy (Robová, Hála, Calda 2013), ale vše se asi nestihne, tj. cvičící rozhodnou, co přesně ve cvičeních 10 a 11 stihne probrat.

10.2 Přednáška 10: Konstrukce oborů \mathbb{Q} , \mathbb{R} , \mathbb{C}

Konstrukce $Z \rightarrow Q$, konstrukce $Q \rightarrow R$, konstrukce $R \rightarrow C$.

Na této přednášce budeme pokračovat v konstrukcích číselných oborů. Začneme konstrukcí $Z \rightarrow Q$:

Věta 33 S využitím věty 31 lze komutativní obor integrity $(Z, +, \cdot)$ injektivně vnořit do tělesa (= rozšířit na těleso) $Q := (Z \times Z^* / \sim, \oplus, \odot)$.



Obrázek 10.15: Injektivní vnoření komutativního oboru integrity $(Z, +, \cdot)$ do tělesa $(Z \times Z^* / \sim, \oplus, \odot)$

Zobrazení ψ definujeme vztahem $\psi(z) = \{[z \cdot 1, 1]\}$.

a) Na $Z \times Z^*$ definujeme relaci ekvivalence \sim takto: $[a, b] \sim [c, d]$, když $a \cdot d = b \cdot c$ ⁴⁰.

b) Vytvoříme faktormnožinu $Z \times Z^* / \sim$ definujeme operace \oplus, \odot takto:

$$\{[a, b]\} \oplus \{[c, d]\} := \{[ad + bc, b \cdot d]\}^{41}{}^{42}$$

$$\{[a, b]\} \odot \{[c, d]\} := \{[a \cdot c, b \cdot d]\}^{43}$$

(Pro $\{[a, b]\}$ je inverzí vzhledem k \oplus prvek $\{[-a, b]\}$,
pro $\{[a, b]\}$ je inverzí vzhledem k \odot prvek $\{[b, a]\}$.)

⁴⁰stará operace \cdot v $(Z, +, \cdot)$

⁴¹„staré“ operace na $(Z, +, \cdot)$; $b \cdot d$ nikdy není rovno 0, protože $b \neq 0, d \neq 0$

⁴²definici si zapamatujte tak, že operace se chová stejně jako sčítání zlomků převodem na společného jmenovatele: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{b \cdot d}$

⁴³chová se podobně jako násobení zlomků $\frac{a}{b} \cdot \frac{c}{d} = \frac{a \cdot c}{b \cdot d}$

Pak $(Z \times Z^*/\sim, \oplus)$ je komutativní grupa,
 $(Z \times Z^*/\sim, \odot)$ je komutativní grupa,
operace \oplus, \odot splňují distributivní zákon, tj celkem $(Z \times Z^*/\sim, \oplus, \odot)$ je těleso!

d) Zobrazení $\psi : Z \rightarrow Z \times Z^*/\sim$ je injektivní homomorfismus, tj. původní výsledky sčítání a násobení celých čísel zůstanou v nové struktuře zachovány.

Tímto způsobem jsme algebraicky přesně jen pomocí celých čísel vytvořili racionální čísla, a dokonce velmi názorně platí, že různé „zlomky“ $[3, 2], [-3, -2], [6, 4]$ atd. jsou jen různými reprezentanty téhož racionálního čísla!

Jak již bylo řečeno na minulé přednášce, konstrukce $Q \rightarrow R, R \rightarrow C$ už jsou jiného charakteru, protože nevytváříme strukturu nového typu (R a C jsou už stále tělesa), pouze obohatíme množinu Q o nějaké další prvky.

Konstrukce $Q \rightarrow R$:

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.

Abyste měli představu, kolik těch iracionálních čísel vlastně je a jak jsou na reálné ose jejich obrazy rozmístěny, podívejme se na dvě zdánlivě protichůdné věty, a pak na dva způsoby konstrukce $Q \rightarrow R$.

Věta 34 *Množina Q je stejně mohutná jako množina N .*⁴⁴

Důkaz: Prvky množiny N lze seřadit do posloupnosti $(1, 2, 3, 4, 5, \dots)$.

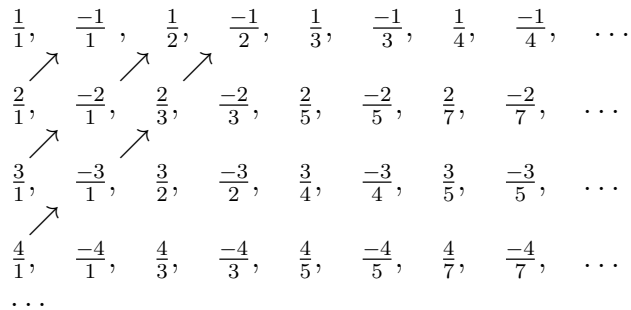
Snad mi věříte, že pokud všechny zlomky seřadíme do jedné posloupnosti, bude jich „stejně“ jako čísel přirozených. Pojdme tedy na to:

- Vezměme vždy zlomky s číslem 1 v čitateli: $\frac{1}{1}, \frac{-1}{1}, \frac{1}{2}, \frac{-1}{2}, \frac{1}{3}, \frac{-1}{3}, \frac{1}{4}, \frac{-1}{4}, \dots$
- Vezměme zlomky s číslem 2 v čitateli, ale vypusťme ty, které po zkrácení dvěma dají nějaký zlomek s čitatelem ± 1 : $\frac{2}{1}, \frac{-2}{1}, \frac{2}{3}, \frac{-2}{3}, \frac{2}{5}, \frac{-2}{5}, \frac{2}{7}, \frac{-2}{7}, \dots$ Ve jmenovateli jsou tedy jen lichá čísla, takových zlomků s čitatelem 2 je stále nekonečně mnoho.
- Vezměme zlomky s číslem 3 v čitateli, které nelze zkrátit na některý zlomek v předchozích dvou posloupnostech: $\frac{3}{1}, \frac{-3}{1}, \frac{3}{2}, \frac{-3}{2}, \frac{3}{4}, \frac{-3}{4}, \frac{3}{5}, \frac{-3}{5}, \dots$
- Vezměme všechny další zlomky s číslem 4 v čitateli: $\frac{4}{1}, \frac{-4}{1}, \frac{4}{3}, \frac{-4}{3}, \frac{4}{5}, \frac{-4}{5}, \frac{4}{7}, \frac{-4}{7}, \dots$
- atd. Takové posloupnosti s různými čitateli lze vyrábět do nekonečna.

⁴⁴Možná bychom mohli nepřesně říci, že všech zlomků je stejný počet jako přirozených čísel, ale u nekonečných množin neříkáme počet prvků, ale mohutnost.

Všechna různá racionální čísla lze tedy vyjádřit jako nekonečně mnoho posloupností. Možná byste intuitivně řekli, že nekonečně mnoho posloupností nelze seřadit do jedné posloupnosti. Ale v této věci intuice selhává, je to možné - níže je naznačen šipkami způsob, jak nekonečně mnoho posloupností lze přeuspořádat a seřadit do jediné:

- jako a_1 vezmeme $\frac{1}{1}$
- jako a_2, a_3 vezmeme 1. zlomek ve 2. řadě, 2. zlomek v 1. řadě: $a_2 = \frac{2}{1}, a_3 = \frac{-1}{1}$
- jako a_4, a_5, a_6 vezmeme 1. zlomek ve 3. řadě, 2. zlomek ve 2. řadě, 3. zlomek v 1. řadě:
 $a_4 = \frac{3}{1}, a_5 = \frac{-2}{1}, a_6 = \frac{1}{2}$
- jako a_7, a_8, a_9, a_{10} vezmeme 1. zlomek ve 4. řadě, 2. zlomek ve 3. řadě, 3. zlomek ve 2. řadě a 4. zlomek v 1. řadě: $a_7 = \frac{4}{1}, a_8 = \frac{-3}{1}, a_9 = \frac{2}{3}, a_{10} = \frac{-1}{2}$
- atd. Tímto postupem se na každý zlomek v daném schématu dostane!



Jedna seřazená posloupnost $\frac{1}{1}, \frac{2}{1}, \frac{-1}{1}, \frac{3}{1}, \frac{-2}{1}, \frac{1}{2}, \frac{4}{1}, \frac{-3}{1}, \frac{2}{3}, \frac{-1}{2}, \dots$

Tímto způsobem seřadíme všechna racionální čísla do jedné posloupnosti, důkaz věty 34 je hotov. \square

Racionálních čísel tedy z jistého úhlu pohledu „není mnoho“ - kdybychom obrazy těchto zlomků trochu „rozhrnuli“ od sebe, aby nebyly tak „nahusto“ (toto „rozhrnování“ by nám mimochodem trvalo nekonečně dlouho), bylo by jich přesně tolik, kolik je čísel přirozených.

Věta 35 *Množina Q je v R hustá, tj. $\forall r \in R \exists$ posloupnost q_n racionálních čísel, jejíž limita je r ($\lim_{n \rightarrow \infty} q_n = r$).*

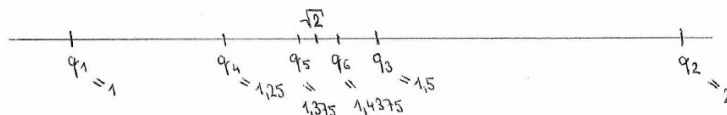
Možná vám někdo už říkal, že tento fakt platí pro číslo π - existuje posloupnost zlomků, jejíž limita = π . Tato skutečnost neplatí jen pro π , ale pro jakékoliv reálné číslo.

Důkaz: Pokud $r \in Q$, nalézt tuto posloupnost je velmi jednoduché: volíme $q_1 = r, q_2 = r, q_3 = r, \dots$ (Např. pro $r = \frac{3}{5}$ je hledaná posloupnost $(\frac{3}{5}, \frac{3}{5}, \frac{3}{5}, \dots)$).

Zajímavější je nalezení posloupnosti pro r iracionální - asi bez újmy na obecnosti zvolme nějaké iracionální r a důkaz proved'eme proň.

Pro $r = \sqrt{2}$ nalezneme posloupnost zlomků q_1, q_2, q_3, \dots s limitou $\sqrt{2}$: volme $q_1 = 1, q_2 = 2$ (tak, aby $q_1 < \sqrt{2}, q_2 > \sqrt{2}$).

- a) Najdeme střed intervalu $q_3 = \frac{q_1+q_2}{2}$. To je racionální číslo, je to součet dvou zlomků dělený dvěma.
- b) $q_3 = 1,5$ rozdělí interval $\langle q_1; q_2 \rangle$ na dva intervaly poloviční délky - vezmeme z nich ten, který obsahuje $\sqrt{2}$.
- c) $q_4 = \frac{q_1+q_3}{2} = 1,25$ rozdělí $\langle q_1; q_3 \rangle$ na dva intervaly poloviční délky - vezmeme z nich $\langle q_4; q_3 \rangle$, protože obsahuje $\sqrt{2}$.
- d) $q_5 = \frac{q_4+q_3}{2} = 1,375$ rozdělí $\langle q_4; q_3 \rangle$ na dva intervaly poloviční délky - vezmeme z nich $\langle q_5; q_3 \rangle$, protože obsahuje $\sqrt{2}$.
- e) $q_6 = \frac{q_5+q_3}{2} = 1,4375$ rozdělí $\langle q_5; q_3 \rangle$ na dva intervaly poloviční délky - vezmeme z nich $\langle q_5; q_6 \rangle$, protože obsahuje $\sqrt{2}$.
- ... atd.



Tato posloupnost středů intervalů se stále víc blíží číslu $\sqrt{2}$, důkaz je hotov. \square

Poznámka: V důkazu věty 35 jsme sestrojili posloupnost čísel $q_n \in Q$, která konverguje, jenže její limita v množině Q neleží!

Odtud plyne elegantní a asi nejjednodušší popis konstrukce $Q \rightarrow R$.

Věta 36 Konstrukce $Q \rightarrow R$ jednoduše: *Doplňme-li množinu Q o limity všech možných posloupností prvků z Q , které v samotné množině Q neleží, dostaneme množinu R .*

Důkaz: Viz věta 35 - iracionální čísla jsou právě ta čísla, která jsou limitami posloupností zlomků z množiny Q , a přitom nejsou prvky množiny Q . \square

Věta 37 Konstrukce $Q \rightarrow R$ trochu méně názorně: *R je množina řezů (A, B) množiny Q , které jsou 1. druhu (ty odpovídají racionálním číslům) nebo 3. druhu (ty odpovídají iracionálním číslům).*

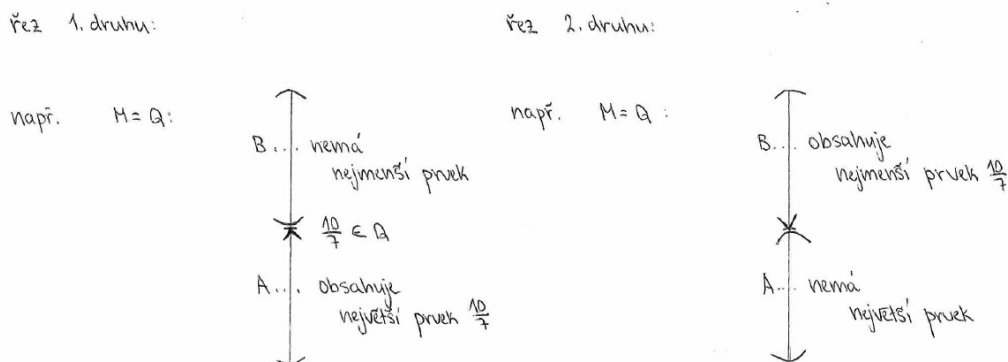
Důkaz či objasnění: Nejprve musíme definovat pojem řezu (A, B) lineárně uspořádané množiny M (tedy M je poset = částečně uspořádaná množina, ve které jsou každé dva prvky srovnatelné = tzv. řetězec).

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 10.16: Řez 1. druhu a řez 2. druhu

Racionálních čísel je právě tolik, kolik existuje řezů 1. druhu množiny Q , tj. existuje bijekce $Q \rightarrow$ 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 $Q \rightarrow$ řezy Q 2. druhu.

Podle toho, kam „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 .

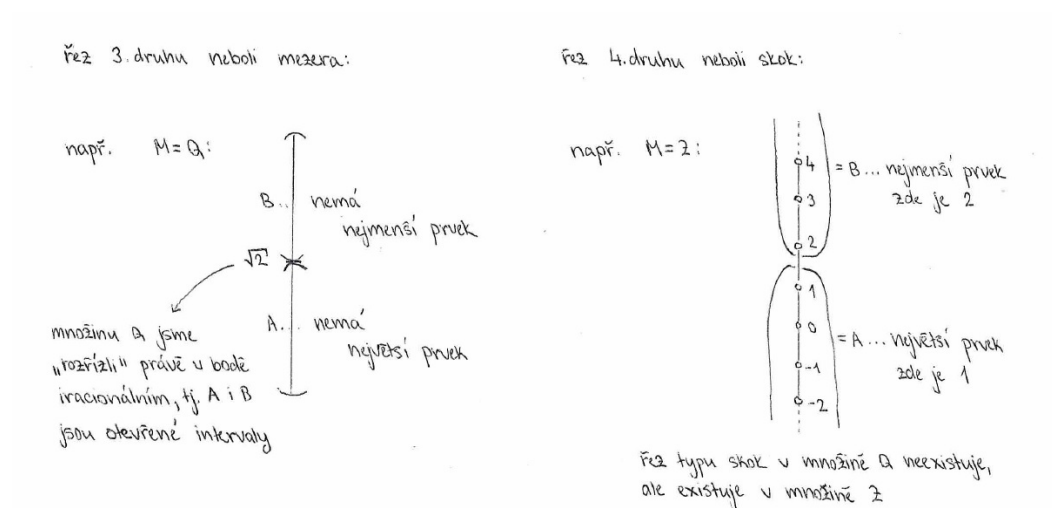
Do tvrzení věty 37 jsme si vybrali racionální čísla reprezentovaná jako řezy množiny Q 1. druhu.

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 $I \rightarrow$ mezery v Q . Například mezeru 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 .



Obrázek 10.17: Řez 3. druhu neboli mezera a řez 4. druhu neboli skok

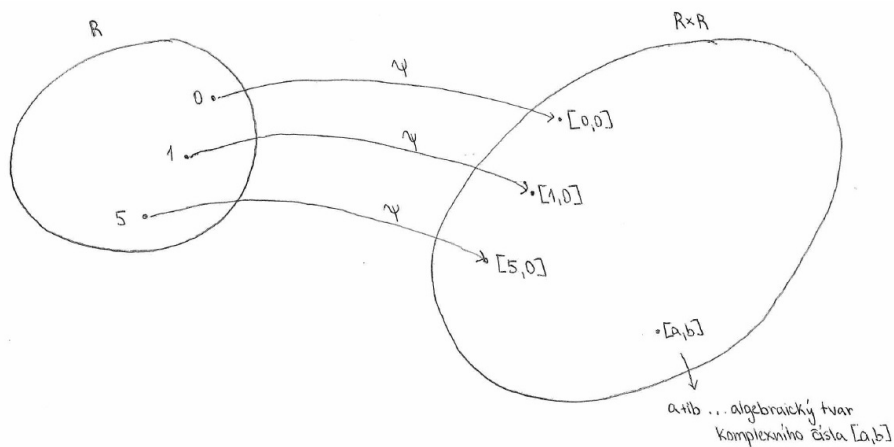
V obrázku mezery $\sqrt{2}$ v \mathbb{Q} neexistuje největší prvek A , ani neexistuje nejmenší prvek množiny B - ovšem $\sqrt{2}$ je supremum množiny A , a současně $\sqrt{2}$ je infimum množiny B . Čili místo terminologie řezů lze konstrukci věty 37 formulovat i jinak: pomocí pojmu infimum nebo supremum - můžeme si vybrat, který z pojmů použijeme, protože $\sqrt{2}$ je současně $\inf B$ i $\sup A$, takže stačí použít jen jeden pojem, např. infimum:

Doplníme-li množinu \mathbb{Q} o infima otevřených intervalů v \mathbb{Q} , která neleží v \mathbb{Q} , dostaneme \mathbb{R} . Konec důkazu či objasnění.

Poznámka: Věty 36, 37 popisují tedy tutéž konstrukci $\mathbb{Q} \rightarrow \mathbb{R}$, pouze pomocí jiných pojmů: věta 36 pomocí pojmu limita posloupnosti, věta 37 pomocí pojmu řez/infimum řetězce. Konstrukce pomocí pojmu řez je součástí bakalářské zkoušky ve 3. ročníku.

Konstrukce $R \rightarrow C$:

Věta 38 Konstrukce $R \rightarrow C$: Těleso $(R, +, \cdot)$ lze vnořit do tělesa $C := R \times R$, ve kterém má rovnice $x^2 + 1 = 0$ řešení.



Obrázek 10.18: Vnoření tělesa $(R, +, \cdot)$ do tělesa $C := R \times R$

Zobrazení ψ definujeme vztahem $\psi(r) = [r, 0]$.

a) Na $R \times R$ definujeme operace $+$, \cdot takto:

$$[a, b] + [c, d] := [a + c, b + d] \dots a + ib + c + id = a + c + i(b + d)$$

$$[a, b] \cdot [c, d] := [ac - bd, ad + bc] \dots (a + ib) \cdot (c + id) = ac + i^2 bd + ibc + iad = ac - bd + i(ad + bc)$$

Pak struktura $(R \times R, +, \cdot)$ je těleso.

Opačný prvek k $[a, b]$ je $[-a, -b]$. Inverzní prvek k $[a, b]$ (mimo $[0, 0]$, ke kterému inverzi nehledáme) je $[\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}]$: $(a + ib) \cdot \frac{1}{(a+ib)} = 1 \dots$ 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 $\psi : R \rightarrow R \times R$ je injektivní homomorfismus $R \rightarrow R \times R$ vzhledem k definovaným operacím, tj. původní výsledky sčítání a násobení reálných čísel jsou v nové struktuře zachovány.

11 Týden 11

11.1 Cvičení 11: Komplexní čísla 02

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

11.2 Přednáška 11: Opakování a příprava ke zkoušce

12 Týden 12

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

12.2 Přednáška 12: Příprava a otázky ke zkoušce

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

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

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

- Co za algebraickou strukturu se dvěma operacemi je $(2^A, \div, \cap)$? Uveďte u každé z operací neutrální prvek a příklad, že existuje-neexistuje inverzní prvek.
- Jednotlivé vlastnosti těchto operací jsou vlastně vztahy mezi množinami. Dokažte některý z nich, ideálně například distributivní zákon (pomocí Vennových diagramů).
- Obsahuje tato struktura nenulové dělitele nuly? Uveďte příklad.
- Doplňující otázka: Operace průniku, sjednocení a symetrického rozdílu jsou tzv. binární operace. Znáte nějaký příklad unární množinové operace – do operace vstupuje jen jedna množina, nikoli dvě? Odpověď: příkladem unární operace je operace doplňku – doplněk vždy hledáme jen pro jednu množinu. Zajímavou vlastností jsou tzv. de Morganova pravidla (Základy mat., přednáška 4), která vyjadřují vztah mezi binární operací sjednocení-průniku a unární operací doplňku. Dokazují se, jak jinak, pomocí Vennových diagramů.
- Mají operace průniku a sjednocení množin nějakou vlastnost, kterou nemají operace sčítání a násobení čísel? Odpověď: jednu zajímavost speciální pro sjednocení a průnik v kombinaci jsem říkal v přednášce: zaměnitelnost operací v distributivním zákonu. Ale existují i další vlastnosti např. samotného průniku či samotného sjednocení (tzv. idempotence⁴⁵), nebo další vlastnosti interakce operací sjednocení a průniku (absorbce, modularita). Všechny se dokazují pomocí Vennových diagramů.

⁴⁵Např. $X^2 = X \cup X = X$, nebo $X^3 = X \cup X \cup X = X$... tj. vzhledem k operaci sjednocení neexistují mocniny, „umocňováním“ dostaneme zase jen množinu X . Naprosto jiné než u čísel.

Otázka 03: Pojem homomorfismu a jeho význam.

- Uveďte definici homomorfismu mezi grupoidy.
- Řekněte, jak se přirozeně (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?

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

- Co je charakteristické pro pojem injektivního homomorfismu?

Odpověď: Pojem injektivního homomorfismu se objevuje například při konstrukci nebo koncepčním přechodu od množiny N na množinu Z . Formálně do množiny N „přidáváme“ další prvky, a přitom ovšem chceme, aby dosavadní pojetí přirozených čísel (včetně výsledků operací sčítání a násobení) zůstalo zachováno. To přesně „kontroluje“, dokazuje či „zaručuje“ homomorfismus $\psi : N \rightarrow N \times N / \sim$. Mluvíme o VNOŘENÍ množiny N do množiny $N \times N / \sim$, která má více prvků (nekonečně mnoho dalších prvků) – ty jsou „modelem“ nuly a záporných čísel. Tedy v tomto pohledu injektivní homomorfismus přesně matematicky ukazuje, že při přechodu od N k Z na $Z\mathbb{S}$ zachováváme dosavadní pojetí práce s čísly, pouze „rozšiřujeme“ toto pojetí čísla na nadmnožinu Z (podobnou argumentaci lze provést při rozšíření Z na Q).

- Nějaké vlastnosti homomorfismu dokažte (tyto vlastnosti platí i pro každý izomorfismus, protože každý izomorfismus je současně homomorfismem):
 - homomorfismus zobrazuje neutrální prvek na neutrální prvek;
 - homomorfismus „zachovává inverze“ v tom smyslu, že $f(x^{-1}) = (f(x))^{-1}$;
 - $\text{Ker}(\varphi)$ je podgrupa grupy (G_1, ∇) při homomorfismu grupy (G_1, ∇) do grupy (G_2, \star) ;
 - $\text{Im}(\varphi)$ je podgrupa grupy (G_2, \star) při homomorfismu grupy (G_1, ∇) do grupy (G_2, \star) ;
- U pojmu jádra homomorfismu se zkuste zamyslet nad příklady 24 a 26 na str. 58, nebo si přečtete příklad 57 na str. 59 a jeho řešení na konci skript.

Otázka 04: Pojem izomorfismu a jeho význam.

- Definice izomorfismu mezi grupoidy⁴⁶.
- Jaký je význam izomorfismu?

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

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

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

- Podgrupa $\langle 2 \rangle := \{0, 2, 4, 6\}$ grupy Z_8 se zobrazí na podgrupu $\langle 2 \rangle := \{0, 2\}$ grupy Z_4 .
- izomorfismus zobrazí prvek řádu 3 na prvek řádu 3. Srovnání s homomorfismem: řád obrazu u homomorfismu může být nižší než řád vzoru – uvažujte například homomorfismus $(Z_8, +)$ na $(Z_4, +)$ (viz výše): řád prvku 2 v Z_8 je roven čtyřem, řád obrazu 2 v Z_4 je roven dvěma (řád obrazu u homomorfismu nemusí být stejný, ale je dělitelem řádu vzoru).
- izomorfismus zobrazí cyklickou podgrupu na cyklickou podgrupu o stejném počtu prvků. Srovnání s homomorfismem, ad homomorfismus $(Z_8, +)$ na $(Z_4, +)$ (viz výše): Cyklická čtyřprvková podgrupa $\langle 2 \rangle$ grupy Z_8 se zobrazí na cyklickou dvouprvkovou podgrupu $\langle 2 \rangle$ grupy Z_4 .
- atd.

Tedy pokud přeznačíme prvky první struktury příslušnými prvky druhé struktury určenými izomorfismem, daná tabulka operace první struktury (pokud prvky v záhlaví tabulky napíšeme ve stejném pořadí⁴⁷) bude naprosto totožná jako tabulka operace druhé struktury.

⁴⁶Grupoidy jsou struktury s nejmenším možným počtem podmínek (jedinou – uzavřeností operace na dané množině), mezi kterými lze homomorfismus nebo izomorfismus definovat. V realitě pak velmi často studujeme či popisujeme homomorfismus či izomorfismus grup, kde platí v každé struktuře už podmínky čtyři.

⁴⁷Studenti někdy říkají-píší, že dané dvě struktury nejsou izomorfní, ale pořadí prvků může být v záhlaví tabulky operace přehozeno vzhledem k záhlaví tabulky operace první množiny – tedy izomorfismus nekontrolujeme pomocí naprosto totožné tabulky, ale pomocí zjišťování vlastností dané množiny, tj. například vztahy mezi inverzními prvky, podgrupy o jistém počtu prvků, apod. – tyto věci mají mnohem větší váhu, než jen první pocit ohledně vzhledu obou tabulek.

- Příklad: Rozhodněte, které z grup $(\{1, -1, i, -i\}, \cdot)$, $(Z_4, +)$, $(Z_2 \times Z_2, +)$ jsou mezi sebou izomorfní (= vykazují naprosto stejné vlastnosti dané operace, kromě toho, že se jedná o bijekci) a které ne.
- Další příklady, které by se mohly objevit: Str. 52, příklad 5.1, například N.4; str. 53. příklad 5.2, různé napříklady o izomorfismu.

Otázka 05: Grupa permutací a Cayleyho věta

- Vypište celou tabulku operace skládání permutací grupy S_3 .
- Z tabulky vyčtěte základní informace o inverzních prvcích a podgrupách, neutrálním prvku.
- Co říká Cayleyho věta?
- Ilustrujte Cayleyho větu na konečné grupě $(Z_3, +)$ a nekonečné grupě $(Z, +)$.
- Mohl by se objevit 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.

Otázka 06: 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.

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

Otázka 07: Struktury se dvěma operacemi.

- Definujte okruh; uveďte příklad okruhu zbytkových tříd, který není oborem integrity, včetně vysvětlení a příkladu nenulových dělitelů nuly.

- Definujte obor integrity; uveďte příklad a) okruhu zbytkových tříd, který je oborem integrity; b) oboru integrity, který není tělesem.
- Definujte těleso; uveďte příklad a) konečného, b) nekonečného tělesa.
- Dokažte větičku: Každý konečný obor integrity je už automaticky tělesem.
- Dokažte větičku: V okruhu platí: Daný okruh $(M, +, \cdot)$ je oborem integrity právě tehdy, když v něm platí vlastnost krácení (7*) pro okruhy:

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

Otázka 08: 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?
- Co říká věta o racionálních kořenech polynomu a jak je lze určit pomocí Hornerova schématu?
- Co říká „věta o odstranění násobných kořenů polynomu“? Popište postup, příklad uvádět nemusíte.
- Co je zajímavé na komplexních kořenech polynomu z $R[x]$? Odpověď: v polynomu s reálnými koeficienty se vyskytují oba současně, v rozkladu polynomu v \mathbb{R} se jedná o dva různé komplexní kořeny jednoho v \mathbb{R} nerozložitelného polynomu 2. řádu.

Otázka 09: Polynomické rovnice – numerické metody řešení.

- Jak lze zhruba vymežit všechny kořeny polynomu? Odpověď: Oddíl D z přednášky 8.
- Jak lze zhruba najít interval, na kterém existuje reálné řešení polynomu, který jsme zbavili násobných kořenů⁴⁸? Odpověď: Využijeme nerovnosti D, zjistíme interval

⁴⁸Tento předpoklad jsem v přednášce 8 nezmínil a je důležitý: Kdybychom totiž zkoumali polynom $p(x)$, aniž bychom snížili stupeň polynomu při vícenásobných kořenech postupem z oddílu B, mohlo by dojít k situaci, že některé reálné kořeny mají násobnost 2 nebo 4 atd. zkrátka násobnost sudou. Při zkoumání grafu funkce $p(x)$ pak neplatí skutečnost, že by funkce přecházela v bodě kořene se sudou násobností ze záporných funkčních hodnot na kladné (nebo z kladných funkčních hodnot na záporné), nýbrž graf funkce $p(x)$ se v blízkosti kořene blíží k ose x , v bodě kořene x_k se jí dotkne a „odrazí se na tutéž stranu“, tj. např. $p(x) < 0$ pro $x < x_k$, pak $p(x_k) = 0$, ale pak $p(x) < 0$ nastane i pro $x > x_k$, tj. neplatí, že by funkční hodnoty $p(x)$ při průchodu proměnné x bodem x_k měnily znaménko. To znamená, že postupné počítání funkčních hodnot z intervalu $(-r; r)$ takový kořen neodhalí. Tomuto problému se vyhneme, když provedeme postup B, tj. odstraníme násobné kořeny polynomu. Potom při výpočtu funkčních hodnot v intervalu $(-r; r)$ s dostatečně malým krokem najdeme všechny intervaly, na kterých existuje jediný jednonásobný kořen.

$(-r; r)$, kde r je poloměr kruhu v nerovnosti D, projdeme tento interval s dostatečně malým krokem, vypočteme $p(x_i)$ v bodech x_i těchto kroků oddíl F přednášky 8.

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

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

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

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

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

Otázka 12: Algebraický popis, jak ze Z zkonstruujeme Q

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

Otázka 13: Algebraický popis, jak z \mathbb{Q} zkonstruujeme \mathbb{R} pomocí řezů množiny \mathbb{Q} .

Otázka 14: Algebraický popis, jak z \mathbb{R} zkonstruujeme \mathbb{C} .

Informace ke zkoušce v předmětu Algebra 1 v roce 2022: budou ještě aktualizovány před koncem semestru. Zatím je plán, že můžete očekávat zhruba čtyři otázky (nebo jen jejich části):

1. jednu z otázek 1,2,7 ... základní definice vlastností operace, algebraických struktur;
2. jednu z otázek 3,4,5,6 ... něco o homomorfismu, izomorfismu, grupě permutací S_n nebo dihedrální grupě D_n ;
3. část ot. 8 a část ot. 9 (tj. přineste si kalkulačku pro vypracování ot. 9) ... polynomy, řešení polynomických rovnic;
4. některou z otázek 10 až 14 nebo jejich části.

13 Výsledky některých příkladů

13.1 Výsledky ke cvičení 1.1 – Opakování definic z předmětu Základy matematiky

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 $M \times M \rightarrow M$, tj. zobrazení, které přiřadí uspořádané dvojici $[a, b]$ z kartézského součinu $M \times M$ výsledek této operace, prvek $a \nabla b$.
- h) Zobrazení $f : N \rightarrow R$ (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 $[x, y] \in f \wedge [x, z] \in f \Rightarrow y = z$.

13.2 Výsledky ke cvičení 1.2 – Určování vlastností různých operací

Ad úloha 1.10:

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

b) $(Z, +)$ je komutativní grupa.

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

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

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

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

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

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

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

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

Ad úloha 1.14 (M, ∇) je komutativní monoid.

Ad úloha 1.15 (M, Δ) je komutativní grupa.

Ad úloha 1.16 $(N - \{0\}, *)$ je grupoid.

Ad úloha 1.17 (R^+, \circ) je komutativní grupoid.

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

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

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

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

Ad F.3: Tabulku lze doplnit na:

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

Ad úloha 3.6 – A.1: H je podgrupou grupy G , protože (1) součet logaritmů je logaritmus součinu a součin kladných hodnot je zase kladná hodnota, tj. H je uzavřená vzhledem k součtu. Dále je neprázdná, obsahuje např. prvek $\log 1$, což je neutrální prvek vzhledem ke sčítání (platí (3)). Asociativita se svezí 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. necht' 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: $\langle 6, 9 \rangle = \{6, 0, 9, 3\}$ 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 3.8

- a) $x = (b^2)^{-1}$
 b) $x = b^{-1} * a$
 c) $x = (a^4)^{-1}$

Ad úloha 3.10: Tabulka operace \circ na množině D_3 symetrií trojúhelníku:

Tabulka 13.10: Tabulka operace \circ na množině D_3 symetrií trojúhelníku.

\circ	R_0	R_1	R_2	R_3	R_4	R_5
R_0	R_0	R_1	R_2	R_3	R_4	R_5
R_1	R_1	R_2	R_0	R_5	R_3	R_4
R_2	R_2	R_0	R_1	R_4	R_5	R_3
R_3	R_3	R_4	R_5	R_0	R_1	R_2
R_4	R_4	R_5	R_3	R_2	R_0	R_1
R_5	R_5	R_3	R_4	R_1	R_2	R_0

Pokud tuto tabulku porovnáme s tabulkou grupy (S_3, \circ) v příkladu 4 je vidět, že mezi oběma grupami existuje izomorfismus, tj. příslušné tabulky operace se liší pouze

přeznačením prvků: $f(e) = R_0$, $f(s) = R_1$, $f(t) = R_2$, $f(u) = R_3$, $f(v) = R_4$, $f(w) = R_5$ (toto izomorfní přiřazení je vidět i na obrázku 1.1). Aby zobrazení f bylo izomorfismem, musíme z tabulky operace první grupy dostat přeznačením prvků vzhledem k zobrazení f přesně tutéž tabulku vzhledem k operaci v druhé grupě.

Ad úloha 3.11 Cyklické podgrupy grupy $(H_{10}, +)$:

$(\{0\}, +)$, $(\{0, 5\}, +)$, $(\{0, 2, 4, 6, 8\}, +)$, $(H_{10}, +)$.

Ad úloha 3.12 Cyklické podgrupy grupy $(H_{12}, +)$:

$(\{0\}, +)$, $(\{0, 6\}, +)$, $(\{0, 2, 4, 6, 8, 10\}, +)$, $(\{0, 3, 6, 9\}, +)$, $(\{0, 4, 8\}, +)$, $(H_{12}, +)$.

13.4 Výsledky ke cvičení 4.1 – Nekomutativní grupy

Ad úloha 4.1: Podle definice skládání zobrazení platí

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

13.5 Výsledky ke cvičení 5.1 – Řád prvku, cyklické grupy, grupy zbytkových tříd

ad Cvičení 5.1.

Například N.4: α i β vyjádříme jako součin navzájem nezávislých cyklů:

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

Pak lze cykly zvlášť umocnit a spojit: $\alpha^3 = (1, 2) \circ \text{id} = (1, 2)$, $\beta^4 = (1, 5, 2, 7, 6)$ ⁴⁹. Spočteme „součin“ a rozložíme na dílčí „součin“ navzájem nezávislých cyklů:

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

Při umocnění na pátou nyní opět umocníme každý cyklus zvlášť:

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

Řád cyklu $(1, 5)$ je 2, řád cyklu $(2, 6, 7)$ je 3, a tedy řád jejich složení je nejmenší společný násobek dílčích řádů, tedy 6.

⁴⁹Mimořádně: protože Podgrupa generovaná permutací β je cyklická a prvek β je řádu 5 (cyklus délky k je řádu k , platí $\beta^5 = \text{id}$, a tedy $\beta^4 = \beta^{-1}$... inverzním prvku k cyklu β je mocnina prvku β o jedničku nižší než řád prvku β).

Ad příklad 31 Ad Například F.1: Řád obrazu je dělitelem řádu vzoru. Lze i celkem jednoduše dokázat: Sporem ... předpokládejme, že prvek a řádu k se zobrazí na prvek řádu l , kde l není dělitelem k , tj. $k = l \cdot q + m$, kde $0 < m < l$. Označme ještě e_1 neutrální prvek v grupě $G_1 = (G, \nabla)$, e_2 je neutrální prvek v grupě $G_2 = (H, *)$. Celkem máme

$$e_2 = \varphi(e_1) = \varphi(a^k) = \varphi(a^{l \cdot q + m}) = \varphi(a)^{l \cdot q} * \varphi(a)^m = e_2 * \varphi(a)^m,$$

což je spor s tím, že řád prvku $\varphi(a)$ není m , ale větší číslo l .

Ad Například N.3: Nevím, jak přesně dokázat, ale nebude to těžké – snad stačí říci, že to plyne z předchozí větičky N.1 a vlastnosti zachování operace u homomorfismu. Pokud zobrazíme generátor na generátor, obrazy všech ostatních prvků už jsou jednoznačně určeny. Důkaz: Když a je generátor cyklické podgrupy první grupy, $\varphi(a)$ jistě také vygeneruje nějaké prvky svými mocninami, a podle větičky N.1 jich bude tolik, že jejich počet dělí řád prvku a v první grupě.

Ad Například N.4: 0 se v každém homomorfismu zobrazí na 0. Dále (Z_8, \oplus) je cyklická grupa generovaná např. prvkem 1. Tedy celý homomorfismus je jednoznačně určen, zadáme-li obraz generátoru 1.

hom 01: $0 \xrightarrow{\varphi} 0, 1 \xrightarrow{\varphi} 0 \dots$ pokud se generátor zobrazí na nulu, aby byla splněna podmínka homomorfismu, všechny další prvky se zobrazí na nulu. Jádrem je tedy celá množina Z_8 .

hom 02: $0 \xrightarrow{\varphi} 0, 1 \xrightarrow{\varphi} 1 \dots$ podle podmínky homomorfismu nyní dopočteme, že musí nastat $2 = 1 + 1 \xrightarrow{\varphi} \varphi(1) + \varphi(1) = 2$, dále $3 = 2 + 1 \xrightarrow{\varphi} \varphi(2) + \varphi(1) = 2 + 1 = 3$, atd. Jádrem je množina $\{0, 4\}$

hom 03: $0 \xrightarrow{\varphi} 0, 1 \xrightarrow{\varphi} 2 \dots$ prvek $2 \in Z_4$ generuje podgrupu $\{0, 2\}$, tj. podle podmínky homomorfismu se 0, 2, 4, 6 zobrazí na nulu, a 1, 3, 5, 7 na dvojku, tj. jádrem je $\{0, 2, 4, 6, \dots\}$.

hom 04: $0 \xrightarrow{\varphi} 0, 1 \xrightarrow{\varphi} 3 \dots$ prvek $3 \in Z_4$ generuje celou Z_4 , a tedy 0, 1, 2, 3 se postupně zobrazí na 0, 3, 2, 1, a pak už se obrazy zopakují: $4 \rightarrow 0, 5 \rightarrow 3, 6 \rightarrow 2, 7 \rightarrow 1$. Jádrem je množina $\{0, 4\}$ grupy Z_8 .

Ad Například N.2: (Z_9, \oplus) sestává z prvků: (operací „umocňování“ je sčítání prvků) [0] je řádu 1, [1] je řádu 9, [2] je řádu 9, [3] je řádu 3, [4] je řádu 9, [5] je řádu 9, [6] je řádu 3, [7] je řádu 9, [8] je řádu 9.

Dále (S_3, \circ) sestává z prvků (ve zkráceném zápisu pomocí disjunktních cyklů): id je řádu 1, (1, 2, 3) je řádu 3, (1, 3, 2) je řádu 3, (1, 2) je řádu 2, (1, 3) je řádu 2, (2, 3) je řádu 2.

Pojďme ke hledání všech různých homomorfismů: neutrální prvek se musí vždy zobrazit na neutrální prvek – tedy [0] se zobrazí na id. Vzhledem k předchozímu příkladu N.1 řád obrazu musí být dělitelem řádu vzoru, tj. žádný z dalších prvků řádu tři nebo devět se nemůže zobrazit na dvouprvkové cykly (1, 2), (1, 3) nebo (2, 3), protože ty jsou řádu 2.

Dále si všimněme, že grupa Z_9 má řadu prvků řádu devět, je tedy cyklická, tj. stačí zobrazit jeden z generátorů celé grupy, například prvek $[1]$, a všechny obrazy ostatních prvků jsou už jednoznačně určeny z podmínky homomorfismu (podmínky zachování výsledku operace). Díky těmto faktům lze dospět ke třem různým homomorfismům:

hom 01: $\varphi_1([0]) = \text{id}$, $\varphi_1([1]) = (1, 2, 3)$, a nyní už

$$\begin{aligned}\varphi_1([2]) &= \varphi_1([1] + [1]) = (1, 2, 3) \circ (1, 2, 3) = (1, 3, 2); \\ \varphi_1([3]) &= \varphi_1([2] + [1]) = (1, 3, 2) \circ (1, 2, 3) = \text{id}; \\ \varphi_1([4]) &= \varphi_1([3] + [1]) = \text{id} \circ (1, 2, 3) = (1, 2, 3); \\ \varphi_1([5]) &= \varphi_1([4] + [1]) = (1, 2, 3) \circ (1, 2, 3) = (1, 3, 2); \\ &\text{atd.}\end{aligned}$$

Je vidět, že jádrem homomorfismu jsou prvky id , $[3]$, $[6]$, protože ty se zobrazí na neutrální prvek druhé grupy.

hom 02: $\varphi_1([0]) = \text{id}$, $\varphi_1([1]) = (1, 3, 2)$, a nyní už

$$\begin{aligned}\varphi_2([2]) &= \varphi_2([1] + [1]) = (1, 3, 2) \circ (1, 3, 2) = (1, 2, 3); \\ \varphi_2([3]) &= \varphi_2([2] + [1]) = (1, 2, 3) \circ (1, 3, 2) = \text{id}; \\ \varphi_2([4]) &= \varphi_2([3] + [1]) = \text{id} \circ (1, 3, 2) = (1, 3, 2); \\ \varphi_2([5]) &= \varphi_2([4] + [1]) = (1, 3, 2) \circ (1, 3, 2) = (1, 2, 3); \\ &\text{atd.}\end{aligned}$$

Je vidět, že jádrem homomorfismu jsou prvky id , $[3]$, $[6]$, protože ty se zobrazí na neutrální prvek druhé grupy.

hom 03: $\varphi_3([0]) = \text{id}$, $\varphi_3([1]) = \text{id}$, a nyní už

$$\begin{aligned}\varphi_3([2]) &= \varphi_3([1] + [1]) = \text{id} \circ \text{id} = \text{id}; \\ \varphi_3([3]) &= \varphi_3([2] + [1]) = \text{id} \circ \text{id} = \text{id}; \\ &\text{atd.}\end{aligned}$$

Je vidět, že jádrem homomorfismu je celá grupa Z_9 , protože všechny její prvky se zobrazí na neutrální prvek.

Seznam literatury:

- Beránek, 2011** Jaroslav Beránek: Vybrané kapitoly z algebry. Skriptum Pdf, počet stran 70. Doplnění obsahu předmětů Algebra 1 a Algebra 3 na Pdf pro budoucí učitele 2.stupně. Brno 2011.
- Budínová, I., 2013** Irena Budínová: Polynomy. Text určený studentům učitelství matematiky, Brno 2013. Počet stran 56.
- Drozd, 2008** P. Drozd – základy práce se softwarem R. Manuál ke stažení z internetu o některých základních funkcích jazyka R, který lze v 1.ročníku VŠ doporučit jako lepší kalkulačku zvládající běžné matematické funkce, a současně jednoduché kreslení obrázků, které lze stáhnout v různých formátech. I jednoduché programy lze v tomto prostředí realizovat. Prostředí po instalaci funguje offline.
- Horák, 2002** P. Horák: Cvičení z algebry a teoretické aritmetiky I, Brno 2002. Sbíрка 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.
- Kolářek J.** Kolářek: 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.