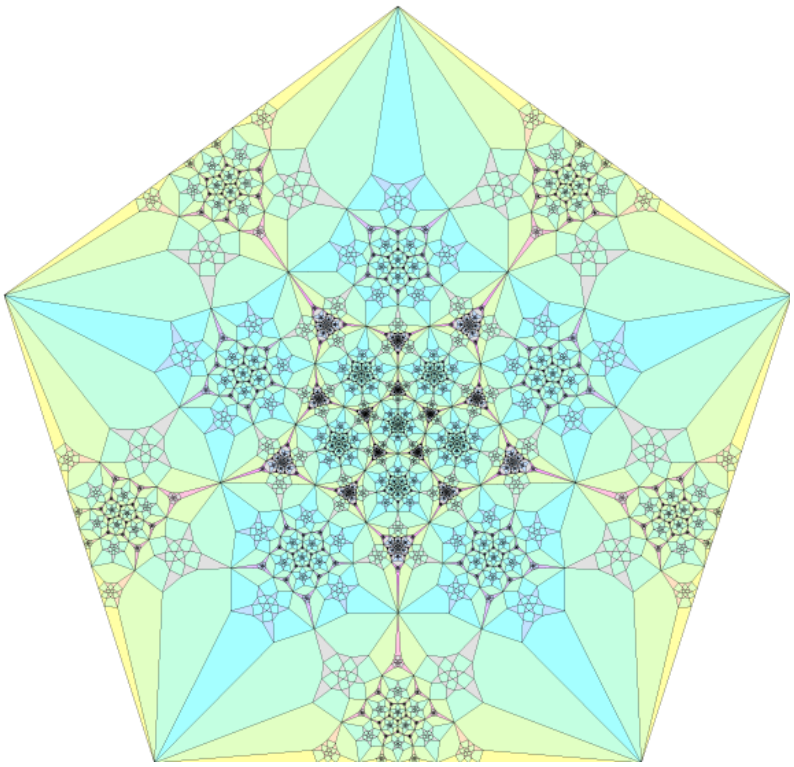
Algebra



Petr Kovář

2023

Petr Kovář
Algebra

Úvodem

Text, který právě čtete, vzniká jako příprava přednášek a cvičení. Současně obsahuje řadu poznámek a postřehů souvisejících s předmětem *Algebra* pro bakalářské či magisterské studium na technické vysoké škole. Při výběru témat a přípravě textu jsem vycházel z osnov předmětu, z knihy *Contemporary Abstract Algebra* Josepha Galliana [G], z knihy *A Book of Abstract Algebra* Charlese Pintera [P], a celé řady dalších zdrojů.

Pokud máte pocit, že v textu je nějaká nesrovnalost, chyba nebo překlep, dejte mi prosím vědět. Budu rád, když mne upozorníte i na méně srozumitelné pasáže, abych je v dalších verzích textu mohl vylepšit.

Jak číst tento text

Text je psán pro čtenáře s hlubším zájmem o oblast algebry, který prošel některým ze základních kurzů kombinatoriky. Nultá kapitola shrnuje základní pojmy a symboly, které se objeví v dalších kapitolách. Doporučuji čtenářům ji prolistovat a při čtení pozdějších kapitol se případně vrátit k příslušnému tématu. Při studiu doporučuji nejprve dobře zvládnout prvních pět kapitol textu, pořadí dalších kapitol už není rozhodující.

Na konci každé podkapitoly najdete příklady k procvičení probrané látky. Protože není smysluplné vybudovat nejdříve celou teorii a teprve potom řešit příklady, tak některá cvičení se odvolávají na pojmy, které budou zavedeny teprve v pozdějších kapitolách. Věřím, že není problém nalistovat si příslušnou definici (na konci textu najdete rejstřík) a pak takové příklady vyřešit.

V textu kapitol a na konci podkapitol jsem zařadil množství odkazů na internet. Prosím o shovívavost, jestliže některé odkazy budou v době vašeho studia zastaralé. Připomínky posílejte na adresu `petr.kovar@vsb.cz`.

Poděkování

Děkuji Matěji Krbečkovi za pečlivé přečtení jedné z verzí tohoto textu. Odhalil mnoho chyb a překlepů, jeho připomínky přispěly ke srozumitelnosti celého textu. Největší dík patří Pavlu Jahodovi, jehož připomínky pomohly k zpřesnění mnoha částí celého textu a od kterého jsem převzal část řešených příkladů i cvičení.

K použitým symbolům

Příklady označené „*“ patří k náročnějším. Jejich řešení obvykle vyžaduje delší výpočet nebo pečlivější rozbor. Pro řešení příkladů označených „**“ je třeba nějaký nápad nebo výsledek z jiné oblasti matematiky. Zdůrazněme ale, že hvězdička neznamená nutně „to nikdy nevyřeším“. Naproti tomu příklady označené „$^{\heartsuit}$“ jsou tak lehké, že jejich řešení je možné zpaměti a jen s užitím základních pojmů.

V Krmelíně 2. února 2023.

Obsah

Úvodem . . . i
Přehled pojmů a označení . . . 1
0.1. Dělitelnost . . . 1
0.2. Množiny . . . 6
0.3. Relace . . . 7
0.4. Zobrazení . . . 11
0.5. Permutace . . . 15
0.6. Operace na množině . . . 18
0.7. Modulární aritmetika . . . 23
0.8. Důkazové techniky . . . 25
0.9. Co se nevešlo . . . 31
1. Symetrie a dihedrální grupy . . . 33
1.1. Symetrie . . . 33
1.2. Dihedrální grupy . . . 37
1.3. Další příklady symetrií . . . 38
2. Algebraické struktury s jednou operací . . . 41
2.1. Grupoidy . . . 41
2.2. Pologrupy . . . 43
2.3. Monoidy . . . 46
2.4. Grupy . . . 48
2.5. Další vlastnosti grup . . . 55
3. Podgrupy a komplexy . . . 61
3.1. Definice pojmů . . . 62
3.2. Ověření podgrupy . . . 65
3.3. Centrum grupy . . . 69
3.4. Komplexy v grupě a operace s nimi . . . 70
3.5. Grupy zbytkových tříd modulo m . . . 72
4. Rozklady grup, Lagrangeova věta . . . 77
4.1. Rozklad grupy podle podgrupy . . . 78
4.2. Řád grupy a index podgrupy . . . 83
4.3. Lagrangeova věta . . . 85
5. Normální podgrupy . . . 93
5.1. Normální podgrupa a faktorová grupa . . . 93
5.2. Vlastnosti normálních podgrup . . . 97
5.3. Normalizátor . . . 99
6. Cyklické grupy . . . 103
6.1. K symbolice mocnin a násobků . . . 103
6.2. Definice cyklické grupy . . . 104
6.3. Řád cyklické grupy a řád prvku . . . 108
6.4. Struktura cyklických grup . . . 110
7. Grupy permutací . . . 115
7.1. Definice grupy permutací . . . 116
7.2. Řád permutace . . . 119
7.3. Parita permutace . . . 121
8. Homomorfismy grup . . . 127
8.1. Definice homomorfismu grup . . . 127
8.2. Jádro homomorfismu . . . 132
8.3. Skládání homomorfismů . . . 138
9. Izomorfismy grup . . . 141
9.1. Definice izomorfismu grup . . . 141
9.2. Klasifikace cyklických grup . . . 144
9.3. Cayleyho věta . . . 146
9.4. Další vlastnosti homomorfismů . . . 149
10. Vnější součin grup . . . 151

10.1. Definice vnějšího součinu . . . 151
10.2. Vlastnosti vnějšího součinu . . . 153
10.3. Grupa jednotek modulo n . . . 155
10.4. Aplikace . . . 157
11. Okruhy, obory integrity a tělesa . . . 161
11.1. Okruh . . . 161
11.2. Vlastnosti okruhů . . . 165
11.3. Podokruhy . . . 166
11.4. Obor integrity . . . 168
11.5. Tělesa . . . 171
12. Ideály a faktorové okruhy . . . 175
12.1. Ideál . . . 175
12.2. Faktorový okruh . . . 176
12.3. Okruh polynomů . . . 179
12.4. Ideály v okruhu polynomů . . . 183
13. Homomorfismy okruhů . . . 189
13.1. Homomorfismus okruhů . . . 189
13.2. Jádro homomorfismu . . . 192
13.3. Faktorový okruh podle jádra . . . 193
Rejstřík . . . 197
Literatura . . . 203
Užitečné tabulky . . . 204
Přehled použitých symbolů . . . 204

Přehled pojmů a označení

Tato úvodní kapitola slouží jako přehled a připomenutí některých známých pojmů a řady tvrzení. Měly by čtenářům být známy ze střední školy, případně z úvodních kurzů vysokoškolské matematiky. V dalších kapitolách budeme předpokládat jejich dobré zvládnutí.

Princip dobrého uspořádání
Následující tvrzení se často používá v důkazech.

Věta 0.1. Princip dobrého uspořádání
Každá neprázdná množina nezáporných celých čísel má nejmenší prvek.

Všimněte si, že toto tvrzení je silnější, než axiom výběru, který (opět v nejjednodušší formě) říká, že z každé neprázdné množiny můžeme vybrat nějaký prvek. Důkaz neuvádíme, protože se jedná o princip, tedy o tvrzení, jehož platnost předpokládáme a považujeme jej za za axiom pro příslušnou matematickou disciplínu.

0.1. Dělitelnost

Pojmy dělení a dělitelnost jsou někdy chybně zaměňovány. Připomeňme, že *dělení* je operace, která některým dvěma číslům (v daném pořadí) z předepsané číselné množiny přiřadí výsledek operace dělení $a : b$, kterému říkáme *podíl*. Operace formálně popisujeme na straně 18. Všimněte si, že výsledek operace dělení závisí na množině čísel, se kterou pracujeme. Počítáme-li například s reálnými nebo racionálními čísly $a = 7$, $b = 2$, tak výsledek dělení $a : b = \frac{7}{2}$, zatímco při počítání s celými čísly není podíl $a : b$ definován, protože výsledek obvyklého dělení celých čísel nemusí být celé číslo.

Naproti tomu *dělitelnost* není operace se dvěma čísly, ale relace mezi dvěma čísly. Pro dvojici čísel a, b (v daném pořadí) platí, že buď „a dělí b“ beze zbytku nebo „a nedělí b“ (resp. zbytek po dělení čísla b číslem a je nenulový.)

Definice Mějme dvě celá čísla a, b. Řekneme, že a *dělí* b, jestliže existuje takové celé číslo k, že $a \cdot k = b$, což zapisujeme $a \mid b$. V opačném případě říkáme, že a *nedělí* b, což zapisujeme $a \nmid b$. Číslu a říkáme *dělitel čísla* b a číslu b říkáme *násobek čísla* a.

Příklad 0.1. Pro názornost uvedeme několik příkladů dělení.

1) Platí $2 \mid 4$, $2 \mid 6$, ale také $2 \mid -4$, $2 \mid -2$ a $2 \mid 0$.
2) Dále platí $-2 \mid 2$, $-6 \mid -6$, $-4 \mid 0$.
3) Naproti tomu $4 \nmid 2$, $2 \nmid 5$, $4 \nmid -6$, $0 \nmid 1$.
4) Nulou sice nemůžeme dělit, avšak nula může být dělitelem, byť je dělitelem pouze nuly. Platí $0 \mid 0$, neboť $0 = k0$, dokonce pro libovolné $k \in \mathbb{Z}$.

Prvočíslem nazveme každé přirozené číslo, které má *právě dva* přirozené dělitele, a to jedničku a sebe sama. Všechna přirozená čísla větší než 1 jsou buď prvočísla, nebo čísla *složená*, tj. mají ještě nějakého dalšího kladného dělitele většího než 1. Nula, záporná čísla ani desetinná čísla pochopitelně nejsou prvočísla. Všimněte si, že podle definice číslo 1 *není* prvočíslo. V některé, zejména informatické literatuře číslo 1 mezi prvočísla zahrnují. To má svá úskalí, například pokud bychom číslo 1 za prvočíslo považovali, tak složená čísla nebudou mít jednoznačně určený rozklad na prvočísla, tj. nebude platit Základní věta aritmetiky 0.8. uvedená v další části.

Největší společný dělitel a nejmenší společný násobek
V návaznosti na pojem dělitelnosti můžeme zavést další známé pojmy jako největší společný dělitel (NSD) a nejmenší společný násobek (NSN) dvou nebo více čísel. *Společným dělitelem* čísel $a_1, a_2, \ldots, a_n$ je takové celé číslo m, že $m \mid a_1$, $m \mid a_2$, $\ldots$, $m \mid a_n$. *Společným násobkem* čísel $a_1, a_2, \ldots, a_n$ je takové celé číslo m, že $a_1 \mid m$, $a_2 \mid m$, $\ldots$, $a_n \mid m$.

Definice Největší společný dělitel
Mějme dvě nenulová celá čísla a, b. *Největší společný dělitel* čísel a, b je takový kladný společný dělitel m čísel a, b, který je dělitelný jejich libovolným společným dělitelem. Značíme je $\mathrm{NSD}(a, b)$ nebo jen (a, b). Jestliže navíc $(a, b) = 1$, říkáme, že a a b jsou *nesoudělná*.

Definici největšího společného dělitele je snadné rozšířit i pro případ, kdy alespoň jedno z čísel je nulové (Cvičení 0.1.1.). Je zajímavé si uvědomit, že největší společný dělitel dvou kladných čísel a a b nikdy nemůže být větší než a či b. Pro záporná nebo nulová čísla tomu tak být nemusí (Cvičení 0.1.4.).

Definice Nejmenší společný násobek
Mějme dvě nenulová celá čísla a, b. *Nejmenší společný násobek* čísel a, b je takový kladný společný násobek m čísel a, b, který je dělitelem jejich libovolného společného násobku. Značíme jej $NSN(a,b)$ nebo $[a,b]$.

Definici nejmenšího společného násobku je také možno rozšířit i pro případ, kdy alespoň jedno z čísel je nulové (Cvičení 0.1.2.).

Celočíselné dělení se zbytkem
Často využívaným tvrzením je, že pro libovolná dvě celá čísla můžeme *jednoznačně* najít jejich podíl a zbytek. Později ukážeme zobecnění tohoto tvrzení i pro jiné množiny než jsou celá čísla.

Věta 0.2. Věta o jednoznačnosti podílu a zbytku
Pro každé celé číslo z a každé přirozené číslo m existují taková jednoznačně určená celá čísla q a r, kde $0 \leq r < m$, že $z = qm + r$.

Číslu q říkáme *podíl* a číslu r *zbytek* po dělení čísla z číslem m.
Důkaz. Nejprve ukážeme, že hledaný podíl q a zbytek r existují. Sestavíme množinu nezáporných čísel $M = \{z - m \cdot k : k \in \mathbb{Z} \wedge z - m \cdot k \geq 0\}$. Množina M má podle Principu dobrého uspořádání (Věta 0.1.) nejmenší prvek, který označíme r. Potom platí $z = qm + r$. Dále jistě platí $0 \leq r$, protože množina M obsahuje nezáporná čísla, a jistě platí $r < m$, jinak by r nebyl nejmenší prvek v množině M.

Dále nepřímo ukážeme jednoznačnost čísel m a q. Předpokládejme, že existuje další dvojice čísel m_0, q_0, pro kterou platí $z = q_0 m + r_0$ a $0 \leq r_0 < m$. Porovnáním $qm + r = z = q_0 m + r_0$ a úpravou dostaneme

$$\begin{aligned} qm + r = z &= q_0 m + r_0 \\ (q - q_0)m &= r_0 - r \\ q - q_0 &= \frac{r_0 - r}{m} \end{aligned} \tag{1}$$

Protože r i r_0 jsou kladná čísla a $r, r_0 < m$, tak $-m < r_0 - r < m$. To znamená, že $-1 < (r_0 - r)/m < 1$, přičemž tento podíl je celé číslo $q - q_0$. Jediným takovým celým číslem je 0, a proto $r = r_0$. Dosazením do (1) dostaneme $q - q_0 = 0$, a tedy $q = q_0$. To znamená, že dvojice čísel m_0, q_0 splňující $z = qm + r$ a $0 \leq r < m$ je určena jednoznačně. □

V některých důkazech využijeme Bézoutovo lemma.

Lemma 0.3. Bézoutovo lemma
Mějme dvě nenulová celá čísla a, b. Jestliže $d = \mathrm{NSD}(a,b)$, potom existují taková dvě celá čísla x, y, že $ax + by = d$. Navíc je nejmenší kladné číslo tvaru $ax + by$ největším společným dělitelem čísel a, b.

Důkaz. Označme $e = as + bt$ nejmenší *kladné* celé číslo, které se dá zapsat ve tvaru $ax + by$ pro pevně zvolená čísla a, b a libovolná celá čísla x, y. Protože $d \mid a$, $d \mid b$, jistě $d \mid e$. Protože e je kladné číslo a d je jeho kladný dělitel, tak $0 < d \leq e$.

Naopak, jestliže jedno z čísel a, b (bez újmy na obecnosti číslo a) vydělíme se zbytkem číslem e, bude zbytek po dělení čísla a číslem e opět číslo tvaru $ax + by$, neboť při dělení se zbytkem od a odečítáme nějaký násobek dělitele e, přičemž dělitel je tvaru $e = as + bt$. Podle Věty 0.2. bude zbytek $ax + by$ menší než e, ale protože e je nejmenší kladné číslo uvedeného tvaru, musí být zbytek 0. To znamená, že $e \mid a$ a analogicky ukážeme, že $e \mid b$. Protože d je největší společný dělitel čísel a, b, tak $e \mid d$, a tedy $e \leq d$.

Celkem dostáváme $e = d$. Číslo e je tedy největším společným dělitelem čísel a, b. □

Koeficientům x, y říkáme *Bézoutovy koeficienty*. Hodnotu koeficientů x, y je možno určit například Euklidovým algoritmem, který popíšeme v dalším textu na straně 3.

Příklad 0.2. Pro názornost uvedeme několik příkladů.

1) Platí $\mathrm{NSD}(12, 9) = 3$ a můžeme psát $3 = 1 \cdot 12 - 1 \cdot 9$. Koeficienty x, y z Bézoutova lemmatu jsou $x = 1$, $y = -1$.
2) Platí $\mathrm{NSD}(13, 10) = 1$, přičemž $1 = -3 \cdot 13 + 4 \cdot 10$. Příslušné koeficienty jsou $x = -3$, $y = 4$.
3) Platí $\mathrm{NSD}(-5, 7) = 1$, přičemž $1 = -3 \cdot (-5) - 2 \cdot 7$. příslušné koeficienty jsou $x = -3$, $y = -2$.

Lemma 0.4. Euklidovo lemma
Mějme prvočíslo p. Jestliže p dělí součin dvou celých čísel ab, tak p dělí a nebo p dělí b.

Důkaz. Předpokládejme, že p je prvočíslo a $p \mid ab$. Jestliže $p \mid a$, tvrzení platí. Jestliže $p \nmid a$, tak $\mathrm{NSD}(p, a) = 1$, neboť prvočíslo p má pouze dva kladné dělitele: číslo p, které není dělitelem a a číslo 1. Podle Bézoutova lemmatu 0.3. proto existují taková dvě celá čísla r a s, že

$$pr + as = 1.$$

Rovnost vynásobíme číslem b

$$prb + abs = b.$$

Nyní si všimneme, že levá strana rovnosti je dělitelná číslem p, neboť jistě $p \mid prb$ a podle předpokladu $p \mid ab$, což znamená, že p dělí i výraz na pravé straně rovnosti, tj. $p \mid b$. □

Euklidův algoritmus
Jedním ze základních tvrzením o celých číslech je tzv. Euklidův algoritmus. Ačkoli se mu říká „algoritmus“, samotné tvrzení žádný algoritmus neobsahuje, ten je popsán v důkazu tvrzení. Nyní můžeme vyslovit Euklidův algoritmus.

Algoritmus 0.5. Euklidův algoritmus
Mějme přirozená čísla a_1, a_2. Pro každé $n \geq 3$, pro které je $a_{n-1} \neq 0$, označme a_n zbytek po dělení čísla a_{n-2} čísel a_{n-1}. Po konečném počtu kroků dostaneme $a_k = 0$ a platí $a_{k-1} = \mathrm{NSD}(a, b)$.

Důkaz. Podle Věty 0.2. víme, že zbytek po dělení je menší než dělitel, proto $a_2 > a_3 > a_4 \ldots$. Protože zbytek po dělení je vždy nezáporné číslo, bude posloupnost kladných celých čísel $a_2, a_3, a_4, \ldots$ konečná a po jistém počtu kroků bude $a_k = 0$, přičemž $a_{k-1} \neq 0$. Z definice čísel $a_3, a_4, \ldots, a_k$ a z Věty 0.2. víme, že existují taková čísla $q_1, q_2, \ldots, q_{k-2}$, že platí

$$\begin{aligned} a_1 &= q_1 \cdot a_2 + a_3 \\ a_2 &= q_2 \cdot a_3 + a_4 \\ &\vdots \\ a_{k-3} &= q_{k-3} \cdot a_{k-2} + a_{k-1} \\ a_{k-2} &= q_{k-2} \cdot a_{k-1} + 0. \end{aligned} \tag{2}$$

Nyní si všimneme, že z poslední rovnosti (2) $a_{k-1} \mid a_{k-2}$. Potom z předposlední rovnice $a_{k-1} \mid a_{k-3}$. Analogicky z každé předchozí rovnice dostaneme, že $a_{k-1} \mid a_{k-4}$, $a_{k-1} \mid a_{k-5}$, …, $a_{k-1} \mid a_1$. To znamená, že a_{k-1} je společným dělitelem čísel a_1, a_2. Naopak, z první rovnice (2) vidíme, že libovolný společný dělitel čísel a_1, a_2 dělí $a_3 = a_1 - q_1 a_2$. Potom z druhé rovnice tento dělitel dělí i $a_4 = a_2 - q_2 a_3$, stejně tak $a_5, a_6, \ldots a_{k-1}$. To znamená, že a_{k-1} je největším společným dělitelem čísel a_1, a_2. □

Důkaz Věty 0.5. je konstruktivní a opravdu popisuje algoritmus, kterým můžeme největšího společného dělitele dvou čísel najít. Algoritmus lze popsat následujícím pseudokódem.

Algoritmus 0.6. Euklidův algoritmus
Mějme dvě přirozená číslo a_1, a_2.

```
int NSD(int a_1, int a_2) {
  int t;
  while (a_2 != 0) {
    t = a_2;
    a_2 = a_1 % a_2;
    a_1 = t;
  }
  return a_1;
}
```

V prvním kroku algoritmu (pokud není dělitel nulový), dělíme dělitele se zbytkem. V každém dalším kroku pak vždy dělíme dělitele předchozího kroku zbytkem předchozího kroku. Proměnná t slouží k dočasnému „zapamatování“ dělitele.

O něco elegantnější je využití rekurze. Celý algoritmus pak nepotřebuje pomocnou proměnnou explicitně, ale využije se předávání hodnotou.

Algoritmus 0.7. Rekurzivní Euklidův algoritmus
Mějme dvě přirozená číslo a_1, a_2.

```
int NSD(int a_1, int a_2) {
  if (a_2 == 0) {
    return a_1;
  }
  return NSD(a_2, a_1 % a_2);
}
```

Příklad 0.3. Najděte největšího společného dělitele čísel 78 a 210.
Postupujeme užitím Euklidova algoritmu. Označíme $a_1 = 210$, $a_2 = 78$. Podle Věty 0.2. zapíšeme $a_1 = qa_2 + r = qa_2 + a_3$, což dává

$$210 = 2 \cdot 78 + 54.$$

Máme $a_2 = 78$, $a_3 = 54$ a postup opakujeme. Dostaneme

$$78 = 1 \cdot 54 + 24.$$

Máme $a_3 = 54$, $a_4 = 24$, postup opakujeme. Dostaneme

$$54 = 2 \cdot 24 + 6.$$

Máme $a_4 = 24$, $a_5 = 6$, postup opakujeme. Konečně dostaneme

$$24 = 4 \cdot 6 + 0,$$

což znamená $a_5 = 6$, $a_6 = 0$. Podle Euklidova algoritmu je $\mathrm{NSD}(a_1, a_2) = \mathrm{NSD}(210, 78) = a_5 = 6$. ✓

Pokud bychom v předchozím příkladu označili $a_1 = 78$, $a_2 = 210$, tak po prvním kroku bychom měli

$$78 = 0 \cdot 210 + 78$$

a dále by $a_2 = 210$ a $a_3 = 78$. Za a_1 proto volíme větší z obou čísel, ušetříme jeden krok algoritmu.

Určení Bézoutových koeficientů
Bézoutovy koeficienty z Lemmatu 0.3. na straně 2 můžeme určit zpětným dosazováním v postupu Euklidova algoritmu. Poslední řádek Euklidova algoritmu vyjadřuje největšího společného dělitele d jako lineární kombinaci dvou členů. Postupným dosazením z předchozích řádků tohoto dělitele d vyjádříme jako lineární kombinaci členů a, b z prvního řádku.

Příklad 0.4. Vyjádřete největšího společného dělitele 6 čísel 78 a 210 jako jejich lineární kombinaci. Určete Bézoutovy koeficienty.
Postupujeme dle Příkladu 0.3. jsme vyjádřili

$$\begin{aligned} 210 &= 2 \cdot 78 + 54 \\ 78 &= 1 \cdot 54 + 24 \\ 24 &= 4 \cdot 6 + 0. \end{aligned}$$

Nyní zpětným dosazením z *předposlední* rovnosti vyjádříme

$$6 = 1 \cdot 54 - 2 \cdot 24.$$

Ihned vidím, že z předchozí rovnosti můžeme dosadit za číslo 24. Dostaneme

$$6 = 1 \cdot 54 - 2 \cdot (78 - 1 \cdot 54) = 3 \cdot 54 - 2 \cdot 78.$$

A konečně číslo 54 vyjádříme z první rovnosti a dosadíme.

$$6 = 3 \cdot (210 - 2 \cdot 78) - 2 \cdot 78 = 3 \cdot 210 - 8 \cdot 78.$$

Hledané Bézoutovy koeficienty jsou 3 a -8. Jistou výhodou celého postupu je, že v každém kroku můžeme udělat zkoušku, pravá a levá strana se musí rovnat. ✓

210	78	54	24	6	0
1	0	1	−1	3	
0	1	−2	3	−8	

Tabulka 0.1.: *Tabulka výpočtu Bézoutových koeficientů.*

Pokud nám při hledání největšího společného dělitele jde o určení Bézoutových koeficientů, můžeme pro zápis výpočtu využít následující úsporné schéma.

Příklad 0.5. Najděte největšího společného dělitele čísel 78 a 210 a určete Bézoutovy koeficienty.
Postupně sestavíme Tabulku 0.1. Celý postup může připomínat výpočet inverzní matice pomocí elementárních řádkových úprav.

Nejprve nadepíšeme první dva sloupce 210 a 78. Do dalších dvou řádků prvního sloupce vepíšeme 1, 0 a ve druhém sloupci 0, 1. Nyní budeme od dělence 210 odečítat vhodný násobek dělitele 78, abychom našli zbytek po dělení. Stejnou aritmetickou operaci zopakujeme i pro členy druhého a třetího řádku. Jestliže od 210 odečteme dvojnásobek 78. Dostaneme 54 a podobně odečtením dvojnásobku druhého sloupce od prvního dostaneme hodnoty 1, −2 třetího sloupce.

Celý postup zopakujeme s druhým a třetím sloupcem. Od 78 odečteme (jedno)násobek 54. Dostaneme 24 a podobně odečtením třetí sloupce od druhého sloupce a ve čtvrtém sloupci dostaneme −1, 3.

Dále od 54 odečteme dvojnásobek 24. Dostaneme 6 a podobně odečtením dvojnásobku čtvrtého sloupce od třetího sloupce dostaneme v pátém sloupci 3, −8.

A konečně, odečteme-li od 24 čtyřnásobek 6 dostaneme zbytek 0. Tím výpočet končí. Hledané Bézoutovy koeficienty jsou 3 a −8. První dva sloupce a pátý sloupec tabulky říkají, že $6 = 3 \cdot 210 - 8 \cdot 78$.

Celý výpočet je úsporně zapsaný. Vystupují v něm jen hodnoty zbytků, se kterými se při výpočtu Bézoutových koeficientů počítá. ✓

Základní věta aritmetiky

Důležitou vlastností (kladných) přirozených čísel je, že je umíme jednoznačně rozložit na součin prvočísel. To shrnuje následující věta.

Věta 0.8. Základní věta aritmetiky
Každé přirozené číslo větší než 1 je buď prvočíslo, nebo jej lze zapsat jako součin prvočísel, přičemž tento součin je jednoznačný až na pořadí činitelů.

Důkaz. Nejprve ukážeme existenci prvočíselného rozkladu, Tj. že každé číslo větší než 1 je buď prvočíslo, nebo jej lze zapsat jako součin prvočísel. Postupujeme silnou indukcí. Nejmenší přípustné číslo je 2, které je prvočíslem a pro něj tvrzení platí. Předpokládejme, že všechna celá čísla větší než 1 a menší než n umíme rozložit na součin prvočísel. Každé (větší) přirozené číslo n je buď prvočíslem (a tvrzení platí) nebo je číslem složeným a platí $n = ab$, přičemž $1 < a, b < n$. Podle indukčního předpokladu umíme čísla a i b napsat jako součin prvočísel $a = p_1 p_2, \ldots, p_k$ a $b = q_1 q_2 \cdots q_l$, a proto také $n = ab = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_l$ je součin prvočísel, a proto každé přirozené číslo větší než 1 je možno napsat jako součin prvočísel.

Dále ukážeme, že rozklad čísla n na prvočísla je jednoznačný až na pořadí činitelů. Postupujeme sporem. Předpokládejme, že přirozené číslo n, kde $n > 1$, umíme rozložit na součin prvočísel dvěma různými způsoby:

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$$

Ukážeme, že $k = l$ a prvočísla $p_1, p_2, \ldots, p_k$ jsou přeuspořádáním prvočísel $q_1, q_2, \ldots, q_l$. Protože p_1 je prvočíslo a p_1 dělí n, tak p_1 dělí podle Euklidova Lemmatu 0.4. některé z prvočísel $q_1, q_2, \ldots, q_l$. Bez újmy na obecnosti (po vhodném přeuspořádání a přeznačení) můžeme předpokládat, že $p_1 \mid q_1$. Protože q_1 je prvočíslo a má jen dva dělitele: 1 a q_1, platí $p_1 = q_1$. Ihned vidíme, že

$$\frac{n}{p_1} = p_2 p_3 \cdots p_k = q_2 q_3 \cdots q_l$$

a celý postup zopakujeme. Po k krocích dostaneme

$$\frac{n}{p_1 p_2 \cdots p_k} = q_{k+1} \cdots q_l$$

a proto $k \leq l$. Zopakováním celého postupu se záměnou prvočísel $p_1, p_2, \ldots, p_k$ a prvočísel $q_1, q_2, \ldots, q_l$ dostaneme $l \leq k$ a proto $k = l$ a oba rozklady čísla n jsou až na pořadí činitelů stejné. □

Později ukážeme, že některé algebraické struktury tuto „pěknou“ vlastnost jednoznačného rozkladu nemají. Budeme umět prvek napsat jako součin „menších“, dále nerozložitelných prvků, avšak takový rozklad nebude určen jednoznačně!

Cvičení

0.1.1. Mějme následující definici největšího společného dělitele: Mějme dvě celá čísla a, b. Největší společný dělitel čísel a, b je takový nezáporný společný dělitel m čísel a, b, který je dělitelný jejich libovolným společným dělitelem. a) Jaký je největší společný dělitel čísel v případě, že alespoň jedno z čísel je nulové? b) Která čísla jsou podle této definice nesoudělná s nulou?

0.1.2. Mějme následující definici nemenšího společného násobku: Mějme dvě nenulová celá čísla a, b. Nejmenší společný násobek čísel a, b je takový nezáporný společný násobek m čísel a, b, který je dělitelem jejich libovolného společného násobku. Značíme jej $NSN(a, b)$ nebo $[a, b]$. Jaký je nejmenší společný násobek čísel v případě, že alespoň jedno z čísel je nulové?

0.1.3. Napište NSD(1 529, 14 039) *jako lineární kombinaci obou čísel.*

0.1.4. a) Pro jaké hodnoty a, b není splněna nerovnost $NSD(a, b) > 0$? b) Pro jaké hodnoty a, b není splněna nerovnost $NSD(a, b) \leq \min\{a, b\}$?

0.2. Množiny

Při klasickém počítání s čísly obvykle pracujeme s nekonečně mnoha prvky v číselném oboru, máme například přirozená čísla $\mathbb{N}$, celá čísla $\mathbb{Z}$, racionální čísla $\mathbb{Q}$, reálná čísla $\mathbb{R}$, komplexní čísla $\mathbb{C}$. Mezi méně obvyklé číselné množiny patří množina prvočísel $\mathbb{P}$, iracionální čísla $\mathbb{I}$, sudá celá čísla $\mathbb{S}$, lichá celá čísla $\mathbb{L}$, množina všech čtvercových matic řádu n označená $M_{n,n}$, množina vektorů v n-rozměrném prostoru $\mathbb{R}^n$ a další. V kapitole 11. budeme pracovat s množinou všech polynomů s proměnnou x. Tuto množinu označíme $P[x]$, kde P bude číselná množina, ze které budou vybrány koeficienty polynomu. Například $\mathbb{R}[x]$ bude množina polynomů s reálnými koeficienty. Podobně zavedeme označení $P_n[x]$ pro množinu všech polynomů řádu nejvýše n s proměnnou x.

Co to však znamená „číselný obor“? A které vlastnosti číselného oboru jsou klíčové, bez kterých bychom se nemohli obejít? Jak se bude „počítat“ s prvky (ne nutně s čísly), pokud některé z obvyklých vlastností číselných množin nebudeme požadovat? To se z velké části dozvíte v následujících kapitolách.

Ukážeme například, že má smysl počítat i s konečnými číselnými soustavami, tj. s množinami čísel, které mají jen konečně mnoho prvků. Vždyť do počítače stejně neuložíme každé číslo. Číslo nemůže být libovolně velké či libovolně malé, počítač vždy pracuje s omezenou přesností.

Množinou rozumíme soubor prvků, množiny mohou být konečné i nekonečné. Množiny označujeme obvykle velkými písmeny $A, B, M, \ldots$. Prázdnou množinu označujeme symbolem $\emptyset$.

Důležitou vlastností množiny je její neuspořádanost – uspořádání *není* důležité a při práci s množinou pořadí prvků v množině nerozlišujeme. Pokud prvek x do množiny M patří, říkáme, že „x náleží množině M“ a píšeme $x \in M$. V opačném případě x do množiny M nenáleží, což zapisujeme $x \notin M$.

Prvek se v množině nemůže vyskytovat ve více kopiích, nemůže se opakovat, prvek do množiny pouze patří nebo nepatří. Tato vlastnost množiny se v obecnosti obtížně implementuje. Obvyklý trik je seřazení prvků množiny postavené na prinipu dobrého uspořádání (Věta 0.1.).

Dvě podmnožiny jsou si rovny, pokud mají všechny prvky stejné, píšeme $A = B$. V opačném případě jsou množiny různé a píšeme $A \neq B$. Jestliže všechny prvky množiny A patří také do množiny B, tak množina A je *podmnožinou* množiny B, což značíme $A \subseteq B$. Prázdná množina je podmnožinou každé množiny, a pokud $A \subseteq B$ a navíc $A \neq B$ (množina B obsahuje alespoň jeden prvek, který nepatří do množiny A), tak A je *vlastní* podmnožinou B a píšeme $A \subset B$.

Operace s množinami

S množinami můžeme provádět řadu obvyklých operací, které jsou známy už ze základní školy: sjednocení množin $A \sup B$, jejich průnik $A \cap B$, rozdíl $A \setminus B$, symetrická diference $A \triangle B$. Množiny můžeme i násobit.

Definice Kartézský součin množin

Mějme dvě množiny A, B. Jejich *kartézským součinem* rozumíme množinu všech uspořádaných dvojic sestavených z prvků množin A a B v tomto pořadí, tj. první prvek je z A a druhý prvek je z B. Kartézský součin značíme $A \times B$ a symbolicky jej můžeme zapsat jako

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

Kartézský součin $A \times A$ je *(druhá) kartézská mocnina*, značíme ji A^2. Podobně definujeme třetí, čtvrtou, a další kartézské mocniny $A^n = \{(a_1, a_2, \ldots, a_n) : a_1, a_2, \ldots, a_n \in A\}$.

Všimněte si, že obecně $A \not\subseteq A \times B$, ani $B \not\subseteq A \times B$, zatímco například platí $A \subseteq A \cup B$. Podobně $A \notin A \times B$, ani $B \notin A \times B$, zatímco $A \in P(A)$ platí. Množství různých operací s množinami je bohatší, než s čísly. Další typ součinu (pod)množin nadefinujeme v Kapitole 3.4. na straně 71.

Otázky:

- Najdete dvě množiny A a B tak, aby $A \in A \cup B$?
- Najdete dvě *různé* množiny A a B tak, aby $A \times B = B \times A$?
- Najdete dvě množiny A a B tak, aby $A \subseteq A \times B$?
- Najdete dvě množiny A a B tak, aby $A \in A \times B$?

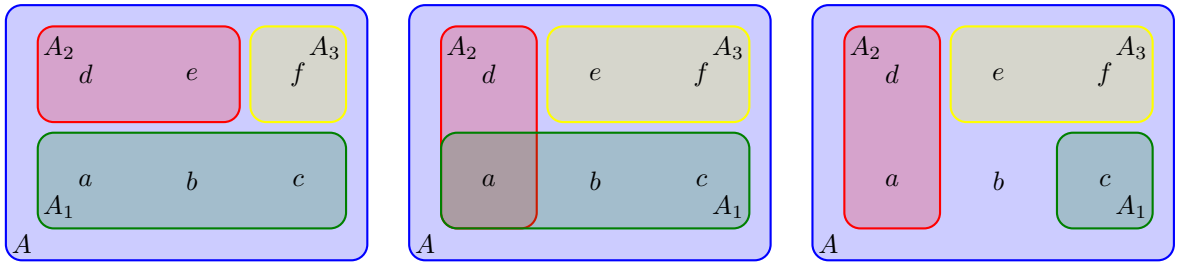
Rozklad množiny

Jestliže množina S obsahuje jako prvky jen množiny, říkáme, že S je *systém* množin. Je to nejen přehlednější, ale i srozumitelnější než „množina množin“. V Kapitole 4. bude pracovat s rozklady množin. Připomeneme definici rozkladu množin.

Definice Rozklad množiny
Rozklad množiny A je takový systém podmnožin množiny A, které jsou

(i) neprázdné,
(ii) po dvou navzájem disjunktní a
(iii) jejichž sjednocení je množina A.

Podmnožinám v tomto sytému podmnožin říkáme *třídy rozkladu*.



Obrázek 0.1.: *Rozklad množiny A a dva systémy podmnožiny, které rozklad množiny A netvoří.*

Na Obrázku 0.1. vlevo je rozklad množiny A na tři podmnožiny A_1, A_2, A_3. Systém podmnožin množiny A na Obrázku 0.1. uprostřed není rozkladem, neboť podmnožiny A_1, A_2 nejsou disjunktní. Systém podmnožin na Obrázku 0.1. vpravo není rozkladem, neboť sjednocení všech podmnožin neobsahuje všechny prvky množiny A.

Symbolicky můžeme rozklad množiny A popsat jako systém podmnožin $A_i \subseteq A$ (kde $i \in I$, přičemž I je nějaká indexová množina), pro který platí

(i) $A_i \neq \emptyset$ pro každé $i \in I$,
(ii) $A_i \cap A_j = \emptyset$ pro každé $i, j \in I$, $i \neq j$,
(iii) $\bigcup_{i \in I} A_i = A$.

Potenční množinou dané množiny A rozumíme množinu (nebo systém) všech podmnožin dané množiny. Potenční množinu množiny A značíme 2^A. Pro konečnou množinu A snadno nahlédneme, že její potenční množina má $2^{|A|}$ prvků (různých množin).

Otázky:

- Jaký je rozdíl mezi $\emptyset$ a $\{\emptyset\}$?
- Jak vypadá potenční množina prázdné množiny?
- Jaká množina má prázdnou potenční množinu?
- Platí $A \in 2^A$ nebo $A \subseteq 2^A$?
- Tvoří prvky potenční množiny $P(A)$ rozklad množiny A?

0.3. Relace

V matematice chápeme „relaci mezi prvky množin“ jako nějaký „vztah“ mezi objekty, které jsou reprezentovány prvky množin. Podobně v běžné řeči chápeme „relaci“ jako (vzájemnou) souvislost mezi nějakými objekty.

Definice **Relace na množině**
Mějme množinu A. *Relací R na množině A* rozumíme libovolnou podmnožinu druhé kartézské mocniny množiny A. Symbolicky můžeme zapsat $R \subseteq A \times A$.

Zatímco relace na množině popisuje vztahy mezi prvky jedné množiny, tak následující definice ukazuje, že vztahy můžeme popisovat i mezi dvěma případně více množinami.

Definice **Relace mezi množinami**
Mějme množiny A, B. *Relací R mezi množinami A, B* rozumíme libovolnou podmnožinu kartézského součinu množin $A \times B$ (v tomto pořadí). Symbolicky můžeme zapsat $R \subseteq A \times B$.

Někdy se nerozlišuje mezi pojmy *relace na množině* a *relace mezi množinami* a mluvíme jen o *relaci*. O který z pojmů se jedná pak vyplývá z kontextu.

Protože relace zachycují vztah mezi prvky nějaké množiny, tak přirozenou otázkou je, zda nějaké dva prvky spolu v relaci jsou nebo nejsou. Navíc rozlišujeme pořadí prvků v relaci. Mějme dva prvky $x, y \in A$ a relaci $R \in A^2$. Jestliže relace R obsahuje uspořádanou dvojici (x, y), tak říkáme, že prvek x je v relaci s prvkem y (v tomto pořadí), což stručně zapisujeme xRy. Upozorňujeme, že současně prvek y *může, ale nemusí* být v relaci s prvkem x. Závisí na tom, zda také $(y, x) \in R$. Pokud ano, tak můžeme říci, prvky x a y jsou navzájem v relaci a pokud ne, tak prvek y s prvkem x v relaci není, což zapisujeme $y \not R x$ nebo případně $(y, x) \notin R$.

Různých relací na nějaké množině existuje i pro malé množiny ohromné množství. Například na desetiprvkové množině existuje $2^{(10^2)} = 2^{100} \doteq 1.27 \cdot 10^{30}$ různých relací, což je číslo skoro o sedm řádů větší, než Avogadrova konstanta $N_A \doteq 6 \cdot 10^{23}$. Připomeňme, že Avogadrova konstanta udává počet atomů v dvanácti gramech nuklidu uhlíku ${}^{12}_{6}C$, který obsahuje v jádře šest protonů a šest neutronů. Proto nemá smysl zabývat se *všemi* relacemi na dané množině, obvykle se omezujeme na takové relace, které mají „pěkné“ vlastnosti.

Relace ekvivalence
Jedním z nejdůležitějších příkladů relací prvků na dané množině je relace ekvivalence. Popisuje vztah mezi prvky jedné množiny, každé dva prvky buď v relaci jsou nebo nejsou. Aby dané relace byla relací ekvivalence, musí splňovat tři vlastnosti popsané v následující definici.

Definice **Relace ekvivalence**
Řekneme, že relace R na množině A je relací *ekvivalence* právě tehdy, když splňuje následující tři vlastnosti:

1) je *reflexivní*, tj. platí $\forall x \in A$ platí $(x, x) \in R$,
2) je *symetrická*, tj. platí $\forall x, y \in A$ platí $(x, y) \in R \Leftrightarrow (y, x) \in R$,
3) je *tranzitivní*, tj. platí $\forall x, y, z \in A$ platí $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$.

Relaci ekvivalence na množině A lze alternativně chápat jako rozklad množiny A, který jsme zavedli na straně 7. Může se zdát překvapivé, že takový alternativní přístup popisuje stejnou věc jen jiným jazykem. Každé relaci ekvivalence na množině A odpovídá jednoznačně určený rozklad množiny A a naopak, každému rozkladu množiny A odpovídá jednoznačně určená relace ekvivalence na množině A (Cvičení 0.3.1.).

Relace kongruence
Důležitým příkladem relace ekvivalence je relace kongruence modulo m.

Fakt, že celé číslo a dává po dělení přirozeným číslem m zbytek r znamená, že podle Věty 0.2. existují taková celá čísla q, r, že platí $a = qm + r$ a r a $0 \leq r < m$. Číslu q říkáme *podíl* a číslu r *zbytek* po dělení čísla a číslem m.

Definice Mějme celá čísla a, b a přirozené číslo m. Řekneme, že čísla a, b jsou *kongruentní modulo m*, jestliže dávají stejný zbytek po dělení číslem m. Zapisujeme $a \equiv b \pmod{m}$.

Na běžných ručičkových hodinách nerozlišíme, pokud interval trvá 1, 13, 25 nebo 49 hodin. Údaj na ciferníku bude odpovídat stejné poloze ručiček. Říkáme, že „1 je kongruentní s číslem 13 modulo 12“. Formálně zapíšeme

$$1 \equiv 13 \pmod{12}.$$

Kongruence je vztah mezi celými čísly, jedná se o relaci, která je reflexivní, symetrická i tranzitivní, a proto se jedná o relaci ekvivalence. Některé dvojice čísel jsou kongruentní, potom je považujeme za ekvivalentní. Jiné dvojice čísel kongruentní nejsou. Například

$$1 \not\equiv 20 \pmod{12}.$$

A proto při počítání modulo 12 nebudeme rozlišovat například číslo 1 a číslo 13, ale budeme rozlišovat například číslo 1 a číslo 20. Podobně nebudeme rozlišovat čísla 8 a 20, protože $20 \equiv 8 \pmod{12}$. Vystačíme s dvanácti různými čísly jako v Tabulce 0.3. na straně 24 (případně v Tabulce 0.4.). Jestliže budeme počítat modulo 6, můžeme analogicky sestavit Tabulku 0.5. Podobná tabulka by šla sestavit pro běžné sčítání všech celých čísel nebo přirozených čísel pouze teoreticky. Prakticky však takovou tabulku nemá smysl sestavovat, protože přirozených i celých čísel je nekonečně mnoho a odpovídající tabulka by měla nekonečně mnoho řádků i sloupců.

Ukážeme dvě ekvivalentní formulace tvrzení, že $a \equiv b \pmod{m}$. První říká, že $a \equiv b \pmod{m}$ právě tehdy, když m dělí rozdíl $b - a$.

Lemma 0.9. *Mějme celá čísla a, b a přirozené číslo m. Potom $a \equiv b \pmod{m}$ právě tehdy, když $m \mid (b - a)$.*

Důkaz. Tvrzení má tvar ekvivalence, ukážeme obě implikace.
„⇒“ Jestliže platí $a \equiv b \pmod{m}$, tak podle definice kongruence existují taková celá čísla q_1, q_2, r, kde $0 \leq r < m$ že platí

$$a = q_1 m + r, \quad b = q_2 m + r.$$

Všimněte si, že zbytek po dělení číslem m je pro obě čísla a, b stejný. Rozdíl čísel $a - b$ pak je roven

$$a - b = (q_1 m + r) - (q_2 m + r) = (q_1 - q_2)m.$$

To ale znamená, že $a - b$ je násobkem modulu m, neboli, že m dělí $a - b$.
„⇐“ Jestliže m dělí $a - b$, tak existuje takové celé číslo k, že $a - b = mk$. To ale znamená $a = b + mk$.

Dále označme zbytek po dělení čísla a číslem m označme r. To znamená, že existuje takové celé číslo q, že

$$a = qm + r,$$

kde $0 \leq r < m$. Dosazením do levé strany rovnosti dostane

$$b + mk = qm + r.$$

Odtud vyjádříme $b = (q - k)m + r$, kde $0 \leq r < m$. Rozdíl celých čísela $q - k$ je jistě celé číslo. To znamená, že b dává po dělení číslem m stejný zbytek r jako číslo a. □

Dále ukážeme, že $a \equiv b \pmod{m}$ právě tehdy, když existuje celé číslo k takové, že b se liší od a přičtením vhodného násobku m.

Lemma 0.10. *Mějme celá čísla a, b a přirozené číslo m. Potom $a \equiv b \pmod{m}$ právě tehdy, když existuje celé číslo k takové, že $b = a + km$.*

Důkaz je ponechán jako Cvičení 0.3.2.

Příklad 0.6. Určete všechna celá čísla x, pro která platí a) $x \equiv 7 \pmod{10}$ b) $x \equiv -3 \pmod{11}$.
a) Podle definice kongruence, hledáme všechna celá čísla, která dávají zbytek 7 po dělení 10. Takových čísel je pochopitelně nekonečně mnoho a všechna jsou tvaru $x = 10t + 7$ pro nějaké celé číslo t. Řešení zapíšeme $x = 10t + 7$, $t \in \mathbb{Z}$.
b) Podle definice kongruence, hledáme všechna celá čísla, která dávají stejný zbytek jako -14 po dělení 11. Zbytek po dělení nemůže být záporný. Víme však, že $-14 + 2 \cdot 11 = 8$ a 8 proto zbytek po dělení čísla x číslem 11 musí být stejný jako zbytek po dělení čísla -14 číslem 11, a proto $x = 11t + 8$. Hledaný čísel je opět nekonečně mnoho a všechna jsou tvaru $x = 11t + 8$ pro nějaké celé číslo t. Řešení zapíšeme $x = 11t + 8$, $t \in \mathbb{Z}$. ✓

Vlastností relace kongruence s výhodou využijeme při ověřování dělitelnosti nebo při hledání zbytku po dělení velkých čísel.

Příklad 0.7. Bez kalkulačky určete zbytek po dělení čísla 64 835 číslem 7.

Využijeme relace kongruence

$$64\,835 \equiv 1\,835 \equiv 435 \equiv 15 \equiv 1 \pmod 7$$

nebo třeba

$$64\,835 \equiv 1\,835 \equiv 435 \equiv -55 \equiv -6 \equiv 1 \pmod 7,$$

přičemž vždy počítáme s čísly, která se liší o nějaký násobek modulu a tedy jsou podle Lemmatu 0.10. kongruentní modulo 7 a dávají podle Lemmatu 0.9. stejný zbytek. Například v prvním řádku využijeme postupně, že číslo 63 000 je násobek 7, že čísla 1 400, 420 a 14 jsou násobky 7. ✓

Uvedený početní postup lze úspěšně používat i zpaměti, při ověřování kontrolních součtů u rodného čísla, u kódů ISBN a podobně.

Relace částečného uspořádání
Dalším důležitým příkladem relací jsou relace částečného uspořádání.

Definice Relace částečného uspořádání
Řekneme, že relace R na množině A je relací *částečného uspořádání* právě tehdy, když splňuje následující tři vlastnosti:

1) je *reflexivní*, tj. platí $\forall x \in A$ platí $(x, x) \in R$,
2) je *antisymetrická*, tj. platí $\forall x, y \in A$ platí $(x, y) \in R \wedge (y, x) \in R \Rightarrow x = y$,
3) je *tranzitivní*, tj. platí $\forall x, y, z \in A$ platí $(x, y), (y, z) \in R \Rightarrow (x, z) \in R$.

Všimněte si, že relace částečného uspořádání a relace ekvivalence se liší v jediné vlastnosti. Zatímco relace ekvivalence je symetrická relace, tak relace částečného uspořádaní je antisymetrická relace. Je-li nějaké relace R na množině A antisymetrická, nemohou dva různé prvky $x, y \in A$ být současně v relaci xRy a yRx. Definice antisymetrie může být vyslovena i jinak, například: pro každé $x, y \in A$, $x \neq y$ platí $xRy \Rightarrow y \not R x$. Pro ověření antisymetrie je však zpravidla šikovnější implikace z definice částečného uspořádání.

Zatímco relace ekvivalence na množině A přirozeně určuje rozklad množiny A, tak relace částečného uspořádání určuje hierarchickou strukturu prvků množiny A. Díky antisymetrii relace R na množině A umíme pro každou dvojici prvků x, y, které jsou navzájem v relaci R, rozhodnout o jejich *pořadí*, neboť nastane právě jedna z možností xRy nebo yRx. Protože prvky x, y nemusí být vzájemně v relaci, tak hovoříme o „částečném“ uspořádání. Klasickým příkladem uspořádání je relace „$\leq$“, která je navíc úplnou (nikoliv jen částečnou) relací uspořádání, neboť pro každá dvě reálná čísla x, y umíme rozhodnout, zda xRy nebo yRx. Naproti tomu relace dělitelnosti „$|$“ je relací částečného uspořádání celých čísel, neboť například $2 \mid 4$, ale $2 \nmid 5$ ani $5 \nmid 2$.

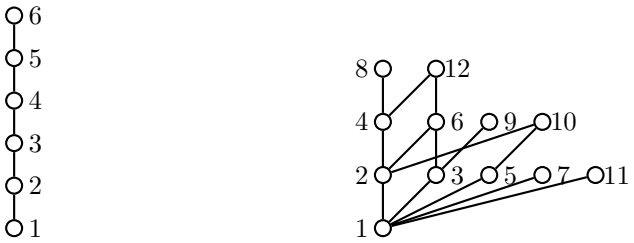
Otázky:

- Může na neprázdné množině A existovat relace, která je současně symetrická i antisymetrická ?
- Může na neprázdné množině A existovat relace, která je současně relací ekvivalence i relací částečného uspořádání?
- Je relace „$<$“ na množině $\mathbb{Z}$ relací částečného uspořádání?
- Se kterým prvky je v relaci dělitelnosti celých čísel v relaci číslo 0 a) zleva, b) zprava?

Hasseovský diagram
Příklad rozkladu množiny A na třídy A_1, A_2, A_3 určený relací ekvivalence je znázorněný na Obrázku 0.1. vlevo. Vezmeme-li relaci částečného uspořádání R množiny A, tak můžeme tuto množině s relací znázornit pomocí hierarchického diagramu, kterému se říká *hasseovský diagram* Obrázek 0.2.). Prvky množiny A znázorníme jako body roviny v různé výšce (v myšlené souřadné soustavě, kterou nezakreslujeme). Pro dvojice různých bodů x, y dodržíme následující dvě pravidla

(i) Je-li xRy, tak bod x zakreslíme níž než bod y.
(ii) Dva body spojíme hranou, jestliže xRy a neexistuje žádné $t \in A$ takové, aby xRt a současně tRy.

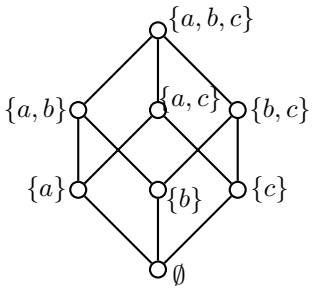
Diagram neobsahuje žádné smyčky, třebaže $(x, x) \in R$ pro každé $x \in A$. Říkáme, že prvek y je *bezprostřední následovník* prvku x. Všimněte si, že vzájemná úroveň každých dvou prvků v relaci je určena jednoznačné,



Obrázek 0.2.: *Lineární uspořádání relace menší nebo rovno „$\leq$“ na množině $[1,6]$ a částečné uspořádání relace dělitelnosti „$|$“ na množině $[1,12]$.*

protože relace R je antisymetrická. Navíc všechny spojnice, které vyplývají z tranzitivity relace, do diagramu nezakreslujeme (Obrázek 0.2.).

Na Obrázku 0.2. vlevo vidíme příklad relace částečného uspořádání, která je navíc úplná. Hasseovský diagram takové relace tvoří řetězec bodů. Naproti tomu relace dělitelnosti „$|$“ na nějaké množině přirozených čísel je pěkným příkladem relace částečného uspořádání, které obecně *není* lineární (Obrázek 0.2. vpravo). Dalším běžným příkladem nelineární relace uspořádání je relace inkluze „$\subseteq$“ na potenční množině nějaké n-prvkové množiny (Obrázek 0.3.).



Obrázek 0.3.: *Relace podmnožiny $\subseteq$ na systému podmnožin množiny $\{a,b,c\}$.*

Velkou výhodou hasseovských digramů je jejich přehlednost. Zakreslené relace na konečných množinách, případně část relace na nekonečných množinách jsou názorně zachyceny, v podstatě ihned lze identifikovat maximální minimální, největší i nejmenší prvky dané příslušnou relací.

Dvojice (A,R) množiny A a relace částečného uspořádání se nazývá „poset“ dle anglického názvu „partially ordered set“. Česky se někdy používá zkratka „ČUM“ (částečně uspořádaná množina), který ovšem nezní tak pěkně.

Cvičení

0.3.1. Ukažte, že a) každé relaci ekvivalence na množině A odpovídá jednoznačně určený rozklad množiny A, b) každému rozkladu množiny A odpovídá jednoznačně určená relace ekvivalence na množině A.

0.3.2. Dokažte Lemma 0.10.: Pro celá čísla a, b platí $a \equiv b \pmod m$ právě tehdy, když existuje celé číslo k takové, že $b = a + km$.

0.3.3. Určete chybějící znak rodného čísla 92102?4219.

0.3.4. Určete chybějící znak rodného čísla 92102?4279.

0.3.5. Kolik existuje různých relací na konečné n prvkové množině A?

0.3.6. Kolik existuje relací na konečné n prvkové množině A takových, které jsou symetrické i antisymetrické současně?

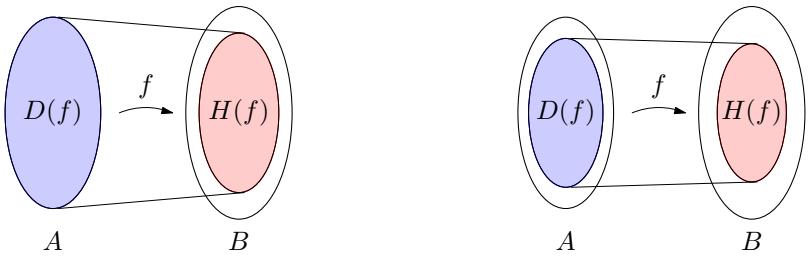
0.3.7. Kolik existuje relací na konečné n prvkové množině, které jsou a) symetrické, b) antisymetrické, c) úplné? Relace na množině A se nazývá úplná, pokud pro každé dva prvky $x, y \in A$ platí xRy nebo yRx.

0.4. Zobrazení

Zobrazení $f : A \to B$ je pravidlo, které každému prvku množiny A (množina *vzorů*) přiřazuje právě jeden prvek z množiny B (množina *obrazů*). Všimněte si, že toto „přiřazení“ je vztahem mezi dvojicemi prvků, kdy jeden prvek je z množiny A a druhý prvek je z množiny B. Proto formálně definujeme *zobrazení*

množiny A do množiny B jako relaci mezi množinami A a B, ve které je každý prvek množiny A v relaci s právě jedním prvkem množiny B. Podle uvedené definice ne každý prvek množiny obrazů B je nutně v relaci (následovníkem) nějakého prvku množiny A. Množina vzorů A je současně *definičním oborem* $D(f)$ zobrazení f a *obor hodnot* zobrazení f je taková podmnožina $H(f)$ množiny B, jež obsahuje všechny prvky B, které jsou v relaci s nějakým prvkem množiny A (jsou následovníkem nějakého prvku z A). Množině A se také říká *levá množina* a množině B *pravá množina* zobrazení f.

Někdy bývá zobrazení definováno jako pravidlo, které některým prvkům z množiny A přiřazuje nejvýše jeden prvek z množiny B. Takové zobrazení pak nazýváme *zobrazení z množiny* A do množiny B (nepřehlédněte předložku „z“ v názvu) a definujeme jej jako relaci mezi množinami A a B, ve které je každý prvek množiny A v relaci s nejvýše jedním prvkem množiny B. Všimněte si, že podle definice nemusí být každý prvek množiny vzorů A v relaci s nějakým prvkem množiny obrazů B. Definičním oborem je pak taková podmnožina množiny A, která obsahuje všechny prvky A, které jsou v relaci s nějakým prvkem množiny B (jsou předchůdcem nějakého prvku z B).

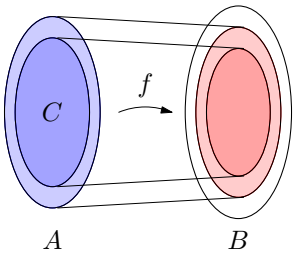


Obrázek 0.4.: *Zobrazení A do B a z A do B se zvýrazněným definičním oborem a oborem hodnot.*

Zobrazení f množiny A (nebo i z množiny A) do množiny B značíme $f : A \to B$. Protože takové přiřazení je pro každý prvek z A jednoznačné, můžeme místo zápisu relace užitím uspořádaných dvojic $(a, b) \in A \times B$ použít stručnější a přehlednější zápis $b = f(a)$, kde $a \in A$ je *vzor* prvku b, $b \in B$, kterému říkáme *obraz* prvku a. V dalším textu budeme téměř vždy předpokládat, že definičním oborem zobrazení $f : A \to B$ je celá množiny A a f je zobrazením množiny A, nikoliv zobrazením z množiny A. Ve zbývajících případech budeme rozlišovat množinu A a definiční obor $D(f)$.

Restrikce zobrazení

Mějme dáno nějaké zobrazení $f : A \to B$ a podmnožinu $C \subseteq A$. *Restrikce* zobrazení f na množinu C je zobrazení $f' : C \to B$ takové, že pro každé c z množiny C, platí $f'(c) = f(c)$.

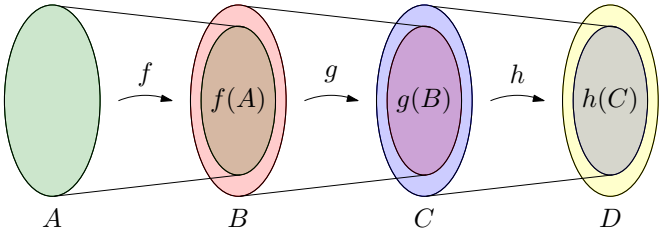


Obrázek 0.5.: *Restrikce zobrazení $f : A \to B$ na množinu C.*

Je zřejmé, že pro každé zobrazení z množiny A do množiny B můžeme najít takovou největší podmnožinu $C \subseteq A$, aby restrikce $f' : C \to B$ byla zobrazením množiny C do množiny B, nikoliv z množiny C do B. Taková největší množina C je definičním oborem zobrazení f.

Asociativita skládání zobrazení

Je dobré si uvědomit, že libovolné skládání zobrazení je vždy asociativní operace. Stačí, aby obor hodnot každého ze skládaných zobrazení patřil do definičního oboru následujícího zobrazení. Mějme tři libovolná zobrazení množin (nikoliv z množin) $f : A \to B$, $g : B \to C$, $h : C \to D$. Zdůrazněme, že z definice zobrazení musí být obraz definován *pro každý* prvek z levé množiny, tj. zobrazení f musí být definováno pro každý



Obrázek 0.6.: *Skládání zobrazení $h \circ g \circ f$.*

prvek z množiny A, zobrazení g musí být definováno pro každý prvek z množiny B a konečně zobrazení h musí být definováno pro každý prvek z množiny C (Obrázek 0.6.).

A protože obor hodnot každého zobrazení je podmnožinou definičního oboru následujícího zobrazení, můžeme ukázat následující lemma.

Lemma 0.11. Asociativita skládání zobrazení
Mějme tři libovolná zobrazení množin $f : A \to B$, $g : B \to C$, $h : C \to D$. Operace skládání zobrazení je asociativní, tj. platí $h \circ (g \circ f) = (h \circ g) \circ f$.

Důkaz. Platí

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

a současně

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

Platí tedy $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x)$, neboť se shodují předpisy, definiční obory a dokonce i obory hodnot. □

Otázka: Pokud bychom chtěli ověřit asociativitu skládání zobrazení na konečné n-prvkové množině tak, že porovnáme obrazy složených zobrazení, kolik trojic zobrazení je nutno složit a vyčíslit pro ověření asociativity?

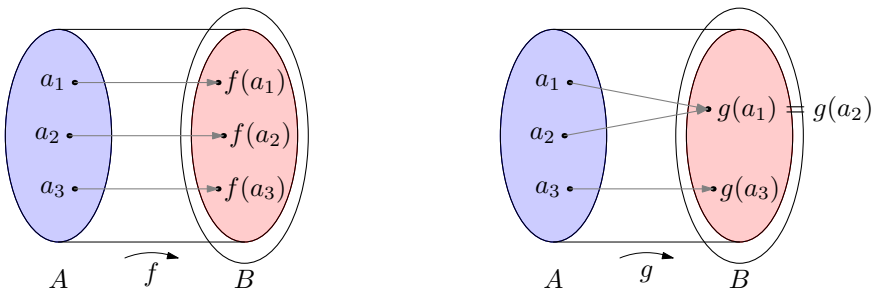
Další vlastnosti zobrazení
Zobrazení $f : A \to B$ se nazývá *injektivní* (nebo *prosté*), jestliže každé dva různé vzory z levé množiny A mají různé obrazy v pravé množině B. Symbolicky můžeme zapsat

$$\forall a_1, a_2 \in A : a_1 \neq a_2 \Rightarrow f(a_1) \neq f(a_2).$$

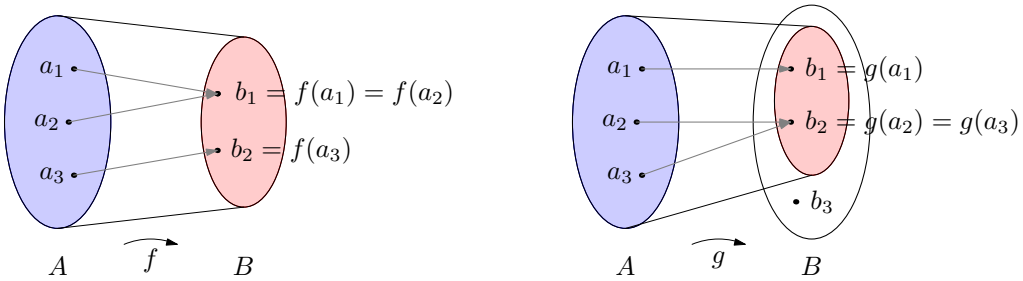
Pro praktické ověření je šikovnější pracovat s rovnostmi (nikoliv nerovnostmi), proto vyslovíme obměnu definice vlastnosti injekce: zobrazení $f : A \to B$ je injektivní, jestliže rovnost dvou obrazů v pravé množině nastane pouze v případě rovnosti vzorů z levé množiny. Symbolicky zapsáno

$$\forall a_1, a_2 \in A : f(a_1) = f(a_2) \Rightarrow a_1 = a_2,$$

což je implikace, která se při známém předpisu ověřuje jako rovnost výrazů snadněji než nerovnost.



Obrázek 0.7.: *Schématické znázornění: zobrazení f je injektivní a zobrazení g není injektivní.*



Obrázek 0.8.: *Schématické znázornění: zobrazení f je surjektivní a zobrazení g není surjektivní.*

Zobrazení $f : A \to B$ se nazývá *surjektivní* (nebo *zobrazení na*), jestliže každý prvek z pravé množiny B je obrazem nějakého vzoru z levé množiny A. Symbolicky můžeme zapsat

$$\forall b \in B\ \exists a \in A : f(a) = b,$$

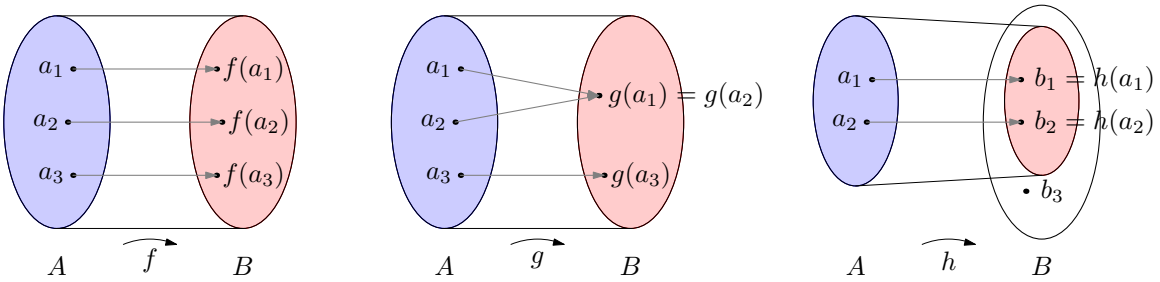
což je implikace, která se při známém předpisu ověřuje například jako řešení rovnice.

Zobrazení $f : A \to B$ se nazývá *bijektivní* (nebo *vzájemně jednoznačné*), jestliže je injektivní a surjektivní současně. To znamená, že každý prvek z pravé množiny B má jiný vzor v levé množině A. Symbolicky můžeme zapsat

$$\forall b \in B\ \exists! a \in A : f(a) = b,$$

což je implikace, kterou je opět možno při známém předpisu ověřit například jako řešení rovnice.

Aby zobrazení nebylo bijektivní, stačí najít alespoň dva vzory v levé množině A se stejným obrazem v pravé množině B (například zobrazení g na Obrázku 0.8. uprostřed) a nebo najít alespoň jeden prvek v pravé množině B, který nemá vzor v levé množně A (například zobrazení h na Obrázku 0.8. vpravo).

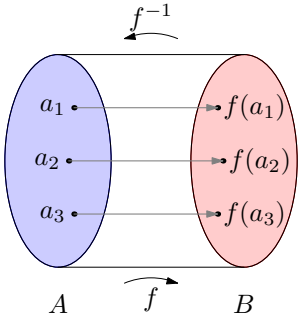


Obrázek 0.9.: *Schématické znázornění: zobrazení f je bijektivní a zobrazení g ani h nejsou bijektivní.*

Pochopitelně „většina“ zobrazení množiny A do množiny B není ani injektivních, ani surjektivních, ani bijektivních. Stačí, aby dva prvky z levé množiny měly společný obraz v pravé množině a současně aby alespoň jeden prvek z pravé množiny neměl vzor v levé množině. Zbývající prvky mohou být přiřazeny libovolně a zobrazení nemůže být ani injektivní ani surjektivní.

Existence inverzního zobrazení

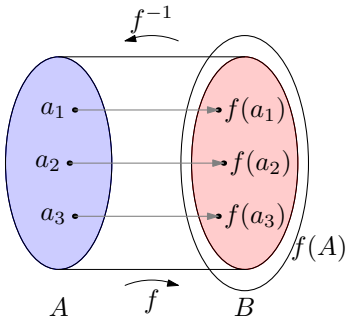
Mějme zobrazení $f : A \to B$. Zobrazení $g : B \to A$, které každému prvku $y \in B$ přiřadí takový prvek $x \in A$, aby platilo $g(y) = x$ právě tehdy, když $f(x) = y$, nazveme *inverzní zobrazení* k zobrazení f. Inverzní zobrazení g zpravidla značíme f^{-1}.



Obrázek 0.10.: *Bijektivní zobrazení f a inverzní zobrazení f^{-1}.*

Aby k zobrazení f existovalo inverzní zobrazení f^{-1}, musí zobrazení f být bijekce množiny A do množiny B (Obrázek 0.10.). Pokud by zobrazení f nebylo prosté, tak g by nebylo zobrazení, neboť k nějaké hodnotě $y \in B$ nebyla funkční hodnota inverzního zobrazení určena jednoznačně. Pokud by zobrazení f nebylo na (surjektivní), tak by g nebyla definována na celé množině B a jednalo by se o zobrazení z $B \to A$, nikoliv $B \to A$.

V některé literatuře se za postačující podmínku existence inverzní funkce považuje prostota funkce $f : A \to B$. Inverzní funkce f^{-1} se pak definuje pouze na oboru hodnot $f(A)$, a potom $f^{-1} : f(A) \to A$ (Obrázek 0.11.).



Obrázek 0.11.: *Injektivní zobrazení f a inverzní zobrazení f^{-1}.*

0.5. Permutace

Bijektivním zobrazením neprázdné množiny A říkáme *permutace* množiny A. Permutace π je kterákoliv bijekce $\pi : A \to A$. Jestliže zvolíme nějaké pevné uspořádání prvků množiny A, tak každou permutaci množiny A můžeme chápat jako nějaké přeuspořádání prvků množiny.

Permutace má smysl zkoumat na každé neprázdné množině A, v tomto textu se omezíme na permutace konečných množin. Máme-li neprázdnou konečnou množinu A, můžeme bez újmy na obecnosti prvky množiny označit $1, 2, \ldots, n$ (čísla můžeme chápat jako indexy jednotlivých prvků množiny A). Počet různých permutací množiny A značíme $P(n)$ a platí $P(n) = n!$. Permutacím a jejich vlastnostem bude věnována Kapitola 7.

Popis permutací pomocí matice

Každou permutaci pak můžeme popsat pomocí dvouřádkové matice, kde v prvním řádku uvedeme každý prvek $a \in A$ a v druhém řádku matice pod něj jeho obraz $\pi(a)$. Zápis permutace π vypadá takto

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n-1 & n \\ \pi(1) & \pi(2) & \cdots & \pi(n-1) & \pi(n) \end{pmatrix}.$$

Zápis permutace pomocí matice není jednoznačný, každou permutaci můžeme zapsat $n!$ různými způsoby.

Příklad 0.8. Mějme permutaci $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$. Zapíšeme ji čtyřmi různými způsoby. Určíme celkový počet různých zápisů.

Permutaci α můžeme zapsat celkem $4! = 24$ různými způsoby. Například

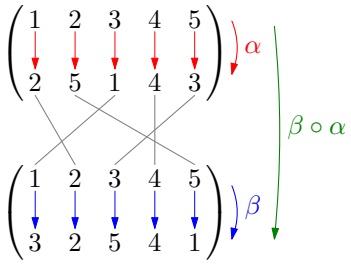
$$\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 & 4 & 5 \\ 5 & 2 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 4 & 5 & 1 \\ 5 & 1 & 4 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 5 & 4 & 3 & 2 & 1 \\ 3 & 4 & 1 & 5 & 2 \end{pmatrix}.$$

Všechny zápisy popisují stejnou permutaci α, neboť $\alpha(1) = 2$, $\alpha(2) = 5$, $\alpha(3) = 1$, $\alpha(4) = 4$ a $\alpha(5) = 3$. ✓

Z praktických důvodů budeme upřednostňovat zápis, kde v prvním řádku matice je nějaké pevně zvolené pořadí prvků. Pokud pracujeme s číselnými množinami $[1, n]$, tak přirozeně volíme pořadí $1, 2 \ldots, n$.

Skládání permutací

Permutace chápeme jako bijektivní zobrazení na nějaké množině A, a protože složením bijekcí je opět bijekce, tak složením dvou permutací na množině A dostaneme opět permutaci na množině A. Jestliže α i β jsou nějaké permutace $A \to A$, tak má smysl zkoumat složené permutace $\beta \circ \alpha$, $\alpha \circ \beta$, nebo například $\alpha \circ \alpha$, či $\alpha \circ (\beta \circ \alpha)$, případně další.



Obrázek 0.12.: *Skládání permutací $\beta \circ \alpha$ množiny* $[1, 5]$.

Příklad 0.9. Mějme permutace $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 1 & 4 & 3 \end{pmatrix}$ a $\beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 2 & 5 & 4 & 1 \end{pmatrix}$. Sestavíme obě složené permutace $\beta \circ \alpha$ i $\alpha \circ \beta$.

Permutace $\beta \circ \alpha$ (čti „beta po alfa“) je složené zobrazení, ve kterém nejprve zobrazíme prvky množiny $[1, 5]$ v zobrazení α a výsledné hodnoty dále zobrazíme v zobrazení β (Obrázek 0.12.).

Dostaneme složenou permutaci $\beta \circ \alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 3 & 4 & 5 \end{pmatrix}$.

Při sestavování složené permutace $\alpha \circ \beta$ dostaneme $\alpha \circ \beta = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 5 & 3 & 4 & 2 \end{pmatrix}$, neboť

$$\begin{aligned} \alpha \circ \beta(1) &= \alpha(\beta(1)) = \alpha(3) = 1 \\ \alpha \circ \beta(2) &= \alpha(\beta(2)) = \alpha(2) = 5 \\ \alpha \circ \beta(3) &= \alpha(\beta(3)) = \alpha(5) = 3 \\ \alpha \circ \beta(4) &= \alpha(\beta(4)) = \alpha(4) = 4 \\ \alpha \circ \beta(5) &= \alpha(\beta(5)) = \alpha(1) = 2. \end{aligned}$$

Všimnete si, že $\beta \circ \alpha \neq \alpha \circ \beta$. ✓

Skládání všech zobrazení je podle Lemmatu 0.11. asociativní, tedy i skládání permutací je asociativní. Skládání permutací však není komutativní, jak ukazuje i Příklad 0.9. V Kapitole 7. ukážeme, že permutace společně s operací skládání zobrazení tvoří zajímavou a důležitou strukturu.

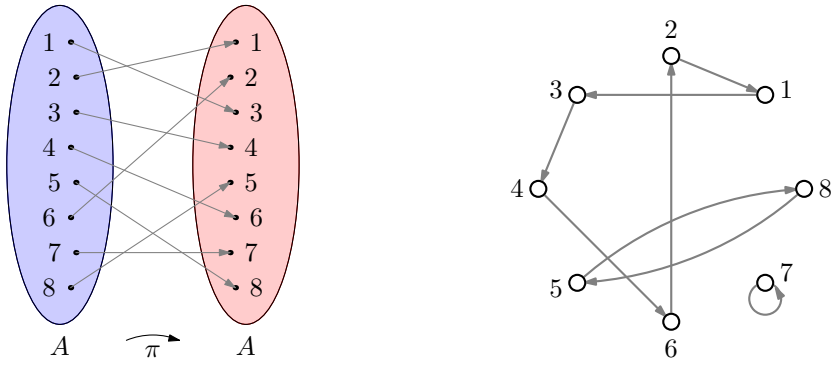
Popis permutací pomocí cyklů

Permutaci může být šikovné zapsat i pomocí tzv. cyklů. Zvolíme libovolný prvek $a \in A$ (jestliže pracujeme s čísly, tak bez újmy na obecnosti lze zvolit nejmenší nepoužitý prvek), zapíšeme jej do závorky a za něj zapíšeme postupně jeho obraz $\pi(a)$, potom obraz tohoto obrazu $\pi(\pi(a))$, atd. Protože zobrazení π je bijekce konečné množiny na sebe, tak dříve nebo později se nějaký prvek zopakuje a není těžké si uvědomit, že nejdříve se zopakuje právě prvek a, proč? Tento opakující se prvek již nezapisujeme a uzavřeme závorku, čímž uzavíráme cyklus permutace. Jestliže v zápisu ještě nejsou obsaženy všechny prvky množiny A, tak zapíšeme další cyklus: otevřeme závorku nového cyklu, zvolíme další nový prvek množiny A (bez újmy na obecnosti například nejmenší nepoužitý prvek dle nějakého klíče) a zapíšeme jej postupně s jeho obrazy jako v předchozím cyklu. Opět je snadné si uvědomit, že se žádný prvek z předchozích cyklů nemůže zopakovat, neboť zobrazení π je bijekce a každý prvek je obrazem právě jednoho prvku z A. Po konečném počtu kroků budou zapsány v cyklech všechny prvky množiny A a zápis permutace π je hotov.

Příklad 0.10. Zapište permutaci $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 1 & 4 & 6 & 8 & 2 & 7 & 5 \end{pmatrix}$ pomocí cyklů.

Při zapisování pomocí cyklů zvolíme první prvek libovolně. Například nejmenší prvek 1. Za ni zapíšeme postupně obrazy $\pi(1) = 3$, $\pi(3) = 4$, $\pi(4) = 6$, $\pi(6) = 2$. Protože $\pi(2) = 1$, tak uzavřeme cyklus a zvolíme další prvek pro zápis dalšího cyklu, například nejmenší nepoužitý prvek 5. Platí $\pi(5) = 8$, a protože $\pi(8) = 5$, cyklus uzavřeme. Konečně, poslední triviální cyklus obsahuje číslo 7. Dostaneme permutaci zapsanou pomocí cyklů.

$$\pi = (1\ 3\ 4\ 6\ 2)(5\ 8)(7)$$



Obrázek 0.13.: *Znázornění cyklů permutace π.*

Na Obrázku 0.13. vlevo je znázorněna permutace π jako zobrazení z množiny A do množiny A. Vpravo je pak znázorněna jako zobrazení na množině A, přičemž jsou pěkně vidět jednotlivé cykly. ✓

Ani zápis permutací pomocí cyklů nemusí být jednoznačný. Každý cyklus s k prvky můžeme zapsat k různými způsoby, neboť zápis cyklu můžeme začít od libovolného prvku cyklu. Navíc může být libovolné i pořadí cyklů. Přesto různé zápisy mohou určovat stejnou permutaci. Například permutaci π z Příkladu 0.10. můžeme zapsat 60 různými způsoby: cyklus délky 5 můžeme zapsat pěti způsoby, cyklus délky 2 dvěma způsoby a pořadí cyklů můžeme zvolit $P(3) = 3! = 6$ způsoby. Výběry možností jsou nezávislé, proto celkový počet možností je $5 \cdot 2 \cdot 6 = 60$.

Příklad 0.11. Zapište permutaci π z Příkladu 0.10. pomocí cyklů alespoň čtyřmi různými způsoby.

Permutaci π můžeme pomocí cyklů zapsat například takto

$$\pi = (1\ 3\ 4\ 6\ 2)(5\ 8)(7) = (5\ 8)(1\ 3\ 4\ 6\ 2)(7) = (8\ 5)(1\ 3\ 4\ 6\ 2)(7) = (7)(8\ 5)(4\ 6\ 2\ 1\ 3).$$

Všechny zápisy popisují stejnou permutaci π, neboť $\pi(1) = 3$, $\pi(2) = 1$, $\pi(3) = 4$, $\pi(4) = 6$, $\alpha(5) = 8$, $\pi(6) = 2$, $\pi(7) = 7$ a $\alpha(8) = 5$. ✓

Z praktických důvodů budeme upřednostňovat zápis, kde každý cyklus začneme sestavovat od „nejmenšího“ prvku v nějakém pevně zvoleném úplném uspořádání prvků. Pokud pracujeme s číselnými množinami $[1, n]$, tak první cyklus začneme sestavovat od prvku 1, případný druhý cyklus od nejmenšího čísla, které se nevyskytuje v prvním cyklu, atd.

Skládání permutací zapsaných pomocí cyklů

Abychom mohli permutace skládat, není potřeba permutace přepisovat do zápisu pomocí matic. Stačí pečlivě a ve správném pořadí číst permutace zapsané pomocí cyklů.

Příklad 0.12. Mějme permutace $\pi = (1\ 3\ 4\ 6\ 2)(5\ 8)(7)$ a $\sigma = (1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$. Sestavíme obě složené permutace $\sigma \circ \pi$ i $\pi \circ \sigma$.

Při skládání permutací můžeme začít nový cyklus od libovolného prvku, dle výše zmíněné úmluvy začneme od nejmenšího nepoužitého prvku a z množiny $[1, 8]$. Čteme od nejvíce pravého cyklu a postupujeme doleva. Hledáme, jaký je obraz prvku b prvku a. Jestliže obraz b určíme, tak stále pokračujeme ve čtení cyklů dále doleva a hledáme případný obraz prvku b. Pokud v cyklech nalevo od prvku b takový obraz již není, našli jsme obraz b prvku a. Pokud v cyklech nalevo od prvku b najdeme obraz c prvku b, znamená to, že ve složené permutaci se prvek a zobrazí na c, případně na další obrazy prvku c, které najdeme v dalších cyklech nalevo od obrazu c. Výsledný obraz zapíšeme jako obraz prvku a a v dalším průchodu budeme postupovat analogicky.

$$\sigma \circ \pi = (1\ 3\ 5\ 7)(2\ 4\ 6\ 8) \circ (1\ 3\ 4\ 6\ 2)(5\ 8)(7) = (1\ 5\ 2\ 3\ 6\ 4\ 8\ 7).$$

Při sestavení druhé složené permutace $\pi \circ \sigma$ postupujeme stejně.

$$\pi \circ \sigma = (1\ 3\ 4\ 6\ 2)(5\ 8)(7) \circ (1\ 3\ 5\ 7)(2\ 4\ 6\ 8) = (1\ 4\ 2\ 6\ 5\ 7\ 3\ 8).$$

✓

Cvičení

0.5.1. Zapište permutaci $\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 5 & 7 & 1 & 4 & 6 & 8 & 3 \end{pmatrix}$ *pomocí cyklů.*

0.5.2. Mějme permutaci $\sigma = (1\ 3\ 5\ 7)(2\ 4\ 6\ 8)$. *Sestavte složené permutace a)* $\sigma \circ \sigma$, *b)* $\sigma \circ \sigma \circ \sigma$, *c)* $\sigma \circ \sigma \circ \sigma \circ \sigma$, *d)* $\sigma \circ \sigma \circ \sigma \circ \sigma \circ \sigma$.

0.5.3. Najděte dvě různé permutace π, σ *a různé od identické permutace* ε *na množině* $\{1, 2, 3\}$, *které komutují, tj. platí* $\pi \circ \sigma = \sigma \circ \pi$.

0.6. Operace na množině

Operace chápeme jako „počítání“ s čísly. Obecněji však můžeme „operovat“ s jakýmikoliv prvky: pro každou dvojici prvků určíme výsledný prvek operace, který může záviset i na pořadí operovaných prvků, například při odečítání. Operace se může týkat i jiného počtu prvků.

Definice Binární operace na množině
Mějme množinu A. *Binární operací* na množině A nazveme každé zobrazení $\circ : A \times A \to A$. *Hodnotu* zobrazení $\circ((a, b))$ nebo *výsledek operace* budeme zapisovat $a \circ b$. Prvky a, b jsou *operandy*.

Uvědomte si, že označení $a \circ b = \circ((a, b))$ pro hodnotu operace má smysl pouze proto, že hodnota je podle definice zobrazení určena jednoznačně.

Pojem binární relace můžeme zobecnit: zobrazení „$\circ$“ definované následujícím způsobem

(i) $\circ : A \to A$ je *unární* operace na množině A,
(ii) $\circ : A \times A \to A$ je *binární* operace na množině A,
(iii) $\circ : A \times A \times A \to A$ je *ternární* operace na množině A,
(iv) $\circ : \underbrace{A \times A \times \cdots \times A}_{n} \to A$ je *n-ární* operace na množině A.

Binární operace dobře známe. Příkladem ternární operace na $\mathbb{R}$ může být aritmetický průměr tří hodnot. Opačné číslo, které každému číslu $x \in \mathbb{R}$ přiřadí číslo $-x$, můžeme chápat jako unární operaci na $\mathbb{R}$.

Na straně 8 jsme zavedli relace na množině i relace mezi množinami. Nyní jsme zavedli operaci na množině. Bylo by možno zavést operaci mezi množinami, například vztah „patřit do podmnožiny M množiny A“ můžeme chápat jako unární operaci mezi množinami A a $\{patří, nepatří\}$, která přiřazuje výsledek operace v množině $\{patří, nepatří\}$. V tomto předmětu se však operacemi mezi množinami zabývat nebudeme.

Příklad 0.13. Rozhodněte, zda následující příklady „operací“ jsou binární operace na dané množině A.

(i) Operace „obvyklého násobení“ na množině $A = \mathbb{R}$.
(ii) Operace „obvyklého násobení“ na množině $A = \mathbb{I} = \mathbb{R} \setminus \mathbb{Q}$.
(iii) Operace „obvyklého sčítání“ na množině $A = \mathbb{L}$ (množina lichých celých čísel).
(iv) Operace „obvyklého odčítání“ na množině $A = \mathbb{N}$.
(v) Operace „obvyklého násobení“ na množině $A = \mathbb{L}$.
(vi) Operace „obvyklého sčítání“ na množině $A = \mathbb{S}$ (množina sudých celých čísel).
(vii) Operace „obvyklého násobení“ na množině $A = \mathbb{S}$.
(viii) Operace „druhé mocniny“ na množině $A = \mathbb{N}$.

Každý příklad rozebereme samostatně. Ověříme, zda se jedná o zobrazení $A^n \to A$ pro nějaké přirozené číslo n.

(i) Dá se ukázat, že součin libovolných dvou reálných čísel je opět reálné číslo. Proto obvyklé násobení na množině $\mathbb{R}$ je binární operace.
(ii) Obvyklé násobení na množině $A = \mathbb{I} = (\mathbb{R} \setminus \mathbb{Q})$ operací není, protože například $\sqrt{2} \cdot \sqrt{2} = 2$, ale 2 (výsledek operace dvou čísel z množiny A) nepatří do množiny A. Je porušena vlastnost, které budeme říkat „uzavřenost operace“ na nosné množině. Operace by nebyla uzavřená.
(iii) Obvyklé sčítání na množině $\mathbb{L}$ není operace, protože například $1 + 1 = 2$ a $2 \notin \mathbb{L}$. Operace by nebyla uzavřená.
(iv) Obvyklé odčítání na množině $\mathbb{N}$ není operace, protože například $1 - 2 = 1$ a $-1 \notin \mathbb{L}$. Operace by nebyla uzavřená.
(v) Obvyklé násobení na množině $\mathbb{L}$ je binární operace, protože součin dvou lichých čísel je opět liché číslo.
(vi) Obvyklé sčítání na množině $\mathbb{S}$ je binární operace, protože součet dvou sudých čísel je opět sudé číslo.
(vii) Obvyklé násobení na množině $\mathbb{S}$ je binární operace, protože součin dvou sudých čísel je opět sudé číslo.

(viii) Druhá mocnina přirozeného čísla je vždy přirozené číslo, ale nejedná se o binární operaci, protože druhá mocnina není binární, ale unární operace.

Jestliže jsme našli obraz prvku z A^n, který nepatřil do množiny A, tak se o operaci nejedná. ✓

Základní typy operací

Počet všech operací i na malé množině je ohromné množství, podobně jako existuje příliš mnoho zobrazení mezi dvěma množinami, než abychom je zkoumali obecně všechny. Má smysl se omezit pouze na operace, které mají některé „pěkné“ a „přirozené“ vlastnosti.

Definice Komutativní operace

Operace „$\circ$“ na množně A se nazývá *komutativní*, jestliže

$$\forall a, b \in A : a \circ b = b \circ a,$$

tj .výsledek operace nezávisí na pořadí operandů.

Typickým příkladem komutativní operace je sčítání nebo násobení přirozených čísel. Typické příklady operace, které *nejsou* komutativní jsou odčítání přirozených čísel, násobení (čtvercových) matic nebo skládání symetrií rovnostranného trojúhelníka (Příklad 1.1.).

Definice Asociativní operace

Operace „$\circ$“ na množně A se nazývá *asociativní*, jestliže

$$\forall a, b, c \in A : (a \circ b) \circ c = a \circ (b \circ c),$$

tj. výsledek postupné operace tří operandů nezávisí na pořadí uzávorkování.

Řada operací je asociativní a obvykle tuto vlastnost považujeme za samozřejmou: sčítání, násobení přirozených čísel i násobení (čtvercových) matic. Ale třeba odečítání přirozených čísel *není* asociativní. Například

$$(3 - 2) - 1 = 0 \neq 2 = 3 - (2 - 1).$$

Protože složením dvou permutací množiny A dostaneme opět permutaci množiny A, tak skládání permutací množiny A můžeme chápat jako operaci na množině permutací množiny A. Na straně 12 jsme ukázali, že tato operace je asociativní. Není těžké si rozmyslet, že skládání permutací není komutativní operace.

Definice Distributivní operace

Mějme množinu A se dvěma operacemi „$+$“, „$\cdot$“. Řekneme, že operace „$\cdot$“ je na množně A (zleva) *distributivní* vzhledem k operaci „$+$“, jestliže

$$\forall a, b, c \in A : a \cdot (b + c) = (a \cdot b) + (a \cdot c),$$

Podobně operace „$\cdot$“ je na množně A zprava *distributivní* vzhledem k operaci „$+$“, jestliže

$$\forall a, b, c \in A : (b + c) \cdot a = (b \cdot a) + (c \cdot a).$$

Klasické násobení přirozených čísel je zleva i zprava distributivní vhledem ke sčítání. Naproti tomu sčítání přirozených čísel *není* distributivní vzhledem k násobení, například $3+(5\cdot 2) \neq (3+5)\cdot(3+2)$. Pro libovolné tři množiny A, B, C platí $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$ a také $A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$.

Chápeme-li sjednocení a průnik množin jako operace na sytému množin, tak průnik množin je distributivní vzhledem ke sjednocení množin a současně sjednocení množin je distributivní vzhledem k průniku množin.

Je-li operace „$\cdot$“ komutativní a zleva distributivní, tak musí být současně zprava distributivní a naopak. Je-li však operace současně zleva i zprava distributivní, tak *nemusí* být komutativní. Například vektorový součin vektorů v $\mathbb{R}^3$ je zleva i zprava distributivní, avšak není komutativní.

Restrikce operací

Víme, že výsledky početních operací sčítání, násobení, odčítání s celými čísly vychází stejně, ať už počítáme v oboru celých, racionálních, reálných nebo komplexních čísel. Operace jsou tak zavedeny. Toto pozorování můžeme zobecnit. Zavedeme restrikci operace „$\circ$“ na množině A na její podmnožinu C podobně, jako jsme na straně 12 zavedli restrikci zobrazení. Operace „$\circ_r$“ na množině C bude definována tak, že pro každé dva

Obrázek 0.14.: *Restrikce operace musí zachovat uzavřenost operace.*

prvky a, b v podmnožině C bude výsledek operace „$\circ\!\!\restriction$“ stejný, jako by byl výsledek operace „$\circ$“ na množině A. Symbolicky

$$\forall a, b \in C \subseteq A : a \circ\!\!\restriction b = a \circ b$$

Pozor, ne pro každou podmnožinu C množiny A bude výsledná restrikce operací. Aby restrikce operace byla operací, musí být uzavřená. Restrikce operace „$\circ$“ na množinu C na Obrázku 0.14. je uzavřená, zatímco restrikce operace „$\circ$“ na množinu D uzavřená není. Naproti tomu komutativita operace „$\circ$“ a asociativita operace „$\circ$“ se při restrikci na (uzavřenou) operaci „$\circ\!\!\restriction$“ zachová, říkáme, že se komutativita „zdědí z operace $\circ$“.

Otázka: Kolik existuje různých operací na n-prvkové množině?

O zadávání operací

Každý zná operace obvyklého sčítání a násobení. Jejich komutativitu a asociativitu považujeme za samozřejmé. Uvědomte si ale, že tato znalost obvykle vychází ze zkušenosti, nikoli z formálního důkazu.

Korektní zavedení a popis klasických operací spadá do předmětu teoretická aritmetika. V tomto textu jen upozorníme, že výsledky operací jsou dány početními pravidly, které jsme se naučili na základní škole a které budeme dále považovat za axiomy.

V dalším textu budeme zavádět operace nové. Popisovat je můžeme několika způsoby:

Předpisem Máme-li množinu čísel M, můžeme operaci na množině M popsat předpisem, sestaveným z klasických operací tak, aby výsledná hodnota opět patřila do M. Například pro libovolnou dvojici celých čísel $(a, b) \in \mathbb{Z}^2$ můžeme definovat operaci φ danou předpisem $\varphi(a, b) = 2a^2 + b$. Výsledek je vždy celé číslo a jedná se o operaci $\varphi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

Tabulkou Pro (malé) konečné množiny M můžeme výsledek operace $M \times M \to M$ popsat tabulkou, která přehledně popisuje výsledky operací pro každou dvojici operandů V záhlaví, tj. v prvním sloupci a prvním řádku, jsou uvedeny všechny prvky konečné množiny. První (levý) operand určuje řádek tabulky, druhý (pravý) operand určí sloupec tabulky, kam vepíšeme výsledek operace. Této tabulce se říká *Cayleyho tabulka*.

U komutativních operací nehraje pořadí operandů roli, tabulka bude symetrická podle hlavní diagonály. Pro nekomutativní operace Cayleyho tabulka symetrická nebude.

S Cayleyho tabulkami začneme pracovat v sekci 0.7.

Popisem symetrií Operace můžeme sestavovat i pro množiny symetrií. Symetrií rozumíme proces, kdy manipulujeme s nějakým objektem tak, abychom před i po manipulaci dostali „shodný“ objekt. Symetriím se podrobně věnujeme v Kapitole 1.

Příklad 0.14. Operace zadané předpisem

Libovolnou funkci dvou proměnných $f_i : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$, která je definována pro libovolnou dvojici reálných čísel můžeme chápat jako operaci.

Například $f_1(x, y) = x \cdot y$, $f_2(x, y) = 2x + 3y$ nebo $f_3(x, y) = x^2 + \frac{2x}{y^2+1}$ můžeme chápat jako operace zadané předpisem $x \circ_1 y = x \cdot y$, $x \circ_2 y = 2x + 3y$ nebo $x \circ_3 y = x^2 + \frac{2x}{y^2+1}$. ✓

Příklad 0.15. Operace zadané tabulkou

Logické spojky, které z jednoduchých výroků dělají výroky složené můžeme chápat jako operace na množině pravdivostních hodnot.

Například Tabulky 0.2. ukazují konjunkci $\wedge$ a disjunkci $\vee$ zapsané jako operace v Cayleyho tabulce.

$\wedge$	T	F
T	T	F
F	F	F

$\vee$	T	F
T	T	T
F	T	F

Tabulka 0.2.: *Tabulka logické operace konjunkce $\wedge$ a disjunkce $\vee$.*

✓

Příklad 0.16. Operace dané popisem symetrií
Značka kruhového objezdu má tři možné symetrie, které můžeme skládat:

(i) identitu označíme I,
(ii) otočení o 120 stupňů, které označíme R_{120}, a
(iii) otoční o 240 stupňů, které označíme R_{240}.

Obrázek 0.15.: *Dopravní značka upozorňující na kruhový objezd.*

Příslušnou operaci skládání pak můžeme popsat Tabulkou 0.X3., která ukazuje výsledky složení jednotlivých symetrií. ✓

$\Leftrightarrow$	I	R_{120}	R_{240}
I	I	R_{120}	R_{240}
R_{120}	R_{120}	R_{240}	I
R_{240}	R_{240}	I	R_{120}

Tabulka 0.X3.: *Tabulka skládání symetrií značky kruhového objezdu.*

Souvislost pojmů relace, zobrazení a operace
Jak spolu souvisí pojmy relace, zobrazení a operace?

Relaci R na množině A jsme nadefinovali jako $R \subseteq A \times A$, jedná se o množinu uspořádaných dvojic prvků z A. Relaci R mezi množinami A, B jsme nadefinovali jako $R \subseteq A \times B$, jedná se o množinu uspořádaných dvojic prvků s první složkou z A a druhou složkou z B.

Zobrazení $\varphi : A \to B$ chápeme jako speciální případ relace mezi množinami A a B, kde A je množina *vzorů* a B je množina *obrazů* v zobrazení φ. Jedná se o takovou relaci $\varphi \subseteq A \times B$, kde ke každému prvku v množině A najdeme právě jednu uspořádanou dvojici (x, y) v relaci φ. Pro každé $x \in A$ je pak druhý prvek $y \in B$ v této uspořádané dvojici (x, y) určen jednoznačně, a tak můžeme psát $y = \varphi(x)$. každé zobrazení $\varphi : A \to B$ je relací mezi A a B, ale ne každá relace mezi A a B je zobrazením.

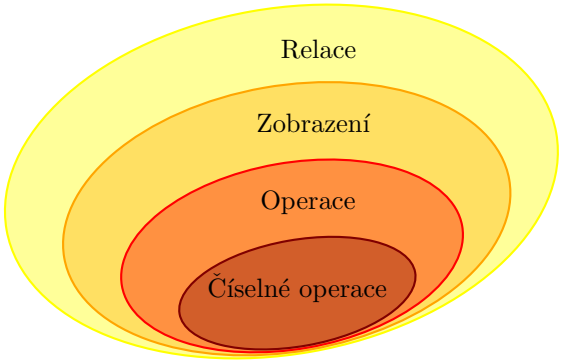
Jsme zvyklí pracovat s číselnými množinami a zobrazením číselných množin říkáme funkce. Například zobrazení $f : A \to B$ pro $A = B \subseteq \mathbb{R}$ nazveme funkcí f. Mluvíme-li o reálné funkci jedné proměnné, tak definičním oborem obvykle chápeme nikoliv celou množinu vzorů A, ale takovou její podmnožinu $D \subseteq A$, pro kterou je funkce definována. Bez dalšího upřesnění za definiční obor bereme dle obecné dohody co největší podmnožinu A, pro kterou má příslušné zobrazení (obvykle dané předpisem funkce) smysl. Podobně oborem hodnot H chápeme podmnožinu takovou $H \subseteq B$, která obsahuje všechny funkční hodnoty, jichž funkce nabývají.

A konečně *operace* na množině A je zobrazení $(A \times A) \to A$. Každé uspořádané dvojici prvků z množiny A přiřadíme nějaký prvek z množiny A.

Každé zobrazení $A \to B$ je speciálním případem relací mezi množinami A a B. Každá operace na množině A je speciálním případem zobrazení $A \times A \to A$. O číselných operacích hovoříme, jestliže množina A je některým z číselných oborů (Obrázek 0.16.).

Příklad 0.17. Uveďme několik klasických příkladů relací, zobrazení a operací na množině.

1) Relace dělitelnosti na množině celých čísel je relací částečného uspořádání na $\mathbb{N}$ a není relací ekvivalence (není symetrická).



Obrázek 0.16.: *Hierarchie relací, funkcí a operací.*

2) Relace kongruence modulo m na množině celých čísel je relací ekvivalence na $\mathbb{Z}$, ale není relací částečného uspořádání (není antisymetrická).
3) Zobrazení $\mathbb{Z} \to \mathbb{Z}$, kdy každému prvku přiřadíme jeho třetí mocninu, je zobrazení s definičním oborem $D = \mathbb{Z}$ a oborem hodnot $H \subset \mathbb{Z}$.
4) Zobrazení $\mathbb{R} \to \mathbb{R}$, kdy každému prvku přiřadíme jeho třetí mocninu, je zobrazení s definičním oborem $D = \mathbb{R}$ a oborem hodnot $H = \mathbb{R}$.
5) Zobrazení $\mathbb{R} \to \mathbb{R}$, kdy každému prvku přiřadíme jeho druhou mocninu, je zobrazení s definičním oborem $D = \mathbb{R}$ a oborem hodnot $H = \mathbb{R}_0^+$
6) Operace sčítání na $\mathbb{N}$ přiřazuje každé dvojici celých čísel jejich součet. Tato operace je komutativní i asociativní.
7) Operace odčítání na $\mathbb{Z}$ přiřazuje každé dvojici celých čísel jejich rozdíl. Tato operace není komutativní.
8) Odčítání na $\mathbb{N}$ není operace, protože pro mnoho dvojic prvků (menšenec, menšitel) není výsledek operace definovaný. Například pro $(2, 5)$ nebo pro $(1, n)$, kde $n \in \mathbb{N}$.
9) Operace násobení na $\mathbb{N}$ přiřazuje každé dvojici celých čísel jejich součin. Tato operace je komutativní i asociativní.
10) Obvyklé dělení na $\mathbb{N}$ není operace, protože pro mnoho dvojic prvků (dělenec,dělitel) není výsledek operace definovaný. Například pro $(1, 2)$ nebo pro $(3n + 1, 3)$, kde $n \in \mathbb{N}$.
11) Obvyklé dělení na $\mathbb{Q}$ není operace, protože pro dvojice prvků (dělenec,dělitel), kde dělitel je 0 není výsledek operace definovaný.
12) Obvyklé dělení na $\mathbb{Q}^+$ je operace, protože podíl dvou kladných racionálních čísel je opět kladné racionální číslo.

V dalších kapitolách ukážeme, že pojem grupy je budován jako zobecnění číselných množin a operací na číselných množinách, tak jak je známe z klasických počtů s celými čísly, nebo reálnými čísly, nebo třeba s maticemi.

Cvičení

0.6.1.$^{\heartsuit}$ *Najděte příklad* různých *množin A, B takových, že výsledek kartézského součinu nezávisí na pořadí $A \times B = B \times A$?*

0.6.2. Pro čísla $n = 5, 12, 23, 24$ najděte všechna přirozená čísla menší než n a nesoudělná s n.

0.6.3. Najděte celá čísla s, t tak, aby $5s + 7t = 1$. Jsou čísla s, t určena jednoznačně?

0.6.4. Najděte nekonečně mnoho zobrazení $f : \mathbb{N} \to \mathbb{N}$, která nejsou ani injektivní, ani surjektivní.

0.6.5. Mějme operaci „$\circ$“ na množině A a operaci „$\circ\prime$“, která je restrikcí „$\circ$“ na množinu C, kde $C \subseteq A$. Ukažte, že restrikce komutativní operace je komutativní operace.

0.6.6. Mějme operaci „$\circ$“ na množině A a operaci „$\circ\prime$“, která je restrikcí „$\circ$“ na množinu C, kde $C \subseteq A$. Ukažte, že restrikce asociativní operace je asociativní operace.

0.6.7. Mějme dvě operace na množině A a jejich restrikce na množinu C, kde $C \subseteq A$: restrikci operace „$+$“ označme „$+\prime$“ a restrikci „$\circ$“ označme „$\cdot\prime$“. Ukažte, že restrikce distributivní (vzhledem k „$+$“) operace je distributivní operace vzhledem k „$+\prime$“.

0.6.8. Zapište Cayleyho tabulky logických operací a) ekvivalence $\Leftrightarrow$, b) implikace $\Rightarrow$, , c) xor $\oplus$.

0.6.9. Zapište Cayleyho tabulky symetrií písmena `W`.

0.6.10. Kolik různých logických operací pro dva operátory lze sestavit?

0.7. Modulární aritmetika

Abychom zavedli analogie známých číselných oborů $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, nebo $\mathbb{R}$ i v případě, že k dispozici bude pouze konečně mnoho číselných hodnot (například byte může nabývat 256 různých hodnot), musíme identifikovat klíčové vlastnosti. Co mají nekonečné a konečné číselné obory společné?

Berme tuto otázku jako motivaci k zavedení pojmu grupy a číselného tělesa. V této kapitole ponecháme počítání s číselnými obory v intuitivní rovině, ukážeme několik příkladů a upozorníme na některé důležité vlastnosti.

Počítání na hodinách

Hodiny „počítáme modulo 24“, protože nerozlišujeme více než 24 hodin během dne. V běžné řeči obvykle rozlišujeme jen 12 hodin. Hodiny uvádíme pouze v intervalu 1 až 12 (případně 0 až 11 nebo 0 až 23). Uvědomte si, že při počítání časových údajů na hodinách existuje pouze konečně mnoho výsledků početních operací! Například řekneme-li v 7 hodin „za čtyři hodiny“, tak mluvíme o čase v 11 hodin. Odkážeme-li se však v 11 hodin na čas „za čtyři hodiny“, tak mluvíme o čase ve 3 hodiny (přičemž z kontextu může, ale nemusí být jasné, zda se jedná o odpoledne nebo hlubokou noc).

Obrázek 0.17.: *Hodiny s čtyřiadvacetihodinovým ciferníkem v Táboře, v Greenwichi, ve Florencii a náramkové polární hodinky.*

Výsledky počítání můžeme popsat Cayleyho tabulkou.

Příklad 0.18. Sestavte Cayleyho tabulku sčítání „modulo 12“ s čísly a) 1 až 12, b) 0 až 11.
Počítání „modulo 12“ s čísly 1 až 12, resp. 0 až 11, shrnou následující Cayleyho tabulky (Tabulky 0.3. a 0.4.). O něco přehlednější je tabulka, která popisuje počítání se zbytky 0 až 11 modulo 12.

Všimněte si, že v Cayleyho tabulce se vždy objevují pouze čísla ze záhlaví, žádná jiná. Tomu říkáme, že operace je *uzavřená*.

Vidíme, že v Tabulce 0.3. má prvek 12 zvláštní postavení. Pro každý prvek $a \in \{1, 2, \ldots, 12\}$ platí $a + 12 = a$, kde na levé straně sčítáme modulo 12. Jedná se o tzv. *neutrální prvek*, který si zavedeme pečlivě až v následující kapitole. V Tabulce 0.4. je tímto prvkem 0.

Při sčítání modulo n se někdy pracuje s čísly 0 až $n-1$, přičemž 0 je neutrálním prvkem a někdy se pracuje s čísly 1 až n, přičemž neutrálním prvkem je n. Všimněte si, že přeznačením prvku 0 v Tabulce 0.4. na prvek 12 a přeuspořádáním sloupců a řádků dostaneme z jedné tabulky druhou (a naopak). ✓

Tabulky 0.3. a 0.4. odpovídají tabulkám operací v konečné grupě, což je pojem, který zavedeme v další kapitole. Analogicky bychom mohli zavést tabulku násobení. Zkuste to sami (Cvičení 0.7.3.).

Operace modulo

V části 0.3. jsme zavedli *relaci* kongruence modulo m. Nyní zavedeme *operaci* kongruence modulo m. To znamená, že budeme pracovat s množinou celých čísel a za výsledek operace (různých operací) místo čísla x vezmeme číslo, které se rovná zbytku po dělení čísla x modulem m. Jinými slovy pro množinu celých čísel $\mathbb{Z}$, případně pro vhodnou podmnožinu $M \subseteq \mathbb{Z}$, za výsledek operace $M \times M \to M$ označíme číslo c z intervalu $[0, m-1]$, pro které platí $c \equiv x \pmod{m}$. Například Tabulka 0.4. popisuje operaci modulo 12.

Protože platí $0 \equiv m \pmod{m}$, někdy se s číslem m při počítání modulo m pracuje jako s nulou. Například na hodinách je počítání s m přirozenější a příslušnou operaci zachycuje tabulka 0.3.

Příklad 0.19. Popišme tabulku operace sčítání „modulo 6“.
Cayleyho tabulka operace sčítání modulo 6 je Tabulka 0.5.

+	1	2	3	4	5	6	7	8	9	10	11	12
1	2	3	4	5	6	7	8	9	10	11	12	1
2	3	4	5	6	7	8	9	10	11	12	1	2
3	4	5	6	7	8	9	10	11	12	1	2	3
4	5	6	7	8	9	10	11	12	1	2	3	4
5	6	7	8	9	10	11	12	1	2	3	4	5
6	7	8	9	10	11	12	1	2	3	4	5	6
7	8	9	10	11	12	1	2	3	4	5	6	7
8	9	10	11	12	1	2	3	4	5	6	7	8
9	10	11	12	1	2	3	4	5	6	7	8	9
10	11	12	1	2	3	4	5	6	7	8	9	10
11	12	1	2	3	4	5	6	7	8	9	10	11
12	1	2	3	4	5	6	7	8	9	10	11	12

Tabulka 0.3.: *Tabulka sčítání „modulo 12“ s čísly 1 až 12.*

+	0	1	2	3	4	5	6	7	8	9	10	11
0	0	1	2	3	4	5	6	7	8	9	10	11
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	3	4	5	6	7	8	9	10	11	0	1
3	3	4	5	6	7	8	9	10	11	0	1	2
4	4	5	6	7	8	9	10	11	0	1	2	3
5	5	6	7	8	9	10	11	0	1	2	3	4
6	6	7	8	9	10	11	0	1	2	3	4	5
7	7	8	9	10	11	0	1	2	3	4	5	6
8	8	9	10	11	0	1	2	3	4	5	6	7
9	9	10	11	0	1	2	3	4	5	6	7	8
10	10	11	0	1	2	3	4	5	6	7	8	9
11	11	0	1	2	3	4	5	6	7	8	9	10

Tabulka 0.4.: *Tabulka sčítání „modulo 12“ s čísly 0 až 11.*

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

Tabulka 0.5.: *Tabulka sčítání „modulo 6“ s čísly 0 až 5.*

Všimněte si, že v Cayleyho tabulce se vždy objevují pouze čísla ze záhlaví, žádná jiná. Tomu říkáme, že operace je uzavřená.

Dále si v Tabule 0.5. všimneme, že v řádku i sloupci značeném 0 je kopie záhlaví. Říkáme, že 0 je neutrálním prvkem operace.

A konečně si všimneme, že v každém řádku i každém sloupci se nachází neutrální prvek 0. Například v řádku 2 a sloupci 4 je 0, což znamená, že $2 + 4 = 0$ a podobně $4 + 2 = 0$. Říkáme, že číslo 4 je inverzní k číslu 2, tj. místo přičtení $x + 2$ můžeme kdykoliv odečíst $x - 4$ a dostaneme stejný výsledek. Například $3 + 2 = 5 = 4 - 4$.

Ověření asociativity operace sčítání modulo 6 je zdlouhavé. Museli bychom ověřit, že pro libovolnou trojici čísel $x, y, z \in [0, 5]$ platí $x + (y + z) = (x + y) + z$. Například $4 + (3 + 5) = 4 + 2 = 0$ a současně $(4 + 3) + 5 = 1 + 5 = 0$. Takových trojic je $6^3 = 218$, stejně bychom ověřili zbývajících 217 trojic. ✓

Příklad 0.20. Popišme tabulku operace násobení „modulo 6“.

·	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	2	4
5	0	5	4	3	4	1

Tabulka 0.6.: *Tabulka násobení „modulo 6“ s čísly 0 až 5.*

Opět budeme počítat pouze s čísly 0, 1, 2, 3, 4 a 5.

Všimněte si, že na rozdíl od Tabulek 0.3. a 0.4. není v Tabulce 0.6. každé číslo ve stejném počtu kopií. Toto pozorování bude hrát roli později při zavedení pojmu grupy (na straně 50).

Všimněte si, že v Cayleyho tabulce se vždy objevují pouze čísla ze záhlaví, žádná jiná a operace je proto uzavřená.

Při podrobnějším zkoumání tabulky vidíme, že operace násobení modulo 6 má neutrální prvek 1, neboť sloupec i řádek 1 je kopií záhlaví. Pro každý prvek $x \in [1,6]$ tedy platí $x \cdot 1 = 1 \cdot x = x$. Tato operace však obecně *nemá* inverzní prvky. Neutrální prvek v řadě sloupců (i řádků) chybí, a proto například $2 \cdot x \neq 1$ pro každý prvek $x \in [1,6]$. K prvku 2 proto neexistuje prvek inverzní. ✓

Cvičení

0.7.1. Sestavte Cayleyho tabulku operace sčítání modulo 5. Ověřte vlastnosti: uzavřenost, existenci neutrálního prvku, existenci inverzního prvku ke každému prvku.

0.7.2. Sestavte Cayleyho tabulku operace násobení modulo 5. Ověřte vlastnosti: uzavřenost, existenci neutrálního prvku, existenci inverzního prvku ke každému prvku.

0.7.3. Sestavte Cayleyho tabulku operace násobení modulo 12. Ověřte vlastnosti: uzavřenost, existenci neutrálního prvku, existenci inverzního prvku ke každému prvku.

0.7.4. Sestavte Cayleyho tabulku operace sčítání a) „modulo 2“, b) „modulo 3“. Při počítání vystačíme pouze s čísly 0, 1, respektive s čísly 0, 1, 2. Říká se, že budeme počítat se zbytkovými třídami, kde třída obsahuje vždy všechna větší či menší celá čísla, která jsou s uvedeným reprezentantem zbytkové třídy kongruentní dle příslušného modulu.

0.7.5. Mějme přirozené číslo n. Ukažte, že součet tří po sobě jdoucích mocnin n^3, $(n+1)^3$ a $(n+2)^3$ je dělitelný devíti.

0.7.6. Platné rodné číslo (až na několik tisíc výjimek) musí být dělitelné 11. Z rodného čísla 63?1225673 vypadla jedna cifra. Určete chybějící cifru. Patří rodné číslo Hynkovi nebo Jarmile?

0.7.7. Jakých hodnot může nabývat poslední znak x rodného čísla $140210850x$?

0.7.8. Určete, kolik existuje rodných čísel tvaru a) ??02291111, b) 02??291111, c) 0229??1111.

0.7.9. V knize „Stopařův průvodce po galaxii“ píše Douglas Adams, že odpověď na fundamentální otázku života Vesmíru a vůbec je 42. V navazující knize se ukáže, že se se jedná o odpověď na otázku „Kolik je 6 krát 9?“ Za jakých předpokladů je tato odpověď správná?

0.8. Důkazové techniky

Matematika, ale i jiné moderní vědní disciplíny se vyznačují svou exaktností. Rozumíme tím schopnost odvodit či doložit pravdivost předkládaných tvrzení, tj. zdůvodnit, proč jisté předpoklady garantují splnění nějakého tvrzení. V moderní matematice je pojem matematického důkazu pečlivě formalizován.

V matematické logice podléhá formulace tvrzení i důkazů přísným pravidlům, včetně použité abecedy, syntaxe, tzv. primitivních pojmů, axiomů a logických kroků. Při formulaci tvrzení a jejich dokazování v matematice zpravidla vystačíme s běžným jazykem. Někdy se tak dopouštíme jistých nepřesností, zejména s víceznačností některých formulací. V tomto textu se snažíme o pečlivé formulace, využíváme ustálené slovní obraty a formulace tak, aby text byl korektní a současně srozumitelný.

Historický vývoj důkazu sahá hluboko do minulosti. K nejznámějším historicky doloženým důkazům patří různé převážně grafické důkazy Pythagorovy věty. Zatímco tvrzení samotné najdeme na Babylonské tabulce z doby cca. 1900–1600 př.n.l., nebo na „Rhindově Papyru“ z Egypta 1788–1580 př.n.l., tak důkaz je přisuzován tzv. Pythagorejské škole (560–480 př.n.l.) a nezávisle také v Číně cca. 500–200 před n.l.

V moderní matematice je matematický důkaz chápán jako posloupnost elementárních ověřitelných kroků vedoucích od známých nebo předpokládaných tvrzení k novému dokazovanému tvrzení. Sytém axiomů se liší dle použité teorie. Zatímco v geometrii se jedná zpravidla o pět Euklidových axiomů, tak v diskrétní matematice (i teorii grafů) se jedná o tzv. Peanovy axiomy. Protože řada myšlenek zasahuje i do dalších matematických disciplin, pracujeme s pojmy a tvrzeními spadajícími například do teorie množin nebo aritmetiky.

V dalším textu připomeneme hlavní myšlenku matematického důkazu i nejběžnější důkazové techniky.

Výrok a výroková forma

Výrokem je takové tvrzení, kterému má smysl přiřadit pravdivostní hodnotu pravda („true“ či 1) nebo nepravda („false“ či 0). Z jednoduchých výroků můžeme sestavovat složené výroky pomocí logických spojek. Mezi nejčastější logické spojky patří *konjunkce* „a současně“, *disjunkce* „nebo“ a unární logický operátor *negace* „není pravda že“. V tomto textu konjunkci značíme „$\wedge$“, disjunkci „$\vee$“ a negaci „$\neg$“.

Další často používanou spojkou je *implikace*, která se používá jednak při formulaci tvrzení vět, kdy tvrzení věty je splněno jen za určitých předpokladů, tak při odvozování a sestavování důkazů tvrzení. V tomto textu implikaci značíme „$\Rightarrow$“ a ekvivalenci „$\Leftrightarrow$“. *Ekvivalence* nám umožní sestavit složený výrok, který říká, že oba výroky mají stejnou pravdivostní hodnotu. Tvrzení ve tvaru ekvivalence mají často hluboký význam, neboť ukazují, jak jeden problém formulovat či dokonce řešit v kontextu jiné úlohy a naopak.

Výroková forma je tvrzení, které obsahuje jakousi výrokovou proměnnou. Výroková forma není výrokem sama o sobě, výrok dostaneme například dosazením konkrétní hodnoty za výrokovou proměnnou. V běžné řeči rozdíl mezi výrokem a výrokovou formou snadno přehlédneme, což bývá zdrojem chyb a zdánlivých paradoxů. Například často uváděný příklad „dnes je pěkně“ není výrokem, neboť pravdivost tvrzení závisí na konkrétním datu nebo místě, kde jeho platnost posuzujeme. Tato výroková forma vyslovená v určitou chvíli může mít jinou pravdivostní hodnotu na různých místech. Napsané tvrzení snadno změní pravdivostní hodnotu podle toho, kdy výrok čteme.

Takovým nepřesně vyjádřeným tvrzením se v matematice snažíme vyhnout pečlivou formulací. Míra podrobnosti formulace závisí na kontextu a očekávaném čtenáři.

Ukažme si rozdíl výroku a výrokové formy na dalším příkladu. Bez dalšího kontextu je

$$x \geq 0$$

výrokovou formou. Nemá smysl rozhodovat o pravdivosti nebo nepravdivosti tvrzení, že x je nezáporné číslo. Často se však zápis $x \geq 0$ objeví na konci výpočetního postupu. Pak chápeme zápis $x \geq 0$ jako součást složeného výroku „jestliže reálné číslo x je řešení nerovnice, tak $x \geq 0$“, případně „řešením nerovnice jsou všechna reálná čísla, pro která platí $x \geq 0$“. Zatímco bez kontextu se o výrok nejedná, tak po zasazení do obvyklého, byť nevysloveného kontextu se o výrok jedná.

Kvantifikátory

Z výrokové formy může získat výrok, aniž bychom dosazovali konkrétní hodnotu výrokové proměnné, a sice použitím kvantifikátoru. *Kvantifikátor* je proto důležitý nástroj, pomocí kterého lze sestavit výroky, které zpravidla mají významnou vypovídací hodnotou. Nejběžnější kvantifikátory jsou univerzální (všeobecný) kvantifikátor a existenční kvantifikátor.

Univerzální kvantifikátor „pro každý prvek x dané množiny M“ značíme $\forall x \in M$. Symbol pochází z prvního písmene anglického slova „all“. Použitím univerzálního kvantifikátoru říkáme, že z výrokové formy dostaneme pravdivý výrok bez ohledu na to, který prvek množiny M zvolíme a do výrokové formy dosadíme. Takový výrok zpravidla říká, že máme množinu řešení nějaké úlohy.

Existenční kvantifikátor čteme „existuje prvek x dané množiny M“ a značíme $\exists x \in M$. Symbol pochází z prvního písmene anglického slova „exist“. Použitím existenčního kvantifikátoru říkáme, že v dané množině existuje alespoň jeden prvek (jeden nebo více prvků), jehož dosazením dostane z výrokové formy pravdivý výrok. Výrok s použitím existenčního kvantifikátoru zpravidla říká, že nějaká úloha má řešení.

Někdy se používá ještě kvantifikátor jednoznačné existence „existuje právě jeden prvek x dané množiny M“, značíme jej $\exists! x \in M$. Použitím kvantifikátoru jednoznačné existence říkáme, že v dané množině existuje jediný prvek, jehož dosazením dostane z výrokové formy pravdivý výrok. Takový výrok zpravidla říká, že nějaká úloha má řešení a toto řešení je určeno jednoznačně.

Ještě připomeneme, že negací výroku s existenčním kvantifikátorem je výrok se všeobecným (v jistém smyslu opačným) kvantifikátorem a negací výrokové formy. Jestliže $P(x)$ je výroková forma, tak negace kvantifikovaných výroků můžeme obecně zapsat:

$$\neg\left(\forall x \in m : P(x)\right) = \exists x \in M : \neg P(x)$$
$$\neg\left(\exists x \in m : P(x)\right) = \forall x \in M : \neg P(x).$$

Abychom mohli popsat nejběžnější důkazové techniky, podívejme se nejprve na obvyklou strukturu dokazovaných tvrzení.

Struktura tvrzení

Matematická tvrzení mají zpravidla tvar implikace $P \Rightarrow T$, kde P je *předpoklad* a T je samotné *tvrzení*. Předpokladu říkáme také *postačující podmínka* implikace a tvrzení je *nutná podmínka* implikace.

Předpoklad může být i nevyslovený, jestliže vyplývá z kontextu. Při sestavování důkazu však s předpokladem zpravidla pracujeme a musíme z kontextu poznat, jaký předpoklad je. Říká-li věta například „Každý pravidelný graf sudého stupně s alespoň jednou hranou má 2-faktor“, tak tvrzení můžeme přirozeně přeformulovat do tvaru implikace „Jestliže G je pravidelný graf sudého stupně, který má alespoň jednu hranu, potom graf G má 2-faktor.“ Předpoklad věty říká, že máme pravidelný graf G sudého stupně, který má alespoň jednu hranu. Tvrzení věty říká, že graf G má 2-faktor. Jestliže věta platí, tak existence 2-faktoru nutně vyplývá ze splnění předpokladu. Naopak, aby platilo tvrzení, stačí aby byl splněn předpoklad.

Většinu důležitých tvrzení formulujeme jako věty. Důsledek věty je takové tvrzení, které snadno vyplyne z již dokázané věty. Důkaz důsledku bývá zpravidla krátký, stačí jeden nebo dva kroky a z tvrzení věty odvodíme tvrzení důsledku. Lemma je pomocné tvrzení, které někdy není zajímavé samo o sobě, ale popisuje nějaký obrat nebo vlastnost, která usnadní konstrukci či důkaz jiné věty.

Ne každé tvrzení však umíme dokázat. Tvrzení, o kterém máme důvod předpokládat, že je pravdivé, ale není znám jeho důkaz, se nazývá *hypotéza*. Jakmile se tvrzení podaří dokázat, stane se z hypotézy věta. Bohužel nemůžeme čekat, že všechna tvrzení se podaří dokázat. Kurt Gödel v roce 1931 ukázal, že axiomatická výstavba teorie má své limity. V každé dostatečně bohaté teorii je možné formulovat tvrzení, tzv. „nerozhodnutelná tvrzení“, která v rámci teorie není možné dokázat, ani vyvrátit.

Struktura důkazu

Důkaz tvrzení je posloupnost kroků, které na sebe logicky navazují, každý krok vyplývá z předchozích kroků dle pravidel odvozování. Posloupnost kroků obvykle vychází z předpokladu tvrzení, využívá již dokázaná tvrzení a axiomy dané teorie, a postupně odvodí dokazované tvrzení. Sestavení důkazu je tvořivá činnost, autor musí správnou posloupnost kroků objevit. Naproti tomu verifikace důkazu je jednodušší, spočívá v ověření všech jednotlivých kroků důkazu.

Některé typy důkazů mají jistou ustálenou strukturu, která nalezení celého postupu usnadňuje. Typickým příkladem je důkaz matematickou indukcí. Elegantní důkazy naopak využívají nějaký překvapivý obrat nebo pozorování, které usnadní náročný krok důkazu a které přináší radost a pozitivní prožitek i čtenáři. Matematik Paul Erdős o obzvláště elegantních důkazech říkal, že pochází z *Knihy* (anglicky „The Book“), bájné příručky, která obsahuje ty nejelegantnější důkazy všech možných tvrzení. V roce 2003 vyšla kniha „Proofs from THE BOOK“, ve které editoři shromáždili 32 důkazů, které jsou často vnímány jako mimořádně pěkné.

V dalších odstavcích připomeneme několik nejčastějších důkazových technik.

Přímý důkaz

Přímý důkaz je nejjednodušší důkazová technika. Jestliže tvrzení ve tvaru implikace $P \Rightarrow T$ dokazujeme přímo, tak vyjdeme z předpokladu P a za použití pravidel odvozování, axiomů a dříve dokázaných tvrzení odvodíme tvrzení věty T.

Příklad 0.21. Ukážeme, že druhá mocnina lichého celého čísla je liché číslo.
Mějme liché celé číslo n, tj. $n = 2t+1$ pro nějaké $t \in \mathbb{Z}$. Druhá mocnina čísla n je $n^2 = (2t+1)^2 = 4t^2+2t+$ $+1 = 2(2t^2+t)+1$. Protože číslo $2t^2+t$ je jistě celé číslo a $2(2t^2+t)$ je jistě sudé číslo, tak $2(2t^2+t)+1$ je liché celé číslo. ✓

Příklad 0.22. Ukážeme, že rovnice $x^2+4x+6=0$ nemá řešení v množině reálných čísel.
Kvadratický trojčlen upravíme na čtverec. Dostaneme $x^2+4x+5 = x^2+4x+4+1 = (x+2)^2+1$. První sčítanec $(x+2)^2$ je jistě nezáporný a druhý sčítanec je kladný. Proto $x^2+4x+6 > 0$ a rovnice nemá řešení v množině reálných čísel. ✓

Nepřímý důkaz

P	T	$P \Rightarrow T$	$\neg T \Rightarrow \neg P$
0	0	1	1
0	1	1	1
1	0	0	0
1	1	1	1

Tabulka 0.7.: *Tabulka pravdivostních hodnot implikace a obměny implikace.*

Nepřímý důkaz tvrzení ve tvaru implikace $P \Rightarrow T$ využívá faktu, že *obměna* $\neg T \Rightarrow \neg P$ má stejnou vždy pravdivostní hodnotu, jako původní implikace $P \Rightarrow T$. Tabulka 0.7. porovnává pravdivostní hodnoty obou složených výroků $P \Rightarrow T$ i $\neg T \Rightarrow \neg P$.

Někdy může být jednodušší místo implikace $P \Rightarrow T$ dokazovat její obměnu $\neg T \Rightarrow \neg P$.

Příklad 0.23. Jestliže součin dvou celých čísel ab je sudý, tak alespoň jedno z čísel a, b je sudé.
Postupuje nepřímo, tj. dokážeme obměnu implikace: jestliže jsou celá čísla a, b lichá, tak jejich součin ab je lichý. Všimněte si, že místo tří možných případů parity čísel a, b tak stačí rozebrat případ jediný.

Protože a je liché číslo, tak existuje celé číslo t takové, že $a = 2t + 1$. Podobně $b = 2s + 1$, kde $s \in \mathbb{Z}$. Potom součin $ab = (2t + 1)(2s + 1) = 4st + 2s + 2t + 1 = 2(2st + s + t) + 1$. Protože $2st + s + t$ je celé číslo, tak $2(2st + s + t)$ je sudé číslo a $2(2st + s + t) + 1$ je liché číslo.

Dokázali jsme obměnu implikace, která platí právě tehdy, když platí původní implikace. Tvrzení je dokázáno. ✓

Důkaz sporem

Dokazujeme-li sporem tvrzení ve tvaru implikace $P \Rightarrow T$, tak ukážeme, že současné splnění předpokladu a neplatnost tvrzení ve ke *sporu*. Sporem rozumíme situaci, kdy odvodíme platnost nějakého tvrzení a současně platnost negace tvrzení: $A \wedge \neg A$. V teorii vybudované z konzistentních axiomů nemáme žádný spor[1]. Symbolicky můžeme zapsat strukturu důkazu implikace $P \Rightarrow T$ sporem takto:

$$P \wedge \neg T \Rightarrow \ldots \Rightarrow A \wedge \neg A. \tag{3}$$

Předpokládáme-li bezespornost teorie, tak v okamžiku, kdy narazíme na spor, můžeme tvrdit, že implikace $P \Rightarrow T$ platí, tj. za předpokladu P platí tvrzení T. Zdůvodnění je následující: Narazíme-li za použití pravidel odvozování v řetězci implikací (3) na spor, tak musí být výchozí krok řetězce implikací neplatný, tj. neplatí konjunkce $P \wedge \neg T$. Konjunkce neplatí, jestliže alespoň jeden z výrazů není pravdivý. Pokud není pravdivý předpoklad P, tak nejsou splněny předpoklady dokazované věty a taková situace není pro důkaz tvrzení relevantní. Jedinou zbývající možností je, že není pravdivá negace tvrzení $\neg T$ a platí $\neg(\neg T)$, tedy platí T. Uvedené zdůvodnění je společné všem důkazům sporem, proto se zpravidla již neuvádí. Zkušený čtenář ví, že dostaneme-li v důkazu sporem dvě navzájem se vylučující tvrzení, dostáváme spor $A \wedge \neg A$. Proto můžeme ihned tvrdit, že za splnění předpokladu P platí tvrzení T. Máme tak dokázanou implikaci $P \Rightarrow T$.

Mezi klasické příklady důkazu sporem patří Euklidův důkaz, že existuje nekonečně mnoho prvočísel.

Příklad 0.24. Ukážeme, že prvočísel je nekonečně mnoho.
Postupujeme sporem. Využijeme základní větu aritmetiky, každé přirozené číslo větší než 1 můžeme napsat jednoznačně jako součin prvočísel. Pro spor předpokládáme, že prvočísel je konečně mnoho, označíme je $p_1, p_2, \ldots, p_n$. Avšak číslo x, kde $x = p_1 \cdot p_2 \cdots p_n + 1$, není dělitelné ani jedním z prvočísel! Dostáváme spor. Předpoklad, že prvočísel je konečně mnoho, vede ke sporu, proto není pravdivý, tj. prvočísel je nekonečně mnoho. ✓

Jen upozorníme, že na konstrukci důkazu sporem se nemůžeme spolehnout v takové teorii, kde samotné axiomy vedou ke sporu. Proto řada autorů preferuje místo důkazu sporem důkaz přímý, či nepřímý, neboť důkaz sporem využívá bezespornost dané teorie.

Důkaz matematickou indukcí

Matematická indukce je důkazová metoda, která se používá zejména pro důkazy tvrzení ve tvaru

$$\forall n \in M : P(n),$$

kde M je nějaká množina čísel aritmetické posloupnosti. Důkaz matematickou indukcí má vždy dvě principiálně různé části. *Základ indukce* je část, ve které ukážeme platnost tvrzení výrokové formy $P(n)$ pro jednu

[1] Z Gödelovy Druhé věty o neúplnosti však vyplývá, že bezespornost dostatečně bohaté teorie, mezi které diskrétní matematika patří, bezespornost můžeme pouze předpokládat, nemůžeme ji však dokázat.

nejmenší, případně několik nejmenších, hodnot n. Hodnotu označíme n_0. V *indukčním kroku* pak ukážeme obecný postup, jak platnost výroku $P(n)$ odvodit na základě platnosti výroku $P(k)$ pro hodnoty k menší než n.

Jestliže k je jedna nebo více hodnot bezprostředně menších než n, říkáme, že používáme klasickou indukci. V případě, že potřebujeme využít platnosti pro jednu nebo více hodnot k z intervalu $[n_0, n-1]$, říkáme, že používáme silnou indukci. Název „silná“ indukce je poněkud zavádějící, protože oba přístupy jsou ekvivalentní co do množiny dokazatelných tvrzení.

Matematická indukce nachází uplatnění při důkazu řady vztahů, rovností, nerovností, relací, ale i algoritmů. Často lze induktivní důkaz nějakého tvrzení implementovat jako rekurzivní algoritmus pro konstruktivní řešení úlohy.

Příklad 0.25. Ukažte že pro každé $n \geq 5$ platí $2^n > n^2$.

Základ indukce: Nejmenší hodnota, pro kterou máme tvrzení dokázat, je $n = 5$. Protože $2^5 = 32 > 25 = = n^2$, tak tvrzení pro $n = 5$ platí. (Všimněte si, že pro menší hodnoty tvrzení platit nemusí: například pro $n = 0$ a $n = 1$ tvrzení sice platí, ale pro $n = 2$, $n = 4$ nastává rovnost a pro $n = 3$ tvrzení také neplatí, neboť $2^3 = 8 < 9 = 3^2$.)

Indukční krok: Předpokládejme, že pro *nějakou* hodnotu n, kde $n \geq 5$, je nerovnost splněna, tj. $2^n > n^2$. Je dobré si uvědomit, že zde nepředpokládáme platnost dokazovaného tvrzení, protože tvrzení dokazujeme pro *všechna* $n \geq 5$, ale platnost předpokládáme pro *nějaké* n, což dle základu indukce máme prověřeno. Nyní ukážeme, že nerovnost je splněna i pro následující hodnotu $n + 1$.

$$2^{n+1} = 2 \cdot 2^n$$

S využitím indukčního předpokladu $2^n > n^2$ můžeme pravou stranu upravit

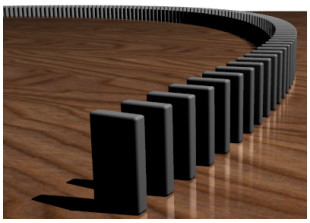
$$\begin{aligned} 2^{n+1} &> 2 \cdot n^2 \\ &= n^2 + n^2 \\ &= n^2 + 2n + (n-2)n, \end{aligned}$$

a protože pro $n \geq 5$ je $(n-2)n > 1$, tak můžeme upravit

$$\begin{aligned} 2^{n+1} &> n^2 + 2n + 1 \\ &= (n+1)^2. \end{aligned}$$

Celkem dostáváme, že $2^{n+1} > (n+1)^2$ a podle principu matematické indukce je nerovnost $2^n > n^2$ splněna pro všechna $n \geq 5$. ✓

Jak může důkaz dvou kroků zajistit platnost tvrzení pro nekonečně mnoho hodnot? Princip matematické indukce bývá někdy přirovnáván k padající řadě dominových kostek (Obrázek 0.18.). Základ indukce odpovídá prvnímu kroku: shození první kostky v řadě. To však nestačí! Musí být zajištěno, že každá padající kostka shodí následující kostku, což zajišťuje platnost indukčního kroku. Uvědomte si, jak se oba kroky principiálně liší: zatímco základ indukce řeší jednu konkrétní hodnotu (kostku), případně několik hodnot (kostek), tak indukční krok řeší vztah mezi obecnou n-tou hodnotou (kostkou) a následující, respektive předchozí hodnotou (kostkou).

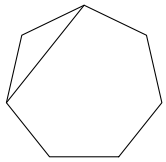


Obrázek 0.18.: *Řada dominových kostek.*

Úplnost důkazu matematickou indukcí, tj. platnost $P(n)$ pro každý prvek množiny M, můžeme opět znázornit padající řadou kostek. Nebude-li shozena první kostka, řada nespadne. Dále, pokud nebude zajištěno, že každá kostka shodí následující kostku, řada kostek také nespadne celá.

V diskrétní matematice a zejména v teorii grafů může mít důkaz matematickou indukcí svou specifickou strukturu. Zatímco v důkazech matematickou indukcí různých algebraických tvrzení hodnotu výrokové proměnné v indukčním kroku zpravidla *zvyšujeme*, z předpokladu platnosti $P(n)$ odvozujeme platnost $P(n+1)$, tak v teorii grafů často hodnotu výrokové proměnné *nejprve zmenšíme*, prozkoumáme strukturu menšího grafu, a poté hodnotu parametru *opět zvýšíme* a odvodíme platnost $P(n)$ na základě pozorování pro hodnoty k z intervalu $[n_0, n-1]$. To má dobrý důvod. Zatímco v algebře je zajímavá pouze hodnota indukční proměnné, kterou můžeme zvýšit nebo snížit, tak v teorii grafů je význam hodnoty indukční proměnné vázán na *strukturu* grafu. Potom nemusí být jasné, zda každou větší strukturu můžeme dostat pouhým přidáváním k menší struktuře. Dokonce je řada příkladů, kde to není pravda: například větší cyklus C_{n+1} nedostaneme pouhým přidáním vrcholu a hrany do menšího cyklu C_n. Museli bychom nějakou hranu také odebrat. Můžeme však z cyklu C_n nejprve hranu odebrat, potom zkoumat vlastnosti vzniklého podgrafu P_n, který má sice stejnou množinu vrcholů, ale menší počet hran. Nebo můžeme z cyklu C_n odebrat vrchol (a obě incidentní hrany) a zkoumat vlastnosti vzniklého podgrafu P_{n-1}. Poté vrátíme odebranou hranu resp. odebraný vrchol zpět a odvodíme platnost tvrzení pro cyklus C_n.

Příklad 0.26. Víme, že součet vnitřních úhlů trojúhelníka je π. Mějme konvexní n-úhelník. Indukcí ukážeme, že součet vnitřních úhlů tohoto n-úhelníka je $(n-2)\pi$.
Základ indukce: Nejmenší hodnota čísla n, pro kterou má smysl sestrojit n-úhelník, je $n = 3$. Pro trojúhelník víme, že součet hodnot vnitřních úhlů je π, což odpovídá dokazovanému vztahu $(n-2)\pi = (3-2)\pi = \pi$.
Indukční krok: Mějme nějaký konvexní n-úhelník pro $n > 3$. Dále předpokládejme, pro hodnoty k, kde $3 \leq k < n$, součet vnitřních úhlů n-úhelníka je $(k-2)\pi$. Nyní určíme součet vnitřních úhlů našeho n-úhelníka. Libovolnou úhlopříčkou rozdělíme n-úhelník na dva menší konvexní mnohoúhelníky. Není těžké si rozmyslet, že pro konvexní mnohoúhelník se vždy může jednat o jeden trojúhelník a jeden $(n-1)$-úhelník (Obrázek 0.19.).



Obrázek 0.19.: *Rozdělení n-úhelníka na trojúhelník a $(n-1)$-úhelník.*

Součet vnitřních úhlů trojúhelníka je π a podle indukčního předpokladu je součet vnitřních úhlů $(n-1)$-úhelníka roven $(n-3)\pi$. Součet vnitřních úhlů daného n-úhelníka je dán součtem vnitřních úhlů trojúhelníka a $(n-1)$-úhelníka, což dává $\pi + (n-3)\pi = (n-2)\pi$.

Podle principu matematické indukce je proto součet vnitřních úhlů každého konvexního n-úhelníka roven $(n-2)\pi$. ✓

Příklad 0.27. Ukážeme, že každé poštovné větší nebo rovno 9 Kč může být zaplaceno užitím známek v hodnotě 3 Kč a 5 Kč.
Tvrzení ukážeme matematickou indukcí vzhledem k ceně c.
Základ indukce: Nejprve ukážeme, že je možno vyplatit částky

- 9 Kč jako $3+3+3=9$,
- 10 Kč jako $5+5=10$,
- 11 Kč jako $5+3+3=11$.

Indukční krok: Ukážeme, že když jde zaplatit poštovné v ceně c, tak jde zaplatit také poštovné o hodnotě $c+3$. Stačí nalepit o jednu tříkorunovou známku navíc.

To podle principu matematické indukce znamená, že pomocí známek v hodnotě 3 a 5 Kč můžeme zaplatit jakékoliv poštovné v hodnotě alespoň 9 Kč.

Všimněte si, že poštovné 8 Kč je také možno zaplatit jako $3+5$ Kč. Dokazované tvrzení by mohlo být obecnější. Naproti tomu hodnotu 7 Kč zaplatit není možné. Pokud bychom platili pouze tříkorunovými známkami, 7 Kč nezaplatíme. Pokud platíme alespoň jednou pětikorunovou známkou, tak zaplatíme částku 5 Kč, 8 Kč, nebo částky vyšší, ale 7 Kč zaplatit nelze. ✓

Otázky:

- Vysvětlete rozdíl mezi pojmem indukce a silná matematická indukce.
- Vysvětlete analogii princip matematické indukce na vystoupání na libovolně vysoký žebřík.

O důkazech matematickou indukcí napsal David S. Gunderson pěknou knihu „Handbook of Mathematical Induction: Theory and Applications“.

Odkazy:

- https://en.wikipedia.org/wiki/Mathematical_proof
- https://en.wikipedia.org/wiki/Gödel's_incompleteness_theorems
- https://www.maa.org/press/maa-reviews/handbook-of-mathematical-induction-theory-and-applications

Cvičení

0.8.1. Dokažte, že číslo $\sqrt{3}$ není racionální.

0.8.2. Ukažte že součet lichého počtu lichých sčítanců je liché číslo.

0.8.3. Mějme přirozené číslo n. Ukažte, že pro číslo $n^4 + 4$ je prvočíslo pouze pro $n = 1$.

0.8.4. Mějme přirozené číslo n. Ukažte, že pokud součet všech kladných dělitelů čísla n je $n + 1$, tak n je prvočíslo.

0.8.5. Ukažte, že $\log_2 3$ je iracionální číslo.

0.8.6. Ukažte, že je-li nějaká operace asociativní pro libovolnou trojici prvků $x, y, z \in A$, tak výsledek operace bude stejný pro libovolné uzávorkování každé posloupnosti prvků $a_1, a_2, \ldots, a_k \in A$ (tj. výsledek operace je asociativní pro k prvků).

0.8.7. Ukažte, že žádný polynom $a_n x^n + a_{n-1} x p^{n-1} + \cdots + a_1 x + a_0$ s celočíselnými koeficienty ($a_i \in \mathbb{Z}$ pro $0 \leq i \leq n$) nemůže mít v přirozených číslech (pro $x \in \mathbb{N}$) pouze prvočíselné funkční hodnoty, jestliže a_0 není prvočíslo ani 1. Platí tvrzení pokud a_0 je prvočíslo? Platí tvrzení pokud a_0 je 1?

0.8.8. Mějme libovolná dvě po sobě následující lichá čísla p a q. Ukažte, že $(p + q) \mid (p^q + q^p)$.

0.9. Co se nevešlo

Následuje několik poznámek, které nespadají do žádné z předchozích podkapitol.

Interval celých čísel
Interval celých čísel $[a, b]$ zavedeme jako množinu $\{x \in \mathbb{Z} : a \leq x \wedge x \leq b\}$. *Mohutnost* (konečné) množiny M udává počet prvků v M a značíme ji $|M|$. Mohutnost má smysl zavést i pro nekonečné (i nespočetné) množiny, v tomto textu ale budeme pracovat s mohutností jen konečných množin.

Skalární a vektorový součin vektorů
Mějme množinu $\mathbb{R}^n$. Každý prvek množiny $\mathbb{R}^n$ nazveme n-rozměrným vektorem a každé dva vektory $\vec{a}, \vec{b} \in \mathbb{R}^n$ můžeme skalárně vynásobit. Označme $\vec{a} = (a_1, a_2, \ldots, a_n)$, $\vec{b} = (b_1, b_2, \ldots, b_n)$, *Skalárním součinem* vektorů $\vec{a}$, $\vec{b}$ rozumíme číslo definované

$$\vec{a} \cdot \vec{b} = a_1 b_1 + a_2 b_2 + \cdots + a_n b_n.$$

Je dobré si uvědomit, že skalární součin vektorů *není operací* na množině $\mathbb{R}^n$, neboť výsledkem skalárního součinu není vektor z množiny $\mathbb{R}^n$.

Jestliže se omezíme na případ $n = 3$, můžeme nadefinovat jiný součin vektorů, který *je operací* na množině $\mathbb{R}^3$. *Vektorovým součinem* vektorů $\vec{a} = (a_1, a_2, a_3)$, $\vec{b} = (b_1, b_2, b_3)$ rozumíme vektor definovaný

$$\vec{a} \times \vec{b} = (a_2 b_3 - a_3 b_2, a_3 b_1 - a_1 b_3, a_1 b_2 - a_2 b_1).$$

Asi nejpřehledněji je vektorový součin popsaný jako determinant matice

$$\vec{a} \times \vec{b} = \begin{vmatrix} \vec{i} & \vec{j} & \vec{k} \\ a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \end{vmatrix},$$

kde $\vec{i} = (1, 0, 0)$, $\vec{j} = (0, 1, 0)$, $\vec{k} = (0, 0, 1)$ jsou jednotkové vektory ve směru jednotlivých os.

Nekonečno

Je nekonečno celé číslo nebo reálné číslo? Tato otázka vypadá možná zajímavě, ale nemá smysl. Pojem nekonečna můžeme chápat několika způsoby, ale v ani jednom z nich není nekonečno chápáno jako obvyklé číslo.

Jednak můžeme „nekonečno“ chápat jako vyjádření velikosti prvku nebo množiny. Staří Řekové pracovali s nekonečnem, jako s „potencionálním“ nekonečnem: přímka je úsečka, kterou můžeme libovolně prodlužovat, ke každému přirozenému číslu můžeme najít větší. Neměli potřebu „mít všechna přirozená čísla“. Taková práce s aktuálním nekonečnem: máme množinu $\mathbb{N}$, která obsahuje všechna přirozená čísla, automaticky předpokládá, že je možné obsáhnout všech nekonečně mnoho přirozených čísel do jedné množiny a pracovat s nimi. Každopádně nemá smysl říkat, že nekonečno je přirozené, nebo celé číslo, ani nebudeme psát $\infty \in \mathbb{N}$. Nekonečný počet čísel chápeme spíše ve smyslu potenciálního nekonečna, tedy, že žádné přirozené číslo není největší, vždy bychom mohli snadno najít větší přirozené číslo.

Podobně je tomu v případě, kdy popisujeme intervaly reálných čísel. Například $\langle a, \infty)$ je interval, který popisuje (a zapisuje) množinu všech reálných čísel, která jsou větší nebo rovna nějakému číslu a. *Nepotřebujeme* tvrdit, že $\infty \in \mathbb{R}$ a ani to není pravda.

Trochy jiná situace nastane, pracujeme-li s rozšířenou množinou reálných čísel R^*. Tady vnímáme, že dva prvky ∞ a $-\infty$ do množiny R^* patří, avšak nepočítáme s nimi jako s jinými reálnými čísly. Víme například, že rovnost $a + 4 = a$ nesplňuje žádné reálné číslo a, protože odečtením a od obou stran dostaneme neplatné tvrzení $4 = 0$. Avšak zápis $\infty + 4 = \infty$ se objevit může, má však jiný význam. Zpravidla jej chápeme tak, že přičtením konstanty k nekonečné hodnotě nedostaneme hodnotu větší. Symbol ∞ je pohodlný i pro vyjádření faktu, že „nekonečno“ je více než libovolné reálné číslo $\infty > a$, respektive $-\infty < a$.

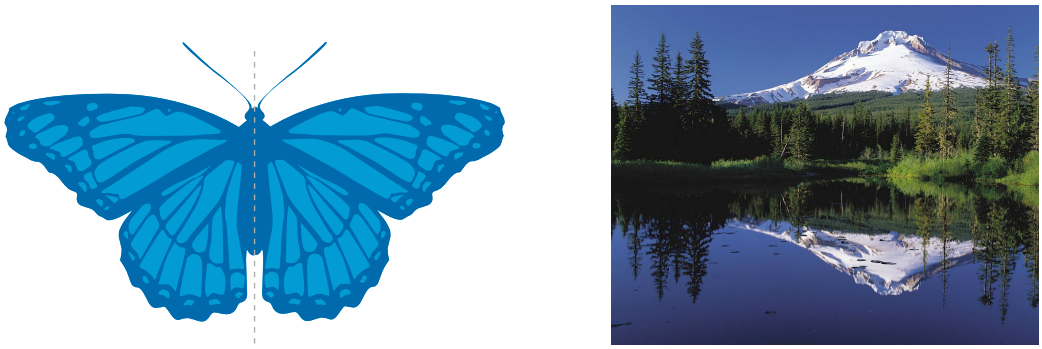
Naproti tomu krátit, zejména zapisujeme-li typ limity, by bylo chybou. Je-li limita typu $\frac{\infty}{\infty}$, tak nemůžeme říci, že limita je rovna 1, jako kdybychom měli například limitu výrazu $\frac{4}{4}$. Zkrátka symbol nekonečna nevnímám jako „číslo“, ale jako prvek, který můžeme porovnávat ($\infty > 4$), můžeme pracovat s některými operacemi ($\infty \cdot (-2) = -\infty$), ale ne se všemi operacemi ($\infty - \infty \neq 0$).

Kapitola 1. Symetrie a dihedrální grupy

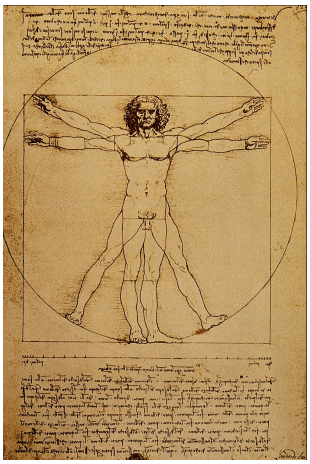
1.1. Symetrie

Jednou z motivací, která stojí za definicí pojmu grup, zejména konečných grup, je pojem „symetrie“. Co je to symetrie? Řekneme, že nějaký objekt je *symetrický*, jestliže je pro něj možné zavést jistou *operaci symetrie*, což je takové zobrazení bodů v rovině nebo v prostoru, kdy příslušný objekt před transformací je totožný s výsledným objektem po transformaci. Říkáme, že zůstane sám sebou. Nutno přiznat, že tím jsme pouze převedli definici pojmu „symetrie objektu“ na předpoklad znalosti pojmu „operace symetrie“ a „transformace“.

Na Obrázku 1.1. vidíme příklady osových symetrií, kterým budeme zkráceně říkat zrcadlení. Na Obrázku 1.2. striktně vzato není osová symetrie, nicméně jako tento obrázek bývá také často uváděn jako příklad „symetrie“ lidského těla.



Obrázek 1.1.: *Osové symetrie.*



Obrázek 1.2.: *Osová symetrie.*

Nyní označíme zobrazení, která každý bod motýla nebo fotografie na Obrázku 1.1. zobrazí tak, aby výsledný obraz byl totožný s původním obrázkem. Pro obrázek vlevo se bude jednat o identitu I a o osovou symetrii V podle vertikální osy. Pro fotografii vpravo se bude jednat o identitu I a o osovou symetrii H podle horizontální osy. Pro každý obrázek můžeme zobrazení skládat. Operaci skládání zapisujeme pomocí operátoru „$\circ$“. Pro symetrie fotografie vlevo jistě platí $I \circ I = I$, $I \circ V = V \circ I = V$ a $V \circ V = I$, což můžeme shrnout do Cayleyho tabulky 1.1. operace skládání zobrazení.

$\circ$	I	V
I	I	V
V	V	I

Tabulka 1.1.: *Skládání symetrií motýlka.*

Podobně pro symetrie fotografie na Obrázku 1.1. vpravo jistě platí $I \circ I = I$, $I \circ H = H \circ I = H$ a $H \circ H = I$, což můžeme shrnout do Cayleyho tabulky 1.2.

$\circ$	I	H
I	I	H
H	H	I

Tabulka 1.2.: *Skládání symetrií fotografie odrazu na hladině.*

Symetrie rovnostranného trojúhelníka

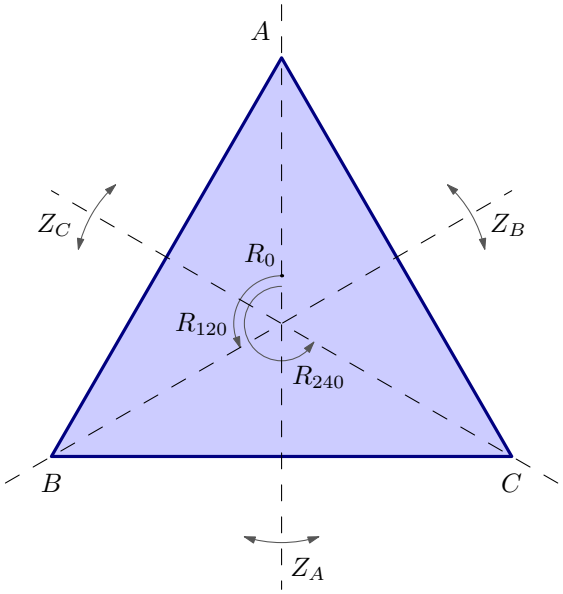
Označíme po řadě vrcholy trojúhelníka ABC. Trojúhelník můžeme zobrazit na sebe (vrcholy zobrazit na vrcholy a hrany zobrazit na hrany tak, aby byla zachována sousednost) šesti různými způsoby. Každé takové zobrazení je nějakou symetrií rovnostranného trojúhelníka. Jednotlivá zobrazení pojmenujeme a označíme:

1) identita; označíme ji R_0
2) otočení o 120°; označíme ji R_{120}
3) otočení o 240°; označíme ji R_{240}
4) zrcadlení s osou souměrnosti na výšce bodem A; označme ji Z_A
5) zrcadlení s osou souměrnosti na výšce bodem B; označme ji Z_B
6) zrcadlení s osou souměrnosti na výšce bodem C; označme ji Z_C

Symetrie můžeme přehledně zapsat pomocí bijektivních zobrazení vrcholů $\{A, B, C\} \to \{A, B, C\}$ rovnostranného trojúhelníka ABC.

$$R_0 = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} \quad R_{120} = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} \quad R_{240} = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$$

$$Z_A = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \quad Z_B = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \quad Z_C = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$$



Obrázek 1.3.: *Rovnostranný trojúhelník má 6 symetrií.*

$\circ$	R_0	R_{120}	R_{240}	Z_A	Z_B	Z_C
R_0	R_0	R_{120}	R_{240}	Z_A	Z_B	Z_C
R_{120}	R_{120}	R_{240}	R_0	Z_C	Z_A	Z_B
R_{240}	R_{240}	R_0	R_{120}	Z_B	Z_C	Z_A
Z_A	Z_A	Z_B	Z_C	R_0	R_{120}	R_{240}
Z_B	Z_B	Z_C	Z_A	R_{240}	R_0	R_{120}
Z_C	Z_C	Z_A	Z_B	R_{120}	R_{240}	R_0

Tabulka 1.3.: *Tabulka skládání symetrií rovnostranného trojúhelníka.*

Uvědomme si, že zobrazení (symetrie) můžeme skládat. Skládání symetrií je operace, neboť složením libovolných dvou z uvedených symetrií dostaneme opět některou z těchto šesti symetrií. Obvykle se operace skládání zobrazení čte zprava doleva, což je opačný postup oproti například sčítání nebo násobení! Zápis skládání symetrií chápeme takto: nejprve aplikujeme symetrii vpravo a další aplikované symetrie jsou postupně zapsány vlevo. Například složením $R_{120} \circ Z_A$ (čti „otočení R_{120} po zrcadlení Z_A“) dostaneme zrcadlení Z_B. Podobně složením $Z_B \circ Z_A$ (čti „složením zrcadlení Z_B po zrcadlení Z_A“) dostaneme otočení R_{120}. Abychom mohli pracovat přehledně s Cayleyho tabulkou operace skládání symetrií rovnostranného trojúhelníka, uděláme úmluvu, že první symetrii operace skládání budeme zapisovat do *levého* záhlaví a druhou symetrii do *horního* záhlaví. Dostaneme Tabulku 1.3.

Příklad 1.1. Další příklady skládání symetrií rovnostranného trojúhelníka jsou

1) $R_{120} \circ R_{120} = R_{240}$, neboť otočením o 120° a dalších 120° dostaneme otočení o 240°.
2) $R_{120} \circ R_{240} = R_0$, neboť složením otočení o 240° a ještě o 120° dostaneme identitu.
3) $R_{240} \circ R_{120} = R_0$
4) $Z_C \circ R_{120} = Z_B$; složením otočení a zrcadlení dostaneme vždy opět zrcadlení.
5) $R_{120} \circ Z_A = Z_B$
6) $Z_B \circ Z_A = R_{120}$; složením dvou zrcadlení dostaneme vždy otočení.
7) $Z_A \circ Z_B = R_{240}$; skládání zrcadlení není komutativní

Naproti tomu například otočení o 60° nebo posunutí (translace) trojúhelníka ABC na Obrázku 1.3. nejsou symetrie, protože jejich výsledkem by nebyl identický trojúhelník na stejném místě. Proto takové transformace za symetrie nepovažujeme.

Všimněte si, že Tabulka 1.3. má na rozdíl od Tabulky 0.6. *jinou* strukturu. Protože operace skládání symetrií rovnostranného trojúhelníka není komutativní, tabulka není symetrická podle hlavní diagonály. Dále je pěkně vidět, že otočení dostaneme jako složení dvou otočení nebo dvou zrcadlení (buď dvou přímých nebo dvou nepřímých shodností), zatímco složením otočení a zrcadlení v libovolném pořadí (jedné přímé a jedné nepřímé shodnosti) dostaneme nepřímou shodnost.

Na druhou stranu si všimneme následujících vlastností:

1) Na žádnou symetrii jsme nezapomněli, existuje jen šest způsobů, jak vrcholy trojúhelníka označit. Složením libovolných dvou symetrií tak dostaneme vždy některou z uvedených šesti symetrií. V další kapitole tomu budeme říkat uzavřenost operace.
2) Identita R_0 má výjimečné postavení. Složíme-li libovolnou symetrii s R_0, výsledná symetrie se nezmění. V další kapitole takovému prvku budeme říkat neutrální.
3) Operace není komutativní, stačí najít jedinou dvojici, která komutativitu porušuje. Například $Z_A \circ Z_B = R_{240}$, zatímco $Z_B \circ Z_A = R_{120}$.
4) Operace skládání zobrazení (nejen symetrií rovnostranného trojúhelníka) je vždy asociativní! To znamená, že při skládání tří operandů nezávisí na uzávorkování. (Například $(Z_A \circ Z_B) \circ Z_A = R_{240} \circ Z_A = Z_C$ a současně $Z_A \circ (Z_B \circ Z_A) = Z_A \circ R_{120} = Z_C$.) Obecný důkaz je na straně 12.

Pokud bychom vzali šestiúhelník, jeho strany zorientovali například ve směru hodinových ručiček a zkoumali symetrie tohoto orientovaného šestiúhelníka, tak dostaneme tabulku se *stejnou* strukturou, jako u sčítání modulo 6 (Tabulka 0.5.). Úkol je ponechán jako Cvičení 1.1.1.

Poznámka 1.1. Pokud bychom symetrie skládali v opačném pořadí zapsáno zleva doprava, dostaneme tabulku převrácenou podle hlavní diagonály. Analogicky, pokud budeme zapisovat první symetrii složené symetrie do levého záhlaví a druhou symetrii do horního záhlaví, tak také dostaneme tabulku převrácenou podle hlavní diagonály.

Symetrie čtverce

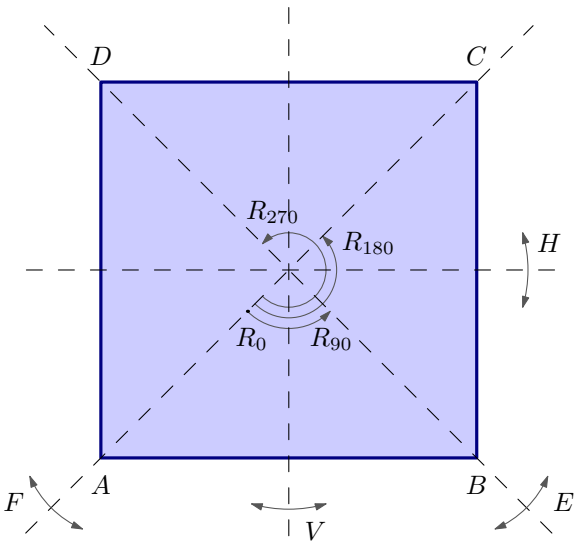
Označíme po řadě vrcholy čtverce $ABCD$. Symetrií čtverce rozumíme takové zobrazení čtverce na sebe, že vrcholy se zobrazí na vrcholy a hrany se zobrazí na hrany čtverce tak, aby byla zachována sousednost. Různých symetrií čtverce existuje celkem osm:

1) identita; označíme ji R_0,
2) otočení o 90°, 180° a 270°; označíme je R_{90}, R_{180} a R_{270},
3) zrcadlení podle vodorovné a svislé osy, označíme je H a V,
4) zrcadlení podle hlavní a vedlejší diagonály, označíme je E a F,

Uvědomme si, že všech permutací čtyřprvkové množiny vrcholů čtverce je $P(4) = 4! = 24$, avšak ne každá permutace odpovídá nějaké symetrii čtverce. Například permutace

$$\begin{pmatrix} A & B & C & D \\ A & C & D & B \end{pmatrix}$$

žádnou *symetrií* není, neboť uvedené pořadí vrcholů nezachovává sousednost vrcholů čtverce.



Obrázek 1.4.: *Čtverec má osm symetrií.*

Opět si všimneme následujících vlastností:

1) Na žádnou symetrii jsme nezapomněli a složením libovolných dvou symetrií dostaneme vždy některou z uvedených osmi symetrií. V další kapitole tomu budeme říkat uzavřenost operace.
2) Identita R_0 má výjimečné postavení. Složíme-li libovolnou symetrii s R_0, výsledná symetrie se nezmění. V další kapitol takovému prvku budeme říkat neutrální.
3) Operace není komutativní, stačí najít jedinou dvojici, která komutativitu porušuje. Například $E \circ V = R_{90}$, zatímco $V \circ E = R_{270}$.
4) Operace skládání zobrazení je opět asociativní!

Sestavení Cayleyho tabulky operace skládání symetrií čtverce je ponecháno jako Cvičení 1.1.2.

Symetrie symbolu recyklace
Kolik různých symetrií má symbol mezinárodní symbol pro recyklaci na Obrázku 1.5.?

Obrázek 1.5.: *Mezinárodní symbol pro recyklaci obsahuje Möbiův list.*

Na první pohled je zřejmé, že na rozdíl od rovnostranného trojúhelníka nepatří žádné zrcadlení do množiny symetrií. Při bližším zkoumání si všimneme, že ani žádné netriviální otočení není symetrií, proto grupa symetrií symbolu na Obrázku 1.5. je triviální (Tabulka 1.4.).

$\circ$	R_0
R_0	R_0

Tabulka 1.4.: *Tabulka skládání symetrií symboly recyklace.*

Cvičení

1.1.1.$^{\heartsuit}$ *Sestavte Cayleyho tabulky symetrií orientovaného šestiúhelníka.*

1.1.2.$^{\heartsuit}$ *Sestavte Cayleyho tabulky symetrií čtverce.*

1.1.3.$^{\heartsuit}$ *Sestavte Cayleyho tabulku symetrií pravidelného pětiúhelníka.*

1.2. Dihedrální grupy

Při popisu symetrií pravidelného n-úhelníka pracujeme zpravidla s tzv. dihedrální grupou. Pro $n \geq 3$ má n-úhelník $2n$ symetrií, které můžeme skládat a výsledkem bude vždy některá z těchto symetrií.

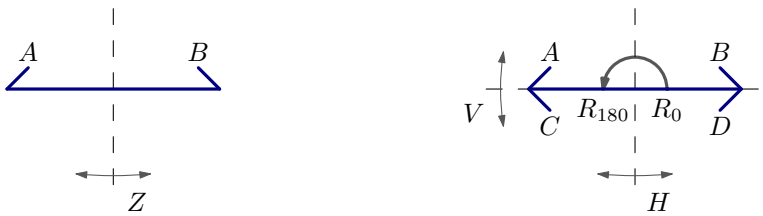
Symetrie pravidelného n-úhelníka

Definice Dihedrální grupa
Dihedrální grupou řádu $2n$ rozumíme množinu symetrií (zobrazení symetrie) pravidelného n-úhelníka s operací skládání zobrazení. Budeme ji značit $(D_n, \circ)$ nebo stručně D_n.

Už víme, že existuje šest symetrií rovnostranného trojúhelníka. Cayleyho Tabulka 1.3. je současně tabulkou dihedrální grupy $(D_3, \circ)$. Čtverec má osm symetrií a Cayleyho tabulka symetrií čtverce je současně tabulkou dihedrální grupy $(D_4, \circ)$ (Cvičení 1.1.2.). Obecně každý pravidelný n-úhelník má právě $2n$ symetrií (například Obrázky 1.3. a 1.4.), proto říkáme, že dihedrální grupa $(D_n, \circ)$ je „řádu $2n$“ (řád grupy budeme definovat na straně 83).

O symetriích n-úhelníka má smysl mluvit pouze pro $n \geq 3$. Úvahy však můžeme rozšířit i pro $n = 1$, kdy $(D_1, \circ)$ chápeme jako dvouprvkovou grupu popsanou Tabulkou 1.5. Dihedrální grupu $(D_1, \circ)$ si můžeme představit jako symetrie modrého obrazce na Obrázku 1.6. vlevo.

Pro $n = 2$ je $(D_2, \circ)$ popsána Tabulkou 1.6. Dihedrální grupu $(D_2, \circ)$ si můžeme představit jako symetrie modrého obrazce na Obrázku 1.6. vpravo. Grupě s takovou strukturou se říká také Kleinova grupa, podrobněji o ní bude psáno v Kapitole 10.



Obrázek 1.6.: *Symetrie dihedrální grupy* $(D_1, \circ)$ *a grupy* $(D_2, \circ)$.

$\circ$	I	Z
I	I	Z
Z	Z	I

Tabulka 1.5.: *Tabulka dihedrální grupy* $(D_1, \circ)$.

$\circ$	R_0	R_{180}	V	H
R_0	R_0	R_{180}	V	H
R_{180}	R_{180}	R_0	H	V
V	V	H	R_0	R_{180}
H	H	V	R_{180}	R_0

Tabulka 1.6.: *Tabulka dihedrální grupy* $(D_2, \circ)$.

$\circ$	R_1 $\cdots$ R_n	Z_1 $\cdots$ Z_n
R_1 $\vdots$ R_n	R_1 $\cdots$ R_n	Z_1 $\cdots$ Z_n
Z_1 $\vdots$ Z_N	Z_1 $\cdots$ Z_n	R_1 $\cdots$ R_n

Tabulka 1.7.: *Tabulka dihedrální grupy řádu* $2n$.

Všechny dihedrální grupy mají společné rysy:

1) dihedrální grupa řádu $2n$ má n rotací (symetrií, které odpovídají přímým shodnostem n-úhelníka) a n zrcadlení, které odpovídají nepřímým shodnostem n-úhelníka),
2) složení dvou rotací dává vždy nějakou (další) rotaci,
3) složení rotace a zrcadlení dává vždy nějaké zrcadlení,
4) složení dvou zrcadlení dává vždy nějakou rotaci,
5) množina rotací sama o sobě tvoří menší Cayleyho tabulku.

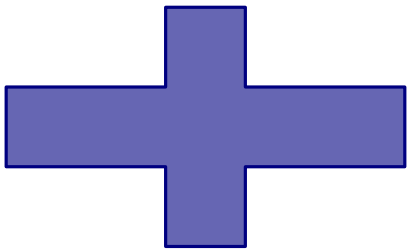
Schematicky můžeme Cayleyho tabulku dihedrální grupy řádu n popsat Tabulkou 1.7.

Cvičení

1.2.1. Které dihedrální grupy $(D_n, \circ)$ jsou komutativní?

1.2.2.$^\heartsuit$ Sestavte Cayleyho tabulky symetrií pravidelného orientovaného a) pětiúhelníka, b) osmiúhelníka.

1.2.3. Popište grupu symetrií obrazce na Obrázku 1.7.



Obrázek 1.7.: *Symetrie kříže.*

1.3. Další příklady symetrií

Symetrie kvádru

Symetrií kvádru jako tělesa je obecně méně, než je symetrií krychle. Pro $a > b > c$ jsou čtyři přímé shodnosti: identita a tři otočení o 180°. Označme je identitu I, otočení podle osy jdoucí středem stran a rovnoběžné s hranou a jako R_a a podobně R_b, R_c. Dostaneme Tabulku 1.8.

Je dobré si všimnout, že Tabulka 1.8. má *jinou* strukturu, než tabulka přímých shodností čtverce s otočeními R_0, R_{90}, R_{180}, R_{270} (Tabulka 1.9.). Například pro každou přímou symetrii S kvádru platí, že složíme-li ji dvakrát, dostaneme identitu, platí $R_a \circ R_a = I$, $R_b \circ R_b = I$, $R_c \circ R_c = I$ a samozřejmě $I \circ I = I$.

$\circ$	I	R_a	R_b	R_c
I	I	R_a	R_b	R_c
R_a	R_a	I	R_c	R_b
R_b	R_b	R_c	I	R_a
R_c	R_c	R_b	R_a	I

Tabulka 1.8.: *Tabulka prostorových symetrií kvádru s hranami $a < b < c$.*

$\circ$	R_0	R_{90}	R_{180}	R_{270}
R_0	R_0	R_{90}	R_{180}	R_{270}
R_{90}	R_{90}	R_{180}	R_{270}	R_0
R_{180}	R_{180}	R_{270}	R_0	R_{90}
R_{270}	R_{270}	R_0	R_{90}	R_{180}

Tabulka 1.9.: *Tabulka přímých symetrií čtverce.*

Avšak pouze dvě přímé shodnosti čtverce dávají složením identitu: $R_0 \circ R_0 = R_0$ a $R_{180} \circ R_{180} = R_{180}$. Pro další dvě symetrie platí $R_{90} \circ R_{90} = R_{180}$, $R_{270} \circ R_{270} = R_{180}$.

Jestliže uvážíme i nepřímé shodnosti kvádru, je shodností celkem osm: označme zrcadlení podle roviny kolmé k hraně a jako Z_a, zrcadlení podle roviny kolmé k hraně b jako Z_b a zrcadlení podle roviny kolmé k hraně c jako Z_c. Poslední symetrií je středová souměrnost podle těžiště kvádru, označme ji Z_s. Sestavení tabulky symetrií je ponecháno jako Cvičení 1.3.3. Ale opět bude taková tabulka mít *jinou* strukturu, než tabulka všech symetrií čtverce, kterou sestavujeme ve Cvičení 1.1.2..

Loydova 15 a permutace

Hlavolam Patnáctka, nebo také Loydova patnáctka, sestává z patnácti kamenů umístěných do krabičky pro 4×4 kameny, přičemž kameny můžeme posouvat na sousední volnou pozici (Obrázek 7.2.). Jeho autorství bývá připisováno Americkému vynálezci a matematikovi Samu Loydovi. Některé prameny však původ hlavolamu připisují poštmistrovi Noyesi Palmeru Chapmanovi z Canastoty ve státě new York. Cílem hlavolamu je přesunout kameny z výchozí pozice do stavu, kdy jsou kameny seřazeny vzestupně po řádcích a volná pozice je na posledním místě. Různá rozmíchání hlavolamu můžeme chápat jako různé symetrie výchozího stavu.

V Kapitole 7. ukážeme, jak Loydovu patnáctku popsat pomocí permutací. Každé rozmístění kamenů do krabičky bude odpovídat některé permutaci šestnáctiprvkové množiny (včetně volné pozice). Ukážeme, že některá rozmístění kamenů nejsou z výchozí pozice dosažitelná pomocí posouvání kamenů. Přípustná rozmíchání budou odpovídat jen vybraným permutacím a ukážeme, jak takové permutace poznat.

Nejzajímavější je si uvědomit, že přípustných rozmíchání (přípustných symetrií) je sice nesmírně mnoho, ale ty symetrie, které se liší posunutím jediného kamene, můžeme považovat za „sousední“ a všechny symetrie, které odpovídají přípustným rozmícháním, můžeme dosáhnout pomocí posloupnosti „sousedních“ symetrií, tj. pomocí posloupnosti přípustných tahů. Naproti tomu ta rozmístění kamenů, která neodpovídají přípustným rozmícháním, pomocí takové posloupnosti tahů dosažitelná nejsou. Podrobně se popisu dosažitelných symetrií věnujeme v sekci 7.3. na straně 122.

Odkazy:

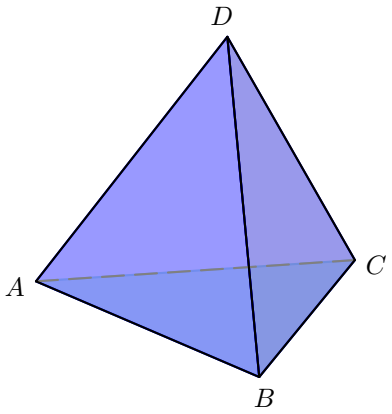
- https://cs.wikipedia.org/wiki/Patnáctka

Cvičení

1.3.1. Sestavte Cayleyho tabulky a) přímých b) přímých i nepřímých symetrií pravidelného čtyřstěnu na Obrázku 1.8.

1.3.2. Sestavte Cayleyho tabulku přímých symetrií (rotací) pravidelného trojbokého hranolu. Porovnejte ji s předchozími Tabulkami 0.5., 0.6. a 1.3.

1.3.3. Sestavte Cayleyho tabulky symetrií kvádru se třemi různými délkami hran $a < b < c$. Porovnejte ji s Cayleyho tabulkou symetrií čtverce.



Obrázek 1.8.: *Pravidelný čtyřstěn.*

Kapitola 2. Algebraické struktury s jednou operací

V této kapitole zavedeme nejběžnější a nejdůležitější algebraické struktury s jednou operací: grupoidy, pologrupy, monoidy a grupy.

2.1. Grupoidy

Nejjednodušší algebraickou strukturou je množina, na které máme definovanou operaci. Připomeňme, že operací na (neprázdné) množině A rozumíme takové zobrazení, které každé dvojici prvků $a, b \in A$ přiřadí prvek $c \in A$. Automaticky tak předpokládáme, že operace je *uzavřená* na A, tj. výsledek operace nemůže padnout mimo množinu A.

Definice Grupoid
Mějme neprázdnou množinu A s operací „$\circ$“ na A. Uspořádaná dvojice $(A, \circ)$ se nazývá *grupoid*. Množině A říkáme *nosič* nebo *nosná množina*.

Uvědomte si, že aby uspořádaná dvojice $(A, \circ)$ byla grupoidem, musí být splněny dvě vlastnosti:

(i) nosič A musí být neprázdná množina,
(ii) operace „$\circ$“ musí být *uzavřená* vzhledem k nosiči A. Jinak by se nejednalo o operaci na A. Tj. musí platit $\forall a, b \in A : a \circ b \in A$.

Proto libovolná neprázdná množina A spolu s libovolnou operací na této množině je grupoidem. V anglické literatuře se pro grupoid zpravidla používá termín „magma“.

Příklad 2.1. Uveďme několik jednoduchých příkladů množin s operací (grupoidů).

1) Množina celých čísel s operací obvyklého sčítání $(\mathbb{Z}, +)$ je grupoid, protože sčítání je operace na $\mathbb{Z}$.
2) Množina celých čísel s operací obvyklého odčítání $(\mathbb{Z}, -)$ je grupoid, protože odčítání je operace na $\mathbb{Z}$.
3) Množina celých čísel s operací obvyklého násobení $(\mathbb{Z}, \cdot)$ je grupoid, protože násobení je operace na $\mathbb{Z}$.
4) Množina všech symetrií n-úhelníka s operací skládání zobrazení $(D_n, \circ)$ je grupoid, protože skládání je operace na D_n.
5) Množina matic s m řádky a n sloupci s operací sčítání matic $(M_{m,n}, +)$ je grupoid.
6) Množina čtvercových matic řádu n s operací násobením matic $(M_{n,n}, \cdot)$ je grupoid.
7) Množina vektorů v $\mathbb{R}^3$ spolu s vektorovým součinem vektorů je grupoid.
8) Množina sudých celých čísel s operací obvyklého sčítání čísel $(\mathbb{S}, +)$ je grupoid, protože součet každých dvou sudých čísel je opět sudé číslo.
9) Označme $F_{\mathbb{R}}$ množinu všech funkcí, jejichž definiční obor je $\mathbb{R}$. Za operaci vezmeme klasické skládání funkcí „$\circ$“. Potom $(F_{\mathbb{R}}, \circ)$ je grupoid.
10) Je-li $F_{\mathbb{R}}$ je množina všech funkcí, jejichž definiční obor je $\mathbb{R}$, a za operaci vezmeme klasické sčítání funkcí „$+$“, tak $(F_{\mathbb{R}}, +)$ je grupoid.
11) Označme F_0 množinu všech spojitých reálných funkcí definovaných na $\mathbb{R}$, které prochází počátkem souřadné soustavy. Potom $(F_0, +)$ i $(F_0, \cdot)$ jsou grupoidy.

Příklad 2.2. Uveďme také několik příkladů, které grupoidem nejsou.

1) Množina přirozených čísel s operací běžného odečítání $(\mathbb{N}, -)$ není grupoid, neboť rozdíl dvou přirozených čísel nemusí být kladné celé číslo. Operace není uzavřená na množině $\mathbb{N}$.
2) Množina lichých celých čísel s operací obvyklého sčítání čísel $(\mathbb{L}, +)$ není grupoid, protože součet žádných dvou lichých čísel není liché číslo. Operace není uzavřená na množině $\mathbb{L}$.
3) Množina reálných čísel s operací obvyklého dělení $(\mathbb{R}, \div)$ není grupoid, protože výsledek dělení reálného čísla (reálným) číslem 0 není definovaný.
4) Množina iracionálních čísel s operací obvyklého násobení $(\mathbb{I}, \cdot) = (\mathbb{R} \setminus \mathbb{Q}, \cdot)$ není grupoid, protože „$\cdot$“ není operace na $\mathbb{I}$. Například $\sqrt{2} \in \mathbb{I}$, $\sqrt{2} \cdot \sqrt{2} = 2$, ale $2 \notin \mathbb{I}$ a proto operace není uzavřená na $\mathbb{I}$.
5) Množina vektorů $\mathbb{R}^n$ spolu se skalárním součinem vektorů není pro $n > 1$ grupoid. Výsledek skalárního součinu není vektor (uspořádaná n-tice reálných čísel), ale reálné číslo. Nejedná se o operaci na množině $\mathbb{R}^n$, operace musí být uzavřená na množině $\mathbb{R}^n$.

Příklad 2.3. Označme F_1 množinu všech spojitých reálných funkcí definovaných na $\mathbb{R}$, které prochází bodem $(0,1)$. Je $(F_1,+)$, kde „$+$“ je běžné sčítání funkcí, grupoid? Je $(F_1,\cdot)$, kde „$\cdot$“ je běžné násobení funkcí, grupoid?
Sečteme-li dvě funkce, které prochází bodem $(0,1)$, tak sečteme i jejich funkční hodnoty v bodě $x=0$. Dostaneme funkci, která prochází bodem $(0,2)$ a proto operace sčítání funkcí není uzavřená na množině F_1. $(F_1,+)$ není grupoid.

Naproti tomu $(F_1,\cdot)$ je grupoid. Vynásobíme-li dvě funkce, které prochází bodem $(0,1)$, tak vynásobíme i jejich funkční hodnoty v bodě $x=0$. Výsledná funkce opět prochází bodem $(0,1)$. ✓

Komutativita operace v grupoidu
Při počítání s běžnými čísly jsme zvyklí, že pořadí operandů obvykle nehraje roli. Je dobré si uvědomit, že v obecném grupoidu to může, ale nemusí být pravda.

Definice Komutativní grupoid
Řekneme, že grupoid $(A,\circ)$ je *komutativní*, právě tehdy, když

$$\forall a,b\in A: a\circ b=b\circ a.$$

Grupoidu s komutativní operací se říká *komutativní* nebo *abelovský* grupoid. Grupoidu, který není komutativní, budeme říkat *nekomutativní* grupoid.

Neutrální prvek grupoidu
Číslo nula hraje při obvyklém sčítání čísel výjimečnou roli, neboť přičtením nuly k prvku x dostaneme opět x. Analogickou roli hraje jednička při obvyklém násobení čísel. Nyní jejich společnou vlastnost popíšeme obecně.

Definice Neutrální prvek
Mějme grupoid $(A,\circ)$ a prvek $e\in A$. Prvek e se nazývá *neutrální prvek* (vzhledem k operaci „$\circ$“) právě tehdy, když

$$\forall a\in A: e\circ a=a\circ e=a.$$

Všimněte si, že v definici požadujeme splnění *obou* rovností $e\circ a=a$ i $a\circ e=a$. Operace „$\circ$“ nemusí být komutativní (jak jsme viděli v Příkladu 2.1.). I v nekomutativních grupoidech či pologrupách má smysl zkoumat neutrální prvky.

Příklad 2.4. U následujících příkladů grupoidů uvedeme, zda jsou komutativní a jaký je jejich neutrální prvek, pokud existuje.

1) $(\mathbb{Z},+)$ je komutativní (abelovský) grupoid. Neutrálním prvkem je číslo 0.
2) $(\mathbb{Z},-)$ je nekomutativní grupoid, který *nemá* neutrální prvek.
3) Dihedrální grupa $(D_n,\circ)$ (zavedli jsme ji na straně 37) je nekomutativní grupoid. Neutrálním prvkem je identita R_0.
4) $(M_{n,n},\cdot)$ je nekomutativní grupoid. Neutrálním prvkem je jednotková matice $E_{n,n}$.
5) Množina vektorů v $\mathbb{R}^3$ spolu s vektorovým součinem vektorů „$\times$“ je nekomutativní grupoid $(\mathbb{R}^3,\times)$. Neutrální prvek v tomto grupoidu není, neboť $\vec{0}$ jistě není neutrální prvek a $\forall\vec{v}\in\mathbb{R}^3,\vec{v}\neq\vec{0}:\vec{v}\times\vec{v}=\vec{0}\neq\vec{v}$.
6) Grupoid s jednoprvkovým nosičem a „libovolnou“ operací $(\{a\},\circ)$ je triviálně komutativní. Jediný prvek grupoidu je současně neutrálním prvkem.
7) Označme $F_{\mathbb{R}}$ množinu všech funkcí, jejichž definiční obor je $\mathbb{R}$. Potom $(F_{\mathbb{R}},\circ)$, kde „$\circ$“ je klasické skládání funkcí, je nekomutativní grupoid. Neutrálním prvkem je identické zobrazení $\iota:\mathbb{R}\to\mathbb{R}$ dané předpisem $\forall x\in\mathbb{R}:\iota(x)=x$.
8) Mějme množinu všech funkcí $F_{\mathbb{R}}$, jejichž definiční obor je $\mathbb{R}$. Za operaci vezmeme obvyklé sčítání funkcí „$+$“, tak $(F_{\mathbb{R}},+)$ je komutativní (abelovský) grupoid. Neutrálním prvkem je konstantní funkce daná předpisem $\forall x\in\mathbb{R}:f(x)=0$.
9) Grupoidy $(F_0,+)$ i $(F_0,\cdot)$ z Příkladu 2.1. jsou komutativní (abelovské) grupoidy. Neutrálním prvkem grupoidu $(F_0,+)$ je konstantní funkce daná předpisem $\forall x\in\mathbb{R}:f(x)=0$. Neutrálním prvkem grupoidu $(F_0,\cdot)$ je konstantní funkce daná předpisem $\forall x\in\mathbb{R}:f(x)=1$.

U předchozích příkladů jsme pracovali s grupoidy, jejichž operace nám byla víceméně známá – nepochybovali jsme, že se jedná o operaci. Následující příklad ukazuje, že je dobré mít na paměti, že ne každý předpis musí nutně být operací.

Příklad 2.5. Na množině $\mathbb{Z}$ máme dáno zobrazení f určené předpisem $f(a,b) = \frac{a+b}{ab}$. Určete, zda zobrazení f určuje operaci a) na $\mathbb{Z}$, tj. za předpokladu $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$, b) na $\mathbb{Q} \setminus \{0\}$, tj. za předpokladu $f : (\mathbb{Q} \setminus \{0\}) \times (\mathbb{Q} \setminus \{0\}) \to (\mathbb{Q} \setminus \{0\})$.

a) Snadno nahlédneme, že se o operaci nejedná. Měli bychom být schopni určit hodnotu operace pro *libovolnou* dvojici prvků z množiny $\mathbb{Z} \times \mathbb{Z}$. Avšak například pro $x = 0$ nebo $y = 0$ není výsledek operace definován. Navíc pro řadu nenulových dvojic prvků není $\frac{a+b}{ab}$ celé číslo, proto se nejedná o operaci.

b) Pro nenulová racionální čísla $a, b \in \mathbb{Q} \setminus \{0\}$ můžeme psát $a = \frac{p}{q}$, $b = \frac{r}{s}$, kde $p, r \in \mathbb{Z} \setminus \{0\}$ a $q, s \in \mathbb{N}$. Potom

$$\frac{a+b}{ab} = \frac{\frac{p}{q} + \frac{r}{s}}{\frac{p}{q} \cdot \frac{r}{s}} = \frac{\frac{ps+qr}{qs}}{\frac{pr}{qs}} = \frac{ps+qr}{pr}$$

Protože žádné z čísel p, q, r ani s není nulové, mohli jsme krátit a výsledný zlomek nemá nulu ve jmenovateli. Platí tedy $\frac{a+b}{ab} \in \mathbb{Q}$. Avšak pro $b = -a$ je výsledek nulový a o operaci se proto *nejedná*. ✓

Vlastnost prvku „být neutrální“ je moc pěkná. Třeba bychom si přáli mít takových prvků v grupoidu více. Následující věta ukazuje, že se to nemůže stát.

Věta 2.1. *V grupoidu existuje nejvýše jeden neutrální prvek.*

Důkaz. Postupujeme přímo. Pokud v grupoidu žádný neutrální prvek neexistuje, tak tvrzení platí.

Předpokládejme dále, že máme dva neutrální prvky e_1, e_2. Protože e_1 je neutrální prvek grupoidu, tak platí $e_1 \circ e_2 = e_2$. Podobně $e_1 \circ e_2 = e_1$, protože e_2 je neutrální prvek grupoidu. Odtud porovnáním ihned plyne $e_1 = e_1 \circ e_2 = e_2$ a neutrální prvek je jediný. □

Příklad 2.6. Najděte neutrální prvek a) v grupoidu $(\mathbb{S}, +)$, b) v grupoidu $(\mathbb{N}, +)$.

a) Dvojice $(\mathbb{S}, +)$ je grupoidem, neboť operace je uzavřená (součtem dvou sudých celých čísel je opět sudé číslo). Víme, že při obvyklém sčítání je neutrálním prvkem číslo 0.

b) Dvojice $(\mathbb{N}, +)$ je grupoidem, neboť operace je uzavřená (součtem dvou přirozených čísel je přirozené číslo), avšak neobsahuje neutrální prvek 0. ✓

V grupoidu celých čísel s operací sčítání je neutrálním prvkem číslo 0, v grupoidu celých čísel s operací násobení je neutrálním prvkem číslo 1. Neutrální prvky jsou různé, což není v rozporu s tvrzením Věty 2.1., protože $(\mathbb{Z}, +)$ a $(\mathbb{Z}, \cdot)$ jsou různé grupoidy.

Cvičení

2.1.1. Najděte příklad grupoidu, který není komutativní.

2.1.2. Je množina sudých čísel s operací násobení grupoidem? Pokud ano, a) má neutrální prvek? b) je komutativní?

2.1.3. Které z následujících uspořádaných dvojic tvoří grupoid? a) $(\mathbb{I}, \cdot)$, kde „$\cdot$“ je restrikce násobení reálných čísel na množinu $\mathbb{I}$ b) $(\mathbb{Q} \setminus \{0\}, \cdot)$.

2.1.4. Najděte příklad grupoidu, který je komutativní, ale není asociativní.

2.1.5. Najděte příklad grupoidu, který je asociativní, ale není komutativní.

2.1.6. Rozborem Cayleyho tabulky zdůvodněte, že v každém grupoidu může existovat nejvýše jeden neutrální prvek.

2.1.7. Zvolme libovolnou neprázdnou podmnožinu $A \subseteq \mathbb{N}$. Zvolme libovolný prvek $a \in A$. Má grupoid s nosnou množinou A a s konstantní operací $\forall x, y \in A : x * y = a$ neutrální prvek?

2.1.8. Podle Příkladu 2.1. víme, že množina vektorů v $\mathbb{R}^3$ spolu s vektorovým součinem vektorů je grupoid $(\mathbb{R}^3, \times)$. Má tento grupoid neutrální prvek?

2.1.9. Mějme množinu A a její potenční množinu 2^A. Dokažte nebo vyvraťte: a) $(2^A, \cup)$ je grupoid, b) $(2^A, \cap)$ je grupoid.

2.1.10.$^\heartsuit$ Kolik existuje různých grupoidů $(G, \circ)$, jestliže nosič G má n prvků?

2.2. Pologrupy

Velmi přirozeným požadavkem je, aby operace „$\circ$“ na množině A v grupoidu $(A, \circ)$ byla asociativní, tj. aby platilo

$$\forall a, b, c \in A : a \circ (b \circ c) = (a \circ b) \circ c.$$

Grupoidy, jejichž operace je asociativní, jsou jednou z nejpraktičtějších algebraických struktur. Budeme jim říkat pologrupy.

Definice Pologrupa
Grupoid $(A, \circ)$ se nazývá *pologrupa* právě tehdy, když operace „$\circ$“ je *asociativní*, tj. platí

(i) $\forall a, b, c \in A : a \circ (b \circ c) = (a \circ b) \circ c.$ (asociativita)

Uvědomte si, že aby $(A, \circ)$ byla pologrupa, musí být splněný tři vlastnosti: jednak, aby $(A, \circ)$ byl grupoid, musí množina A být neprázdná a operace „$\circ$“ musí být uzavřená na množině A; navíc musí být operace „$\circ$“ asociativní.

Příklad 2.7. Uvedeme několik příkladů pologrup.

1) $(\mathbb{Z}, +)$ je komutativní (abelovská) pologrupa s neutrálním prvkem 0, neboť sčítání celých čísel je asociativní.
2) $(D_n, \circ)$ je nekomutativní pologrupa s neutrálním prvkem R_0.
3) $(M_{n,n}, \cdot)$ je nekomutativní pologrupa s neutrálním prvkem $E_{n,n}$, kde $E_{n,n}$ značí jednotkovou matici.
4) Grupoid s jednoprvkovým nosičem A a s „libovolnou“ operací „$\circ$“ je pologrupa, neboť operace je triviálně asociativní (Tabulka 2.4.).
5) Mějme grupoid $(A, \circ)$, ve kterém pro každé $a, b \in A$ položíme $a \circ b = c$, kde c je libovolný pevně zvolený prvek A. Potom $(A, \circ)$ je pologrupa (Cvičení 2.2.1.).
6) Označme $F_{\mathbb{R}}$ množinu všech funkcí, jejichž definiční obor je $\mathbb{R}$. Potom $(F_{\mathbb{R}}, \circ)$ je nekomutativní pologrupa s neutrálním prvkem ι (identické zobrazení), neboť skládání zobrazení je asociativní podle Lemmatu 0.11.
7) Je-li $F_{\mathbb{R}}$ je množina všech funkcí, jejichž definiční obor je $\mathbb{R}$, a za operaci vezmeme obvyklé sčítání funkcí „$+$“, tak $(F_{\mathbb{R}}, +)$ je komutativní pologrupa s neutrálním prvkem f_0, kde funkce f_o je definována tak, že $\forall x \in \mathbb{R} : f_0(x) = 0$ (konstantní funkce), neboť sčítání funkcí je asociativní.
8) Grupoidy spojitých reálných funkcí $(F_0, +)$ i $(F_0, \cdot)$ z Příkladu 2.1. jsou komutativní (abelovské) pologrupy, neboť sčítání i násobení funkcí jsou asociativní operace.

Příklad 2.8. Uveďme několik příkladů grupoidů, které asociativní nejsou.

1) Množina celých čísel s operací obvyklého odčítání $(\mathbb{Z}, -)$ pologrupou není, protože například $1 - (2 - 3) = 1 - (-1) = 2$, avšak $(1 - 2) - 3 = (-1) - 3 = -4$.
2) Množina vektorů v $\mathbb{R}^3$ spolu s vektorovým součinem vektorů není pologrupa, neboť vektorový součin není asociativní operace. Mějme například vektory $\vec{a} = (1, 1, 0)$, $\vec{b} = (0, 1, 1)$, $\vec{c} = (1, 0, 1)$, platí

$$(\vec{a} \times \vec{b}) \times \vec{c} = (1, -1, 1) \times (1, 0, 1) = (-1, 0, 1),$$
$$\vec{a} \times (\vec{b} \times \vec{c}) = (1, 1, 0) \times (1, 1, -1) = (-1, 1, 0).$$

Vidíme, že operace „$\times$“ není asociativní.

Příklad 2.9. Mějme grupoid na množině $A = \{0, 1\}$ určený Cayleyho Tabulkou 2.1. s operací „$\circ$“. Rozhodněte, zda se jedná o pologrupu.

$\circ$	0	1
0	0	1
1	0	0

Tabulka 2.1.: *Cayleyho tabulka grupoidu.*

Jedná se o grupoid, protože operace je evidentně uzavřená. Operace však není asociativní, protože

$$1 \circ (0 \circ 1) = 1 \circ 1 = 0$$
$$(1 \circ 0) \circ 1 = 0 \circ 1 = 1.$$

Grupoid $(A, \circ)$ proto není pologrupou. ✓

Příklad 2.10. Na straně 34 jsme popsali symetrie trojúhelníka pomocí permutací množiny $\{A, B, C\}$. Asociativita skládání permutací vyplývá z Lemmatu 0.11. Asociativitu skládání demonstrujeme složením tří vybraných symetrií.

$$R_{240} = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \quad Z_A = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \quad Z_B = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$$

Ukažte, že $(Z_B \circ R_{240}) \circ Z_A = Z_B \circ (R_{240} \circ Z_A)$. Dále ukažte, že skládání symetrií trojúhelníka není komutativní.
Oba vztahy upravíme.

$$\begin{aligned}(Z_B \circ R_{240}) \circ Z_A &= \left(\begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \circ \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}\right) \circ \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} \\ &= \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} \circ \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}\end{aligned}$$

$$\begin{aligned}Z_B \circ (R_{240} \circ Z_A) &= \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \circ \left(\begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} \circ \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}\right) \\ &= \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \circ \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}\end{aligned}$$

Asociativita nezaručuje komutativitu, například $Z_B \circ R_{240} = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} \circ \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$, ale $R_{240} \circ Z_B = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$. ✓

Otázky:

- Kolik operací trojic prvků je nutno porovnat pro ověření asociativity operace podle definice pro množinu s n prvky?
- Kolik operací trojic je nutno porovnat pro ověření asociativity podle definice v případě, že grupoid je komutativní?

Cvičení

2.2.1.$^{\heartsuit}$ *Mějme grupoid $(A, \circ)$, ve kterém pro každé $a, b \in A$ položíme $a \circ b = c$, kde c je libovolný pevně zvolený prvek A. Ukažte, že $(A, \circ)$ je pologrupa.*

2.2.2.$^{\heartsuit}$ *Ukažte, že operace „$\circ$“ v grupoidu daném Cayleyho tabulkou 2.2. je asociativní.*

$\circ$	1	2	3
1	1	2	3
2	1	2	3
3	1	2	3

Tabulka 2.2.: Grupoid $(\{1, 2, 3\}, \circ)$.

$\circ$	0	1	2	3	4	5
0	0	0	2	3	0	5
1	0	0	2	3	1	5
2	2	2	2	3	2	5
3	3	3	3	3	3	5
4	0	1	2	3	4	5
5	5	5	5	5	5	5

Tabulka 2.3.: Tabulka grupoidu.

2.2.3. Ukažte, že neutrální prvek grupoidu $(G, \circ)$ nemůže porušit asociativitu, tj. rovnost $(x \circ y) \circ z = x \circ (y \circ z)$ je splněna vždy, jestliže alespoň jeden z prvků x, y, z je neutrální prvek.

2.2.4. Máme grupoid $(G, \circ)$ s nosnou množinou $M = \{0, 1, 2, 3, 4, 5\}$ daný Tabulkou 2.3. a) Je tento grupoid komutativní? b) Je tento grupoid asociativní? Dokažte svá tvrzení.*

2.2.5. Máme dán konečný grupoid $(G, \circ)$, jehož nosná množina má n prvků. Abychom ověřili, že operace „$\circ$“ je asociativní, musíme ověřit, že $\forall a, b, c \in G$ platí $a \circ (b \circ c) = (a \circ b) \circ c$. a) Kolik trojic musíme ověřit? b) Kolik trojic musíme ověřit v případě, že operace je komutativní?

2.2.6. Ukažte, že pro každou množinu A s alespoň čtyřmi prvky existuje grupoid, ve kterém právě jedna trojice prvků poruší asociativitu.*

2.2.7. Operace „$\circ$“ v grupoidu $(G, \circ)$ se nazývá idempotentní*, jestliže pro každý prvek $g \in G$ platí $g \cdot g = g$. Ukažte, že a) operace „$\cup$“ klasického sjednocení množin je idempotentní v grupoidu $(I, \cup)$, kde I je nějaký konečný systém množin, b) operace klasického sčítaní není idempotentní v pologrupě $(\mathbb{Z}, +)$.*

2.2.8. Prvek $g \in G$ grupoidu $(G, \circ)$ se nazývá idempotentní*, jestliže platí $g \cdot g = g$. a) Ukažte, že neutrální prvek grupoidu je vždy idempotentní. b) Najděte příklad grupoidu, který obsahuje alespoň dva idempotentní prvky i prvky, které nejsou idempotentní.*

2.3. Monoidy

Každou pologrupu, ve které kromě uzavřenosti a asociativity operace bude navíc existovat neutrální prvek, nazveme monoid.

Definice Monoid
Grupoid $(A, \circ)$ se nazývá *monoid* právě tehdy, když

(i) $\forall a, b, c \in A : a \circ (b \circ c) = (a \circ b) \circ c$, (asociativita)
(ii) $\exists e \in A \, \forall a \in A : e \circ a = a \circ e = a$. (existence neutrálního prvku)

Z definice je ihned zřejmé, že monoid je speciální případ pologrupy. Monoid bychom mohli definovat i jako takovou pologrupu, ve které existuje neutrální prvek.

Je dobré připomenout, že aby uspořádaná dvojice $(A, \circ)$ byla monoidem, tak musí být splněný čtyři vlastnosti: jednak, aby dvojice $(A, \circ)$ byla grupoidem, musí množina A být neprázdná a operace „$\circ$“ musí být uzavřená na množině A. Navíc musí být operace „$\circ$“ asociativní a v grupoidu musí existovat neutrální prvek.

Příklad 2.11. Uvedeme několik jednoduchých příkladů monoidů včetně určení jejich neutrálního prvku.

1) $(\mathbb{Z}, +)$ je monoid. Už víme, že se jedná o komutativní pologrupu, neutrálním prvek je číslo 0.
2) $(\mathbb{N}, \cdot)$ je monoid. Už víme, že se jedná o komutativní pologrupu, neutrálním prvek je číslo 1.
3) $(M_{n,n}, \cdot)$ (čtvercové matice řádu n s operací násobení matic) je nekomutativní monoid. Už víme, že se jedná o pologrupu, neutrálním prvkem je jednotková matice $E_{n,n}$.
4) $(F_{\mathbb{R}}, \circ)$ (reálné funkce definované na $\mathbb{R}$ s operací skládání) je monoid, neutrální prvek je funkce identity $\iota(x) = x$, což snadno ověříme. Pro každé $f \in F$ vyčíslíme $\iota \circ a$, dostaneme $\forall x \in \mathbb{R} : (\iota \circ a)(x) = \iota(a(x)) = a(x)$, takže $\iota \circ a = a$. Podobně vyčíslíme $a \circ \iota$, dostaneme $\forall x \in \mathbb{R} : (a \circ \iota)(x) = a(\iota(x)) = a(x)$, takže $a \circ \iota = a$.

Příklad 2.12. Uvedeme také několik příkladů struktur, které monoidem nejsou.

1) $(\mathbb{N}, +)$ není monoid, v pologrupě $(\mathbb{N}, +)$ není neutrální prvek.
2) $(\mathbb{Z}, -)$ není monoid. Operace není asociativní, protože například $(1-2)-3 = -4 \neq 2 = 1-(2-3)$.
3) Označme A libovolnou množinu s alespoň dvěma prvky. Zvolme libovolný prvek $a \in A$ a pro každé $x, y \in X$ definujeme operaci $x \circ y = a$ (konstantní operace). Dvojice $(A, \circ)$ je komutativní asociativní grupoid, avšak nemá neutrální prvek, protože označíme-li nějaký prvek $b \in A, b \neq a$, tak prvek a není neutrálním v $(A, \circ)$, protože $a \circ b = a \neq b$ a ani prvek b není neutrální, protože $b \circ b = a \neq b$. Proto $(A, \circ)$ je pologrupa, která není monoidem.
4) Množina vektorů v $\mathbb{R}^3$ spolu s vektorovým součinem vektorů je grupoid $(\mathbb{R}^3, \times)$, který není pologrupou, neboť operace není asociativní (Příklad 2.8.), a navíc ani nemá neutrální prvek (Cvičení 2.1.8.).

Zatímco v grupoidu neutrální prvek existovat může, ale nemusí, tak v monoidu je jeho existence vyžadována z definice. Můžeme vyslovit silnější tvrzení, než byla Věta 2.1.

Věta 2.2. O jednoznačnosti neutrálního prvku
Mějme pologrupu $(A, \circ)$ s neutrálním prvkem e. $(A, \circ)$ je monoid a prvek e je jediný neutrální prvek v pologrupě vzhledem k operaci „$\circ$“.

Důkaz. Podle předpokladu máme v pologrupě $(A, \circ)$ neutrální prvek a pologrupa $(A, \circ)$ s neutrálním prvkem je monoid ihned z definice monoidu. Podle Věty 2.1. víme, že neutrální prvek je určen jednoznačně. □

Věta 2.2. je vlastně důsledkem Věty 2.1., pro její význam ji přesto budeme nazývat větou.

Cvičení

2.3.1. Rozhodněte, které z následujících příkladů jsou monoidy. a) $(\mathbb{I}, +)$, kde „$+$“ je restrikce sčítání reálných čísel na množinu $\mathbb{I}$, b) $(\mathbb{Z}, +)$, kde „$+$“ je obvyklé sčítání celých čísel.

2.3.2. Zavedeme následující definici: „Stereoid“ je takový grupoid $(A, \circ)$, ve kterém máme dva různé neutrální prvky e_1, e_2, tj. pro každé $a \in A$ platí $a \circ e_1 = e_1 \circ a = a$ a současně $a \circ e_2 = e_2 \circ a = a$. Ukažte, že operace „$\circ$“ nemůže být a) komutativní ani b) asociativní. Najdete příklad stereoidu? Jaký je hlavní problém tohoto tvrzení?

2.3.3. Pro libovolné $n \in \mathbb{N}$ mějme množinu $A = [1, n]$. Na množině A definujeme operaci „$\circ$“ předpisem $\forall a, b \in A : a \circ b = \max\{a, b\}$. Ukažte, že dvojice $(A, \circ)$ je monoidem.

2.3.4. Sestavte Cayleyho tabulko monoidu ze Cvičení 2.3.3.

2.3.5. Pro libovolné $n \in \mathbb{N}$, $n \geq 2$ najděte příklad monoidu s n prvky, ve kterém žádný jiný prvek než neutrální nemá inverzi.

2.3.6. Ukažte, že triviální grupoid $(\{a\}, \circ)$ s „libovolnou“ operací „$\circ$“ (Tabulka 2.4.) je monoid.

$\circ$	a
a	a

Tabulka 2.4.: Triviální grupoid $(\{a\}, \circ)$.

2.3.7. Mějme libovolnou pologrupu $(G, \circ)$. Ukažte, že vždy je možno přidat nový prvek e (tj. $e \notin G$) tak, aby $(G \cup \{e\}, *)$ byl monoid s neutrálním prvkem e, přičemž pro každé $x, y \in G$ položíme $x * y = x \circ y$. Pokud $(G, \circ)$ byl monoid s neutrálním prvkem f, co můžeme říci o prvku f v monoidu $(G \cup \{e\}, *)$?

2.3.8. Mějme Cayleyho tabulku 2.5. Vysvětlete, proč tabulka nepopisuje monoid. Poznámka: *Výraz $0 \circ \infty$ je neurčitý výraz. I kdybychom položili $0 \circ \infty = 1$, tak cvičení ukazuje, že některé běžné početní operace nebudou dávat očekávané výsledky.*

$\circ$	0	1	∞
0	0	0	1
1	0	1	∞
∞	1	∞	∞

Tabulka 2.5.: Tabulka operace v grupoidu $(A, \circ)$.

2.3.9. Mějme grupoid $(A, \circ)$. Vysvětlete, jaký je rozdíl mezi definicí neutrálního prvku $\exists e \in A \forall a \in A : e \circ a = a \circ e = a$ a definicí s prohozeným pořadím kvantifikátorů $\forall a \in A \exists e \in A : e \circ a = a \circ e = a$.

2.3.10. Pro každé $n \in \mathbb{N}$ najděte příklad alespoň n různých pologrup, které nejsou monoidem.

2.3.11. Označme $G = \{a + b\sqrt{2} : a, b \in \mathbb{Z}, (a, b) \neq (0, 0)\}$. Dále nechť „$\cdot$“ je restrikce obvyklého násobení reálných čísel na množinu G. Ukažte, že $(G, \cdot)$ je monoid.

2.4. Grupy

Než přistoupíme k definici grupy, popíšeme další důležitou vlastnost prvků v algebraických strukturách s jednou operací.

Inverzní prvky

Budeme zkoumat, zda k vybranému případně každému prvku monoidu existuje prvek v jistém smyslu opačný nebo převrácený. Řešíme-li v $\mathbb{R}$ například rovnici

$$x + 2 = 0,$$

dobře víme, že řešením je číslo $x = -2$, které umíme vyjádřit „přičtením opačného prvku -2 k oběma stranám rovnice“. Podobně při řešení rovnice

$$2x = 1$$

v $\mathbb{R}$ vyjádříme hledané řešení tím, že rovnici vynásobíme převrácenou hodnotou koeficientu 2, tj. jednou polovinou. Jestliže ale v $\mathbb{R}$ hledáme řešení rovnice

$$0x = 1,$$

násobit převrácenou hodnotou koeficientu nemůžeme, protože 0 nemá převrácenou hodnotu. A konečně, jestliže řešíme soustavu rovnice popsanou maticovou rovnicí

$$Ax = b$$

a pokud existuje inverzní matice A^{-1} a známe ji, můžeme ihned vyjádřit řešení $x = A^{-1}b$. Má smysl se ptát, ke kterým prvkům existuje a ke kterým prvkům neexistuje opačný nebo převrácený prvek. Pokud existuje, budeme mu říkat inverzní prvek.

Definice Inverzní prvek

Mějme grupoid $(A, \circ)$ s neutrálním prvkem e vzhledem k operaci „$\circ$“. *Inverzním prvkem k prvku $a \in A$* (vzhledem k operaci „$\circ$“) rozumíme takový prvek $b \in A$, pro který platí obě následující rovnosti.

$$a \circ b = e, \quad b \circ a = e$$

Všimněte si, že v definici opět požadujeme splnění *obou* rovností $a \circ b = e$ i $b \circ a = e$, protože operace „$\circ$“ nemusí být komutativní. I v nekomutativních grupoidech má smysl hledat inverzní prvky. Například Cayleyho tabulka symetrií rovnostranného trojúhelníka (Tabulka 1.3.) odpovídá algebraické struktuře s nekomutativní operací, kde ke každému prvku existuje inverzní prvek.

Příklad 2.13. Uveďme několik jednoduchých příkladů grupoidů a inverzí jejich prvků.

1) Máme-li množinu celých čísel s operací obvyklého sčítání $(\mathbb{Z}, +)$, tak neutrálním prvkem je číslo 0 a ke každému celému číslu $a \in \mathbb{Z}$ existuje inverzní prvek $-a$. Zejména číslo 0 je inverzí samo k sobě.
2) Množina celých čísel s operací obvyklého násobení $(\mathbb{Z}, \cdot)$ je monoid s neutrálním prvek 1; inverze existují pouze ke dvěma prvkům, k neutrálnímu prvku $1^{-1} = 1$ a k číslu -1 je inverzí také samotné číslo -1.
3) V monoidu čtvercových matic řádu n s operací násobením matic $(M_{n,n}, \cdot)$ je neutrálním prvkem jednotková matice $E_{n,n}$ a inverze A^{-1} existují pouze k regulárním maticím A.
4) Podle Příkladu 2.7. víme, že množina všech funkcí s definičním oborem $\mathbb{R}$ a s operací obvyklého sčítání funkcí „$+$“ je komutativní pologrupa $(F_{\mathbb{R}}, +)$ s neutrálním prvkem f_0, kde funkce f_o je konstantní funkce $\forall x \in \mathbb{R} : f_0(x) = 0$. Inverzním prvkem ke každé funkci $f \in F$ je funkce $-f$.

Příklad 2.14. Uveďme několik jednoduchých příkladů grupoidů, ve kterých neexistují inverze.

1) V pologrupě $(\mathbb{S}, \cdot)$ neexistuje neutrální prvek, a proto nemá smysl definovat inverzní prvky.
2) Obvyklé odčítání celých čísel tvoří neasociativní grupoid $(\mathbb{Z}, -)$, ve kterém nemá smysl definovat inverzní prvky, neboť nemá neutrální prvek. Číslo 0 není neutrálním prvkem, neboť pro nenulový prvek a je $0 - a = -a \neq a$.
3) Pologrupa $(\mathbb{R}_0^+, +)$ tvoří komutativní pologrupu s neutrálním prvkem 0, avšak žádný nenulový prvek $x \in \mathbb{R}^+$ nemá inverzi, neboť $-x \notin \mathbb{R}^+$.

Příklad 2.15. Najdeme inverzní prvky ke všem prvkům v dihedrální grupě $(D_3, \circ)$. Využijeme Cayleyho tabulku 1.3.
Z Tabulky 1.3. ihned vidíme, že neutrálním prvkem je R_0. Dále vidíme, že $R_0^{-1} = R_0$, $R_{120}^{-1} = R_{240}$, $R_{240}^{-1} = R_{120}$, $Z_A^{-1} = Z_A$, $Z_B^{-1} = Z_B$ a $Z_C^{-1} = Z_C$. ✓

Příklad 2.16. Cayleyho tabulka 2.6. udává příklad monoidu s neutrálním prvkem 1 (Cvičení 2.4.14.). Najdeme inverze ke všem prvkům, pokud existují.

$\circ$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	2

Tabulka 2.6.: *Tabulka operace v monoidu* $(A, \circ)$.

Prvky 0 a 2 nemají inverzi, protože $0 \circ a \neq 1$ ani $2 \circ a \neq 1$ pro žádné $a \in \{0, 1, 2\}$. Naproti tomu neutrální prvek 1 je inverzní sám k sobě, protože $1 \circ 1 = 1$. To znamená, že obecně k některým prvkům inverze existovat mohou, zatímco k jiným nemusí. Ve Cvičení 2.4.2. ukážeme, že v každém monoidu je neutrální prvek inverzní sám k sobě. ✓

O jednoznačnosti inverzního prvku v monoidu
Všimněte si, že v definici inverzního prvku na straně 48 požadujeme existenci neutrálního prvku v grupoidu $(A, \circ)$. Nevyžadujeme, aby $(A, \circ)$ byla asociativní. To znamená, že inverzní prvky můžeme hledat i v algebraických strukturách, které nejsou monoidem. Například grupoid uvedený v Tabulce 2.7. má neutrální prvek 1. K prvku 2 najdeme dva inverzní prvky: 2 i 3, což jsou dva inverzní prvky i k prvku 3. Ale grupoid uvedený v Tabulce 2.7. není asociativní, například $(2 \circ 2) \circ 3 = 1 \circ 3 = 3$, ale $2 \circ (2 \circ 3) = 2 \circ 1 = 2$.

$\circ$	1	2	3
1	1	2	3
2	2	1	1
3	3	1	1

Tabulka 2.7.: *Grupoid, kde k některým prvkům existuje více inverzí.*

Dále nesmíme zapomenout, že v obecném grupoidu nemusí být neutrální prvek, nesmíme (chybně) spoléhat na vžité označení „1“. Například operace daná Tabulkou 2.8. je triviálně asociativní, avšak uvedený grupoid nemá neutrální prvek. Nemůžeme proto tvrdit, že prvky 1, 2 a 3 jsou navzájem inverzní, neboť inverzní prvky v takovém grupoidu nejsou definovány.

$\circ$	1	2	3
1	1	1	1
2	1	1	1
3	1	1	1

Tabulka 2.8.: *Asociativní grupoid bez neutrálního prvku.*

Jestliže k nějakému prvku existuje více inverzí, tak příslušná operace na množině není asociativní (a proto nemáme monoid). Následující věta ukazuje, že asociativita operace „$\circ$“ vynutí jednoznačnost inverzních prvků: v monoidu existuje ke každému prvku nejvýše jeden inverzní prvek.

Věta 2.3. *Mějme monoid $(A, \circ)$ s neutrálním prvkem e. Pro každé $a \in A$ existuje nejvýše jeden inverzní prvek.*

Důkaz. Mějme prvek a v monoidu $(A, \circ)$. Jestliže k prvku a neexistuje inverze, tvrzení platí. Dále postupujeme přímo. Označme b_1 a b_2 inverzní prvky k prvku a v monoidu $(A, \circ)$.

$$b_1 = b_1 \circ e = b_1 \circ (a \circ b_2) = (b_1 \circ a) \circ b_2 = e \circ b_2 = b_2.$$

Při úpravě jsme postupně využili: existenci neutrálního prvku e, dále vlastnost, že b_2 je inverzí k a, potom asociativitu operace, dále vlastnost, že b_1 je inverze k prvku a a nakonec definici neutrálního prvku. Proto k libovolnému prvku a neexistuje více různých inverzních prvků vzhledem k operaci „$\circ$“. □

Grupa

Nyní je čas vyslovit ústřední definici celého kurzu: definici grupy. Na grupy se můžeme dívat jako zobecnění obvyklého sčítání celých čísel, nosič i operace mohou být libovolné, ale budeme vyžadovat některé „pěkné“ vlastnosti. Monoid je asociativní grupoid s neutrálním prvek a pokud navíc budeme požadovat existenci inverze ke každému prvku, dostaneme grupu.

Definice Grupa

Grupoid $(G, \circ)$ se nazývá *grupa* právě tehdy, když

(i) $\forall a, b, c \in G : a \circ (b \circ c) = (a \circ b) \circ c$, (asociativita)
(ii) $\exists e \in G \, \forall a \in G : e \circ a = a \circ e = a$, (existence neutrálního prvku)
(iii) $\forall a \in G \, \exists b \in G : a \circ b = b \circ a = e$, kde e je neutrální prvek vzhledem k operaci „$\circ$“. (existence inverze)

Prvek b se nazývá *inverzní k prvku* a (vzhledem k operaci „$\circ$“) a značíme jej a^{-1}, případně $-a$.

Značení a^{-1} používáme, pokud operace „$\circ$“ je analogií běžného násobení. Značení $-a$ používáme, pokud operace „$\circ$“ je analogií běžného sčítání, a říkáme *opačný* prvek k prvku a. Často budeme inverznímu prvku k prvku a říkat stručně „inverze k a“. Značení je korektní, neboť podle Věty 2.3. je v grupě inverze k prvku a určena jednoznačně.

Poznámka 2.1. Všimněte si, že v grupoidu daném Cayleyho tabulkou 2.7. existují k prvkům 2 i 3 dvě inverze (což se v monoidu stát nemůže). Je nešikovné zapisovat $2^{-1} = 2$ a $2^{-1} = 3$, protože by mohl vzniknout dojem, že $2 = 3$. O něco lepší je pracovat s množinou inverzí $2^{-1} \in \{2, 3\}$, to však řeší pouze situace, kde nebudeme pracovat s *prvkem* 2^{-1}. Nejkorektnější je slovní formulace, že inverzní prvky k 2 jsou 2 a 3 a nepoužívat značení 2^{-1}, které si vyhradíme pro případ, kdy jsou inverzní prvky určeny jednoznačně (například v grupě). V dalším textu budeme označení a^{-1} používat pouze v případě, že inverzní prvek je určen jednoznačně.

Připomínáme, že aby uspořádaná dvojice $(G, \circ)$ byla grupou, tak musí být splněno pět vlastností: jednak, aby $(G, \circ)$ byl grupoid, musí množina A být neprázdná a operace „$\circ$“ musí být uzavřená na množině G. Navíc musí být operace „$\circ$“ asociativní, v grupoidu musí existovat neutrální prvek a ještě ke každému prvku musí existovat prvek inverzní.

V dalším textu budeme operaci v obecné grupě zpravidla označovat „$\cdot$“ a používat multiplikativní terminologii.

Příklad 2.17. Uvedeme několik jednoduchých příkladů grup včetně určení neutrálního prvku.

1) $(\mathbb{Z}, +)$ je komutativní grupa. Už víme, že se jedná o monoid s neutrálním prvkem 0, inverzní k prvku $a \in \mathbb{Z}$ je opačný prvek $-a$.
2) $(\mathbb{Q}, +)$ a $(\mathbb{R}, +)$ jsou komutativní grupy se stejným zdůvodněním jako v předchozím příkladu. Opačným prvkem k prvku x je vždy prvek $-x$.
3) $(\mathbb{R} \setminus \{0\}, \cdot)$ je komutativní grupa. Násobení nenulových čísel je grupoid, operace je komutativní i asociativní, neutrálním prvkem je číslo 1 a inverzí k (nenulovému) prvku a je prvek $\frac{1}{a}$.
4) $((0, \infty), \cdot)$ je komutativní grupa. Násobení kladných čísel je jistě grupoid, operace je (stejně jako u předchozího příkladu) komutativní i asociativní, neutrálním prvkem je číslo 1 a inverzí ke kladnému prvku a je (kladný) prvek $\frac{1}{a}$.
5) Symetrie rovnostranného trojúhelníka (Tabulka 1.3.) tvoří grupu. Už víme, že se jedná o monoid, R_{120} a R_{240} jsou navzájem inverzní, ostatní prvky jsou inverzí sami sobě (Příklad 2.15.).

6) Symetrie libovolného pravidelného n-úhelníka tvoří dihedrální grupu $(D_n, \circ)$. Neutrálním prvkem je otočení R_0.
7) $(\mathbb{Z}_4, +)$, $(\mathbb{Z}_5, +)$ (sčítání modulo 4 nebo modulo 5) jsou grupy s neutrálním prvkem $\overline{0}$.
8) $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ (násobení nenulových čísel modulo 5) tvoří grupu. Neutrálním prvkem je $\overline{1}$.
9) $(M^*_{n,n}, \cdot)$, kde $M^*_{n,n} = \{A \in M_{n,n} : \det(A) \neq 0\}$, regulární čtvercové matice řádu n s operací násobení matic tvoří grupu. Neutrálním prvkem je jednotková matice E_n.

Příklad 2.18. Uvedeme také několik příkladů, které grupou nejsou.

1) $(\mathbb{N}, +)$ není grupou, protože není ani monoidem, neboť v pologrupě $(\mathbb{N}, +)$ není neutrální prvek.
2) $(\mathbb{Z}, -)$ není grupa protože operace „$-$“ není asociativní.
3) $(\mathbb{N}, \cdot)$ není grupa. Už víme, že se jedná o monoid, neutrálním prvek je číslo 1, avšak k číslům větším než 1 neexistují inverze.
4) $(\mathbb{R}, \cdot)$ není grupa, protože k prvku 0 neexistuje inverze.
5) $(\mathbb{R}^*, \cdot)$, kde $\mathbb{R}^*$ je rozšířená množina reálných čísel včetně ∞ a $-\infty$, není grupa. Dokonce, i pokud bychom dodefinovali $0 \cdot \infty = 1$, dostaneme $0^{-1} = \infty$ a $\infty^{-1} = 0$, tak stále není jasná inverze k $-\infty$. Inverzí už nemůže být 0, protože inverze jsou určeny jednoznačně.
6) Množina vektorů v $\mathbb{R}^3$ spolu s vektorovým součinem vektorů je grupoid $(\mathbb{R}^3, \times)$, který není grupou, neboť operace není asociativní (Příklad 2.8.), a navíc ani nemá neutrální prvek (Cvičení 2.1.8.), a proto nemá smysl k vektorům hledat inverzní prvky.
7) $(\mathbb{Z}_4 \setminus \{0\}, \cdot)$ (násobení nenulových čísel modulo 4) netvoří grupu. Prvek $\overline{2}$ nemá inverzi.
8) $(M_{n,n}, \cdot)$ (čtvercové matice řádu n s operací násobení matic) netvoří grupu, protože k singulárním maticím neexistují inverzní matice.

Poznámka 2.2. Je dobré upozornit, že grupu chápeme jako strukturu, která je přirozeným zobecněním sčítání celých čísel. Už jsme viděli, že celá čísla tvoří grupoid: operace sčítání je uzavřená na (neprázdné) množině celých čísel. Víme, že obvyklé sčítání je asociativní, a také víme, že neutrálním prvkem je číslo 0 a ke každému číslu a snadno najdeme inverzi: opačné číslo $-a$.

V Kapitole 11. uvidíme, jak dále zobecnit počítání s celými čísly s využitím dvou operací.

Příklad 2.19. Mějme přirozené číslo n větší než 1. Symbolem $U(n)$ označme množinu všech přirozených čísel a, která jsou menší než číslo n a nesoudělná s n, tj. platí $\mathrm{NSD}(a, n) = 1$. Ukážeme, že $(U(n), \cdot)$, kde násobení provádíme modulo n, tvoří komutativní grupu, které říkáme *grupa jednotek modulo n*.
Množina $U(n)$ je jistě neprázdná, neboť například $1 \in U(n)$. Ukážeme, že operace „$\cdot$“ je na $U(n)$ uzavřená. Mějme $a, b \in U(n)$. Protože $\mathrm{NSD}(a, n) = 1$, tak podle Bézoutova Lemmatu 0.3. existují celá čísla r, s, že $ar + ns = 1$. Analogicky musí existovat taková celá čísla u, v, že $bu + nv = 1$. Potom

$$1 = 1 \cdot 1 = (ar + ns)(bu + nv)$$
$$1 = (ab)ru + n(arv + sbu + nsv).$$

To podle Bézoutova Lemmatu 0.3. znamená, že $\mathrm{NSD}(ab, n) = 1$ (s využitím faktu, že koeficienty r, u jsou nesoudělné s n) a proto je operace „$\cdot$“ modulo n je uzavřená na $U(n)$.

Dále podle Cvičení 0.6.6. je operace „$\cdot$“ na $U(n)$ asociativní, protože násobení celých čísel modulo n je asociativní. Neutrální prvkem je číslo 1 které do $U(n)$ patří.

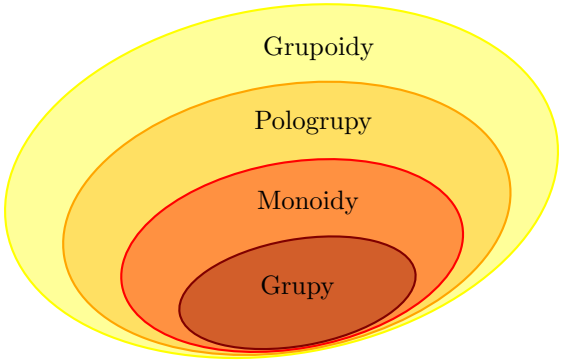
Konečně, mějme libovolný prvek a. Ukážeme, že v $U(n)$ existuje jeho inverze. Protože $\mathrm{NSD}(a, n) = 1$, tak podle Bézoutova Lemmatu 0.3. existují celá čísla r, s, že $ar + ns = 1$. Potom $1 = ar + ns \equiv ar \pmod{n}$ a r je inverzí ke k modulo n. Zbývá ukázat, že $r \in U(n)$, což plyne opět z rovnosti $ar + ns = 1$ a druhé části Bézoutova Lemmatu 0.3., podle které je $\mathrm{NSD}(r, n) = 1$, a tedy r je nesoudělné s n. ✓

Příklad 2.20. Sestavíme Cayleyho tabulku grupy $(U(8), \cdot)$ (grupy jednotek modulo 8).
Ihned vidíme, že $U(8) = \{1, 3, 5, 7\}$. Sestavíme Cayleyho Tabulku 2.X26. ✓

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Tabulka 2.8.: *Cayleyho tabulka grupy* $(U(8), \cdot)$.

O jednoznačnosti inverzního prvku v grupě
Grupy jsou speciální případy pologrup a ty jsou speciálním případem monoidů (Obrázek 2.1.). Proto podle Věty 2.3. v grupě ke každému prvku existuje nejvýše jedna inverze. Následující věta ukazuje, že můžeme označit neutrální prvek k prvku a symbolem a^{-1}, protože inverzní prvek vždy existuje a je určen jednoznačně. Proto teprve následující věta ospravedlňuje používání označení a^{-1}, které jsme pro inverzní prvky v grupě zavedli.



Obrázek 2.1.: *Hierarchie grupoidů, pologrup, monoidů a grup.*

Věta 2.4. O existenci a jednoznačnosti inverzního prvku v grupě
Mějme grupu $(G, \cdot)$ s neutrálním prvkem e. Pro každé $a \in G$ existuje jediný inverzní prvek $b \in G$ tak, že $a \cdot b = b \cdot a = e$.

Důkaz. Postupujeme přímo. Grupa $(G, \cdot)$ je monoidem a podle Věty 2.3. ke každému prvku existuje nejvýše jedna inverze. Podle definice grupy však víme, že $\forall a \in G$ existuje alespoň jedna inverze, a tak ke každému prvku grupy existuje právě jeden inverzní prvek vzhledem k operaci „$\cdot$“. □

Poznámka 2.3. Dělení v číselném oboru racionálních čísel nebo dělení v oboru reálných čísel není novou operací, ale násobením prvkem, který je inverzní k děliteli různému od nuly. V oboru přirozených čísel s operací obvyklého násobení existuje inverzní prvek jen k prvku 1. V oboru celých čísel existuje inverzní prvek k prvkům 1 a -1, k ostatním prvkům inverzní prvek neexistuje. Proto $(\mathbb{Z}, \cdot)$ není grupou, zatímco $(\mathbb{Z}, +)$ grupou je, protože opačný prvek najdeme ke každému celému číslu.

Následující příklad ukazuje, že jednoznačnost inverze je zaručena pouze v grupě. V grupoidu mohou existovat prvky, které inverzi nemají, ale současně mohou v grupoidu existovat prvky, které mají více inverzí.

Příklad 2.21. Určete inverzní prvky všech prvků množiny $G = [1, 4]$ v grupoidu $(G, \circ)$, který je dán Tabulkou 2.9. vlevo. Je tento grupoid grupou? Grupoid $(G, *)$ se liší jedinou změnou v Tabulce 2.9. vpravo: $3 * 1 = 2$. Jak se změní odpovědi pro grupoid $(G, *)$?

$\circ$	1	2	3	4
1	4	1	2	3
2	1	2	3	4
3	4	3	2	2
4	3	4	2	1

$*$	1	2	3	4
1	4	1	2	3
2	1	2	3	4
3	2	3	2	2
4	3	4	2	1

Tabulka 2.9.: *Grupoidy $(G, \circ)$ a $(G, *)$.*

Abychom mohli hledat inverze v grupoidu $(G, \circ)$, musíme nejprve najít neutrální prvek vzhledem k operaci „$\circ$“. Z tabulky je ihned vidět, že neutrálním prvkem je prvek 2.

- Prvek 1 inverze nemá, protože ve sloupci 1 není neutrální prvek 2. Prvek 3 není inverzí k prvku 1, ačkoliv $1 \circ 3 = 2$, ale $3 \circ 1 \neq 2$.
- Inverzní prvek k prvku 2 je samotný prvek 2, protože $2 \circ 2 = 2$; prvky 1, 3 ani 4 inverzemi nejsou, protože $1 \circ 2 \neq 2$, $3 \circ 2 \neq 2$ ani $4 \circ 2 \neq 2$.
- Inverzní prvky k prvku 3 jsou *oba* prvky 3 a 4, protože $3 \cdot 4 = 4 \cdot 3 = 2$ a $3 \cdot 3 = 2$. Prvky 1 ani 2 nejsou inverzí k prvku 3, ačkoliv $1 \circ 3 = 2$. Platí ale $3 \circ 1 \neq 2$ a $3 \circ 2 \neq 2$.
- Inverzní prvek k prvku 4 je prvek 3, protože $3 \cdot 4 = 4 \cdot 3 = 2$; prvky 1, 2 ani 4 inverzemi nejsou, protože $4 \cdot 1 \neq 2$, $4 \cdot 2 \neq 2$ ani $4 \cdot 4 \neq 2$.

Prvek 1 nemá žádnou inverzi, proto grupoid $(G, \circ)$ *není* grupou. Stejně bychom mohli říci, že se nemůže jednat o grupu, protože k prvku 3 jsme našli dva inverzní prvky. Všimněte si, že existence dvou inverzních prvků není v rozporu s Větou 2.4., neboť uvedený grupoid není grupou. Využili jsme, že neutrální prvek i inverzní prvky je podle definice možno hledat nejen v grupě, ale i v grupoidu (pokud grupoid má neutrální prvek). A konečně grupoid $(G, \circ)$ určený Tabulkou 2.9. nemůže být grupou už proto, že operace „$\circ$“ ani není asociativní. Platí $3 \circ (3 \circ 4) = 3$, ale $(3 \circ 3) \circ 4 = 4$, a proto grupoid $(G, \circ)$ není ani pologrupou.

Pro grupoid $(G, *)$ dostaneme následující odpovědi. Neutrálním prvek je opět prvek 2.

- Inverze k prvku 1 inverze je prvek 3.
- Inverzní prvek k prvku 2 je samotný prvek 2.
- Inverzní prvky k prvku 3 jsou *tři* prvky 1, 3 a 4.
- Inverzní prvek k prvku 4 je prvek 3.

Přesto grupoid $(G, *)$ určený Tabulkou 2.9. není být grupou, neboť prvek 3 má více než jednu inverzi vzhledem k operaci „$*$“, což je způsobeno tím, že operace „$*$“ není asociativní. Můžeme si všimnout, že $3 * (3 * 4) = 3$, avšak $(3 * 3) * 4 = 4$. ✓

Následující lemma ukazuje, že inverzí k inverzi daného prvku je vždy prvek sám.

Lemma 2.5. *Mějme grupu $(G, \cdot)$ a libovolný prvek $a \in G$. Potom platí $(a^{-1})^{-1} = a$.*

Důkaz. Ukážeme, že inverzní prvek k a^{-1} je prvek a. Označme $x = a^{-1}$. Protože $x = a^{-1}$ je inverzní prvek k a, tak platí $x \cdot a = a \cdot x = e$, kde e je neutrální prvek grupy $(G, \cdot)$. To však současně znamená, že a je inverzní k prvku $x = a^{-1}$. Tj. $a = (x)^{-1} = (a^{-1})^{-1}$. □

Předchozí Lemma 2.5. říká, že prvky a jejich inverze jsou buď totožné ($a^{-1} = a$), nebo tvoří páry v nosné množině grupy $(G, \cdot)$. Prvek a^{-1} je inverzní prvek k a, což současně znamená, že a je inverzní prvek k prvku a^{-1}.

Otázky:

- Může v nějaké grupě $(G, \cdot)$ existovat více než jeden takový prvek a, $a \in G$, že $a^{-1} = a$?
- Může v nějaké grupě $(G, \cdot)$ existovat více než dva takové prvky a, že $a^{-1} = a$?
- Může pro každé přirozené číslo n existovat taková grupa $(G, \cdot)$, ve které existuje alespoň n takových prvků a, že $a^{-1} = a$?

Cvičení

2.4.1. Které z následujících dvojic jsou grupy? a) $(\mathbb{N} \cup \{0\}, +)$, b) $(P, \circ)$, kde P je množina všech prostých *reálných funkcí s definičním oborem $\mathbb{R}$ a oborem hodnot $\mathbb{R}$.*

2.4.2.$^{\heartsuit}$ Ukažte, že v každém monoidu $(G, \cdot)$ (a tedy i v každé grupě) s neutrálním prvkem e platí $e^{-1} = e$, tj. neutrální prvek je sám k sobě inverzní.

2.4.3. Vysvětlete, proč $(P, \circ)$, kde P je množina všech prostých *reálných funkcí s definičním oborem $\mathbb{R}$, není grupa.*

2.4.4. Mějme dihedrální grupu $(D_n, \circ)$ symetrií n-úhelníka. Popište inverzní prvek každé symetrie. (Toto cvičení je zobecněním Příkladu 2.15.)

2.4.5. Mějme grupu $(G, \cdot)$ a dva prvky $a, b \in G$. Ukažte, že pokud b je inverzí k prvku a, tak a je inverzní k prvku b. Můžeme proto říkat, že a a b jsou navzájem inverzní. (Jedná se o jinou formulaci Lemmatu 2.5.)

2.4.6. Mějme pologrupu $(G, \cdot)$ a v něm takový prvek e, že $ae = a$ pro každý prvek $a \in G$, a dále ke každému prvku $a \in G$ existuje v G inverzní prvek, tj. takový prvek a^{-1}, pro který platí $aa^{-1} = e = a^{-1}a$. Ukažte, že musí současně platit $ea = a$. (V definici grupy je možno zaměnit jednu rovnost za požadavek jednoznačnosti inverze.)

2.4.7. Ukažte, že $(\mathbb{S}, \cdot)$ s operací obvyklého násobení (sudých) čísel není grupa.

2.4.8. Mějme grupu $(G, \cdot)$. Sestavíme množinu inverzních prvků $H = \{g^{-1} : g \in G\}$. Ukažte, že množiny $H = G$.

2.4.9. Mějme libovolné dva prvky a, b grupy $(G, \cdot)$. Najděte takový prvek $x \in G$, že platí $xabx^{-1} = ba$.

$*$	0	1	∞
0	0	0	1
1	0	1	∞
∞	1	∞	∞

Tabulka 2.10.: Cayleyho tabulka násobení vybraných reálných čísel a ∞.

$*$	0	1	-1	x	y	∞	$-\infty$
0	0	0	0	0	0	1	-1
1	0	1	-1	x	y	∞	$-\infty$
-1	0	-1	1	$-x$	$-y$	$-\infty$	∞
x	0	x	$-x$	x^2	xy	$\operatorname{sgn}(x)\infty$	$-\operatorname{sgn}(x)\infty$
y	0	y	$-y$	yx	y^2	$\operatorname{sgn}(y)\infty$	$-\operatorname{sgn}(y)\infty$
∞	1	∞	∞	$\operatorname{sgn}(x)\infty$	$\operatorname{sgn}(x)\infty$	∞	$-\infty$
$-\infty$	-1	$-\infty$	∞	$-\operatorname{sgn}(x)\infty$	$-\operatorname{sgn}(x)\infty$	$-\infty$	∞

Tabulka 2.11.: Cayleyho tabulka násobení vybraných prvků v $\mathbb{R}^*$.

2.4.10. Mějme Tabulku 2.10. operace „součinu $*$“ na množině $\{0,1,\infty\}$ (na množině vybraných reálných číslech včetně ∞). Vysvětlete, proč tabulka nepopisuje grupu.

2.4.11. Mějme Tabulku 2.11. operace „součinu $*$“ na množině rozšířených reálných číslech $\mathbb{R}^*$, kde x, y jsou libovolná reálná čísla. Vysvětlete, proč tabulka nepopisuje grupu.

2.4.12. Dokažte nebo vyvraťte následující tvrzení: a) součin dvou nenulových celých čísel je nenulové reálné číslo, b) součin dvou nenulových komplexních čísel je nenulové komplexní číslo, c) součin dvou nenulových čtvercových matic s celočíselnými koeficienty je nenulová matice.

2.4.13. Existují dvě nenulové matice A, B takové, že $A \cdot B$ i $B \cdot A$ dá nulovou matici?

2.4.14. Dokažte, že Tabulka 2.6. popisuje monoid.

2.4.15. Mějme množinu komplexních čísel $G = \{1, -1, -i, i\}$. Ukažte, že $(G, \cdot)$ je grupa, kde operace „$\cdot$“ je restrikce obvyklého násobení komplexních čísel na prvky množiny G.

2.4.16. Označme $G = \{a + b\sqrt{2} : a, b \in \mathbb{Q}, (a,b) \neq (0,0)\}$. Dále nechť „$\cdot$“ je restrikce obvyklého násobení reálných *čísel na množinu G. Ukažte, že $(G, \cdot)$ je grupa.*

2.4.17. Ukažte, že sčítání zbytkových tříd modulo 4 je grupa $(\mathbb{Z}_4, +)$.

2.4.18. Sestavte Cayleyho tabulku monoidů $(\mathbb{Z}_4, \cdot)$ a $(\mathbb{Z}_4 \setminus \{0\}, \cdot)$ s operacemi násobení modulo 4. Ukažte, že $(\mathbb{Z}_4, \cdot)$ a $(\mathbb{Z}_4 \setminus \{0\}, \cdot)$ a) jsou monoidy; b) nejsou grupy.

2.4.19. Dokažte nebo vyvraťte: Mějme grupoid $(A, \circ)$, ve kterém existuje neutrální prvek e. Jestliže k nějakému prvku a, $a \in A$ existují dva různé inverzní prvky $b_1, b_2 \in A$, tak operace „$\circ$“ není asociativní

2.4.20. Navážeme na Příklad 2.3.7. Mějme libovolnou grupu $(G, \circ)$. Do grupy přidáme nový prvek e (tj. $e \notin G$) tak, aby $(G \cup \{e\}, *)$ byl monoid s neutrálním prvkem e, přičemž $\forall x, y \in G$ položíme $x * y = x \circ y$, $x * e = x$, $e * x = x$ a $e * e = e$. Ukažte, že $(G \cup \{e\}, *)$ není grupa.

2.4.21. Sestavte Cayleyho tabulku grupy $U(12)$

2.4.22. Navážeme na Cvičení 2.3.3. Pro libovolné $n \in \mathbb{N}$ mějme množinu $A = [1, n]$. Na množině A definujeme operaci $\circ$ $\forall a, b \in A : a \circ b = \max\{a, b\}$. Ukažte, že pro $n \geq 2$ je dvojice $(A, \circ)$ monoidem, který není grupou.

2.4.23. Mějme šachovnici o rozměru $r \times s$ políček, označme $n = rs$. Řádky i sloupce jsou značeny například čísly a písmeny. Na každém políčku šachovnice leží jedna mince, celkem na šachovnici leží n mincí. Mince jsou náhodně otočené, některé hlavou vzhůru, některé hlavou dolů. Jedno políčko šachovnice je výjimečné, například že se pod ním skrývá poklad.*

Dva kamarádi Adam a Bedřich mohou si předem mohou domluvit vhodnou strategii, aby uspěli v následující hře. Nejprve šachovnici a mince uvidí Adam. Adam se dozví, které políčko je výjimečné, a pak musí zvolit jedinou minci, kterou (někdo) otočí naopak, než mince leží. Adam odejde a už nijak nesmí napovídat Bedřichovi.

Nyní Bedřich poprvé uvidí šachovnici a na ní položené mince. Pokud pozná, které políčko šachovnice je výjimečné, oba ve hře uspěli. Jakmile si kamarádi domluví strategii, tak veškerá komunikace mezi Adamem

a Bedřichem probíhá pouze volbou otočené mince, které mince jsou otočeny hlavou vzhůru. Bedřich nepozná, která mince byla otočena, například podle toho, že bude na políčku posunuta, nebo že bude teplejší a podobně.

Pro $n = 2^k$, $k \in \mathbb{N}$, navrhněte strategii, kterou si mohou Adam a Bedřich domluvit, aby ve hře uspěli.

(Poznámka: v předmětu „Teorie grafů“ ukážeme, že pro jiné hodnoty n než 2^k taková strategie nemůže existovat.*)*

2.5. Další vlastnosti grup

Grupy byly zavedeny jako zobecnění počítání s celými čísly. Některá dobře známá početní pravidla, která používáme při počítání s celými čísly platí i pro jakékoliv grupy. Některá z nich uvedeme.

O krácení v grupě

Následující věta ukazuje, že i v obecné algebraické struktuře grup můžeme využívat úpravu, na kterou jsme zvyklí při počítání s čísly. Věta říká, že v grupě můžeme krátit.

Věta 2.6. Věta o krácení v grupě

Mějme grupu $(G, \cdot)$. Potom pro všechna $a, b, c \in G$ platí

(i) jestliže $a \cdot c = b \cdot c$, potom $a = b$, *(krácení zprava)*

(ii) jestliže $c \cdot a = c \cdot b$, potom $a = b$. *(krácení zleva)*

Důkaz. Mějme rovnost $a \cdot c = b \cdot c$ pro libovolné $a, b, c \in G$. V grupě existuje ke každému prvku inverze, zejména existuje c^{-1}. Vynásobením rovnosti zprava c^{-1} dostaneme $a \cdot c \cdot c^{-1} = b \cdot c \cdot c^{-1}$, proto $a \cdot e = b \cdot e$, kde e je neutrální prvek grupy. S využitím vlastnosti neutrálního prvku je $a = b$.

Druhá rovnost se odvodí analogicky vynásobením c^{-1} zleva. □

Následující příklad ukazuje, že v obecném grupoidu, pologrupě nebo monoidu uvedená věta platit nemusí.

Příklad 2.22. Mějme monoid $(A, \circ)$ daný Cayleyho tabulkou 2.12. Ukážeme, že Věta o krácení v monoidu $(A, \circ)$ neplatí.

$\circ$	1	2
1	1	2
2	2	2

Tabulka 2.12.: *Monoid, který není grupou.*

V obecném monoidu věta o krácení neplatí. V monoidu $(A, \circ)$ nemůžeme krátit zprava, neboť $1 \cdot 2 = 2 = 2 \cdot 2$ avšak $1 \neq 2$. Nemůžeme krátit ani zleva, neboť $2 \cdot 1 = 2 = 2 \cdot 2$ avšak $1 \neq 2$. Prvek 2 nemá v uvedeném monoidu inverzi. ✓

Podle tvrzení a důkazu Věty 2.6. a podle předchozího příkladu by se mohlo zdát, že bude-li k nějakému prvku existovat inverze, můžeme tímto prvkem krátit. Není to pravda. Následující příklad ukazuje, že je nutná i jednoznačnost inverze, která je zaručena pouze v grupě.

Příklad 2.23. Mějme grupoid $(A, \circ)$ daný Cayleyho tabulkou 2.7. ze strany 49. Neutrálním prvkem je 1, prvky 2 a 3 mají inverzní prvky 2 a 3. Ukážeme, že Věta o krácení v grupoidu $(A, \circ)$ neplatí.

$\circ$	1	2	3
1	1	2	3
2	2	1	1
3	3	1	1

Tabulka 2.13.: *Cayleyho tabulka operace grupoidu, kde prvky 2 a 3 mají dva inverzní prvky.*

Prvky 2 i 3 mají v uvedeném grupoidu stejnou inverzi. V grupoidu $(A, \circ)$ nemůžeme krátit zprava, neboť $3 \cdot 2 = 1 = 2 \cdot 2$ avšak $3 \neq 2$. Nemůžeme krátit ani zleva, neboť $2 \cdot 3 = 1 = 2 \cdot 2$ avšak $3 \neq 2$. ✓

Otázky:

- Jaká vlastnost grupy je porušena, pokud v grupoidu existuje neutrální prvek e a ke každému prvku a existuje inverze a^{-1}, avšak v Cayleyho tabulce bude některý prvek v některém řádku nebo sloupci v alespoň dvou kopiích?
- Můžete demonstrovat vaši odpověď na Tabulce 2.13. z Příkladu 2.23.?
- Můžeme říci, že pokud se v některém řádku Cayleyho tabulky grupoidu $(G, \circ)$ některý prvek opakuje, tak operace „$\circ$“ není asociativní?

V grupě inverzní prvky komutují

Ukážeme, že v každé (i nekomutativní!) grupě, stačí pro existenci inverzního prvku a^{-1} ověřovat jen jednu z rovností $a \cdot a^{-1} = e$, $a^{-1} \cdot a = e$. Jestliže platí jedna z rovností, bude vždy druhá platit také.

Lemma 2.7. V grupě inverzní prvky komutují
Mějme grupu $(G, \cdot)$ s neutrálním prvkem e. Pro každé $a, b \in G$ platí, jestliže $a \cdot b = e$, potom také $b \cdot a = e$.

Důkaz. Postupujeme přímo. Z rovnosti $a \cdot b = e$ odvodíme rovnost $b \cdot a = e$.

$$\begin{aligned}
a \cdot b &= e && \text{z předpokladu věty}\\
a^{-1} \cdot (a \cdot b) &= a^{-1} \cdot e && \text{z existence inverzního prvku } a^{-1} \text{ a vynásobením zleva}\\
(a^{-1} \cdot a) \cdot b &= a^{-1} \cdot e && \text{z asociativity operace}\\
e \cdot b &= a^{-1} \cdot e && \text{z definice inverzního prvku } a^{-1}\\
b &= a^{-1} && \text{z definice neutrálního prvku}\\
b \cdot a &= a^{-1} \cdot a && \text{vynásobením zprava prvkem } a\\
b \cdot a &= e && \text{z definice inverzního prvku } a^{-1}
\end{aligned}$$

Tím je důkaz ukončen. □

Všimněte si, že v důkazu jsme využili existenci neutrálního prvku, existence inverzního prvku a asociativitu. Následující příklad ukazuje, že v grupoidu inverzní prvky komutovat nemusí.

Příklad 2.24. Mějme grupoid $(G, \cdot)$ určený Cayleyho tabulkou 2.14. Ukážeme, že a) $(G, \cdot)$ není asociativní, b) v grupoidu $(G, \cdot)$ inverzní prvky nekomutují (neplatí analogie Lemmatu 2.7.).

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	2	2	1
3	3	1	2	2
4	4	2	1	2

Tabulka 2.14.: *Grupoid $(G, \cdot)$ není asociativní, není komutativní má neutrální prvek, nemá inverze.*

a) Operace „$\cdot$“ není asociativní, neboť například $(4 \cdot 2) \cdot 4 = 1$, ale $4 \cdot (2 \cdot 4) = 4$.
b) Z Tabulky 2.14. je zřejmé, že jediný prvek, který má oboustrannou inverzi, je prvek 1. Naproti tomu platí $2 \cdot 4 = 1$, ale $4 \cdot 2 \neq 1$. Podobně platí $3 \cdot 2 = 1$, ale $2 \cdot 3 \neq 1$ a platí $4 \cdot 3 = 1$, ale $3 \cdot 4 \neq 1$. ✓

Opakovaná operace se stejným prvkem

Nyní zavedeme jedno obvyklé značení.

Definice Označení opakované aditivní a multiplikativní operace
Mějme grupu $(G, \cdot)$ a prvek $a \in G$. Zavedeme následující obvyklé označení.
Jestliže operaci „$\cdot$“ chápeme jako aditivní operaci „$+$“, tak „součet“ n kopií prvku a zapíšeme

$$\underbrace{a + a + \cdots + a}_{n} = na,$$

přičemž položíme $1a = a$ a také $0a = 0$. Výraz na je *n-násobek prvku*. Neutrální prvek v aditivním zápisu značíme 0 a říkáme mu *nulový prvek* nebo *nula*. Inverzní (opačný) prvek k prvku a v aditivním zápisu značíme $-a$.

Jestliže operaci „$\cdot$“ chápeme jako multiplikativní operaci „$\cdot$“, tak „součin“ n kopií prvku a zapíšeme

$$\underbrace{a \cdot a \cdots a}_{n} = a^n,$$

přičemž položíme $a^1 = a$ a také $a^0 = 1$. Výraz a^n je n-tá *mocnina prvku*. Neutrální prvek v multiplikativním zápisu značíme 1 a říkáme mu *jednička* nebo *jednotkový prvek*. Inverzní prvek k prvku a v multiplikativním zápisu značíme a^{-1}.

Všimněte si, že vzhledem k asociativitě operace v každé grupě jsme si mohli dovolit v zavedeném označení vynechat závorky. Nejedná se o n-ární operaci, ale o opakované složení operace „$+$“ resp. „$\cdot$“.

$$\underbrace{(\ldots((a \cdot a) \cdot a) \cdots a)}_{n} = \underbrace{a \cdot a \cdots a}_{n}$$
$$\underbrace{(\ldots((a + a) + a) \ldots + a)}_{n} = \underbrace{a + a + \cdots + a}_{n}$$

Příklad 2.25. Ukážeme, že v grupě $(A, \cdot)$ s operací „$\cdot$“ (analogie operace součinu) platí vztah $a^n \cdot a^m = a^{n+m}$.
Podle zavedeného značení můžeme psát

$$a^n \cdot a^m = \underbrace{a \cdot a \cdots a}_{n} \cdot \underbrace{a \cdot a \cdots a}_{m} = \underbrace{a \cdot a \cdots a}_{n+m} = a^{n+m}.$$

Další vztahy se ukáží podobně (Cvičení 2.5.15. a 2.5.14.). ✓

Věta o ponožkách a botách
Nyní zformulujeme a dokážeme jedno důležité tvrzení.

Věta 2.8. *Mějme grupu $(G, \cdot)$ a prvky $a, b \in G$. Potom platí $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$.*

Důkaz. Podle definice inverzního prvku víme, že $(a \cdot b) \cdot (a \cdot b)^{-1} = e$. Dále s využitím asociativity dostaneme, že $(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot e \cdot a^{-1} = a \cdot a^{-1} = e$. Tím jsme ověřili, že prvek $(b^{-1} \cdot a^{-1})$ je inverzí k prvku $(a \cdot b)$. Opačná rovnost $(a \cdot b)^{-1} \cdot (a \cdot b) = e$ plyne ihned z Věty 2.7. Protože podle Věty 2.4. je v grupě inverzní prvek k prvku $a \cdot b$ určen jednoznačně, tak platí rovnost $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$. □

Příklad 2.26. Mějme například grupu $(M_{2,2}, \cdot)$ regulárních matic řádu 2 s operací obvyklého násobení matic. Zvolme $A = \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ -2 & 0 \end{pmatrix}$ a ukážeme, že $(AB)^{-1} = B^{-1}A^{-1}$ avšak $(AB)^{-1} \neq A^{-1}B^{-1}$.

Nejprve snadno vypočítáme

$$AB = \begin{pmatrix} 1 & 3 \\ 1 & 4 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -2 & 0 \end{pmatrix} = \begin{pmatrix} -5 & 3 \\ -7 & 4 \end{pmatrix}$$

Snadno lze ověřit, že

$$A^{-1} = \begin{pmatrix} 4 & -3 \\ -1 & 1 \end{pmatrix}, \quad B^{-1} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, \quad (AB)^{-1} = \begin{pmatrix} 4 & -3 \\ 7 & -5 \end{pmatrix}.$$

Nyní vypočítáme

$$B^{-1}A^{-1} = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} \begin{pmatrix} 4 & -3 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 4 & -3 \\ 7 & -5 \end{pmatrix} = (AB)^{-1}.$$

Naproti tomu

$$A^{-1}B^{-1} = \begin{pmatrix} 4 & -3 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix} = \begin{pmatrix} -2 & -3 \\ 1 & 1 \end{pmatrix} \neq (AB)^{-1}.$$

Poslední výpočet ukazuje, že v grupě obecně neplatí $\forall a, b \in G : (a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$. ✓

Poznámka 2.4. **Věta o ponožkách a botách**

Větě 2.8. se v literatuře někdy říká „Věta o ponožkách a botách“. Obvykle si obouváme nejprve ponožky a pak boty (v naší zemi případně i sandály). Jestliže se naopak vyzouváme, tak musíme nejprve vyzout boty a teprve potom ponožky.

V Kapitole 1.2. jsme zmínili, že pomocí grup můžeme popsat otáčení stěn Rubikovy kostky. Věta 2.8. říká, že pokud otočíme stěny kostky v nějakém pořadí, tak otočením stěn v opačném pořadí a v opačném směru dostaneme vždy výchozí rozmíchání stěn Rubikovy kostky.

Nyní uvedeme zobecněnou verzi věty o ponožkách a botách.

Věta 2.9. *Mějme grupu $(G,\cdot)$ a prvky $a_1, a_2, \ldots, a_n \in G$. Platí $(a_1 \cdot a_2 \cdots a_n)^{-1} = a_n^{-1} \cdots a_2^{-1} \cdot a_1^{-1}$.*

Důkaz je ponechán jako Cvičení 2.5.8.

Poznámka 2.5. Zápis multiplikativní operace v grupě
Při zápisu obecné operace preferujeme multiplikativní zápis. Jestliže nebude moci dojít k mýlce, často si dovolíme symbol operace vynechat, podobně jako se vynechává symbol operace v multiplikativním zápisu. Je-li například $(G,\cdot)$ grupa a $a \in G$, tak píšeme

$$a \cdot a = aa.$$

Cvičení

2.5.1.$^{\heartsuit}$ *Najděte takovou vlastní podmnožinu $A \in \mathbb{R}$, aby $(A,\cdot)$ byl komutativní grupoid (operace „$\cdot$“ je restrikce operace běžného násobení). a) Najdete takovou podmnožinu A se dvěma prvky? b) Najdete takovou konečnou podmnožinu A se třemi nebo více prvky? c) Najdete takovou nekonečnu vlastní podmnožinu A? Pokud neexistují, dokažte to.*

2.5.2. Najděte příklad a) grupoidu, kde nějaký prvek má jednu inverzi a jiný prvek dvě inverze, b) grupoidu ve kterém najdeme takové čtyři prvky, že jeden prvek má jednu inverzi, druhý dvě, třetí tři a čtvrtý čtyři inverze. c) grupoidu s n prvky, kde pro každé $i \in [1, n-1]$ najdeme prvek, který má i inverzí.

2.5.3. Ukažte, že v monoidu musí být alespoň jeden prvek, který má právě jednu inverzi.

2.5.4. Mějme grupu $(G,\cdot)$. Ukažte, že v každém řádku a v každém sloupci je nějaká permutace všech prvků z G. Návod*: ukažte, že v řádku Cayleyho tabulky, který odpovídá prvku a, se neopakuje žádný prvek grupy $(G,\cdot)$.*

2.5.5. Mějme takový (konečný) grupoid $(G,\circ)$, že v každém řádku a každém sloupci Cayleyho tabulky je permutace všech prvků z G. Dokažte nebo vyvraťte, že $(G,\circ)$ je grupa.

2.5.6. Máme operaci „$\cdot$“ na množině $A = \{e, r, s, t, u, v\}$ popsanou Tabulkou 2.15. a) Je $(A,\cdot)$ grupou? b) Pokud ano, je tato grupa komutativní?

$\cdot$	e	r	s	t	u	v
e	e	r	s	t	u	v
r	r	s	e	u	v	t
s	s	e	r	v	t	u
t	t	v	u	e	s	r
u	u	t	v	r	e	s
v	v	u	t	s	r	e

Tabulka 2.15.: Tabulka operace „$\cdot$“ na množině $\{e, r, s, t, u, v\}$.

2.5.7. Mějme grupoid $(G, \circ)$ s neutrálním prvek e. Pro každou dvojici prvků $x, y \in G$ definujeme novou operaci.

$$x * y = \begin{cases} e & \text{pro } x \neq e \text{ a } y \neq e \\ x \circ y & \text{pro } x = e \text{ nebo } y = e \end{cases}$$

a) Je dvojice $(G, *)$ grupoidem? b) Pokud ano, je e jeho neutrálním prvkem? c) Pokud ano, jak vypadají inverze každého prvku $x \in G$?

2.5.8. Dokažte Větu 2.9.

2.5.9. Mějme grupoid $(G, \circ)$ s neutrálním prvkem e. Dokažte nebo vyvraťte: prvek y je inverzní k prvku x právě tehdy, když $y \circ (x \cdot y) = y$.

2.5.10. Mějme pologrupu $(G, \cdot)$ s neutrálním prvkem e. Dokažte nebo vyvraťte: prvek y je inverzní k prvku x právě tehdy, když $y \cdot (x \cdot y) = y$.

2.5.11. Mějme neprázdnou částečně uspořádanou množinu čísel M s relací dělitelnosti a s největším prvkem vzhledem k této relaci. Každé dvojici prvků a, b přiřadíme nejmenší společný násobek v množině M a označíme jej $a \wedge b$. a) Jedná se operaci na M? b) je $(M, \wedge)$ grupoid? c) je $(M, \wedge)$ pologrupa? d) je $(M, \wedge)$ grupa?

2.5.12. Ukažte, že existuje asociativní nekomutativní monoid $(M, \circ)$, ve kterém najdeme takové dva prvky f, g, že $f \circ g = e$ (kde e je neutrální prvek monoidu), ale $g \circ f \neq e$.*

2.5.13. Definujme operaci „$\cdot$“ na $G = \mathbb{R} \times \mathbb{R}$ následujícím způsobem: $(a, b) \cdot (c, d) = (a \cdot c, b \cdot c + d)$. Všimněte si různých významů symbolu „$\cdot$“. a) Ukažte, že $(G, \cdot)$ je grupoid. b) Je tento grupoid komutativní? c) Je tento grupoid asociativní? d) Má tento grupoid neutrální prvek? e) Jestliže neutrální prvek existuje, existuje k nějakým prvkům inverzní prvek?

2.5.14. Ukažte, že pro aditivní operaci „$+$“ v obecné grupě platí vztahy a) $ma + na = (m + n)a$, b) $m(na) = (mn)a = n(ma)$.

2.5.15. Ukažte, že pro multiplikativní operaci „$\cdot$“ v obecné grupě platí vztah $(a^n)^m = a^{mn} = (a^m)^n$.

2.5.16. Doplňte Tabulku 2.16. tak, aby se jednalo o Cayleyho tabulku grupy.

$\cdot$	a	b	c
a	a	b	c
b	b		
c	c		

Tabulka 2.16.: Část Cayleyho tabulky.

2.5.17. Doplňte Tabulku 2.17. tak, aby se jednalo o Cayleyho tabulku grupy.

$\cdot$	a	b	c	d
a	a	b	c	
b	b			a
c		d		
d	d			c

Tabulka 2.17.: Část Cayleyho tabulky.

2.5.18. Ukažte, že má-li nosná množina grupy $(G, \cdot)$ sudý počet prvků, tak musí existovat takový prvek $g \in G$ různý od neutrálního prvku e, že platí $g \cdot g = e$.

2.5.19. Ukažte, že Tabulka 2.12. reprezentuje monoid.

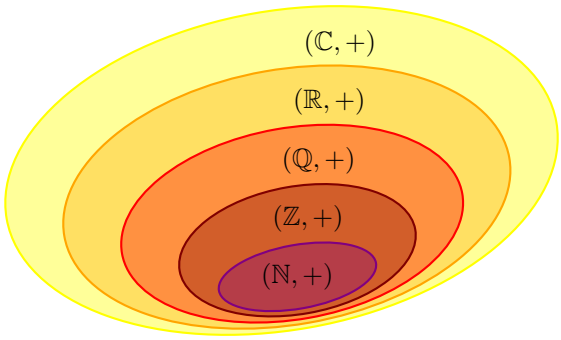
2.5.20. Mějme grupoid $(G, \circ)$ s neutrálním prvkem e, ve kterém navíc ke každému prvku a existuje inverze a^{-1}. Ukažte, že pokud se v Cayleyho tabulce vyskytuje některý prvek v některém řádku nebo sloupci v alespoň dvou kopiích, tak a) operace „$\circ$“ není asociativní, b) najdete trojici prvků grupoidu, které poruší asociativitu?

2.5.21. Využijte Větu o krácení (Věta 2.6.) k důkazu, že všechny grupy řádu 3 jsou komutativní.

2.5.22. Na straně 46 jsme zavedli idempotentní prvky grupoidu $(G, \cdot)$, pro které platí $g \cdot g = g$. Ukažte, že v grupě existuje pouze jediný idempotentní prvek.

Kapitola 3. Podgrupy a komplexy

Víme, že přirozená čísla jsou podmnožinou množiny celých čísel. Avšak po celých číslech požadujeme více, než jen aby jich bylo více. Očekáváme, že v obou množinách početní operace se společnými čísly vychází stejně. Víme už, že na rozdíl od pologrupy $(\mathbb{N},+)$ tvoří celá čísla grupu $(\mathbb{Z},+)$. To mimo jiné znamená, že při počítání s celými čísly si můžeme dovolit odečítat i větší číslo od menšího čísla. Podobně jsou celá čísla podmnožinou racionálních nebo reálných čísel. Naprosto přirozeně očekáváme, že omezíme-li se při počítání s reálnými nebo racionálními čísly na čísla celá, tak výsledek početní operace $x+y$ bude stejný pro $x,y\in\mathbb{Z}$, jako když vezmeme stejná čísla $x,y\in\mathbb{Q}$ nebo $x,y\in\mathbb{R}$. Celá čísla $(\mathbb{Z},+)$ tvoří podstrukturu v grupě $(\mathbb{Q},+)$ i v grupě $(\mathbb{R},+)$ a přirozená čísla $(\mathbb{N},+)$ tvoří podstrukturu v grupě $(\mathbb{Z},+)$ (Obrázek 3.1.), která však není grupou. Tato pozorování budeme formulovat pro obecné grupy.



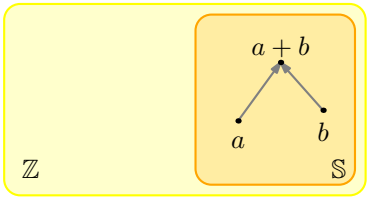
Obrázek 3.1.: *Grupy* $(\mathbb{C},+)$, $(\mathbb{R},+)$, $(\mathbb{Q},+)$, $(\mathbb{Z},+)$ *a pologrupa* $(\mathbb{N},+)$.

Otázka: Proč není $(\mathbb{N},+)$ grupou?

Příklad 3.1. Víme, že množina celých čísel s operací sčítání tvoří grupu $(\mathbb{Z},+)$. Uvažujme množinu $\mathbb{S}=2\mathbb{Z}=\{2k:k\in\mathbb{Z}\}$ jejíž prvky budeme sčítat stejně jako prvky množiny $\mathbb{Z}$. Tj. zavedeme operaci $\oplus:\mathbb{S}\times\mathbb{S}\to\mathbb{S}$ definovanou předpisem:

$$\forall x,y\in\mathbb{S}: x\oplus y=x+y.$$

Evidentně $\mathbb{S}\subset\mathbb{Z}$. Operace „$\oplus$“ je tak restrikcí obvyklého sčítání „$+$“ celých čísel na množinu $\mathbb{S}$. Ukážeme, že $\mathbb{S}$ spolu s operací „$\oplus$“ také tvoří grupu, kterou později nazveme podgrupou grupy $(\mathbb{Z},+)$.



Obrázek 3.2.: *Podgrupa* $(\mathbb{S},+)$ *v grupě* $(\mathbb{Z},+)$.

Snadno nahlédneme že $(\mathbb{S},\oplus)$ je grupoid, tj. platí

(i) množina $\mathbb{S}$ je jistě neprázdná,
(ii) operace sčítání „$\oplus$“ je uzavřená na množině $\mathbb{S}$, neboť pro každé $a,b\in\mathbb{S}$ existují taková čísla $s,t\in\mathbb{S}$, že $a=2s$, $b=2t$; potom ale $a+b=2s+2t=2(s+t)$, kde $(s+t)\in\mathbb{Z}$ a proto $a+b\in\mathbb{S}$.

Dále ukážeme, že $(\mathbb{S},\oplus)$ tvoří grupu:

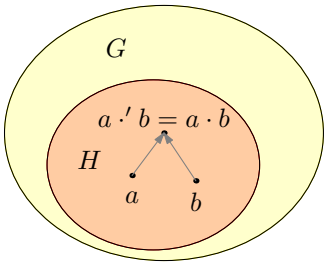
(i) operace „$\oplus$“ je asociativní, neboť operace „$\oplus$“ je restrikcí operace „$+$“ definované na celé množině $\mathbb{Z}$ na množinu $\mathbb{S}$, asociativita se „zdědí“ z asociativity operace sčítání celých čísel v grupě $(\mathbb{Z},+)$ (Cvičení 0.6.6.),
(ii) neutrální prvek nula do $\mathbb{S}$ patří, protože $0=2\cdot 0$ a opět platí $a\oplus 0=0\oplus a=a$,
(iii) ke každému prvku $a\in\mathbb{S}$ najdeme inverzní prvek: inverzním prvkem k prvku $a=2k\in\mathbb{S}$ je prvek $2\cdot(-k)\in\mathbb{S}$, protože $2k+2(-k)=0$ pro každé $k\in\mathbb{Z}$.

Jestliže uděláme úmluvu, že operaci „$\oplus$“ na množině $\mathbb{S}$ budeme značit stejně, jako operaci sčítání na množině $\mathbb{Z}$, tak můžeme říci, že $(\mathbb{S}, +)$ je grupa. ✓

Později ukážeme, že vlastnost „být neutrálním prvkem grupy“ zůstane zachována i v každé algebraické podstruktuře, do které bude neutrální prvek patřit. V následující podkapitole tyto algebraické podstruktury zavedeme a nazveme je podgrupami dané grupy.

3.1. Definice pojmů

Hlavní myšlenku Příkladu 3.1. popíšeme obecně. V nosiči G nějaké grupy $(G, \cdot)$ vybereme vhodnou podmnožinu H a pro prvky podmnožiny H nadefinujeme operaci „stejně“ jako byla definována operace „$\cdot$“.



Obrázek 3.3.: *Grupa a její podgrupa.*

Definice Podgrupa
Mějme grupu $(G, \cdot)$. Uspořádaná dvojice $(H, \cdot')$ je *podgrupa grupy* $(G, \cdot)$ právě tehdy, když

(i) $H \subseteq G$, (H je podmnožina v G)
(ii) pro každé $a, b \in H$ platí $a \cdot' b = a \cdot b$, („$\cdot'$“ je restrikcí „$\cdot$“)
(iii) $(H, \cdot')$ je grupa. (je grupou)

Druhá podmínka v definici říká, že operace „$\cdot'$“ je restrikce operace „$\cdot$“ na množinu H. Dále si všimněte, že obecně pro některé podmnožiny H množiny G, množina obrazů (výsledků operace „$\cdot'$“) *nemusí* být podmnožinou H. Teprve poslední podmínka (mimo jiné) zaručuje, že zobrazení „$\cdot'$“ je operace uzavřená na množině H.

Poznámka 3.1. Formálně vzato je operace „$\cdot'$“ jiná operace než operace „$\cdot$“, neboť „$\cdot$“ je zobrazení $G \times G \to G$, zatímco „$\cdot'$“ je zobrazení $H \times H \to H$. Dále v textu však nebudeme rozlišovat značení operace v grupě $(G, \cdot)$ od značení operace v její podgrupě $(H, \cdot')$. Zejména budeme hovořit o podgrupě $(H, \cdot)$ grupy $(G, \cdot)$.

Příklad 3.2. Uveďme několik klasických příkladů podgrup.

1) V grupě celých čísel s operací obvyklého sčítání $(\mathbb{Z}, +)$ je podgrupou každá množina všech násobků čísla k, kde k je libovolné přirozené číslo. Značíme je $(k\mathbb{Z}, +)$.
2) Grupa celých čísel s operací obvyklého sčítání $(\mathbb{Z}, +)$ je podgrupou v grupě racionálních čísel s operací obvyklého sčítání $(\mathbb{Q}, +)$. Podobně grupa $(\mathbb{Q}, +)$ je podgrupou v grupě reálných čísel $(\mathbb{R}, +)$ a grupa $(\mathbb{R}, +)$ je podgrupou v grupě komplexních čísel $(\mathbb{C}, +)$.
3) Množina nenulových racionálních čísel s operací obvyklého násobní $(\mathbb{Q} \setminus \{0\}, \cdot)$ je podgrupou v grupě nenulových reálných čísel s operací obvyklého násobení $(\mathbb{R} \setminus \{0\}, \cdot)$.
4) Množina diagonálních regulárních matic řádu n s racionálními koeficienty s operací obvyklého násobení matic $(D_{n,n}(\mathbb{Q}), \cdot)$ je podgrupou v grupě $(M^*_{n,n}(\mathbb{Q}), \cdot)$ regulárních matic řádu n s racionálními koeficienty s operací obvyklého násobní matic.
5) Dvouprvková množina $\{1, -1\}$ spolu s operací obvyklého násobení tvoří konečnou podgrupu nekonečné grupy $(\mathbb{R} \setminus \{0\}, \cdot)$.
6) Grupa $(U(10), \cdot)$ *je* podgrupou grupy $(U(20), \cdot)$. Je snadné ověřit, že $U(10) \subseteq U(20)$, neboť $\{1, 3, 7, 9\} \subseteq \{1, 3, 7, 9, 11, 13, 17, 19\}$. Pracnější je ověřit, že operace jsou definovány stejně. Vskutku, jistě platí $1 \cdot a = a$ pro každé $a \in U(10)$ i $a \in U(20)$ a dále $3 \cdot 3 = 9$, $3 \cdot 7 = 1$, $3 \cdot 9 = 7$, $7 \cdot 7 = 9$, $7 \cdot 9 = 3$ a $9 \cdot 9 = 1$ vychází stejně jak v $(U(10), \cdot)$, tak v $(U(20), \cdot)$ (Cvičení 3.2.9.). ∎

Příklad 3.3. Uveďme několik dalších příkladů struktur, které podgrupou grupy nejsou.

1) Množina lichých celých čísel s operací obvyklého sčítání $(\mathbb{L}, +)$ není podgrupou v grupě celých čísel s operací obvyklého sčítání $(\mathbb{Z}, +)$, neboť lichá čísla nejsou uzavřená vzhledem ke sčítání.
2) Množina celých čísel s operací obvyklého násobení $(\mathbb{Z} \setminus \{0\}, \cdot)$ není podgrupou v grupě racionálních čísel s operací obvyklého násobení $(\mathbb{Q} \setminus \{0\}, \cdot)$, neboť celá čísla vzhledem k násobení netvoří grupu. Kromě 1 a -1 k celým číslům nenajdeme v $(\mathbb{Z} \setminus \{0\}, \cdot)$ čísla inverzní.
3) Množina zbytkových tříd $(\mathbb{Z}_3, +)$ s operací sčítání modulo 4 není podgrupou v grupě $(\mathbb{Z}_6, +)$ zbytkových tříd modulo 6, neboť jednak mají nosné množiny jiné prvky: zatímco v $\mathbb{Z}_6$ číslo 3 patří do třídy $\overline{3}$, tak v $\mathbb{Z}_3$ číslo 3 patří do třídy $\overline{0}$, a jednak i kdybychom odhlédli od obsahu tříd rozkladu a pracovali pouze s reprezentanty tříd rozkladu, tak jsou na obou množinách jinak definované operace: zatímco v $\mathbb{Z}_3$ je $2 + 2 = 1$, tak v $\mathbb{Z}_6$ je $2 + 2 = 4$.
4) Grupa $(U(10), \cdot)$ není podgrupou grupy $(U(40), \cdot)$. Sice platí $U(10) \subseteq U(40)$, avšak operace je obecně definována jinak! Například $3 \cdot 7 = 1$ v grupě $(U(10), \cdot)$, avšak $3 \cdot 7 = 21$ v grupě $(U(40), \cdot)$.

Triviální podgrupa a nevlastní podgrupa grupy

Snadno uhodneme, že nejmenší (ve smyslu počtu prvků) podgrupou grupy $(G, \cdot)$ je grupa $(\{e_G\}, \cdot)$, kde e_G je neutrální prvek v grupě $(G, \cdot)$. Musíme ověřit vlastnosti podgrupy:

(i) Platí $\{e_G\} \subseteq G$, neboť $e_G \in G$.
(ii) Operace na nosiči $\{e_G\}$ je restrikcí operace „$\cdot$“, platí $e_G \cdot e_G = e_G$. Říkáme, že „předpis operace se nemění“.
(iii) Zbývá ukázat, že $(\{e_G\}, \cdot)$ tvoří grupu. Množina $(\{e_G\}$ je neprázdná a operace „$\cdot$“ je uzavřená na $\{e_G\}$, protože pro každé $e_G \in \{e_G\}$ platí $e_G \cdot e_G = e_G \in \{e_G\}$. Proto $(\{e_G\}, \cdot)$ je grupoid. Operace „$\cdot$“ je asociativní, protože $e_G \cdot (e_G \cdot e_G) = e_G \cdot e_G = (e_G \cdot e_G) \cdot e_G$.
Grupoid $(\{e_G\}, \cdot)$ má neutrální prvek e_G, neboť z vlastností neutrálního prvku víme $e_G \cdot e_G = e_G$. Ke každému prvku nosiče $\{e_G\}$ najdeme prvek inverzní, neboť $e_G \cdot e_G = e_G$, tj. $e_G^{-1} = e_G$. Neutrální prvek je inverzní sám k sobě jak v $(\{e_G\}, \cdot)$, tak v původní grupě $(G, \cdot)$.

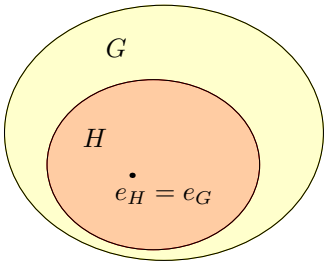
Grupu $(\{e_G\}, \cdot)$ nazýváme *triviální podgrupou* grupy $(G, \cdot)$. Ostatní podgrupy (pokud existují) se nazývají *netriviální podgrupy* grupy $(G, \cdot)$.

Naopak největší podgrupou (ve smyslu počtu prvků) grupy $(G, \cdot)$ je celá $(G, \cdot)$. Této grupě říkáme *nevlastní podgrupa* grupy $(G, \cdot)$. Ostatní podgrupy (pokud existují) se nazývají *vlastní podgrupy* grupy $(G, \cdot)$.

Otázka: Označme x nějaký prvek, který je inverzní sám k sobě v grupě $(G, \cdot)$. Je $(\{x\}, \cdot)$ podgrupou grupy $(G, \cdot)$?

Neutrální prvek podgrupy

Vyvstává přirozená otázka: jaký je vztah mezi neutrálním prvkem grupy a neutrálním prvkem její podgrupy. Mějme grupu $(G, \cdot)$ a její podgrupu $(H, \cdot)$. Protože $(H, \cdot)$ je podgrupa grupy $(G, \cdot)$ a $(H, \cdot)$ je grupa, tak musí mít neutrální prvek. Označme e_G neutrální prvek $(G, \cdot)$ a označme e_H neutrální prvek $(H, \cdot)$. Je možné, aby grupa a její podgrupa měly různé neutrální prvky? Tj. aby platilo $e_H \neq e_G$? Ukážeme, že neutrální prvek každé podgrupy musí být totožný s neutrálním prvkem grupy (Obrázek 3.4.).



Obrázek 3.4.: *Neutrální prvek podrupy je totožný s neutrálním prvkem grupy.*

Věta 3.1. *Mějme grupu $(G,\cdot)$ a její podgrupu $(H,\cdot)$. Neutrální prvek e_G grupy $(G,\cdot)$ patří do H a je současně neutrálním prvkem $(H,\cdot)$.*

Důkaz. Víme, že $(H,\cdot)$ je grupa, proto $H \neq \emptyset$. Označme neutrální prvek grupy $(H,\cdot)$ jako e_H. Potom pro každé $h \in H$ platí $h \cdot e_H = e_H \cdot h = h$. Potom ale také platí $h \cdot e_G = h$, kde e_G je neutrální prvek grupy $(G,\cdot)$, $e_G \in G$. Porovnáním dostaneme $h \cdot e_H = h = h \cdot e_G$ a s využitím věty o krácení (Věta 2.6.) v grupě $(G,\cdot)$ dostáváme $e_G = e_H$. Proto platí $e_G \in H$ a $e_G = e_H$ je současně neutrálním prvkem podgrupy $(H,\cdot)$. □

Otázka: Proč v důkazu Věty 3.1. stačí ověřit rovnost $h \cdot e_H = h = h \cdot e_G$ a nemusíme ověřovat rovnost $e_H \cdot h = h = e_G \cdot h$?

Příklad 3.4. Uveďme několik příkladů podgrup a jejich neutrálních prvků.

1) Grupa celých čísel s operací obvyklého sčítání $(\mathbb{Z},+)$ je podgrupou v grupě racionálních čísel s operací obvyklého sčítání $(\mathbb{Q},+)$ a obě mají neutrální prvek 0.
2) V grupě celých čísel s operací obvyklého sčítání $(\mathbb{Z},+)$ je neutrálním prvkem číslo 0 a číslo 0 je neutrálním prvkem všech podgrup $(k\mathbb{Z},+)$ (grupy násobků čísla k, kde k je libovolné přirozené číslo).
3) V grupě nenulových reálných $(\mathbb{R}\setminus\{0\},\cdot)$ je neutrálním prvkem číslo 1 a proto i její podgrupa nenulových racionálních čísel $(\mathbb{Q}\setminus\{0\},\cdot)$ má neutrální prvek 1.
4) V grupě $(M_{n,n}(\mathbb{Q}),\cdot)$ regulárních matic řádu n s racionálními koeficienty s operací obvyklého násobní matic je neutrálním prvkem jednotková matice $E_{n,n}$. Matice $E_{n,n}$ je současně neutrálním prvkem i v podgrupě $(D_{n,n}(\mathbb{Q}),\cdot)$ diagonálních regulárních matic řádu n s racionálními koeficienty s operací obvyklého násobení matic.

Průnik dvou podgrup

Následující věta říká, že průnik dvou podgrup dané grupy je také podgrupou této grupy.

Věta 3.2. *Mějme grupu $(G,\cdot)$ a její podgrupy $(H_1,\cdot)$ a $(H_2,\cdot)$. Potom $(H_1 \cap H_2,\cdot)$ je také podgrupa grupy $(G,\cdot)$.*

Důkaz. Ukážeme, že $(H_1 \cap H_2,\cdot)$ splňuje definici podgrupy. Nejprve si uvědomíme, že $(H_1 \cap H_2) \subseteq G$, neboť podle předpokladu musí být $H_1 \subseteq G$ a $H_2 \subseteq G$. Dále podle Věty 3.1. jistě neutrální prvek e grupy G patří do H_1 i H_2, proto $H_1 \cap H_2 \neq \emptyset$, neboť $e \in (H_1 \cap H_2)$. Dále podle definice ukážeme, že $(H_1 \cap H_2,\cdot)$ je podgrupou $(G,\cdot)$.

(i) Uzavřenost si uvědomíme snadno: Protože pro každé $a,b \in H_1 \cap H_2$ je $a \cdot b \in H_1$ a současně $a \cdot b \in H_2$, tak $a \cdot b \in (H_1 \cap H_2)$. To znamená, že $(H_1 \cap H_2,\cdot)$ je grupoid.
(ii) Asociativita se „zdědí“ z asociativity operace na celé množině G (Cvičení 0.6.6.).
(iii) Existence neutrálního prvku v $H_1 \cap H_2$ plyne z Věty 3.1.
(iv) Mějme libovolný $a \in (H_1 \cap H_2)$. Protože $(H_1,\cdot)$ je podgrupa, tak $a^{-1} \in H_1$. Analogicky $a^{-1} \in H_2$ a proto $a^{-1} \in (H_1 \cap H_2)$.

Tím jsme ověřili všechny vlastnosti podgrupy, proto $(H_1 \cap H_2,\cdot)$ je podgrupou v $(G,\cdot)$. □

Příklad 3.5.

1) V grupě celých čísel s operací obvyklého sčítání $(\mathbb{Z},+)$ máme podgrupy $(2\mathbb{Z},+)$ a $(3\mathbb{Z},+)$. Jejich průnik je podgrupa $(6\mathbb{Z},+)$, neboť $2\mathbb{Z} \cap 3\mathbb{Z} = 6\mathbb{Z}$.
2) Grupy $(\mathbb{Z}_2,+)$ a $(\mathbb{Z}_3,+)$ mají prázdný průnik, neboť žádná zbytková třída není společná množina. Z Příkladu 3.3. víme, že grupa $(\mathbb{Z}_2,+)$ ani grupa $(\mathbb{Z}_3,+)$ nejsou podgrupou $(\mathbb{Z})$, navíc nejsou současně podgrupou žádné grupy, neboť ani nemají žádné společné prvky.

Tvrzení o průniku podgrup je možno zobecnit, jak ukážeme na straně 106. Naopak sjednocení podgrup zpravidla podgrupou není (Cvičení 6.2.5.).

Cvičení

3.1.1. Ukažte, že pro každý prvek $a \in G$, kde a není neutrální v grupě $(G,\cdot)$, platí $a \cdot a \neq a$.

3.1.2. Použijte Cvičení 3.1.1. k důkazu tvrzení, že jediná jednoprvková podgrupa libovolné grupy $(G,\cdot)$ je $(\{e\},\cdot)$, kde e je neutrální prvek grupy $(G,\cdot)$.

3.1.3. Uvažujme množinu $5\mathbb{Z} = \{5k : k \in \mathbb{Z}\}$ a zavedeme operaci „$\oplus$“ $5\mathbb{Z} \times 5\mathbb{Z} \to 5\mathbb{Z}$ definovanou předpisem $\forall x, y \in 5\mathbb{Z} : x \oplus y = x + y$. Ukažte, že $(5\mathbb{Z}, \oplus)$ je podgrupou grupy $(\mathbb{Z}, +)$.

3.1.4. Zobecněte Cvičení 3.1.3. pro množinu $n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$, kde $n \in \mathbb{N}$. Ukažte, že $(n\mathbb{Z}, \oplus)$ je podgrupou grupy $(\mathbb{Z}, +)$.

3.1.5. Mějme dihedrální grupu $(D_6, \circ)$. Najděte nějakou její podgrupu s a) jedním prvkem, b) dvěma prvky, c) třemi prvky. d) Kolik takových podgrup existuje? e) Najdete nějakou podgrupu se čtyřmi prvky?

3.1.6. Najděte příklad dvou různých vlastních podgrup dihedrální grupy $(D_6, \circ)$, jejichž sjednocení a) je podgrupou $(D_6, \circ)$, b) není podgrupou $(D_6, \circ)$.

3.1.7. Mějme grupu $(G, \cdot)$ a množinu X všech jejích podgrup. Na množině X zavedeme relaci $\subseteq$ „být podgrupou“. Ukažte, že tato relace je relací částečného uspořádání.

3.2. Ověření podgrupy

Přirozeně vystává otázka pro $H \subseteq G$, jak poznáme, zda $(H, \cdot)$ je podgrupa $(G, \cdot)$? V této podkapitole ukážeme několik vět, které ověření usnadní. Některé vlastnosti, jejichž platnost nepřímo vyplývá z definice podgrupy, ověřovat nemusíme.

Věta 3.3. Test podgrupy
Mějme grupu $(G, \cdot)$. Nechť platí následující podmínky:

(i) $H \subseteq G$, *(H je podmnožina v G)*
(ii) $H \neq \emptyset$, *(H je neprázdná)*
(iii) $\forall a, b \in H : a \cdot b \in H$, *(operace je uzavřená na H)*
(iv) $\forall a \in H : a_G^{-1} \in H$ (kde a_G^{-1} je inverzní prvek k a vzhledem ke grupě G). *(v H existují inverze)*

Potom $(H, \cdot)$ je podgrupa grupy $(G, \cdot)$.

Důkaz. Ověříme vlastnosti podgrupy dle definice.

(i) $H \subseteq G$ je splněno dle předpokladu (i) věty.
(ii) Operace na $(H, \cdot)$ je restrikce operace z $(G, \cdot)$ a dle předpokladu (iii) věty je uzavřená na H.
(iii) Ověříme, že $(H, \cdot)$ je sama grupou: Nosič je neprázdná množina ($H \neq \emptyset$ platí ihned z předpokladu (ii) věty), uzavřenost operace „$\cdot$“ plyne z předpokladu (iii) věty $\forall a, b \in H : a \cdot b \in H$. Proto je $(H, \cdot)$ grupoid.
Asociativita operace „$\cdot$“ je dána asociativitou operace na G. Máme-li operaci, pro kterou pro každé $a, b, c \in G$ platí $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ na celé množině G, tak podle Cvičení 0.6.6. totéž platí i na libovolné (uzavřené) podmnožině H.
Existence neutrálního prvku plyne z uzavřenosti operace a z existence inverze: je-li $a \in H$, tak podle předpokladu (iv) věty platí $a_G^{-1} \in H$. Protože v grupě G platí $a \cdot a_G^{-1} = e_G \in G$, tak z uzavřenosti (předpoklad (iii)) je také $e_G \in H$. Nyní v grupě $(G, \cdot)$ pro každé $a \in H$ platí $a \cdot e_G = e_G \cdot a = e_G$, což musí platit i v restrikci na množinu H a proto neutrální prvek v restrikci na množinu H je také e_G.
A konečně existence inverzního prvku ke každému prvku plyne ihned z předpokladu (iv) věty.

Místo podmínek v definici podgrupy stačí ověřovat jednodušší podmínky (i) až (iv). □

Otázka: Proč v důkazu Věty 3.3. nemůžeme říci, že existence neutrálního prvku v podgrupě $(H, \cdot)$ plyne z Věty 3.1.?

Příklad 3.6. Mějme komutativní grupu $(G, \cdot)$ s neutrálním prvkem e. Označme H množinu všech prvků a z G, pro které platí, že $a^2 = e$. Ukažte, že $(H, \cdot)$ je podgrupou grupy $(G, \cdot)$.
Ověříme všechny předpoklady Věty 3.3. Evidentně platí $H \subseteq G$ a jistě je množina H neprázdná, protože například neutrální prvek grupy $(G, \cdot)$ do H patří, neboť $e^2 = e$.

Dále ukážeme, že operace „$\cdot$“ je na množině H uzavřená. Jestliže $a, b \in H$, tak podle definice H platí $a^2 = e$ a $b^2 = e$. Potom s využitím komutativity operace dostaneme $(a \cdot b)^2 = (a \cdot b) \cdot (a \cdot b) = a \cdot b \cdot a \cdot b = a \cdot a \cdot b \cdot b = a^2 \cdot b^2 = e \cdot e = e$.a Platí $e \in H$, což znamená, že $(a \cdot b) \in H$ a operace je uzavřená na H.

A konečně je-li $a \in H$, tak krácením rovnosti $a^{-1} \cdot a = e = a \cdot a$ ihned vidíme, že $a^{-1} = a$. To znamená, že každý prvek a je inverzní sám k sobě, tj. pro každé $a \in H$ je $a^{-1} = a$ a $a^{-1} \in H$. Můžeme shrnout, že podle Věty 3.3. je $(H, \cdot)$ podgrupou grupy $(G, \cdot)$. ✓

Otázka: Je nutno v Příkladu 3.6. předpokládat, že grupa $(G,\cdot)$ je komutativní?

Podmnožiny, které nejsou podgrupou
Abychom ukázali, že podmnožina $H \subseteq G$ grupy $(G,\cdot)$ není podgrupou, stačí například ukázat, že nastala některá z následujících situací.

- Najdeme dva prvky $a, b \in H$, pro které výsledek operace $a \cdot b$ nepatří do H.
- Neutrální prvek e grupy $(G,\cdot)$ nepatří do H.
- Najdeme prvek $a \in H$, jehož inverze do H nepatří.

Příklad 3.7. Je grupoid $(\mathbb{N},+)$ podgrupou grupy $(\mathbb{Z},+)$?
Grupoid $(\mathbb{N},+)$ není podgrupou grupy $(\mathbb{Z},+)$, protože sám není grupou. Neobsahuje neutrální prvek operace „+“ ani inverzní prvky k žádnému prvku $a \in \mathbb{N}$. ✓

Příklad 3.8. Je grupa $(\mathbb{Z}_n,+)$ podgrupou grupy $(\mathbb{Z},+)$? (O grupách zbytkových tříd je psáno v Kapitole 3.5.)
Grupa $(\mathbb{Z}_n,+)$ je grupou zbytkových tříd modulo n, zatímco grupa $(\mathbb{Z},+)$ obsahuje celá čísla. Proto $\mathbb{Z}_n \not\subseteq \mathbb{Z}$ a tudíž grupa zbytkových tříd modulo n není podgrupou celých čísel. Dokonce i pro $n = 1$ je $\mathbb{Z}_1 = \{\overline{0}\} = \{\mathbb{Z}\} \neq \mathbb{Z}$.

Kdybychom místo zbytkových tříd pracovali jen s reprezentanty a grupu $(\mathbb{Z}_n,+)$ chápali jako množinu čísel $\{0,1,\ldots,n-1\}$ operací danou Cayleyho tabulkou, tak rozlišíme dva případy. Výsledky operací jsou pro nenulová čísla definovány jinak, a proto se nejedná o podgrupu celých čísel. Například součet n jedniček $1+1+\cdots+1 = n$ v grupě $(\mathbb{Z},+)$, avšak v $(\mathbb{Z}_n,+)$ je součet roven 0. Jedině pro $n = 1$ bude $(\mathbb{Z}_n,+) = (\{\overline{0}\},+)$ a tuto grupu je možno chápat jako podgrupu $(\mathbb{Z},+)$, pokud třídu $\overline{0}$ ztotožníme s prvkem 0. ✓

Další testy podgrupy
Následující věta říká, že počet ověřovaných vlastností podgrupy je možno zkrátit. Test uzavřenosti operace a test existence inverzních prvků lze spojit v jediný.

Věta 3.4. Rychlý test podgrupy
Mějme grupu $(G,\cdot)$. Jestliže platí následující podmínky

(i) $H \subseteq G$, *(podmnožina v G)*
(ii) $H \neq \emptyset$, *(H neprázdná)*
(iii) $\forall a,b \in H : a \cdot b^{-1} \in H$, *(uzavřená s inverzemi)*

potom $(H,\cdot)$ je podgrupa grupy $(G,\cdot)$.

Důkaz. Opět ověříme vlastnosti podgrupy požadované v definici:

(i) $H \subseteq G$ je splněno dle předpokladu (i) věty.
(ii) Operace na $(H,\cdot)$ je restrikce operace z $(G,\cdot)$.
(iii) Jedná se o grupu: Nosič H je neprázdná množina dle předpokladu (ii) věty. Uzavřenost operace v grupoidu $(H,\cdot)$ ukážeme nakonec.
Asociativita operace „$\cdot$“ na množině H se „zdědí“ z asociativity operace „$\cdot$“ na množině G (Cvičení 0.6.6.).
Víme, že $H \neq \emptyset$ a proto existuje prvek $a \in H$. Dle předpokladu (iii) věty pro každé $a,b \in H$ platí $a \cdot b^{-1} \in H$. Neutrální prvek patří do grupoidu $(H,\cdot)$, neboť volbou $a = b$ dostaneme, že $bb^{-1} = e_G \in H$, tedy $e_H = e_G \in H$.
Dále ukážeme, že pro každé $x \in H$ patří inverzní prvek x^{-1} do H. Vhodnou volbou $a = e_G$ a volbou $b = x$, dostaneme z předpokladu (iii) věty, že $a \cdot b^{-1} = e_G \cdot x^{-1} = x^{-1} \in H$.
A konečně uzavřenost operace „$\cdot$“ plyne z předpokladu (iii). Stačí vzít za b prvek b^{-1}, o kterém jsme již z předpokladu (iii) dokázali, že $b^{-1} \in H$. Opět s využitím předpokladu (iii) dostaneme $a \cdot (b^{-1})^{-1} = a \cdot b \in H$.

Tím jsme ověřili předpoklady definice podgrupy $(H,\cdot)$ v grupě $(G,\cdot)$. □

Příklad 3.9. Mějme grupu celých čísel s operací sčítání $(\mathbb{Z},+)$. Ukážeme, že $(\mathbb{S},+)$ je podgrupou v dané grupě.
Podle Rychlého testu podgrupy (Věta 3.4.) stačí ověřit tři vlastnosti. Množina $\mathbb{S}$ je jistě podmnožinou $\mathbb{Z}$ a je jistě neprázdná. Nyní stačí ověřit, že pro libovolná dvě sudá čísla $a,b \in \mathbb{S}$ je i $a - b \in \mathbb{S}$. Je však jasné, že rozdíl dvou sudých čísel je opět sudé číslo, a proto $(\mathbb{S},+)$ je podgrupou v grupě $(\mathbb{Z},+)$. ✓

Pro konečné podgrupy můžeme využít ještě jednodušší ověření. Jestliže H je konečná podmnožina, není třeba ověřovat existenci inverze jako ve Větě 3.4.

Věta 3.5. Test konečné podgrupy
Mějme grupu $(G,\cdot)$. Jestliže platí následující podmínky

(i) $H \subseteq G$, *(H je podmnožina v G)*
(ii) $H \neq \emptyset$, *(H je neprázdná)*
(iii) H *je konečná množina,* *(H je konečná)*
(iv) $\forall a,b \in H : a \cdot b \in H$, *(operace je uzavřená na H)*

potom $(H,\cdot)$ je (konečná) podgrupa $(G,\cdot)$.

Důkaz. Podle Věty 3.3. stačí už jen dokázat, že pro všechna $a \in H$ platí $a^{-1} \in H$. Už víme, že $H \neq \emptyset$, proto existuje $a \in H$.

Je-li $a = e_G$, tak jistě $a_G^{-1} = e_G$, přičemž podle Věty 3.1. je $e_G \in H$. Je-li $a \neq e_G$, tak podle posledního předpokladu (iv) věty musí být $a^2 = a \cdot a \in H$, potom $a^3 = a \cdot a^2 \in H$ a také $a^4 = a \cdot a^3 \in H$ a tak dále. Pro každé $n \in \mathbb{N}$ je $a^n \in H$. Protože H je konečná množina, tak nemohou být všechny mocniny různé a proto existují $n_1, n_2 \in \mathbb{N}$, $n_1 > n_2$ taková, že $a^{n_1} = a^{n_2}$.

Nyní přepíšeme $n_1 = n_2 + d$, kde $d \in \mathbb{N}$.

$$\begin{aligned} a^{n_1} &= a^{n_2} \\ a^{n_2+d} &= a^{n_2} \\ a^{n_2} \cdot a^d &= a^{n_2} \cdot e_G. \end{aligned}$$

Podle Věty 2.6. můžeme v grupě $(G,\cdot)$ krátit. Krácením dostaneme

$$a^d = e_G.$$

Máme neutrální prvek grupy $(G,\cdot)$ v množině H a tento prvek je neutrálním prvkem i grupoidu $(H,\cdot)$, protože pracujeme s restrikcí operace „$\cdot$“. Navíc pro $d > 1$ je $a^d = a^{d-1} \cdot a = a \cdot a^{d-1} = e$. To ale podle definice inverze znamená, že $a^{-1} = a^{d-1}$ a navíc $a^{d-1} \in H$. Pro $d = 1$ je $a^d = a = e_G$, což je případ řešený na začátku důkazu. □

V předpokladech Věty 3.5. požadujeme, aby množina H byla konečná. Je dobré si uvědomit, že pro nekonečné grupy tvrzení Věty 3.5. platit nemusí. Například $(\mathbb{Z},+)$ je grupa, $\mathbb{N}$ je neprázdná podmnožina $\mathbb{Z}$ a platí, že pro všechna $a,b \in \mathbb{N}$ je $a+b \in \mathbb{N}$, avšak množina $\mathbb{N}$ není konečná a $(\mathbb{N},+)$ není podgrupou v $(\mathbb{Z},+)$. Pro nenulové prvky neexistují v $\mathbb{N}$ opačné prvky, není $(\mathbb{N},+)$ grupou.

Příklad 3.10. Mějme grupu $(\mathbb{Z}_5 \setminus \{\overline{0}\},\cdot) = (\{1,2,3,4\},\cdot)$ (operaci „násobení modulo 5“), kde operace „$\cdot$“ je popsána Tabulkou 3.1. (Ověření, že se jedná o grupu, je ponecháno jako Cvičení 3.2.3.)

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Tabulka 3.1.: *Operace násobení nenulových prvků $\{1,2,3,4\}$ modulo 5.*

a) Ukažte že pro $H = \{1,4\}$ je $(H,\cdot)$ podgrupa dané grupy. b) Dále ukažte, že pro $H' = \{1,3\}$ dvojice $(H',\cdot)$ není podgrupa dané grupy.
a) Je zřejmé, že $H \subseteq G$, $H \neq 0$. Protože H je konečná množina, můžeme ověřit uzavřenost tabulkou podle Věty 3.5. Operace na H je popsána Tabulkou 3.2. Z tabulky je zřejmé, že operace „$\cdot$“ je uzavřená na H (v tabulce jsou pouze prvky ze záhlaví), proto je $(H,\cdot)$ podgrupa grupy $(G,\cdot)$.

$\cdot$	1	4
1	1	4
4	4	1

Tabulka 3.2.: *Tabulka restrikce operace na množině $H = \{1,4\}$.*

$\cdot$	1	3
1	1	3
3	3	4

Tabulka 3.3.: *Tabulka restrikce operace z množiny* $G = \{1, 2, 3, 4\}$ *na množinu* $H' = \{1, 3\}$ *není tabulkou operace.*

b) Kdybychom vzali dvojici $H' = \{1, 3\}$, tak sice $H \subseteq G$, $H \neq \emptyset$ a podmnožina H je konečná, ale tabulka operace (Tabulku 3.3.) není uzavřená vhledem k restrikci operace „$\cdot$“ na množinu H', protože tabulka obsahuje kromě prvků 1 a 3 navíc prvek 4. $(H', \cdot)$ není podgrupa dané grupy. ✓

Všimněte si, že formulace Věty 3.5. umožňuje ověřovat konečné podgrupy i v nekonečné grupě $(G, \cdot)$. Jestliže H je konečná a neprázdná podmnožina v G, tak abychom ukázali, že $(H, \cdot)$ je konečnou podgrupou, tak stačí uvěřit uzavřenost na množině H.

Příklad 3.11. Ukažte, že v (nekonečné) grupě $(\mathbb{Q} \setminus \{0\}, \cdot)$ tvoří dvouprvková množina $H = \{1, -1\}$ konečnou podgrupu.
Tvrzení ukážeme přímo, ověříme předpoklady Věty 3.5.

(i) Jistě platí, že $H \subseteq \mathbb{Q}$,
(ii) dále H je neprázdná a
(iii) H je konečná množina.
(iv) Uzavřenost ihned vidíme z Cayleyho Tabulky 3.4.

Celkem dostáváme, že $(\{1, -1\}, \cdot)$ je konečná podgrupa grupy $(\mathbb{Q}, \cdot)$. ✓

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

Tabulka 3.4.: *Tabulka restrikce operace z množiny* $\mathbb{Q}$ *na množinu* $H = \{1, -1\}$.

Příklad 3.12. Sestavíme tabulku násobení *lichých čísel* (tříd) modulo 10. Dostaneme Tabulku 3.5.

$\cdot$	1	3	5	7	9
1	1	3	5	7	9
3	3	9	5	1	7
5	5	5	5	5	5
7	7	1	5	9	3
9	9	7	5	3	1

Tabulka 3.5.: *Operace násobení nenulových prvků* $\{1, 3, 5, 7, 9\}$ *modulo* 5.

Operace „$\cdot$“ je na množině $\{1, 3, 5, 7, 9\}$ jistě uzavřená, neboť součin dvou lichých čísel je opět liché číslo modulo 10 Podle Testu konečné podgrupy (Věta 3.5.) by se proto mohlo zdát, že se jedná o podgrupu $(\mathbb{Z}_{10}, \cdot)$. Při bližším rozboru však vidíme, že prvek 5 nemá inverzi a o grupu se nejedná. Vysvětlíme, kde nastal problém s použitím Věty 3.5.
Třebaže $\{1, 3, 5, 7, 9\} \subseteq \mathbb{Z}_{10}$ a operace „$\cdot$“ je na množině $\{1, 3, 5, 7, 9\}$ uzavřená, tak Test konečné podgrupy (Větu 3.5.) použít nelze, neboť grupoid $(\mathbb{Z}_{10}, \cdot)$ není grupou a nejsou tak splněny všechny předpoklady Věty 3.5. ✓

Pro úplnost zmíníme, že vynecháme-li prvek 5 z nosné množiny grupoidu z Příkladu 3.12., tak dostaneme grupu jednotek $(U(10), \cdot)$, kterou jsme zavedli v Příkladu 2.19. na straně 51.

Cvičení

3.2.1. Mějme komutativní grupu $(G, \cdot)$ s neutrálním prvkem (jedničkou) e. Označme $H = \{h \in G : h = h^{-1}\}$ (množina prvků, které jsou inverzní samy k sobě). Dokažte, že $(H, \cdot)$ je podgrupa grupy $(G, \cdot)$.

3.2.2. Ukažte, že v nekomutativní grupě $(G, \cdot)$ tvrzení ze Cvičení 3.2.1. nemusí platit.

3.2.3. Ukažte, že $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ je grupa.

3.2.4. Najděte příklad grupy $(G, \cdot)$, ve které pro každé přirozené číslo n existuje podgrupa $(H_n, \cdot)$ taková, že H_n má právě n prvků. Vlastnosti podgrupy ověřte.

3.2.5. Najděte všechny podgrupy v grupě určené Tabulkou 2.15. ve Cvičení 2.5.6.

3.2.6. Najděte příklad nekomutativní grupy a její netriviální podgrupy, která je komutativní.

3.2.7. Mějme grupu nenulových komplexních čísel s operací násobení $(\mathbb{C}\setminus\{0\},\cdot)$. Označme $J=\{z\in\mathbb{Z}: |z|=1\}$. Ukažte, že $(J,\cdot)$ je podgrupou grupy $(\mathbb{C}\setminus\{0\},\cdot)$.

3.2.8. Pro každé přirozené číslo n najděte příklad konečné grupy $(G,\cdot)$ a takových jejích podgrup $(H_n,\cdot)$, že H_n má právě n prvků.*

3.2.9. Ukažte, že grupa $(U(10),\cdot)$ je podgrupou grupy $(U(20),\cdot)$.

3.2.10. Dokažte nebo vyvraťte následující tvrzení: Mějme liché přirozené číslo m. Grupa $(U(2m),\cdot)$ je podgrupou grupy $(U(4m),\cdot)$.

3.3. Centrum grupy

Důležitým příkladem podgrup je tzv. centrum grupy.

Definice Centrum grupy
Centrem grupy $(G,\cdot)$ je podmnožina všech prvků G, které komutují s každým prvkem grupy $(G,\cdot)$. Centrum grupy $(G,\cdot)$ značíme $Z(G)$ a platí $Z(G)=\{a\in G:$ pro každé $g\in G$ platí $ag=ga\}$.

Příklad 3.13. Uveďme několik klasických příkladů center grup.

1) V komutativní grupě $(G,\cdot)$ je vždy centrem celá množina G.
2) V libovolné grupě $(G,\cdot)$ je centrum vždy neprázdná množina, neboť neutrální prvek do centra vždy patří.
3) V grupě regulárních matic řádu 2 s operací obvyklého násobní $(M_{2,2},\cdot)$ je centrum vlastní podmnožinou množiny $M_{2,2}$. Například jednotkové matice $E_{2,2}$ a jejich násobky do centra vždy patří (Cvičení 3.3.2.). Na druhou stranu například regulární matice $I+E_{i,j}$, kde I a jednotková matice a $E_{i,j}$ obsahuje $a_{i,j}=1$ a zbývající prvky má nulové, s maticemi v $M_{2,2}$ zpravidla nekomutuje. Pro libovolnou matici $A\in M_{2,2}$ obsahuje součin $A\cdot(I+E_{i,j})=A+AE_{i,j}$, kde druhý člen $AE_{i,j}$ obsahuje jen nulové prvky a v i-tém řádku kopii j-tého řádku matice A, zatímco v součinu $(I+E_{i,j})\cdot A=A+E_{i,j}A$ obsahuje druhý člen nulové prvky a v j-tém sloupci kopii i-tého sloupce matice A.
Například pro $A=\begin{pmatrix}1&2\\3&4\end{pmatrix}$, $E_{1,2}=\begin{pmatrix}0&5\\0&0\end{pmatrix}$ dostaneme

$$A\cdot(I+E_{i,j})=\begin{pmatrix}1&2\\3&4\end{pmatrix}\cdot\begin{pmatrix}1&5\\0&1\end{pmatrix}=\begin{pmatrix}1&7\\3&19\end{pmatrix}\neq(I+E_{i,j})\cdot A=\begin{pmatrix}1&5\\0&1\end{pmatrix}\cdot\begin{pmatrix}1&2\\3&4\end{pmatrix}=\begin{pmatrix}16&22\\3&4\end{pmatrix}.$$

Příklad 3.14. Uveďme několik podmnožin, které nejsou centrem grupy.

1) Celá množina G *není* centrem nekomutativní grupy $(G,\cdot)$, neboť v nekomutativní grupě existují $a,b\in G$ takové, že $a\cdot b\neq b\cdot a$.
2) Množina rotací $R=\{R_0,R_{360/n},\ldots,R_{360(n-1)/n}\}$ pro $n>1$ *není* centrem dihedrální grupy $(D_n,\circ)$, neboť existují zrcadlení $f\in D_n$ taková, že $f\circ R_{360/n}\neq R_{360/n}\circ f$ (Cvičení 3.3.6.).

Následující věta ukazuje, že množina centra spolu se „zděděnou“ operací tvoří podgrupu.

Věta 3.6. *Mějme grupu $(G,\cdot)$ a její centrum $Z(G)$. Centrum $Z(G)$ spolu s restrikcí operace „$\cdot$“ tvoří podgrupu $(Z(G),\cdot)$ grupy $(G,\cdot)$.*

Důkaz. Užitím Věty 3.3. ukážeme, že $(Z(G),\cdot)$ je podgrupa grupy $(G,\cdot)$. Protože neutrální prvek e komutuje se všemi prvky g grupy G (pro každé $g\in G$ platí $ge=eg$), tak je centrum vždy neprázdné množina a podle definice centra platí $Z(G)\subseteq G$. Dále operace grupy je na centru uzavřená neboť pro každé $a,b\in Z(G)$ a každé $g\in G$ platí $(ab)g=a(bg)=a(gb)=(ag)b=(ga)b=g(ab)$, přičemž druhá a předposlední rovnost vyplývá z definice vlastností prvků $Z(G)$ a ostatní rovnosti plynou z asociativity operace „$\cdot$“.

Zbývá ověřit existenci inverze ke každému prvku $a \in Z(G)$. Ukážeme, že $a^{-1} \in Z(G)$. Vskutku, stačí rovnost $ag = ga$ zleva i zprava vynásobit prvkem a^{-1}. Dostaneme

$$\begin{aligned} a^{-1}aga^{-1} &= a^{-1}gaa^{-1} \\ ega^{-1} &= a^{-1}ge \\ ga^{-1} &= a^{-1}g, \end{aligned}$$

což znamená, že a^{-1} také patří do centra $Z(G)$. □

Ve Cvičení 3.3.7. ukážeme, že centrum je dokonce komutativní podgrupa (i v nekomutativní grupě).

Cvičení

3.3.1.$^{\heartsuit}$ *Ukažte, že každá grupa $(G, \cdot)$ má neprázdné centrum.*

3.3.2. Ukažte, že násobky jednotkové matice $E_{n,n}$ patří do centra grupy regulárních matic $(M_{n,n}, \cdot)$.

3.3.3. Najděte centra následujících grup: a) $(\mathbb{Z}_5, +)$, b) $(U(20), \cdot)$, c) $(D_6, \circ)$, d) $(D_8, \circ)$.

3.3.4. Ukažte, že do centra grupy regulárních matic $(M_{n,n}, \cdot)$ nepatří jiné matice, než násobky jednotkových matic.*

3.3.5. Ukažte, že centrum dihedrální grupy $(D_n, \circ)$ je $\{R_0\}$ pro n liché a $\{R_0, R_{180}\}$ pro n sudé.

3.3.6. Ukažte, že množina rotací $R = \{R_0, R_{360/n}, \ldots, R_{360(n-1)/n}\}$ pro $n > 1$ není centrem dihedrální grupy $(D_n, \circ)$. Návod: najděte takové zrcadlení $f \in D_n$, že $f \circ R_{360/n} \neq R_{360/n} \circ f$.

3.3.7.$^{\heartsuit}$ *Ukažte, že v libovolné grupě $(G, \cdot)$ je centrum $Z(G)$ spolu s restrikcí operace „$\cdot$“ komutativní podgrupa $(Z(G), \cdot)$.*

3.4. Komplexy v grupě a operace s nimi

Nejprve zavedeme jednu přirozenou operaci s podmnožinami (ne nutně podgrupami) dané grupy. V Kapitole 4. ukážeme, jak z podgrup konstruovat takové systémy komplexů, které budou samy grupami.

Definice Komplex
Mějme grupu (případně pologrupu) $(G, \cdot)$. *Komplexem* v grupě $(G, \cdot)$ nazveme libovolnou neprázdnou podmnožinu množiny G.

Připomeňme, že symbolem 2^A označujeme potenční množinu množiny A. Někdy se potenční množina množiny A značí také $P(A)$. Potenční množina 2^A obsahuje všechny možné komplexy dané množiny A a navíc prázdnou množinu $\emptyset$, která komplexem není.

Příklad 3.15. Uveďme několik jednoduchých příkladů komplexů.

1) V grupě celých čísel s operací obvyklého sčítání $(\mathbb{Z}, +)$ tvoří množina sudých čísel $\mathbb{S}$ i množina lichých čísel $\mathbb{L}$ komplexy. Dvojice $(\mathbb{S}, +)$ tvoří dokonce podgrupu v $(\mathbb{Z}, +)$, avšak $(\mathbb{L}, +)$ podgrupu netvoří. Dále máme například komplexy $\mathbb{N}$, $\mathbb{P}$, $[1, 10]$ a nebo $\{42\}$. Prázdná podmnožina $\emptyset$ komplexem v grupě $(\mathbb{Z}, +)$ (ani žádné jiné grupě) není.
2) Racionální čísla $\mathbb{Q}$ jsou komplexem v grupě reálných čísel s operací sčítání $(\mathbb{R}, +)$.
3) V grupě reálných čísel s operací obvyklého sčítání $(\mathbb{R}, +)$ je komplexem například množina $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$. Podobně máme komplexy $\mathbb{Z}[\sqrt{3}]$ a $\mathbb{Z}[\sqrt{5}]$.
4) V grupě nenulových reálných čísel s operací obvyklého násobení $(\mathbb{R} \setminus \{0\}, \cdot)$ je komplexem například množina $\mathbb{Z}[\sqrt{2}] \setminus \{0\}$, kde $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$.
5) V grupě nenulových komplexních čísel s operací obvyklého násobení $(\mathbb{C} \setminus \{0\}, \cdot)$ je komplexem například množina $\mathbb{Z}[\sqrt{-2}] \setminus \{0\}$, kde $\mathbb{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbb{Z}\}$.
6) Množina $2\mathbb{Z}_n$ je komplexem v grupě $(\mathbb{Z}_n, +)$.
7) Množina všech rotací R_n tvoří komplex v dihedrální grupě $(D_n, \circ)$ symetrií pravidelného n-úhelníka. Navíc $(R_n, \circ)$ je podgrupou $(D_n, \circ)$. Množina všech zrcadlení tvoří komplex v dihedrální grupě $(D_n, \circ)$, netvoří však podgrupu.
8) V každé konečné grupě s n prvky najdeme n jednoprvkových komplexů, $n(n-1)/2$ dvouprvkových komplexů, obecně $\binom{n}{k}$ k-prvkových komplexů s k prvky pro každé kladné k, $k \leq n$.

Příklad 3.16. Uveďme několik příkladů podmnožin či množin, které komplexem v dané grupě nejsou.

1) Racionální čísla $\mathbb{Q}$ nejsou komplexem v grupě nenulových reálných čísel s operací násobení $(\mathbb{R}\setminus\{0\},\cdot)$, neboť obsahují navíc nulu.
2) Množina $\mathbb{Z}_n$ není komplexem v grupě $(\mathbb{Z},+)$, protože $\mathbb{Z}_n \not\subseteq \mathbb{Z}$.
3) Množiny $[1,10]$, $\{42\}$, ani $\mathbb{Z}_{50}$ nejsou komplexy v grupě $(\mathbb{Z}_{100},+)$, protože nejsou podmnožiny $\mathbb{Z}_{100}$.
4) Množina prvočísel $\mathbb{P}$ není komplexem v $(\mathbb{N},+)$, neboť $(\mathbb{N},+)$ není grupa.

Na první pohled se může zdát zbytečné zavádět nový termín „komplex“, když bychom vystačili s termínem „neprázdná podmnožina“. Máme-li nějakou grupu s operací „$\cdot$“, tak ukážeme, jak zavést operaci s komplexy. Nově zavedený pojem „komplex“ tak v sobě ponese dodatečnou informaci, že s komplexy budeme zacházet jako s prvky nějaké nové grupy, přičemž operace bude vycházet z operace na výchozí grupě. Definujme následující operaci pro podmnožiny (komplexy) S_1 a S_2 nosné množiny G grupy $(G,\cdot)$.

Definice Násobení komplexů
Mějme grupu $(G,\cdot)$ a její komplexy S_1 a S_2. *Násobení komplexů* je operace „$\boxdot$“ na množině $2^G\setminus\{\emptyset\}$ (potenční množině množiny G bez prázdné množiny) definovaná vztahem

$$S_1 \boxdot S_2 = \{s_1\cdot s_2 : s_1\in S_1, s_2\in S_2\}.$$

Jestliže nebude hrozit mýlka, budeme operaci součinu komplexů pro jednoduchost značit stejně jako součin prvků grupy, tj. $S_1\cdot S_2$. V případě, že $S_1=\{a\}$ (je jednoprvková) a H je nějaký komplex $H\subseteq G$, tak definujeme

$$a\odot H = \{a\}\boxdot H = \{a\cdot h : h\in H\}$$

a tento součin komplexů můžeme pro jednoduchost značit $a\cdot H$ nebo jen aH.

Jestliže pracujeme s grupou v aditivní notaci, hovoříme o *sčítání komplexů* a píšeme analogicky $S_1\boxplus S_2$, $\{a\}\boxplus H$, nebo $a\oplus H$. Jestliže nebude hrozit mýlka, budeme operaci součtu komplexů pro jednoduchost značit stejně jako součet prvků grupy, tj. S_1+S_2, $\{a\}+H$ nebo $a+H$.

Příklad 3.17. Uveďme několik jednoduchých příkladů násobení komplexů.

1) V grupě celých čísel s operací obvyklého sčítání $(\mathbb{Z},+)$ tvoří množina sudých čísel $\mathbb{S}$ i množina lichých čísel $\mathbb{L}$ komplexy. Součinem komplexů $\mathbb{S}\boxplus\mathbb{L}$ je komplex $\mathbb{S}$. Součinem komplexů $\mathbb{L}\boxplus\mathbb{L}$ je komplex $\mathbb{L}$. Součinem komplexů $\mathbb{L}\boxplus\{1\}$ je komplex $\mathbb{S}$. Součinem komplexů $\mathbb{L}\boxplus\{2\}$ je komplex $\mathbb{L}$.
2) Množiny $\{1,3,4\}$, $\{2,3\}$ a $\{-1,4\}$ jsou komplexy v grupě $(\mathbb{Z},+)$. Součinem komplexů $\{1,3,4\}\boxplus\{2,3\}$ je komplex $\{3,5,4,6,7\}$. Součinem komplexů $\{1,3,4\}\boxplus\{-1,4\}$ je komplex $\{0,2,3,5,7,8\}$.
3) Množiny $\overline{2}_7$ a $\overline{3}_7$ jsou komplexy v grupě $(\mathbb{Z},+)$. Součinem komplexů $\overline{2}_7\boxplus\overline{3}_7$ je komplex $\overline{5}_7$. Součinem komplexů $\overline{2}_7\boxplus\{6\}$ je komplex $\overline{1}_7$.
4) Množiny $\overline{2}_7$ a $\overline{3}_7$ jsou komplexy v grupě $(\mathbb{Z},\cdot)$. Součinem komplexů $\overline{2}_7\boxplus\overline{3}_7$ není komplex $\overline{6}_7$, neboť například číslo 13 do komplexu $\overline{6}_7$ patří, avšak nepatří do uvedeného součinu. Součinem komplexů $\overline{2}_7\boxdot\{2\}$ není komplex $\overline{4}_7$, neboť například číslo 11 do komplexu $\overline{4}_7$ patří, avšak nepatří do uvedeného součinu.
5) Množina všech rotací R_n i množina všech zrcadlení Z tvoří komplexy v dihedrální grupě $(D_n,\circ)$ symetrií pravidelného n-úhelníka. Jejich součin $R_n\boxdot Z$ je komplex Z (množina všech zrcadlení).

Upozorňujeme, že násobení komplexů je jiné násobení než kartézský součin komplexů (kartézský součin neprázdných podmnožin). V kartézském součinu *sestavujeme* dvojice prvků z jednoho a druhého komplexu, při násobení komplexů dvojice prvků *vynásobíme*. Proto součin komplexů (podmnožin) nosné množiny G grupy $(G,\cdot)$ je opět komplex (podmnožina) množiny G. Naproti tomu kartézský součin komplexů je množina uspořádaných dvojic prvků množiny G a obecně není komplexem nosné množiny G, protože se nemusí jednat o podmnožinu G.

Otázky:

- Najdete takové dva komplexy $S_1,S_2\in G$ pro vhodně zvolenou grupu G, že $S_1\boxdot S_2 = S_1\times S_2$ (kde $S_1\times S_2$ značí kartézský součin množin S_1 a S_2)?
- Jak by se změnila definice součinu komplexů, pokud bychom místo grupy $(G,\cdot)$ vzali jen (neprázdnou) množinu G?

Poznámka 3.2. Uvědomte si, že přísně vzato není správně značit operaci „$\boxdot$“ násobení komplexů stejným symbolem „$\cdot$“. Jedná se totiž o operaci na potenční množině 2^G, nikoliv na množině G. Jedná se tak o zcela jinou operaci než „$\cdot$“ na G. Přesto si často dovolíme pro obě operace používat stejný symbol „$\cdot$“, případně při použití multiplikativní notace symbol operace zcela vynechat.

Podobně není korektní používat symbol „$\cdot$“ ani „$\boxdot$“ pro označení komplexu $a \cdot H$, protože a není komplex, ale prvek množiny G a ani H není prvek množiny G, ale komplex. Opět tímto stanovujeme úmluvu, že symbol operace obvykle ztotožníme se symbolem operace grupy $(G, \cdot)$. V případech, že budeme chtít zdůraznit odlišnost operací, tak použijeme speciální označení $a \odot H$. V ostatních případech budeme psát $a \cdot H$, případně označení operace při použití multiplikativní notace zcela vynecháme a budeme psát jen aH.

Následující věta ukazuje, že asociativita operace „$\boxdot$“ násobení komplexů grupy plyne ihned z asociativity operace „$\cdot$“ v grupě $(G, \cdot)$. Protože se jedná o první tvrzení o operacích s komplexy, zdůrazníme rozdíl značením operací mezi komplexy a operací v nosné množině grupy použitím symbolu „$\boxdot$“.

Věta 3.7. *Násobení komplexů v pologrupě $(G, \cdot)$ je asociativní.*

Důkaz. Ověříme asociativitu přímým důkazem. Mějme komplexy $A, B, C \subseteq G$. Podle definice násobení komplexů platí

$$A \boxdot (B \boxdot C) = A \boxdot \{b \cdot c : b \in B, c \in C\} = \{a \cdot (b \cdot c) : a \in A, b \in B, c \in C\}.$$

Analogicky platí také

$$(A \boxdot B) \boxdot C = \{(a \cdot b) \cdot c : a \in A, b \in B, c \in C\}.$$

Z definice pologrupy víme, že operace „$\cdot$“ v pologrupě $(G, \cdot)$ je asociativní, tak pro každé $a, b, c \in G$ platí $a \cdot (b \cdot c) = (a \cdot b) \cdot c$. Proto $\{a \cdot (b \cdot c) : a \in A, b \in B, c \in C\} = \{(a \cdot b) \cdot c : a \in A, b \in B, c \in C\}$ a proto $A \boxdot (B \boxdot C) = (A \boxdot B) \boxdot C$. To znamená, že operace „$\boxdot$“ mezi komplexy na potenční množině 2^G je také asociativní. □

V následujícím důsledku opět zdůrazníme použitím symbolu $a \odot H$ rozdíl mezi operací násobení komplexů a operací „$\cdot$“ v nosné množině grupy $(G, \cdot)$.

Důsledek 3.8. *Mějme grupu $(G, \cdot)$. Mějme komplex $H \subseteq G$ a prvky $a, b \in G$. Potom platí*

$$a \odot (b \odot H) = (a \cdot b) \odot H.$$

Dle výše uvedených úmluv označení operací můžeme také psát $(a \cdot b) \odot H = ab \odot H = ab \cdot H = abH$.

Cvičení

3.4.1. Mějme grupu $(\mathbb{Z}, +)$ a tři komplexy $S_1 = \{0\}$, $S_2 = \{1, 2\}$, $S_1 = \{5, 6, 9\}$. Sestavte následující komplexy a) $S_1 \boxplus S_1$, b) $S_1 \boxplus S_2$, c) $S_1 \boxplus S_3$, d) $S_2 \boxplus S_3$, e) $S_1 \boxdot S_2$, pokud existují.

3.4.2. Mějme grupu $(\mathbb{Z}, +)$ a její komplexy $\mathbb{S}$ a $\mathbb{L}$. Sestavte komplexy a) $\mathbb{S} + \mathbb{L}$, b) $\mathbb{S} + \mathbb{S}$, c) $\mathbb{L} + \mathbb{L}$.

3.4.3. Najděte takovou grupu $(G, \cdot)$ a takové dva její komplexy S_1, S_2, že kartézský součin $S_1 \times S_2$ je opět komplexem v $(G, \cdot)$. Pokud taková grupa a komplexy neexistují, dokažte to.

3.4.4. Mějme grupu $(G, \cdot)$ a tři její komplexy H_1, H_2 a H_3. Ukažte, že platí následující implikace. a) Jestliže $H_1 \subseteq H_2$, potom $H_3 \boxdot H_1 \subseteq H_3 \boxdot H_2$. b) Jestliže $H_1 \supseteq H_2$, potom $H_3 \boxdot H_1 \supseteq H_3 \boxdot H_2$. c) Jestliže $H_1 = H_2$, potom $H_3 \boxdot H_1 = H_3 \boxdot H_2$.

3.5. Grupy zbytkových tříd modulo m

Z pohledu praktických aplikací nezastupitelnou roli hrají *konečné* grupy. Nyní zavedeme důležitou třídu konečných grup – zbytkové třídy modulo m.

Definice Zbytkové třídy modulo m
Mějme přirozené číslo m a celé číslo $i \in \{0, 1, \ldots, m-1\}$. Označme množinu

$$\bar{i}_m = \{x \in \mathbb{Z} : \text{celé číslo } x \text{ dává po dělení číslem } m \text{ zbytek } i\}.$$

Množina $\overline{i}_m$ se nazývá *zbytková třída i modulo m.*

Definici můžeme rozšířit tak, že

$$\overline{i}_m = \{x \in \mathbb{Z} : x \equiv i \pmod{m}\}. \tag{4}$$

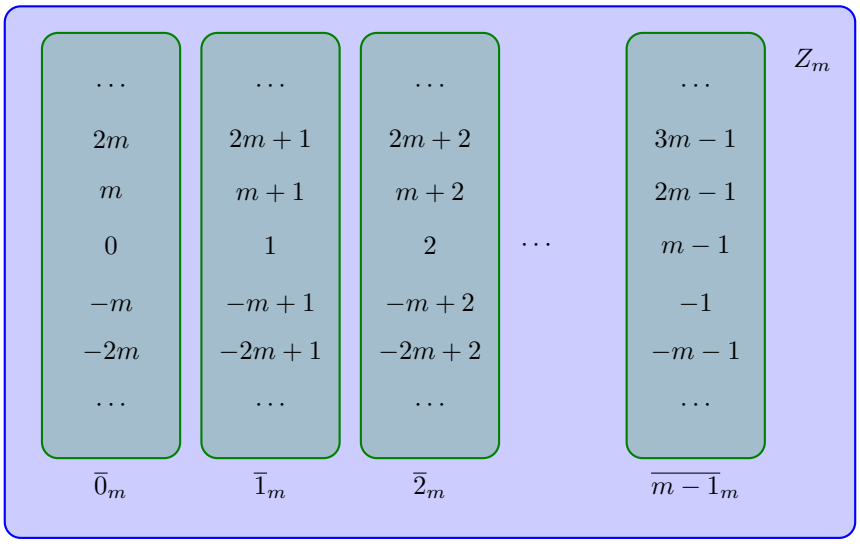
Na rozdíl od definice zbytkových tříd modulo m nepožadujeme, aby zbytkovou třídu označoval zbytek, ale jakýkoliv reprezentant z této zbytkové třídy. V tomto textu budeme pracovat téměř výhradně s reprezentanty z celočíselného intervalu $[0, m-1]$, neboť je to přehlednější.

Poznámka 3.3. Úmluva o značení zbytkových tříd
Často dovolíme zjednodušit značení: pokud bude z kontextu zřejmé s jakým modulem pracujeme, tak místo $\overline{i}_m$ použijeme jen $\overline{i}$. Navíc, pokud budeme pracovat s čísly, tak místo třídy $\overline{i}$ můžeme psát pouze některého reprezentanta, například místo $\overline{2}$ budeme pracovat s třídou 2.

Pro $m = 1$ je zbytková třída triviálně jediná, platí $\overline{0}_1 = \mathbb{Z}$. Pro $m > 1$ tvoří zbytkové třídy rozklad množiny $\mathbb{Z}$. Například pro dostatečně velké m můžeme zbytkové třídy znázornit Obrázkem 3.5. nebo schématem:

$$\begin{aligned}
\overline{0}_m &= \{\ \ldots,\ -2m,\ -m,\ 0,\ m,\ 2m,\ \ldots\ \} \\
\overline{1}_m &= \{\ \ldots,\ -2m+1,\ -m+1,\ 1,\ m+1,\ 2m+1,\ \ldots\ \} \\
\overline{2}_m &= \{\ \ldots,\ -2m+2,\ -m+2,\ 2,\ m+2,\ 2m+2,\ \ldots\ \} \\
&\ \ \vdots \\
\overline{(m-1)}_m &= \{\ \ldots,\ -m-1,\ -1,\ m-1,\ 2m-1,\ 3m-1,\ \ldots\ \}
\end{aligned}$$

Množinu všech zbytkových tříd modulo m označíme $\mathbb{Z}_m$, platí $\mathbb{Z}_m = \{\overline{0}_m, \overline{1}_m, \ldots, \overline{m-1}_m\}$.



Obrázek 3.5.: *Třídy rozkladu grupy zbytkových tříd* $(\mathbb{Z}_m, +)$.

Příklad 3.18. Uveďme několik příkladů zbytkových tříd.

1) Množina sudých čísel $\mathbb{S}$ je vlastně zbytková třída $\overline{0}_2$ a množina lichých čísel $\mathbb{L}$ je zbytková třída $\overline{1}_2$.
2) „Zbytkové třída“ $\overline{2}_2$ je podle definice prázdná množina, avšak podle úmluvy ze vztahu (4) je $\overline{2}_2 = \overline{0}_2 = \mathbb{S}$.
3) Zbytková třída $\overline{0}_{12}$ obsahuje všechny celočíselné násobky 12.
4) Zbytková třída $\overline{5}_{10}$ obsahuje všechny *liché* násobky násobky 5.

Otázka: Má smysl definovat zbytkové třídy pro modul 0?

Otázka: Je množina $5\mathbb{L} = \{5t : t \in \mathbb{L}\}$ nějakou zbytkovou třídou modulo 10?

Zbytkové třídy modulo m jsou vždy neprázdné množiny a tvoří komplexy z grupě $(\mathbb{Z}, +)$. Ukážeme, že tyto komplexy s operací sčítání komplexů tvoří grupu a někdy dokonce tvoří grupu s operací násobení komplexů.

Věta 3.9. *Zbytkové třídy modulo m s operací sčítání komplexů tvoří komutativní grupu $(\mathbb{Z}_m, +)$. Nenulové zbytkové třídy modulo m s operací násobení komplexů tvoří komutativní grupu $(\mathbb{Z}_m \setminus \{\overline{0}_m\}, \cdot)$ právě tehdy, když m je prvočíslo.*

Důkaz. Nejprve si uvědomíme, že operace jsou dobře definovány, neboť součet libovolných dvou reprezentantů zbytkové třídy $\overline{i}_m$ a třídy $\overline{j}_m$ je reprezentant třídy $\overline{i+j}_m$, resp. jejich součin je reprezentant třídy $\overline{i \cdot j}_m$ (Cvičení 3.5.7.).

Snadno nahlédneme, že množina zbytkových tříd je jistě neprázdná a operace sčítání komplexů je uzavřená na $\mathbb{Z}_m$. Asociativita i komutativita sčítání zbytkových tříd vyplývají z asociativity a komutativity obvyklého sčítání celých čísel. Neutrálním prvkem je třída $\overline{0}_m$ a opačným prvkem k třídě $\overline{a}_m$ je třída $\overline{-a}_m$. Sčítání zbytkových tříd je jistě komutativní a proto zbytkové třídy modulo m s operací sčítání komplexů tvoří komutativní grupu $(\mathbb{Z}_m, +)$.

Pozor! Operace násobení komplexů na množině $\mathbb{Z}_m$ obecně netvoří grupu, protože operace násobení komplexů nemusí být uzavřená na $(\mathbb{Z}_m \setminus \{\overline{0}_m\}, \cdot)$ a násobení tak nemusí tvořit ani grupoid. Například $\overline{2}_4 \cdot \overline{2}_4 = \overline{0}_4$ a proto $(\mathbb{Z}_4 \setminus \{\overline{0}_m\}, \cdot)$ není grupoidem. Obecně, máme-li dvě taková celá čísla $a, b \in [0, m-1]$, že $ab = km$ pro nějaké celé číslo k, tak součin odpovídajících zbytkových tříd $\overline{a}_m \cdot \overline{b}_m = \overline{0}_m$ do nosné množiny nepatří. Je-li m prvočíslo, tak součin libovolných dvou nenulových komplexů je nenulový komplex a proto $(\mathbb{Z}_m, \setminus\{\overline{0}_m\}, \cdot)$ je grupoid.

Pokud však uzavřenost splněna je, tak asociativita i komutativita operace násobení zbytkových tříd vyplývají z asociativity a komutativity operace obvyklého násobení celých čísel. Neutrálním prvkem je $\overline{1}_m$. Inverzním prvek ke každé třídě $\overline{i}_m$ najdeme pouze, pokud m je prvočíslo. Protože $0 \leq i < m$, tak pro prvočíselné m platí $\mathrm{NSD}(i, m) = 1$ a podle Bézoutova Lemamtu 0.3. existují taková celá čísla r, s, že $ir + ms = 1$. To znamená, že $ir = (-s)m + 1 \equiv 1 \pmod{m}$ a proto pro každý prvek r_0 třídy $\overline{r}_m$ je součin ir_0 ve třídě $\overline{1}_m$ a proto je třída $\overline{r}_m$ multiplikativní inverzí třídy $\overline{i}_m$. Pro prvočíslo m dostáváme, že $(\mathbb{Z}_m \setminus \{\overline{0}_m\}, \cdot)$ tvoří komutativní grupu. □

Poznámka 3.4. Všimněte si, že v důkazu Věty 3.9. využíváme, že m je prvočíslo. Pokud m není prvočíslo, tak multiplikativní inverze k prvku i v monoidu $(\mathbb{Z}_m \setminus \{\overline{0}_m\}, \cdot)$ existuje pouze, pokud $\mathrm{NSD}(i, m) = 1$. Jestliže $\mathrm{NSD}(i, m) = a$, kde $a > 1$, tak multiplikativní inverze k prvku i v monoidu $(\mathbb{Z}_m \setminus \{\overline{0}_m\}, \cdot)$ neexistuje (Cvičení 3.5.3.).

Je dobré zdůraznit, že grupa zbytkových tříd modulo m s operací násobení neobsahuje zbytkovou třídu $\overline{0}_m$. V dalším textu tuto zbytkovou třídu budeme značit 0. Jestliže bude z kontextu jasné, s jakým modulem pracujeme, tak v dalším textu budeme všechny třídy $\overline{i}_m$ značit pouze i.

Otázky:

- Je uspořádaná dvojice $(\mathbb{Z}_m, \cdot)$ grupou?
- Je grupa $(\mathbb{Z}_m, +)$ podgrupou grupy $(\mathbb{Z}, +)$?
- Je grupa $(\mathbb{Z}_m \setminus \{\overline{0}_m\}, \cdot)$ podgrupou grupy $(\mathbb{Z}, \cdot)$?
- Je grupa $(\mathbb{Z}_2, +)$ podgrupou grupy $(\mathbb{Z}_4, +)$?

Počet prvků (tříd) grupy $(\mathbb{Z}_m, +)$ je vždy roven modulu m, neboť různých zbytků po dělení číslem m je právě m. Pro libovolný (konečný) řád umíme takovou grupu s operací „sčítání modulo m“ sestavit. Počet prvků (tříd) grupy $(\mathbb{Z}_m \setminus \{\overline{0}_m\}, \cdot)$ je $m - 1$.

Příklad 3.19. Sestavte a porovnejte a) Cayleyho tabulku grupy $(\mathbb{Z}_5, +)$, b) Cayleyho tabulku **monoidu** $(\mathbb{Z}_5, \cdot)$, c) Cayleyho tabulku grupy $(\mathbb{Z}_5 \setminus \{\overline{0}_m\}, \cdot)$.

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
0	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Tabulka 3.6.: *Cayleyho tabulky grupy* $(\mathbb{Z}_5, +)$, *monoidu* $(\mathbb{Z}_5, \cdot)$ *a grupy* $(\mathbb{Z}_5 \setminus \{\overline{0}_5\}, \cdot)$.

V Tabulce 3.6. ihned vidíme, že obě operace jsou na $\mathbb{Z}_5$ uzavřené. Víme, že obě operace jsou asociativní, neboť klasické sčítání i násobení jsou asociativní. Všimněte si, že na rozdíl od $(\mathbb{Z}_5, +)$ není $(\mathbb{Z}_5, \cdot)$ grupa. Neutrálním prvkem grupoidu $(\mathbb{Z}_5, \cdot)$ vzhledem k násobení je (třída) 1 a (třída) 0 nemá inverzní prvek. Proto je $(\mathbb{Z}_5, \cdot)$ monoidem. Prvek (třída) 0 je jediný prvek, který vlastnost být grupou pokazí, pokud jej odstraníme, tak dvojice $(\mathbb{Z}_5 \setminus \{\overline{0}_5\}, \cdot)$ grupou je: operace násobení je uzavřená na menší množině $\mathbb{Z}_5 \setminus \{\overline{0}_5\}$; neutrálním prvkem je (třída) 1; (třídy) 1 a 4 jsou inverzní samy k sobě a (třídy) 2 a 3 jsou inverzní navzájem. ✓

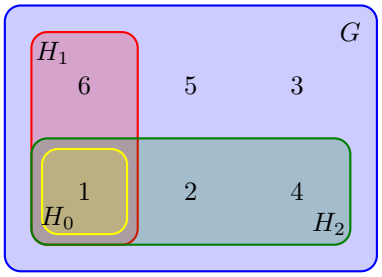
Příklad 3.20. Sestavte Cayleyho tabulku grupy $(\mathbb{Z}_7 \setminus \{\overline{0}_7\}, \cdot)$. Najděte čtyři různé podgrupy.
Cayleyho tabulka je 3.7.

$\cdot$	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

Tabulka 3.7.: *Cayleyho tabulky grupy* $(\mathbb{Z}_7 \setminus \{\overline{0}_7\}, \cdot)$.

Vidíme, že operace „$\cdot$“ je na množině $\mathbb{Z}_7 \setminus \{\overline{0}_7\}$ uzavřená; neutrálním prvkem je (třída) 1; asociativita se „zdědí“ z obvyklého násobení čísel a inverzní (třídy) jsou $1^{-1} = 1$, $2^{-1} = 4$, $3^{-1} = 5$, $4^{-1} = 2$, $5^{-1} = 3$ a $6^{-1} = 6$.

Kromě triviální podgrupy $(H_0, \cdot) = (\{1\}, \cdot)$ a nevlastní podgrupy $(G, \cdot) = (\mathbb{Z}_7 \setminus \{\overline{0}_7\}, \cdot)$ najdeme ještě další podmnožiny, na kterých je operace uzavřená: $H_1 = \{1, 6\}$ a $H_2 = \{1, 2, 4\}$ (Obrázek 3.6.). Podle Věty 3.5. stačí na ověření podgrupy uzavřenost operace „$\cdot$“.



Obrázek 3.6.: *Podgrupy v grupě* $(\mathbb{Z}_7 \setminus \{\overline{0}_7\}, \cdot)$.

Protože podle Věty 3.1. je třída 1 obsažena v každé podgrupě, tak triviální podgrupa je jediná. Dále prozkoumáním hlavní diagonály Cayleyho tabulky 3.7. vidíme, že dvouprvková podgrupa existuje pouze s nosičem $H_1 = \{1, 6\}$ a tříprvková podgrupa pouze s nosičem $H_2 = \{1, 2, 4\}$. Podgrupy vyšších řádů kromě nevlastní podgrupy existovat nemohou, což ukážeme v Kapitole 4.3. ✓

Cvičení

3.5.1. Mějme grupu zbytkových tříd modulo 7 s operací „$\cdot$“ násobení $(\mathbb{Z}_7 \setminus \{\overline{0}_7\}, \cdot)$, neboli grupu $([1, 6], \cdot)$. Mějme $H = \{\overline{1}_7, \overline{2}_7, \overline{4}_7\}$. Ukažte, že $(H, \cdot)$ je podgrupa v grupě $(\mathbb{Z}_7 \setminus \{\overline{0}_7\}, \cdot)$.

3.5.2. Mějme grupu zbytkových tříd modulo 7 s operací „$\cdot$“ násobení $(\mathbb{Z}_7 \setminus \{\overline{0}_7\}, \cdot)$, neboli grupu $([1, 6], \cdot)$. Mějme $H = \{\overline{1}_7, \overline{2}_7, \overline{4}_7\}$. Sestavte komplexy $\overline{1}_7 H$, $\overline{2}_7 H$, …, $\overline{6}_7 H$ a znázorněte je.

3.5.3. Najděte takové složené číslo m a takové dvě třídy a, b monoidu $(\mathbb{Z}_m \setminus \{\overline{0}_m\}, \cdot)$, že a) třída a má inverzní prvek v monoidu $(\mathbb{Z}_m \setminus \{\overline{0}_m\}, \cdot)$; b) třída b nemá inverzní prvek v monoidu $(\mathbb{Z}_m \setminus \{\overline{0}_m\}, \cdot)$.

3.5.4. Mějme grupu $(G, \cdot)$ a nějakou neprázdnou podmnožinu $H \subseteq G$. Ukažte, že $\bigcup_{g \in G}(gH) = G$.

3.5.5. Na množině čtyř celých čísel $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ definujeme operaci $\oplus$ takto.

$$\forall a, b \in \mathbb{Z}_4 : a \oplus b = \begin{cases} a + b & a + b < 4 \\ a + b - 4 & a + b \geq 4 \end{cases}$$

Ukažte, že $(\mathbb{Z}_4, \oplus)$ je grupa. (Všimněte si, že stejné označení jako pro množinu zbytkových tříd modulo 4 nevadí, neboť při porovnání tabulek operací nenajdeme rozdíl.)

3.5.6. Mějme sudé kladné číslo n. Označme $(H,+)$ libovolnou podgrupu v $(\mathbb{Z}_n,+)$. Ukažte, buď jsou všechny prvky H sudé, nebo právě polovina prvků v H je sudých.

3.5.7. Ukažte, že sčítání a násobní zbytkových tříd jsou dobře definované operace, tj. a) součet libovolných dvou reprezentantů zbytkové třídy $\overline{i}_m$ a třídy $\overline{j}_m$ je reprezentant třídy $\overline{i+j}_m$, b) součin dvou libovolných reprezentantů zbytkové třídy $\overline{i}_m$ a třídy $\overline{j}_m$ je reprezentant třídy $\overline{i\cdot j}_m$.

Kapitola 4. Rozklady grup, Lagrangeova věta

Začneme motivačním příkladem, který ukáže, jak lze prvky grupy rozdělit do disjunktních podmnožin užitím vlastností grupy a nějaké její podgrupy.

Příklad 4.1. Uvažujme grupu $(\mathbb{Z}_6, +)$ zbytkových tříd modulo 6. Pro jednoduchost třídu $\overline{i}$ označíme i. Pro $H = \{0, 2, 4\}$ ukážeme, že $(H, +)$ je podgrupa grupy $(\mathbb{Z}_6, +)$. Dále sestavíme komplexy $0 + H, 1 + H, \ldots, 5 + H$ a prozkoumáme jejich vztah k množině $\mathbb{Z}_6$.
Protože H je konečná podmnožina množiny $[0, 5]$, tak podle Věty 3.5. stačí ověřit, že

1) $H \subseteq G$, což plyne už ze zadání,
2) $H \neq \emptyset$, což opět plyne ihned ze zadání.
3) Uzavřenost operace „+“ na množině H ověříme Tabulkou 4.1.

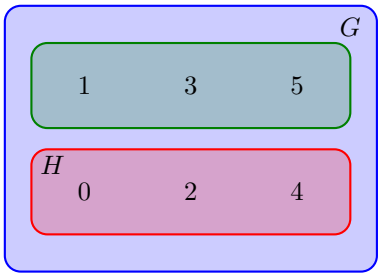
$+$	0	2	4
0	0	2	4
2	2	4	0
4	4	0	2

Tabulka 4.1.: *Cayleyho tabulka podgrupy* $(H, +)$.

Nyní sestavíme komplexy $0 + H, 1 + H, \ldots, 5 + H$.

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

Všimněte si, že komplexy nejsou nutně různé množiny, ale nastane právě jedna ze dvou možností: buď jsou výsledné komplexy stejné, nebo jsou disjunktní (Obrázek 4.1.). Navíc má každý výsledný komplex stejný počet prvků jako množina H. ✓



Obrázek 4.1.: *Komplexy* $0 + H$, $1 + H$, $2 + H$, $3 + H$, $4 + H$ *a* $5 + H$ *pro* $H = \{0, 2, 4\}$ *v grupě* $(\mathbb{Z}_6, +)$.

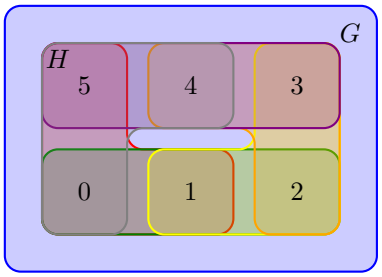
Následující příklad ukazuje, jak důležitý je fakt, že $(H, +)$ je podgrupou grupy $(\mathbb{Z}_6, +)$, nikoliv pouze komplexem (neprázdnou podmnožinou) nosiče G.

Příklad 4.2. Uvažujme opět grupu $(\mathbb{Z}_6, +)$ zbytkových tříd modulo 6. Vezměme její *podmnožinu* $H = \{0, 1, 2\}$, která *není* podgrupu grupy $(\mathbb{Z}_6, +)$. Opět sestavíme komplexy $1 + H, 2 + H, \ldots, 6 + H$ a prozkoumáme jejich vztah k množině $\mathbb{Z}_6$.
Předně si všimneme, že množina H není uzavřená vzhledem k operaci „+“, protože $1 + 2 = 3$, ale $3 \notin H$. Proto $(H, +)$ není podgrupou v $(\mathbb{Z}_6, +)$.

Dále sestavíme komplexy $0+H, 1+H, \ldots, 5+H$.

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

Všimněte si, že výsledné množiny netvoří rozklad nosiče G (Obrázek 4.2.). Jedná se sice o různé tříprvkové podmnožiny G, ale tyto různé množiny nejsou nutně disjunktní. ✓



Obrázek 4.2.: *Komplexy* $0+H$, $1+H$, $2+H$, $3+H$, $4+H$ *a* $5+H$ *pro* $H=\{0,1,2\}$ *v grupě* $(\mathbb{Z}_6,+)$.

Pozorování z předchozích příkladů nyní zobecníme. Ukážeme, že pokud pracujeme s podgrupou $(H,\cdot)$ nějaké grupy $(G,\cdot)$, tak platí následující tvrzení.

- Rovnost $x+H=H$ platí právě tehdy, když $x\in H$.
- Sjednocení tříd $x+H$ dá vždy celou množinu G, tj. $\bigcup_{x\in G}(x+H)=G$.
- Všechny třídy $x+H$ mají vždy stejný počet prvků, tj. pro každé $x\in G$ platí $|x+H|=|H|$.
- Počet prvků třídy dělí počet prvků nosné množiny G; podíl je počtem tříd a pro velikosti množin platí dokonce $|G|=\left|G/H\right|\cdot|H|$.

V následujících podkapitolách všechna uvedená pozorování pečlivě zformulujeme a dokážeme.

4.1. Rozklad grupy podle podgrupy

V této sekci ukážeme, že systematičnost výsledných komplexů z úvodního Příkladu 4.1. není náhoda. Ukážeme, že pro libovolnou podgrupu $(H,\cdot)$ grupy $(G,\cdot)$ bude obecně platit, že výsledné komplexy tvoří rozklad (buď jsou disjunktní nebo totožné) a jednotlivé třídy mají vždy stejný počet prvků. Připomeňme, že symbolem $a\odot H$ označujeme násobení komplexů zavedené na straně 71.

Definice Rozklad grupy podle podgrupy
Mějme grupu $(G,\cdot)$ a její podgrupu $(H,\cdot)$. Zavedeme označení $G/H=\{a\odot H : a\in G\}$. Systému komplexů G/H říkáme *(levý) rozklad grupy* $(G,\cdot)$ *podle podgrupy* $(H,\cdot)$. Analogicky můžeme zavést pravý rozklad grupy $(G,\cdot)$ podle podgrupy $(H,\cdot)$ jako $H\backslash G=\{H\odot a : a\in G\}$.

Prvky rozkladu jsou komplexy, se kterými můžeme dále pracovat. V této kapitole nejprve ukážeme, že název „rozklad grupy podle podgrupy“ je zasloužený, že komplexy rozkladu G/H opravdu tvoří rozklad množiny G. V Kapitole 5. pak ukážeme, že komplexy v rozkladu G/H grupy $(G,\cdot)$ podle podgrupy $(H,\cdot)$ mohou společně s operací násobení (resp. sčítání) komplexů za splnění dalších podmínek dokonce tvořit grupu.

Příklad 4.3. Uvedeme několik jednoduchých příkladů grup a jejich rozkladů podle podgrup.

1) V Příkladu 4.1. jsme uvedli příklad rozkladu grupy $(\mathbb{Z}_6,+)$ podle podgrupy $(\{0,2,4\},+)$.
2) Rozklad grupy $(\mathbb{Z},+)$ podle podgrupy $(\mathbb{S},+)$ má dvě třídy rozkladu: $\mathbb{S}$ a $\mathbb{L}$.
3) Rozklad grupy $(\mathbb{Z},+)$ podle podgrupy $(k\mathbb{Z},+)$ má k tříd rozkladu: $k\mathbb{Z}$, $1+k\mathbb{Z}$, $\ldots$, $k-1+\mathbb{Z}$.
4) Rozklad grupy $(\mathbb{Q},+)$ podle podgrupy $(\mathbb{Z},+)$ má nekonečně mnoho tříd rozkladu, například $\mathbb{Z}$, $\frac{1}{2}+\mathbb{Z}$, $\frac{2}{7}+\mathbb{Z}$, $\ldots$ Pro každé racionální číslo z intervalu $\langle 0,1)$ je jedna taková třída.

5) Mějme grupu $(G,\cdot)$ a její triviální podgrupu $(\{e\},\cdot)$. Rozklad grupy $G/\{e\}$ má $|G|$ tříd rozkladu, přičemž každá třída obsahuje jediný prvek.
6) V diherdální grupě D_3 symetrií rovnostranného trojúhelníka (Tabulka 1.3.) máme podgrupu rotací $(R,\circ)$. Levý rozklad D_3/R má dvě třídy rozkladu $R=\{R_0,R_{120},R_{240}\}$ a $Z=\{Z_A,Z_B,Z_C\}$. Pravý rozklad $R\backslash D_3$ má stejné dvě třídy rozkladu $R=\{R_0,R_{120},R_{240}\}$ a $Z=\{Z_A,Z_B,Z_C\}$.
7) V diherdální grupě D_3 symetrií rovnostranného trojúhelníka máme podgrupu $(\{R_0,Z_A\},\circ)$. Levý rozklad $D_3/\{R_0,Z_A\}$ grupy $(D_3,\circ)$ podle podgrupy $(\{R_0,Z_A\},\circ)$ má tři třídy rozkladu $\{R_0,Z_A\}$, $\{R_{120},Z_C\}$ a $\{R_{240},Z_B\}$. Pravý rozklad $\{R_0,Z_A\}\backslash D_3$ grupy $(D_3,\circ)$ podle podgrupy $(\{R_0,Z_A\},\circ)$ má také tři třídy rozkladu, avšak jiné: $\{R_0,Z_A\}$, $\{R_{120},Z_B\}$ a $\{R_{240},Z_C\}$. Sestavení tříd rozkladu je ponecháno jako Cvičení 4.1.8.

Příklad 4.4. Uvedeme několik jednoduchých příkladů, kdy se o rozklady grup nejedná.

1) V Příkladu 4.2. jsme ukázali, že množina $H=\{0,1,2\}$ není podgrupou grupy $(\mathbb{Z}_6,+)$ a komplexy $0+H$, $1+H$, $2+H$, $3+H$, $4+H$, $5+H$ rozklad netvoří.
2) Rozklad grupy $(\mathbb{Z},+)$ podle $\mathbb{N}$ nemá smysl tvořit, neboť $(\mathbb{N},+)$ netvoří grupu. Je sice možné pro každé $z\in\mathbb{Z}$ sestavit komplexy $z+\mathbb{N}$, avšak výsledné komplexy nebudou tvořit rozklad množiny $\mathbb{Z}$.
3) Rozklad grupy $(\mathbb{Z},+)$ podle „podgrupy“ $(\mathbb{Z}_n,+)$ nemá smysl tvořit, protože $\mathbb{Z}_n\not\subseteq\mathbb{Z}$ a grupa $(\mathbb{Z}_n,+)$ není podgrupou grupy $(\mathbb{Z},+)$ ani v případě, že bychom čísla i, $i=0,1,\ldots,n-1$ ztotožnili s třídami $\overline{0}_n$, $\overline{1}_n$, …, $\overline{n-1}_n$, neboť operace na $\mathbb{Z}$ a $\mathbb{Z}_n$ by nebyly definovány stejně.

Podgrupa a její komplexy

Dříve než budeme formulovat a dokazovat tvrzení této kapitoly, ukážeme následující jednoduché pozorování.

Lemma 4.1. *Mějme komplex H grupy $(G,\cdot)$ a prvek $x\in G$. Pro každý prvek $y\in x\odot H$ existuje právě jeden prvek $h\in H$, že $y=x\cdot h$.*

Důkaz. Důkaz plyne ihned z definice násobení komplexů na straně 71. Každý prvek $y\in x\odot H$ je tvaru $x\cdot h$ pro nějaké $h\in H$.

Navíc, protože $(G,\cdot)$ je grupa, tak s využitím Věty o krácení (Věta 2.6.) snadno ukážeme, že prvek h je určený jednoznačně. Pokud $y=x\cdot h_1=x\cdot h_2$, tak krácením dostáváme $h_1=h_2$. □

Otázky:

- Platí, že prvek h z Lemmatu 4.1. je určen jednoznačně i v pologrupě $(G,\circ)$?
- Platí, že prvek h z Lemmatu 4.1. je určen jednoznačně i v monoidu $(G,\circ)$?

V dalším textu využijeme úmluvu, že součin komplexů $x\odot H$ budeme stručně zapisovat xH. Ukážeme, že při násobení prvku a komplexu podgrupy podgrupa „pohltí své prvky“. To znamená, že nosič H podgrupy $(H,\cdot)$ je vždy jedním z komplexů xH grupy $(G,\cdot)$.

Věta 4.2. *Mějme grupu $(G,\cdot)$ a její podgrupu $(H,\cdot)$. Pro každé $x\in G$ platí:*

(i) $xH=H$ právě tehdy, když $x\in H$,
(ii) $Hx=H$ právě tehdy, když $x\in H$.

Důkaz. Tvrzení věty obsahuje dvě ekvivalence. Dokážeme jen první ekvivalenci, druhá ekvivalence se ukáže zcela analogicky.

„⇒“ Předpokládejme, že $xH=H$ a mějme libovolné $x\in G$. Pro libovolné $x\in G$ rozepíšeme $x=x\cdot e$ a protože $e\in H$, tak je $x=x\cdot e\in xH$ z definice komplexu xH. To znamená, že $x\in xH$ a protože podle předpokladu je $xH=H$, platí také $x\in H$.

„⇐“ Předpokládejme, že $x\in H$. Ukážeme množinovou rovnost $xH=H$ jako dvě inkluze $xH\subseteq H$ a $H\subseteq xH$.

Nejprve ukážeme, že $xH\subseteq H$. Pro každé $x\cdot h\in xH$ existuje podle Lemmatu 4.1. odpovídající prvek $h\in H$. Potom ale $x\cdot h\in H$ díky uzavřenosti operace „$\cdot$“ na H.

Dále ukážeme, že $H\subseteq xH$. Označme e neutrální prvek grupy $(G,\cdot)$, který je podle Věty 3.1. současně neutrálním prvkem i její podgrupy $(H,\cdot)$. Potom pro libovolné $h\in H$ můžeme psát $h=e\cdot h=x\cdot x^{-1}\cdot h$, kde $x\in H$ můžeme zvolit libovolně. Protože $(H,\cdot)$ je (pod)grupa, tak také $x^{-1}\in H$ a dále $x^{-1}h$ patří

do H, protože operace „$\cdot$“ je uzavřená na (pod)grupě $(H, \cdot)$. A konečně dle definice komplexu xH platí $x \cdot (x^{-1} \cdot h) \in xH$. To znamená, že pro libovolné $h \in H$ je $h = x \cdot (x^{-1} \cdot h) \in xH$.

Tím jsme ukázali, že pro libovolné $x \in H$ je komplex xH totožný s nosičem H podgrupy $(H, \cdot)$. □

Příklad 4.5. V Příkladu 4.1. jsme uvedli rozklad grupy $(\mathbb{Z}_6, +)$ (grupy zbytkových tříd modulo 6) podle podgrupy $(\{0, 2, 4\}, +)$. Všimněte si, že komplexy $0 + H$, $2 + H$ a $4 + H$ jsou totožné s nosičem podgrupy H, zatímco tři zbývající komplexy $1 + H$, $3 + H$ a $5 + H$ jsou jiné. Celou situaci pěkně ilustruje Obrázek 4.1.

Ihned vidíme, že platí následující důsledek Věty 4.2.

Důsledek 4.3. *Mějme grupu $(G, \cdot)$. Pro každý prvek $g \in G$ platí $gG = G = Gg$.*

Je zajímavé si uvědomit, že z Důsledku 4.3. mimo jiné plyne také, že v každém řádku Cayleyho tabulky operace grupy $(G, \cdot)$ je nějaká permutace *všech* prvků nosiče grupy. V grupoidu, pologrupě nebo monoidu toto platit nemusí, avšak v grupě existence inverze si vynutí, že každý řádek (i každý sloupec) je permutací nosiče grupy.

Příklad 4.6. Mějme grupu $(G, \cdot)$ a představme si její Cayleyho tabulku. Pro každé $g \in G$ je množina prvků gG uvedena v řádku Cayleyho tabulky, který odpovídá prvku g. A naopak množinu prvků Gg najdeme ve sloupci Cayleyho tabulky, který odpovídá prvku g.

Vztahy mezi komplexy jedné podgrupy

Následující věta říká, že pokud dva komplexy tvaru xH, kde H je nosič nějaké podgrupy dané grupy, mají nějaký společný prvek, pak tyto komplexy jsou totožné.

Věta 4.4. *Mějme grupu $(G, \cdot)$, její podgrupu $(H, \cdot)$ a prvky $a, b \in G$. Jestliže $(aH) \cap (bH) \neq \emptyset$, tak $aH = bH$.*

Důkaz. Předpokládejme, že existuje prvek $x \in (aH \cap bH)$. Protože prvek x patří do průniku komplexů, tak patří do každého z obou komplexů aH, bH. Proto podle Lemmatu 4.1. existují takové prvky $h_1, h_2 \in H$, že $x = a \cdot h_1 = b \cdot h_2$. Vynásobením druhé rovnosti zprava inverzním prvkem k prvku h_1 dostaneme $a = bh_2h_1^{-1}$. Označme $h = h_2 \cdot h_1^{-1}$, přičemž z uzavřenosti operace v grupě $(H, \cdot)$ víme, že $h \in H$. Proto můžeme napsat $a = b \cdot h$, kde $h \in H$.

S využitím Věty 3.7. dostáváme, že $aH = (bh)H = b(hH)$. Protože $h \in H$, tak podle Věty 4.2. víme $hH = H$. Celkem máme $aH = (bh)H = b(hH) = bH$, což je dokazované tvrzení. □

Obměna předchozího tvrzení věty říká, že různé komplexy tvaru xH, kde H je nosič nějaké podgrupy dané grupy, nemohou mít žádný společný prvek (jsou disjunktní).

Důsledek 4.5. *Mějme grupu $(G, \cdot)$, její podgrupu $(H, \cdot)$ a prvky $a, b \in G$. Pokud $aH \neq bH$, tak $(aH) \cap (bH) = \emptyset$.*

Příklad 4.7. Tvrzení Věty 4.5. opět ilustruje Příklad 4.1. V rozkladu grupy $(\mathbb{Z}_6, +)$ (grupy zbytkových tříd modulo 6) podle podgrupy $(\{0, 2, 4\}, +)$ jsou komplexy $0 + H$, $2 + H$ a $4 + H$ jsou totožné s nosičem podgrupy H, zatímco tři zbývající komplexy $1 + H$, $3 + H$ a $5 + H$ jsou *disjunktní*, což opět ilustruje Obrázek 4.1.

Nyní ukážeme, že při sestavení komplexů tvaru gH, kde g patří do nosiče grupy $(G, \cdot)$, se žádný prvek nosiče G neztratí, tj. každý prvek grupy G bude patřit do některého komplexu gH.

Věta 4.6. *Mějme grupu $(G, \cdot)$ a její podgrupu $(H, \cdot)$. Platí $\bigcup_{g \in G} gH = G$.*

Důkaz. Množinovou rovnost opět ukážeme jako dvě inkluze.

Nejprve ukážeme $\bigcup_{g \in G} gH \subseteq G$. Mějme libovolné $x \in gH$. Z Lemmatu 4.1. víme, že $x = g \cdot h$ pro nějaké $h \in H$. Protože $H \subseteq G$, tak $h \in G$. Z uzavřenosti operace na G dostáváme $x = (g \cdot h) \in G$, tedy $\bigcup_{g \in G} gH \subseteq G$.

Zbývá ukázat, že $\bigcup_{g \in G} gH \supseteq G$. Stačí si uvědomit, že pro každé $g \in G$ je $g \in gH$, neboť $e \in H$ a platí $g = ge \in gH$. Dostáváme, že $G \subseteq \bigcup_{g \in G} gH$. □

Příklad 4.8. Tvrzení Věty 4.6. opět ilustruje Příklad 4.1. Všimněte si, že v rozkladu grupy $(\mathbb{Z}_6, +)$ (grupy zbytkových tříd modulo 6) podle podgrupy $(\{0, 2, 4\}, +)$ je každý prvek g obsažen v komplexu $g + H$.

Tvrzení Věty 4.6. můžeme poměrně snadno zobecnit. Množina H nemusí být nosičem podgrupy a nemusí obsahovat prvek e a proto se může stát, že $g \notin gH$. Přesto pro každou neprázdnou podmnožinu H množiny G platí $\bigcup_{g \in G} gH = G$.

Věta 4.7. *Mějme grupu $(G,\cdot)$ a nějakou neprázdnou podmnožinu $H \subseteq G$. Platí $\bigcup_{g\in G} gH = G$.*

Důkaz je ponechán jako Cvičení 4.1.10.

Příklad 4.9. Tvrzení Věty 4.7. ilustruje Příklad 4.2. Jednotlivé komplexy $0+H$, $1+H$, $2+H$, $3+H$, $4+H$, $5+H$ sice nejsou disjunktní a netvoří rozklad nosiče $G=\{0,1,2,3,4,5\}$, avšak každý prvek g grupy je obsažen v některém komplexu $a+H$, pro nějaké $a\in G$ (Obrázek 4.2.).

Rozklad grupy sestavený z komplexů podgrupy

Pozorování z předchozích odstavců shrneme do jediné následující věty. Postupně jsme ukázali, že komplexy rozkladu grupy $(G,\cdot)$ podle podgrupy $(H,\cdot)$ jsou neprázdné, navzájem disjunktní a obsahují každý prvek nosiče grupy G. Tvoří proto rozklad množiny G.

Důsledek 4.8. *Mějme grupu $(G,\cdot)$ a její podgrupu $(H,\cdot)$. Systém komplexů G/H tvoří rozklad množiny G.*

Důkaz. Ukážeme, že systém podmnožin G/H splňuje všechny tři vlastnosti rozkladu:

(i) $\bigcup_{g\in G} gH = G$, což plyne z Věty 4.6.,
(ii) pro každé $a,b\in G$ platí, že pokud $aH\neq bH$, tak $(aH)\cap(bH)=\emptyset$, což platí podle Důsledku 4.5.,
(iii) pro každé $g\in G$ je množina gH neprázdná, což plyne z pozorování $g = g\cdot e \in gH$, neboť $e\in H$, přičemž $(H,\cdot)$ je podgrupa grupy $(G,\cdot)$.

Poroto různé komplexy sestavené z podgrupy tvoří rozklad množiny G. □

Poznámka 4.1. Analogické tvrzení jako v Důsledku 4.8. lze vyslovit i pro pravý rozklad $H\backslash G$ grupy G podle podgrupy H. V dalším textu se však pro jednoduchost zaměříme pouze na levé rozklady.

Příklad 4.10. Mějme grupu $(\mathbb{Z}_7\setminus\{\bar{0}_7\},\cdot) = ([1,6],\cdot)$ (grupu zbytkových tříd modulo 7 s operací „$\cdot$“ násobení) z Příkladu 3.20. Mějme $H=\{1,6\}$. a) Ukážeme, že $(H,\cdot)$ je podgrupa v grupě $(G,\cdot)$. b) Sestavíme $1H$, $2H$, …, $6H$. c) Sestavíme G/H.

a) Nejprve ukážeme, že $(H,\cdot)$ je podgrupa v grupě $(G,\cdot)$. Protože jistě je $H\neq\emptyset$ a $H\subseteq G$, tak stačí ukázat, že H je uzavřená vzhledem k operaci „$\cdot$“. Uzavřenost je zřejmá z Cayleyho tabulky 4.2. restrikce operace „$\cdot$“ na množinu H. Proto je $(H,\cdot)$ podgrupou grupy $(G,\cdot)$.

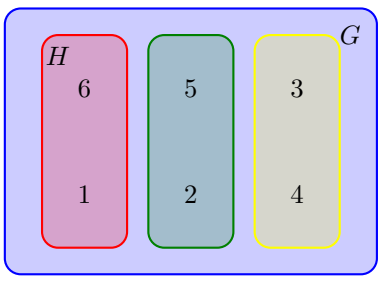
$\cdot$	1	6
1	1	6
6	6	1

Tabulka 4.2.: *Tabulka restrikce operace na podgrupu $H=\{1,6\}$.*

b) Nyní sestavíme komplexy $1\odot H = 1H$, $2H$, …, $6H$.

$$\begin{aligned}
1H &= \{1\cdot 1, 1\cdot 6\} = \{1,6\} = H\\
2H &= \{2\cdot 1, 2\cdot 6\} = \{2,5\}\\
3H &= \{3\cdot 1, 3\cdot 6\} = \{3,4\}\\
4H &= \{4\cdot 1, 4\cdot 6\} = \{4,3\}\\
5H &= \{5\cdot 1, 5\cdot 6\} = \{5,2\}\\
6H &= \{6\cdot 1, 6\cdot 6\} = \{6,1\} = H
\end{aligned}$$

c) Dostaneme rozklad $G/H = \{\{1,6\},\{2,5\},\{3,4\}\}$ (Obrázek 4.3.) množiny G. ✓



Obrázek 4.3.: *Třídy rozkladu grupy $(\mathbb{Z}_7\setminus\{\bar{0}_7\},\cdot)$ podle podgrupy $(\{1,6\},\cdot)$.*

Všimněte si, že komplexy nejsou různé, ale nastane právě jedna ze dvou možností: buď jsou výsledné komplexy stejné, nebo mají prázdný průnik (jsou disjunktní). Výsledný rozklad má tři třídy, každou se dvěma prvky, což je vždy stejný počet prvků, jako má nosná množina H. Navíc platí $3 \cdot |H| = 6 = |G|$.

Podobná situace nastane, pokud vezmeme podgrupu $H = \{1, 2, 4\}$ v grupě zbytkových tříd $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$ (Cvičení 3.5.2.). Systém komplexů tvoří rozklad $G/H = \{\{1, 2, 4\}, \{3, 5, 6\}\}$ nosné množiny G. Pokud vezmeme podgrupu $H = \{1\}$ v grupě zbytkových tříd $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$, tak dostaneme rozklad se šesti třídami rozkladu, každá s jedním prvkem (Cvičení 4.1.4.). V další sekci ukážeme, že to není náhoda. Pokud ale například vezmeme $H = \{1, 3\}$ (tedy H není podgrupou $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$), tak podobným postupem rozklad nedostaneme (Cvičení 4.1.3.).

Příklad 4.11. Mějme grupu symetrií rovnostranného trojúhelníka $(D_3, \circ)$ z Příkladu 1.1. na straně 34. Sestavte rozklad grupy $(D_3, \circ)$ podle následujících podgrup $H_1 = \{R_0\}, H_2 = \{R_0, Z_A\}, H_3 = \{R_0, Z_B\}, H_4 = \{R_0, Z_C\}, H_5 = \{R_0, R_{120}, R_{240}\}$ a $H_6 = D_3$, tj. a) D_3/H_1, b) D_3/H_2, c) D_3/H_3, d) D_3/H_4, e) D_3/H_5, f) D_3/H_6.

a) Sestavíme rozklad $D_3/\{R_0\}$.

$$\begin{aligned} R_0 \circ \{R_0\} &= \{R_0\} \\ R_{120} \circ \{R_0\} &= \{R_{120}\} \\ R_{240} \circ \{R_0\} &= \{R_{240}\} \\ Z_A \circ \{R_0\} &= \{Z_A\} \\ Z_B \circ \{R_0\} &= \{Z_B\} \\ Z_C \circ \{R_0\} &= \{Z_C\} \end{aligned}$$

Dostaneme rozklad $D_3/H_1 = \{\{R_0\}, \{R_{120}\}, \{R_{240}\}, \{Z_A\}, \{Z_B\}, \{Z_C\}\}$.

b) Sestavíme rozklad $D_3/\{R_0, Z_A\}$.

$$\begin{aligned} R_0 \circ \{R_0, Z_A\} &= \{R_0, Z_A\} \\ R_{120} \circ \{R_0, Z_A\} &= \{R_{120}, Z_B\} \\ R_{240} \circ \{R_0, Z_A\} &= \{R_{240}, Z_C\} \end{aligned}$$

Dostaneme rozklad $D_3/\{R_0, Z_A\} = \{\{R_0, Z_A\}, \{R_{120}, Z_B\}, \{R_{240}, Z_C\}\}$.

c) Sestavíme rozklad $D_3/\{R_0, Z_B\}$.

$$\begin{aligned} R_0 \circ \{R_0, Z_B\} &= \{R_0, Z_B\} \\ R_{120} \circ \{R_0, Z_B\} &= \{R_{120}, Z_C\} \\ R_{240} \circ \{R_0, Z_B\} &= \{R_{240}, Z_A\} \end{aligned}$$

Dostaneme rozklad $D_3/\{R_0, Z_B\} = \{\{R_0, Z_B\}, \{R_{120}, Z_C\}, \{R_{240}, Z_A\}\}$. Všimněte si, že rozklad je jiný než $D_3/\{R_0, Z_A\}$.

d) Sestavíme rozklad $D_3/\{R_0, Z_C\}$.

$$\begin{aligned} R_0 \circ \{R_0, Z_C\} &= \{R_0, Z_C\} \\ R_{120} \circ \{R_0, Z_C\} &= \{R_{120}, Z_A\} \\ R_{240} \circ \{R_0, Z_C\} &= \{R_{240}, Z_B\} \end{aligned}$$

Dostaneme rozklad $D_3/\{R_0, Z_C\} = \{\{R_0, Z_C\}, \{R_{120}, Z_A\}, \{R_{240}, Z_B\}\}$. Všimněte si, že rozklad je opět jiný!

e) Sestavíme rozklad $D_3/\{R_0, R_{120}, R_{240}\}$.

$$\begin{aligned} R_0 \circ \{R_0, R_{120}, R_{240}\} &= \{R_0, R_{120}, R_{240}\} \\ Z_A \circ \{R_0, R_{120}, R_{240}\} &= \{Z_A, Z_B, Z_C\} \end{aligned}$$

Ostatní musí vyjít stejně jako některá z uvedených tříd. Dostaneme rozklad $D_3/\{R_0, R_{120}, R_{240}\} = \{\{R_0, R_{120}, R_{240}\}, \{Z_A, Z$

f) Sestavíme rozklad $D_3/\{R_0, R_{120}, R_{240}, Z_A, Z_B, Z_C\}$. Protože

$$R_0 \circ \{R_0, R_{120}, R_{240}, Z_A, Z_B, Z_C\} = D_3$$

a ostatní součiny musí vyjít stejně celé D_3, tak dostaneme rozklad $D_3/\{R_0, R_{120}, R_{240}, Z_A, Z_B, Z_C\} = \{\{R_0, R_{120}, R_{240}, Z_A, Z_B, Z_C\}\}$. Dostali jsme šest různých rozkladů grupy $(D_3, \circ)$. ✓

Příklad 4.12. Porovnejte rozklad D_3/H_2 pro $H_2 = \{R_0, Z_A\}$ z Příkladu 4.11. s pravým rozkladem $H_2\backslash D_3$.
První uvedený rozklad známe. Platí $D_3/\{R_0, Z_A\} = \{\{R_0, Z_A\}, \{R_{120}, Z_B\}, \{R_{240}, Z_C\}\}$. Avšak rozklad $\{R_0, Z_A\}\backslash D_3$ obsahuje *jiné* množiny

$$\{R_0, Z_A\} \circ R_0 = \{R_0, Z_A\}$$
$$\{R_0, Z_A\} \circ R_{120} = \{R_{120}, Z_C\}$$
$$\{R_0, Z_A\} \circ R_{240} = \{R_{240}, Z_B\}$$

Všimněte si, že poslední dvě třídy rozkladu jsou různé! ✓

Cvičení

4.1.1. Označme $V = \{V_1, V_2, \ldots, V_6\}$ množinu vrcholů pravidelného šestiúhelníka. Mějme zobrazení σ definované předpisem $\sigma(V_1) = V_2$, $\sigma(V_2) = V_3$, $\ldots$, $\sigma(V_6) = V_1$. Vezmeme operaci skládání zobrazení „$\circ$“. Označme $\sigma^1 = \sigma$, $\sigma^2 = \sigma \circ \sigma$, $\sigma^3 = \sigma^2 \circ \sigma$ atd. Položme $\sigma^0 = \iota$, kde ι je identita, a $\sigma^{-n} = (\sigma^{-1})^n$. Nyní definujme množinu $G = \{\sigma^n : n \in \mathbb{Z}\}$. a) Kolik různých prvků má množina G? b) Ukažte, že $(G, \circ)$ je grupa.

4.1.2. Mějme grupu $(G, \circ)$ šesti možných otočení vrcholů pravidelného šestiúhelníka ze Cvičení 4.1.1. a) Najděte vlastní podgrupu $(H, \circ)$, která obsahuje prvek σ^2. b) Sestavte rozklad grupy $(G, \circ)$ podle podgrupy $(H, \circ)$.

4.1.3. Mějme grupu $(\mathbb{Z}_7 \setminus \{\bar{0}_7\}, \cdot) = ([1, 6], \cdot)$ (grupu zbytkových tříd modulo 7 s operací „$\cdot$“ násobení). Mějme $H = \{1, 3\}$. a) Ukažte že $(H, \cdot)$ není podgrupa v $(G, \cdot)$. b) Přesto sestavte komplexy $1H$, $2H$, $\ldots$, $6H$. c) Můžeme říci, že G/H je rozklad množiny G?

4.1.4. Mějme grupu $(\mathbb{Z}_7 \setminus \{\bar{0}_7\}, \cdot) = ([1, 6], \cdot)$ (grupu zbytkových tříd modulo 7 s operací „$\cdot$“ násobení). Mějme $H = \{1\}$. a) Ukažte, že $(H, \cdot)$ je podgrupa v grupě $(G, \cdot)$. b) Sestavte $1H$, $2H$, $\ldots$, $6H$. c) Sestavte G/H.

4.1.5. Sestavte rozklad grupy $(\mathbb{Z}, +)$ podle podgrupy $(3\mathbb{Z}, +)$, kde $3\mathbb{Z} = \{3k : k \in \mathbb{Z}\}$.

4.1.6. Zobecněte Cvičení 4.1.5.: Sestavte rozklad grupy $(\mathbb{Z}, +)$ podle podgrupy $(n\mathbb{Z}, +)$, kde $n \in \mathbb{N}$ a $n\mathbb{Z} = \{kn : k \in \mathbb{Z}\}$.

4.1.7. Sestavte rozklad grupy $(\mathbb{Z}, +)$ podle podgrupy $(0\mathbb{Z}, +)$.

4.1.8. Sestavte a porovnejte levý a pravý rozklad dihedrální grupy $(D_3, \circ)$ podle podgrupy $(\{R_0, Z_A\}, \circ)$.

4.1.9. Dokažte nebo vyvraťte následující tvrzení: Mějme grupu $(G, \cdot)$ a její komplex H. Všechny komplexy $g \odot H$ mají stejný počet prvků.

4.1.10. Dokažte Větu 4.7., tj. ukažte, že pokud máme grupu $(G, \cdot)$ a nějakou neprázdnou podmnožinu $H \subseteq G$, tak platí $\bigcup_{g \in G} gH = G$.

4.1.11. Dokažte nebo vyvraťte následující tvrzení: Mějme pologrupu $(G, \cdot)$ a její komplex H. Všechny komplexy $g \odot H$ mají stejný počet prvků.

4.2. Řád grupy a index podgrupy

Jeden z ústředních výsledků teorie (konečných) grup je Lagrangeova věta. Abychom jej mohli formulovat, musíme zavést několik pojmů.

Definice Řád grupy
Mějme grupu $(G, \cdot)$. Počet prvků konečné nosné množiny G nazýváme *řádem grupy* $(G, \cdot)$ a značíme jej $|G|$. Jestliže nosič G je nekonečná množina, říkáme, že řád grupy je *nekonečný*.

Příklad 4.13. Uvedeme několik jednoduchých příkladů grup a jejich řádu.

1) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ a $(\mathbb{R} \setminus \{0\}, \cdot)$ jsou grupy nekonečného řádu.

2) Diherdální grupa symetrií rovnostranného trojúhelníka (Tabulka 1.3.) tvoří grupu řádu 6.
3) Symetrie libovolného pravidelného n-úhelníka tvoří dihedrální grupu $(D_n, \circ)$ řádu $2n$.
4) $(\mathbb{Z}_n, +)$ je grupa řádu n pro každé přirozené číslo n.
5) $(\mathbb{Z}_n \setminus \{0\}, \cdot)$ je grupa řádu $n-1$ pro každé *prvočíslo* n. Pokud n není prvočíslo, o grupu se nejedná.
6) $(U(15), \cdot)$ z Příkladu 2.19. je grupa řádu 8. Nosná množina $U(15)$ obsahuje čísla nesoudělná s číslem 15, platí $U(15) = \{1, 2, 4, 7, 8, 11, 13, 14\}$.
7) Symetrickou grupu $(S_n, \circ)$ (grupu všech permutací n-prvkové množiny s operací skládání zobrazení) zavedeme na straně 116. Symetrická grupa $(S_n, \circ)$ obsahuje všech $n!$ permutací n-prvkové množiny a je proto řádu $n!$.

Vlastní podgrupa konečné grupy má méně prvků než samotná grupa. Počty prvků grupy a její podgrupy však nejsou nezávislé. Zavedeme následující pojem.

Definice Index podgrupy
Mějme grupu $(G, \cdot)$ a její podgrupu $(H, \cdot)$. *Indexem podgrupy* $(H, \cdot)$ v grupě $(G, \cdot)$ nazveme počet prvků rozkladu G/H. Značíme $(G : H) = \left|G/H\right|$.

Příklad 4.14. Uvedeme několik jednoduchých příkladů podgrup a jejich indexu.

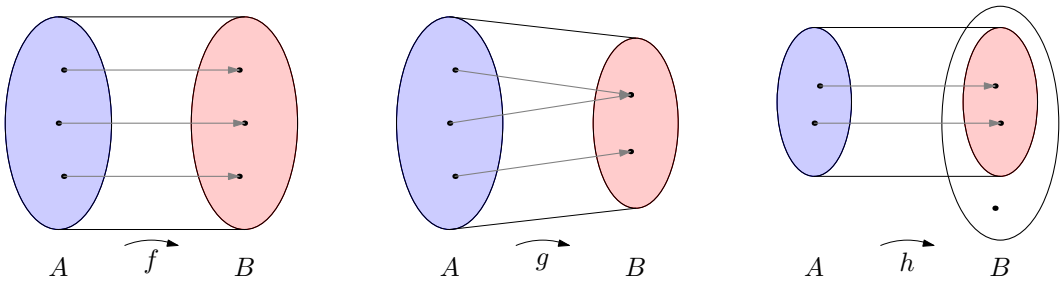
1) Index podgrupy $(\mathbb{S}, +)$ v grupě $(\mathbb{Z}, +)$ je $(\mathbb{Z} : \mathbb{S}) = 2$.
2) Index podgrupy rotací $(R_n, \circ)$ pravidelného n-úhelníka v dihedrální grupě $(D_n, \circ)$ je $(D_n : R_n) = 2$.
3) Index podgrupy $(5\mathbb{Z}, +)$ v grupě $(\mathbb{Z}, +)$ je $(\mathbb{Z} : 5\mathbb{Z}) = 5$.
4) Index podgrupy $(\{1, 6\}, \cdot)$ v grupě $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$ je $(\mathbb{Z}_7 \setminus \{0\} : \{1, 6\}) = 3$.
5) Mějme $H = \{\overline{0}_{12}, \overline{4}_{12}, \overline{8}_{12}\}$. Grupa $(H, +)$ je podgrupa v grupě $(\mathbb{Z}_{12}, +)$ a index této podgrupy je $(\mathbb{Z}_{12} : H) = 4$.
6) Avšak index grupy $(\mathbb{Z}_3, +)$ v grupě $(\mathbb{Z}_{12}, +)$ nemá smysl stanovovat, neboť grupa $(\mathbb{Z}_3, +)$ není podgrupa v $(\mathbb{Z}_{12}, +)$.

Všimněte si, že index všech podgrup v Příkladu 4.14. vyšel celočíselný. To není náhoda. Ukážeme, že všechny třídy rozkladu podle konečné množiny mají stejný počet prvků a definice indexu podgrupy pak bude mít hlubší význam: index podgrupy $(G : H)$ musí vždy být celé číslo.

O porovnávání velikostí množin
Už jsme viděli, že konečné množiny A, B mají stejný počet prvků, jestliže existuje bijekce f mezi množinami A a B, tj. existuje zobrazení množiny A do množiny B, které je současně

(i) injektivní (pro každé $a_1, a_2 \in A$ platí $(f(a_1) = f(a_2)) \Rightarrow (a_1 = a_2)$) a
(ii) surjektivní (pro každé $b \in B$ platí existuje takové $a \in A$, že $f(a) = b$).

Jsou-li A, B dvě konečné množiny, tak dobře víme, že A a B mají stejný počet prvků právě tehdy, když existuje bijekce $A \to B$. I pro nekonečné množiny A, B má smysl porovnávat jejich velikosti: řekneme, že dvě množiny jsou stejně velké, jestliže existuje bijektivní zobrazení $A \to B$ (Obrázek 4.4. vlevo). Jestliže najdeme surjektivní zobrazení $A \to B$, tak množina A je větší nebo stejně velká jako množina B (Obrázek 4.4. uprostřed). Jestliže najdeme injektivní zobrazení $A \to B$, tak množina A je nejvýše tak velká jako množina B (Obrázek 4.4. vpravo). Pro nekonečné množiny není úplně přesné mluvit o počtu prvků, avšak při porovnávání velikostí množin platí stejná tvrzení.



Obrázek 4.4.: *Schématické znázornění porovnání množin A, B: bijekce f, surjekce g a injekce h.*

Nyní ukážeme, že každá třída rozkladu G/H grupy $(G,\cdot)$ má stejný počet prvků jako podgrupa $(H,\cdot)$.

Věta 4.9. *Mějme grupu $(G,\cdot)$, její podgrupu $(H,\cdot)$. Pro každý prvek $a \in G$ platí $|aH| = |H|$.*

Důkaz. Ukážeme, že zobrazení $f : H \to aH$ dané pro každé $h \in H$ předpisem $f(h) = ah$ je bijekce. Nejprve ukážeme, že zobrazení je injektivní. Mějme $h_1, h_2 \in H$. Jestliže $f(h_1) = f(h_2)$, tak $ah_1 = ah_2$. Podle Věty o krácení (Věty 2.6.) v grupě $(G,\cdot)$ platí $h_1 = h_2$ a zobrazení f je injektivní.

Dále ukážeme, že zobrazení f je surjektivní. Podle Lemmatu 4.1. najdeme pro každý prvek y ve třídě aH (jediný) vzor $h \in H$ při zobrazení f, a proto je zobrazení f surjektivní. Dostáváme, že f je bijekce mezi množinami H a aH a proto mají obě množiny stejnou velikost. □

Cvičení

4.2.1. Určete řád dihedrální grupy $(D_n,\circ)$ symetrií pravidelného n-úhelníka a index podgrupy rotací.

4.2.2. V dihedrální grupě $(D_n,\circ)$ symetrií pravidelného n-úhelníka určete řád a index podgrupy $(H,\circ)$ pro a) $H = \{R_0\}$ b) $H = \{R_0, F\}$, kde F je některé ze zrcadlení.

4.2.3. Určete index podgrupy $(\mathbb{Z},+)$ v grupě $(\mathbb{Q},+)$ a nalezněte alespoň dva reprezentanty tříd rozkladu a) $\frac{1}{2}+\mathbb{Z}$ a b) $\frac{3}{2}+\mathbb{Z}$.

4.2.4.$^\heartsuit$ Pro každé přirozené číslo k uveďte takový příklad grupy $(G,\cdot)$ a její podgrupy $(H,\cdot)$, aby index $(G:H)$ byl roven číslu k.

4.2.5. Víme, že grupa $(U(10),\cdot)$ je podgrupou grupy $(U(20),\cdot)$. Určete její index.

4.2.6. V grupě $(\mathbb{Z},+)$ najděte podgrupu $(G,+)$, která má a) nekonečný index b) index k, kde $k \in \mathbb{N}$.

4.3. Lagrangeova věta

V předchozí podkapitole jsme zavedli řád grupy, což je číslo, které popisuje (pro konečné i nekonečné grupy) velikost nosné množiny. Nyní zavedeme číslo, které bude popisovat vlastnost každého prvku nosné množiny dané grupy.

Definice Řád prvku
Mějme grupu $(G,\cdot)$ s neutrálním prvkem e. *Řád prvku a* v grupě $(G,\cdot)$ je nejmenší přirozené číslo n takové, že $a^n = e$. Řád prvku a značíme $|a|$. Jestliže takové přirozené číslo n neexistuje, tak prvek a je *nekonečného řádu*.

Příklad 4.15. Uvedeme několik jednoduchých příkladů řádů prvků grupy.

1) V grupě $(\mathbb{Z},+)$ je řád prvku 0 roven jedné, $|0| = 1$, a řád ostatních prvků je nekonečný.
2) V dihedrální grupě $(D_3,\circ)$ (Tabulka 1.3.) je řád identity $|R_0| = 1$, řád rotací $|R_{120}| = |R_{240}| = 3$ a řád všech zrcadlení je $|Z_A| = |Z_B| = |Z_C| = 2$.
3) V grupě $(\mathbb{Z}_7 \setminus \{\overline{0}\},\cdot)$ z Příkladu 3.20. můžeme z Tabulky 3.7. určit řád prvku 1 roven $|1| = 1$, řády dalších prvků jsou následující: $|2| = 3$, neboť $2^1 \neq 1$, $2^2 = 4 \neq 1$ a $2^3 = 1$ $|3| = 6$, neboť $3^1 \neq 1$, $3^2 = 2 \neq 1$, $3^3 = 6 \neq 1$, $3^4 = 4 \neq 1$, $3^5 = 5 \neq 1$ a $3^6 = 1$. Podobně určíme $|4| = 3$, $|5| = 6$ a $|6| = 2$.
4) V grupě jednotek $(U(12),\cdot)$ z Příkladu 2.19. je prvek 1 řádu 1, prvky 5, 7 a 11 jsou řádu 2.
5) V grupě $(\mathbb{Q} \setminus \{0\},\cdot)$ je $|1| = 1$, $|-1| = 2$ a všechny ostatní prvky jsou nekonečného řádu.

Příklad 4.16. Sestavíme grupu jednotek $(U(15),\cdot)$ a určíme řády všech prvků.

$\cdot$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Tabulka 4.3.: *Cayleyho tabulka grupy* $(U(15),\cdot)$.

a	a	a^2	a^3	a^4
1	1			
2	2	4	8	1
4	4	1		
7	7	4	13	1
8	8	4	2	1
11	11	1		
13	13	4	7	1
14	14	1		

Tabulka 4.4.: *Tabulka mocnin prvků grupy* $(U(15),\cdot)$.

Z Příkladu 2.19. víme, že $(U(15),\cdot)$ je grupa. Cayleyho tabulka je Tabulka 4.3. Z tabulky snadno ověříme, že $|1|=1$, $|4|=|11|=|14|=2$.

Dále z tabulky ihned vidíme $2^2=4$, $2^3=2^2\cdot 2=4\cdot 2=8$ a $2^4=2^3\cdot 2=8\cdot 2=1$, tak $|2|=4$. Podobně $7^2=4$, $7^3=13$ a $7^4=1$, a proto $|7|=4$. Platí $8^2=4$, $8^3=2$ a $8^4=1$, a proto $|8|=4$. A konečně $13^2=4$, $13^3=7$ a $13^4=1$, a proto $|13|=4$. Situaci pěkně shrnuje Tabulka 4.4.

Všimněte si, že řád grupy $(U(15),\cdot)$ je 8, přičemž žádný z prvků grupy $(U(15),\cdot)$ není řádu 8. ✓

Pokud bychom chtěli počítat další mocniny a Tabulku 4.4. rozšířit, budou se posloupnosti mocnin opakovat, neboť označíme-li $|a|=n$, tak $a^n=e$, $a^{n+1}=a^n\cdot a=e\cdot a=a$, $a^{n+2}=a^n\cdot a^2=e\cdot a^2=a^2$, a tak dále.

Otázky:

- Mohou být v grupě současně prvky konečného i nekonečného řádu?
- Co můžeme říci o prvku grupy, jehož řád je 1?
- Co můžeme říci o prvku grupy, jehož řád je 2?
- Mějme grupu a v ní prvek a řádu n, kde $n>1$. Jak vypadá inverzní prvek k prvku a?
- Co můžeme říci o prvku a nějaké grupy, pro který platí $|a|=0$?

Podgrupa generovaná prvkem

Mohlo by se zdát, že je nešikovné používat stejný termín i stejné značení pro velikosti nosné množiny grupy („řád“ grupy) a současně pro jakousi vlastnost prvků („řád“ prvku). Následující příklad ukáže, že oba „řády“ spolu souvisí. Nejprve si uvědomíme, že jestliže nějaká podgrupa $(G,\cdot)$ obsahuje prvek a konečného řádu, tak tato podgrupa musí díky uzavřenosti operace „$\cdot$“ obsahovat všechny kladné mocniny prvku a, neboť $a^1=a$, $a^2=a\cdot a$, $a^3=a\cdot a^2$, …, $a^n=e$.

Příklad 4.17. Mějme grupu $(G,\cdot)$ a její prvek $a\in G$ konečného řádu $n\in\mathbb{N}$. Sestavíme množinu $H=\{a=a^1,a^2,\ldots,a^n=e=a^0\}$. Ukážeme, že $(H,\cdot)$ je podgrupou grupy $(G,\cdot)$ a že řád $|H|$ podgrupy $(H,\cdot)$ je roven řádu $|a|$ prvku a.

Protože n je konečné číslo, tak množina H je konečná podmnožina G a dále H je jistě neprázdná, protože $a\in H$. Podle Věty 3.5. (test konečné podgrupy) stačí ověřit uzavřenost vzhledem k operaci „$\cdot$“. Pro $i,j\in\{1,2,\ldots,n\}$ platí $a^i\cdot a^j=a^{i+j}$ a pokud $i+j>n$, tak $a^{i+j}=a^{n+k}$, kde $k=i+j-n$ a $k\in\{1,2,\ldots,n\}$. To znamená, že $a^i\cdot a^j=a^n\cdot a^k=e\cdot a^k=a^k$ a operace „$\cdot$“ je uzavřená na množině H a $(H,\cdot)$ je podgrupou grupy $(G,\cdot)$. ✓

V Kapitole 6.2. tvrzení příkladu 4.17. zobecníme pro libovolné grupy a libovolné prvky konečného i nekonečného řádu. Grupě $(H,\cdot$ z Příkladu 4.17. budeme říkat cyklická grupa a budeme ji značit $(\langle a\rangle,\cdot)$.

Příklad 4.18. Mějme komutativní grupu $(G,\cdot)$. Označme H množinu všech prvků z G, které jsou konečného řádu. Ukážeme, že $(H,\cdot)$ je podgrupou grupy $(G,\cdot)$.
Stačí ověřit předpoklady testu podgrupy (Věta 3.3.). Jistě platí $H \subseteq G$. Dále řád neutrálního prvku e je 1, proto $e \in H$ a $H \neq \emptyset$. Dále pro libovolné dva prvky $a, b \in H$ (prvky jsou konečného řádu $|a| = m$, $|b| = n$) platí $(a \cdot b)^{mn} = (a^m)^n \cdot (b^n)^m = e^m \cdot e^n = e \cdot e = e$ a proto řád prvku $a \cdot b$ je také konečný, nejvýše mn. A konečně je-li prvek a konečného řádu m, tak inverzní prvek a^{-1} je také (konečného) řádu m (Cvičení 4.3.8.). ✓

Tvrzení příkladu není prázdné, neboť triviální podgrupa je (triviálním) příkladem konečné podgrupy v každé grupě. Netriviálním příkladem může být například dvouprvková podgrupa $(\{1,-1\},\cdot)$ v grupě $(\mathbb{Q}\setminus\{0\},\cdot)$ nebo v grupě $(\mathbb{R}\setminus\{0\},\cdot)$.

Řád prvku, řád grupy a index podgrupy

Klíčovým tvrzením této kapitoly je následující věta, která ukazuje, že řád grupy, řád podgrupy, index podgrupy a řády prvků jsou v grupě spolu svázány a terminologie není náhodná.

Věta 4.10. Lagrangeova věta
Mějme konečnou grupu $(G,\cdot)$ a její podgrupu $(H,\cdot)$. Potom platí

(i) $|G| = (G:H)\cdot|H|$,
(ii) $|H|$ *dělí* $|G|$,
(iii) Jestliže $a \in G$ je prvek řádu n, potom n dělí $|G|$,
(iv) Jestliže $(K,\cdot)$ je podgrupa $(H,\cdot)$ a $(H,\cdot)$ je podgrupa v $(G,\cdot)$, potom $(G:K) = (G:H)\cdot(H:K)$.

Důkaz.
(i) Protože G/H je rozklad množiny G, tak v každé třídě rozkladu G/H je podle Věty 4.9. stejný počet prvků $|H|$. Počet tříd rozkladu je $(G:H)$, a proto počet prvků v G je vskutku $|H|\cdot(G:H)$.
(ii) Ihned z předchozího kroku (i) vidíme, že řád $|G|$ je násobkem řádu $|H|$.
(iii) Označme $X = \{a, a^2, a^3, \ldots, a^n = e\}$. Protože $(X,\cdot)$ je podle Příkladu 4.17. podgrupou v $(G,\cdot)$, tak $|X|$ dělí $|G|$ podle již dokázaného bodu (ii) této věty. Z definice množiny X je zřejmé, že řád podgrupy $|X|$ je roven řádu prvku $|a|$ a proto dostáváme, že $|a| = n$ a n dělí $|G|$.
(iv) Podle již dokázané části (i) této věty platí

$$|G| = (G:H)\cdot|H|, \quad |G| = (G:K)\cdot|K|$$

Stejně tak platí $|H| = (H:K)\cdot|K|$ a dosazením do první rovnosti ihned dostaneme

$$|G| = (G:H)\cdot|H| = (G:H)\cdot(H:K)\cdot|K| = (G:K)\cdot|K|$$
$$(G:H)\cdot(H:K) = (G:K).$$

Protože podle definice grupy je řád $|K| \neq 0$, tak v poslední rovnosti můžeme krátit $|K|$. □

Uvědomte si, že mezi různými třídami rozkladu může pouze jediná třída být nosičem podgrupy, neboť podgrupa musí obsahovat neutrální prvek grupy. Různé podgrupy tak nemohou nikdy společně tvořit jeden rozklad grupy.

Příklad 4.19. Sestavte všechny podgrupy dihedrální grupy $(D_3,\circ)$ (grupy symetrií rovnostranného trojúhelníka), která je popsána Cayleyho tabulkou 1.3.
Podle Lagrangeovy věty (Věta 4.10.) mohou v dihedrální grupě $(D_3,\circ)$ existovat podgrupy pouze řádů, které dělí číslo 6, tj.podgrupy řádů 1, 2, 3 a 6. Čtyř- a pětiprvkové prvkové podgrupy podle Lagrangeovy věty neexistují.

Jednoprvková podgrupa je jediná, pouze triviální podgrupa $(\{R_0\},\circ) = (H_1,\circ)$.

Dvouprvkové podgrupy musí obsahovat neutrální prvek R_0. Takové podgrupy jsou tři, což ověříme z Cayleyho tabulky 1.3. Označíme si je $(H_2,\circ) = (\{R_0, Z_A\},\circ)$, $(H_3,\circ) = (\{R_0, Z_B\},\circ)$ a $(H_4,\circ) = (\{R_0, Z_C\},\circ)$. Druhý prvek kromě R_0 musí být svou vlastní inverzí (jinak by inverzní prvek také musel patřit do této podgrupy, která by už nemohla být dvouprvková), proto dvouprvkové podgrupy obsahují vždy jen neutrální prvek R_0 a nějaké zrcadlení, které je dle Příkladu 4.15. řádu 2.

Jestliže podgrupa dihedrální grupy $(D_3,\circ)$ obsahuje prvek R_{120}, tak z uzavřenosti operace skládání musí do této podgrupy patřit také inverzní prvek R_{240} a naopak, zařazení prvku R_{240} si vynutí zařazení prvku R_{120}. Dostaneme tříprvkovou podgrupu $(\{R_0, R_{120}, R_{240}\},\circ)$. Dále, jestliže do nějaké podgrupy patří některá dvě různá zrcadlení, tak jejich složením bude otočení (což je pěkně vidět z Cayleyho tabulky 1.3.) a každá

taková podgrupa by měla alespoň čtyři prvky: identitu, dvě zrcadlení a alespoň jedno otočení. Tříprvkové podgrupy obsahující zrcadlení proto neexistují. Tříprvková podgrupa je proto jedině podgrupa $(H_5, \circ) = (\{R_0, R_{120}, R_{240}\}, \circ)$.

Šestiprvková podgrupa dihedrální grupy $(D_3, \circ)$ je celá grupa $(H_6, \circ) = (D_3, \circ)$. ✓

Příklad 4.20. Mějme grupu $(G, \cdot) = (\mathbb{Z}_{12}, +)$ a její podgrupy $(H, +)$ a $(K, +)$, kde $H = \{0, 2, 4, 6, 8, 10\}$ a $K = \{0, 4, 8\}$. Navíc platí, že $(K, +)$ je podgrupou v $(H, +)$. a) Určíme řád grupy $(G, +)$ i řády obou podgrup $(H, +)$ a $(K, +)$ a navzájem je porovnáme. b) Určíme řády jednotlivých prvků v grupě $(G, +)$ a porovnáme je s řádem grupy. c) Určíme řády prvků v (pod)grupách $(H, +)$ a $(K, +)$.

a) Určit řády všech grup je snadné: stačí určit počet prvků. Platí $|G| = 12$, $|H| = 6$ a $|K| = 3$. Ihned vidíme, že řád $|H| = 6$ dělí řád $|G| = 12$ a že řád $|K| = 3$ dělí řád $|G| = 12$ i řád $|H| = 6$.

b) Sestavíme tabulku mocnin (v aditivní notaci násobků) jednotlivých prvků grupy $(G, +)$ a určíme řády prvků. Z Tabulky 4.5. ihned vidíme, že $|0| = 1$, $|1| = |5| = |7| = |11| = 12$, $|2| = |10| = 6$, $|3| = |9| = 4$, $|4| = |8| = 3$ a $|6| = 2$.

a	a	$2a$	$3a$	$4a$	$5a$	$6a$	$7a$	$8a$	$9a$	$10a$	$11a$	$12a$
0	0											
1	1	2	3	4	5	6	7	8	9	10	11	0
2	2	4	6	8	10	0						
3	3	6	9	0								
4	4	8	0									
5	5	10	3	8	1	6	11	4	9	2	7	0
6	6	0										
7	7	2	9	4	11	6	1	8	3	10	5	0
8	8	4	0									
9	9	6	3	0								
10	10	8	6	4	2	0						
11	11	10	9	8	7	6	5	4	3	2	1	0

Tabulka 4.5.: *Tabulka mocnin prvků grupy* $(\mathbb{Z}_{12}, +)$.

c) Analogicky jako v předchozí části určíme řády jednotlivých prvků v podgrupách. Sestavíme Tabulky 4.6. Všimněte si, že řád prvku v podgrupě je stejný jako řád stejného prvku v celé grupě (Cvičení 4.3.2.). ✓

a	a	$2a$	$3a$	$4a$	$5a$	$6a$
0	0					
2	2	4	6	8	10	0
4	4	8	0			
6	6	0				
8	8	4	0			
10	10	8	6	4	2	0

a	a	$2a$	$3a$
0	0		
4	4	8	0
8	8	4	0

Tabulka 4.6.: *Tabulky mocnin prvků grupy* $(H, +)$ *a grupy* $(K, +)$.

Na Příklad 4.20. navážeme. Vezmeme rozklady grupy $(G, +)$ podle různých podgrup $(H, +)$, $(K, +)$ a jestliže navíc $(K, +)$ je podgrupou grupy $(H, +)$, bude rozklad grupy $(G, +)$ podle podgrupy $(K, +)$ navíc rozkládat třídy rozkladu grupy $(G, +)$ podle podgrupy $(H, +)$.

Příklad 4.21. Mějme grupu $(\mathbb{Z}_{12}, +)$ a její podgrupy $(H, +)$ a $(K, +)$ z Příkladu 4.20. Sestavíme rozklad grupy $(\mathbb{Z}_{12}, +)$ a) podle podgrupy $(H, +)$, b) podle podgrupy $(K, +)$, c) určíme index podgrupy $(H, +)$ i podgrupy $(K, +)$ v grupě $(\mathbb{Z}_{12}, +)$ a ukážeme, že menší podgrupa má větší index.

a) Rozklad grupy $(\mathbb{Z}_{12}, +)$ podle její podgrupy $(H, +)$ je rozkladem dle Důsledku 4.8.

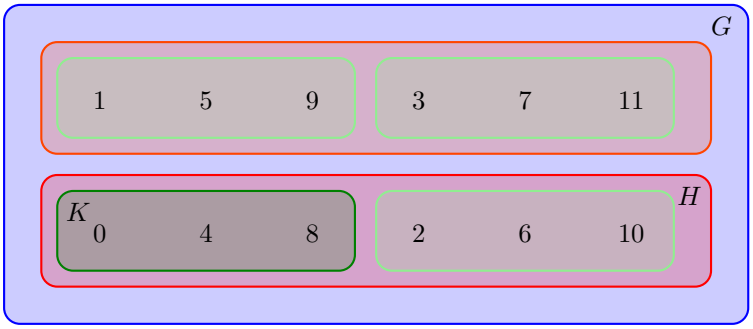
$$0 + H = \{0, 2, 4, 6, 8, 10\} = H$$
$$1 + H = \{1, 3, 5, 7, 9, 11\}$$

Nyní s využitím Věty 4.2. už víme, že například $3 + H = 1 + (2 + H) = 1 + H$ nebo $6 + H = 4 + (2 + H) = 4 + H = \ldots = H$.

b) Druhý rozklad, rozklad grupy $(\mathbb{Z}_{12}, +)$ podle její podgrupy $(K, +)$, je rozkladem opět dle Důsledku 4.8.

$$\begin{aligned} 0 + K &= \{0, 4, 8\} = K \\ 1 + K &= \{1, 5, 9\} \\ 2 + K &= \{2, 6, 10\} \\ 3 + K &= \{3, 7, 11\} \end{aligned}$$

c) Index podgrupy $(H, +)$ v grupě $(\mathbb{Z}_{12}, +)$ je $(\mathbb{Z}_{12} : H) = 2$ a index podgrupy $(K, +)$ je $(\mathbb{Z}_{12} : K) = 4$. Podgrupa poloviního řádu má dvakrát větší index. Na Obrázku 4.5. je ilustrováno tvrzení Lagrangeovy věty (Věty 4.10.). Všimněte si, protože navíc je grupa $(K, +)$ podgrupou grupy $(H, +)$, tak množina K a její třída rozkladu $\{2, 6, 10\}$ tvoří rozklad nosiče H. ✓



Obrázek 4.5.: *Třídy rozkladu grupy* $(\mathbb{Z}_{12}, +)$ *podle podgrup* $(\{0, 2, 4, 6, 8, 10\}, +)$ *a* $(\{0, 4, 8\}, +)$.

Nyní ukážeme, že pozorování z předchozího příkladu platí obecně.

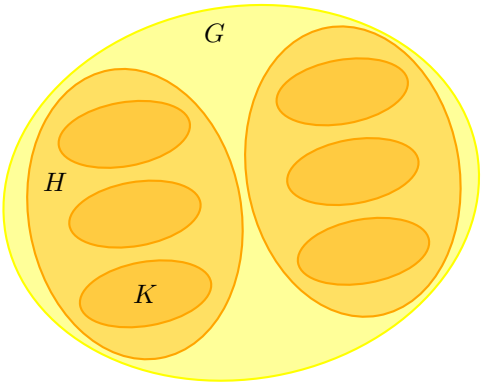
Věta 4.11. *Mějme grupu* $(G, \cdot)$ *a její podgrupy* $(H, \cdot)$, $(K, \cdot)$. *Jestliže index* $(G : K)$ *je konečné číslo a* $K \subseteq H$, *pak platí*

(i) $(G : K) \geq (G : H)$,
(ii) $(G : K) \geq (H : K)$.

Důkaz.
i) Víme, že index $(G : K)$ je konečné číslo. Potom $(G : K) = n$, kde $n \in \mathbb{N}$. Třídy rozkladu G/K si můžeme napsat jako $G/K = \{g_1K, g_2K, \ldots, g_nK\}$ pro vhodné prvky $g_1, g_2, \ldots, g_n \in G$ a podle Věty 4.6. platí $\cup_{i=1}^{n} g_iK = G$. Protože $K \subseteq H$, tak podle definice součinu komplexů pro každé $i = 1, 2, \ldots, n$ platí $g_iK \subseteq g_iH$. To ale znamená, že

$$G = \bigcup_{i=1}^{n} g_iK \subseteq \bigcup_{i=1}^{n} g_iH \subseteq G,$$

protože $\cup_{i=1}^{n} g_iH \subseteq G$. Víme tedy, že platí $\cup_{i=1}^{n} g_iH = G$. Množiny g_iH sice nemusí pro $i = 1, 2, \ldots, n$ tvořit rozklad, protože některé třídy rozkladu se mohou opakovat, ale různé třídy jsou podle Důsledku 4.5. navzájem disjunktní (Obrázek 4.6.). Proto $|G/H| \leq n = |G/K|$, což je dokazované tvrzení.



Obrázek 4.6.: *Grupa* $(G, \cdot)$ *a indexy jejích podgrup* $(H, \cdot)$ *a* $(K, \cdot)$.

ii) Víme, že index $(G:K)$ je konečné číslo. Potom opět označme $(G:K)=n$, kde $n\in\mathbb{N}$. Třídy rozkladu G/K si opět můžeme napsat jako $G/K=\{g_1K,g_2K,\ldots,g_nK\}$ pro vhodné prvky $g_1,g_2,\ldots,g_n$ a platí $\cup_{i=1}^{n}g_iK=G$.

Nyní $H/K=\{hK:h\in H\}$. Jestliže místo $h\in H$ vezmeme všechny $g\in G$, tak dostaneme

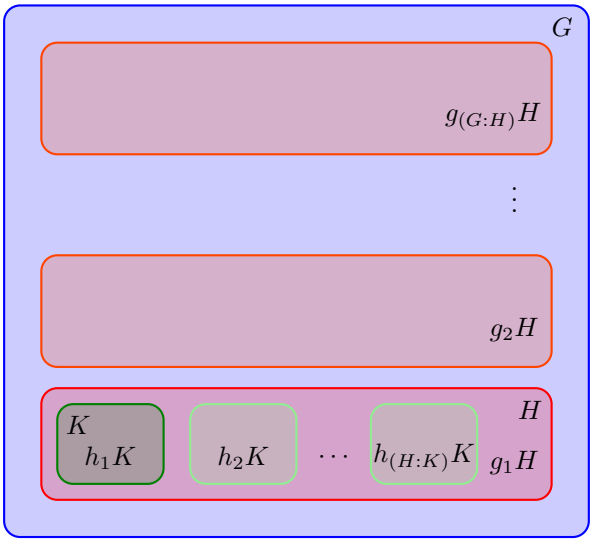
$$H/K=\{hK:h\in H\}\subseteq\{gK:g\in G\}=G/K,$$

přičemž $G/K=\{g_1K,g_2K,\ldots,g_nK\}$ obsahuje navzájem disjunktní třídy rozkladu G/K. Třídy $\{hK:h\in H\}$ sice nemusí být nutně navzájem různé, ale třídy g_iK navzájem různé jistě jsou, proto pro každé $hK\in H/K$ existuje právě jedna taková třída $g_iK\in G/K$, že $hK=g_iK$ (Obrázek 4.6.). Proto $\left|G/K\right|\geq\left|H/K\right|$, což je dokazované tvrzení. □

Příklad 4.22. Lagrangeova věta říká, že pro konečnou grupu $(G,\cdot)$ a její podgrupy $(H,\cdot)$ a $(K,\cdot)$, kde $K\subseteq H\subseteq G$ platí $(G:K)=(G:H)(H:K)$. Na příkladu ukážeme, že tvrzení platí i pro nekonečné grupy $(G,\cdot)$ za předpokladu $(G:K)$ je konečné číslo.

Podle předpokladu víme, že index $(G:K)=n$, kde $n\in\mathbb{N}$ (n je konečné číslo). Podle Lagrangeovy věty (Věta 4.11.) je také $(G:H)\in\mathbb{N}$ a $(H:K)\in\mathbb{N}$.

Můžeme rozepsat, že $G/H=\{g_1H,g_2H,\ldots,g_{(G:H)}H\}$ a platí $\bigcup_{i=1}^{(G:H)}g_iH=G$. Podobně můžeme psát $H/K=\{h_1K,h_2K,\ldots,h_{(H:K)}K\}$ a platí $\bigcup_{j=1}^{(H:K)}h_jK=H$. Situaci popisuje obrázek 4.7.



Obrázek 4.7.: *Třídy rozkladu G/H a v nich třídy rozkladu H/K.*

Dosadíme H rozepsané dle H/K do rozkladu G/H. Dostaneme

$$G=\bigcup_{i=1}^{(G:H)}g_iH=\bigcup_{i=1}^{(G:H)}g_i\left(\bigcup_{j=1}^{(H:K)}h_jK\right)=\bigcup_{i=1}^{(G:H)}\left(\bigcup_{j=1}^{(H:K)}g_ih_jK\right).$$

Jistě platí $g_ih_j\in G$ a proto g_ih_jK je nějaká třída rozkladu G/K. Ukážeme, že tyto třídy rozkladu G/K jsou po dvou disjunktní. Postupujeme nepřímo. Předpokládejme, že $g_{i_1}h_{j_1}K\cap g_{i_2}h_{j_2}K\neq\emptyset$. To znamená, že existují $k_1,k_2\in K$ takové, že $g_{i_1}h_{j_1}k_1=g_{i_2}h_{j_2}k_2$. Jistě platí $h_{j_1}k_1\in H$ a $h_{j_2}k_2\in H$, neboť $K\subseteq H$. Jenže $\{g_1H,g_2H,\ldots,g_{(G:H)}H\}$ tvoří rozklad množiny G, a pokud jsou třídy rozkladu neprázdné, tak podle Věty 4.4. platí $g_{i_1}H=g_{i_2}H$ pouze v případě, že $g_{i_1}=g_{i_2}$, tedy pro $i_1=i_2$.

Analogicky, protože $\{h_1K,h_2K,\ldots,h_{(H:K)}K\}$ tvoří rozklad množiny H, tak $h_{j_1}K=h_{j_2}K$ pouze v případě, že $h_{j_1}=h_{j_2}$, tedy $j_1=j_2$. To ale znamená, že množiny v $\bigcup_{i=1}^{(G:H)}\left(\bigcup_{j=1}^{(H:K)}g_ih_jK\right)$ jsou navzájem disjunktní a tvoří rozklad $G/K=\{g_ih_jK:i\in\{1,2,\ldots,(G:K)\},j\in\{1,2,\ldots,(H:K)\}\}$. Platí $(G:K)=$ $=(G:H)(H:K)$, což je konečné číslo. ✓

Reprezentanti tříd rozkladu

Máme-li grupu $(G,\cdot)$ a její podgrupy $(H,\cdot)$, tak i pro různé prvky $a,b\in G$ můžeme dostat stejné třídy $aH = bH$ rozkladu G/H. Pokud nás zajímají třídy rozkladu, nikoliv prvky samotné, můžeme stejnou třídu popsat pomocí různých prvků. Budeme jim říkat reprezentanti.

Definice Mějme grupu $(G,\cdot)$ a její podgrupy $(H,\cdot)$. Mějme rozklad $G/H = \{gH : g\in G\}$. *Reprezentantem* třídy rozkladu gH nazveme libovolné $x\in G$, pro které platí $x\in gH$.

Příklad 4.23. Uvedeme několik jednoduchých příkladů reprezentantů tříd rozkladů.

1) Mějme rozklad $(\mathbb{Z},+)/(\mathbb{S},+)$ se dvěma třídami rozkladu $\mathbb{S}$ a $\mathbb{L}$. Reprezentantem třídy $\mathbb{S}$ je kterékoliv sudé číslo a reprezentantem třídy $\mathbb{L}$ je kterékoliv liché číslo.
2) Rozklad $(\mathbb{Z},+)/(n\mathbb{Z},+)$ má n tříd rozkladu. Reprezentantem třídy $\overline{i+n\mathbb{Z}}$ je kterékoliv číslo, které dává po dělení číslem n stejný zbytek jako číslo i. Například v rozkladu $(\mathbb{Z},+)/(4\mathbb{Z},+)$ je reprezentantem třídy $\overline{3+4\mathbb{Z}}$ číslo 111 nebo číslo -109.
3) V rozkladu diherdální grupy symetrií rovnostranného trojúhelníka podle podrgupy rotací D_n/R_n jsou dvě třídy rozkladu. Reprezentantem třídy rotací R_n je kterákoliv rotace a reprezentantem třídy zrcadlení je kterékoliv zrcadlení.

Podle definice je prvek a je reprezentantem třídy gH rozkladu grupy $(G,\cdot)$ podle podgrupy $(H,\cdot)$ právě tehdy, když $a\in gH$. Ve Cvičení 4.3.6. ukážeme, že pokud H není nosičem podgrupy, tak analogické tvrzení platit nemusí.

Cvičení

4.3.1. Nechť p je prvočíslo, $(G,\cdot)$ je grupa a $(H,\cdot)$ je její podgrupa indexu p. Jestliže $(X,\cdot)$ je podgrupa grupy $(G,\cdot)$ taková, že $H\subseteq X\subseteq G$, pak $X=G$ nebo $X=H$.

4.3.2. Mějme grupu $(G,\cdot)$, její podgrupu $(H,\cdot)$ a prvek $a\in H$. Ukažte, že řád prvku a v grupě $(G,\cdot)$ je stejný jako v podgrupě $(H,\cdot)$.

4.3.3. Mějme grupu $(G,\cdot)$ a její podgrupu $(H,\cdot)$. Ukažte, že pro všechna $a,b\in G$ platí $aH=bH$ právě tehdy, když $b^{-1}aH=H$.

4.3.4. Mějme grupu $(G,\cdot)$ a její podgrupu $(H,\cdot)$. Ukažte, že pro všechna $a,b\in G$ platí $aH=bH$ právě tehdy, když $b^{-1}a\in H$.

4.3.5. Ukažte, že $a\in G$ je reprezentantem třídy rozkladu $gH\in G/H$ právě tehdy, když $aH=gH$.

4.3.6. Dokažte nebo vyvraťte: mějme grupu $(G,\cdot)$, podmnožinu $H\subseteq G$ a prvek $g\in G$. Pro každé $a\in gH$ platí $aH=gH$.

4.3.7. Určete řády všech prvků v dihedrální grupě $(D_3,\circ)$.

4.3.8. Ukažte, že v grupě je řád prvku a stejný jako řád inverzního prvku a^{-1}.

4.3.9. Mějme komutativní grupu $(G,\cdot)$. Ukažte, že prvky konečného řádu tvoří podgrupu v grupě $(G,\cdot)$.

4.3.10. Najděte příklad grupy $(G,\cdot)$, ve které existuje nekonečně mnoho prvků konečného řádu.

4.3.11.$^\heartsuit$ Ukažte, že v libovolné grupě je každý prvek řádu 2 inverzní sám k sobě.

4.3.12.$^\heartsuit$ Mějme grupu $(G,\cdot)$ a její prvek a řádu 12. Najděte nějaký prvek a) řádu 3, b) řádu 4 a c) řádu 6. Co můžeme říci o prvcích řádu 5?

4.3.13. Ukažte, že v libovolné grupě řádu 8 existuje prvek řádu 2.

4.3.14.$^\heartsuit$ Ukažte, že v každé grupě lichého řádu neexistuje prvek řádu 2.

4.3.15. Ukažte, že v každé grupě sudého řádu existuje prvek řádu 2.

4.3.16. Mějme konečnou grupu $(G,\cdot)$. Ukažte, že počet prvků řádu 3 v množině G je sudý.

4.3.17. Mějme grupu $(G,\cdot)$ a nějaký její prvek a řádu 7. Ukažte, že prvek a je třetí mocninou nějakého prvku grupy $(G,\cdot)$.

4.3.18. Mějme dvě nesoudělná přirozená čísla p, q. Mějme grupu $(G,\cdot)$ a nějaký její prvek a řádu p. Ukažte, že prvek a je q-tou mocninou nějakého prvku grupy $(G,\cdot)$.*

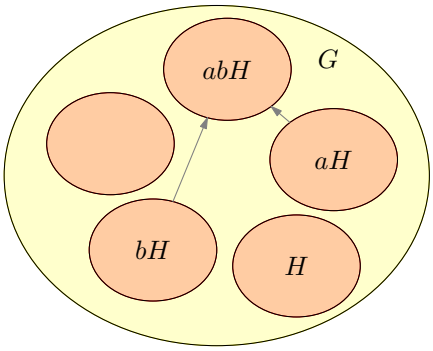
4.3.19.$^\heartsuit$ Mějme libovolný prvek a grupy $(G,\cdot)$. Ukažte, že platí $a^{|G|}=e$.

4.3.20.$^{\heartsuit}$ *Mějme grupu $(G,\cdot)$ prvočíselného řádu p. Ukažte, že každý prvek grupy je buď neutrální nebo stejného řádu p.*

4.3.21. Mějme grupu $(G,\cdot)$ řádu n. Ukažte, že opačné tvrzení k částem (ii) a (iii) Lagrangeovy věty neplatí: jestliže číslo k dělí řád n, tak grupa $(G,\cdot)$ nemusí mít prvek řádu k, ani podgrupu řádu k.*

Kapitola 5. Normální podgrupy

V předchozí kapitole jsme ukázali, jak rozložit grupu $(G, \cdot)$ podle podgrupy. Víme, že třídy rozkladu jsou komplexy se stejnou mohutností. Tyto komplexy umíme násobit (respektive sčítat). Ukážeme, že někdy, *avšak ne vždy*, tyto komplexy rozkladu grupy $(G, \cdot)$ podle podgrupy $(H, \cdot)$ spolu s operací násobení komplexů budou tvořit algebraickou strukturu. Klíčové bude, zda operace násobení komplexů bude uzavřenou operací na množině G/H. Ukážeme, že pokud podgrupa $(H, \cdot)$ má jisté pěkné vlastnosti, tak množina G/H spolu s operací násobení komplexů bude dokonce tvořit grupu (Obrázek 5.1.).



Obrázek 5.1.: *Operace s třídami rozkladu* G/H.

5.1. Normální podgrupa a faktorová grupa

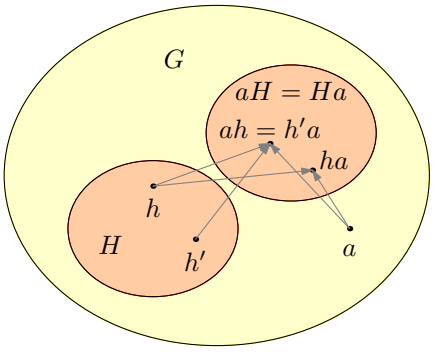
Zatím jsme rozlišovali, zda grupa je komutativní nebo nekomutativní. Má však smysl jemnější dělení, kdy nekomutativní podgrupa nějaké grupy se „navenek“ jeví jako komutativní a pouze „uvnitř“ podgrupy dojde k rozlišení výsledku operace v závislosti na pořadí operandů. Proto zavádíme následující definici.

Definice Normální podgrupa
Mějme grupu $(G, \cdot)$. Její podgrupu $(H, \cdot)$ nazveme *normální podgrupou grupy* $(G, \cdot)$ právě tehdy, když pro každé $g \in G$ platí $g \odot H = H \odot g$.

Připomeňme, že „$\odot$“ značí operaci mezi prvkem a komplexem. V dalším budeme podle úmluvy značení této multiplikativní operace vynechávat a v definici normální podgrupy budeme psát například $\forall g \in G : gH = Hg$.

Uvědomte si, že každá podgrupa komutativní grupy je normální, neboť $gH = \{gh : h \in H\} = \{hg : h \in H\} = Hg$. V nekomutativních grupách jsou některé podgrupy normální a některé ne. Neříkáme však, že jsou „nenormální“.

Normální podgrupa $(H, \cdot)$ grupy $(G, \cdot)$ má jistý aspekt komutativity. Operace „$\cdot$“ je komutativní vně podgrupy $(H, \cdot)$: pro každý prvek a grupy platí $aH = Ha$. Uvnitř podgrupy $(H, \cdot)$ můžeme prvek „popravit“. Jestliže $a \in G$ a $h \in H$, tak obecně nemusí platit $ah = ha$, avšak můžeme najít takový prvek h' v podgrupě $(H, \cdot)$, že $ah = h'a$ (Obrázek 5.2.).



Obrázek 5.2.: *Normální podgrupa* $(H, \cdot)$ *grupy* $(G, \cdot)$.

Příklad 5.1. Uvedeme několik jednoduchých příkladů normálních podgrup.

1) V komutativní grupě $(G,\cdot)$ je každá podgrupa normální.
2) Triviální podgrupa je v každé grupě $(G,\cdot)$ normální, neboť podle definice neutrálního prvku e pro všechny prvky $a \in G$ platí $e \cdot a = a \cdot e$.
3) Nevlastní podgrupa je v každé grupě $(G,\cdot)$ normální (Cvičení 5.2.4.).
4) V dihedrální grupě $(D_3,\circ)$ je netriviální vlastní normální podgrupa $(\{R_0, R_{120}, R_{240}\},\circ)$ (Příklad 5.3.).
5) Centrum $(Z(G),\cdot)$ každé grupy $(G,\cdot)$ je normální podgrupa v $(G,\cdot)$ (Cvičení 5.1.2.).
6) Podgrupa regulárních čtvercových matic s determinantem 1 je normální podgrupou grupy $(M^*_{n,n},\cdot)$, což je grupa regulárních čtvercových matic řádu n s operací násobení matic (Cvičení 5.2.1.).

Příklad 5.2. Uvedeme také několik příkladů podgrup, které normální podgrupou nejsou.

1) V dihedrální grupě $(D_6,\circ)$ není ani jedna z dvouprvkových podgrup $(\{R_0, Z_A\},\circ)$, $(\{R_0, Z_B\},\circ)$, ani $(\{R_0, Z_C\},\circ)$ normální podgrupou (Příklad 5.4.). Podobně v dihedrální grupě $(D_4,\circ)$ není ani jedna z dvouprvkových podgrup $(\{R_0, V\},\circ)$, $(\{R_0, H\},\circ)$, $(\{R_0, F\},\circ)$, ani $(\{R_0, E\},\circ)$ normální podgrupou.
2) Podgrupa regulárních diagonálních matic $(D^*_{n,n},\cdot)$ není normální podgrupou v grupě regulárních čtvercových matic řádu n s operací násobení matic $(M^*_{n,n},\cdot)$ (Příklad 5.8.).

Příklad 5.3. Mějme dihedrální grupu $(D_3,\circ)$ symetrií trojúhelníka. Ukažte, že její podgrupa všech rotací $(R_n,\circ)$ pro $R_n = \{R_0, R_{120}, R_{240}\}$ je normální.
Ověříme definici normální podgrupy. Pro každý prvek $a \in D_3$ platí $a \circ R_n = R_n \circ a$.

$$\begin{aligned}
R_0 \circ \{R_0, R_{120}, R_{240}\} &= \{R_0, R_{120}, R_{240}\} = \{R_0, R_{120}, R_{240}\} \circ R_0\\
R_{120} \circ \{R_0, R_{120}, R_{240}\} &= \{R_{120}, R_{240}, R_0\} = \{R_0, R_{120}, R_{240}\} \circ R_{120}\\
R_{240} \circ \{R_0, R_{120}, R_{240}\} &= \{R_{240}, R_0, R_{120}\} = \{R_0, R_{120}, R_{240}\} \circ R_{240}\\
Z_A \circ \{R_0, R_{120}, R_{240}\} &= \{Z_A, Z_B, Z_C\} = \{R_0, R_{120}, R_{240}\} \circ Z_A\\
Z_B \circ \{R_0, R_{120}, R_{240}\} &= \{Z_B, Z_C, Z_A\} = \{R_0, R_{120}, R_{240}\} \circ Z_B\\
Z_C \circ \{R_0, R_{120}, R_{240}\} &= \{Z_C, Z_A, Z_B\} = \{R_0, R_{120}, R_{240}\} \circ Z_C.
\end{aligned}$$

To znamená, že podgrupa $(R_n,\circ)$ je normální v $(G,\circ)$. ✓

Příklad 5.4. Mějme dihedrální grupu symetrií trojúhelníka $(D_3,\circ)$. Ukažte, že její podgrupa $(H,\circ)$, kde $H = \{R_0, Z_A\}$, není normální.
Stačí najít takový prvek g grupy D_3, že $g \cdot H \neq H \cdot g$. Vezmeme-li například $g = R_{120}$, tak

$$g \circ H = R_{120} \circ \{R_0, Z_A\} = \{R_{120}, Z_B\},$$

ale

$$H \circ g = \{R_0, Z_A\} \circ R_{120} = \{R_{120}, Z_C\}.$$

To znamená, že výsledné množiny jsou různé a podgrupa $(H,\circ)$ není normální v $(G,\circ)$. ✓

Následující věta ukáže, že na třídách rozkladu grupy podle *normální* podgrupy můžeme přirozeným způsobem zavést operaci. Tato operace odpovídá násobení komplexů, které jsme zavedli na straně 71.

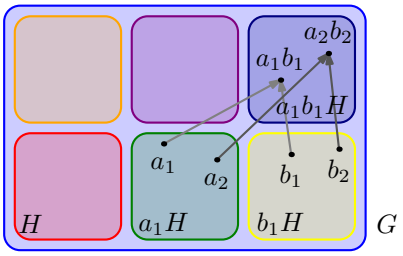
Věta 5.1. *Mějme normální podgrupu $(H,\cdot)$ grupy $(G,\cdot)$. Na množině $G/H = \{aH : a \in G\}$ definujeme operaci „$\star$“ předpisem*

$$\forall a, b \in G : (aH) \star (bH) = (a \cdot b)H.$$

Potom $(G/H, \star)$ je grupa.

Důkaz. Nejprve ověříme korektnost definice operace „$\star$“, protože na první pohled není jasné, zda výsledek operace „$\star$“ mezi dvěma komplexy závisí nebo nezávisí na volbě reprezentantů. Předpokládejme, že $a_1H = a_2H$ a $b_1H = b_2H$. Ukážeme, že $a_1H \star b_1H = a_2H \star b_2H$. Protože $a_1H = a_2H$, tak existují takové prvky $h_1, h_2 \in H$, pro které platí $a_1h_1 = a_2h_2$ a tedy $a_1 = a_2h_2h_1^{-1} = a_2h$, kde jsme označili $h = h_2h_1^{-1}$. Podobně se ukáže, že pokud $b_1H = b_2H$, tak $b_1 = b_2h'$, pro nějaké $h' \in H$. Platí

$$a_1H \star b_1H = (a_1b_1)H = a_1b_2h'H = a_1b_2H,$$



Obrázek 5.3.: *Operace s třídami rozkladu* $(G/H, \star)$ *je dobře definovaná.*

přičemž poslední rovnost plyne z Věty 4.2. Nyní z normálnosti podgrupy H dostáváme, že

$$a_1b_2H = a_1Hb_2 = a_2hHb_2 = a_2Hb_2.$$

Dále opět z normálnosti podgrupy H vidíme, že

$$a_2Hb_2 = a_2b_2H = a_2H \star b_2H,$$

což znamená, že operace „$\star$“ je korektně definovaná (Obrázek 5.3.).

Nyní dokážeme, že $(G/H, \star)$ je grupa. Nosná množina G/H je jistě neprázdná, protože $H \in G/H$. Operace „$\star$“ je uzavřená na G/H, protože pro každé $aH, bH \in G/H$ platí

$$aH \star bH = (ab)H \in G/H.$$

Asociativita operace „$\star$“ plyne z asociativity operace „$\cdot$“, neboť pro každé $aH, bH, cH \in G/H$ platí

$$aH \star (bH \star cH) = aH \star (bc)H = a(bc)H = (ab)cH = (ab)H \star cH = (aH \star bH) \star cH.$$

První rovnost plyne z definice operace „$\star$“, třetí rovnost z asociativity operace „$\cdot$“. Neutrálním prvkem v pologrupě $(G/H, \star)$ je třída $eH = H$, neboť pro každé $aH \in G/H$ platí

$$aH \star eH = (a \cdot e)H = aH \quad \text{a současně} \quad eH \star aH = (e \cdot a)H = aH.$$

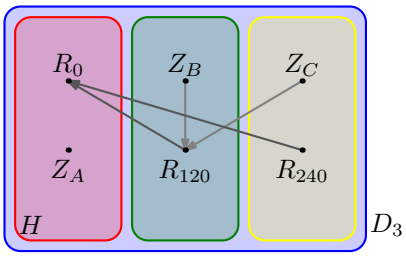
A konečně ukážeme, že inverzní prvek k třídě aH je třída $a^{-1}H$. Pro každé $aH \in G/H$ platí

$$aH \star a^{-1}H = (a \cdot a^{-1})H = eH, \quad a^{-1}H \star aH = (a^{-1} \cdot a)H = eH.$$

Tím jsme ověřili, že operace „$\star$“ na množině všech tříd rozkladu G/H tvoří grupu. □

Poznámka 5.1. Všimněte si, proč požadujeme, aby příslušná podgrupa byla normální. Pro podgrupy, které nejsou normální, uvedená operace „$\star$“ nemusí být operací: pro různé reprezentanty komplexů dostaneme různé výsledky a operace pak není dobře definovaná. Například podgrupa $(\{R_0, Z_A\}, \circ)$ není normální v dihedrální grupě $(D_3, \circ)$ (Obrázek 5.4.). Zatímco složením $R_{120} \circ R_{240}$ dostaneme prvek R_0, tak složením $Z_B \circ Z_C$ dostaneme prvek R_{120} z jiné třídy.

Obyčejné násobení komplexů zpravidla *není* operací na množině komplexů. Pokud však komplexy (třídy rozkladu) vychází z rozkladu grupy podle normální podgrupy, tak operace „$\star$“ bude dobře definovaná.



Obrázek 5.4.: *Pokud podgrupa není normální, operace s třídami rozkladu není dobře definovaná.*

Nyní můžeme vyslovit následující definici.

Definice Faktorová grupa
Mějme grupu $(G,\cdot)$ a její normální podgrupu $(H,\cdot)$. Grupa $(G/H,\star)$ z Věty 5.1. se nazývá *faktorová grupa* grupy $(G,\cdot)$ podle podgrupy $(H,\cdot)$.

Poznámka 5.2. Pokud nebude možná mýlka, tak nebudeme rozlišovat označení operace na grupě $(G,\cdot)$ a její faktorové grupě $(G/H,\star)$. Proto budeme v dalším textu faktorovou grupu $(G/H,\star)$ značit $(G/H,\cdot)$.

Příklad 5.5. Uvedeme několik jednoduchých příkladů faktorových grup.

1) Faktorová grupa $(\mathbb{Z}/\mathbb{S},+)$ je dvouprvková grupa.
2) Faktorová grupa $(\mathbb{Z}/n\mathbb{Z},+)$ je n-prvková grupa, která odpovídá grupě $(\mathbb{Z}_n,+)$. Formálně tuto „podobnost grup“ nazveme isomorfismus, který zavedeme v Kapitole 8.
3) Mějme grupu $(G,\cdot)$. Faktorová grupa $(G/G,\cdot)$ je triviální grupa, její nosič obsahuje jediný prvek, a sice třídu G.
4) Mějme grupu $(G,\cdot)$ s neutrálním prvkem e. Faktorová grupa $(G/\{e\},\cdot)$ je grupa, která odpovídá grupě $(G,\cdot)$. Její prvky jsou však jednoprvkové množiny.
5) V dihedrální grupě $(D_n,\circ)$ je máme normální podgrupu rotací $(R_n,\circ)$ (Příklad 5.3.). Faktorová grupa $(D_n/R_n,\circ)$ má dva prvky, kterými jsou třída rotací R_n a třída zrcadlení.
6) Faktorová grupa $(\mathbb{Q}/\mathbb{Z},+)$ obsahuje nekonečně mnoho nekonečně velkých tříd rozkladu.

Příklad 5.6. Mějme grupu $(G,\cdot)=(\mathbb{Z},+)$. Vezměme její podgrupu $(H,\cdot)=(3\mathbb{Z},+)$ zbytkových tříd modulo 3. Sestavíme faktorovou grupu $(\mathbb{Z}/3\mathbb{Z},+)$, pokud existuje.
Grupa $(3\mathbb{Z},+)$ je podgrupa $(\mathbb{Z},+)$, která je díky komutativitě grupy $(\mathbb{Z},+)$ normální. Proto faktorová grupa $\mathbb{Z}/3\mathbb{Z}$ existuje a její prvky jsou

$$\begin{aligned}0+3\mathbb{Z}&=\{3k:k\in\mathbb{Z}\}=3\mathbb{Z},\\1+3\mathbb{Z}&=\{3k+1:k\in\mathbb{Z}\},\\2+3\mathbb{Z}&=\{3k+2:k\in\mathbb{Z}\}.\end{aligned}$$

Další třídy už jsou identické s některou z uvedených tříd, například $5+3\mathbb{Z}=2+3\mathbb{Z}$, neboť $\{3k+5:k\in\mathbb{Z}\}=$ $=\{3k'+2:k'=k+1\in\mathbb{Z}\}$. Množina $G/H=\mathbb{Z}/3\mathbb{Z}=\{3\mathbb{Z},1+3\mathbb{Z},2+3\mathbb{Z}\}$ tvoří grupu s operací sčítání komplexů.

Sestavíme Cayleyho tabulku 5.1. operace „$\star$“ sčítání faktorů, kterou budeme dle úmluvy značit „$+$“.

$+$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$0+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$
$1+3\mathbb{Z}$	$1+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$
$2+3\mathbb{Z}$	$2+3\mathbb{Z}$	$0+3\mathbb{Z}$	$1+3\mathbb{Z}$

Tabulka 5.1.: *Cayleyho tabulka sčítání faktorů v grupě* $(\mathbb{Z}/3\mathbb{Z},+)$.

Zavedeme označení $\overline{0}=0+3\mathbb{Z}$, $\overline{1}=1+3\mathbb{Z}$, $\overline{2}=2+3\mathbb{Z}$ a Cayleyho tabulka může být jednodušší (Tabulka 5.2.), jedná se o Cayleyho tabulku grupy, která odpovídá grupě $(\mathbb{Z}_3,+)$ sčítání moulo 3. Podrobněji o analogických grupách budeme mluvit v Kapitole 9. ✓

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

Tabulka 5.2.: *Cayleyho tabulka faktorové grupy* $(\mathbb{Z}/3\mathbb{Z},+)$.

Podobně je možno sestavit faktorovou grupu $(\mathbb{Z}/n\mathbb{Z}, \cdot)$, což je ponecháno jako Cvičení 5.1.3.

Otázky:

- Jestliže $(H, \cdot)$ je normální podgrupa grupy $(G, \cdot)$, je faktorová grupa $(G/H, \star)$ komutativní?
- Pokud podgrupa $(H, \cdot)$ není normální v grupě $(G, \cdot)$, proč nemusí být faktorová grupa $(G/H, \star)$ dobře definována?

V Příkladu 5.6. jsme sestavili faktorovou grupu komutativní grupy podle normální podgrupy. Faktorové grupy však můžeme sestavit i z nekomutativní grupy, pokud rozkládáme podle normální podgrupy, jak ukazuje následující příklad.

Příklad 5.7. Sestavíme faktorovou grupu rozkladu grupy $(D_3, \circ)$ podle podgrupy $(\{R_0, R_{120}, R_{240}\}, \circ)$. Sestavíme Cayleyho tabulku operace „$\star$“ na této faktorové grupě.
Pro přehlednost třídy rotací barveně odlišíme od tříd zrcadlení. Dostaneme Tabulku 5.3.

$\circ$	R_0	R_{120}	R_{240}	Z_A	Z_B	Z_C
R_0	R_0	R_{120}	R_{240}	Z_A	Z_B	Z_C
R_{120}	R_{120}	R_{240}	R_0	Z_C	Z_A	Z_B
R_{240}	R_{240}	R_0	R_{120}	Z_B	Z_C	Z_A
Z_A	Z_A	Z_B	Z_C	R_0	R_{120}	R_{240}
Z_B	Z_B	Z_C	Z_A	R_{240}	R_0	R_{120}
Z_C	Z_C	Z_A	Z_B	R_{120}	R_{240}	R_0

Tabulka 5.3.: *Barevně odlišená tabulka skládání symetrií rovnostranného trojúhelníka.*

Třídy rozkladu nyní označíme R a Z stejně jako v Příkladu 4.11.

$$R_0 \circ \{R_0, R_{120}, R_{240}\} = \{R_0, R_{120}, R_{240}\} = R$$
$$Z_A \circ \{R_0, R_{120}, R_{240}\} = \{Z_A, Z_B, Z_C\} = Z$$

Dostaneme $G/\{R_0, R_{120}, R_{240}\} = \{\{R_0, R_{120}, R_{240}\}, \{Z_A, Z_B, Z_C\}\} = \{R, Z\}$. Cayleyho tabulka operace „$\star$“ je Tabulka 5.4., neboť $R \star R = (R_0 R) \star (R_0 R) = (R_0 \circ R_0)R = R_0 \circ R = R$. Zápis výpočtu zjednodušuje využití známých vlastností násobení komplexů.

$\star$	R	Z
R	R	Z
Z	Z	R

Tabulka 5.4.: *Tabulka operace na faktorové grupě.*

Analogicky dostaneme $R \star Z = (R_0 R) \star (Z_A R) = (R_0 \circ Z_A)R = Z_A \circ R = Z$, $Z \star R = (Z_A R) \star (R_0 R) = (Z_A \circ R_0)R = Z_A \circ R = Z$ a konečně $Z \star Z = (Z_A R) \star (Z_A R) = (Z_A \circ Z_A)R = R_0 \circ R = R$. ✓

Faktorové grupy lze použít ke zjišťování informací o původní grupě. Zjednoduší a zpřehlední strukturu, podobně jako Tabulka 5.4. přehledně ukazuje vztah mezi rotacemi a zrcadleními v dihedrální grupě. Můžeme říci: Složení rotace a rotace dá opět rotaci, složení libovolné rotace a zrcadlení dá některé zrcadlení (v libovolném pořadí) a složení dvou libovolných zrcadlení dá rotaci.

Cvičení

5.1.1. Je některá z podgrup ze Cvičení 3.2.5. v grupě určené Tabulkou 2.15. normální? Pokud ano, která?

5.1.2. Ukažte, že centrum $(Z(G), \cdot)$ každé grupy $(G, \cdot)$ je normální podgrupa v $(G, \cdot)$.

5.1.3. Mějme grupu $(\mathbb{Z}, +)$ a její normální podgrupu $(n\mathbb{Z}, +)$ n-násobků celých čísel. Sestavte faktorovou grupu $(\mathbb{Z}/n\mathbb{Z}, +)$.

5.1.4. Mějme podgrupu $(\{1, 6\}, \cdot)$ grupy $(\mathbb{Z}_7 \setminus \{\overline{0}_7\}, \cdot)$ (grupy zbytkových tříd modulo 7 s operací „$\cdot$“ násobení) z Příkladu 4.10. Ukažte, že tato podgrupa je normální a sestavte faktorovou grupu $\left((\mathbb{Z}_7 \setminus \{\overline{0}_7\})/\{\overline{1}_7, \overline{6}_7\}, \cdot\right)$.

5.2. Vlastnosti normálních podgrup

Existuje několik ekvivalentních způsobů, jak poznat, zda je podgrupa v dané grupě normální. Jeden praktický způsob dává následující věta.

Věta 5.2. Test normální podgrupy
Mějme grupu $(G,\cdot)$ a její podgrupu $(H,\cdot)$. Podgrupa $(H,\cdot)$ je normální podgrupa grupy $(G,\cdot)$ právě tehdy, když pro každé $x \in G$ platí $xHx^{-1} \subseteq H$, tzn. právě tehdy, když pro každé $x \in G$ a pro každé $h \in H$ platí $xhx^{-1} \in H$.

Důkaz.
„⇒“ Předpokládejme, že $(H,\cdot)$ je normální podgrupa grupy $(G,\cdot)$. Z definice normální podgrupy platí $xH = Hx$. Jedná se o množinovou rovnost, která zůstane zachována i když každý prvek v množině na levé a na pravé straně vynásobme zprava prvkem x^{-1}. Proto $xHx^{-1} = Hxx^{-1} = He$, což podle Věty 4.2. znamená, že $xHx^{-1} = H$, neboť $e \in H$. Vezmeme-li libovolný prvek $h \in H$ a libovolný prvek $x \in G$ a vynásobíme h zleva prvkem x a zprava prvkem x^{-1}, tak výsledek bude opět (díky rovnosti množin) v H. Tj. pro každé $h \in H$ platí $xhx^{-1} \in H$, což je dokazované tvrzení této implikace.
„⇐“ Předpokládejme, že pro každé $x \in G$ a pro každé $h \in H$ platí $xhx^{-1} \in H$, tj. $xHx^{-1} \subseteq H$. Pro názornost označíme $x = a$, kde $a \in G$, potom platí, že $aHa^{-1} \subseteq H$. Vlevo máme některé prvky množiny H a vpravo všechny, což bude s využitím Věty 4.3. a Cvičení 3.4.4. platit (pro jiné komplexy) i po vynásobení zprava jednoprvkovým komplexem $\{a\}$. Takže pro každý prvek $a \in G$ platí $aHa^{-1}a \subseteq Ha$. Platí $aHa^{-1}a = He$, a protože podle Věty 4.2. je $He = H$, tak dostáváme $aHe = aH$, $aH \subseteq Ha$. (Jeden součin komplexů je podmnožinou druhého.)

Podobně zvolme $x = a^{-1}$, kde $a \in G$, potom platí, že $a^{-1}H(a^{-1})^{-1} \subseteq H$ tj. $a^{-1}Ha \subseteq H$. Vlevo máme některé prvky a vpravo všechny, což bude platit (pro jiné komplexy) i po vynásobení zleva prvkem a. Takže pro každý prvek $a \in G$ platí $aa^{-1}Ha \subseteq aH$. Dle Věty 4.2. je $eH = H$, proto platí $Ha \subseteq aH$.

Celkem dostáváme $Ha \subseteq aH$ a $aH \subseteq aH$ a proto $aH = Ha$, což znamená, že $(H,\cdot)$ je normální podgrupa v $(G,\cdot)$. □

Příklad 5.8. Ukážeme, že grupa regulárních diagonálních $(D^*_{n,n},\cdot)$ matic není normální podgrupou grupy regulárních čtvercových matic řádu n s operací násobení matic $(M^*_{n,n},\cdot)$.
Najdeme příklady matic $A \in M^*_{n,n}$ a $D \in D^*_{n,n}$, takových, že $ADA^{-1} \notin D^*_{n,n}$. Označme

$$D = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix}$$

Potom platí

$$ADA^{-1} = \begin{pmatrix} 1 & 2 \\ 3 & 5 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \begin{pmatrix} -5 & 2 \\ 3 & -1 \end{pmatrix} = \begin{pmatrix} 7 & -2 \\ 15 & -4 \end{pmatrix}.$$

Výsledná matice evidentně není diagonální, proto $ADA^{-1} \notin D^*_{n,n}$, a podle Věty 5.2. není podgrupa $(D^*_{n,n},\cdot)$ normální podgrupou v grupě $(M^*_{n,n},\cdot)$. ✓

Poznámka 5.3. Jestliže je z kontextu zřejmé, v jaké grupě se pohybujeme, budeme stručně říkat, že podgrupa $(H,\cdot)$ je normální.

Podle Věty 3.2. je průnik podgrup opět podgrupou. Analogické tvrzení platí i pro průnik normálních podgrup.

Věta 5.3. *Mějme normální podgrupy $(H_1,\cdot)$ a $(H_2,\cdot)$ grupy $(G,\cdot)$. Potom také $(H_1 \cap H_2,\cdot)$ je normální podgrupa grupy $(G,\cdot)$.*

Důkaz. Protože $(H_1,\cdot)$ a $(H_2,\cdot)$ jsou podgrupy grupy $(G,\cdot)$, proto podle Věty 3.2. je také $(H_1 \cap H_2,\cdot)$ podgrupa grupy $(G,\cdot)$. Zbývá ukázat, že $(H_1 \cap H_2,\cdot)$ je také normální podgrupa grupy $(G,\cdot)$.

Využijme předchozí Větu 5.2. Protože $(H_1,\cdot)$ je normální podgrupa grupy $(G,\cdot)$, tak pro každé $x \in G$ a pro každé $h \in H_1$ platí $xhx^{-1} \in H_1$. Analogicky, protože $(H_2,\cdot)$ je normální podgrupa grupy $(G,\cdot)$, tak pro každé $x \in G$ a pro každé $h \in H_2$ platí $xhx^{-1} \in H_2$.

Bez újmy na obecnosti můžeme předpokládat, že h je stejný prvek v H_1 i H_2, tedy pro $h \in H_1 \cap H_2$.

$$h \in H_1 \cap H_2 : (xhx^{-1} \in H_1) \wedge (xhx^{-1} \in H_2)$$

To ale znamená, že $xhx^{-1} \in (H_1 \cap H_2)$ a podle Věty 5.2. je $(H,\cdot)$ normální podgrupa v $(G,\cdot)$. □

Všimněte si, že každá (netriviální) grupa má alespoň dvě normální podgrupy. Kromě triviální podgrupy je i nevlastní podgrupa vždy normální (Cvičení 5.2.4.).

Cvičení

5.2.1. Ukažte, že grupa regulárních čtvercových matic s determinantem 1 je normální podgrupou grupy regulárních čtvercových matic řádu n s operací násobení matic $(M^*_{n,n}, \cdot)$.

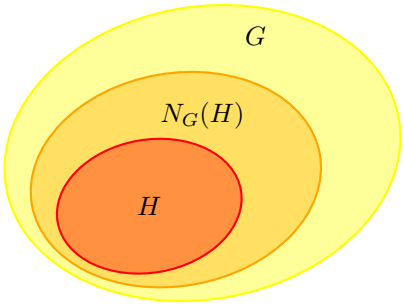
5.2.2. Mějme libovolné přirozené číslo k. Ukažte že grupa regulárních čtvercových matic s determinantem, který je roven nějaké celočíselné mocnině k je normální podgrupou grupy regulárních čtvercových matic řádu n s operací násobení matic $(M^*_{n,n}, \cdot)$.

5.2.3. Vezměme dihedrální grupu $(D_6, \circ)$ a její podgrupu vybraných rotací $(\{R_0, R_{120}, R_{240}\}, \circ)$. Ukažte, že se jedná o normální podgrupu.

5.2.4. Mějme grupu $(G, \cdot)$. Ukažte, že pro každé $g \in G$ platí $gG = G = Gg$, tj. nevlastní podgrupa je normální podgrupou.

5.3. Normalizátor

I když není $(H, \cdot)$ normální podgrupou grupy $(G, \cdot)$, tak má smysl najít v grupě $(G, \cdot)$ podgrupu $(N_G(H), \cdot)$, jejíž nosič $N_G(H)$ obsahuje H a přitom podgrupa $(H, \cdot)$ je navíc normální v podgrupě $(N_G(H), \cdot)$ (Obrázek 5.5.). Takové množině budeme říkat normalizátor podgrupy H.



Obrázek 5.5.: *Podgrupa $(H, \cdot)$ a její normalizátor $N_G(H)$ v grupě $(G, \cdot)$.*

Definice Mějme podgrupu $(H, \cdot)$ grupy $(G, \cdot)$. *Normalizátorem podgrupy $(H, \cdot)$ v grupě $(G, \cdot)$* nazveme podgrupu $(N_G(H), \cdot)$, kde $N_G(H) = \{x \in G : xH = Hx\}$.

Nejprve ověříme korektnost definice, tj. že $(N_G(H), \cdot)$ opravdu je podgrupa v $(G, \cdot)$. Jistě platí, že $N_G(H) \subseteq G$ a dále je určitě množina $N_G(H)$ neprázdná, protože $He = eH$ a tedy $e \in N_G(H)$. Abychom ukázali, že normalizátor $(N_G(H), \cdot)$ je podgrupou v $(G, \cdot)$, tak podle Věty 3.3. stačí ověřit uzavřenost operace „$\cdot$“ a existenci inverzního prvku.

Uzavřenost zdůvodníme přímo. Pro každé $a, b \in N_G(H)$ platí $aH = Ha$ a současně $bH = Hb$. Nyní s využitím Věty 3.7., která říká, že násobení komplexů je asociativní, dostaneme $(ab)H = a(bH) = a(Hb) = = (aH)b = (Ha)b = H(ab)$.

A konečně ke každému prvku a existuje v $(G, \cdot)$ inverzní prvek a^{-1}. Navíc pro každé $a \in N_G(H)$ platí $aH = Ha$, takže vynásobením komplexem $\{a^{-1}\}$ zprava dostaneme s využitím Cvičení 3.4.4. $aHa^{-1} = = Haa^{-1} = He = H$. A podobně vynásobením komplexem $\{a^{-1}\}$ zleva dostaneme $Ha^{-1} = a^{-1}H$, což znamená, že $a^{-1} \in N_G(H)$.

Ukázali jsme, že normalizátor spolu s restrikcí operace $(N_G(H), \cdot)$ je podgrupa v $(G, \cdot)$ a definice je korektní. Ještě bychom měli prověřit, zda Obrázek 5.5. není zavádějící a zda opravdu platí $H \subseteq N_G(H) \subseteq G$. Důkaz první inkluze je ponechán jako Cvičení 5.3.2. Druhá inkluze plyne ihned z definice normalizátoru $N_G(H)$.

Příklad 5.9. Uvedeme několik jednoduchých příkladů normalizátorů podgrup.

1) V komutativní grupě $(G, \cdot)$ je každá podgrupa $(H, \cdot)$ normální podgrupou a normalizátorem takové podgrupy je vždy celá grupa $N_G(H) = G$.
2) Nevlastní podgrupa grupy $(G, \cdot)$ je normální a je svým vlastním normalizátorem.
3) Každá podgrupa $(H, \cdot)$ grupy $(G, \cdot)$ má normalizátor $(N_G(H), \cdot)$ (Věta 5.4.) a navíc platí $H \subseteq N_G(H)$ (Cvičení 5.3.2.).

Je důležité si uvědomit, že každá podgrupa má jednoznačně určený normalizátor.

Věta 5.4. *Pro libovolnou podgrupu $(H,\cdot)$ grupy $(G,\cdot)$ existuje právě jeden normalizátor $(N_G(H),\cdot)$.*

Důkaz. Abychom ověřili existenci, stačí si uvědomit, že $H \subseteq N_G(H)$, neboť z uzavřenosti operace na množině H pro každé $h \in H$ platí $hH = Hh$. Jednoznačnost plyne přímo z definice, neboť do $N_G(H)$ zařadíme všechny prvky $x \in G$, které splňují rovnost $xH = Hx$. □

Otázky:

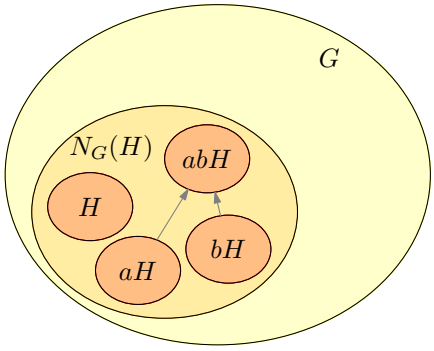
- Mohou dvě různé podgrupy $(H_1,\cdot)$ a $(H_2,\cdot)$ grupy $(G,\cdot)$ mít stejný normalizátor?
- Může mít podgrupa $(H,\cdot)$ grupy $(G,\cdot)$ dva různé normalizátory?

Je dobré připomenout, že libovolná podgrupa $(H,\cdot)$ grupy $(G,\cdot)$ (i taková, která není normální!) je normální podgrupou svého normalizátoru $(N_G(H),\cdot)$. Právě tak byl pojem normalizátoru definován.

Věta 5.5. *Mějme normalizátor $(N_G(H),\cdot)$ podgrupy $(H,\cdot)$ v grupě $(G,\cdot)$. Potom $(H,\cdot)$ je normální podgrupa grupy $(N_G(H),\cdot)$.*

Důkaz. Nejprve si všimneme, že $H \subseteq N_G(H)$, protože pro každé $h \in H$ platí $hH = Hh$ a tedy $h \in N_G(H)$. Dále $(H,\cdot)$ je neprázdná podgrupa v $(G,\cdot)$, a protože $H \subseteq N_G(H)$, tak $(H,\cdot)$ je současně podgrupou v $(N_G(H),\cdot)$. Zbývá ukázat, že $(H,\cdot)$ je normální podgrupa v $(N_G(H),\cdot)$. Avšak podle definice normalizátoru pro všechna $n \in N_G(H)$ platí $nH = Hn$, takže $(H,\cdot)$ je normální podgrupa v $(N_G(H),\cdot)$. □

Z předchozí věty plyne, že v libovolné grupě $(G,\cdot)$ můžeme pro libovolnou podgrupu sestavit *nějakou* faktorovou grupu, avšak ne nutně faktorovou grupu grupy $(G,\cdot)$.



Obrázek 5.6.: *Faktorová grupa* $\left(N_G(H)/H,\cdot\right)$.

Důsledek 5.6. *Mějme grupu $(G,\cdot)$ a její podgrupu $(H,\cdot)$. Potom platí $(N_G(H)/H,\cdot)$ je grupa.*

Důkaz. Podle definice normalizátoru $(N_G(H),\cdot)$ je $(N_G(H),\cdot)$ grupou a podle Věty 5.5. je $(H,\cdot)$ je normální podgrupa grupy $(N_G(H),\cdot)$. A konečně podle Věty 5.1. je $(N_G(H)/H,\cdot)$ grupa. □

Jestliže sestavíme normalizátor pro nějakou normální podgrupu $(H,\cdot)$ grupy $(G,\cdot)$, tak tento normalizátor bude samozřejmě totožný s celou grupou $(G,\cdot)$.

Věta 5.7. *Mějme normalizátor $(N_G(H),\cdot)$ podgrupy $(H,\cdot)$ v grupě $(G,\cdot)$. Jestliže $(H,\cdot)$ je normální podgrupa grupy $(G,\cdot)$, tak $N_G(H) = G$.*

Důkaz je ponechán jako Cvičení 5.3.1.

Otázky:

- Mějme grupu $(G,\cdot)$ a její podgrupu $(H,\cdot)$. Je $(H,\cdot)$ normální podgrupou normalizátoru $(N_G(H),\cdot)$?
- Mějme grupu $(G,\cdot)$ a její podgrupu $(H,\cdot)$. Je normalizátor $(N_G(H),\cdot)$ normální podgrupou v $(G,\cdot)$?

Příklad 5.10. Navážeme na Příklad 4.19. na straně 87. Najdeme normalizátory a) podgrupy $(\{R_0\},\circ)$, b) podgrupy $(\{R_0,Z_A\},\circ)$, c) podgrupy $(\{R_0,R_{120},R_{240)}\},\circ)$ a d) nevlastní podgrupy $(D_3,\circ)$ dihedrální grupy $(D_3,\circ)$.
a) Podgrupa $(\{R_0\},\circ)$ je normální, neboť obsahuje pouze neutrální prvek R_0 a pro každý prvek $g \in \{R_0,R_{120},R_{240},Z_A,Z_B,Z_C\}$ platí $gH_1 = H_1g$, protože $\{g\}\circ R_0 = R_0 \circ \{g\}$. Normalizátor této podgrupy je celé $(D_3,\circ)$, tedy platí $N_{D_3}(\{R_0\}) = D_3$.

b) Označme $H_2 = \{R_0, Z_A\}$. Podle Příkladu 5.4. víme, že podgrupa $(H_2, \circ)$ není normální v $(D_3, \circ)$. Protože index podgrupy $(D_3 : H_2) = 3$ je prvočíslo, tak podle Cvičení 4.3.1. je normalizátor $N_{D_3}(H_2)$ je buď H_2 nebo celé D_3. V druhém případě by však podgrupa $(H_2, \cdot)$ musela být v $(D_3, \circ)$ normální, což není. Proto $N_{D_3}(H_2) = H_2$.
c) Označme $H_5 = \{R_0, R_{120}, R_{240}\}$. Podle Příkladu 5.3. víme, že podgrupa $(H_5, \circ)$ je normální. Proto $N_{D_3}(H_5) = D_3$. Můžeme sestavit faktorovou grupu (Příklad 5.7.).
d) Podle Cvičení 5.2.4. je grupa normální podgrupou sama v sobě. Všimněte si, že příslušná faktorová grupa je triviální, má jediný prvek $G/H_6 = \{\{R_0, R_{120}, R_{240}, Z_A, Z_C, Z_B, \}\}$. ✓

Normalizátory zbývajících dvou podgrup dihedrální grupy $(D_3, \circ)$ odpovídají samotným podgrupám, neboť tyto podgrupy nejsou normální (Cvičení 5.3.3.) a zdůvodnění je stejné jako v části b) Příkladu 5.10. Vidíme, že ani jedna z podgrup řádu 2 v dihedrální grupě $(D_3, \circ)$ není normální. Každá je svým vlastním normalizátorem a proto triviálně je normální podgrupou svého normalizátoru. Naproti tomu tento normalizátor není normální podgrupou grupy $(D_3, \circ)$.

Cvičení

5.3.1.$^{\heartsuit}$ *Dokažte Větu 5.7., tj. je-li $(N_G(H), \cdot)$ je normalizátor podgrupy $(H, \cdot)$ v grupě $(G, \cdot)$ a $(H, \cdot)$ je normální podgrupa grupy $(G, \cdot)$, tak $N_G(H) = G$.*

5.3.2.$^{\heartsuit}$ *Mějme grupu $(G, \cdot)$, její podgrupu $(H, \cdot)$ a normalizátor $(N_G(H), \cdot)$. Ukažte, že $H \subseteq N_G(H)$.*

5.3.3. Mějme dihedrální grupu symetrií trojúhelníka $(D_3, \circ)$. Ukažte, že její podgrupy a) $(\{R_0, Z_B\}, \circ)$, ani b) $(\{R_0, Z_C\}, \circ)$ nejsou normální. Nejděte normalizátory obou podgrup.

5.3.4. Najděte takový příklad grupy $(G, \cdot)$ a její podgrupy $(H, \cdot)$, že podgrupa $(H, \cdot)$ není normální v $(G, \cdot)$ a normalizátor $(N_G(H), \cdot)$ je různý od $(H, \cdot)$ a současně různý od $(G, \cdot)$.*

5.3.5. Dokažte nebo vyvraťte: Jestliže $(H_1, \cdot)$, $(H_2, \cdot)$, kde $H_1 \subseteq H_2$, jsou podgrupy v $(G, \cdot)$, tak $N_G(H_1) \subseteq N_G(H_2)$.

5.3.6. Dokažte nebo vyvraťte: Jestliže $(H_1, \cdot)$, $(H_2, \cdot)$, kde $H_1 \subseteq H_2$, jsou podgrupy v $(G, \cdot)$, tak $N_G(H_1) \supseteq N_G(H_2)$.

5.3.7. Najděte příklad grupy $(G, \cdot)$ a její podgrupy $(H, \cdot)$, ve které platí $(Z(G), \cdot) \neq (N_G(H), \cdot)$.

Kapitola 6. Cyklické grupy

Cyklické grupy můžeme získat z jediného prvku libovolné dané grupy. Umocňováním, respektive opakovaným sčítáním zvoleného prvku získáme nosnou množinu takové cyklické grupy, která pochopitelně bude podgrupou dané grupy, jako jsme ukázali v Příkladu 4.17. Později, v Kapitole 9., ukážeme, že až na izomorfismus existuje pro každý konečný řád jediná cyklická grupa a že existuje také jediná nekonečná cyklická grupa.

6.1. K symbolice mocnin a násobků

Nejprve zobecníme značení zavedené dříve. Na straně 56 jsme zavedli značení pro operace součtu či součinu n kopií prvku a v dané grupě, kde n je přirozené číslo. Nyní tuto definici rozšíříme. Zavedeme označení násobků a mocnin s koeficientem n, kde n je celé číslo (kladné, záporné i nulové).

Definice Značení opakované operace s inverzními prvky
Mějme grupu $(A, \cdot)$ a prvek $a \in A$. Jestliže operaci „$\cdot$“ chápeme jako aditivní operaci „$+$“, tak „součet“ n kopií prvku $-a$ (prvku opačného prvku k a) zapíšeme

$$\underbrace{-a + (-a) + \cdots + (-a)}_{n} = -(na) = -na,$$

přičemž $-1a = -a$. Připomeňme, že $0a = e$, kde e je neutrální prvek grupy, nebo $0a = 0$, kde 0 značí nulový prvek (neutrální prvek vzhledem k aditivní operaci „$\cdot$“).

Jestliže operaci „$\cdot$“ chápeme jako multiplikativní operaci „$\cdot$“, tak „součin“ n kopií prvku a^{-1} (prvku inverzního prvku k a) zapíšeme

$$\underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{n} = (a^n)^{-1} = a^{-n}.$$

Připomeňme, že $a^0 = e$, kde e je neutrální prvek grupy, nebo $a^0 = 1$, kde 1 značí jedničku (neutrální prvek vzhledem multiplikativní k operaci „$\cdot$“).

Poznámka 6.1. Korektnost zápisu opakované operace s inverzními prvky
Všimněte si rozdílu mezi právě zavedenou definicí a definicí na straně 56. Podle dříve zavedené definice platí

$$\underbrace{-a + (-a) + \cdots + (-a)}_{n} = n(-a).$$

Nyní říkáme, že navíc $n(-a) = -na = -(na)$, respektive že $\left(a^{-1}\right)^n = (a^n)^{-1} = a^{-1}$ v multiplikativní notaci. Je dobré zdůraznit, že zatímco a je nějaký prvek dané grupy a $-a$ je prvek k němu opačný, tak n a $-n$ jsou celá čísla. Platnost rovností $n(-a) = -(na)$ nemusí být zřejmá, proto její platnost dokážeme. Platí

$$n(-a)+(na) = \underbrace{-a + (-a) + \cdots + (-a)}_{n} + \underbrace{a + a + \cdots + a}_{n} = \underbrace{-a + (-a) + \cdots + (-a)}_{n-1} + e + \underbrace{a + a + \cdots + a}_{n-1} = e,$$

přičemž v poslední rovnosti opakovaně využijeme, že platí $-a + a = e$. Rovnost $(na) + n(-a) = e$ se ukáže zcela analogicky, a proto prvek $n(-a)$ je opačný k prvku (na) a tedy platí $n(-a) = -(na)$. Zbývá označit $-(na) = -na$ (opačný prvek označíme záporným číslem) a korektnost definice je dokázána.

Důkaz rovnosti $\left(a^{-1}\right)^n = (a^n)^{-1}$ pro multiplikativní notaci je ponechán jako Cvičení 6.1.1. Stačí už jen označit $(a^n)^{-1} = a^{-n}$ (inverzní prvek označíme zápornou mocninou) a důkaz, že nově zavedená definice je korektní a je v souladu s definicí ze strany 56 je kompletní.

Při zápisu obecné operace „$\cdot$“ i nadále preferujeme multiplikativní označení a terminologii. Všimněte si, že zavedená symbolika odpovídá obvyklým vztahům v aritmetice. Pro multiplikativní operaci „$\cdot$“ platí například následující vztahy (Příklad 6.1. a Cvičení 6.1.3.).

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

Uvědomte si, že zatímco operace „$\cdot$“ odpovídá operaci v nějaké grupě $(A, \cdot)$, tak znaménko operace „$+$“ nebo (vynechané) znaménko „$\cdot$“ v exponentu odpovídá klasickému sčítání a násobení celých čísel.

Podobně, pro aditivní operaci „+“ platí podobné vztahy (Cvičení 6.1.2.).

$$na + ma = (m+n)a, \qquad na - ma = (n-m)a, \qquad -m(na) = (-mn)a = n(-ma)$$

Dále si všimněte, že symboly 0 a 1 použité v rovnostech $0a = 0$ a $a^0 = 1$ mají jiný význam na levé a jiný význam na pravé straně rovnosti. Na levé straně se jedná o celá čísla, zatímco na pravé straně o zápis neutrálního prvku příslušné grupy.

Příklad 6.1. Ukážeme, že v grupě $(A, \cdot)$ s operací „$\cdot$“ (analogie operace součinu) platí vztah $a^n \cdot a^{-m} = a^{n-m}$.

Podle značení zavedeného na straně 58 a výše zavedeného značení pro inverzní prvky můžeme pro $n \geq m$ psát

$$a^n \cdot a^{-m} = \underbrace{a \cdot a \cdots a}_{n} \cdot \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{m} = \underbrace{a \cdot a \cdots a}_{n-m} = a^{n-m},$$

protože $a \cdot a \cdot a^{-1} = a \cdot e = a$. Podobně, pro $n < m$ můžeme psát

$$a^n \cdot a^{-m} = \underbrace{a \cdot a \cdots a}_{n} \cdot \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{m} = \underbrace{a^{-1} \cdot a^{-1} \cdots a^{-1}}_{m-n} = (a^{-1})^{m-n} = a^{n-m},$$

s využitím $a \cdot a^{-1} \cdot a^{-1} = e \cdot a^{-1} = a^{-1}$. Další vztahy se ukáží podobně. ✓

Na druhou stranu je dobré zdůraznit, že následující vztahy nebo značení běžné používané při práci s reálnými čísly *nejsou* či *nemusí* být pro prvky obecné grupy definovány a proto ani *nemusí mít smysl*.

$$a^{-n} = \frac{1}{a^n}, \qquad a^{\frac{3}{2}}, \qquad \sqrt{a}$$

Další negativní příklad známe z lineární algebry: můžeme sice násobit maticí inverzí (pokud existuje), avšak maticemi nebudeme dělit. Je-li A regulárním matice řádu n, pak existuje $inv(A) = A^{-1}$, ale obecně nemá smysl sestavovat zlomky

$$A^{-1} = \frac{1}{A},$$

pokud jsme zlomky s maticemi nebo operaci dělení matic (zlomky s maticemi) nijak nedefinovali.

Cvičení

6.1.1. Dokažte, že platí vztah $\left(a^{-1}\right)^n = (a^n)^{-1}$.

6.1.2. Ukažte, že pro aditivní operaci „+“ platí vztahy a) $na - ma = (n-m)a$, *b)* $-m(na) = (-mn)a = n(-ma)$.

6.1.3. Ukažte, že pro multiplikativní operaci „$\cdot$“ platí vztah $(a^{-n})^m = a^{-mn} = (a^m)^{-n}$.

6.2. Definice cyklické grupy

Připomeňme, že na straně 83 jsme zavedli řád grupy $(G, \cdot)$, který udává počet prvků nosné množiny G. Řád grupy značíme $|G|$. Dále připomeňme, že řád prvku a v grupě $(G, \cdot)$ jsme zavedli na straně 85 jako nejmenší přirozené číslo n takové, že $a^n = e$, kde e je neutrální prvek grupy $(G, \cdot)$. Řád prvku a značíme $|a|$. Jestliže takové přirozené číslo n neexistuje, tak říkáme, že a je nekonečného řádu.

V Příkladu 4.17. a také při studiu dihedrální grupy jsme využili, že máme-li grupu $(G, \cdot)$ s prvkem a řádu n v grupě $(G, \cdot)$, tak množina

$$A = \{e, a, a^2, \ldots, a^{n-1}\} = \{a, a^2, \ldots, a^{n-1}, a^n = e\},$$

tvoří spolu s restrikcí operace „$\cdot$“ na množinu A podgrupu grupy $(G, \cdot)$. Toto pozorování vede k následující definici.

Definice Cyklická grupa

Mějme grupu $(G, \cdot)$ a nějaký prvek $a \in G$. Označme množinu $A = \{a^n : n \in \mathbb{Z}\}$. Množina A spolu s restrikcí operace „$\cdot$“ na množinu A tvoří grupu, které budeme říkat *cyklická grupa* a budeme ji značit $(\langle a \rangle, \cdot)$ nebo jen $\langle a \rangle$. Prvek a je *generátorem* grupy $\langle a \rangle$.

V Příkladu 4.17. jsme ukázali, že definice je korektní, tj. že $\langle a \rangle$ je opravdu grupa. Podívejme se na vlastnosti této grupy. Ihned z definice je zřejmé, že $e \in A$, protože $a^0 = e$, a proto množina A je neprázdná a obsahuje neutrální prvek grupy $(G, \cdot)$ vzhledem k operaci „$\cdot$“. Dále operace „$\cdot$“ je na množině A uzavřená, neboť pro libovolná celá čísla m, n platí $a^m \cdot a^n = a^{m+n}$, jak jsme ukázali na straně 57. Asociativita operace „$\cdot$“ plyne z toho, že se jedná o restrikci asociativní operace (Cvičení 0.6.6.). A konečně inverzním prvkem k libovolnému prvku $a^n \in A$ je prvek $a^{-n} = (-a)^n$ který do A podle definice množiny A také patří.

Dále upozorníme, že generátor a grupy $\langle a \rangle$ nemusí být určen jednoznačně. Stejná grupa $\langle a \rangle$ může mít více různých generátorů.

Příklad 6.2. Uveďme několik jednoduchých grup, které jsou cyklické.

1) Množina přirozených čísel $1, 2, \ldots, n$ (reprezentantů zbytkových tříd) s operací sčítání modulo n $(\mathbb{Z}_n, +)$ je konečná cyklická grupa generovaná prvkem 1.
2) Množina celých čísel s operací obyčejného sčítání $(\mathbb{Z}, +)$ je nekonečná cyklická grupa generovaná prvkem 1 (Příklad 6.6.).
3) Množina sudých čísel s operací obyčejného sčítání $(\mathbb{S}, +)$ je nekonečná cyklická grupa generovaná prvkem 2.
4) Množina k-násobků čísel s operací obyčejného sčítání je nekonečná cyklická grupa generovaná prvkem k. Značíme ji $(k\mathbb{Z}, +)$.
5) Triviální grupa (s jednoprvkovým nosičem) je cyklická. Grupa generovaná neutrálním prvkem je vždy triviální cyklická grupa.
6) Množina M všech celočíselných mocnin čísla 2 s operací obyčejného násobení tvoří nekonečnou cyklickou grupu $(M, \cdot)$ generovanou prvkem 2.
7) Množina n-tých odmocnin čísla 1 v grupě nenulových komplexních čísel s operací obvyklého násobení komplexních čísel tvoří konečnou cyklickou grupu řádu n v nekonečné grupě $(\mathbb{C} \setminus \{0\}, \cdot)$ generovanou prvkem $\sqrt[n]{1} = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$.

Příklad 6.3. Uveďme také několik příkladů grup, které nejsou cyklické.

1) Dihedrální grupa všech symetrií pravidelného n-úhelníka s operací skládání zobrazení $(D_n, \circ)$ není cyklická grupa, protože neobsahuje prvek řádu $2n$.
2) Grupa jednotek $(U(15), \cdot)$ z Příkladu 4.16. není cyklická, protože nemá prvek řádu 8. Každý prvek grupy $(U(15), \cdot)$ je generátorem cyklické podgrupy, avšak tyto podgrupy mají nejvýše čtyři prvky.
3) Grupa racionálních čísel s operací obyčejného sčítání $(\mathbb{Q}, +)$ není cyklická grupa, protože neexistuje takové racionální číslo, které by bylo generátorem (Cvičení 6.2.8.).
4) Grupa reálných čísel s operací obyčejného sčítání $(\mathbb{R}, +)$ není cyklická grupa, protože neexistuje takové reálné číslo, které by bylo generátorem (Cvičení 6.2.9.).
5) Množina vektorů v $\mathbb{R}^2$ spolu s operací sčítání vektorů není cyklická grupa, protože neexistuje takový (jediný) vektor, který by byl generátorem celé grupy $(\mathbb{R}^2, +)$.
6) Grupa regulárních čtvercových matic $(M^*_{n,n}, \cdot)$ s operací násobení matic není cyklická grupa, protože neexistuje taková regulární matice, která by byla generátorem celé grupy $(M^*_{n,n}, \cdot)$.

Ukážeme, že cyklické podgrupy mají řadu pěkných vlastností, v jistém smyslu až příliš pěkných. Všechny cyklické podgrupy mají velmi jednoduchou strukturu. V Kapitole 9. ukážeme, že rozlišíme jen konečné a nekonečné cyklické grupy (až na izomorfismus, který zavedeme právě v Kapitole 9.). Na druhou stranu cyklické grupy lze použít jako základní kameny při výstavbě obrovské třídy grup, podobně jako prvočísla jsou základními stavebními kameny při zkoumání přirozených (nebo celých čísel).

Příklad 6.4. V dihedrální grupě $(D_3, \circ)$ určete cyklické podgrupy $\langle R_0 \rangle$, $\langle R_{120} \rangle$, $\langle R_{240} \rangle$, $\langle Z_A \rangle$, $\langle Z_B \rangle$ a $\langle Z_C \rangle$.
Cayleyho tabulka grupy $(D_3, \circ)$ je na straně 35.
Z Tabulky 1.3. snadno určíme mocniny všech prvků. Dostaneme Tabulku 6.1. Z Tabulky 6.1. snadno určíme, že $\langle R_0 \rangle = (\{R_0\}, \cdot)$, $\langle R_{120} \rangle = \langle R_{240} \rangle = (\{R_0, R_{120}, R_{240}\}, \cdot)$, $\langle Z_A \rangle = (\{R_0, Z_A\}, \cdot)$, $\langle Z_B \rangle = (\{R_0, Z_B\}, \cdot)$, $\langle Z_C \rangle = (\{R_0, Z_C\}, \cdot)$.

Řády prvků jsou $|R_0| = 1$, $|R_{120}| = |R_{240}| = 3$, $|Z_A| = |Z_B| = |Z_C| = 2$. Všimněte si, že řády prvků dělí řád grupy, což odpovídá tvrzení Lagrangeovy věty (Věty 4.10.). Sestavili jsme šest cyklických podgrup, avšak ani jeden z prvků není řádu 6. To znamená, že samotná $(D_3, \circ)$ *není* cyklická grupa, neboť $(D_3, \circ)$ není generována žádným svým prvkem. ✓

Příklad 6.5. Mějme grupu $(\mathbb{Z}_6, +)$ (sčítání modulo 6). Určete podgrupy generované jednotlivými prvky.

x	x^2	x^3	x^4	x^5	x^6
R_0	R_0	R_0	R_0	R_0	R_0
R_{120}	R_{240}	R_0	R_{120}	R_{240}	R_0
R_{240}	R_{120}	R_0	R_{240}	R_{120}	R_0
Z_A	R_0	Z_A	R_0	Z_A	R_0
Z_B	R_0	Z_B	R_0	Z_B	R_0
Z_C	R_0	Z_C	R_0	Z_C	R_0

Tabulka 6.1.: *Tabulka mocnin prvků grupy* $(D_3, \circ)$.

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

Tabulka 6.2.: *Cayleyho tabulka sčítání „modulo 6“ s čísly 0 až 5.*

a	$2a$	$3a$	$4a$	$5a$	$6a$
0	0	0	0	0	0
1	2	3	4	5	0
2	4	0	2	4	0
3	0	3	0	3	0
4	2	0	4	2	0
5	4	3	2	1	0

Tabulka 6.3.: *Tabulka násobků prvků grupy* $(\mathbb{Z}_6, +)$.

Z Tabulky 6.2. přečteme násobky jednotlivých prvků. Násobky odpovídají mocninám v multiplikativní notaci. Jsou uvedeny v Tabulce 6.3.

Nyní snadno určíme, že $\langle 0\rangle = (\{0\}, +)$, $\langle 1\rangle = \langle 5\rangle = (\{0,1,2,3,4,5\}, +)$, $\langle 2\rangle = \langle 4\rangle = (\{0,2,4\}, +)$ a $\langle 3\rangle = (\{0,3\}, +)$.

Všimněte si, že $|0| = 1$, $|1| = |5| = 6$, $|2| = |4| = 3$ a $|3| = 2$. Jedná se o grupu, která je cyklická a má čtyři různé cyklické podgrupy. ✓

Předchozí příklady ilustrují Definici 6.2., podle které každý prvek a nějaké konečné grupy $(G, \cdot)$ je generátorem cyklické podgrupy. Zkonstruovat cyklickou podgrupu je snadné, stačí vzít restrikci operace „$\cdot$“ na podmnožinu $\{a = a^1, a^2, \ldots, a^n\}$, respektive restrikci operace „$+$“ na podmnožinu $\{a = a, 2a, \ldots, na\}$ v aditivní notaci, kde n je řád prvku a. Následující příklad ukazuje, že analogicky lze postupovat i pro nekonečné grupy, kde řád prvku může být nekonečný.

Příklad 6.6. Určete $\langle 1\rangle$, kde za operaci vezmete obvyklé sčítání reálných čísel.
Podle Definice 6.2. ihned dostáváme, že $\langle 1\rangle = (\{n1 : n \in \mathbb{Z}\}, +) = (\mathbb{Z}, +)$. Vidíme, že grupa $(\mathbb{Z}, +)$ je cyklická grupa s generátorem 1. ✓

Obecný průnik a sjednocení grup

Podle Věty 3.1. víme, že všechny podgrupy téže grupy mají společný neutrální prvek. Dále podle Věty 3.2. víme, že průnik dvou podgrup grupy $(G, \cdot)$ je opět podgrupou v $(G, \cdot)$. Není těžké ukázat, že platí i následující silnější tvrzení.

Lemma 6.1. Průnik podgrup je opět podgrupa
Mějme grupu $(G, \cdot)$ a její podgrupy $(H_i, \cdot)$, kde $i \in J$. Platí, že $(\bigcap_{i\in J} H_i, \cdot)$ je opět podgrupa v grupě $(G, \cdot)$.

Důkaz je ponechán jako Cvičení 6.2.1. Všimněte si, že zápis $\bigcap_{i\in J} H_i$ připouští průnik nekonečného počtu podgrup.

Otázka: Čemu je roven průnik $\bigcap_{i\in\mathbb{N}} i\mathbb{Z}$?

Máme-li grupu $(G, \cdot)$, tak pochopitelně ne každá podmnožina M nosné množiny G tvoří spolu s restrikcí operace „$\cdot$“ podgrupu grupy $(G, \cdot)$. Následující definice elegantně zavádí co možná nejmenší podgrupu dané grupy tak, aby zvolenou podmnožinu M obsahovala.

Definice Podgrupa generovaná množinou
Mějme grupu $(G,\cdot)$ a libovolnou podmnožinu $M \subseteq G$. Symbolem $\langle M\rangle$ označíme průnik všech podgrup v grupě $(G,\cdot)$, které obsahují množinu M. Říkáme mu *podgrupa generovaná množinou* M a značíme jej $(\langle M\rangle,\cdot)$, případně jen $\langle M\rangle$.

Podle Lemmatu 6.1. je definice korektní, neboť $(\langle M\rangle,\cdot)$ je podgrupa v $(G,\cdot)$. Uvědomte si také, že definice nevylučuje případ $M=\emptyset$. Platí $\langle\emptyset\rangle=\{e\}$, kde e je neutrální prvek grupy $(G,\cdot)$.

Příklad 6.7. Uveďme několik jednoduchých příkladů grup generovaných množinou.

1) Mějme dihedrální grupu $(D_3,\circ)$. Platí $\langle\{R_0\}\rangle=(\{R_0\},\circ)$, $\langle\{R_{120}\}\rangle=(\{R_0,R_{120},R_{240}\},\circ)$, $\langle\{Z_A\}\rangle=$ $=(\{R_0,Z_A\},\circ)$ a $\langle\{R_{120},Z_B\}\rangle=(D_3,\circ)$.
2) Mějme grupu celých čísel s operací obyčejného sčítání. Platí $\langle\{1\}\rangle=(\mathbb{Z},+)$, $\langle\{2\}\rangle=(\mathbb{S},+)$, $\langle\{7\}\rangle=$ $=(7\mathbb{Z},+)$, $\langle\{2,3\}\rangle=(\mathbb{Z},+)$, $\langle\{6,10\}\rangle=(\mathbb{S},+)$ (Cvičení 6.2.7.).

Poznámka 6.2. Sjednocení grup
Je dobré upozornit, že analogie Lemmatu 6.1. pro sjednocení podgrup obecně *neplatí*. Dokonce se dá ukázat, že sjednocení dvou podgrup je podgrupa *pouze* v případě, že nosič jedné podgrupy je podmnožinou nosiče druhé podgrupy (Cvičení 6.2.5.). Jestliže máme dvě podgrupy $(H_1,\cdot)$ a $(H_2,\cdot)$ grupy $(G,\cdot)$ a nosič H_1 obsahuje prvky, které v H_2 nejsou a současně nosič H_2 obsahuje prvky, které v H_1 nejsou, tak $(H_1\cup H_2,\cdot)$ není grupa (Cvičení 6.2.4.).

Cyklická grupa a podgrupa generovaná prvkem
Jestliže $M=\{m\}$ je jednoprvková podmnožina nosiče G grupy $(G,\cdot)$, tak místo $\langle\{m\}\rangle$ budeme psát pouze $\langle m\rangle$. Mohlo by se zdát, že dochází ke konfliktu označení: $\langle\{m\}\rangle$ jako množina generovaná jednoprvkovou množinou a současně $\langle m\rangle$ jako cyklická grupa generovaná prvkem m. Následující lemma ukazuje, že sjednocení symboliky je oprávněné, výsledná struktura je vždy stejná.

Lemma 6.2. *Mějme grupu $(G,\cdot)$ a jednoprvkovou podmnožinu $M=\{m\}$, $M\subseteq G$. Potom podgrupa generovaná množinou M je stejná, jako cyklická grupa generovaná prvkem m, tj. platí $\langle\{m\}\rangle=\langle m\rangle$.*

Důkaz. Už víme, že $\langle\{m\}\rangle$ i $\langle m\rangle$ jsou podgrupy $(G,\cdot)$. Proto pochopitelně i operace je v obou podgrupách stejná. Dále označme $H=\{m^k : k\in\mathbb{Z}\}$ (H je nosič cyklické grupy $\langle m\rangle$) a nosič $\langle\{m\}\rangle$ označme F. Stačí ukázat, že obě nosné množiny jsou shodné, což ukážeme jako množinovou rovnost $H=F$.

Mějme libovolný prvek $a\in H$, platí $a=m^k$ pro nějaké $k\in\mathbb{Z}$. Z definice je zřejmé, že $m\in F$ a potom z uzavřenosti operace na $\langle\{m\}\rangle$ a s využitím úmluvy ze začátku kapitoly je $m^k\in\langle\{m\}\rangle$ a proto $H\subseteq F$.

Zbývá ukázat opačnou inkluzi. Mějme libovolný prvek $a\in F$. Chceme ukázat, že $a\in H$, tj. $a=m^k$ pro nějaké celé číslo k. Sestavíme množinu $X=\{a^k : k\in\mathbb{Z}\}$. Tato množina X s operací „$\cdot$“ tvoří podle Věty 3.4. podgrupu v $(G,\cdot)$, neboť jistě paltí $X\subseteq G$ a $X\neq\emptyset$ (proč?) a pro dva libovolné prvky $a^r,a^s\in X$ platí $a^r\cdot a^{-s}=a^{r-s}\in X$. To ale z definice grupy $\langle\{m\}\rangle$ jako průniku všech grup obsahujících $\{m\}$ znamená, že $F\subseteq X$. Protože $X=H$, tak ihned dostáváme $F\subseteq H$. Proto $H=F$ a obě grupy $(\langle\{m\}\rangle,\cdot)$ a $(\langle m\rangle,\cdot)$ jsou stejné. □

Příklad 6.8. Sestavíme $\langle 5\rangle$, přičemž za operaci mějme běžné sčítání přirozených čísel.
Sestavujeme cyklickou podgrupu v grupě $(\mathbb{Z},+)$. Podle definice cyklické grupy víme, že $\langle 5\rangle$ obsahuje všechny násobky čísla 5. Proto ihned dostáváme, že

$$\langle 5\rangle=(\{k5 : k\in\mathbb{Z}\},+).$$

kde $\langle 5\rangle$ je (cyklická) grupa celých čísel, které jsou násobky pěti. Grupu značíme také $(5\mathbb{Z},+)$. ✓

Příklad 6.9. Sestavíme $\langle 5\rangle$ v grupě $(\mathbb{R}\setminus\{0\},\cdot)$.
Podle definice cyklické grupy víme, že $\langle 5\rangle$ obsahuje všechny mocniny čísla 5. Ihned dostáváme, že

$$\langle 5\rangle=(\{5^k : k\in\mathbb{Z}\},\cdot).$$

✓

Příklad 6.10. Sestavíme podgrupy generované každým prvkem v $(\mathbb{Z}_8,+)$.
Připomeňme, že $(\mathbb{Z}_8,+)$ je množina zbytkových tříd modulo 8 a dále symbolem $\overline{1}_m$ označujeme třídu, která obsahuje čísla, která dávají po dělení modulem m zbytek 1. Platí $(\mathbb{Z}_8,+)=\mathbb{Z}/8\mathbb{Z}$. Snadno nahlédneme, že

$\langle \overline{1}_8 \rangle = (\mathbb{Z}_8, +)$. Podobně $\langle \overline{3}_8 \rangle = \langle \overline{5}_8 \rangle = \langle \overline{7}_8 \rangle = (\mathbb{Z}_8, +)$. Naproti tomu $\langle \overline{2}_8 \rangle = \langle \overline{6}_8 \rangle = (\{\overline{0}_8, \overline{2}_8, \overline{4}_8, \overline{6}_8\}, +)$, $\langle \overline{4}_8 \rangle = (\{\overline{0}_8, \overline{4}_8\}, +)$ a $\langle \overline{0}_8 \rangle = (\{\overline{0}_8\}, +)$. ✓

Cvičení

6.2.1. Dokažte tvrzení Lemmatu 6.1.: mějme grupu $(G, \cdot)$ a její podgrupy $(H_i, \cdot)$, kde $i \in J$. Potom $(\bigcap_{i \in J} H_i, \cdot)$ je opět podgrupa v grupě $(G, \cdot)$.

6.2.2. Je grupa $(G, \cdot)$ určená Tabulkou 6.4. cyklická?

$\cdot$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	f	d	e
c	c	a	b	e	f	d
d	d	e	f	a	b	c
e	e	f	d	c	a	b
f	f	d	e	b	c	a

Tabulka 6.4.: Cayleyho tabulka grupy $(G, \cdot)$.

6.2.3. Mějme grupu $(G, \cdot)$, kde $G = \{a, b, c, d, e, f\}$ a operace je určena Tabulkou 6.4. Určete cyklické grupy $\langle a \rangle$, $\langle b \rangle$, $\langle c \rangle$, $\langle d \rangle$, $\langle e \rangle$ a $\langle f \rangle$.

6.2.4. Mějme grupu $(G, \cdot)$ a dvě její podgrupy $(H_1, \cdot)$ a $(H_2, \cdot)$. Ukažte, že pokud nosič H_1 obsahuje prvky, které v H_2 nejsou a současně nosič H_2 obsahuje prvky, které v H_1 nejsou, tak $(H_1 \cup H_2, \cdot)$ není grupa.

6.2.5. Ukažte, že sjednocení dvou podgrup $(H_1, \cdot)$ a $(H_2, \cdot)$ grupy $(G, \cdot)$ je podgrupa v $(G, \cdot)$ právě tehdy, když $H_1 \subseteq H_2$ nebo $H_2 \subseteq H_1$.

6.2.6. Mějme grupu $(\mathbb{Z}, +)$. Ukažte, že $(\langle \{6, 10\} \rangle, +) = (\mathbb{S}, +)$.

6.2.7. Mějme grupu $(\mathbb{Z}, +)$. Ukažte, že $\langle \{a_1, a_2, \ldots, a_n\} \rangle = (\mathrm{NSD}(a_1, a_2, \ldots, a_n)\mathbb{Z}, +)$.

6.2.8. Ukažte, že grupa $(\mathbb{Q}, +)$ není cyklická.

6.2.9. Ukažte, že grupa $(\mathbb{R}, +)$ není cyklická.

6.2.10. Dokažte nebo vyvraťte: a) každá podgrupa se spočetným počtem prvků je cyklická, b) každá podgrupa s nespočetným počtem prvků není cyklická.

6.3. Řád cyklické grupy a řád prvku

Cyklické grupy byly historicky jedny z prvních zkoumaných grup. Teprve později byla definice grupy zobecněna, aby zahrnula i jiné algebraické struktury než jen cyklické grupy. Následující tvrzení ukazuje, že všechny cyklické grupy jsou v závislosti na řádu generátoru jen dvou různých typů.

Věta 6.3. *Mějme grupu $(G, \cdot)$, libovolný prvek $a \in G$ a $i, j \in \mathbb{Z}$. Potom platí následující tvrzení.*

(i) Jestliže řád prvku a je nekonečný, tak $a^i = a^j$ právě tehdy, když $i = j$.
(ii) Jestliže prvek a je konečného řádu n, tak $\langle a \rangle = (\{e, a, a^2, \ldots, a^{n-1}\}, \cdot)$. Navíc platí $a^i = a^j$ právě tehdy, když n dělí $i - j$.

Důkaz. Dokážeme obě části věty.
i) Z předpokladu $a^i = a^j$ můžeme psát $a^{i-j} = e$, neboť a^{-j} je inverzním prvkem k a^j. Je-li řád prvku a nekonečný, tak $i - j = 0$, protože jinak by existovalo přirozené číslo $i - j$ (případně $j - i$), pro které by platilo $a^{i-j} = e$, a dostali bychom spor s nekonečností řádu prvku a.
ii) Pro důkaz druhé části předpokládejme, že řád prvku a je konečné číslo, tj. $|a| = n$. Nejprve ukážeme, že pro nosnou množinu A cyklické grupy $\langle a \rangle$ platí $A = \{e, a, a^2, \ldots, a^{n-1}\}$; ověříme obě jednostranné inkluze. Protože $\langle a \rangle = \{a^k : k \in \mathbb{Z}\}$, tak jistě $\{e, a, a^2, \ldots, a^{n-1}\} \subseteq \langle a \rangle$. A naopak, je-li $a^k \in \langle a \rangle$, tak podle Věty 0.2. najdeme taková celá čísla q, r, že $k = qn + r$, kde $0 \leq r < n$. Potom můžeme (s využitím definice v Kapitole 6.1.) psát $a^k = a^{qn+r} = (a^n)^q \cdot a^r = e^q \cdot a^r = a^r$, kde $0 \leq r < n$. To ale současně znamená, že $a^k \in \{e, a, a^2, \ldots, a^{n-1}\}$, protože $a^r \in \{e, a, a^2, \ldots, a^{n-1}\}$.

A konečně, je-li a (konečného) řádu n a platí $a^i = a^j$, tak rovnost vynásobíme inverzním prvkem a^{-j} k prvku a^j a dostaneme $a^{i-j} = e = a^0$. Opět najdeme celá čísla q, r, kde $0 \leq r < n$, tak, aby platilo $i - j = qn + r$. (Čísla q a r jsou obecně jiná než v předchozí části důkazu!) Protože $e = a^{i-j} = a^{qn+r} = (a^n)^q \cdot a^r = e \cdot a^r = a^r$, tak musí být $a^r = e$, kde $0 \leq r < n$. Ale n je nejmenší *přirozené* číslo, pro které je $a^n = e$, což znamená, že $r = 0$. To ale současně znamená, že $i - j = qn$ a tedy n dělí $i - j$.

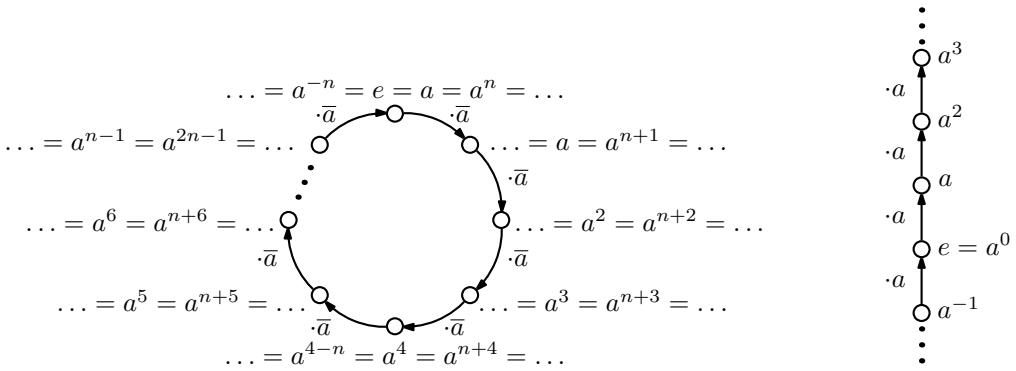
Zbývá ukázat, že pokud n dělí $i - j$, tak $a^i = a^j$. Avšak pokud n dělí $i - j$, tak $i - j = kn$ a můžeme psát $a^i a^{-j} = a^{i-j} = a^{nk} = (a^n)^k = e^k = e$. Roznásobením prvkem a^j dostaneme $a^i a^{-j} a^j a^i = e \cdot a^j$, proto $a^i = a^j$. Tím důkaz končí. □

Otázka: Kde a jak se v důkazu Věty 6.3. využila definice z Kapitoly 6.1.?

Název cyklická grupa

Mějme grupu $(G, \cdot)$ a nějaký její prvek a. Podgrupám s nosičem $A = \{a^n : n \in \mathbb{Z}\}$ se říká „cyklické grupy“ bez odkazu na původní grupu $(G, \cdot)$, neboť struktura původní grupy $(G, \cdot)$ není podstatná.

Postupným násobením prvku a dostáváme nové prvky a^n až do okamžiku, kdy $a = e$, kde e je neutrální prvek grupy $(G, \cdot)$ (i její cyklické podgrupy s nosičem A). Při dalším násobení prvkem a se výsledky opakují. Z Věty 6.3. plyne, že se opakují cyklicky. Struktura cyklické podgrupy je znázorněna na Obrázku 6.1. vlevo. Pokud řád prvku a je nekonečný, dostáváme nové a nové prvky jak pro kladné hodnoty n, tak pro záporné hodnoty n (Obrázek 6.1. vpravo).



Obrázek 6.1.: *Konečná cyklická grupa $\langle a \rangle$ i nekonečná cyklická grupa $\langle a \rangle$.*

Poznámka 6.3. Z Věty 6.3. plyne důležité pozorování: operace „$\cdot$“ v cyklické grupě $\langle a \rangle$ řádu n se v ničem neliší od počítání modulo n. Například $a^i \cdot a^j = a^k$ právě tehdy, když $i + j \equiv k \pmod{n}$. Jedno z jaké grupy jsme prvek a vybrali, nakonec počítáme jako v grupě $(\mathbb{Z}_n, +)$. Je-li řád prvku a nekonečným, tak $\langle a \rangle$ „odpovídá“ grupě $(\mathbb{Z}, +)$. Co přesně rozumíme pojmem „odpovídá“ zavedeme v Kapitole 9. o izomorfismech grup. To znamená, že cyklické grupy $(\mathbb{Z}_n, +)$ a $(\mathbb{Z}, +)$ jsou (až na izomorfismus, kterému se budeme věnovat právě v Kapitole 9.) jedinými případy cyklických grup.

Věta 6.3. ukazuje, proč se „řád prvku“ a „řád grupy“ nazývají stejným slovem. Řád prvku odpovídá řádu cyklické grupy generované tímto prvkem, což zformulujeme jako důsledek Věty 6.3.

Důsledek 6.4. *Mějme libovolný prvek a grupy $(G, \cdot)$. Řád prvku a je roven řádu cyklické grupy $\langle a \rangle$.*

Tvrzení Důsledku 6.4. můžeme zapsat symbolicky stručně jako $|a| = |\langle a \rangle|$.

Příklad 6.11. Uveďme několik příkladů cyklických grup generovaných nějakým prvkem grupy a porovnejme řády generátorů a řády cyklických grup.

1) Mějme grupu $(\mathbb{Z}_6, +)$ z Příkladu 6.5. Platí $|0| = 1 = |\langle 0 \rangle|$, $|1| = 6 = |\langle 1 \rangle|$, $|2| = 3 = |\langle 2 \rangle|$, $|3| = 2 = |\langle 3 \rangle|$, $|4| = 3 = |\langle 4 \rangle|$, $|5| = 6 = |\langle 5 \rangle|$.
2) Mějme dihedrální grupu $(D_3, \circ)$ ze strany 34. Platí $|R_0| = 1 = |\langle R_0 \rangle|$, $|R_{120}| = 3 = |\langle R_{120} \rangle|$, $|R_{240}| = 3 = |\langle R_{240} \rangle|$, $|Z_A| = 2 = |\langle Z_A \rangle|$, $|Z_B| = 2 = |\langle Z_B \rangle|$, $|Z_C| = 2 = |\langle Z_C \rangle|$.
3) Mějme grupu celých čísel s operací obvyklého sčítání $(\mathbb{Z}, +)$. Platí $|0| = 1 = |\langle 0 \rangle|$. Grupa $(\langle 0 \rangle, +)$ je triviální. Platí $|1| = \infty = |\langle 1 \rangle|$ a navíc $(\langle 1 \rangle, +) = (\mathbb{Z}, +)$. Platí $|2| = \infty = |\langle 2 \rangle|$ a navíc $(\langle 2 \rangle, +) = (\mathbb{S}, +)$. Také pro $k > 2$ platí $|k| = \infty = |\langle k \rangle|$ a navíc $(\langle k \rangle, +) = (k\mathbb{Z}, +)$.
4) Mějme grupu regulárních matic řádu 2 s operací násobení matic $(\mathbb{R}^*_{2,2}, \cdot)$. Pro jednotkovou matici E řádu 2 platí $|E| = 1 = |\langle E \rangle|$. Grupa $(\langle E \rangle, \cdot)$ je triviální.

Platí $\left|\begin{pmatrix}1&0\\0&-1\end{pmatrix}\right| = 2 = \left|\left\langle\begin{pmatrix}1&0\\0&-1\end{pmatrix}\right\rangle\right|$ a navíc $\left(\left\langle\begin{pmatrix}1&0\\0&-1\end{pmatrix}\right\rangle, \cdot\right) = \left(\left\{\begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}1&0\\0&-1\end{pmatrix}\right\}, \cdot\right)$.

5) Mějme grupu komplexních čísel s operací obvyklého násobení $(\mathbb{C}, \cdot)$. Platí $|i| = 4 = |\langle i\rangle|$. Grupa $(\langle i\rangle, \cdot)$ obsahuje čtyři prvky $1, -1, i, -i$.
Dále platí $|1+i| = \infty = |\langle 1+i\rangle|$. Grupa $(\langle 1+i\rangle, \cdot)$ obsahuje nekonečně mnoho komplexních čísel, ale zdaleka ne všechna komplexní čísla. Například číslo $\frac{1}{2} \notin \langle 1+i\rangle$, neboť velikost generátoru je $\sqrt{2}$ a proto všechna nenulová komplexní čísla z cyklické grupy $\langle 1+i\rangle$ mají podle Moivreovy věty velikost $t\sqrt{2}$, kde $t \in \mathbb{N}_0$, a žádné nemá velikost $\frac{1}{2}$.

Víme, že ne každá grupa je cyklická. Následující příklad však ukazuje, že pokud máme grupu prvočíselného řádu, tak musí být cyklická.

Příklad 6.12. Ukážeme, že každá grupa prvočíselného řádu je cyklická.
Mějme grupu $(G, \cdot)$ řádu p, kde p je prvočíslo. Podle Lagrangrovy věty (Věta 4.10.) musí řád každého prvku $a \in G$ dělit řád grupy p. Prvočíslo p má však pouze dva přirozené dělitele, a sice 1 a p. Navíc v každé grupě existuje je jediným prvkem řádu 1 neutrální prvek $e \in G$. Máme-li jakýkoliv jiný prvek $a \in G$, $a \neq e$, tak řád prvku a je $|a| = p$. To současně znamená, že všechny mocniny $a^1, a^2, \ldots, a^p = e$ jsou (všechny) různé prvky grupy G, a proto platí $G = \langle a\rangle$ a grupa $(G, \cdot)$ je cyklická. ✓

Všimněte si, že z Příkladu 6.12. současně plyne, že každá grupa prvočíselného řádu je komutativní. Pro každou nekomutativní grupu musí její řád n být složené číslo.

Další důležité a jednoduché pozorování o prvcích konečného řádu je zformulováno v následujícím důsledku.

Důsledek 6.5. *Mějme grupy $(G, \cdot)$ s neutrálním prvkem e a libovolný prvek a. Jestliže $a^k = e$, tak řád prvku a je dělitelem čísla k.*

Všimněte si, že $a^k = e$ *neznamená*, že řád prvku a je k. Uvedená rovnost znamená, že řád prvku a je *nejvýše* k a *navíc* řád prvku a *dělí* k. Všimněte si, že řád prvku a dělí k i v triviálním případě, kdy $k = 0$.

Příklad 6.13. Tvrzení Důsledku 6.5. ilustruje Příklad 6.1. Pro každý prvek a dihedrální grupy $(D_3, \circ)$ ze strany 34 platí $a^6 = R_0$, avšak řád ani jednoho prvku a není 6. Řády jsou $|R_0| = 1$, $|R_{120}| = |R_{240}| = 3$, $|Z_A| = |Z_B| = |Z_C| = 2$, což všechno jsou dělitelé čísla 6.

Cvičení

6.3.1. Určete, pro která n je dihedrální grupa $(D_n, \circ)$ cyklická.

6.3.2. Mějme grupu $(\mathbb{R}, +)$. Určete řád prvku $\sqrt{2}$. Určete řád cyklické grupy $\langle\sqrt{2}\rangle$. Platí $\langle\sqrt{2}\rangle = (\mathbb{R}, +)$?

6.3.3. Mějme přirozené číslo n a přirozeného dělitele r čísla n. Ukažte, že v libovolné cyklické grupě řádu n existuje prvek řádu r.

6.4. Struktura cyklických grup

Nyní se budeme podrobně věnovat konečným cyklickým grupám. Ukážeme několik tvrzení o struktuře a o prvcích konečných cyklických grup. Následující věta dá jednoduchý nástroj, jak určit, zda $\langle a^i\rangle = \langle a^j\rangle$. Připomeňme, že je-li $d = \mathrm{NSD}(x, y)$ největší společný dělitel čísel x, y, tak podle Bézoutova Lemmatu 0.3. existují taková celá čísla s, t, že $d = sx + ty$.

Věta 6.6. *Mějme prvek a (konečného) řádu n v grupě $(G, \cdot)$ a mějme přirozené číslo k. Potom platí $\langle a^k\rangle = \langle a^{\mathrm{NSD}(n,k)}\rangle$ a řád prvku a^k je $n/\mathrm{NSD}(n, k)$.*

Důkaz. Nejprve označme $d = \mathrm{NSD}(n, k)$ a dále $k = dr$. Ještě označíme $A = \langle a^k\rangle$ a $A' = \langle a^{\mathrm{NSD}(n,k)}\rangle = \langle a^d\rangle$.

Abychom ukázali $\langle a^k\rangle = \langle a^d\rangle$, tak jistě stačí ukázat, že obě cyklické grupy mají stejné nosné množiny prvků. Protože $a^k = (a^d)^r$, jistě a^k patří do A'. Z uzavřenosti cyklické grupy je také každá mocnina prvku a^k v množině A' a proto je $A \subseteq A'$. Abychom ukázali platnost opačné inkluze, rozepíšeme si $d = \mathrm{NSD}(n, k)$ podle Bézoutova Lemmatu 0.3. jako $d = ns + kt$ pro nějaká celá čísla s a t. Nyní $a^d = a^{ns+kt} = (a^n)^s(a^k)^t = e(a^k)^t = (a^k)^t$ a proto $a^d \in A$. Dostáváme opačnou inkluzi $A' \subseteq A$, proto $A' = A$.

Abychom ukázali druhou část věty, tak si nejprve všimneme, že rovnost $|a^d| = n/d$ platí nejen pro největšího dělitele d čísel n a k, ale vlastně pro *každého* dělitele čísla n. Jistě platí $(a^d)^{n/d} = a^n = e$ a proto $|a^d| \leq n/d$. A naopak, pokud by existovalo takové přirozené číslo $i < n/d$ že $(a^d)^i = e$, přičemž $di < n$,

tak dostaneme spor s velikostí řádu $|a| = n$. Nyní pro $d = \mathrm{NSD}(n,k)$ můžeme psát $\left|a^k\right| = \left|\langle a^k\rangle\right| = \left|\langle a^{\mathrm{NSD}(n,k)}\rangle\right| = \left|a^{\mathrm{NSD}(n,k)}\right| = n/\mathrm{NSD}(n,k)$. □

Všimněte si, že tvrzení Věty 6.6. je v souladu s Lagrangeovou větu, tj. pro každý prvek $x \in \langle a\rangle$ platí, že řád $|x|$ dělí řád $|\langle a\rangle|$.

Příklad 6.14. Mějme grupu $(\mathbb{Z}_{12},+)$. a) Jaké jsou řády jednotlivých prvků $a \in \mathbb{Z}_{12}$? b) Sestavte $\langle 1\rangle$, $\langle 2\rangle$, $\langle 3\rangle$, $\langle 4\rangle$, $\langle 5\rangle$, $\langle 6\rangle$, $\langle 8\rangle$ a určete jejich řády. Porovnejte s výsledky v části a).
a) Řády jednotlivých prvků jsou v tabulce

a	0	1	2	3	4	5	6	7	8	9	10	11
$\lvert a\rvert$	1	12	6	4	3	12	2	12	3	4	6	12

Tabulka 6.5.: *Řády prvků v grupě* $(\mathbb{Z}_{12},+)$.

b) Sestavíme cyklické grupy

$$\begin{aligned}
\langle 1\rangle &= (\{0,1,2,3,4,5,6,7,8,9,10,11\},+) \text{ řádu } 12, \quad \mathrm{NSD}(12,1) = 1\\
\langle 2\rangle &= (\{0,2,4,6,8,10\},+) \text{ řádu } 6, \quad \mathrm{NSD}(12,2) = 2\\
\langle 3\rangle &= (\{0,3,6,9\},+) \text{ řádu } 4, \quad \mathrm{NSD}(12,3) = 3\\
\langle 4\rangle &= (\{0,4,8\},+) \text{ řádu } 3, \quad \mathrm{NSD}(12,4) = 4\\
\langle 5\rangle &= (\{0,1,2,3,4,5,6,7,8,9,10,11\},+) \text{ řádu } 12, \quad \mathrm{NSD}(12,5) = 1\\
\langle 6\rangle &= (\{0,6\},+) \text{ řádu } 2, \quad \mathrm{NSD}(12,6) = 6\\
\langle 8\rangle &= (\{0,4,8\},+) \text{ řádu } 3, \quad \mathrm{NSD}(12,8) = 4
\end{aligned}$$

✓

Důsledek 6.7. *Mějme prvek a (konečného) řádu n v grupě $(G,\cdot)$ a mějme čísla $i,j \in \mathbb{N}$. Potom platí následující tvrzení.*

(i) $\langle a^i\rangle = \langle a^j\rangle$ *právě tehdy, když* $\mathrm{NSD}(n,i) = \mathrm{NSD}(n,j)$.
(ii) $\left|a^i\right| = \left|a^j\right|$ *právě tehdy, když* $\mathrm{NSD}(n,i) = \mathrm{NSD}(n,j)$.

Důkaz.
i) Podle předpokladu je prvek a řádu n a podle Věty 6.6. víme, že $\langle a^i\rangle = \langle a^{\mathrm{NSD}(n,i)}\rangle$ a také $\langle a^j\rangle = \langle a^{\mathrm{NSD}(n,j)}\rangle$. Zbývá tedy ukázat, že $\langle a^{\mathrm{NSD}(n,i)}\rangle = \langle a^{\mathrm{NSD}(n,j)}\rangle$ právě tehdy, když $\mathrm{NSD}(n,i) = \mathrm{NSD}(n,j)$. Ihned je zřejmé, že pokud $\mathrm{NSD}(n,i) = \mathrm{NSD}(n,j)$, tak $\langle a^{\mathrm{NSD}(n,i)}\rangle = \langle a^{\mathrm{NSD}(n,j)}\rangle$. Abychom ukázali opačnou implikaci, tak si uvědomíme, že $\langle a^{\mathrm{NSD}(n,i)}\rangle = \langle a^{\mathrm{NSD}(n,j)}\rangle$ znamená, že generátory jsou stejného řádu, tj. $\left|a^{\mathrm{NSD}(n,i)}\right| = \left|a^{\mathrm{NSD}(n,j)}\right|$. Z druhé části tvrzení Věty 6.6. plyne, že $n/\mathrm{NSD}(n,i) = n/\mathrm{NSD}(n,j)$, tedy, že $\mathrm{NSD}(n,i) = \mathrm{NSD}(n,j)$.
ii) Druhé tvrzení dostaneme ihned kombinací tvrzení části i) a Důsledku 6.4. Dosazením dostaneme $\left|a^i\right| = \left|\langle a^i\rangle\right| = \left|\langle a^j\rangle\right| = \left|a^j\right|$. □

Speciální případy Důsledku 6.7. jsou následující dvě tvrzení.

Důsledek 6.8. *Mějme prvek a (konečného) řádu n v grupě $(G,\cdot)$. Označme $i \in \mathbb{N}$. Potom platí následující dvě tvrzení.*

(i) $\langle a^i\rangle = \langle a\rangle$ *právě tehdy, když* $\mathrm{NSD}(n,i) = 1$.
(ii) $\left|a^i\right| = |\langle a\rangle|$ *právě tehdy, když* $\mathrm{NSD}(n,i) = 1$.

Důkaz. Tvrzení dostaneme ihned z Důsledku 6.7. volbou $j = 1$. □

Uvedené tvrzení říká, jak snadno určit všechny generátory cyklické grupy $\langle a\rangle$. Jsou to právě ty prvky a^i, kde i je nesoudělné s řádem n prvku a.

Příklad 6.15. Mějme grupu $(\mathbb{Z}_{12},+)$. a) Najdeme všechny generátory cyklické podgrupy generované prvkem 3, tj. $\langle 3\rangle = (\{0,3,6,9\},+)$. b) Určíme řády těchto generátorů.
a) Generátor grupy $\langle 3\rangle$ je prvek 3 řádu $n = 4$. Mezi násobky prvku 3 najdeme všechny jejichž řád je nesoudělný s $n = 4$. V aditivní notaci je $1\cdot 3 = 3$, $2\cdot 3 = 6$, $3\cdot 3 = 9$, $4\cdot 3 = 0$. Protože $\mathrm{NSD}(4,1) = 1$, tak

prvek 3 je (ihned) jeden z generátorů $\langle 3\rangle$. Protože $\mathrm{NSD}(4,2)\neq 1$, tak prvek 6 není generátor $\langle 3\rangle$. Protože $\mathrm{NSD}(4,3)=1$, tak prvek 9 je druhý generátor $\langle 3\rangle$. A konečně protože $\mathrm{NSD}(4,4)\neq 1$, tak prvek 0 není generátor $\langle 3\rangle$. Hledané generátory jsou prvky 3 a 9.
b) V Tabulce 6.5. vidíme, že $|3|=|9|=4$. ✓

Například v grupě $(\mathbb{Z}_n,+)$, kde třídy ztotožníme s celočíselnými reprezentanty $1,2,\ldots,n$, jsou generátory právě přirozená čísla k nesoudělná s modulem n (n je současně řádem).

Důsledek 6.9. *Přirozené číslo k je generátorem grupy $(\mathbb{Z}_n,+)$ právě tehdy, když $\mathrm{NSD}(n,k)=1$.*

Je-li n prvočíslo, tak generátorem grupy je každý její prvek různý od neutrálního prvku.

Příklad 6.16. Mějme grupu $(\mathbb{Z}_{12},+)$. a) Najdeme všechny generátory grupy $(\mathbb{Z}_{12},+)$. b) Určíme, která čísla z intervalu $[0,|(\mathbb{Z}_{12},+)|-1]$ jsou nesoudělná s 12.
a) Generátory jsou právě prvky řádu 12: $1,5,7,11$.
b) Čísla nesoudělná s řádem grupy $(\mathbb{Z}_{12},+)$ jsou právě čísla $1,5,7,11$. ✓

Příklad 6.17. Navážeme na Příklad 4.16. Určíme, zda a) grupa jednotek $(U(15),\cdot)$ je cyklická, b) grupa jednotek $(U(18),\cdot)$ je cyklická.
a) V Příkladu 4.16. jsme určili řády všech prvků. Grupa $(U(15),\cdot)$ má 8 prvků a žádný z prvků není řádu 8, proto $(U(15),\cdot)$ není cyklická grupa.
b) Grupa $(U(18),\cdot)$ obsahuje 6 prvků: $1,5,7,11,13,17$, neboť ostatní přirozená čísla menší než 18 jsou s 18 soudělná. Určíme řády prvků a pokud najdeme prvek řádu 6, tak $(U(18),\cdot)$ je cyklická grupa. Číslo 1 je neutrálním prvkem grupy $(U(18),\cdot)$, proto $|1|=1$. Dále počítáme modulo 18. Platí $5\cdot 5\equiv 7 \pmod{18}$, $7\cdot 5\equiv 17 \pmod{18}$, $17\cdot 5\equiv 13 \pmod{18}$, $13\cdot 5\equiv 11 \pmod{18}$ a $11\cdot 5\equiv 1 \pmod{18}$. Protože řád prvku $|5|=6$, tak grupa jednotek $(U(18),\cdot)$je cyklická, platí $(U(18),\cdot)=\langle 5\rangle$. ✓

Nyní můžeme vyslovit tvrzení, které shrne předchozí výsledky o cyklických grupách do jednoho tvrzení, které říká, jak vypadají *všechny* podgrupy cyklické grupy dané nějakým prvkem.

Věta 6.10. Hlavní věta o cyklických grupách
Mějme prvek a (konečného) řádu n v grupě $(G,\cdot)$. Potom

(i) každá podgrupa cyklické grupy $\langle a\rangle$ je cyklická,
(ii) řád každé její podgrupy dělí n,
(iii) pro každého kladného dělitele k čísla n existuje v grupě $\langle a\rangle$ právě jedna podgrupa řádu k, a sice podgrupa $\langle a^{n/k}\rangle$.

Důkaz. Postupně dokážeme každou ze tří částí.
(i) Mějme libovolnou podgrupu H cyklické grupy $\langle a\rangle$. Jestliže H obsahuje pouze neutrální prvek, tak H je triviálně cyklická. Jestliže H obsahuje i jiný než neutrální prvek, tak protože se jedná o prvek cyklické grupy $\langle a\rangle$, má tento prvek tvar a^t. Víme, že grupa H musí obsahovat inverzní prvek a^{-t}, a proto bez újmy na obecnosti můžeme můžeme předpokládat, že číslo t je *kladné*. Mezi všemi takovými mocninami a^t podgrupy H vybereme ten s nejmenším kladným exponentem m. Ukážeme, že $H=\langle a^m\rangle$. Z uzavřenosti operace na H jistě platí $\langle a^m\rangle\subseteq H$. Naopak, libovolný prvek $h\in H$ je současně v $\langle a\rangle$ a je tvaru a^k pro nějaké celé číslo k. Podle Věty o jednoznačnosti podílu a zbytku (Věta 0.2.) existují taková jednoznačně určená celá čísla q a r, kde $0\leq r<m$, že $k=qm+r$. Potom platí $a^k=a^{qm+r}=a^{mq}a^r$ a $a^r=a^k(a^m)^{-q}$. Jelikož $a^k=h\in H$ a $a^m\in H$, je také $a^r=a^k(a^m)^{-q}\in H$, kde $0\leq r<m$. Číslo m bylo vybráno jako *nejmenší* kladné číslo s vlastností $a^m\in H$, proto je $r=0$. Můžeme psát $a^k=(a^m)^q$, což znamená, že $a^k\in\langle a^m\rangle$, a tedy $H\subseteq\langle a^m\rangle$. Ukázali jsme, že H je cyklická grupa $\langle a^m\rangle$ a tedy každá podgrupa $\langle a\rangle$ je cyklická.
(ii) Tvrzení plyne ihned z Lagrangeovy věty (Věta 4.10.).
(iii) A konečně zbývá ukázat, že pro každého dělitele k čísla n je $\langle a^{n/k}\rangle$ jediná podgrupa řádu k v grupě $\langle a\rangle$. už víme, že $\langle a^{n/k}\rangle$ je podgrupa $\langle a\rangle$ a její řád je podle Věty 6.6. roven $n/\mathrm{NSD}(n,n/k))=n/(n/k)=k$. Dále označme H libovolnou podgrupu řádu k grupy $\langle a\rangle$. V důkazu části (ii) jsme ukázali, že $H=\langle a^m\rangle$, kde m je dělitel čísla n. Nyní, protože $m=\mathrm{NSD}(n,m)$, můžeme podle Věty 6.6. psát $k=|a^m|=\left|a^{\mathrm{NSD}(n,m)}\right|=$ $=n/\mathrm{NSD}(n,m)=n/m$. To ale znamená, že $m=n/k$ a $H=\langle a^m\rangle=\langle a^{n/k}\rangle$. □

Všimněte si, že důkaz je konstruktivní. Tvrzení říká, jakých řádů najdeme v $\langle a\rangle$ podgrupy a důkaz věty spolu s Důsledkem 6.7. ukazuje, jak tyto podgrupy najít.

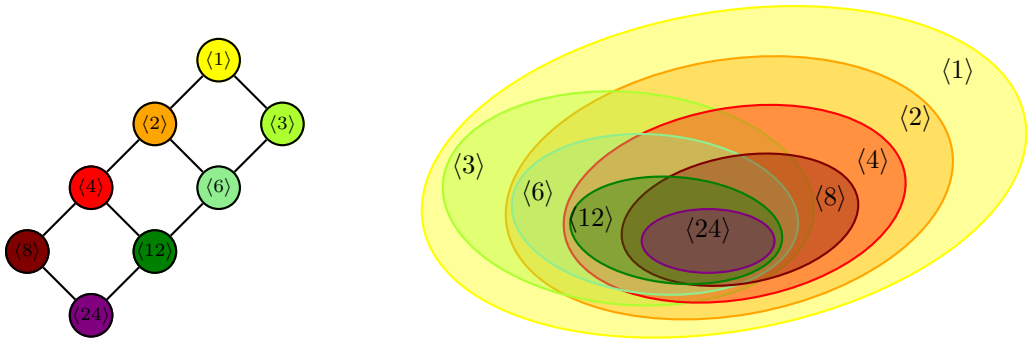
Příklad 6.18. Najděte všechny podgrupy v grupě $(\mathbb{Z}_{24},+)$.

Protože grupa $(\mathbb{Z}_{24}, +)$ je cyklická, tak na základě Věty 6.10. stačí probrat všechny dělitele čísla 24, a sice $1, 2, 3, 4, 6, 8, 12, 24$. Všechny podgrupy jsou následující:

$$\begin{aligned}
\langle 1\rangle &= (\{0, 1, \ldots, 23\}, +) \text{ řádu } 24\\
\langle 2\rangle &= (\{0, 2, \ldots, 22\}, +) \text{ řádu } 12\\
\langle 3\rangle &= (\{0, 3, \ldots, 21\}, +) \text{ řádu } 8\\
\langle 4\rangle &= (\{0, 4, \ldots, 20\}, +) \text{ řádu } 6\\
\langle 6\rangle &= (\{0, 6, 12, 18\}, +) \text{ řádu } 4\\
\langle 8\rangle &= (\{0, 8, 16, \}, +) \text{ řádu } 3\\
\langle 12\rangle &= (\{0, 12\}, +) \text{ řádu } 2\\
\langle 24\rangle &= (\{0\}, +) \text{ řádu } 1
\end{aligned}$$

✓

Jestliže na množině všech podgrup $\{\langle 1\rangle, \langle 2\rangle, \langle 3\rangle, \langle 4\rangle, \langle 6\rangle, \langle 8\rangle, \langle 12\rangle, \langle 24\rangle\}$ grupy $(\mathbb{Z}_{24}, +)$ zavedeme relaci „být podgrupou“, která je podle Cvičení 3.1.7. relací částečného uspořádání a má smysl nakreslit hasseovský diagram této relace (Obrázek 6.2. vlevo). Inkluze mezi jednotlivými podgrupami je na Obrázku 6.2. vpravo.



Obrázek 6.2.: *Znázornění systému podgrup cyklické grupy* $(\mathbb{Z}_{24}, +)$.

Příklad 6.19. Najděte všechny generátory podgrupy řádu 8 v grupě $(\mathbb{Z}_{24}, +)$.
Na základě Věty 6.10. víme že jedním generátorem je prvek $24/8 = 3$. Dále s využitím Důsledku 6.7. víme, že další generátory jsou prvky i, pro které platí $\mathrm{NSD}(24, i) = \mathrm{NSD}(24, 8) = 8$. Dalším generátorem je proto pouze prvek 16, neboť pro jiná nenulová čísla i z množiny Z_{24} je $\mathrm{NSD}(24, i) \neq 8$.

i	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
$\mathrm{NSD}(24, i)$	1	2	3	4	1	6	1	8	3	2	1	12	1	2	3	8	1	6	1	4	3	2	1

Tabulka 6.6.: *Největší společní dělitelé* $\mathrm{NSD}(24, i)$.

✓

Cvičení

6.4.1. Mějme grupu $(G, \cdot)$ a prvek $a \in G$. Ukažte, že $|\langle a\rangle| = \left|\langle a^{-1}\rangle\right|$.

6.4.2. Mějme grupu $(G, \cdot)$ a prvek $a \in G$. Ukažte, že $\langle a\rangle = \langle a^{-1}\rangle$.

6.4.3. Najděte všechny podgrupy a) grupy $(\mathbb{Z}_7, +)$, b) grupy $(\mathbb{Z}_8, +)$.

6.4.4. Ukažte, že a) grupy jednotek $(U(2), \cdot)$, $(U(4), \cdot)$, $(U(6), \cdot)$ jsou cyklické, b) grupa jednotek $(U(8), \cdot)$ není cyklická.

6.4.5. Je grupa jednotek $(U(30), \cdot)$ cyklická?

6.4.6. Ukažte, že pro prvočíselné hodnoty n je grupa jednotek $(U(n), \cdot)$ cyklická. Najděte příslušné generátory grupy $(U(n), \cdot)$.*

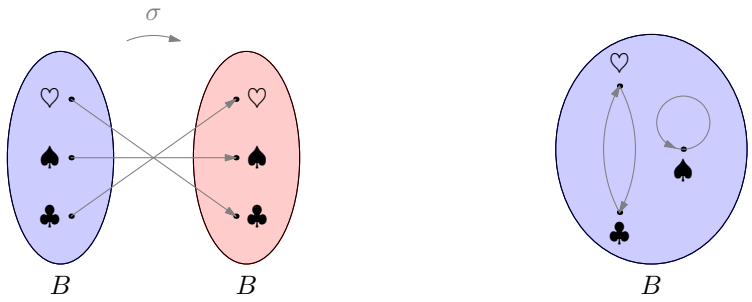
*6.4.7.**Určete, pro která n je grupa jednotek $(U(n), +)$ cyklická. Najděte příslušné generátory.*

Kapitola 7. Grupy permutací

S pojmem permutace se setkáváme v různých matematických disciplínách, například v diskrétní matematice. Už na střední škole jsme permutací konečné množiny rozuměli seřazení všech prvků množiny do nějaké posloupnosti. Permutace lze také chápat jako bijektivní zobrazení konečné množiny na sebe sama. Připomeňme, že bijektivní zobrazení je takové zobrazení, které je současně prosté a současně na (současně injektivní a surjektivní). O popisu permutací je psáno v úvodní Kapitole 0.5. na straně 15. V této kapitole ukážeme, jak oba přístupy souvisí a co umíme o permutacích říci obecně.

V matematické analýze jsou zobrazení obvykle popsána funkčním předpisem, který každému prvku definičního oboru přiřadí nějaký prvek oboru hodnot. Naproti tomu zobrazení konečných množin je zpravidla zadáno explicitním popisem dvojic prvků: vzoru a obrazu. Ke každému vzoru je přiřazen obraz, jako v Příkladu 7.1.

Příklad 7.1. Mějme množinu $B = \{\heartsuit, \spadesuit, \clubsuit\}$. Popíšeme permutaci $\sigma : B \to B$ předpisem $\sigma(\heartsuit) = \clubsuit$, $\sigma(\spadesuit) = \spadesuit$, $\sigma(\clubsuit) = \heartsuit$. Permutaci σ znázorníme jako zobrazení množiny B do množiny B i jako zobrazení na množině B. Dále permutaci σ zapíšeme pomocí dvouřádkové matice vzorů a obrazů i pomocí cyklů.
Obrázek 7.1. vlevo znázorňuje permutaci σ jako zobrazení $B \to B$. Obrázek 7.1. vpravo znázorňuje tutéž permutaci σ jako zobrazení na množině B.



Obrázek 7.1.: *Zobrazení $\sigma : B \to B$.*

Maticový zápis permutace obsahuje v prvním i druhém řádku všechny prvky množiny B. V prvním řádku jsou vzory a v druhém řádku je pod každým vzorem zapsán jeho obraz.

$$\sigma = \begin{pmatrix} \heartsuit & \spadesuit & \clubsuit \\ \clubsuit & \spadesuit & \heartsuit \end{pmatrix}$$

V zápisu pomocí cyklů píšeme za každý prvek jeho obraz. Jestliže obraz prvku již v permutaci byl vzorem, zapíšeme tento fakt uzavřením závorky, která obsahuje všechny prvky takového cyklu permutace. Protože v permutaci (i každém bijektivním zobrazení) je každý prvek právě jednou vzorem a právě jednou obrazem, objeví se v zápisu každý prvek právě jednou. Cyklický zápis permutace σ je

$$\sigma = (\heartsuit\clubsuit)(\spadesuit).$$

Srovnejte zápis permutace σ pomocí cyklů se znázorněním cyklů na Obrázku 7.1. vpravo. Další podobný příklad je Příklad 0.10. na straně 16. ✓

Triviální cykly s jediným prvkem zpravidla nebudeme zapisovat. Výjimkou je identická permutace ε, ve které je každý prvek součástí cyklu s jediným prvkem, a tak aby zápis permutace ε nebyl prázdný, zapíšeme ε jako jeden triviální cyklus s libovolným prvkem.

Jestliže v permutaci π množiny A se prvek $a \in A$ zobrazuje sám na sebe, tj. platí $\pi(a) = a$, tak říkáme, že prvek a je *pevným bodem* permutace π, nebo permutace π *fixuje* prvek a. Například prvek $\spadesuit$ je pevným bodem permutace σ v Příkladu 7.1.

Symetrie čtverce $ABCD$ jsme v příkladu na straně 36 popsali pomocí permutací vrcholů (Cvičení 1.1.2.). Tyto permutace můžeme skládat a dostáváme dihedrální grupu $(D_4, \circ)$.

Připomeňme, že při skládání operací skládání „$\circ$“ (čti „po“) postupujeme zprava doleva, neboť $\pi \circ \sigma(x) = \pi(\sigma(x))$. To znamená, že nejprve aplikujeme permutaci σ a teprve potom permutaci π. Dále připomeňme, že operace „$\circ$“ skládání zobrazení *není* komutativní: obecně $\sigma \circ \pi$ a $\pi \circ \sigma$ nemusí být stejnou permutací.

Příklad 7.2. Navážeme na Příklad 7.1. Složíme permutaci σ s permutací $\pi = (\heartsuit\,\clubsuit\,\spadesuit)$ v různém pořadí. Složením permutací $\sigma = (\heartsuit\,\clubsuit)(\spadesuit)$ a $\pi = (\heartsuit\,\clubsuit\,\spadesuit)$ dostaneme $\sigma \circ \pi = (\heartsuit)(\clubsuit\,\spadesuit)$, avšak $\pi \circ \sigma = (\heartsuit\,\spadesuit)(\clubsuit)$. Vidíme, že obě složené permutace $\sigma \circ \pi$ a $\pi \circ \sigma$ jsou různé, například permutace $\sigma \circ \pi(\clubsuit) = \spadesuit$, zatímco $\pi \circ \sigma(\clubsuit) = \clubsuit$. ✓

7.1. Definice grupy permutací

Nyní zavedeme důležitou grupu, jejíž prvky budou všechny permutace nějaké pevně zvolené množiny. Operací v grupě bude skládání permutací.

Definice Mějme neprázdnou množinu A. Každé bijektivní zobrazení $A \to A$ nazveme *permutací* množiny A. Množina A je *nosná* množina. Identické zobrazení je *identická permutace*, kterou budeme značit ε.

Grupu všech permutací n-prvkové množiny A spolu s operací skládání zobrazení „$\circ$“ nazveme *grupou permutací* nebo *symetrickou grupou* a budeme ji značit $(S_n, \circ)$, případně jen S_n.

Příklad 7.3. Uveďme některé příklad grup symetrií, které odpovídají grupě permutací.

1) Triviální grupa je vlastně symetrická grupa $(S_1, \circ)$ jednoprvkové množiny.
2) Každá dvouprvková grupa je symetrickou grupou $(S_2, \circ)$ nějaké dvouprvkové množiny. Například symetrie motýlka (Obrázek 1.1.) tvoří dvouprvkovou grupu danou Tabulkou 1.1. Pokud označíme špičky tykadel motýla jako dva body A, B, tak identita I odpovídá identické permutaci $\varepsilon = (A)$ dvouprvkové množiny $\{A, B\}$ a zrcadlení podle svislé osy V odpovídá transpozici (AB).
3) Symetrická grupa $(S_3, \circ)$ je grupou symetrií trojúhelníka (Sekce 1.1.). Každá z šesti permutací tříprvkové množiny vrcholů $\{A, B, C\}$ odpovídá některé symetrii trojúhelníka.
4) Symetrická grupa $(S_4, \circ)$ odpovídá grupě symetrií krychle (Cvičení 7.3.9.).

Odkazy:

- https://twitter.com/i/status/1295041342486114304

Třebaže má smysl zabývat se i permutacemi nekonečných množin, my se omezíme jen na permutace konečných množin. Navíc budeme v této kapitole pro jednoduchost předpokládat, že nosná množina grupy permutací je konečná množina prvních n přirozených čísel $[1, n]$ (bez nuly!). Můžeme ji chápat jako indexovou množinu libovolné (konečné) n-prvkové množiny.

Nejprve zdůvodníme, že definice je korektní, tj. že množina permutací množiny s operací skládání zobrazení opravdu tvoří grupu. Množina všech bijekcí množiny $[1, n]$ je neprázdná, obsahuje například identické zobrazení dané předpisem $\varepsilon(a) = a$, pro každé $a \in [1, n]$. Operace skládání bijekcí je podle Lemmatu 0.11. asociativní operace a je uzavřená na $[1, n]$, neboť složení dvou bijekcí $\pi : A \to A$ a $\sigma : A \to A$ je opět bijekce $\sigma \circ \pi : A \to A$. Neutrálním prvkem je identická permutace ε a inverzním prvkem k permutaci π je inverzní permutace (inverzní zobrazení) π^{-1}. Můžeme proto konstatovat, že $(S_n, \circ) = ([1, n], \circ)$ opravdu tvoří grupu.

Do poloviny devatenáctého století byly grupy permutací jedinými grupami, které byly zkoumané. V Kapitole 9.3. se budeme věnovat permutacím obecných množin a ukážeme, že zkoumání grup permutací není na újmu obecnosti.

Ukážeme některé důležité vlastnosti grupy permutací, nejprve se zaměříme na skládání permutací.

Disjunktní cykly

Libovolná permutace (neboli bijektivní zobrazení nosné množiny A) může být popsána pomocí jednoho nebo několika cyklů. Zápis permutací pomocí cyklů je popsán v Kapitole 0.5. Podrobné procvičení spadá do jiného předmětu, například do předmětu Diskrétní matematika.

Každá permutace se může skládat z několika cyklů a složení permutací pak může být popsáno postupným složením více cyklů. Protože skládání permutací je skládání zobrazení, tak i při skládání cyklů budeme zapisovat a číst zprava doleva. Máme-li složení dvou cyklů $\alpha \circ \beta$, tak nejprve aplikujeme permutaci danou cyklem β a teprve potom permutaci danou cyklem α.

Různá složení permutací mohou dát stejnou výslednou permutaci, zpravidla budeme usilovat o co nejpřehlednější zápis. Nejprve ukážeme, že v zápisu každé permutace vystačíme s nejvýše jedním výskytem každého prvku (vzoru) a že zápis složených permutací můžeme často zjednodušit.

Definice Řekneme, že dva cykly v dané permutaci jsou *disjunktní*, jestliže nemají žádný společný prvek nosné množiny.

Ukážeme, že každá permutace může být popsána pomocí disjunktních cyklů. To znamená, že i složené permutace bude možné zapsat efektivně tak, aby se každý prvek v zápisu složené permutace pomocí cyklů vyskytoval nejvýše jednou.

Věta 7.1. *Každá permutace může být zapsána jako složení disjunktních cyklů.*

Důkaz. Mějme permutaci σ nosné množiny A. Přímo ukážeme, jak permutaci σ zapsat pomocí disjunktních cyklů. Zvolme libovolný prvek $a_1 \in A$ a sestavíme cyklus obsahující prvek a_1. Další prvek cyklu bude a_2, kde $a_2 = \sigma(a_1)$, třetí prvek bude $a_3 = \sigma(a_2) = \sigma^2(a_1)$, atd., dokud $\sigma^m(a_1) = a_1$. Víme, že některý prvek se musí opakovat, neboť bijekce σ je prvek grupy $(S_n, \circ)$, a protože množina A je konečná, je i řád r prvku σ konečný a platí $\sigma^r = \varepsilon$. Číslo m označíme nejmenší přirozené číslo, pro které platí $\sigma^m(a_1) = a_1$. Dostaneme cyklus $\alpha = (a_1\, a_2\, \ldots\, a_m)$. Zdůrazněme, že zápis pomocí tří teček připouští možnost $m = 1$, kdy cyklus má délku 1 a prvek a_1 je v permutaci σ fixovaný, i možnost $m = 2$, kdy $\sigma(a_1) = a_2$, $\sigma(a_2) = a_1$.

Nyní, pokud cyklus α obsahuje všechny prvky množiny A, je permutace σ dána cyklem α. Pokud ale cyklus α neobsahuje všechny prvky množiny A, zvolíme libovolný prvek $b_1 \in A$, který není v cyklu α, a sestavíme další cyklus $\beta = (b_1\, b_2\, \ldots\, b_n)$, kde $b_i = \sigma(b_{i-1})$. A protože σ je bijekce, tak se žádný prvek cyklu β nemůže shodovat s prvkem cyklu α, neboť rovnost $\sigma^i(a_i) = \sigma^j(b_j)$ by implikovala $\sigma^{i-j}(a_1) = b_1$, což není možné. Bez újmy na obecnosti jsme mohli předpokládat, že $i \geq j$.

Protože množina A je konečná, tak po konečném počtu kroků dostaneme všechny další cykly permutace σ, které budou po dvou disjunktní. Platí $\sigma = \alpha \circ \beta \circ \cdots \circ \gamma$, neboť obrazy prvků zapsané v jednom cyklu nijak neovlivní obrazy prvků v jiném cyklu. □

Otázka: V důkazu Věty 7.1. jsme řád prvku σ označili r a nejmenší přirozené číslo m, pro které platí $\sigma^m(a_1) = a_1$ Platí $m = r$?

V Příkladu 7.2. jsme uvedli dvě permutace $\sigma = (\heartsuit\clubsuit)(\spadesuit)$ a $\pi = (\heartsuit\clubsuit\spadesuit)$ a složením jsme dostali například permutaci $\sigma \circ \pi = (\heartsuit)(\clubsuit\spadesuit)$, která je také popsána dvěma disjunktními cykly.

Příklad 7.4. Mějme permutace $\varphi = (1\,2)(3\,4\,5)$, $\psi = (6\,7\,8)$ a $\tau = (1\,3\,5\,7)$ množiny $A = [1, 10]$. Sestavíme složené permutace $\varphi \circ \psi$, $\psi \circ \varphi$, $\varphi \circ \tau$ a $\tau \circ \varphi$.
Protože cykly permutací φ a ψ nemají žádný společný prvek, tak složením dostaneme permutaci se stejnými cykly, jako mají obě permutace. Platí $\varphi \circ \psi = (1\,2)(3\,4\,5) \circ (6\,7\,8) = \psi \circ \varphi = (1\,2)(3\,4\,5)(6\,7\,8)$. Dokonce je možné vynechat znaménko operace „$\circ$“, neboť výsledná permutace obsahuje tři disjunktní cykly.

Naproti tomu cykly permutací φ a τ sdílí prvky 1, 3 a 5, proto při skládání je důležité, zda se prvek 1 zobrazí nejprve na prvek 2 v permutaci φ nebo na prvek 3 v permutaci τ. Složením dostaneme různé permutace $\varphi \circ \tau = (1\,2)(3\,4\,5) \circ (1\,3\,5\,7) = (1\,4\,5\,7\,2)(3) = (1\,4\,5\,7\,2)$ a $\tau \circ \varphi = (1\,3\,5\,7) \circ (1\,2)(3\,4\,5) = (1\,2\,3\,4\,7)(5) = (1\,2\,3\,4\,7)$. Výsledná permutace obecně obsahuje jiný cyklus (jiné cykly), než původní permutace φ, τ. ✓

Skládání cyklů

Pozorování z první části Příkladu 7.4. lze zobecnit. Ukážeme, že složená permutace nezávisí na pořadí skládání cyklů, pokud jsou cykly disjunktní. Proto si můžeme dovolit v zápisu složení disjunktních cyklů vynechat symbol operace „$\circ$“.

Věta 7.2. *Mějme dva disjunktní cykly $\alpha = (a_1, a_2 \ldots, a_m)$, $\beta = (b_1, b_2, \ldots, b_n)$. Platí $\alpha \circ \beta = \beta \circ \alpha$, tj. disjunktní cykly v součinu komutují.*

Důkaz. Pro názornost předpokládejme, že nosná množina A daných permutací je

$$A = \{a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n, c_1, c_2, \ldots, c_p\},$$

kde prvky $c_1, c_2, \ldots, c_p$ jsou případné prvky zafixované v permutaci α i β. Ukážeme, že pro každý prvek $x \in A$ platí $\alpha \circ \beta(x) = \beta \circ \alpha(x)$. Je-li $x = a_i$ pro $1 \leq i \leq m$, tak $\alpha \circ \beta(a_i) = \alpha(\beta(a_i)) = \alpha(a_i) = a_{i+1}$ a současně $\beta \circ \alpha(a_i) = \beta(\alpha(a_i)) = \beta(a_{i+1}) = a_{i+1}$, neboť β neovlivní prvky a_i pro žádné $i = 1, 2 \ldots, m$. Zcela analogicky ukážeme, že pokud $x = b_i$ pro $1 \leq i \leq n$, tak $\alpha \circ \beta(b_i) = b_{i+1} = \beta \circ \alpha(b_i)$ pro každé $i = 1, 2 \ldots, n$.

A konečně, pokud $x = c_i$ pro $1 \leq i \leq p$, tak $\alpha \circ \beta(c_i) = \alpha(\beta(c_i)) = \alpha(c_i) = c_i$ a současně $\beta \circ \alpha(c_i) = \beta(\alpha(c_i)) = \beta(c_i) = c_i$, neboť ani α ani β neovlivní prvky c_i pro žádné $i = 1, 2 \ldots, p$.

Tím jsme ukázali, že $\alpha \circ \beta(x) = \beta \circ \alpha(x)$ pro každý prvek $x \in A$. □

Tvrzení Věty 7.2. však není možné obecně zesílit. Netriviální cykly, které nejsou disjunktní, nemusí komutovat, jak ukazuje následující příklad.

Příklad 7.5. Ukážeme, že cykly $\alpha = (1\,2\,3)$ a $\beta = (1\,4)$ na množině $[1,4]$ nekomutují, byť sdílejí jediný prvek.
Stačí porovnat permutace, které vzniknou složením cyklů v opačném pořadí.

$$\alpha \circ \beta = (1\,2\,3) \circ (1\,4) = (1\,4\,2\,3)$$
$$\beta \circ \alpha = (1\,4) \circ (1\,2\,3) = (1\,2\,3\,4)$$

Protože $\alpha \circ \beta \neq \beta \circ \alpha$, tak cykly α a β nekomutují. ✓

Všimněte si, že při zápisu složených permutací pomocí matic jsme symbol operace „$\circ$“ zapsali vždy, avšak při zápisu složených permuací pomocí cyklů jsme mezi cykly někdy symbol operace „$\circ$“ zapisovali a někdy ne. Tvrzení Vět 7.1. a 7.2. můžeme shrnout:

- jestliže zapisujeme jednu permutaci popsanou pomocí disjunktních cyklů, tak symbol operace „$\circ$“ zpravidla vynecháváme,
- jestliže zapisujeme složenou permutaci, kdy cykly nejsou disjunktní (nebo nemusí být disjunktní v závislosti na volbě konkrétních prvků), tak symbol operace „$\circ$“ použijeme vždy, aby bylo zřejmé pořadí permutací,
- a jestliže zapisujeme složení permutací, jejichž cykly jsou disjunktní, tak symbol operace „$\circ$“ můžeme vynechat, závisí na tom, zda chceme zdůraznit, že cykly permutací jsou disjunktní, nebo že skládáme různé permutace.

Pevné body permutací

Pevné body permutací poznáme snadno, v zápisu permutace pomocí cyklů by odpovídaly triviálnímu cyklu s jediným prvkem. Triviální cyklus pochopitelně komutuje s libovolnou permutací, neboť se jedná o identické zobrazení, které fixuje všechny body dané množiny. Proto triviální cykly dle úmluvy zpravidla nezapisujeme.

Jestliže nějaká permutace množiny A obsahuje dva disjunktní cykly $(a_1\,a_2\,\ldots\,a_k)$ a $(b_1\,b_2\,\ldots\,b_l)$, tak je můžeme chápat jako složení dvou permutací. Jedna, která sestává z cyklu $(a_1\,a_2\,\ldots\,a_k)$ a fixuje všechny ostatní prvky množiny A a druhá, která sestává z cyklu $(b_1\,b_2\,\ldots\,b_l)$ a fixuje všechny zbývající prvky množiny A. Tyto dvě permutace podle Věty 7.2. komutují.

Inverzní permutace

Jestliže máme permutace π popsanou dvouřádkovou maticí, tak sestavení inverzní permutace π^{-1} je snadné. Stačí prohodit oba řádky matice. Z obrazů se stanou vzory zobrazení a naopak. Pro přehlednost zpravidla přeuspořádáme sloupce. Máme-li například permutaci

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 5 & 3 & 1 \end{pmatrix},$$

tak inverzní permutace je

$$\pi^{-1} = \begin{pmatrix} 2 & 4 & 5 & 3 & 1 \\ 1 & 2 & 3 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 4 & 2 & 3 \end{pmatrix}.$$

Jestliže máme permutaci π popsanou cyklem α, tak inverzní permutace je dána „opačným cyklem“ α^{-1}. Stačí zapsat prvky cyklu α v opačném pořadí a dostaneme inverzní permutaci α^{-1}. Opět pro přehlednost zápis cyklu zpravidla upravíme tak, aby začínal nejmenším prvkem. Vskutku, pokud $\alpha = (a_1\,a_2,\ \ldots\,a_n)$, tak složení s cyklem $(a_n\,a_{n-1}\,\ldots, a_1)$ ihned dává

$$(a_n\,a_{n-1}\,\ldots\,a_1) \circ (a_1\,a_2\,\ldots\,a_n) = (a_1)(a_2)\ldots(a_n) = \varepsilon.$$

Bez újmy na obecnosti stejně dopadne i složení v opačném pořadí, a proto $\alpha^{-1} = (a_n\,a_{n-1}\,\ldots, a_1)$.

Jestliže je permutace π dána více cykly, tj. platí $\pi = \alpha_1 \circ \alpha_2 \circ \ldots \circ \alpha_k$, tak podle Věty 2.8. (Věta o ponožkách a botách) ihned dostáváme $\pi^{-1} = \alpha_k^{-1} \circ \alpha_{k-1}^{-1} \circ \ldots \circ \alpha_1^{-1}$. Stačí tedy složit cykly v opačném pořadí a navíc v každém cyklu zapsat prvky v opačném pořadí. Jestliže jsou cykly navíc disjunktní, stačí dokonce jen opačné pořadí prvků každého cyklu a pořadí cyklů je libovolné.

Příklad 7.6. Mějme permutace $\varphi = (1\,2)(3\,4\,5)$, $\psi = (6\,7\,8)$ a $\tau = (1\,3\,5\,7)$ z Příkladu 7.4. Sestavíme inverzní permutace φ^{-1}, ψ^{-1} a τ^{-1}. Dále určíme inverzi ke složené permutaci $\tau \circ \psi$.
Při sestavení inverzní permutace φ^{-1} zapíšeme prvky cyklů v opačném pořadí, a protože cykly jsou disjunktní, nemusíme měnit pořadí cyklů. Dostaneme $\varphi^{-1} = (1\,2)(3\,5\,4)$. Podobně $\psi^{-1} = (6\,8\,7)$ a $\tau^{-1} = = (1\,7\,5\,3)$.

Protože známe inverze k permutacím ψ a τ, můžeme podle Věty 2.8. (Věta o ponožkách a botách) psát $(\tau\circ\psi)^{-1} = \psi^{-1}\circ\tau^{-1} = (6\,8\,7)\circ(1\,7\,5\,3) = (1\,6\,8\,7\,5\,3)$. Alternativně bychom mohli nejprve složit permutace $\tau\circ\psi = (1\,3\,5\,7)\circ(6\,7\,8) = (1\,3\,5\,7\,8\,6)$ a teprve potom najít inverzní permutaci, tj. zapsat prvky cyklů v opačném pořadí a zaměnit pořadí cyklů. Dostaneme $(\tau\circ\psi)^{-1} = (1\,3\,5\,7\,8\,6)^{-1} = (1\,6\,8\,7\,5\,3)$. ✓

Cykly délky 2 mají výjimečné postavení, bude jim věnována část Sekce 7.3. Všimněte si, že každý cyklus délky 2 je inverzní sám k sobě, platí $\alpha = (a_1\,a_2)$, $\alpha^{-1} = (a_2\,a_1) = (a_1\,a_2) = \alpha$. Proto je cyklus délky 2 permutací řádu 2 a $\alpha^2 = (a_1\,a_2)\circ(a_1\,a_2) = (a_1)(a_2) = \varepsilon$.

Cvičení

7.1.1. Najděte příklad dvou různých netriviálních cyklů na množině $A = \{1,2,3,4\}$, které a) nekomutují b) komutují c) komutují, třebaže nejsou disjunktní.

7.1.2. Najděte inverze k následujícím permutacím na množině $[1,10]$. a) $\pi = (1\,5\,3\,8)(2\,4\,9\,7\,6)$, b) $\rho = (1\,5)(2\,8)(3\,7\,4)$, c) $\sigma = (1\,2\,3\,4\,5\,6\,7\,8\,9\,10)$, d) $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 4 & 3 & 2 & 8 & 1 & 5 & 6 & 10 & 9 \end{pmatrix}$.

7.2. Řád permutace

Permutace α, která sestává z jediného cyklu délky n, je prvek řádu n v grupě $(S_n,\circ)$. Vskutku, je-li $\alpha = (a_1\,a_2\,\ldots\,a_n)$, tak nejmenší k, pro které platí $\alpha^k(a_1) = a_1$, je právě n, neboť $\alpha^k(a_1) = a_k \neq a_1$ pro $k = 1,2,\ldots,n-1$ a naopak $\alpha^n(a_i) = a_i$ pro každé $i = 1,2\ldots,n$.

Příklad 7.7. Mějme permutace $\psi = (6\,7\,8)$ a $\tau = (1\,3\,5\,7)$ z Příkladu 7.4. Určíme řády těchto prvků.
Protože $\psi^1 = (6\,7\,8) \neq \varepsilon$, $\psi^2 = \psi\circ\psi = (6\,8\,7) \neq \varepsilon$ a $\psi^3 = \varepsilon$, tak $|\psi| = 3$. Podobně, protože $\tau^1 = (1\,3\,5\,7) \neq \varepsilon$, $\tau^2 = (1\,5)(3\,7) \neq \varepsilon$, $\tau^3 = (1\,7\,5\,3) \neq \varepsilon$ a $\tau^4 = \varepsilon$, tak $|\tau| = 4$. ✓

Permutace ψ i τ jsou podle zadání prvky grupy S_{10}. Podle Cvičení 4.3.2. však víme, že řád prvku však nezávisí na grupě, podle Důsledku 6.4. řád permutace odpovídá řádu cyklické grupy, kterou generuje. Ukážeme, jak snadno určit řád každé permutace, nejen řád permutace, která sestává z jediného cyklu.

Příklad 7.8. Mějme permutaci $\varphi = (1\,2)(3\,4\,5)$ z Příkladu 7.4. Určíme její řád.
Snadno určíme mocniny permutace φ.

$$\varphi^1 = (1\,2)(3\,4\,5) \neq \varepsilon, \quad \varphi^2 = (3\,5\,4) \neq \varepsilon, \quad \varphi^3 = (1\,2) \neq \varepsilon, \quad \varphi^4 = (3\,4\,5) \neq \varepsilon, \quad \varphi^5 = (1\,2)(3\,5\,4) \neq \varepsilon$$

Teprve $\varphi^6 = (1) = \varepsilon$. Proto $|\varphi| = 6$.

Řád permutace φ můžeme určit také následující úvahou. Protože prvek 1 patří do cyklu délky 2, tak $\varphi^k(1) = 1$ pouze pokud k je násobkem čísla 2. A protože třeba prvek 5 patří do cyklu délky 3, tak $\varphi^k(5) = 5$ pouze pokud k je násobkem čísla 3. Proto řád permutace φ budou společným násobkem čísel 2 i 3 a nejmenší takovou mocninou, kde $\varphi^k = \varepsilon$, je právě 6. ✓

Následující tvrzení ukazuje, že pozorování z Příkladu 7.8. můžeme zobecnit. Řád permutace snadno určíme z délek jednotlivých cyklů.

Věta 7.3. Ruffiniho věta
Řád permutace konečné množiny, která je popsána pomocí disjunktních cyklů, je roven nejmenšímu společnému násobku délek jednotlivých cyklů.

Důkaz. Mějme permutaci $\sigma \in S_n$. Podle Věty 7.1. můžeme σ zapsat pomocí disjunktních cyklů. Délky jednotlivých cyklů označme $n_1, n_2, \ldots, n_\ell$. Užitím matematické indukce vzhledem k počtu disjunktních cyklů permutace ukážeme, že řád permutace $|\sigma| = \mathrm{NSN}(n_1, n_2, \ldots, n_\ell)$.
Základ indukce: Jestliže σ obsahuje jediný cyklus α délky n, tak řád $|\sigma| = n$ a tvrzení platí.
Indukční krok: Jestliže σ obsahuje více disjunktních cyklů, označme α libovolný z těchto cyklů a permutaci tvořenou zbývajícími cykly označme β. Permutace β sestává z méně než ℓ disjunktních cyklů a předpokládejme, že řád $|\beta|$ je nejmenší společný násobek délek těchto $\ell - 1$ cyklů.

Platí $\sigma = \alpha\circ\beta$, kde cyklus α a permutace β jsou tvořeny *disjunktními* cykly, bez újmy na obecnosti označme řád $|\alpha| = p$ a řád $|\beta| = q$. Dále označme $k = \mathrm{NSN}(p,q)$.

S využitím Věty 7.2. dostaneme $(\alpha\circ\beta)^k = \alpha^k\circ\beta^k = \varepsilon\circ\varepsilon = \varepsilon$, což podle Důsledku 6.5. znamená, že řád $|\alpha\circ\beta|$ dělí číslo k.

Označme řád $|\alpha\circ\beta| = t$. Ukážeme, že vskutku $t = k$. Platí $(\alpha\circ\beta)^t = \varepsilon$, a proto s využitím Věty 7.2. je $\alpha^t = \beta^{-t}$. Víme ale, že α a β jsou složeny z disjunktních cyklů a rovnost $\alpha^t = \beta^{-t}$ nastane jedině, když

jsou obě permutace totožné. S využitím Cvičení 4.3.8., podle kterého je $|\beta| = \left|\beta^{-1}\right|$ dostáváme $\alpha^t = \beta^{-t} = = \beta^t = \varepsilon$. To však současně znamená, že řád p cyklu α dělí t a podobně řád q permutace β dělí t. A tedy i $k = \mathrm{NSN}(p, q)$ dělí t. Dostáváme, že řád $t = k = \mathrm{NSN}(p, q)$, což je dokazované tvrzení.

Podle principu matematické indukce tvrzení platí pro libovolný počet disjunktních cyklů. □

Ruffiniho věta je silný nástroj. Nyní snadno určíme řád libovolné permutace π, což je současně řád prvku π v grupě permutací, a také řád příslušné cyklické grupy $\langle\pi\rangle$.

Příklad 7.9. Určíme řády všech prvků v symetrické grupě $(S_6, \circ)$.
S výhodou využijeme zápisu permutací pomocí cyklů. Třebaže grupa $(S_6, \circ)$ má 720 prvků, tak abychom určili všechny možné řády, bude stačit si rozmyslet, jaký může být zápis každého prvku grupy $(S_6, \circ)$ pomocí disjunktních cyklů. Máme následující možnosti, jak disjunktní cykly vypadají:

cyklus délky 6	permutace řádu 6,
cykly délky 5 a 1	permutace řádu 5,
cykly délky 4 a 2	permutace řádu 4,
cykly délky 4, 1 a 1	permutace řádu 4,
cykly délky 3 a 3	permutace řádu 3,
cykly délky 3, 2 a 1	permutace řádu 6,
cykly délky 3, 1 a 1	permutace řádu 3,
cykly délky 2, 2 a 2	permutace řádu 2,
cykly délky 2, 2, 1 a 1	permutace řádu 2,
cykly délky 2, 1, 1, 1 a 1	permutace řádu 2,
identická permutace s cykly délky 1	permutace řádu 1.

Každý prvek grupy $(S_6, \circ)$ je pouze některého z řádů 1, 2, 3, 4, 5, nebo 6. ✓

Všimněte si, že třebaže má grupa $(S_6, \circ)$ 720 různých prvků a číslo 720 má 30 různých dělitelů, tak každý prvek je pouze některého z šesti uvedených řádů. Podobně se dá ukázat, že v grupě $(S_7, \circ)$ je každý prvek některého z devíti různých řádů (Cvičení 7.2.2.). Další příklad ukazuje, že není těžké určit ani počet permutací nějakého pevně zvoleného řádu v dané grupě $(S_n, \circ)$.

Příklad 7.10. Navážeme na Příklad 7.9. a ukážeme, kolik je v symetrické grupě $(S_6, \circ)$ prvků řádu 3, prvků řádu 7 a prvků řádu 12.
Prvky řádu 3 jsou dvou druhů: jedná se jednak o permutace se dvěma cykly délky tři a jednak o permutace s jedním cyklem délky 3 a třemi cykly délky 1. Určíme počty permutací obou typů:

Permutací se dvěma 3-cykly je

$$\binom{6}{3} \cdot 2 \cdot 2 \cdot \frac{1}{2} = 40,$$

neboť prvky jednoho cyklu můžeme zvolit $\binom{6}{3}$ způsoby, každé tři prvky můžeme do cyklu seřadit dvěma způsoby (pořadí určuje jen orientaci cyklu) a nerozlišujeme vzájemné pořadí obou cyklů, proto dělíme 2.

Permutací s jedním 3-cyklem a třemi pevnými body je

$$\binom{6}{3} \cdot 2 = 40,$$

neboť prvky cyklu můžeme zvolit $\binom{6}{3}$ způsoby a seřadit tři prvky do cyklu můžeme dvěma způsoby (pořadí určuje jen orientaci cyklu). Pořadí zbývajících prvků je jednoznačné.

Celkem máme $40 + 40 = 80$ prvků řádu 3 mezi 720 prvky symetrické grupy $(S_6, \circ)$.

V grupě $(S_6, \circ)$ není žádný prvek řádu 7, neboť 7 nedělí řád grupy 720. Existence takového prvky by byla ve sporu s Lagrangeovou větou (Věta 4.10.).

V grupě $(S_6, \circ)$ neexistuje žádný žádný prvek řádu 12, třebaže 12 dělí řád grupy 720. Z šesti prvků nelze sestavit permutaci řádu 12, neboť z 6 prvků nelze sestavit cyklus délky 12 ani dva cykly délky 3 a 4, které by Podle Ruffiniho věta (Věta 7.3.) dávaly permutaci řádu 12. ✓

Cvičení

7.2.1. Určete, kolik je v symetrické grupě $(S_6, \circ)$ prvků řádu každého přípustného řádu.

7.2.2. Určete, jaké jsou řády prvků v symetrické grupě $(S_7, \circ)$.

7.2.3. Určete, kolik je v symetrické grupě $(S_7, \circ)$ prvků řádu 6.

7.2.4. Jakého nejvyššího řádu jsou prvky v grupě $(S_{10}, \circ)$?

7.2.5. Mějme funkci ř $: \mathbb{N} \to \mathbb{N}$, *která udává nejvyšší řád prvků v grupě* $(S_n, \circ)$. *Ukažte, že funkce* ř *je neklesající.*

7.2.6. Mějme permutaci $\pi = (1\,4\,2\,8)(3\,9\,7\,6\,5)$ *množiny* $[1, 9]$. *Určete a)* π^2, *b)* π^{142}.

7.3. Parita permutace

Parita celého čísla popisuje, zda je číslo sudé nebo liché („parita“ od slova „pár“).

Každou permutaci lze zapsat různými způsoby pomocí disjunktních cyklů. Zápis sice obecně není jednoznačný, můžeme však jednoznačně volit pořadí cyklů i zápis každého cyklu. V této kapitole ukážeme, že každou permutaci lze zapsat jako složení cyklů délky 2 (2-cyklů), které obecně nebudou disjunktní. Takový zápis sice také není jednoznačně určený, ukážeme ale, že jednoznačně určena parita počtu takových 2-cyklů.

Transpozice

Abychom popsali paritu permutace, zavedeme tzv. transpozici.

Definice Transpozice

Mějme permutaci τ grupy $(S_n, \circ)$. Permutace τ se nazývá *transpozice* právě tehdy, když tato permutace zamění pouze dva prvky a ostatní prvky jsou fixované, tj. $\tau(i) = j$, $\tau(j) = i$ a $\tau(k) = k$ pro $k \in [1, n] \setminus \{i, j\}$.

Transpozice existuje pouze na nosné množině s alespoň dvěma prvky, tedy v symetrické grupě S_n pro $n \geq 2$. Maticový zápis transpozice τ je

$$\tau = \begin{pmatrix} 1 & 2 & \dots & i-1 & i & i+1 & \dots & j-1 & j & j+1 & \dots & n \\ 1 & 2 & \dots & i-1 & j & i+1 & \dots & j-1 & i & j+1 & \dots & n \end{pmatrix}.$$

Jednodušší zápis transpozice je pomocí cyklů, neboť transpozice odpovídá právě 2-cyklu $(i\,j)$.

Příklad 7.11. Mějme permutaci σ popsanou maticí $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$. Permutaci zapíšeme jako složení tří transpozic.

Vezmeme tři transpozice (je zřejmé, že se jedná o transpozice)

$$\tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}, \quad \tau_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}, \quad \tau_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}.$$

Platí $\sigma = \tau_3 \circ \tau_2 \circ \tau_1$, neboť složením dostaneme

$$\tau_3 \circ \tau_2 \circ \tau_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \sigma.$$

✓

Ještě přehlednější je zápis Příkladu 7.11. pomocí cyklů.

Příklad 7.12. Mějme permutaci σ popsanou cyklem $\sigma = (1\,2\,3\,4)$. Permutaci zapíšeme jako složení tří 2-cyklů (transpozic).

Vezmeme tři 2-cykly (je zřejmé, že se jedná o transpozice) $\tau_1 = (1\,2), \tau_2 = (1\,3), \tau_3 = (1\,4)$. Platí $\sigma = \tau_3 \circ \tau_2 \circ \tau_1$, neboť složením dostaneme $\tau_3 \circ \tau_2 \circ \tau_1 = (1\,4) \circ (1\,3) \circ (1\,2) = (1\,2\,3\,4) = \sigma$. ✓

Transpozice permutace

Mějme permutaci π popsanou maticí

$$\pi = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ a_1 & a_2 & \dots & a_i & \dots & a_j & \dots & a_n \end{pmatrix},$$

kde prvky $a_1, a_2, \dots, a_n$ tvoří permutaci množiny $[1, n]$. Permutace π', kterou dostaneme záměnou jediné dvojice prvků permutace π, je „transpozicí permutace π“.

$$\pi' = \tau \circ \pi = \begin{pmatrix} 1 & 2 & \dots & i & \dots & j & \dots & n \\ a_1 & a_2 & \dots & a_j & \dots & a_i & \dots & a_n \end{pmatrix}$$

Symbolicky můžeme zapsat $\pi' = \tau \circ \pi$, kde τ je příslušná transpozice. Ukážeme, že každý cyklus délky n můžeme dostat pomocí $n-1$ postupných transpozic identity, a proto i každou permutaci můžeme dostat jako složení jistého počtu transpozic.

Příklad 7.13. Ukážeme, že cyklus $\alpha = (a_1, a_2, \ldots, a_n)$ můžeme zapsat jako složení $n-1$ transpozic.
Myšlenka vychází z řešení Příkladu 7.12. Mějme transpozice $\tau_1 = (a_1\, a_2)$, $\tau_2 = (a_1\, a_3)$, $\ldots$, $\tau_{n-1} = (a_1\, a_n)$. Jejich složením $\tau_n \circ \tau_{n-1} \circ \cdots \circ \tau_1$ dostaneme

$$\tau_n \circ \tau_{n-1} \circ \cdots \circ \tau_1 = (a_1\, a_n) \circ (a_1\, a_{n-1}) \circ \cdots \circ (a_1\, a_3) \circ (a_1\, a_2) = (a_1\, a_2\, \ldots\, a_{n-1}\, a_n) = \alpha.$$

Cyklus $\alpha = (a_1, a_2, \ldots, a_n)$ umíme zapsat pomocí transpozic, kdy postupně skládáme transpozice, které postupně prohodí prvek z pozice j s prvkem na pozici 1 následně prvek z pozice $j+1$ s prvkem na pozici 1 (kde byl prvek z pozice j). ✓

Příklad 7.14. Na straně 34 jsme popsali prvky dihedrální grupy $(D_3, \circ)$ jako permutace množiny vrcholů $\{A, B, C\}$. Ukážeme, že $(S_3, \circ) = (D_3, \circ)$ a ukážeme, jak jednotlivé symetrie zapsat pomocí transpozic.
Platí $S_3 = D_3$, neboť všech šest permutací množiny $\{A, B, C\}$ patří do D_3. Permutace

$$\begin{aligned}
R_0 &= \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix} = (A) = \varepsilon \\
R_{120} &= \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix} = (A\, B\, C) = (A\, C) \circ (A\, B) \\
R_{240} &= \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} = (A\, C\, B) = (A\, B) \circ (A\, C) \\
Z_A &= \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix} = (B\, C) \\
Z_B &= \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix} = (A\, C) \\
Z_C &= \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} = (A\, B)
\end{aligned}$$

Všimněte si, že všechny rotace sestávají ze sudého počtu transpozic, zatímco všechna zrcadlení sestávají z lichého počtu transpozic. ✓

Otázka: Je pravda, že přímé symetrie rovnostranného trojúhelníka (rotace) sestávají ze sudého počtu transpozic a nepřímé symetrie (zrcadlení) z lichého počtu transpozic?

Sudé a liché permutace

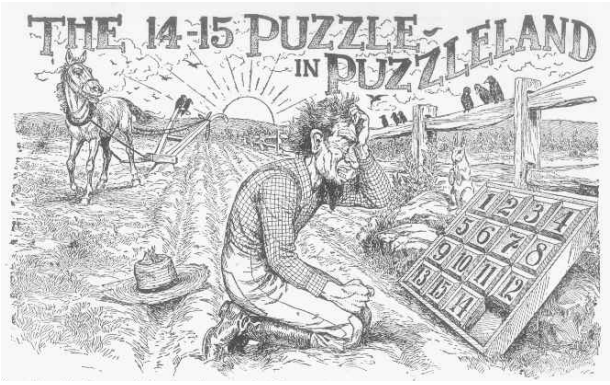
Počet transpozic a parita počtu těchto transpozic je důležitou vlastností, která má zajímavé praktické důsledky. Permutace se nazývá *sudá*, jestliže je možno ji napsat pomocí sudého počtu transpozic. Jinak se permutace nazývá *lichá*. Ve Větě 7.6. ukážeme, že definice je korektní a třebaže stejnou permutaci můžeme zapsat mnoha způsoby pomocí transpozic, parita počtu těchto transpozic zůstane zachována.

V některých knihách je parita permutace zavedena pomocí tzv. inverzí v permutaci.

Parita permutace může pomoci zdůvodnit nedosažitelnost některých rozmíchání kombinačních hlavolamů jako je Rubikova kostka nebo Loydova patnáctka, kterou jsme popsali v Sekci 1.3. na straně 39. Loydova patnáctka sestává z patnácti čtverečků umístěných do krabičky pro 4×4 čtverečky, přičemž čtverečky můžeme posouvat na sousední volnou pozici (Obrázek 7.2.). Všimněte si, že prázdný čtvereček hlavolamu můžeme vždy považovat za číslo 16 a řádky hlavolamy číst jako nějakou permutaci čísel $1, 2, \ldots, 16$.

Každým tahem posuneme na volné místo čtvereček ze sousedního políčka. Každým takovým přípustným tahem se změní parita p uvedené permutace: posuneme-li libovolný čtvereček v řádku na volné políčko, tak toto odpovídá jedné transpozici čtverečku s číslem 16, neboť dvojice sousedních čísel si prohodí místa; posuneme-li libovolný čtvereček ve sloupci na volné políčko, tak není těžké si rozmyslet, že takové transpozice jsme udělali tři – tři postupně transpozice se třemi čtverečky, které se nacházejí mezi oběma prohozenými místy čteno po řádcích.

Na druhou stranu vyjádříme-li součet q řádku a sloupce volného políčka hlavolamu (počítáno v taxikářské metrice například od posledního pole vpravo dole), tak každý tah změní paritu čísla q, neboť vždy se změní právě jedna souřadnice o jedničku.



Obrázek 7.2.: *Ilustrace Loydovy patnáctky z roku 1914.*

Nyní si všimneme, že každý tah zachová paritu součtu $p+q$, protože každý tah změní paritu obou sčítanců p i q. To znamená, že všechny pozice, ze kterých můžeme dosáhnout vyřešeného stavu hlavolamu pomocí přípustných tahů, mají stejnou paritu součtu $p+q$. Avšak stav, ve kterém prohodíme čtverečky na sousedních políčcích 14 a 15, odpovídá permutaci, která má *opačnou* paritu než vyřešený stav. Takové stavy nelze pomocí žádné posloupnosti přípustných tahů vyřešit.

Permutace pomocí transpozic

Nyní ukážeme, že transpozice mohou být jakýmsi stavebním kamenem libovolné permutace.

Věta 7.4. *Každá permutace v grupě $(S_n, \circ)$ může být zapsána pomocí transpozic (ne nutně disjunktních 2-cyklů).*

Důkaz. Podle Příkladu 7.13. víme, že každý cyklus $\alpha = (a_1\, a_2\, \ldots\, a_n)$ délky n umíme napsat jako složení $n-1$ transpozic. Platí, že $\alpha = (a_1\, a_2\, \ldots\, a_n) = (a_1\, a_n) \circ (a_1\, a_{n-1}) \circ \cdots \circ (a_1\, a_2)$, neboť obě permutace jsou shodné: platí $\alpha(a_1) = a_2$, $\alpha(a_2) = a_3$, $\ldots$, $\alpha(a_{n-1}) = a_n$.

Dále označme libovolnou permutaci $\sigma \in S_n$ množiny $[1, n]$. Podle Věty 7.1. umíme σ zapsat pomocí pomocí disjunktních cyklů. Každý tento cyklus umíme přepsat jako složení transpozic, a zopakováním postupu pro každý cyklus permutace σ napíšeme permutaci σ pomocí transpozic. □

Příklad 7.15. V Příkladu 1.1.2. na straně 37 jsme popsali prvky dihedrální grupy $(D_4, \circ)$ jako vybrané(!) permutace množiny vrcholů $\{A, B, C, D\}$. Ukážeme, jak symetrie čtverce zapsat pomocí transpozic.
Permutace z Příkladu 1.1.2. zapíšeme pomocí transpozic.

$$R_0 = \begin{pmatrix} A & B & C & D \\ A & B & C & D \end{pmatrix} = (A) = \varepsilon$$

$$R_{90} = \begin{pmatrix} A & B & C & D \\ B & C & D & A \end{pmatrix} = (A\,B\,C\,D) = (A\,D) \circ (A\,C) \circ (A\,B)$$

$$R_{180} = \begin{pmatrix} A & B & C & D \\ C & D & A & B \end{pmatrix} = (A\,C) \circ (B\,D)$$

$$R_{270} = \begin{pmatrix} A & B & C & D \\ D & A & B & C \end{pmatrix} = (A\,D\,C\,B) = (A\,B) \circ (A\,C) \circ (A\,D)$$

$$H = \begin{pmatrix} A & B & C & D \\ D & C & B & A \end{pmatrix} = (A\,D) \circ (B\,C)$$

$$V = \begin{pmatrix} A & B & C & D \\ B & A & D & C \end{pmatrix} = (A\,B) \circ (C\,D)$$

$$E = \begin{pmatrix} A & B & C & D \\ C & B & A & D \end{pmatrix} = (A\,C)$$

$$F = \begin{pmatrix} A & B & C & D \\ A & D & C & B \end{pmatrix} = (B\,D)$$

Všimněte si, že některé rotace sestávají z lichého počtu a některé ze sudého počtu transpozic. Podobně některá zrcadlení sestávají z lichého počtu a některá ze sudého počtu transpozic. ✓

Otázka: Je pravda, že přímé symetrie čtverce (rotace) sestávají ze sudého počtu transpozic a nepřímé symetrie (zrcadlení) z lichého počtu transpozic?

Lemma 7.5. *Pro identickou permutaci $\varepsilon = \beta_1 \circ \beta_2 \circ \cdots \circ \beta_r$ zapsanou pomocí transpozic (2-cyklů) $\beta_1, \beta_2, \ldots, \beta_r$ je číslo r udávající počet transpozic sudé.*

Důkaz. Mějme nosnou množinu $A = [1, n]$. Tvrzení ukážeme matematickou indukcí vzhledem k počtu transpozic r.
Základ indukce: Nejprve si uvědomíme, že $r > 1$, neboť jedna transpozice (2-cyklus) není identitou. Pro $r = 2$ tvrzení ihned platí, neboť $\varepsilon = \beta \circ \beta$ a proto dále předpokládáme, že $r \geq 3$.
Indukční krok: Předpokládejme, že je-li ε vyjádřeno pomocí menšího počtu transpozic (2-cyklů) než r, tak je počet 2-cyklů sudý. Je-li 2-cyklus $\beta_r = (a\,b)$, tak rozlišíme čtyři případy podle tvaru 2-cyklu β_{r-1}, přičemž vyžijeme pozorování, že pro každý 2-cyklus platí $(i\,j) = (j\,i)$.

1) Je-li $\beta_{r-1} \circ \beta_r = (a\,b) \circ (a\,b)$, tak $\beta_{r-1} \circ \beta_r = \varepsilon$ a tvrzení platí podle indukčního předpokladu.
2) Je-li $\beta_{r-1} \circ \beta_r = (a\,c) \circ (a\,b)$, tak upravíme $\beta_{r-1} \circ \beta_r = (a\,c) \circ (a\,b) = (a\,b) \circ (b\,c)$.
3) Je-li $\beta_{r-1} \circ \beta_r = (b\,c) \circ (a\,b)$, tak upravíme $\beta_{r-1} \circ \beta_r = (b\,c) \circ (a\,b) = (a\,c) \circ (c\,b)$.
4) A je-li $\beta_{r-1} \circ \beta_r = (c\,d) \circ (a\,b)$, tak cykly komutují a $\beta_{r-1} \circ \beta_r = (c\,d) \circ (a\,b) = (a\,b) \circ (c\,d)$.

V prvním případě se nám podařilo ε přepsat pomocí $r - 2$ transpozic (2-cyklů) a ve všech zbývajících třech případech byl prvek a přesunut do 2-cyklu s nižším indexem. Opakováním téhož postupu pro 2-cykly $\beta_{r-2} \circ \beta_{r-1}$ buď přesuneme prvek a do 2-cyklu β_{r-2}, nebo počet 2-cyklů snížíme o 2. A stačí si uvědomit, že takto bychom mohli prvek a přesunout do prvního (a jediného!) 2-cyklu β_1, což není možné, neboť ε je identická permutace, která prvek a fixuje (prvek a nemůže být v jediném 2-cyklu). Proto vždy dříve nebo později snížíme v zápisu identity počet transpozic (2-cyklů) o 2, což znamená, že r je sudé, stejně jako $r - 2$ podle indukčního předpokladu. □

Věta 7.6. *Pro každou permutaci α v grupě $(S_n, \circ)$, platí, že všechna vyjádření α zapsaná pomocí transpozic (2-cyklů) mají stejnou paritu, tj. je-li $\alpha = \beta_1 \circ \beta_2 \circ \cdots \circ \beta_r = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s$ tak r a s mají stejnou paritu.*

Důkaz. Levou i pravou stranu rovnosti

$$\beta_1 \circ \beta_2 \circ \cdots \circ \beta_r = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s$$

roznásobíme postupně prvky $\beta_r^{-1}, \beta_{r-1}^{-1}, \ldots, \beta_1^{-1}$ a dostaneme

$$\varepsilon = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s \circ \beta_r^{-1} \circ \beta_{r-1}^{-1} \circ \cdots \circ \beta_1^{-1}.$$

Protože 2-cykly jsou rovny své inverzi, dostaneme

$$\varepsilon = \gamma_1 \circ \gamma_2 \circ \cdots \circ \gamma_s \circ \beta_r \circ \beta_{r-1} \circ \cdots \circ \beta_1.$$

Podle Lemmatu 7.5. je ε sudá permutace, proto $r + s$ je sudé číslo. To znamená, že r i s jsou současně sudá nebo současně lichá čísla. □

Každá permutace má podle Věty 7.6. jednoznačně určenou paritu. Permutaci možno zapsat různým způsobem pomocí matic, počet transpozic může být pro různé zápisu různý, avšak vždy je počet transpozic sudý, nebo vždy lichý. Podobně tutéž permutaci je možno zapsat pomocí 2-cyklů (ne nutně disjunktních 2-cyklů) mnoha různými způsoby, avšak vždy má počet 2-cyklů stejnou paritu: je pro danou permutaci vždy sudý, nebo vždy lichý.

Alternující grupa

Podmnožinu všech sudých permutací symetrické grupy $(S_n, \circ)$ značíme A_n. Následující věta říká, že tato podmnožina grupy $(S_n, \circ)$ tvoří podgrupu $(A_n, \circ)$, které se říká *alternující grupa*.

Věta 7.7. *Množina sudých permutací A_n (permutací sudého řádu) množiny $[1, n]$ tvoří podgrupu $(A_n, \circ)$ v symetrické grupě $(S_n, \circ)$.*

Důkaz je ponechán jako Cvičení 7.3.5.

Příklad 7.16. Ukážeme, že alternující grupa $(A_n, \circ)$ je normální podgrupa symetrické grupy $(S_n, \circ)$.
Podle Věty 7.7. je grupa $(A_n, \circ)$ podgrupou $(S_n, \circ)$. Je-li $\sigma \in S_n$ libovolná permutace a $\pi \in A_n$ nějaká sudá permutace, tak složená permutace $\sigma \circ \pi \circ \sigma^{-1}$ je stejné parity jako permutace σ, neboť podle Cvičení 7.3.4. mají permutace σ i σ^{-1} stejnou paritu. To znamená, že $\sigma \circ \pi \circ \sigma^{-1} \in A_n$. Podle Věty 5.2. je $(A_n, \circ)$ normální podgrupa v $(S_n, \circ)$. ✓

Příklad 7.17. Ukážeme, že pro $n > 1$ je řád alternující grupy $(A_n, \circ)$ je $n!/2$.

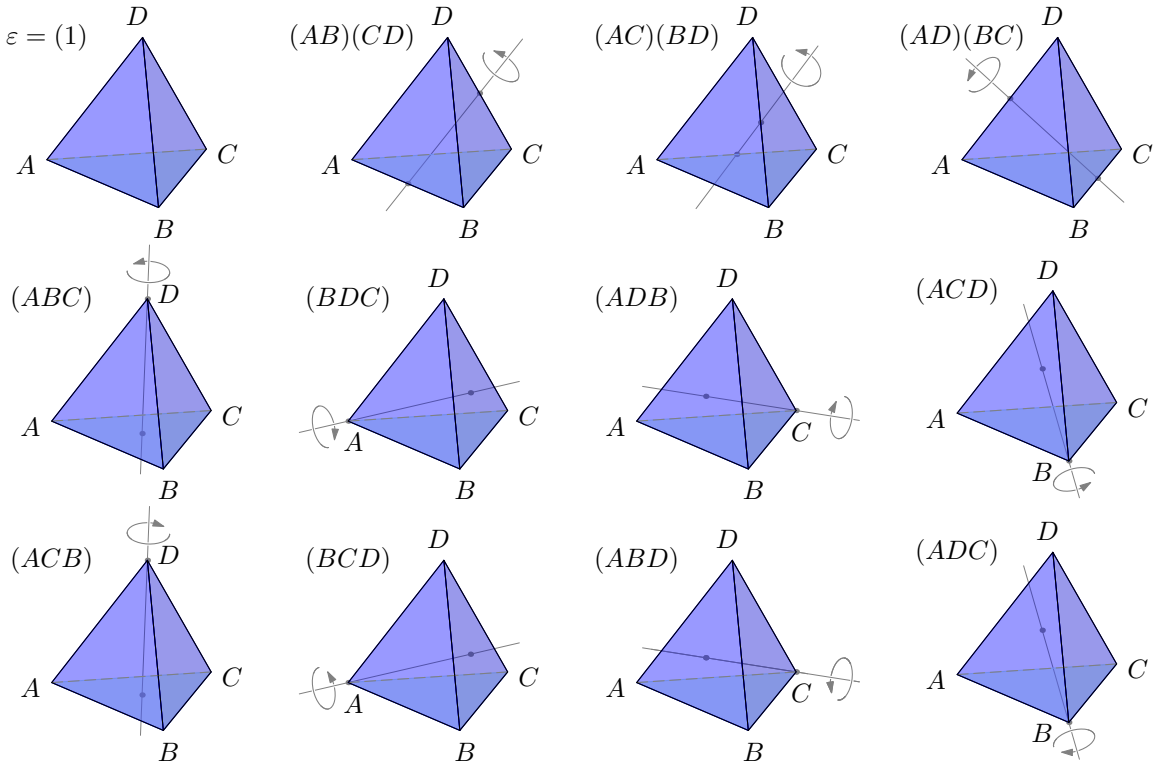
Ukážeme, že právě polovina permutací netriviální symetrické grupy je sudých a polovina je lichých. Podle Příkladu 7.16. je $(A_n, \circ)$ normální podgrupou $(S_n, \circ)$, a proto můžeme sestavit faktorovou grupu $(A_n/S_n, \circ)$. Tato faktorová grupa má dvě třídy rozkladu: sudé permutace A_n a liché permutace $S_n \setminus A_n$. Obě třídy rozkladu jsou podle Věty 4.9. stejně velké. Řád symetrické grupy $(S_n, \circ)$ je $n!$, proto $|A_n| = n!/2$. ✓

Otázky:

- Proč v Příkladu 7.17. požadujeme, aby symetrická grupa byla netriviální?
- Tvoří podmnožina všech lichých permutací podgrupu symetrické grupy $(S_n, \circ)$?

Všechna rozmíchání Rubikovy kostky můžeme popsat jako permutace množiny nálepek na kostce. Není těžké si rozmyslet, že otočení každé stěny odpovídá *sudé* permutaci nálepek, proto například není možné otáčením stěn kostky dosáhnout takového uspořádání, kde je pootočena jediná hranová kostka, neboť takové rozmíchání by odpovídalo *liché* permutaci nálepek.

Příklad 7.18. Popíšeme všechny přímé symetrie pravidelného čtyřstěnu. Ukážeme, že tvoří alternující grupu $(A_n, \circ)$.
Nejprve znázorníme všechny symetrie pravidelného čtyřstěnu (Obrázek 7.3.).



Obrázek 7.3.: *Symetrie pravidelného čtyřstěnu.*

Všimneme si, že každou z dvanácti symetrií je možno zapsat pomocí sudého počtu transpozic, přičemž se jedná právě o sudé permutace alternující grupy $(A_4, \circ)$ ✓

Cvičení

7.3.1. Mějme přirozené číslo n, $n \geq 2$. Ukažte, že pokud množina $K = \{(1\,i) : i \in [2, n]\}$, tak množina všech permutací generovaných množinou K je grupa všech permutací S_n n-prvkové množiny $[1, n]$.

7.3.2. Mějme přirozené číslo n, $n \geq 3$. Ukažte, že pokud množina $K = \{(1\,i\,j) : i, j \in [2, n]$ a současně $i \neq j\}$, tak množina všech permutací generovaných množinou K je grupa všech sudých permutací A_n n-prvkové množiny $[1, n]$.

7.3.3. Mějme permutaci σ, kde $\sigma \in S_n$. Jak vypadá zápis permutace σ^{-1}, jestliže σ je zapsána pomocí transpozic $\sigma = (a_1\,a_2)(a_3\,a_4)\ldots(a_{m-1}a_m)$?

7.3.4. Mějme permutaci $\sigma \in S_n$. Ukažte, že inverzní permutace σ^{-1} a) má stejnou paritu jako permutace σ, b) řád permutace σ^{-1} je stejný jako řád permutace σ.

7.3.5. Dokažte Větu 7.7., že množina sudých permutací A_n množiny $[1,n]$ tvoří podgrupu $(A_n,\circ)$ v symetrické grupě $(S_n,\circ)$.

7.3.6. Najděte všechny cyklické alternující grupy $(A_n,\circ)$.

7.3.7. Mějme permutaci π množiny $[1,n]$. Určete a) jaký je nejmenší a b) jaký je největší počet inverzí v permutaci π.

7.3.8. Ukažte, že alternující grupa $(A_8,\circ)$ obsahuje prvek řádu 15.

7.3.9. Ukažte, že grupa symetrií krychle je právě symetrická grupa S_4.

7.3.10. Ukažte, že grupa symetrií pravidelného osmistěnu je právě symetrická grupa S_4.

Kapitola 8. Homomorfismy grup

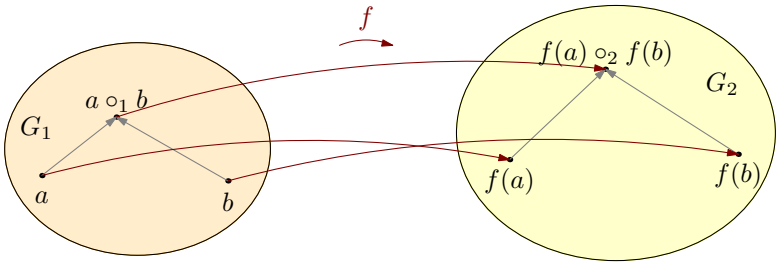
V této kapitole se budeme věnovat jednomu z ústředních témat teorie grup – homomorfismům. Název pochází z latiny, kdy „homo“ znamená „stejný“ a „morphe“ znamená „tvar“. Ukážeme, že homomorfismy jsou šikovným nástrojem pro analýzu struktur grup i pro popis jisté podobnosti grup. Homomorfismy jsou přirozeným zobecněním izomorfismů, kterým bude věnována Kapitola 9.

V předchozích kapitolách jsme často narazili na příklady různých grup, které měly stejnou strukturu. Například dihedrální grupa $(D_3, \circ)$ odpovídá symetrické grupě $(S_3, \circ)$. Na druhou stranu, dihedrální grupa $(D_3, \circ)$ má jinou strukturu než grupa $(\mathbb{Z}_6, +)$. Nyní těmto úvahám dáme formální rámec.

8.1. Definice homomorfismu grup

Homomorfismus bude takové zobrazení jedné grupy do druhé, které zachová operaci.

Definice Mějme grupy $(G_1, \circ_1)$ a $(G_2, \circ_2)$. Zobrazení $f : G_1 \to G_2$ nazveme *homomorfismem grupy* $(G_1, \circ_1)$ *do grupy* $(G_2, \circ_2)$ právě tehdy, když zachovává operaci, tj. pro každé $a, b \in G_1$ platí $f(a \circ_1 b) = f(a) \circ_2 f(b)$. Grupě $(G_1, \circ_1)$ říkáme *levá* grupa a grupě $(G_2, \circ_2)$ *pravá* grupa homomorfismu f.



Obrázek 8.1.: *Homomorfismus f grupy $(G_1, \circ_1)$ do grupy $(G_2, \circ_2)$ zachovává operaci.*

Připomeňme, že bijektivní zobrazení $f : A \to B$ je takové zobrazení množiny A do množiny B, které je současně prosté a současně na (injektivní a současně surjektivní). Všimněte si, že homomorfismus *nemusí* být ani injekce, ani surjekce, ani bijekce.

Příklad 8.1. Uvedeme několik jednoduchých příkladů grupových homomorfismů.

1) Zobrazení $f : \mathbb{Z} \to \mathbb{Z}$ definované předpisem $f(x) = 0$ je homomorfismus grupy $(\mathbb{Z}, +)$ do grupy $(\mathbb{Z}, +)$.
2) Zobrazení f definované předpisem $f(x) = |x|$ je homomorfismus grupy $(\mathbb{R} \setminus \{0\}, \cdot)$ do grupy $(\mathbb{R} \setminus \{0\}, \cdot)$.
3) Zobrazení f definované předpisem $f(x) = x^2$ je homomorfismus grupy $(\mathbb{R} \setminus \{0\}, \cdot)$ do grupy $(\mathbb{R} \setminus \{0\}, \cdot)$.
4) Zobrazení $f : \mathbb{Z} \to \mathbb{Z}_n$ definované předpisem $f(z) = z \bmod n$ (celému číslu z přiřadíme zbytek po dělení čísla z číslem n) je homomorfismus grupy $(\mathbb{Z}, +)$ do grupy $(\mathbb{Z}_n, +)$.
5) Zobrazení $f : M^*_{n,n} \to \mathbb{R}$ definované předpisem $f(A) = \det(A)$ je homomorfismus grupy čtvercových metic $(M_{n,n}, \cdot)$ do grupy $(\mathbb{R} \setminus \{0\}, \cdot)$.

Příklad 8.2. Uvedeme několik jednoduchých příkladů zobrazení, která nejsou grupovým homomorfismem.

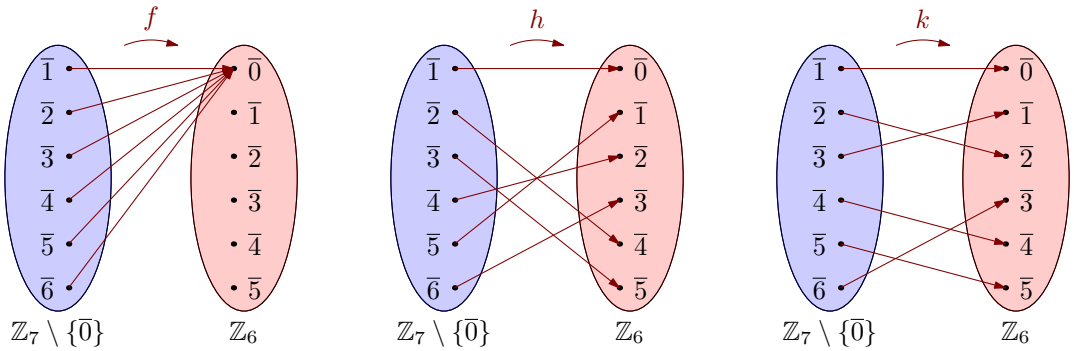
1) Zobrazení $f : \mathbb{Z} \to \mathbb{Z}$ definované předpisem $f(x) = 1$ není homomorfismus grupy $(\mathbb{Z}, +)$ do grupy $(\mathbb{Z}, +)$, neboť nezachovává operaci. Například $f(2) = 1$, avšak $f(1 + 1) \neq f(1) + f(1) = 1 + 1 = 2$.
2) Zobrazení f definované předpisem $f(x) = |x|$ není homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{R}, +)$, neboť nezachovává operaci Platí $f(1) = 1$, avšak $f(-2 + 3) \neq f(-2) + f(3) = 2 + 3 = 5$.
3) Zobrazení f definované předpisem $f(x) = x^2$ není homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{R}, +)$. Zobrazení nezachovává operaci, neboť například $f(8) = 64$, avšak $f(4 + 4) \neq f(4) + f(4) = 16 + 16 = 32$.
4) Zobrazení $\sin(x)$ není homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{R}, +)$. Zobrazení nezachovává operaci, neboť například $\sin(\pi) = 0$, avšak $\sin(\frac{\pi}{2} + \frac{\pi}{2}) \neq \sin(\frac{\pi}{2}) + \sin(\frac{\pi}{2}) = 1 + 1 = 2$.

Příklad 8.3. Mějme grupy $(\mathbb{R}^+, \cdot)$ a $(\mathbb{R}, +)$ (podle Příkladu 2.17. víme, že se jedná o grupy). Zobrazení $f : \mathbb{R}^+ \to \mathbb{R}$ definované předpisem $f(x) = \ln x$ je homomorfismus grupy $(\mathbb{R}^+, \cdot)$ do grupy $(\mathbb{R}, +)$.

Ověříme, že zobrazení f splňuje definici homomorfismu. Mějme $x, y \in \mathbb{R}^+$. Pak platí $f(x) + f(y) = \ln x + \ln y = \ln(x \cdot y) = f(x \cdot y)$. ✓

Příklad 8.4. Mějme grupy $(\mathbb{R}, +)$ a $(\mathbb{R}^+, \cdot)$. Zobrazení $f : \mathbb{R} \to \mathbb{R}^+$ definované předpisem $f(x) = 5^x$ je homomorfismus grupy $(\mathbb{R}, +)$ do grupy $(\mathbb{R}^+, \cdot)$.
Ověříme, že zobrazení f splňuje definici homomorfismu. Mějme $x, y \in \mathbb{R}$. Pak platí $f(x) \cdot f(y) = 5^x \cdot 5^y = 5^{(x+y)} = f(x + y)$. ✓

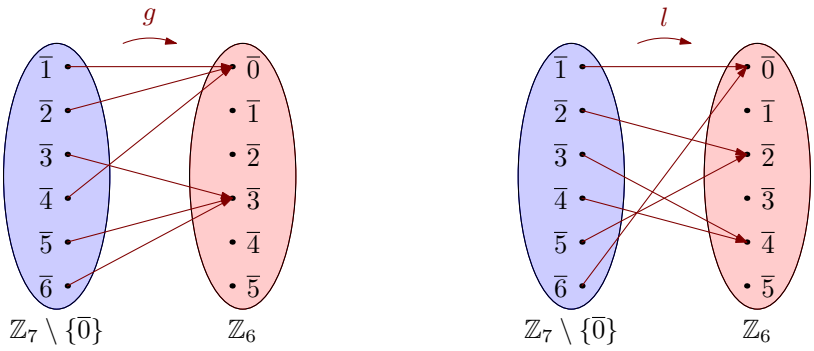
Příklad 8.5. Najdeme pět různých homomorfismů grupy $(\mathbb{Z}_7 \setminus \{\overline{0}\}, \cdot)$ do grupy $(\mathbb{Z}_6, +)$.
Triviální homomorfismus f, který každému prvku grupy $(\mathbb{Z}_7 \setminus \{\overline{0}\}, \cdot)$ přiřadí prvek $\overline{0}$ grupy $(\mathbb{Z}_6, +)$ je homomorfismem, neboť pro každé $a, b \in \mathbb{Z}_7 \setminus \{\overline{0}\}$ platí $f(a \cdot b) = \overline{0} = \overline{0} + \overline{0} = f(a) + f(b)$ (Obrázek 8.2. vlevo).



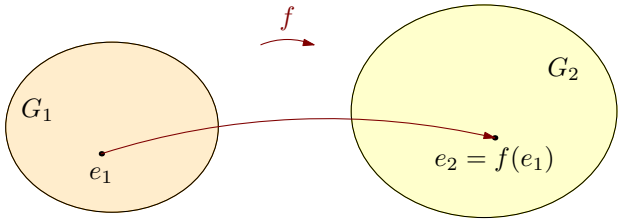
Obrázek 8.2.: *Různé homomorfismy grupy* $(\mathbb{Z}_7 \setminus \{\overline{0}\}, \cdot)$ *do grupy* $(\mathbb{Z}_6, +)$.

Dále zobrazení h dané rovnostmi $h(\overline{1}) = \overline{0}$, $h(\overline{2}) = \overline{4}$, $h(\overline{3}) = \overline{5}$, $h(\overline{4}) = \overline{2}$, $h(\overline{5}) = \overline{1}$, $h(\overline{6}) = \overline{3}$ je homomorfismem, neboť obraz součinu dvou libovolných prvků je vždy roven součtu obrazů jednotlivých prvků (Obrázek 8.2. uprostřed). Například $h(\overline{3} \cdot \overline{6}) = h(\overline{4}) = \overline{2}$ a současně $h(\overline{3}) + h(\overline{6}) = \overline{5} + \overline{3} = \overline{8} = \overline{2}$, neboť $8 \equiv 2 \pmod 6$. Obecně využijeme faktu, že $\overline{1} = \overline{5^0}$, $\overline{2} = \overline{5^4}$, $\overline{3} = \overline{5^5}$, $\overline{4} = \overline{5^2}$, $\overline{5} = \overline{5^1}$, $\overline{6} = \overline{5^3}$ modulo 7 a obecně $h(\overline{5^i}) = \overline{i}$. Potom $h(\overline{5^i} \cdot \overline{5^j}) = h(\overline{5^{i+j}}) = \overline{i + j}$, kde součet počítáme modulo 6 a současně $h(\overline{5^i}) + h(\overline{5^j}) = \overline{i} + \overline{j}$ modulo 6.

Analogicky můžeme zavést i zobrazení k dané rovnostmi $k(\overline{1}) = \overline{0}$, $k(\overline{2}) = \overline{2}$, $k(\overline{3}) = \overline{1}$, $k(\overline{4}) = \overline{4}$, $k(\overline{5}) = \overline{5}$, $k(\overline{6}) = \overline{3}$, které vychází z pozorování, že $\overline{1} = \overline{3^0}$, $\overline{2} = \overline{3^2}$, $\overline{3} = \overline{3^1}$, $\overline{4} = \overline{3^4}$, $\overline{5} = \overline{3^5}$, $\overline{6} = \overline{3^3}$ a obecně $k(\overline{3^i}) = \overline{i}$ (Obrázek 8.2. vpravo). Zobrazení k je opět homomorfismem, neboť obraz součinu dvou libovolných prvků je vždy roven součtu obrazů jednotlivých prvků. Platí $k(\overline{3^i} \cdot \overline{3^j}) = k(\overline{3^{i+j}}) = \overline{i + j}$, kde součet počítáme modulo 6 a současně $k(\overline{3^i}) + k(\overline{3^j}) = \overline{i} + \overline{j}$ modulo 6. Například $k(\overline{3} \cdot \overline{6}) = k(\overline{4}) = \overline{4}$ a současně $k(\overline{3}) + k(\overline{6}) = \overline{1} + \overline{3} = \overline{4}$.



Obrázek 8.3.: *Další homomorfismy grupy* $(\mathbb{Z}_7 \setminus \{\overline{0}\}, \cdot)$ *do grupy* $(\mathbb{Z}_6, +)$.



Obrázek 8.4.: *Homomorfismus f grupy $(G_1, \circ_1)$ do grupy $(G_2, \circ_2)$ zachovává neutrální prvek.*

Také zobrazení g dané rovnostmi $g(\overline{1}) = g(\overline{2}) = g(\overline{4}) = \overline{0}$ a $g(\overline{3}) = g(\overline{5}) = g(\overline{6}) = \overline{3}$ je homomorfismem (Obrázek 8.3. vlevo) a zobrazení l dané rovnostmi $l(\overline{1}) = l(\overline{6}) = \overline{0}$, $l(\overline{2}) = l(\overline{5}) = \overline{2}$ a $l(\overline{3}) = l(\overline{4}) = \overline{4}$ je homomorfismem (Obrázek 8.3. vpravo). Důkaz je ponechán jako Cvičení 8.1.1. ✓

Upozorněme, že homomorfismy f, g, l v předchozím příkladu nejsou bijekce (ani injekce nebo surjekce), zatímco homomorfismy h i k jsou bijektivní homomorfismy.

Obraz neutrálního prvku

Všimněte si, že v každém homomorfismu v Příkladu 8.5. se neutrální prvek první grupy zobrazil na neutrální prvek druhé grupy. Následující věta říká, že tomu tak musí být vždy (Obrázek 8.4.).

Věta 8.1. *Mějme neutrální prvek e_1 grupy $(G_1, \circ_1)$ a neutrální prvek e_2 grupy $(G_2, \circ_2)$. Jestliže zobrazení $f : G_1 \to G_2$ je homomorfismus grupy $(G_1, \circ_1)$ do grupy $(G_2, \circ_2)$, pak $f(e_1) = e_2$.*

Důkaz. Pro každé $a \in G_1$ platí

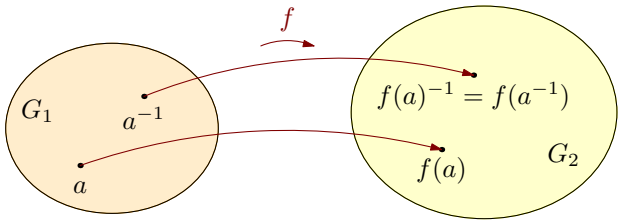
$$f(a) \circ_2 f(e_1) = f(a \circ_1 e_1) = f(a) = f(a) \circ_2 e_2.$$

První rovnost vychází z definice homomorfismu. Druhá rovnost platí, protože e_1 je neutrálním prvkem grupy $(G_1, \circ_1)$. Třetí rovnost platí, protože e_2 je neutrálním prvkem grupy $(G_2, \circ_2)$. V grupě $(G_2, \circ_2)$ platí zákony o krácení (Věta 2.6.), proto můžeme (zleva) vykrátit prvkem $f(a)$. Dostaneme $f(e_1) = e_2$. □

Příklad 8.6. Mějme grupy $(G_1, \circ_1)$ a $(G_2, \circ_2)$. Neutrální prvek grupy $(G_2, \circ_2)$ označme e. Ukážeme, že zobrazení $f : G_1 \to G_2$ definované pro každé $a \in G_1$ předpisem $f(a) = e$ je homomorfismus grupy grupy $(G_1, \circ_1)$ do grupy $(G_2, \circ_2)$. Tomuto homomorfismu se říká *triviální* homomorfismus.
Ověříme, že zobrazení f splňuje definici homomorfismu. Mějme $x, y \in G_1$. Pak platí $f(x) \circ_1 f(y) = e \circ_2 e = e = f(x \circ_1 y)$. ✓

Obrazy inverzních prvků

Dále ukážeme, že pro libovolný homomorfismus f dvou grup obraz inverze prvku je inverze obrazu prvku, tj. je-li $f(a)$ obraz prvku a, tak $f(a)^{-1}$ je obrazem prvku a^{-1} (Obrázek 8.5.).



Obrázek 8.5.: *Homomorfismus f grupy $(G_1, \circ_1)$ do grupy $(G_2, \circ_2)$ zachovává inverze.*

Věta 8.2. *Mějme homomorfismus $f : G_1 \to G_2$ grupy $(G_1, \circ_1)$ do grupy $(G_2, \circ_2)$. Potom pro každé $a \in G_1$ platí $f(a_{G_1}^{-1}) = (f(a))_{G_2}^{-1}$.*

Důkaz. Dle definice inverze pro každé $a \in G_1$ platí $a \circ_1 a^{-1} = e_1$ a $a^{-1} \circ_1 a = e_1$, kde e_1 je neutrální prvek grupy $(G_1, \circ_1)$. Neutrální prvek grupy $(G_2, \circ_2)$ označme e_2. Nyní s využitím definice homomorfismu a předchozí Věty 8.1. dostaneme

$$f(a_{G_1}^{-1}) \circ_2 f(a) = f(a_{G_1}^{-1} \circ_1 a) = f(e_1) = e_2.$$

Podobně vyjde

$$f(a) \circ_2 f(a_{G_1}^{-1}) = f(a \circ_1 a_{G_1}^{-1}) = f(e_1) = e_2.$$

To znamená, že podle definice inverzního prvku je prvek $f(a_{G_1}^{-1})$ inverzní k prvku $f(a)$ v grupě $(G_2, \circ_2)$, a proto platí $(f(a))_{G_2}^{-1} = a_{G_1}^{-1}$. □

Příklad 8.7. Mějme homomorfismus $f(x) = \log_2 x$ grupy $(\mathbb{R}^+, \cdot)$ do grupy $(\mathbb{R}, +)$. Například platí $f(4) = \log_2(4) = 2$ a současně obraz inverze je $f(4^{-1}) = \log_2(4^{-1}) = -\log_2(4) = -2$. Prvek -2 je opačným k prvku 2 v grupě $(\mathbb{R}, +)$.

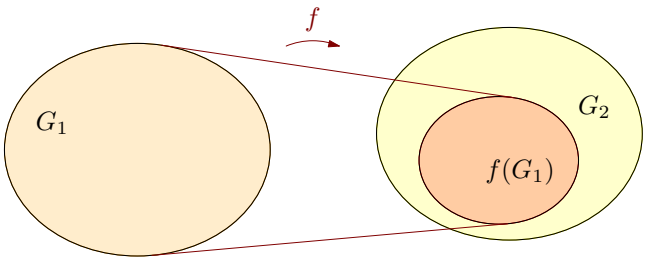
Příklad 8.8. V homomorfismu h z Příkladu 8.5. porovnáme obrazy prvků a obrazy jejich inverzí. Platí

$$\begin{aligned} h(1) &= 0, & h(1^{-1}) &= h(1) = 0 = -0, \\ h(2) &= 4, & h(2^{-1}) &= h(4) = 2 = -4, \\ h(3) &= 5, & h(3^{-1}) &= h(5) = 1 = -5, \\ h(4) &= 2, & h(4^{-1}) &= h(2) = 4 = -2, \\ h(5) &= 1, & h(5^{-1}) &= h(3) = 5 = -1, \\ h(6) &= 3, & h(6^{-1}) &= h(6) = 3 = -3, \end{aligned}$$

což odpovídá tvrzení $f(a_{G_1}^{-1}) = (f(a))_{G_2}^{-1}$ z Věty 8.2. ✓

Obraz grupy

Už víme, že neutrální prvek levé grupy se v každém homomorfismu zobrazí na neutrální prvek pravé grupy, a dále víme, že obraz inverze je inverze obrazu. Nyní ukážeme, že v každém homomorfismu tvoří množina všech obrazů prvků levé grupy podgrupu v pravé grupě (Obrázek 8.6.).



Obrázek 8.6.: *Obraz grupy* $(G_1, \circ_1)$ *je podgrupa v grupě* $(G_2, \circ_2)$.

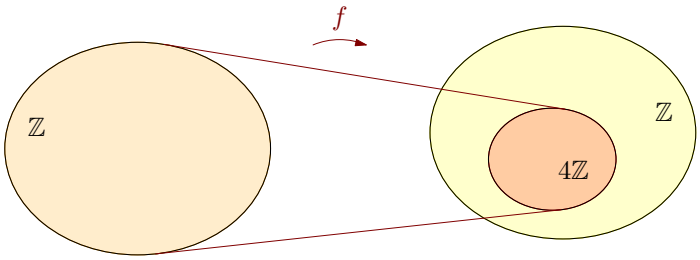
Věta 8.3. *Mějme homomorfismus* $f : G_1 \to G_2$ *grupy* $(G_1, \circ_1)$ *do grupy* $(G_2, \circ_2)$. *Označme* $f(G_1) = \{f(a) : a \in G_1\}$. *Potom* $(f(G_1), \circ_2)$ *je podgrupa grupy* $(G_2, \circ_2)$.

Důkaz. Ověříme předpoklady Věty 3.3. (Testu podgrupy).

(i) Jistě platí, že množina $f(G_1)$ je podmnožinou v G_2.
(ii) Neutrální prvek e_2 grupy $(G_2, \circ_2)$ podle Věty 8.1. do $f(G_1)$ patří, protože $f(e_1) = e_2$. Množina $f(G_1)$ je proto neprázdná.
(iii) Ověříme uzavřenost operace „$\circ_2$“. Pro každé $f(a), f(b) \in G_2$ platí s využitím vlastnosti homomorfismu $f(a) \circ_2 f(b) = f(a \circ_1 b)$ a $f(a \circ_1 b) \in f(G_1)$, proto $(f(G_1), \circ_2)$ je grupoid.
(iv) Podle Věty 8.2. pro každé $f(a) \in f(G_1)$ existuje v $f(G_1)$ inverze, neboť platí $(f(a))^{-1} = f(a^{-1})$ a $f(a^{-1}) \in f(G_1)$.

Podle Věty 3.3. je $(f(G_1), \circ_2)$ podgrupou v grupě $(G_2, \circ_2)$. □

Příklad 8.9. Mějme zobrazení $f : \mathbb{Z} \to \mathbb{Z}$ dané předpisem $f(x) = 4x$. Ukážeme, že f je homomorfismus grupy $(\mathbb{Z}, +)$ do grupy $(\mathbb{Z}, +)$. To současně znamená, že $(4\mathbb{Z}, +) = (f(\mathbb{Z}), +)$ je podgrupa grupy $(\mathbb{Z}, +)$. Ověříme definici homomorfismu. Pro každé $a, b, \in \mathbb{Z}$ platí $f(a+b) = 4(a+b) = 4a+4b = f(a)+f(b)$. Využili jsme známý vztah pro celá čísla $4(a+b) = 4a+4b$. To znamená, že zobrazení f je opravdu homomorfismus.



Obrázek 8.7.: *Homomorfismus f grupy $(\mathbb{Z},+)$ do grupy $(4\mathbb{Z},+)$.*

Uvědomte si, že $f(\mathbb{Z}) = \{4a : a \in \mathbb{Z}\} = 4\mathbb{Z}$. Podle Věty 8.3. je proto $(4\mathbb{Z},+) = (f(\mathbb{Z}),+)$ podgrupa grupy $(\mathbb{Z},+)$ (Obrázek 8.7.). ✓

Otázky:

- Mějme dvě grupy $(G_1,\circ_1)$ a $(G_2,\circ_2)$ a zobrazení $f : G_1 \to G_2$. Jestliže f není homomorfismus, bude $(f(G_1),\circ_2)$ grupoid?
- Mějme dvě grupy $(G_1,\circ_1)$ a $(G_2,\circ_2)$ a zobrazení $f : G_1 \to G_2$. Jestliže f není homomorfismus, které vlastnosti grupy mohou být pro $(f(G_1),\circ_2)$ porušeny?
- Mějme dvě grupy $(G_1,\circ_1)$ a $(G_2,\circ_2)$ a zobrazení $f : G_1 \to G_2$. Jestliže f není homomorfismus, může být $(f(G_1),\circ_2)$ podgrupa v $(G_2,\circ_2)$?

Příklad 8.10. Mějme grupy $(\mathbb{R}\setminus\{0\},\cdot)$ a $(\mathbb{R}^+,\cdot)$. Podle Příkladu 2.17. víme, že se vskutku jedná o grupy. Ukážeme, že a) zobrazení $f : \mathbb{R}\setminus\{0\} \to \mathbb{R}^+$ dané předpisem $f(x) = |x|$ je homomorfismus grupy $(\mathbb{R}\setminus\{0\},\cdot)$ do grupy $(\mathbb{R}^+,\cdot)$, b) zobrazení f je surjektivní homomorfismus c) a nakonec prověříme, zda zobrazení f je injektivní.

a) Ověříme, zda zobrazení f je homomorfismus $\mathbb{R}\setminus\{0\} \to \mathbb{R}^+$. Pro každé $x, y \in \mathbb{R}\setminus\{0\}$ platí $f(x\cdot y) = |x\cdot y| = |x|\cdot|y| = f(x)\cdot f(y)$, proto je zobrazení f homomorfismus.

b) Homomorfismus f je surjektivní, neboť pro každé $a \in \mathbb{R}^+$ najdeme jeho vzor v množině $\mathbb{R}\setminus\{0\}$. Vzorem je prvek a, platí $f(a) = |a| = a$.

c) Homomorfismus f není injektivní, protože například $f(8) = f(-8) = 8$. ✓

Cvičení

8.1.1. Ukažte, že a) zobrazení g, b) zobrazení l z Příkladu 8.5. jsou homomorfismy.

8.1.2. Určete, zda zobrazení $f : \mathbb{R} \to \mathbb{R}$ dané předpisem $f(x) = x + 1$ je homomorfismus grupy $(\mathbb{R},+)$ do grupy $(\mathbb{R},+)$.

8.1.3. Určete, zda zobrazení $f : \mathbb{R} \to \mathbb{R}$ dané předpisem $f(x) = 2x$ je homomorfismus grupy $(\mathbb{R},+)$ do grupy $(\mathbb{R},+)$.

8.1.4. Určete, zda zobrazení $f : \mathbb{Z}_5 \to \mathbb{Z}_5$ dané předpisem $f(z) = 2x \bmod 5$ (číslu $2x$ přiřadíme zbytek po dělení čísla $2x$ číslem 5) je homomorfismus grupy $(\mathbb{Z}_5,+)$ do grupy $(\mathbb{Z}_5,+)$.

8.1.5. Mějme surjektivní homomorfismus f grupy $(G_1,\circ_1)$ do grupy $(G_2,\circ_2)$. Ukažte, že je-li operace „$\circ_1$“ komutativní, je také operace „$\circ_2$“ komutativní.

8.1.6. Jak se změní tvrzení Cvičení 8.1.5., pokud homomorfismus f není surjektivní?

8.1.7. Mějme surjektivní homomorfismus f grupy $(G_1,\circ_1)$ do grupy $(G_2,\circ_2)$. Dokažte nebo vyvraťte: je-li operace „$\circ_2$“ komutativní, je také operace „$\circ_1$“ komutativní.

8.1.8. Mějme grupy $(\mathbb{R}\setminus\{0\},\cdot)$ a $(\mathbb{R},+)$. Podle Příkladu 2.17. víme, že se vskutku jedná o grupy. Ukažte, že a) zobrazení $f : \mathbb{R}\setminus\{0\} \to \mathbb{R}$ dané předpisem $f(x) = \ln|x|$ je homomorfismus grupy $(\mathbb{R}\setminus\{0\},\cdot)$ do grupy $(\mathbb{R},+)$. b) Dále zjistěte, zda je zobrazení f surjektivní, a c) zda je zobrazení f injektivní.

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

Tabulka 8.1.: Cayleyho tabulka podgrupy $(\{0,2,4\},+)$.

8.1.9. Najděte nějaký netriviální homomorfismus grupy určené Tabulkou 8.1. do dihedrální grupy $(D_3,\circ)$. *Ověřte vlastnosti homomorfismu. Pokud žádný takový homomorfismus neexistuje, dokažte to.*

8.1.10. Mějme homomorfismus f *grupy* $(G_1,\circ_1)$ *do grupy* $(G_2,\circ_2)$ *a prvek* $a\in G_1$. *Dokažte nebo vyvraťte: řád prvku* $f(a)$ *je stejný jako řád prvku* a.

8.1.11. Mějme homomorfismus f *grupy* $(G_1,\circ_1)$ *do grupy* $(G_2,\circ_2)$ *a prvek* $a\in G_1$. *Dokažte nebo vyvraťte: řád prvku* $f(a)$ *je dělitelem řádu prvku* a.

8.1.12. Najděte nějaký netriviální homomorfismus dihedrální grupy $(D_3,\circ)$ *do grupy určené Tabulkou 8.1. Ověřte vlastnosti homomorfismu. Pokud žádný takový homomorfismus neexistuje, dokažte to.*

8.1.13. Mějme komutativní grupu $(G,\cdot)$. *Definujeme zobrazení* $f: G\to G$ *předpisem* $f(a)=a^{-1}$ *pro každé* $a\in G$. *a) Ukažte, že* f *je homomorfismus. b) Platí tvrzení i pro nekomutativní grupy?*

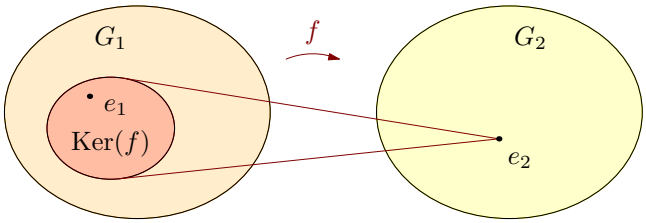
8.1.14. Ukažte, že pokud grupa* $(G,\cdot)$ *není komutativní, tak zobrazení* f *ze Cvičení 8.1.13. nikdy není homomorfismus.*

8.2. Jádro homomorfismu

Ukážeme, že jisté vybrané prvky z levé množiny homomorfismu tvoří podgrupu v levé grupě.

Definice Mějme grupu $(G_1,\circ_1)$ a grupu $(G_2,\circ_2)$ s neutrálním prvkem e_2. Mějme homomorfismus $f: G_1\to G_2$ grupy $(G_1,\cdot)$ do grupy $(G_2,\circ_2)$. *Jádrem homomorfismu* f nazveme množinu $\mathrm{Ker}(f)=\{g_1\in G_1 : f(g_1)=e_2\}$.

Všimněte si, že neutrální prvek grupy $(G_1,\circ_1)$ vždy do jádra homomorfismu patří. Někdy však do jádra patří i další prvky (Obrázek 8.8.).



Obrázek 8.8.: *Jádro homomorfismu* f *grupy* $(G_1,\circ_1)$ *do grupy* $(G_2,\circ_2)$.

Příklad 8.11. Uveďme několik jednoduchých příkladů jader homomorfismů.

1) Lineární zobrazení $a: V_1\to V_2$ vektorových prostorů je homomorfismus grup vektorů s operací sčítaní vektorů. Jádro lineárního zobrazení a budou prvky v levé grupě, které se zobrazí na neutrální prvek (nulový vektor) pravé grupy.
2) V homomorfismu grupy $(\mathbb{R}^+,\cdot)$ do grupy $(\mathbb{R},+)$ daném předpisem $f(x)=\ln x$ je jednoprvkové jádro $\mathrm{Ker}(f)=\{1\}$.
3) Mějme homomorfismus grup $(\mathbb{C}\setminus\{0\},\cdot)$ do sebe daném předpisem $f(z)=z^n$, kde n je přirozené číslo. Zobrazení f je surjektivní homomorfismus a jádro $\mathrm{Ker}(f)$ má n prvků: n odmocnin komplexního čísla 1.
4) Jádro homomorfismu $f:\mathbb{Z}\to\mathbb{Z}$ grupy $(\mathbb{Z},+)$ do grupy $(\mathbb{Z},+)$ definovaného předpisem $f(x)=0$ je $\mathrm{Ker}(f)=\mathbb{Z}$.
5) Jádro triviálního homomorfismu $f: G_1\to G_2$ grupy $(G_1,\circ_1)$ do grupy $(G_2,\circ_2)$ daného předpisem $f(x)=e_2$, kde e_2 je neutrální prvek pravé grupy, je celý nosič G_1.
6) Homomorfismus f grupy $(\mathbb{R}\setminus\{0\},\cdot)$ do grupy $(\mathbb{R}\setminus\{0\},\cdot)$ definovaný předpisem $f(x)=|x|$ má jádro $\mathrm{Ker}(f)=\{-1,1\}$.

7) Homomorfismus f grupy $(\mathbb{R}\setminus\{0\},\cdot)$ do grupy $(\mathbb{R}\setminus\{0\},\cdot)$ definovaný předpisem $f(x)=x^2$ má jádro $\mathrm{Ker}(f)=\{-1,1\}$.
8) Jádro homomorfismu $f:\mathbb{Z}\to\mathbb{Z}_n$ grupy $(\mathbb{Z},+)$ do grupy $(\mathbb{Z}_n,+)$ definovaného předpisem $f(x)=x+n\mathbb{Z}$ je $\mathrm{Ker}(f)=n\mathbb{Z}$.
9) Zobrazení $f:M_{n,n}^*\to\mathbb{R}$ definované předpisem $f(A)=\det(A)$ je homomorfismus grupy regulárních čtvercových matic $(M_{n,n}^*,\cdot)$ do grupy $(\mathbb{R}\setminus\{0\},\cdot)$. Do jádra patří všechny regulární matice s determinantem 1.
10) Mějme $\alpha\in\mathbb{R}$. Zobrazení $f:\mathbb{R}^2\to\mathbb{R}^2$ definované předpisem $f((x,y))=(x\cos\alpha-\sin\alpha, x\sin\alpha+{}+\cos\alpha)$ je homomorfismus grupy uspořádaných dvojic reálných čísel $(\mathbb{R}^2,+)$ do grupy $(\mathbb{R}^2,+)$. Do jádra patří prvek $(0,0)$, který si můžeme představit jako střed $(0,0)$ při transformaci bodů roviny otočením o úhel α.

Jádro je normální podgrupa

Nyní ukážeme, že množina prvků jádra spolu s restrikcí operace levé grupy je podgrupa, která je dokonce normální podgrupou levé grupy.

Věta 8.4. *Mějme homomorfismus $f:G_1\to G_2$ grupy $(G_1,\circ_1)$ do grupy $(G_2,\circ_2)$. Potom $(\mathrm{Ker}(f),\circ_1)$ je normální podgrupa grupy $(G_1,\circ_1)$.*

Důkaz. Nejprve užitím Věty 3.3. (Testu podgrupy) dokážeme, že $(\mathrm{Ker}(f),\circ_1)$ je podgrupa grupy $(G_1,\circ_1)$ (Obrázek 8.8.).

(i) Jádro $\mathrm{Ker}(f)$ je jistě podmnožina G_1 z definice jádra $\mathrm{Ker}(f)$.
(ii) Jádro není nikdy prázdné, neboť do $\mathrm{Ker}(f)$ jistě patří neutrální prvek e_1, protože podle Věty 8.1. platí $f(e_1)=e_2$.
(iii) Operace „$\circ_1$“ je na $\mathrm{Ker}(f)$ uzavřená, protože pro každé $g_1,g_2\in\mathrm{Ker}(f)$ platí $f(g_1\circ_1 g_2)=f(g_1)\circ_2 f(g_2)=e_2\circ_2 e_2=e_2$. To znamená, že $g_1\circ_1 g_2\in\mathrm{Ker}(f)$.
(iv) A konečně ke každému prvku z $\mathrm{Ker}(f)$ najdeme v $\mathrm{Ker}(f)$ inverzi. Podle Věty 8.2. pro každé $a\in\mathrm{Ker}(f)$ platí $f(a_{G_1}^{-1})=(f(a_{G_1}))_{G_2}^{-1}=(e_2)_{G_2}^{-1}=e_2$. Zápisem $(f(a_{G_1}))_{G_2}^{-1}$ chceme zdůraznit, že se jedná o inverzi v pravé grupě. To znamená, že $a^{-1}\in\mathrm{Ker}(f)$.

Zbývá ukázat, že podgrupa $(\mathrm{Ker}(f),\circ_1)$ je normální. Využijeme Větu 5.2. (Test normální podgrupy), která říká, že pro každé $z\in G_1$ platí $x\circ_1\mathrm{Ker}(f)=\mathrm{Ker}(f)\circ_1 x$ (neboli jádro je normální podgrupa) právě tehdy, když pro každé $x\in G_1$ a každé $h\in\mathrm{Ker}(f)$ platí $x\circ_1 h\circ_1 x_{G_1}^{-1}\in\mathrm{Ker}(f)$. Nyní s využitím definice homomorfismu pro každé $x\in G_1$ a pro každé $h\in\mathrm{Ker}(f)$ platí

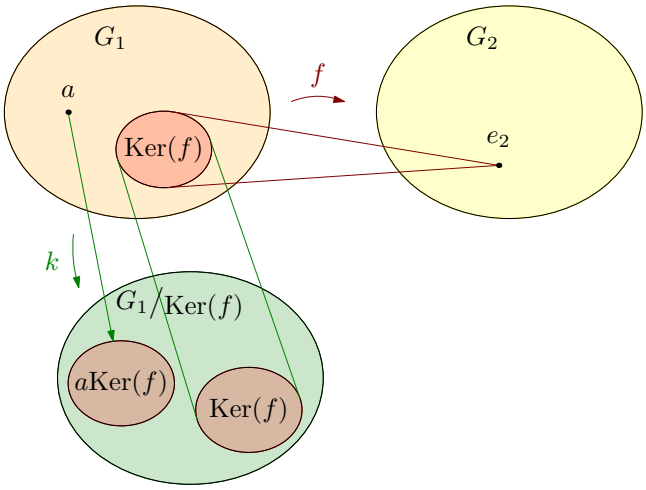
$$\begin{aligned}f(x\circ_1 h\circ_1 x^{-1})&=f(x)\circ_2 f(h\circ_1 x^{-1})=f(x)\circ_2 f(h)\circ_2 f(x^{-1})=\\&=f(x)\circ_2 e_2\circ_2 f(x^{-1})=f(x)\circ_2 f(x^{-1})=f(x)\circ_2 (f(x))_{G_2}^{-1}=e_2.\end{aligned}$$

To podle Věty 5.2. znamená, že prvek $x\circ_1 h\circ_1 x^{-1}\in\mathrm{Ker}(f)$ a to znamená, že jádro $(\mathrm{Ker}(f),\circ_1)$ je normální podgrupa v grupě $(G_1,\circ_1)$. □

Věta 8.4. říká, že najdeme-li nějaký homomorfismus grupy $(G_1,\circ_1)$ do nějaké grupy, tak vždy můžeme podle Věty 5.1. tvořit rozklady grupy $(G_1,\circ_1)$ podle jádra homomorfismu $\mathrm{Ker}(f)$ (Obrázek 8.9.). Můžeme sestavit faktorovou grupu levé grupy.

Na straně 96 jsme zavedli úmluvu, že operaci na faktorové grupě budeme značit stejným symbolem jako operaci na grupě. Protože nyní pracujeme se třemi operacemi (operace v levé grupě, v pravé grupě a ve faktorové grupě), tak v několika následujících tvrzeních budeme pro dobré porozumění operaci na faktorové grupě odlišovat čárkou.

Důsledek 8.5. *Mějme homomorfismus $f:G_1\to G_2$ grupy $(G_1,\circ_1)$ do grupy $(G_2,\circ_2)$. Potom platí, že $(G_1/\mathrm{Ker}(f),\circ_1')$ je (faktorová) grupa.*



Obrázek 8.9.: *Faktorová grupa* $(G_1/\mathrm{Ker}(f), \circ_1')$.

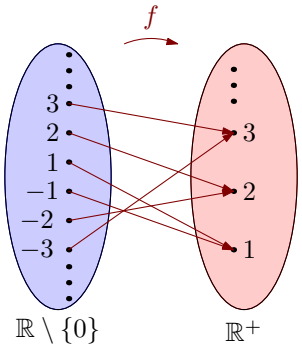
Příklad 8.12. Uveďme několik jednoduchých příkladů faktorových grup homomorfismů.

1) Faktorová grupa homomorfismu $f : \mathbb{Z} \to \mathbb{Z}$ grupy $(\mathbb{Z}, +)$ do grupy $(\mathbb{Z}, +)$ definovaného předpisem $f(x) = 0$ je grupa $(G, +)$, kde $G = \{\{a\} : a \in \mathbb{Z}\}$.
2) Faktorová grupa homomorfismus f grupy $(\mathbb{R} \setminus \{0\}, \cdot)$ do grupy $(\mathbb{R} \setminus \{0\}, \cdot)$ definovaného předpisem $f(x) = x^2$ je grupa $(G, \cdot)$, kde $G = \{\{a, -a\} : a \in \mathbb{R} \setminus \{0\}$.
3) Faktorová grupa homomorfismu $f : \mathbb{Z} \to \mathbb{Z}_n$ grupy $(\mathbb{Z}, +)$ do grupy $(\mathbb{Z}_n, +)$ definovaného předpisem $f(x) = x + n\mathbb{Z}$ je grupa $(n\mathbb{Z}, +)$.

Příklad 8.13. Navážeme na Příklad 8.10. Máme grupy $(\mathbb{R}\setminus\{0\}, \cdot)$ a $(\mathbb{R}^+, \cdot)$ a homomorfismus $f : \mathbb{R}\setminus\{0\} \to \mathbb{R}^+$ daný předpisem $f(x) = |x|$. Najdeme jádro $\mathrm{Ker}(f)$ a sestavíme rozklad $\mathbb{R} \setminus \{0\}/\mathrm{Ker}(f)$.
Homomorfismus f je na Obrázku 8.10. Jádro homomorfismu f je množina všech prvků levé grupy $(\mathbb{R}\setminus\{0\}, \cdot)$, které se zobrazí na neutrální prvek 1 pravé grupy $(\mathbb{R}^+, \cdot)$. Platí $\mathrm{Ker}(f) = \{x \in \mathbb{R}\setminus\{0\} : f(x) = 1\} = \{-1, 1\}$, neboť rovnice $|x| = 1$ má dvě řešení $x = 1$ a $x = -1$. Jádro $\{-1, 1\}$ homomorfismu f tvoří podle Věty 8.4. normální podgrupu v $(\mathbb{R} \setminus \{0\}, \cdot)$, jen proto můžeme vytvořit faktorovou grupu. Platí

$$(\mathbb{R} \setminus \{0\})/\mathrm{Ker}(f) = \{a \cdot \mathrm{Ker}(f) : a \in \mathbb{R} \setminus \{0\}\} = \{a \cdot \{-1, 1\} : a \in \mathbb{R} \setminus \{0\}\} = \{\{-a, a\} : a \in \mathbb{R} \setminus \{0\}\}$$

a faktorová grupa je $((\mathbb{R} \setminus \{0\})/\mathrm{Ker}(f), \cdot)$. ✓



Obrázek 8.10.: *Homomorfismus* $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}^+$ *daný předpisem* $f(x) = |x|$.

Kanonický homomorfismus

V předchozí části jsme na základě homomorfismu dvou grup uměli najít normální podgrupu levé grupy. Nyní ukážeme, že pokud máme v grupě $(G,\cdot)$ normální podgrupu $(H,\cdot)$, tak umíme sestavit homomorfismus grupy $(G,\cdot)$ do faktorové grupy podle normální podgrupy $(G/H,\cdot\prime)$ (Obrázek 8.11.).

Věta 8.6. Kanonický homomorfismus

Mějme grupu $(G,\cdot)$ a její normální podgrupu $(H,\cdot)$. Potom zobrazení $k : G \to G/H$ dané pro každé $a \in G$ předpisem $k(a) = a \odot H$ je surjektivní homomorfismus grupy $(G,\cdot)$ do grupy $(G/H,\cdot\prime)$.

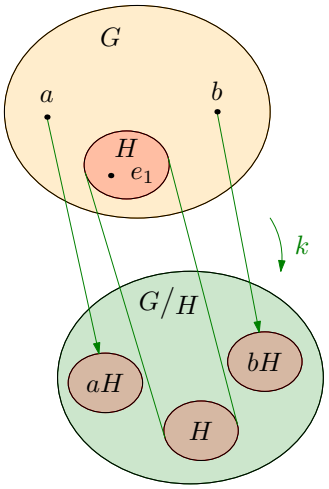
Důkaz. Uvedený homomorfismus k se nazývá *kanonický homomorfismus* a proto jej značíme k. Nejprve ukážeme, že zobrazení k je homomorfismus. Pro každé $a, b \in G$ platí

$$k(a \cdot b) = (a \cdot b) \odot H.$$

Dále podle Věty 5.1. o násobení tříd rozkladu na G/H a podle definice kanonického homomorfismu víme, že platí

$$(a \cdot b) \odot H = (a \odot H) \cdot\prime (b \odot H) = k(a) \cdot\prime k(b),$$

proto je zobrazení k homomorfismus.



Obrázek 8.11.: *Kanonický homomorfismus.*

Surjektivita homomorfismu k je zřejmá, neboť vzorem prvku $x \cdot\prime H$ v zobrazení k je prvek x. Pro každé $a \cdot H \in G/H$ vezmeme $a \in G$ a platí $k(a) = a \odot H$. Tím jsme ukázali, že $k : G \to G/H$ je surjektivní homomorfismus. □

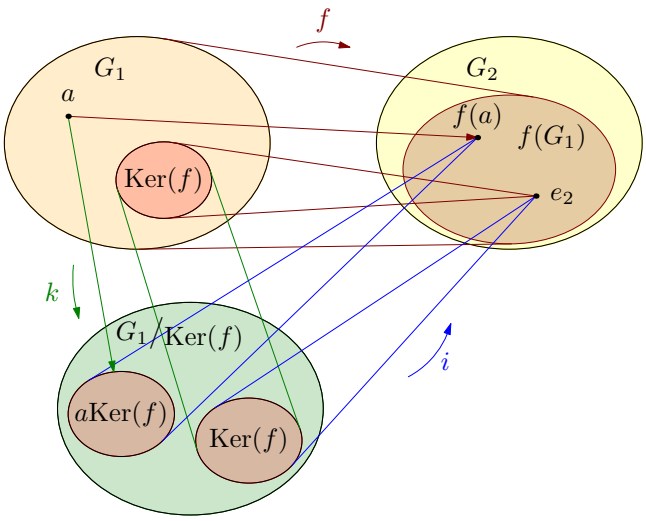
Spojením tvrzení Vět 8.4. a 8.6. ihned dostaneme následující důsledek.

Důsledek 8.7. *Mějme homomorfismus $f : G_1 \to G_2$ grupy $(G_1,\circ_1)$ do grupy $(G_2,\circ_2)$. Potom existuje surjektivní homomorfismus grupy $(G_1,\circ_1)$ do grupy $(G_1/\mathrm{Ker}(f),\circ_1\prime)$.*

Hledaným surjektivním homomorfismem je právě kanonický homomorfismus k, neboť pro každé $a \in G$ platí $k(a) = a \circ_1 H$. Kanonický homomorfismus je na Obrázky 8.11. a je vyznačený už na Obrázku 8.9. „Kanonický“ se mu říká proto, že se jedná o nejpřirozenější homomorfismus, který můžeme z grupy $(G,\cdot)$ do faktorové grupy $(G/H,\cdot\prime)$ definovat – každému prvku $a \in G$ přiřadíme právě třídu aH.

První věta o izomorfismech

Nyní ukážeme další důležité tvrzení, jehož první formulace pochází již z roku 1870 od Camillea Jordana. Najdeme homomorfismus mezi faktorovou grupu $(G_1/\mathrm{Ker}(f),\circ_1\prime)$ a (pod)grupou $(f(G_1),\circ_2)$. Tento homomorfismus bude dokonce bijekce! Ukážeme, že třídě $a \cdot\prime \mathrm{Ker}(f)$ odpovídá přesně prvek $f(a)$ v podgrupě



Obrázek 8.12.: *Izomorfismus i mezi $(G_1/\mathrm{Ker}(f), \circ_1\prime)$ a $(f(G_1), \circ_2)$.*

$(f(G_1), \cdot)$. To znamená, že bude existovat bijektivní homomorfismus (izomorfismus) mezi $(G_1/\mathrm{Ker}(f), \cdot\prime)$ a $(f(G_1), \circ_2)$ (Obrázek 8.12.).

Věta 8.8. První věta o izomorfismech
Mějme homomorfismus $f : G_1 \to G_2$ grupy $(G_1, \circ_1)$ do grupy $(G_2, \circ_2)$. Potom existuje bijektivní homomorfismus (izomorfismus) grupy $(G_1/\mathrm{Ker}(f), \circ_1\prime)$ do grupy $(f(G_1), \circ_2)$.

Důkaz. Ukážeme, že zobrazení $i : (G_1/\mathrm{Ker}(f), \circ_1\prime) \to (f(G_1), \circ_2)$ dané pro každé $a \in G_1$ předpisem $i(a \circ_1 \mathrm{Ker}(f)) = f(a)$ je hledaný izomorfismus (Obrázek 8.12.).

Nejprve ukážeme korektnost definice zobrazení i, tj. že se opravdu jedná o zobrazení. Musíme ukázat, že v zobrazení i nedostaneme pro stejný prvek $a\,\mathrm{Ker}(f)$ (rozuměj stejnou třídu rozkladu) různé obrazy, jestliže v zobrazení i vezmeme různé reprezentanty třídy $a\,\mathrm{Ker}(f)$. Předpokládejme, že $a_1 \circ_1 \mathrm{Ker}(f) = a_2 \circ_1 \mathrm{Ker}(f)$. Chceme ukázat, že $f(a_1) = f(a_2)$. Vyjdeme z předpokladu

$$a_1 \circ_1 \mathrm{Ker}(f) = a_2 \circ_1 \mathrm{Ker}(f).$$

Nyní ale pro každé $x \in (a_1 \circ_1 \mathrm{Ker}(f))$ existuje takové $h_1 \in \mathrm{Ker}(f)$, že $x = a_1 \circ_1 h_1$ a podobně protože $x \in (a_2 \circ_1 \mathrm{Ker}(f))$ existuje $h_2 \in \mathrm{Ker}(f)$ takové, že $x = a_2 \circ_1 h_2$. Z rovnosti $x = a_1 \circ_1 h_2 = a_2 \circ_1 h_2$ dostaneme $a_1 = a_2 \circ_1 h_2 \circ_1 h_2^{-1}$, proto existuje takové $h \in \mathrm{Ker}(f)$, že $a_1 = a_2 \circ_1 h$. Nyní z této rovnosti a definice homomorfismu platí

$$f(a_1) = f(a_2 \circ_1 h) = f(a_2) \circ_2 f(h) = f(a_2) \circ_2 e_2 = f(a_2),$$

kde e_2 je neutrální prvek pravé grupy. Tím jsme ukázali korektnost definice zobrazení i.

Nyní ukážeme, že zobrazení i je homomorfismus. Připomeňme, že z definice zobrazení i víme, že obraz $i(c \circ_1 \mathrm{Ker}(f)) = f(c)$. Potom z vlastnosti operace „$\circ_1\prime$“ dostaneme

$$i((a \circ_1 \mathrm{Ker}(f)) \circ_1\prime (b \circ_1 \mathrm{Ker}(f))) = i((a \circ_1 b) \circ_1\prime \mathrm{Ker}(f)) = f(a \circ_1 b),$$

což z definice homomorfismu f dává

$$f(a \circ_1 b) = f(a) \circ_2 f(b) = i(a \circ_1 \mathrm{Ker}(f)) \circ_2 i(b \circ_1 \mathrm{Ker}(f)).$$

Tím jsme ukázali, že i je homomorfismus grupy $(G/\mathrm{Ker}(f), \circ_1)$ do grupy $(G_2, \circ_2)$.

Zbývá ukázat, že i je bijektivní homomorfismus. Nejprve ukážeme, že zobrazení i je injektivní. Postupujeme nepřímo. Předpokládejme, že $i(a \circ_1 \mathrm{Ker}(f)) = i(b \circ_1 \mathrm{Ker}(f))$. To znamená, že $f(a) = f(b)$. Rovnost zůstane zachována, i když ji zprava „pronásobíme“ v druhé grupě prvkem $f(b^{-1})$. Dostaneme

$$f(a) \circ_2 f(b^{-1}) = f(b) \circ_2 f(b^{-1}).$$

Podle věty o inverzním prvku (Věta 8.2.) platí $f(b^{-1}) = f(b)^{-1}$, dosadíme a dostaneme

$$f(b) \circ_2 f(b^{-1}) = f(b) \circ_2 f(b)^{-1} = e_2$$

a podle definice homomorfismu f můžeme psát

$$f(a) \circ_2 f(b^{-1}) = f(a \circ_1 b^{-1}) = e_2.$$

To ale znamená, že prvek $a \circ_1 b^{-1}$ patří do jádra homomorfismu f. Označme $h = a \circ_1 b^{-1}$, kde $h \in \mathrm{Ker}(f)$, proto $a = h \circ_1 b$. Nyní můžeme psát

$$a \circ_1 \mathrm{Ker}(f) = h \circ_1 b \circ_1 \mathrm{Ker}(f).$$

S využitím normálnosti jádra dostaneme

$$h \circ_1 b \circ_1 \mathrm{Ker}(f) = h \circ_1 \mathrm{Ker}(f) \circ_1 b = \mathrm{Ker}(f) \circ_1 b = b \circ_1 \mathrm{Ker}(f),$$

čímž dostáváme $a \circ_1 \mathrm{Ker}(f) = b \circ_1 \mathrm{Ker}(f)$.

A konečně ukážeme, že homomorfismus i je surjektivní zobrazení. Pro každé $f(a) \in f(G_1)$ je v homomorfismu i vzorem třída $(a \circ_1 \mathrm{Ker}(f)) \in G_1/\mathrm{Ker}(f)$, neboť podle definice zobrazení i platí $i(a \circ_1 \mathrm{Ker}(f)) = f(a)$. Zobrazení i je bijektivní homomorfismus. □

Podle První věty o izomorfismech (Věta 8.8.) není z pohledu homomorfismu rozdíl, zda máme podgrupu $(f(G_1), \circ_2)$ pravé grupy $(G_2, \circ_2)$ nebo faktorovou grupu $(G_1/\mathrm{Ker}(f), \circ_1\prime)$. Místo grupy $(f(G_1), \circ_2)$, jejíž prvky jsou svázány operací „$\circ_2$“, můžeme pracovat s faktorovou grupou $(G_1/\mathrm{Ker}(f), \circ_1\prime)$, jejíž prvky jsou třídy rozkladu G_1/H svázané operací „$\circ_1\prime$“, a naopak. Celý proces je ilustrován posloupností Příkladů 8.10., 8.13. a následujícího Příkladu 8.14.

Příklad 8.14. Navážeme na Příklad 8.13. Máme grupy $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{R}^+, \cdot)$, homomorfismus $f : \mathbb{R} \setminus \{0\} \to \mathbb{R}^+$ daný předpisem $f(x) = |x|$ a faktorovou grupu $(G_1/\mathrm{Ker}(f), \circ_1\prime)$. Ukážeme, které grupy jsou izomorfní ve smyslu Věty 8.8.

Násobení komplexů na množině $G_1/\mathrm{Ker}(f)$ je operace. Platí

$$(a \cdot \mathrm{Ker}(f)) \cdot (b \cdot \mathrm{Ker}(f)) = ((a \cdot b) \cdot \mathrm{Ker}(f)).$$

Například $\{-a, a\} \cdot \{-b, b\} = \{-ab, ab\}$.

Grupa $(\mathbb{R}^+, \cdot)$ je obvyklé násobení kladných reálných čísel. Násobení absolutních hodnot reálných čísel lze chápat dvojím způsobem: jednak mezi obrazy homomorfismu platí

$$|r| \cdot |s| = |rs|$$

a jednak ve faktorové grupě platí

$$\{-r, r\} \cdot \{-s, s\} = \{-rs, rs\}.$$

Jedná se o jinak zapsané stejné tvrzení. ✓

Příklad 8.15. Ukážeme, že homomorfismus f grupy $(G_1, \circ_1)$ do grupy $(G_2, \circ_2)$ je injektivní právě tehdy, když jádro obsahuje pouze neutrální prvek, tj. $\mathrm{Ker}(f) = \{e_1\}$.

Tvrzení má tvar ekvivalence, ukážeme obě implikace.

„⇒“ Postupujeme nepřímo. Ukážeme, že pokud $\mathrm{Ker}(f) \neq \{e_1\}$, tak daný homomorfismus nemůže být injektivní.

Víme, že $\mathrm{Ker}(f) \neq \{e_1\}$, tj. existuje takové $a \in G_1$, pro které platí $a \neq e_1$. Potom ale $f(a) = e_2$, kde e_2 je neutrální prvek pravé grupy, protože $a \in \mathrm{Ker}(f)$ a tedy $f(a) = f(e_1)$, avšak $a \neq e_1$. To znamená, že homomorfismus f není injektivní.

„⇐“ Postupujeme opět nepřímo. Ukážeme, že pokud existuje takové $, b \in G_1$, pro které platí $a \neq b \wedge f(a) = = f(b)$, tak jádro homomorfismu f není triviální $\{e_1\}$.

$$\begin{aligned} f(a) &= f(b) \\ f(a) \circ_2 f(b)^{-1} &= f(b) f(b)^{-1} \\ f(a) \circ_2 f(b^{-1}) &= e_2 \\ f(a \circ_1 b^{-1}) &= e_2 \end{aligned}$$

To znamená, že prvek $a \circ_1 b^{-1}$ patří do jádra, které obsahuje pouze neutrální prvek e_2 a platí

$$\begin{aligned} a \circ_1 b^{-1} &= e_1 \\ a &= b. \end{aligned}$$

To ale znamená, že $a \circ_1 b^{-1} \in \mathrm{Ker}(f)$. ✓

Cvičení

8.2.1. Mějme množinu $P_3(x) = \{ax^2+bx+c : a,b,c \in \mathbb{R}\}$ a množinu $\mathbb{R}^2 = \{(a,b) : a,b \in \mathbb{R}\}$. a) Ukažte, že $(P_3(x),+)$, kde „+“ je obvyklé sčítání polynomů, je grupa. b) Ukažte, že $(\mathbb{R}^2,+)$, kde „+“ je obvyklé sčítání uspořádaných dvojic (vektorů) je grupa. c) Ověřte, zda zobrazení $f : P_3(x) \to \mathbb{R}^2$ je homomorfismus $(P_3(x),+)$ do $(\mathbb{R}^2,+)$, jestliže $f(ax^2+bx,c) = (2a+b,b+c)$, například $f(x^2-1) = (2,-1)$. d) Ověřte, zda zobrazení $g : P_3(x) \to \mathbb{R}^2$ je homomorfismus $(P_3(x),+)$ do $(\mathbb{R}^2,+)$, jestliže $g(ax^2+bx,c) = (2ab,bc)$.

8.2.2. Mějme grupu $(P_3(x),+)$ z Příkladu 8.2.1. Ověřte, zda zobrazení $f : P_3(x) \to P_2(x)$ definované jako derivace $f(ax^2+bx+c) = (ax^2+bx+c)' = 2ax+b$ je homomorfismus $(P_3(x),+)$ do $(P_3(x),+)$.

8.2.3. Navážeme na Cvičení 8.1.8. Mějme grupy $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{R},+)$ a homomorfismus $f : \mathbb{R}\setminus\{0\} \to \mathbb{R}$ daný předpisem $f(x) = \ln|x|$ grupy $(\mathbb{R}\setminus\{0\},\cdot)$ do grupy $(\mathbb{R},+)$. Najděte jádro $\mathrm{Ker}(f)$ a sestavte rozklad $\mathbb{R}\setminus\{0\}/\mathrm{Ker}(f)$.

8.2.4. Navážeme na Cvičení 8.2.3. Mějme grupy $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{R},+)$ a homomorfismus $f : \mathbb{R}\setminus\{0\} \to \mathbb{R}$ daný předpisem $f(x) = \ln|x|$ grupy $(\mathbb{R}\setminus\{0\},\cdot)$ do grupy $(\mathbb{R},+)$. Je homomorfismus f injektivní?

8.2.5. Navážeme na Cvičení 8.2.4. Mějme grupy $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{R},+)$ a homomorfismus $f : \mathbb{R}\setminus\{0\} \to \mathbb{R}$ daný předpisem $f(x) = \ln|x|$ grupy $(\mathbb{R}\setminus\{0\},\cdot)$ do grupy $(\mathbb{R},+)$. Jak vypadá kanonický homomorfismus popsaný v Důsledku 8.7.?

8.2.6. Navážeme na Cvičení 8.2.5. Mějme grupy $(\mathbb{R}\setminus\{0\},\cdot)$, $(\mathbb{R},+)$ a homomorfismus $f : \mathbb{R}\setminus\{0\} \to \mathbb{R}$ daný předpisem $f(x) = \ln|x|$ grupy $(\mathbb{R}\setminus\{0\},\cdot)$ do grupy $(\mathbb{R},+)$. Jak vypadá bijektivní homomorfismus popsaný ve Větě 8.8.?

8.2.7. Mějme grupu regulárních čtvercových matic řádu n s operací násobení $(M^*_{n,n},\cdot)$, grupu násobení nenulových reálných čísel $(\mathbb{R}\setminus\{0\},\cdot)$ a zobrazení $f : M^*_{n,n} \to \mathbb{R}\setminus\{0\}$ dané předpisem $f(A) = \det(A)$ pro každé $A \in M^*_{n,n}$. a) Ukažte, že zobrazení f je homomorfismus. b) Najděte jádro homomorfismu f.

8.2.8. Existuje podgrupa grupy $(P_3(x),+)$ z Příkladu 8.2.1., pro kterou zobrazení f je homomorfismem $(P_3(x),+)$ do $(\mathbb{R}^2,+)$? Pokud ano, najděte ji.

8.2.9. Mějme grupy $(S_5,\circ)$ a $(D_4,\circ)$. Definujeme zobrazení $s : S_5 \to D_4$ tak, že sudým permutacím přiřadíme identitu R_0 a lichým permutacím prvek H (zrcadlení podle vodorovné osy). a) Ukažte, že zobrazení s je homomorfismus grupy $(S_5,\circ)$ do grupy $(D_4,\circ)$. b) Určete jádro homomorfismu a ověřte, že se jedná o normální podgrupu grupy $(S_5,\circ)$. c) Bude zobrazení $t : S_5 \to D_2$, které sudým permutacím přiřadí H a lichým permutacím R_0 homomorfismem? Vysvětlete.

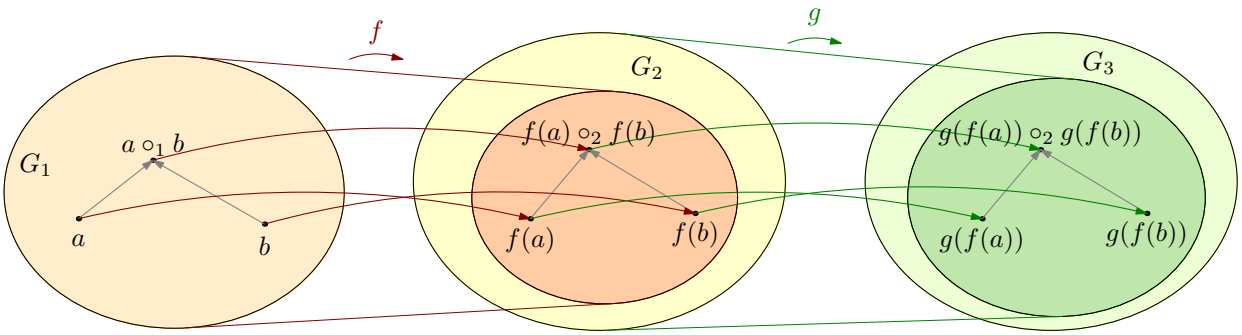
8.2.10. Mějme homomorfismus f grupy jednotek $GUX30$ do grupy $(U(30),\cdot)$, pro který platí $\mathrm{Ker}(f) = \{1,11\}$. a) Jak vypadá obraz prvku 7? b) Jak vypadá homomorfismus f?

8.3. Skládání homomorfismů

Protože homomorfismy jsou zobrazení (která navíc zachovávají operaci), tak můžeme homomorfismy množinami skládat.

Věta 8.9. *Mějme homomorfismus $f : G_1 \to G_2$ grupy $(G_1,\circ_1)$ do grupy $(G_2,\circ_2)$ a dále mějme homomorfismus $g : G_2 \to G_3$ grupy $(f(G_1),\circ_2)$ do grupy $(G_3,\circ_3)$. Potom platí následující tvrzení.*

(i) Složené zobrazení $g \circ f$ je homomorfismus grupy $(G_1,\circ_1)$ do grupy $(G_3,\circ_3)$.
(ii) Jestliže f i g jsou bijekce, potom i složené zobrazení $g \circ f$ je bijekce.



Obrázek 8.13.: *Složení homomorfismů $f : G_1 \to G_2$ a $g : G_2 \to G_3$.*

Důkaz. Ukážeme obě části tvrzení.
(i) Protože zobrazení f a g jsou homomorfismy, tak pro každé $a, b \in G_1$ platí

$$g \circ f(a \circ_1 b) = g(f(a) \circ_2 f(b)) = g(f(a)) \circ_3 g(f(b)) = (g \circ f(a)) \circ_3 (g \circ f(b)).$$

To znamená, že složené zobrazení $g \circ f$ je homomorfismus grupy $(G_1, \circ_1)$ do grupy $(G_3, \circ_3)$.
(ii) Dále ukážeme, že zobrazení $g \circ f$ je bijekce. Nejprve nepřímo ukážeme, že $g \circ f$ je injektivní.

Mějme libovolné $a, b \in G_1$. Jestliže nastane rovnost

$$g \circ f(a) = g \circ f(b)$$

tak protože g je injektivní (dokonce bijektivní), dostaneme

$$f(a) = f(b)$$

a protože f je injektivní (dokonce bijektivní), tak

$$a = b.$$

To znamená, že zobrazení $g \circ f$ je injektivní.

Zbývá ještě ukázat, že zobrazení $g \circ f$ je surjekce. Z předpokladu víme, že zobrazení g je surjektivní, to znamená, že pro každý obraz $c \in G_3$ existuje vzor $b \in f(G_1)$ a platí $g(b) = c$. Podobně z předpokladu víme, že *zobrazení* f je surjektivní, a proto pro každý obraz $b \in G_2$ existuje vzor $a \in G_1$ a platí $f(a) = b$. Protože množina obrazů $f(G_1) \subseteq G_2$, tak můžeme shrnout, že pro každé $c \in G_3$ existuje vzor $a \in G_1$ a platí $c = g(b) = g(f(a)) = (g \circ f)(a)$. Našli jsme vzor libovolného prvku $a \in G_1$, a proto je zobrazení $g \circ f$ surjektivní. Tím důkaz končí. □

Příklad 8.16. Uvedeme několik jednoduchých příkladů skládání homomorfismů.

1) Složením homomorfismu $f : \mathbb{Z} \to \mathbb{Z}$ definované předpisem $f(x) = 2x$ a homomorfismu $g : \mathbb{Z} \to \mathbb{Z}_n$ definované předpisem $f(x) = x \bmod n$ dostaneme homomorfismus $g \circ f$ grupy $(\mathbb{Z}, +)$ do grupy $(\mathbb{Z}_n, +)$.
2) Složením homomorfismu $f : M^*_{n,n} \to \mathbb{R} \setminus \{0\}$ daného pro regulární matice předpisem $f(A) = \det(A)$ a homomorfismu $g : \mathbb{R} \setminus \{0\} \to \mathbb{R} \setminus \{0\}$ daného předpisem $f(x) = x^2$ dostaneme homomorfismus grupy regulárních čtvercových matic $(M_{n,n}, \cdot)$ do grupy $(\mathbb{R} \setminus \{0\}, \cdot)$.

Cvičení

8.3.1. Navážeme na Cvičení 8.2.2. Máme homomorfismus $f : P_3(x) \to P_2(x)$ derivace polynomu $f(ax^2 + +bx+c) = (ax^2+bx+c)' = 2ax+b$ grupy $(P_3(x), +)$ do grupy $(P_3(x), +)$. Analogicky mějme homomorfismus $g : P_2(x) \to P_1(x)$ derivace polynomu $f(ax + b) = (ax + b)' = a$ grupy $(P_2(x), +)$ do grupy $(P_1(x), +)$. Dokažte, že složené zobrazení $g \circ f : P_3(x) \to P_1(x)$ definované $f(ax^2 + bx + c) = (ax^2 + bx + c)'' = 2a$ (druhá derivace) je homomorfismus grupy $(P_3(x), +)$ do grupy $(P_3(x), +)$.

Kapitola 9. Izomorfismy grup

Když porovnáme první dvě Cayleyho tabulky 9.1., ihned si všimneme podobnosti obou tabulek. Pokud v první tabulce s operací „$\circ$“ nahradíme identitu R_0 písmenem a, rotace R_{120}, R_{240} písmeny b, c (v tomto pořadí) a zrcadlení Z_A, Z_B, Z_C písmeny d, e, f (v tomto pořadí), tak ihned dostaneme druhou tabulku s operací „$\cdot$“.

$\circ$	R_0	R_{120}	R_{240}	Z_A	Z_B	Z_C
R_0	R_0	R_{120}	R_{240}	Z_A	Z_B	Z_C
R_{120}	R_{120}	R_{240}	R_0	Z_C	Z_A	Z_B
R_{240}	R_{240}	R_0	R_{120}	Z_B	Z_C	Z_A
Z_A	Z_A	Z_B	Z_C	R_0	R_{120}	R_{240}
Z_B	Z_B	Z_C	Z_A	R_{240}	R_0	R_{120}
Z_C	Z_C	Z_A	Z_B	R_{120}	R_{240}	R_0

$\cdot$	a	b	c	d	e	f
a	a	b	c	d	e	f
b	b	c	a	f	d	e
c	c	a	b	e	f	d
d	d	e	f	a	b	c
e	e	f	d	c	a	b
f	f	d	e	b	c	a

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

Tabulka 9.1.: *Cayleyho tabulky dihedrální grupy* $(D_{\_}, \circ)$ *grupy* $(G, \cdot)$ *a grupy* $(\mathbb{Z}_6, +)$.

Přirozená otázka je, zda podobným nahrazením je možné dostat třetí tabulku. Není těžké si uvědomit, že to možné není! Dihedrální grupa $(D_3, \circ)$ má prvky řádu 1, 2 a 3, zatímco ve třetí tabulce grupy $(\mathbb{Z}_6, +)$ mají prvky 1 a 5 řád 6, což je snadné prověřit opakovaným sčítáním. Jestliže symboly jen jinak označíme, tak nezměníme řád prvku, který je určen strukturou tabulky, nikoliv samotným označením prvků.

Přirozeně se tak dostáváme k otázce, zda nějaké dvě grupy se liší pouze označením prvků a grupy jsou „izomorfní“, nebo zda mají jinou strukturu a jedná se o jinou „neizomorfní“ grupu.

Další zajímavou a složitější otázkou je, kolik existuje různých grup s předepsaným počtem prvků. Tuto druhou otázku zodpovíme jen pro některé vybrané řády. V kapitole 9.3. navíc ukážeme, že každou konečnou grupu můžeme popsat jako nějakou podgrupu grupy permutací.

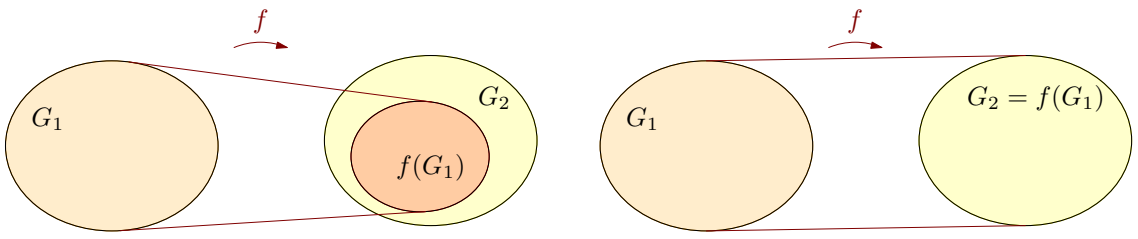
9.1. Definice izomorfismu grup

Nejprve zavedeme pojem izomorfismu grup.

Definice Bijektivní homomorfismus $f : G_1 \to G_2$ grupy $(G_1, \circ_1)$ do grupy $(G_2, \circ_2)$ nazýváme *izomorfismem grupy* $(G_1, \circ_1)$ do grupy $(G_2, \circ_2)$.

Jestliže existuje izomorfismus grupy $(G_1, \circ_1)$ do grupy $(G_2, \circ_2)$, tak říkáme, že grupy $(G_1, \circ_1)$ a $(G_2, \circ_2)$, *jsou izomorfní* a píšeme $(G_1, \circ_1) \simeq (G_2, \circ_2)$. Navíc, pokud nemůže vzniknout mýlka a je zřejmé s jakými operacemi pracujeme, tak píšeme $G_1 \simeq G_2$.

Všimněte si rozdílu mezi izomorfismem a homomorfismem grup. Izomorfismus je navíc bijektivní zobrazení (Obrázek 9.1.).



Obrázek 9.1.: *Homomorfismus a isomorfismus grup* $(G_1, \circ_1)$ *a* $(G_2, \circ_2)$.

Příklad 9.1. Mějme grupu $(\mathbb{Z}_3, +)$ a množinu $B = \{\circ, \triangle, \square\}$. Mějme zobrazení $f : \mathbb{Z}_3 \to B$ dané předpisem $f(0) = \circ$, $f(1) = \triangle$, $f(2) = \square$. Jsou dány Tabulky 9.2. Ověříme, že se zobrazení f je izomorfismus grup $(\mathbb{Z}_3, +)$ a $(B, \star)$.

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

$\star$	$\circ$	$\triangle$	$\square$
$\circ$	$\circ$	$\triangle$	$\square$
$\triangle$	$\triangle$	$\square$	$\circ$
$\square$	$\square$	$\circ$	$\triangle$

Tabulka 9.2.: *Tabulka grupy* $(\mathbb{Z}_3, +)$ *a grupy* $(\{\circ, \triangle, \square\}, \star)$.

Nejprve ověřit definici homomorfismu, tj. že výsledek operace vzorů se zobrazí na výsledek operace obrazů. Stačí ověřit 9 dvojic:

$$\begin{aligned}
f(0+0) &= f(0) = \circ = \circ \star \circ = f(0) \star f(0)\\
f(0+1) &= f(1) = \triangle = \circ \star \triangle = f(0) \star f(1)\\
f(0+2) &= f(2) = \square = \circ \star \square = f(0) \star f(2)\\
f(1+0) &= f(1) = \triangle = \triangle \star \circ = f(1) \star f(0)\\
f(1+1) &= f(2) = \square = \triangle \star \triangle = f(1) \star f(1)\\
f(1+2) &= f(0) = \circ = \triangle \star \square = f(1) \star f(2)\\
f(2+0) &= f(2) = \square = \square \star \circ = f(2) \star f(0)\\
f(2+1) &= f(0) = \circ = \square \star \triangle = f(2) \star f(1)\\
f(2+2) &= f(1) = \triangle = \square \star \square = f(2) \star f(2).
\end{aligned}$$

Ze zadání ihned vidíme, že zobrazení f je bijekce tříprvkové množiny na tříprvkovou množinu. Celkem dostáváme, že zobrazení f je izomorfismem grup $(G_1, \circ_1)$ a $(G_2, \circ_2)$. Platí $\mathbb{Z}_3 \simeq B$. ✓

Příklad 9.2. Mějme dvě grupy $(\mathbb{Z}, +)$ a $(\mathbb{S}, +)$. Jedná se o dvě různé grupy (například grupa s nosnou množinou $\mathbb{S}$ neobsahuje číslo 1), ukážeme však, že jsou izomorfní.
Ukážeme, že zobrazení $f : \mathbb{Z} \to \mathbb{S}$ definované předpisem $f(x) = 2x$ je izomorfismem. Vskutku zobrazení f je homomorfismus, neboť pro každé $x, y \in \mathbb{Z}$ platí

$$f(x+y) = 2(x+y) = 2x + 2y = f(x) + f(y).$$

Homomorfismus f je bijektivní, neboť vzorem každého sudého čísla $2t \in \mathbb{S}$ je číslo $t \in \mathbb{Z}$. ✓

Příklad 9.3. Mějme dvě grupy $(\mathbb{Q} \setminus \{0\}, \cdot)$ a $(\mathbb{R} \setminus \{0\}, \cdot)$. Jedná se o dvě různé grupy (například grupa s nosnou množinou $\mathbb{Q}$ neobsahuje číslo $\sqrt{2}$). Ukážeme, že tyto grupy nejsou izomorfní.
Homomorfismus $f : \mathbb{Q} \to \mathbb{R}$ sice existuje, například daný předpisem $f(x) = x$. Avšak tento homomorfismus nikdy nebude bijektivní, neboť množina $\mathbb{Q} \setminus \{0\}$ je spočetná zatímco množina $\mathbb{R} \setminus \{0\}$ je nespočtená, a proto mezi nimi neexistuje žádné bijektivní zobrazení. ✓

Věta 9.1. *Relace „býti izomorfní“ je relací ekvivalence na množině všech grup. Tj., nechť $(A, \circ_1)$, $(B, \circ_2)$, $(C, \circ_3)$ jsou libovolné grupy, potom platí*

(i) $A \simeq A$,
(ii) $A \simeq B \Leftrightarrow B \simeq A$,
(iii) $(A \simeq B \wedge B \simeq C) \Rightarrow A \simeq C$.

Důkaz. Dokážeme jednotlivé části věty.

(i) Nejprve dokážeme reflexivitu „$A \simeq A$“ relace „být izomorfní“. Dokážeme, že zobrazení $f : A \to A$ dané předpisem $f(a) = a$ je izomorfismus $(A, \circ_1)$ na sebe. Zobrazení f je homomorfismus, neboť $f(a \circ_1 b) = a \circ_1 b = f(a) \circ_1 f(b)$, zobrazení f je injektivní, neboť $f(a) = f(b) \Rightarrow a = b$ a konečně zobrazení f je surjektivní, neboť pro každé $b \in A$ platí $b = f(b)$. Proto zobrazení f je bijektivní homomorfismus, neboli izomorfismus.

(ii) Dále ukážeme symetrii „$A \simeq B \Leftrightarrow B \simeq A$“ relace „být izomorfní“. Bez újmy na obecnosti stačí ukázat $A \simeq B \Rightarrow B \simeq A$, neboť druhou implikaci dostaneme přeznačením. Proto v definici ekvivalence zpravidla bývá uvedena jen implikace.
Je-li $A \simeq B$, tak existuje bijekce $f : A \to B$, která je izomorfismem. Protože zobrazení f je bijekce, tak existuje zobrazení f^{-1}, které je také bijekce. Zbývá ukázat, že zobrazení $f^{-1} : B \to A$ je homomorfismus. Zobrazení f je surjektivní, vzorem prvku a je vždy samotný prvkem a. Potom jistě pro každé dva prvky $a', b' \in B$ existuje takové $a, b \in A$, že platí $a' = f(a), b' = f(b)$. Nyní $f^{-1}(a' \circ_2 b') = f^{-1}(f(a) \circ_2 f(b))$. A protože zobrazení f je homomorfismus, tak platí $f^{-1}(f(a) \circ_2 f(b)) = f^{-1}(f(a \circ_1 b)) = a \circ_1 b = f^{-1}(a') \circ_1 f^{-1}(b')$. Celkem dostáváme $f^{-1}(a' \circ_2 b') = f^{-1}(a') \circ_1 f^{-1}(b')$ a zobrazení f je homomorfismus.

(iii) Tranzitivitu „$(A \simeq B \wedge B \simeq C) \Rightarrow A \simeq C$“ relace „být izomorfní“ plyne z Věty 8.9.

Tím je důkaz ukončen. □

Ve Cvičeních 8.1.10. a 8.1.11. jsme položili otázku, zda řád obrazu v homomorfismu odpovídá řádu vzoru. Nyní ukážeme, že izomorfismus řád prvku zachová.

Věta 9.2. *Mějme grupu $(G_1, \cdot)$ s prvkem $g \in G_1$ konečného řádu n, respektive nekonečného řádu. Jestliže $f : G_1 \to G_2$ je izomorfismus grupy $(G_1, \cdot)$ do grupy $(G_2, \cdot)$, pak prvek $f(g)$ je prvek grupy $(G_2, \circ_2)$ řádu n, respektive nekonečného řádu.*

Důkaz. Z asociativity operací a definice homomorfismu vidíme, že

$$f(g^k) = f(\underbrace{g \circ_1 g \circ_1 \ldots \circ_1 g}_{k}) = \underbrace{f(g) \circ_2 f(g) \circ_2 \ldots \circ_2 f(g)}_{k} = (f(g))^k.$$

Zobrazení f je izomorfismus, proto je f je injektivní a podle Příkladu 8.15. víme, že $\operatorname{Ker} f = \{e_1\}$, kde e_1 je neutrální prvek levé grupy, tj. pouze prvek $e_1 \in G_1$ se zobrazí na $e_2 \in G_2$, kde e_2 je neutrální prvek pravé grupy. Pro každé $g \in G_1$ to znamená, že pokud $g^k \neq e_1$, potom také $f(g)^k \neq e_2$ a pokud $g^k = e_1$, potom také $f(g)^k = e_2$. Pro každé přirozené číslo k můžeme psát

$$g^k = e_1 \Leftrightarrow f(g)^k = e_2. \tag{5}$$

Je-li $g \in G_1$ je nekonečného řádu, potom pro každé přirozené číslo k je $g^k \neq e_1$, a proto podle (5) je $f(g)^k = f(g^k) \neq e_2$, a to znamená, že $f(g)$ je také nekonečného řádu.

Stejně tak, je-li $g \in G_1$ konečného řádu n, tak pro hodnoty k menší než n je $g^k \neq e_1$ a podle (5) je $f(g)^k = f(g^k) \neq e_2$. A konečně pokud $g^n = e_1$, tak je také $f(g^n) = f(e_1) = e_2$. To znamená, že $f(g)$ je také konečného řádu n. Tím je důkaz ukončen. □

Příklad 9.4. Najdeme dvě neizomorfní grupy řádu 6 a ukážeme, proč nejsou izomorfní.
Mějme dvě grupy řádu 6, a sice grupu $(\mathbb{Z}_6, +)$ a dihedrální grupu $(D_3, \circ)$. Víme, že grupa $(\mathbb{Z}_6, +)$ je cyklická, platí $\mathbb{Z}_6 = \langle \overline{1} \rangle$, neboť prvek $\overline{1}$ je řádu 6. Naproti tomu dihedrální grupa $(D_3, \circ)$ žádný prvek řádu 6 nemá, protože každé zrcadlení je řádu 2, identita R_0 je řádu 1 a rotace R_{120}, R_{240} jsou řádu 3. Podle Věty 9.2. žádný izomorfismus grup $(\mathbb{Z}_6, +)$ a $(D_3, \circ)$ neexistuje, neboť obraz prvku $\overline{1} \in \mathbb{Z}$ řádu 6 nemůže být žádný z prvků grupy $(D_3, \circ)$. ✓

Cvičení

9.1.1. Najděte dvě různé neizomorfní grupy se čtyřmi prvky. Pokud to není možné, dokažte to.

9.1.2. Najděte všechny izomorfismy grupy $(G, \cdot)$ určené Cayleyho tabulkou 9.3. do cyklické grupy $(\mathbb{Z}_4, +)$.

$\cdot$	a	b	c	d
a	c	d	a	b
b	d	a	b	c
c	a	b	c	d
d	b	c	d	a

Tabulka 9.3.: Grupa $(G, \cdot)$

9.1.3. Navážeme na Cvičení 8.1.13. Mějme komutativní grupu $(G, \cdot)$. Definujeme zobrazení $f : G \to G$ předpisem $f(a) = a^{-1}$ pro každé $a \in G$. Ukažte, že f je izomorfismus.

9.1.4. Mějme libovolnou grupu $(G, \cdot)$ a pevný prvek $g \in G$. Definujme zobrazení $f : G \to G$ pro každé $a \in G$ předpisem $f(a) = g \cdot a$. Pro jaké prvky g je zobrazení izomorfismem?

9.1.5. Mějme grupu $(G, \cdot)$. Definujme zobrazení $g : G \to G$ pro každé $a \in G$ předpisem $f(a) = a^2$. Ukažte, že zobrazení f je izomorfismem právě tehdy, když $(G, \cdot)$ je komutativní grupa.

9.1.6. Nechť $\mathbb{Q}(\sqrt{2}) = \{a + \sqrt{2}b : a, b \in \mathbb{Q}\}$. Mějme grupu $(\mathbb{Q}(\sqrt{2}), +)$. Nechť $\mathbb{Q} \times \mathbb{Q} = \{(a, b) : a, b \in \mathbb{Q}\}$ a sčítání „+“ na $\mathbb{Q} \times \mathbb{Q}$ definujeme předpisem $(a_1, b_1) + (a_2, b_2) = (a_1 + b_1, a_2 + b_2)$. Mějme grupu $(\mathbb{Q} \times \mathbb{Q}, +)$. Dokažte, že $(\mathbb{Q}(\sqrt{2}), +)$ je izomorfní s $(\mathbb{Q} \times \mathbb{Q}, +)$. Najděte příslušný izomorfismus.

9.1.7. Mějme grupu $(G, \cdot)$. Definujme zobrazení $g : G \to G$ pro každé $a \in G$ předpisem $f(a) = a^n$. Ukažte, že když $(G, \cdot)$ je komutativní grupa, tak zobrazení f je izomorfismus.

9.1.8. Vezměme symetrickou grupu $(S_3, \circ)$ a zobrazení $f(a) = a^5$. Je f grupovým izomorfismem?

9.1.9. Mějme grupu $(G, \cdot)$. Definujme zobrazení $g : G \to G$ pro každé $a \in G$ předpisem $f(a) = a^n$. Najděte takové $n > 2$ a takovou nekomutativní grupu $(G, \cdot)$, aby zobrazení f byl izomorfismus.

9.1.10. Mějme dvě grupy $(\mathbb{R}\setminus\{0\},\cdot)$ a $(\mathbb{R}^+,\cdot)$. Dokažte nebo vyvraťte: grupy $(\mathbb{R}\setminus\{0\},\cdot)$ a $(\mathbb{R}^+,\cdot)$ jsou izomorfní.

9.1.11. Mějme dvě grupy $(\mathbb{R}\setminus\{0\},\cdot)$ a $(\mathbb{C}\setminus\{0\},\cdot)$. Dokažte nebo vyvraťte: grupy $(\mathbb{R}\setminus\{0\},\cdot)$ a $(\mathbb{C}\setminus\{0\},\cdot)$ jsou izomorfní.

9.1.12. Mějme dvě grupy $(\mathbb{R},+)$ a $(\mathbb{R}^+,\cdot)$. Dokažte nebo vyvraťte: grupy $(\mathbb{R},+)$ a $(\mathbb{R}^+,\cdot)$ jsou izomorfní.

9.2. Klasifikace cyklických grup

Vrátíme se k tvrzení, které jsme avizovali v Kapitole 6. Ukážeme, že nekonečná cyklická grupa i každá konečná cyklická grupa pevně zvoleného řádu mají jednoznačně určenou strukturu. Nejprve ukážeme snadné pozorování, že cyklická grupa je vždy izomorfní s cyklickou grupou.

Lemma 9.3. *Izomorfní obraz cyklické grupy je cyklická grupa stejného řádu.*

Důkaz. Předpokládejme, že zobrazení $f : G_1 \to G_2$ je izomorfismus a že grupa $(G_1,\cdot)$ je cyklická grupa konečného řádu n, respektive nekonečného řádu. Platí $G_2 = f(G_1) = \{f(a^k) : k \in \mathbb{Z}\} = \{f(a)^k : k \in \mathbb{Z}\}$, kde a je generátor grupy $(G_1,\cdot)$. Cyklická grupa je jednoznačně určena svým generátorem a a generátor se podle Věty 9.2. v homomorfismu zobrazí na prvek $f(a)$ stejného řádu. Grupa $(G_2,\circ_2)$ je proto cyklická grupa s generátorem $f(a)$ a je stejného řádu jako grupa $(G_1,\circ_1)$. □

Příklad 9.5. Ukážeme, že libovolné dvě grupy $(A,\circ_1)$ a $(B,\circ_2)$ řádu 5 jsou izomorfní.
Protože podle Lagrangeovy věty (Věta 4.10.) musí řád každého prvku dělit řád grupy, má každá z grup pouze prvky řádu 1 a 5. Navíc prvek řádu 1 je v každé grupě jediný, neboť řád 1 má vždy pouze neutrální prvek e. Pro každý jiný prvek a platí $a = a^1 \neq e$.

Každý prvek řádu 5 je generátorem grupy řádu 5. Označme a libovolný prvek řádu 5 v grupě $(A,\circ_1)$ a dále označme b libovolný prvek řádu 5 v grupě $(B,\circ_2)$. Platí $A = \langle a\rangle$ a $B = \langle b\rangle$. Zobrazení $f : A \to B$, pro které platí $f(a) = b$, jednoznačně určí obrazy všech prvků. Pro každé $n \in [1,5]$ platí $f(a^n) = f(a)^n = b^n$, přičemž první rovnost vyplývá z definice izomorfismu a druhá z definice zobrazení f. To znamená, že zobrazení f je izomorfismem grup $(A,\circ_1)$ a $(B,\circ_2)$ a grupy jsou izomorfní. ✓

Otázky:

- Kolik existuje různých izomorfismů grup $(A,\circ_1)$ a $(B,\circ_2)$ z Příkladu 9.5.?
- Existují dvě neizomorfní grupy řádu 7?

Nyní ukážeme, že struktura každé nekonečné cyklické grupy odpovídá grupě obvyklého sčítání celých čísel a struktura každé konečné cyklické grupy odpovídá grupě sčítání zbytkových tříd celých čísel.

Věta 9.4. *Mějme libovolný prvek a grupy $(G,\cdot)$. Jestliže řád prvku a je nekonečný, tak $(\langle a\rangle,\cdot) \simeq (\mathbb{Z},+)$. Jestliže řád prvku a je (konečné) přirozené číslo n, tak $(\langle a\rangle,\cdot) \simeq (\mathbb{Z}_n,+)$.*

Důkaz. Nejprve uvažujme případ, kdy řád prvku a je nekonečný. Víme, že $\langle a\rangle = \{a^k : k \in \mathbb{Z}\}$ a budeme definovat zobrazení $f : G \to \mathbb{Z}$ předpisem $f(a^k) = k$. Abychom ukázali, že zobrazení f je izomorfismus, tak ukážeme, že f je homomorfismus, který je navíc injektivní i surjektivní.

S využitím známých vlastností celých čísel dostaneme

$$f(a^r \cdot a^s) = f(a^{r+s}) = r + s = f(a^r) + f(a^s).$$

Zobrazení f je tedy homomorfismus.

Injektivitu zobrazení f ukážeme nepřímo. Jsou-li obrazy dvou prvků a^p, a^q cyklické grupy $(\langle a\rangle,\cdot)$ stejné, tak $f(a^p) = f(a^q)$ znamená $p = q$. Z definice zobrazení ihned dostáváme, že $a^p = a^q$ a zobrazení f je injektivní. Surjektivitu ukážeme tak, že pro každý prvek $k \in \mathbb{Z}$ najdeme vzor. Pro každé $k \in \mathbb{Z}$ stačí vzít prvek $a^k \in \langle a\rangle$ a platí $f(a^k) = k$.

Tvrzení pro prvek a konečného řádu se ukáže analogicky. Mějme cyklickou grupu $(\langle a\rangle,\cdot)$ řádu n, to znamená, že $\langle a\rangle = \{a^1, a^2, \ldots, a^n = e\}$. Víme, že $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ a definujeme zobrazení $f : \langle a\rangle \to \mathbb{Z}/n\mathbb{Z}$ tak, že pro každé $k \in \{1,2,\ldots,n\}$ položíme $f(a^k) = k + n\mathbb{Z}$. S využitím vlastností sčítání komplexů dostáváme

$$f(a^r \cdot a^s) = f(a^{r+s}) = (r+s) + n\mathbb{Z} = (r + n\mathbb{Z}) + (s + n\mathbb{Z}) = f(a^r) + f(a^s).$$

Zobrazení f je tedy homomorfismus.

Injektivitu zobrazení f ukážeme opět nepřímo. Je-li $f(a^p) = f(a^q)$, tak $p + n\mathbb{Z} = q + n\mathbb{Z}$, což znamená $(p - q) + n\mathbb{Z} = n\mathbb{Z}$. Rovnost nastane podle Věty 4.2. právě tehdy, když $p - q \in n\mathbb{Z}$. To ale znamená, že $p - q = nl$ pro vhodné přirozené číslo l, tedy $p = q + nl$. Dostáváme $a^p = a^{q+nl} = a^q(a^n)^l = a^q(e)^l = a^q$ a zobrazení f je proto injektivní. Surjektivitu ukážeme opět tak, že pro každý prvek $k + n\mathbb{Z}$ najdeme vzor, kterým je prvek $a^k \in \langle a \rangle$, neboť platí $f(a^k) = k + n\mathbb{Z}$. □

Z předchozí věty snadno plyne následující tvrzení.

Důsledek 9.5. *Nekonečná grupa $(G, \cdot)$ je cyklická právě tehdy, když $(G, \cdot) \simeq (\mathbb{Z}, +)$. Konečná grupa $(G, \cdot)$ řádu n je cyklická právě tehdy, když $(G, \cdot) \simeq (\mathbb{Z}/n\mathbb{Z}, +)$.*

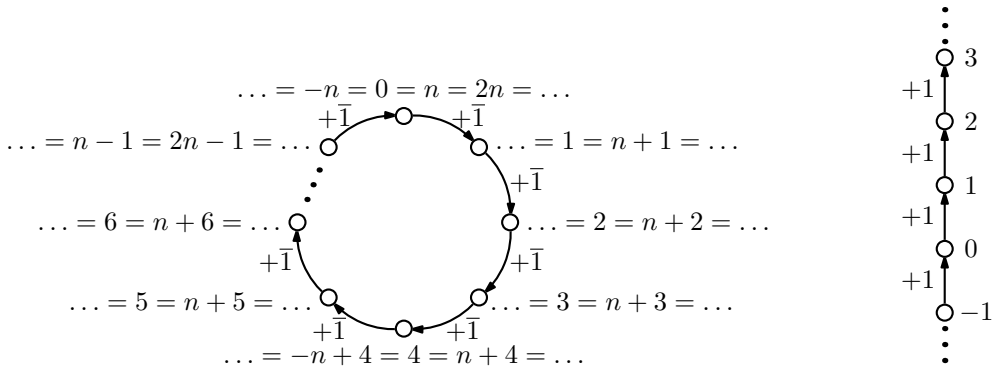
Důkaz. Obě části tvrzení mají tvar ekvivalence, měli bychom ukázat čtyři implikace. Obě implikace „⇒“ plynou ihned z předchozí Věty 9.4.

Obě implikace „⇐“ ukážeme snadno. Víme, že $(\mathbb{Z}, +)$ i $(\mathbb{Z}_n, +)$ jsou cyklické grupy a podle Lemmatu 9.3. izomorfní obraz cyklické grupy $(\mathbb{Z}, +)$ je opět cyklická grupa. □

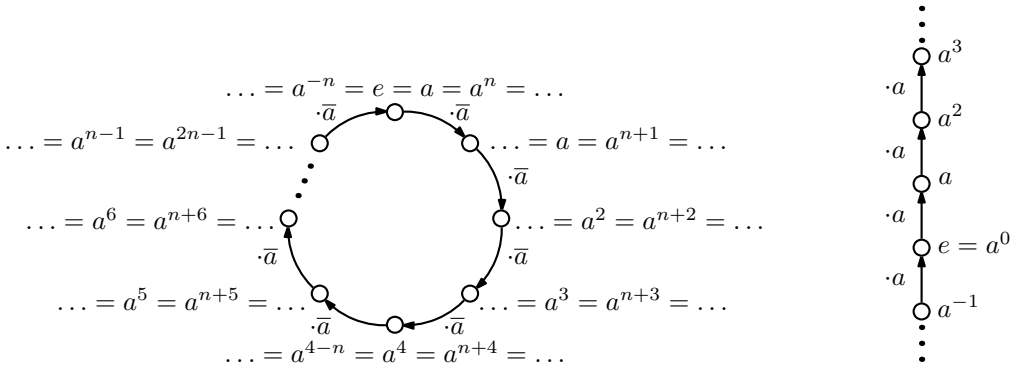
Z tranzitivity relace „být izomorfní“ ihned dostáváme ještě další důsledek.

Důsledek 9.6. *Každé dvě cyklické grupy stejného řádu jsou izomorfní.*

Izomorfismus cyklických grup je pěkně patrný z Obrázků 9.2. a 9.3. Zatímco na Obrázku 9.2. jsou znázorněny grupy $(\mathbb{Z}_n, +)$ a $(\mathbb{Z}, +)$, ta na Obrázku 6.1. jsou znázorněny obecné konečné a nekonečné cyklické grupy $(\langle a \rangle, \cdot)$. Obrázek 9.3. je stejný jako Obrázek 6.1., jen jsme jej zde pro názornost zopakovali. Rozdíl obou struktur je patrný pouze označením prvků. Struktura každé cyklické grupy je tak dobře prozkoumána.



Obrázek 9.2.: *Konečná cyklická grupa $(\mathbb{Z}_n, +)$ jako $\langle \overline{1} \rangle$ i nekonečná cyklická grupa $(\mathbb{Z}, +)$ jako $\langle 1 \rangle$.*



Obrázek 9.3.: *Konečná cyklická grupa $\langle a \rangle$ i nekonečná cyklická grupa $\langle a \rangle$.*

Ihned dostáváme například následující důsledek.

Důsledek 9.7. *Každá cyklická grupa je komutativní.*

Důkaz je snadný, stačí si uvědomit, že $(\mathbb{Z}, +)$ i $(\mathbb{Z}_n, +)$ jsou komutativní grupy.

Cvičení

9.2.1. Najděte dvě různé neizomorfní grupy se třemi prvky. Pokud to není možné, dokažte to.

9.2.2. Ukažte, že libovolné dvě grupy prvočíselného řádu p jsou izomorfní.

9.2.3. Ukažte, že grupa $(\mathbb{Q}, +)$ není cyklická.

9.2.4. Dokažte, že grupa $\mathbb{Q}(\sqrt{2})$ není cyklická.

9.2.5. Rozhodněte o pravdivosti následujícího tvrzení: Každá podgrupa nekonečné cyklické grupy je nekonečná.

9.2.6. Rozhodněte o pravdivosti následujícího tvrzení: Každá netriviální podgrupa nekonečné cyklické grupy je nekonečná.

9.2.7. Rozhodněte o pravdivosti následujícího tvrzení: Každá netriviální podgrupa nekonečné grupy je nekonečná.

9.2.8. Mějme čtyři matice $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $A = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $C = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$. a) Ukažte, že množina $M = \{A, B, C, D\}$ s operací násobení matic tvoří grupu. b) Je tato grupa řádu 4 izomorfní s grupou $(\mathbb{Z}_4, +)$?

9.3. Cayleyho věta

V této podkapitole ukážeme, že grupy permutací mají jednu důležitou vlastnost: každá grupa je izomorfní s nějakou grupou permutací nebo s její podgrupou. To znamená, že budeme-li zkoumat grupy permutací, tak současně zkoumáme (až na izomorfismus) libovolnou grupu. Nejprve na dvou příkladech ukážeme hlavní myšlenku.

Příklad 9.6. Mějme grupu $(G, \cdot)$, kde $G = \mathbb{Z}_5 \setminus \{0\}$ a operace „$\cdot$“ je násobení modulo 5. Označme S_G množinu čtyř vybraných permutací prvků množiny G, které jsou určeny řádky Tabulky 9.4. Ukážeme, že $(S_G, \circ)$ tvoří grupu.

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Tabulka 9.4.: *Cayleyho tabulka grupy násobení modulo 5.*

Každý řádek můžeme popsat permutací množiny $\{1, 2, 3, 4\}$.

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \qquad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix} \qquad \sigma_4 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Všimněte si, že například $\sigma_3 \circ \sigma_2 = \sigma_1$ nebo $\sigma_2 \circ \sigma_4 = \sigma_3$. Dokonce obecně pro každé $a, g \in \{1, 2, 3, 4\}$ platí $\sigma_a(g) = a \cdot g$. Dále si všimneme, že platí

$$\sigma_{a \cdot b}(g) = (a \cdot b) \cdot g,$$

ale současně platí

$$\sigma_a \circ \sigma_b(g) = \sigma_a(\sigma_b(g)) = \sigma_a(b \cdot g) = a \cdot (b \cdot g) = (a \cdot b) \cdot g.$$

Proto pro všechny $a, b, g \in G$ obecně platí $\sigma_a \circ \sigma_b(g) = \sigma_{a \cdot b}(g)$. ✓

Množiny S_G, $S_{|G|}$ a S_n

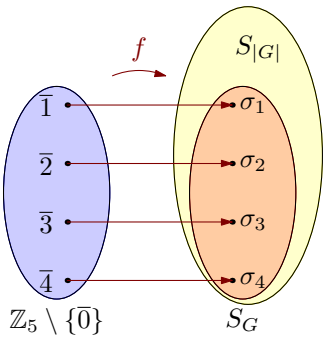
Nejprve si všimněte si rozdílu množin S_G a $S_{|G|}$. Zatímco $S_{|G|}$ je množina *všech* permutací n-prvkové množiny G, tak množina S_G obsahuje vybrané permutace množiny G.

Rozdíl množin $S_{|G|}$ a S_n je spíše formální. Zatímco $S_{|G|}$ je množina všech permutací n-prvkové *množiny* G, tak S_n je množina permutací *číselné množiny* $[1,n]$. Dle výsledků Kapitoly 7. víme, že S_n tvoří grupu. Formálně můžeme pro každou konečnou grupu G řádu n zavést zobrazení $s : G \to [1,n]$ tak, že prvky množiny G označíme $g_1, g_2, \ldots, g_n$ a položíme $s(g_i) = i$ (Cvičení 9.3.5.). Proto $S_{|G|}$ je izomorfní s grupou S_n, ve které místo každého prvku i vezmeme prvek množiny G s indexem i při nějakém indexování prvků G indexy z množiny $[1,n]$.

Dle Příkladu 9.6. víme, že i vybrané permutace S_G obecně tvoří grupu $(S_G, \circ)$. V následujícím příkladu ukážeme, že existuje přirozeně definovaný homomorfismus mezi grupou $(G,\cdot)$ a jejím obrazem $(f(G),\circ) = (S_G,\circ)$ v grupě permutací $(S_{|G|},\circ)$.

Příklad 9.7. Definujeme zobrazení $f : G \to (S_4,\circ)$, tj. zobrazení $f : \mathbb{Z}_5 \setminus \{0\} \to (S_4,\circ)$ předpisem $f(a) = \sigma_a$ (Obrázek 9.4.). Ukážeme, že zobrazení f je homomorfismus $(\mathbb{Z}_5 \setminus \{0\},\cdot) \to (S_4,\circ)$ a platí

$$f(a \cdot b) = \sigma_{a\cdot b} = \sigma_a \circ \sigma_b (a \cdot b) = f(a) \circ (b).$$



Obrázek 9.4.: *Homomorfismus* $f : (\mathbb{Z} \setminus \{0\},\cdot) \to (f(\mathbb{Z} \setminus \{0\}),\circ)$.

Zobrazení f sice není surjektivní, protože množina S_4 obsahuje 24 prvků, přičemž její podmnožina $f(\mathbb{Z}\setminus\{0\})$ obsahuje pouze čtyři prvky, nicméně zobrazení f je injektivní, neboť

$$f(a) = f(b)$$
$$\sigma_a = \sigma_b,$$

což pro všechny prvky $g \in G$ znamená

$$\sigma_a(g) = \sigma_b(g)$$
$$a \cdot g = b \cdot g.$$

S využitím Věty o krácení (Věta 2.6.) je

$$a = b.$$

Vidíme, že pokud se omezíme na množinu obrazů $f(\mathbb{Z}_5 \setminus \{0\}) = S_{\mathbb{Z}_5\setminus\{0\}} = \{\sigma_1,\sigma_2,\sigma_3,\sigma_4\}$, tak zobrazení f je bijekcí. Všimněte si, že je-li $b = a^{-1}$, tak $\sigma_b = \sigma_{a^{-1}}$ je inverzní k σ_a (Cvičení 9.3.3.). Proto zobrazení f je nejen homomorfismus $(\mathbb{Z} \setminus \{0\},\cdot) \to (S_4,\circ)$, ale navíc izomorfismus $(\mathbb{Z} \setminus \{0\},\cdot)$ a podgrupy $(f(\mathbb{Z} \setminus \{0\}),\circ) = ((S_{\mathbb{Z}\setminus\{0\}},\circ))$ grupy permutací $(S_4,\circ)$ prvků dané množiny $\{1,2,3,4\}$. ✓

Prvkům přiřadíme permutace

Připomeňme, že permutace lze chápat jako bijektivní zobrazení množiny do sebe (formální definice je v Kapitole 7.1.). Potom také $\sigma_a(x)$ zavedené v předchozím příkladu jsou permutace množiny G, což má smysl definovat jak pro konečnou, tak i pro nekonečnou množinu G. Dostáváme Větu 9.8.

Věta 9.8. *Mějme grupu $(G,\cdot)$ a prvek $a \in G$. Pro každé $x \in G$ definujme zobrazení $\sigma_a : G \to G$ předpisem $\sigma_a(x) = a \cdot x$. Potom σ_a je bijekce, tj. σ_a je permutace prvků z G.*

Důkaz. Nejprve ukážeme, že zobrazení σ_a je injektivní. Pro každé dva prvky x, y z množiny G s využitím Věty o krácení (Věta 2.6.) platí

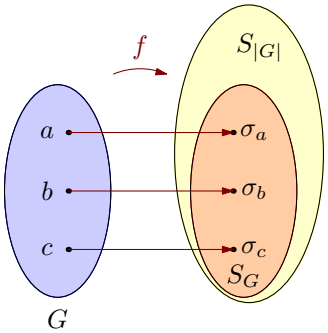
$$\begin{aligned}\sigma_a(x) &= \sigma_a(y)\\ a \cdot x &= a \cdot y\\ x &= y\end{aligned}$$

Zbývá ukázat, že zobrazení f je surjektivní, tj. že pro každé $y \in G$ existuje vzor. Využijeme, že v G existuje prvek zapsaný jako součin $a^{-1}y$. Nyní pro každé $y \in G$ existuje takový prvek $a^{-1}y \in G$, že platí

$$\sigma_a(a^{-1}y) = a \cdot a^{-1} \cdot y = y.$$

Vzorem prvku y je prvek $a^{-1}y$, a proto je zobrazení σ_a surjektivní. Celkem dostáváme, že $\sigma_a : G \to G$ je bijekce. □

Na straně 115 jsou zavedeny grupy permutací $(S_n, \circ)$. V Příkladu 9.6. jsme ukázali, že grupa $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ je isomorfní nějaké podgrupě $(S_G, \circ)$ v grupě permutací $(S_4, \circ)$. Nyní naše pozorování dále zobecníme. Jestliže $(G, \cdot)$ je grupa, symbol $(S_G, \circ)$ označuje podgrupu grupy permutací $(S_{|G|}, \circ)$, jejíž nosič S_G, $S_G = f(G)$, je tvořen permutacemi $\sigma_a(g) = a \cdot g$ pro každé $a, g \in G$. Následující Věta 9.9. říká, že mezi výchozí grupou $(G, \cdot)$ a podgrupou $(S_G, \circ)$ grupy $(S_{|G|}, \circ)$ existuje homomorfismus, který je navíc injektivní (Obrázek 9.5.).



Obrázek 9.5.: *Homomorfismus* $f : G \to S_{|G|}$.

Věta 9.9. *Mějme grupu $(G, \cdot)$ a prvek $a \in G$. Pro každé $a \in G$ definujme zobrazení $\sigma_a : G \to G$ předpisem $\sigma_a(x) = a \cdot x$ pro každé $x \in G$. Označme $S_G = \{\sigma_a : a \in G\}$. Potom zobrazení $f : G \to S_G$ dané předpisem $f(a) = \sigma_a$ pro každé $a \in G$ je injektivní homomorfismus grupy $(G, \cdot)$ do grupy $(S_G, \circ)$.*

Důkaz. Ukážeme, že zobrazení f je injektivní homomorfismus.

Nejprve nepřímo ukážeme, že zobrazení f je injektivní. Pokud se rovnají obrazy $f(a), f(b) \in S_G$ (permutace σ_a, σ_b v $S_G \subseteq S_{|G|}$) nějakých dvou prvků $a, b \in G$, tak s využitím definice zobrazení f dostáváme

$$\begin{aligned}f(a) &= f(b)\\ \sigma_a &= \sigma_b\\ a \cdot x &= b \cdot x \quad \forall x \in G\\ a &= b.\end{aligned}$$

To znamená, že zobrazení f je injektivní.

Dále ukážeme, že zobrazení f je homomorfismus. Pro každé $x \in G$ s využitím definice permutace σ_a a asociativity operace „$\cdot$“ platí

$$\sigma_a(x) \circ \sigma_b(x) = a(bx) = (ab)x = \sigma_{ab}(x)$$

a s využitím definice σ_{ab} ihned vidíme, že

$$\sigma_a \circ \sigma_b(x) = \sigma_{ab}(x).$$

To znamená, že zobrazení $f : G \to S_G$ je injektivní homomorfismus. □

Nyní můžeme zformulovat důležité tvrzení teorie grup. Ukazuje, že grupy permutací mají klíčové postavení mezi všemi grupami. Každou grupou lze totiž popsat pomocí skládání nějakých permutací, jestliže permutace chápeme jako bijekce nosné množiny (Obrázek 9.5.).

Důsledek 9.10. Cayleyho věta
Každá grupa je izomorfní s nějakou podgrupou grupy permutací svých prvků.

Důkaz. Podle předchozí Věty 9.9. víme, že existuje injektivní homomorfismus $G \to S_G$. Stačí ukázat, že zobrazení $f : G \to S_G$ je bijekce (platí $f(G) = S_G$, $S_G \subseteq S_{|G|}$). Injektivita zobrazení f je dána Větou 9.9. Surjektivita zobrazení f je zřejmá, neboť každé zobrazení je surjektivní na svůj obor hodnot. Pro každé $\sigma_a \in f(G)$ vezmeme $a \in G$ a podle definice permutace σ_a platí $f(a) = \sigma_a$. □

Otázky:

- Mějme dihedrální grupu $(D_3, \circ)$. Podle Cayleyho věty (Věta 9.10.) je $(D_3, \circ)$ izomorfní s podgrupou nějaké grupy permutací. Jaké?
- Mějme symetrickou grupu S_n. Podle Cayleyho věty (Věta 9.10.) je S_n izomorfní s podgrupou nějaké grupy permutací. Jaké?

Cvičení

9.3.1. Najděte všechny izomorfismy grupy $(\mathbb{Z}_7 \setminus \{0\}, \cdot)$ a grupy $(\mathbb{Z}_6, +)$.

9.3.2. Najděte nějaký izomorfismus grupy $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ a grupy $(\mathbb{Z}_4, +)$.

9.3.3. Mějme grupu $(G, \cdot)$, prvky $a, b \in G$ a grupu vybraných permutací $(S_G, \circ)$. Ukažte, že je-li $b = a^{-1}$, tak $\sigma_b = \sigma_{a^{-1}}$ je inverzní k σ_a v grupě $(S_G, \circ)$.

9.3.4. Uvažujme grupu $(\mathbb{C}, +_{\mathbb{C}})$, kde $\mathbb{C} = \{a + bi : a, b \in \mathbb{R}\}$ a operace $+_{\mathbb{C}}$ je dána předpisem

$$(a_1 + b_1 i) +_{\mathbb{C}} (a_2 + b_2 i) = (a_1 +_{\mathbb{R}} a_2) + (b_1 +_{\mathbb{R}} b_2)i,$$

kde „$+_{\mathbb{R}}$“ je obvyklé sčítání čísel. Dále mějme grupu $(\mathbb{R}^2, \oplus)$, kde $\mathbb{R}^2 = \{(a, b) : a, b \in \mathbb{R}\}$ a operace $\oplus$ je dána předpisem

$$(a_1, b_1) \oplus (a_2, b_2) = (a_1 +_{\mathbb{R}} b_1, b_1 +_{\mathbb{R}} b_2).$$

Dokažte, že grupy $(\mathbb{C}, +_{\mathbb{C}})$ a $(\mathbb{R}^2, \oplus)$ jsou izomorfní.

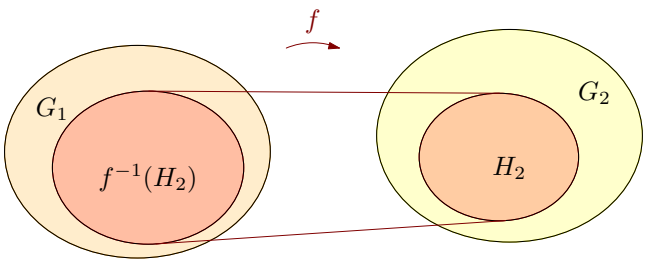
9.3.5. Dokažte tvrzení ze strany 147: Mějme grupy permutací $(S_{|G|}, \circ)$ množiny G řádu n a grupu permutací $(S_n, \circ)$ množiny $[1, n]$. Ukažte, že obě grupy jsou izomorfní.

9.3.6. Mějme dihedrální grupu $(D_3, \circ)$. Sestavte zobrazení popsaná ve Větě 9.8. Dále sestavte injektivní homomorfismus popsaný ve Větě 9.9.

9.4. Další vlastnosti homomorfismů

Nyní ukážeme, že tvrzení Věty 8.3. je možno obrátit. Nejenže množina obrazů levé grupy v homomorfismu f je podgrupou pravé grupy, ale pro každou podgrupu pravé grupy je také množina vzorů podgrupou levé grupy (Obrázek 9.6.). Symbol $f^{-1}(G)$ v následujícím tvrzení chápeme jako označení množiny vzorů, nikoliv jako množinu obrazů inverzního zobrazení, neboť inverzní zobrazení f^{-1} nemusí existovat, pokud homomorfismus f není injektivní.

Lemma 9.11. *Mějme homomorfismus $f : G_1 \to G_2$ grupy $(G_1, \circ_1)$ do grupy $(G_2, \circ_2)$. Mějme podgrupu $(H_2, \circ_2)$ grupy $(G_2, \circ_2)$. Označme množinu vzorů $H_1 = f^{-1}(H_2) = \{x \in G_1 : f(x) \in H_2\}$. Potom $(H_1, \circ_1)$ je podgrupa v grupě $(G_1, \circ_1)$. Jestliže $(H_2, \circ_2)$ je navíc normální podgrupa grupy $(G_2, \circ_2)$, tak $(H_1, \circ_1)$ je normální podgrupa v $(G_1, \circ_1)$.*



Obrázek 9.6.: *Vzor podgrupy $(H_2, \circ_2)$ je podgrupa $(f^{-1}(H_2), \circ_1)$.*

Důkaz. S využitím Věty 3.3. ukážeme, že $(H_1, \circ_1)$ je podgrupa v $(G_1, \circ_1)$.

(i) Množina H_1 je jistě neprázdná, protože vzor neutrálního prvku $e_2 \in H_2$ v homomorfismu f je neutrální prvek $e_1 \in H_1$, neboť podle Věty 8.1. platí $f(e_{H_1}) = e_{H_2}$.
(ii) Z vlastností zobrazení f ihned víme, že $H_1 \subseteq G_1$
(iii) Ukážeme, že restrikce operace „$\circ_1$“ na množinu H_1 je uzavřená. Protože zobrazení f je homomorfismus, tak pro každé $a, b \in H_1$ platí $f(a \circ_1 b) = f(a) \circ_2 f(b)$. Je-li $f(a), f(b) \in H_2$, tak z uzavřenosti podgrupy $(H_2, \circ_2)$ výsledek operace $f(a) \circ_2 f(b)$ patří do H_2, a proto podle definice $H_1 = f^{-1}(H_2)$ je $a \circ_1 b \in H_1$.
(iv) Inverzní prvky ke každému prvku $a \in H_1$ existují, protože pro každé $f(a) \in H_2$ existuje $(f(a))^{-1} = f(a^{-1}) \in H_2$, neboť $(H_2, \circ_2)$ je podgrupa v $(G_2, \circ_2)$. To ale současně znamená, že $a^{-1} \in H_1$.

Zbývá ukázat normálnost. Jestliže $(H_2, \circ_2)$ je normální podgrupa v $(G_2, \circ_2)$, tak podle definice normální podgrupy pro každé $g \in G_2$ platí $g \circ_2 H_2 = H_2 \circ_2 g$. Potom pro každé $x \in G_1$ platí $f(x) \circ_2 H_2 = H_2 \circ_2 f(x)$, neboli podle Věty 5.2. platí $f(x) \circ_2 H_2 \circ_2 (f(x))^{-1} \in H_2$. Dále pro každé $x \in G_1$ a každé $h \in H_1$ platí $f(x \circ_1 h \circ_1 x) = f(x) \circ_2 f(h) \circ_2 f(x^{-1}) \in H_2$. Potom vzor $x \circ_1 h \cdot x^{-1}$ patří do H_1, což jsme chtěli ukázat. To podle Věty 5.2. znamená, že $(H_1, \circ_1)$ je normální podgrupa v $(G_1, \circ_1)$. □

Důsledek 9.12. *Mějme homomorfismus $f : G_1 \to G_2$ grupy $(G_1, \circ_1)$ do grupy $(G_2, \circ_2)$. Potom platí $(H_1, \circ_1)$ je podgrupa v grupě $(G_1, \circ_1)$ právě tehdy, když $(f(H_1), \circ_2)$ je podgrupa grupy $(G_2, \circ_2)$.*

Důkaz. Podle Věty 8.3. víme, že je-li $(H_1, \circ_1)$ podgrupou grupy $(G_1, \circ_1)$, tak $(f(H_1), \circ_2)$ je podgrupou grupy $(G_2, \circ_2)$. Dále v Lemmatu 9.11. jsme se ukázali, že když $(f(H_1), \circ_2)$ je podgrupa grupy $(G_2, \circ_2)$, tak také $(H_1, \circ_1) = (f^{-1}(f(H_1)), \circ_1)$ je podgrupa grupy $(G_1, \circ_1)$. Spojením dostáváme hledané tvrzení. □

Cvičení

9.4.1. Mějme surjektivní homomorfismus $f : G_1 \to G_2$ grupy $(G_1, \circ_1)$ na grupu $(G_2, \circ_2)$. Mějme normální podgrupu $(H_2, \circ_2)$ grupy $(G_2, \circ_2)$. Ukažte, že $(G_2/H_2, \circ_2)$ je izomorfní s grupou $(G_1/f^{-1}(H_2), \circ_1)$.

Kapitola 10. Vnější součin grup

V této kapitole ukážeme, jak zkombinovat menší grupy, abychom získaly grupy větší. Operace tzv. „vnějšího součinu“ grup přirozeně vychází z klasického kartézského součinu nosných množin. Jednak množina výsledné grupy bude kartézským součinem nosných množin jednotlivých grup, ale také operace výsledné grupy bude přirozeně „po složkách“ definována pomocí operací na jednotlivých grupách.

Hlavním cílem však není jen sestavovat větší grupy. Důležitý bude zejména opačný proces, kdy větší grupu „rozložíme“ na vnější součin menších grup, podobně jako složená čísla lze rozložit na součin prvočísel. Tento proces nám pomůže nahlédnout do struktury mnoha konečných grup, neboť ukážeme, že jsou součinem menších grup.

Pomocí vnějšího součinu grup je možné dokonce úplně klasifikovat všechny konečné komutativní grupy.

10.1. Definice vnějšího součinu

Nejprve zavedeme vnější součin dvou grup jako množinu uspořádaných dvojic s operací „po složkách“.

Definice Mějme grupy $(G_1, \circ_1)$, $(G_2, \circ_2)$. *Vnější součin grup* $(G_1, \circ_1)$, $(G_2, \circ_2)$ je množina uspořádaných dvojic prvků z množin G_1, G_2 (v tomto pořadí) s operací, kde první složka je vždy určena operací „$\circ_1$“ a druhá složka je určena operací „$\circ_2$“. Vnější součin grupy $(G_1, \circ_1)$, $(G_2, \circ_2)$ značíme $(G_1, \circ_1) \oplus (G_2, \circ_2)$. Symbolicky zapsáno je

$$(G_1, \circ_1) \oplus (G_2, \circ_2) = (G_1 \times G_2, \cdot),$$

kde pro každé $(g_1, g_2), (h_1, h_2) \in G_1 \times G_2$ platí $(g_1, g_2) \cdot (h_1, h_2) = (g_1 \circ_1 h_1, g_2 \circ_2 h_2)$.

Pokud bude z kontextu jasné s jakými grupami se ve vnějším součinu pracuje, tak místo $(G_1, \circ_1) \oplus (G_2, \circ_2)$ budeme používat stručný zápis $G_1 \oplus G_2$.

Definici vnějšího součinu je snadné zobecnit pro vnější součin konečného počtu grup.

Definice Mějme grupy $(G_1, \circ_1)$, $(G_2, \circ_2)$, …, $(G_n, \circ_n)$. *Vnější součin grup* $(G_1, \circ_1)$, $(G_2, \circ_2)$, …, $(G_n, \circ_n)$ je množina uspořádaných n-tic prvků po řadě z množin $G_1, G_2, \ldots, G_n$ s operací „$\cdot$“, kde i-tá složka n-tice je vždy určena i-tou operací „$\circ_i$“ a značíme jej $(G_1, \circ_1) \oplus (G_2, \circ_2) \oplus \cdots \oplus (G_n, \circ_n)$. Symbolicky zapsáno je

$$(G_1, \circ_1) \oplus (G_2, \circ_2) \oplus \cdots \oplus (G_n, \circ_n) = (G_1 \times G_2 \times \cdots \times G_n, \cdot),$$

kde pro každé $(g_1, g_2, \ldots, g_n), (h_1, h_2, \ldots, h_n) \in G_1 \times G_2 \times \cdots \times G_n$ platí

$$(g_1, g_2, \ldots, g_n) \cdot (h_1, h_2, \ldots, h_n) = (g_1 \circ_1 h_1, g_2 \circ_2 h_2, \ldots, g_n \circ_n h_n).$$

V duchu stejné úmluvy jako u vnějšího součinu dvou grup budeme místo $(G_1, \circ_1) \oplus (G_2, \circ_2) \oplus \cdots \oplus (G_n, \circ_n)$ používat zápis $G_1 \oplus G_2 \oplus \cdots \oplus G_n$.

Příklad 10.1. Uveďme několik klasických příkladů vnějších součinů grup.

1) Z fyziky i z geometrie známe sčítání vektorů, které lze chápat jako operace v grupách $(\mathbb{R}^2, +)$ nebo $(\mathbb{R}^3, +)$. Je však dobré upozornit, že geometrický či fyzikální prostory označované $\mathbb{R}^2$ či $\mathbb{R}^3$ jsou komplexnější struktury – tzv. „prostory“, ve kterých vektory umíme nejen sčítat, ale také násobit skalárem, násobit navzájem skalárně a určovat velikosti vektorů.
2) Sčítání matic v grupě $(M_{2,2}(Z), +)$ můžeme chápat jako sčítání po složkách v grupě $\mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z} \oplus \mathbb{Z}$. Místo zapisování prvků do uspořádaných čtveřic, zapisujeme prvky do matice se dvěma řádky a dvěma sloupci.
3) Sčítání vektorů ve vektorovém prostoru dimenze n odpovídá vnějšímu součinu n grup $(\mathbb{R}, +)$, tj. vektory sčítáme jako prvky grupy $\underbrace{\mathbb{R} \oplus \mathbb{R} \oplus \cdots \oplus \mathbb{R}}_{n}$. Připomeňme, že ve vektorovém prostoru $\mathbb{R}^n$ máme navíc násobení skalárem a požadujeme distributivitu mezi násobením skalárem i mezi sčítáním vektorů.
4) Vektorový součin vektorů *neodpovídá* žádnému vnějšímu součinu grup $(\mathbb{R}, +)$ ani $(\mathbb{R}, \cdot)$. Ve vektorovém součinu se nenásobí „po složkách“, ale vektorový součin vektorů (dimenze 3) je definován jinak.
5) Skalární součin vektorů *neodpovídá* žádnému vnějšímu součinu, neboť se nejedná o operaci $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}^n$, ale o zobrazení $\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$. Výsledkem není vektor z $\mathbb{R}^n$, ale skalár z $\mathbb{R}$.

Příklad 10.2. Mějme cyklickou grupu $(\mathbb{Z}_2, +)$. Vnější součin $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ je grupa se čtyřmi prvky $(0,0)$, $(0,1)$, $(1,0)$, $(1,1)$, které se říká *Kleinova grupa*. Jedná se o grupu řádu 4, která *není* cyklická, neboť všechny prvky jsou řádu 1 nebo 2. Kleinova grupa proto není izomorfní s grupou $\mathbb{Z}_4$, tj. platí $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \not\simeq \mathbb{Z}_4$.

$\cdot$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,0)$	$(0,0)$	$(0,1)$	$(1,0)$	$(1,1)$
$(0,1)$	$(0,1)$	$(0,0)$	$(1,1)$	$(1,0)$
$(1,0)$	$(1,0)$	$(1,1)$	$(0,0)$	$(0,1)$
$(1,1)$	$(1,1)$	$(1,0)$	$(0,1)$	$(0,0)$

Tabulka 10.1.: *Tabulka Kleinovy grupy* $\mathbb{Z}_2 \oplus \mathbb{Z}_2$.

Příklad 10.3. Mějme cyklické grupy $(\mathbb{Z}_2, +)$, $(\mathbb{Z}_3, +)$. Jejich součin $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ je také cyklická grupa. Nosič grupy $\mathbb{Z}_2 \oplus \mathbb{Z}_3$ je množina $\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$ a generátorem grupy je prvek $(1,1)$. Platí

$$(1,1), \quad 2(1,1) = (0,2), \quad 3(1,1) = (1,0), \quad 4(1,1) = (0,1), \quad 5(1,1) = (1,2), \quad 6(1,1) = (0,0).$$

Můžeme tedy psát $\mathbb{Z}_2 \oplus \mathbb{Z}_3 \simeq \mathbb{Z}_6$. Toto pozorování později zobecníme.

Nejprve ukážeme, že definice je korektní a že dvojice $(G_1 \times G_2, \cdot)$ vskutku tvoří grupu.

Lemma 10.1. *Mějme grupy $(G_1, \circ_1)$, $(G_2, \circ_2)$. Vnější součin grup $G_1 \oplus G_2$, kde $G_1 \oplus G_2 = (G_1 \times G_2, \cdot)$ tvoří grupu.*

Důkaz. Důkaz tvrzení je snadný, přímo ověříme všechny vlastnosti grupy. Protože množiny G_1, G_2 jsou neprázdné, tak nosič $G_1 \times G_2$ je také neprázdná množina. Operace „$\cdot$“ je na množině uzavřená, neboť pro každé dva prvky $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$ víme, že $a_1 \circ_1 b_1 = c_1 \in G_1$ a také $a_2 \circ_2 b_2 = c_2 \in G_2$. To současně z definice vnějšího součinu grup znamená, že $(a_1 \circ_1 b_1, a_2 \circ_2 b_2) = (c_1, c_2) \in G_1 \oplus G_2$.

Z definice operace „$\cdot$“ vidíme, že pro každé $(a_1, a_2), (b_1, b_2), (c_1, c_2) \in G_1 \times G_2$ platí $((a_1, a_2) \cdot (b_1, b_2)) \cdot (c_1, c_2) = (a_1 \circ_1 b_1, a_2 \circ_2 b_2) \cdot (c_1, c_2) = ((a_1 \circ_1 b_1) \circ_1 c_1, (a_2 \circ_2 b_2) \circ_2 c_2)$ a také $(a_1, a_2) \cdot ((b_1, b_2) \cdot (c_1, c_2)) = (a_1, a_2) \cdot (b_1 \circ_1 c_1, b_2 \circ_2 c_2) = (a_1 \circ_1 (b_1 \circ_1 c_1), a_2 \circ_2 (b_2 \circ_2 c_2))$. Protože každá z operací „$\circ_1$“, „$\circ_2$“ je asociativní, tak platí $((a_1 \circ_1 b_1) \circ_1 c_1, (a_2 \circ_2 b_2) \circ_2 c_2) = (a_1 \circ_1 (b_1 \circ_1 c_1), a_2 \circ_2 (b_2 \circ_2 c_2))$, a proto také operace „$\cdot$“ je asociativní.

Neutrální prvek grupy $(G_1, \circ_1)$ označme e_1 a neutrální prvek grupy $(G_2, \circ_2)$ označme e_2. Neutrálním prvkem jejich součinu $(G_1 \times G_2, \cdot)$ je prvek (e_1, e_2), neboť pro libovolné $(a, b) \in G_1 \times G_2$ je $(e_1, e_2) \cdot (a, b) = (e_1 \circ_1 a, e_2 \circ_2 b) = (a, b)$ a současně $(a, b) \cdot (e_1, e_2) = (a \circ_1 e_1, b \circ_2 e_2) = (a, b)$.

A konečně inverzním prvkem k prvku $(a, b) \in G_1 \times G_2$ je prvek (a^{-1}, b^{-1}), neboť $(a^{-1}, b^{-1}) \cdot (a, b) = (a^{-1} \circ_1 a, b^{-1} \circ_2 b) = (e_1, e_2)$ a současně $(a, b) \cdot (a^{-1}, b^{-1}) = (a \circ_1 a^{-1}, b \circ_2 b^{-1}) = (e_1, e_2)$. □

Analogicky se ukáže následující lemma. Důkaz je ponechán jako Cvičení 10.1.3.

Lemma 10.2. *Mějme grupy $(G_1, \circ_1)$, $(G_2, \circ_2)$, …, $(G_n, \circ_n)$. Vnější součin množin $G_1 \oplus G_2 \oplus \cdots \oplus G_n = (G_1 \times G_2 \times \cdots \times G_n, \cdot)$ tvoří grupu.*

Všimněte si, že přísně vzato $(G_1 \oplus G_2) \oplus G_3 \neq G_1 \oplus (G_2 \oplus G_3) \neq G_1 \oplus G_2 \oplus G_3$, neboť v prvních dvou vnějších součinech máme uspořádané dvojice, v nichž jedna složka je opět uspořádanou dvojicí, zatímco v třetím součinu máme uspořádanou trojici. Často se však všechny tři vztahy považují za rovnocenné na základě úmluvy, že například vnější součin $(G_1 \oplus G_2) \oplus G_3$ chápeme jako uspořádanou trojici nebo $G_1 \oplus ((G_2 \oplus G_3) \oplus G_4)$ chápeme jako uspořádanou čtveřici.

Řád součinu konečných grup

Všimněte si, že podle uvedených definic je grup ve vnějším součinu $G_1, G_2, \ldots, G_n$ vždy konečně mnoho. Z definice součinu je zřejmé, jak vypadá řád grupy, pokud všechny členy součinu jsou konečné grupy. Platí $|G_1 \oplus G_2 \oplus \cdots \oplus G_n| = |G_1||G_2| \cdots |G_n|$.

Při zápisu operace mezi prvky vnějšího součinu je obvyklé užívat multiplikativní zápis bez užití symbolu operace „$\cdot$“. Například pro prvky (g_1, g_2), (h_1, h_2) součinu $G_1 \oplus G_2$ píšeme místo $(g_1, g_2) \cdot (h_1, h_2)$ pouze $(g_1, g_2)(h_1, h_2)$.

Cvičení

10.1.1.$^{\heartsuit}$ *Mějme grupu $(\mathbb{R}, +)$, součin $(\mathbb{R}, +) \oplus (\mathbb{R}, +)$. Jaký je výsledek operace dvou prvků $(1,2) + (3,3)$?*

10.1.2.$^{\heartsuit}$ *Mějme grupu* $(\mathbb{R}\setminus\{0\},\cdot)$, *součin* $(\mathbb{R}\setminus\{0\},\cdot)\oplus(\mathbb{R}\setminus\{0\},\cdot)$. *Jaký je výsledek operace dvou prvků* $(1,2)\cdot(3,3)$*?*

10.1.3. Dokažte Větu 10.2., tj. ukažte, že vnější součin množin $G_1\oplus G_2\oplus\cdots\oplus G_n=(G_1\times G_2\times\cdots\times G_n,\cdot)$ *tvoří grupu.*

10.1.4. Dokažte nebo vyvraťte: Kleinova grupa (Tabulka 10.1.) je izomorfní s dihedrální grupou $(D_2,\circ)$ *(Tabulka 1.6.).*

10.1.5. Ukažte, že Kleinova grupa (Tabulka 10.1.) není izomorfní s grupou $(\mathbb{Z}_4,+)$.

10.1.6. Mějme čtverečkovanou síť (šachovnici) o rozměru 3×7 *políček na povrchu toru. Souřadnice kratšího rozměru popíšeme pomocí prvků grupy* $(\mathbb{Z}_3,+)$ *a souřadnice delšího rozměru popíšeme pomocí prvků grupy* $(\mathbb{Z}_7,+)$. *Mějme libovolný prvek* $(a,b)\in\mathbb{Z}_3\oplus\mathbb{Z}_7$. *Čemu odpovídá a) opakované přičítání prvku* $(1,0)$ *k prvku* (a,b)*? b) opakované přičítání prvku* $(0,1)$ *k prvku* (a,b)*? c) opakované přičítání prvku* $(1,1)$ *k prvku* (a,b)*? d) Po kolika přičteních v předchozích částech dostaneme opět prvek* (a,b)*?*

10.2. Vlastnosti vnějšího součinu

Následující věta ukazuje, že jestliže známe řády prvků v jednotlivých grupách můžeme snadno určit řád libovolného prvku vnějšího součinu grup.

Věta 10.3. *Řád prvku ve vnějším součinu je roven nejmenšímu společnému násobku řádů jeho složek, tj. pro každé* $(g_1,g_2)\in G_1\oplus G_2$ *platí* $|(g_1,g_2)|=\mathrm{NSN}(|g_1|,|g_2|)$.

Větu 10.3. nebudeme dokazovat, neboť tvrzení je snadné zobecnit pro vnější součin konečného počtu grup. Dokážeme obecnější tvrzení.

Věta 10.4. *Řád prvku ve vnějším součinu je roven nejmenšímu společnému násobku řádů jeho složek, tj. pro každé* $(g_1,g_2,\ldots,g_n)\in G_1\oplus G_2\oplus\cdots\oplus G_n$ *platí* $|(g_1,g_2,\ldots,g_n)|=\mathrm{NSN}(|g_1|,|g_2|,\ldots,|g_n|)$.

Důkaz. Symbolem e_i označme neutrální prvek grupy $(G_i,\circ_i)$ pro $i=1,2,\ldots,n$. Dále označme řád $r=|(g_1,g_2,\ldots,g_n)|$ a nejmenší společný násobek $s=NSN(|g_1|,|g_2|,\ldots,|g_n|)$. Protože číslo s je násobkem všech řádů $|g_1|,|g_2|,\ldots,|g_n|$, tak platí $(g_1,g_2,\ldots,g_n)^s=(e_1,e_2,\ldots,e_n)$. To znamená, že řád $r\le s$. Naopak, protože podle definice vnějšího součinu platí $(g_1^r,g_2^r,\ldots,g_n^r)=(g_1,g_2,\ldots,g_n)^r=(e_1,e_2,\ldots,e_n)$, tak číslo r je násobkem všech řádů $|g_1|,|g_2|,\ldots,|g_n|$. Proto $s\le r$. Celkem dostáváme $|(g_1,g_2,\ldots,g_n)|=r=s=NSN(|g_1|,|g_2|,\ldots,|g_n|)$. □

Příklad 10.3. a následující Příklad 10.4. pěkně ilustrují tvrzení Věty 10.3. (i obecnější verze z Věty 10.4.). Zatímco součin $\mathbb{Z}_2\oplus\mathbb{Z}_3$ je cyklická grupa, která je součinem dvou cyklických grup nesoudělného řádu, tak součin $\mathbb{Z}_2\oplus\mathbb{Z}_4$ není cyklická grupa, neboť řády 2 a 4 nejsou nesoudělné.

Příklad 10.4. Mějme cyklické grupy $\mathbb{Z}_2$, $\mathbb{Z}_4$. Ukážeme, že jejich součin $\mathbb{Z}_2\oplus\mathbb{Z}_4$ není cyklická grupa. Nosič grupy $\mathbb{Z}_2\oplus\mathbb{Z}_4$ je množina $\{(0,0),(0,1),(0,2),(0,3),(1,0),(1,1),(1,2),(1,3)\}$. Určíme řády jednotlivých prvků: Neutrální prvek $(0,0)$ je řádu 1. Ihned vidíme, že prvek $(1,0)$ je řádu 2, neboť $(1,0)^1\neq(0,0)$, ale $(1,0)^2=(0,0)$. Stejně řády prvků $(0,2)$ a $(1,2)$ jsou rovny 2. Platí

$$(0,2)^1\neq(0,0),\quad (0,2)^2=(0,0),\qquad (1,2)^1\neq(0,0),\quad (1,2)^2=(0,0).$$

Všechny čtyři zbývající prvky $(0,1)$, $(0,3)$, $(1,1)$ a $(1,3)$ jsou řádu 4. Platí

$$\begin{array}{llll}(0,1)^1\neq(0,0), & (0,1)^2=(0,2), & (0,1)^3=(0,3), & (0,1)^4=(0,0),\\ (0,3)^1\neq(0,0), & (0,3)^2=(0,2), & (0,3)^3=(0,1), & (0,3)^4=(0,0),\\ (1,1)^1\neq(0,0), & (1,1)^2=(0,2), & (1,1)^3=(1,3), & (1,1)^4=(0,0),\\ (1,3)^1\neq(0,0), & (1,3)^2=(0,2), & (1,3)^3=(1,1), & (1,3)^4=(0,0).\end{array}$$

Toto znamená, že žádný z jejích prvků není generátorem celé grupy a že grupa $\mathbb{Z}_2\oplus\mathbb{Z}_4$ není cyklická.

Příklad 10.5. Mějme grupy $(\mathbb{Z}_2,+)$ a $(D_3,\circ)$. Jejich součin $(\mathbb{Z}_2,+)\oplus(D_3,\circ)$ je grupa, která není cyklická grupa. Nosič součinu $(\mathbb{Z}_2,+)\oplus(D_3,\circ)$ má dvanáct prvků $(0,R_0)$, $(0,R_{120})$, $(0,R_{240})$, $(0,Z_A)$, $(0,Z_B)$, $(0,Z_C)$, $(1,R_0)$, $(1,R_{120})$, $(1,R_{240})$, $(1,Z_A)$, $(1,Z_B)$, $(1,Z_C)$ a žádný není generátorem řádu 12. Řády jednotlivých prvků jsou podle Věty 10.3. nejmenším společným násobkem řádů jednotlivých prvků. A protože

grupa $(\mathbb{Z}_2,+)$ obsahuje prvky řádu 1 a 2 a grupa $(D_3,\circ)$ obsahuje prvky řádů 1, 2 a 3, tak nejvyšší řád prvků v součinu je $\mathrm{NSN}(2,3)=6\neq 12$. Pro názornost určíme řád každého prvku.

$$\begin{aligned}
|(0,R_0)| &= \mathrm{NSN}(1,1)=1, & |(0,R_{120})| &= \mathrm{NSN}(1,3)=3, & |(0,R_{420})| &= \mathrm{NSN}(1,3)=3,\\
|(0,Z_A)| &= \mathrm{NSN}(1,2)=2, & |(0,Z_B)| &= \mathrm{NSN}(1,2)=2, & |(0,Z_C)| &= \mathrm{NSN}(1,2)=2,\\
|(1,R_0)| &= \mathrm{NSN}(2,1)=2, & |(1,R_{120})| &= \mathrm{NSN}(2,3)=6, & |(1,R_{420})| &= \mathrm{NSN}(2,3)=6,\\
|(1,Z_A)| &= \mathrm{NSN}(2,2)=2, & |(1,Z_B)| &= \mathrm{NSN}(2,2)=2, & |(1,Z_C)| &= \mathrm{NSN}(2,2)=2
\end{aligned}$$

Následující dva příklady ukazují význam Věty 10.3. Jestliže víme, že daná grupa je součinem menších grup, tak díky znalosti struktury grupy umíme určit počet prvků daného řádu i počet podgrup některých řádů.

Příklad 10.6. Mějme grupy $(\mathbb{Z}_3,+)$ a $(\mathbb{Z}_9,+)$. Určíme počet prvků a) řádu 3, b) řádu 9, c) řádu 27.

a) Spočítáme všechny prvky řádu 3. Aby prvek $(a,b)\in\mathbb{Z}_3\oplus\mathbb{Z}_9$ byl řádu 3, tak nastane právě jedna z možností. Buď $|a|=3$ a $|b|=1$ nebo 3, nebo $|a|=1$ a $|b|=3$. V prvním případě je prvek $a\in\mathbb{Z}_3$ kterýkoliv ze dvou prvků různých od neutrálního. V grupě $(\mathbb{Z}_9,+)$ je jediný prvek řádu 1 a právě dva prvky řádu 3, a sice $b=3$ nebo $b=6$. Ostatní prvky jsou s 9 nesoudělné, a jsou proto řádu 9. Máme proto $2\cdot 3=6$ prvků řádu 3.

Druhá možnost pro $|a|=1$ připouští pouze dva možné prvky $b=3,6$. Dostáváme $1\cdot 2=2$ prvky řádu 3.

Celkem má grupa $\mathbb{Z}_3\oplus\mathbb{Z}_9$ $6+2=8$ prvků řádu 3. Pro názornost uvedeme, že se jedná o prvky $(1,0)$, $(2,0)$, $(1,3)$, $(2,3)$, $(1,6)$, $(2,6)$, $(0,3)$, $(0,6)$.

b) Aby prvek $(a,b)\in\mathbb{Z}_3\oplus\mathbb{Z}_9$ byl řádu 9, tak musí být $|b|=9$ a dále buď $|a|=1$, nebo $|a|=3$. Prvek a tedy může být libovolný prvek grupy $(\mathbb{Z}_3,+)$. V grupě $(\mathbb{Z}_9,+)$ je jediný prvek řádu 1, právě dva prvky řádu 3 ($b=3$, $b=6$) a všech 6 zbývajících prvků je s řádem grupy nesoudělných, a proto jsou řádu 9. Celkem máme proto $3\cdot 6=18$ prvků řádu 9. Jedná se právě o prvky (a,b), kde $a\in\{0,1,2\}$, $b\in\{1,2,4,5,7,8\}$.

c) V grupě $(\mathbb{Z}_3,+)\oplus(\mathbb{Z}_9,+)$ žádný prvek řádu 27 neexistuje, neboť v grupě $(\mathbb{Z}_3,+)$ jsou pouze prvky řádu 1 nebo 3 a v grupě $(\mathbb{Z}_9,+)$ jsou pouze prvky řádu 1, 3, nebo 9. Řád prvky v součinu grup je nejmenším společným násobkem řádů jednotlivých prvků, a je proto nejvýše $\mathrm{NSN}(3,9)=9$.

Všimněte si, že tuto informaci jsme mohli získat také z výsledků předchozím částí. Prvek $(0,0)$ je jediný prvek řádu 1, dále je v součinu 8 prvků řádu 3 a 18 prvků řádu 9. To dává celkem všech $1+8+18=27$ prvků grupy, a proto žádný prvek jiného řádu v grupě $(\mathbb{Z}_3,+)\oplus(\mathbb{Z}_9,+)$ není. ✓

Příklad 10.7. Mějme grupy $(\mathbb{Z}_3,+)$ a $(\mathbb{Z}_9,+)$. Určíme počet a) podgrup řádu 3, b) cyklických podgrup řádu 9.

Podle Příkladu 10.6. víme, že v grupě $(\mathbb{Z}_3,+)\oplus(\mathbb{Z}_9,+)$ je 8 prvků řádu 3 a 18 prvků řádu 9.

a) Každý prvek řádu 3 je generátorem cyklické grupy řádu 3, která obsahuje právě dva takové prvky. Žádné dvě podgrupy řádu 3 nemají kromě neutrálního prvku jiné společné prvky, proto existuje právě $8/2=4$ takových grup.

b) Každý prvek řádu 9 je generátorem cyklické grupy řádu 9. Každá cyklická grupa řádu 9 obsahuje právě šest takových prvků. Žádné dvě různé cyklické grupy nemají společný generátor, proto existují právě $18/6=3$ takových grup. ✓

Otázky:

- Existuje takový vnější součin grup $(G_1,\circ_1)\oplus(G_2,\circ_2)$, aby součin byl cyklickou grupou, ale alespoň jedna z grup $(G_1,\circ_1)$, $(G_2,\circ_2)$ nebyla cyklickou grupou?
- Najdete příklad vnějšího součinu grup $(G_1,\circ_1)\oplus(G_2,\circ_2)$ a jeho vlastní podgrupy H takové, aby podgrupa H byla jiného řádu než $|G_1|$ a $|G_2|$ a aby podgrupa H nebyla cyklickou grupou?

Věta 10.5. *Mějme konečné cyklické grupy $(G_1,\circ_1)$ a $(G_2,\circ_2)$. Grupa $G_1\oplus G_2$ je cyklická grupa právě tehdy, když $|G_1|$ a $|G_2|$ jsou nesoudělná čísla.*

Důkaz. Označme řády grup $n_1=|G_1|$ a $n_2=|G_2|$. Jedná se o tvrzení ve tvaru ekvivalence, dokážeme obě implikace.

„⇒“ Jestliže je součin $G_1\oplus G_2$ cyklická grupa, označme (g_1,g_2) nějaký její generátor. Dále označme $d=\mathrm{NSD}(n_1,n_2)$. Platí $(g_1,g_2)^{n_1n_2/d}=(g_1^{n_1n_2/d},g_2^{n_1n_2/d})=((g_1^{n_1})^{n_2/d},(g_2^{n_2})^{n_1/d})=(e_1^{n_2/d},e_2^{n_1/d})=(e_1,e_2)$, kde e_1 je neutrální prvek grupy $(G_1,\circ_1)$ a e_2 je neutrální prvek grupy $(G_2,\circ_2)$. Protože prvek (g_1,g_2) je

generátorem cyklické grupy řádu n_1n_2, jeho řád je $|(g_1,g_2)| = n_1n_2$. Současně ale $n_1n_2 = |(g_1,g_2)| \leq n_1n_2/d$, proto $d = 1$, tj. řády n_1 a n_2 jsou nesoudělná čísla.
„⇐“ Označme generátory $G_1 = \langle g_1\rangle$, $G_2 = \langle g_2\rangle$ a předpokládejme, že n_1 a n_2 jsou nesoudělná čísla. Potom řád prvku (g_1,g_2) je podle Věty 10.3. $|(g_1,g_2)| = \mathrm{NSN}(n_1,n_2) = n_1n_2 = |G_1 \oplus G_2|$, a proto prvek (g_1,g_2) řádu n_1n_2 je jejím generátorem. Součin $G_1 \oplus G_2$ je cyklická grupa. □

Není těžké ukázat následující obecnější tvrzení. Důkaz je ponechán jako Cvičení 10.2.2.

Důsledek 10.6. *Mějme konečné cyklické grupy $(G_1,\circ_1)$, $(G_2,\circ_2)$, až $(G_n,\circ_n)$. Grupa $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ je cyklická grupa právě tehdy, když $|G_i|$ a $|G_j|$ jsou nesoudělná čísla pro každé $i \neq j \in \{1,2,\ldots,n\}$.*

Speciálně, protože každá konečná cyklická grupa řádu k je izomorfní s grupou $(\mathbb{Z}_k,+)$, tak dostáváme následující tvrzení.

Důsledek 10.7. *Mějme přirozené číslo $m = n_1 \cdot n_2 \ldots n_k$, kde $n_i \in \mathbb{N}$. Grupa $\mathbb{Z}_m \simeq \mathbb{Z}_{n_1} \oplus \mathbb{Z}_{n_2} \oplus \ldots \oplus \mathbb{Z}_{n_k}$ právě tehdy, když n_i a n_j jsou nesoudělná čísla pro každé $i \neq j \in \{1,2,\ldots,k\}$.*

Příklad 10.8. Dihedrální grupa $(D_3,\circ)$ není izomorfní s žádným vnějším součinem netriviálních grup. Stačí si uvědomit, že $(D_3,\circ)$ je řádu 6 a pokud by byla vnějším součinem nějakých dvou netriviálních grup, muselo by se jednat nějaké dvě grupy řádu 2 a 3. Avšak takové grupy jsou až na izomorfismus jediné, a sice cyklické grupy $(\mathbb{Z}_2,+)$ a $(\mathbb{Z}_3,+)$. Jejich součin by musel podle Věty 10.5. být také cyklickou grupou. Dihedrální grupa $(D_3,\circ)$ však není podle Příkladu 6.4. cyklická.

Cvičení

10.2.1. Je grupa $\mathbb{Z}_7 \oplus \mathbb{Z}_{13}$ cyklická? Pokud ano, najděte nějaký její generátor.

10.2.2. Mějme konečné cyklické grupy $(G_1,\circ_1)$, $(G_2,\circ_2)$, až $(G_n,\circ_n)$. Dokažte Důsledek 10.6., tj. dokažte, že grupa $G_1 \oplus G_2 \oplus \cdots \oplus G_n$ je cyklická grupa právě tehdy, když $|G_i|$ a $|G_j|$ jsou nesoudělná čísla pro každé $i \neq j \in \{1,2,\ldots,n\}$.

10.2.3.$^\heartsuit$ Najděte všechny neizomorfní grupy a) řádu 1, b) řádu 2, c) řádu 3, d) prvočíselného řádu p.

10.2.4. Najděte všechny neizomorfní grupy řádu 4.

10.2.5. Ukažte, že vnější součin dvou komutativních grup je také komutativní grupa.

10.2.6. Ukažte, že dihedrální grupa $(D_4,\circ)$ není vnějším součinem žádných dvou netriviálních grup.

10.2.7. Na povrchu toru máme rovnoměrně nakreslenou mřížku, jejíž políčka odpovídají šachovnici o rozměru 8×9 políček (políčka sítě odpovídají prvkům grupy $\mathbb{Z}_8 \oplus \mathbb{Z}_9$). Lze tuto šachovnici projet jezdcem tak, abychom na každé políčko vstoupili právě jednou?

10.2.8. Mějme libovolné pevně zvolené $n \in \mathbb{N}$. Uveďte příklad takového homomorfismu f grupy $(G_1,\circ_1)$ do grupy $(G_2,\circ_2)$, aby nosič grupy $(G_1,\circ_1)$ byl nekonečně mohutnosti a aby platilo $|\mathrm{Ker}(f)| = n$.

10.2.9. Mějme grupy $(K,\circ_1)$ řádu k a $(H,\circ_2)$ řádu h, které nejsou cyklické. Může jejich součin $K \oplus H$ obsahovat cyklickou podgrupu řádu většího než $\max\{k,h\}$?

10.2.10. Najděte všechny neizomorfní grupy řádu 6.*

10.3. Grupa jednotek modulo n

V této kapitole ukážeme, jak vnější součin grup umožní popsat strukturu větších grup tak, že je zapíšeme jako vnější součin menších grup.

Nejprve připomeňme, že v Příkladu 2.19. jsme zavedli grupu $U(n)$ (grupu jednotek modulo n). Nyní v Příkladu 10.9. koncept grupy jednotek modulo n doplníme o další vlastnost. Ukážeme, jak sestavit podgrupy $U_k(n)$ v grupě jednotek modulo n.

Příklad 10.9. Mějme přirozené číslo n větší než 1, mějme jeho přirozeného dělitele k většího než 1 a mějme grupu jednotek $(U(n),\cdot)$. Symbolem $U_k(n)$ označme množinu $\{x \in U(n) : x \equiv 1 \pmod k\}$. Ukážeme, že dvojice $(U_k(n),\cdot)$ tvoří podgrupu grupy jednotek $(U(n),\cdot)$.
Množina $U_k(n)$ je jistě neprázdná a konečná podmnožina množiny $U(n)$, například $1 \in U_k(n)$ a množina $U(n)$ obsahuje nejvýše $n-1$ prvků. Abychom ukázali, že $(U_k(n),\cdot)$ tvoří podgrupu grupy $(U(n),\cdot)$, použijeme Test konečné podgrupy (Věta 3.5.). Stačí ukázat, že operace „$\cdot$“ je na množině $U_k(n)$ uzavřená.

Mějme $a, b \in U_k(n)$ a $U_k(n) \subseteq U(n)$. Podle Příkladu 2.19., že $a \cdot b \in U(n)$. To znamená, že existuje $p \in \mathbb{Z}$ takové, že $ab = 1 + pn$. Nyní, pokud k je dělitelem čísla n, tak existuje $q \in \mathbb{N}$ takové že $n = qk$. Můžeme psát $ab = 1 + pn = 1 + pqk$, což znamená, že $a \cdot b \equiv 1 \pmod{k}$ a tedy $a \cdot b \in U_k(n)$. Operace „$\cdot$“ je na množině $U_k(n)$ uzavřená a $(U_k(n), \cdot)$ tvoří podgrupu grupy $(U(n), \cdot)$. ✓

Všimněte si, že pokud číslo k není dělitelem čísla n, tak $(U_k(n), \cdot)$ obecně *netvoří* podgrupu grupy jednotek $(U(n), \cdot)$, protože operace „$\cdot$“ nebude na množině $U_k(n)$ uzavřená. Podle Věty o jednoznačnosti podílu a zbytku (Věta 0.2.) můžeme psát $n = qk + r$, kde $0 \leq r < k$. Podobně jako v předchozím odstavci můžeme pro každé $a, b \in U_k(n)$ psát $ab = 1 + pn = 1 + p(qk + r) = 1 + pr + pqk \equiv 1 + pr \pmod{k}$, což pro $r \neq 0$ je číslo, které obecně není kongruentní s 1 modulo k, a proto $ab \notin U_k(n)$.

Příklad 10.10. Mějme grupu jednotek $(U(15), \cdot)$. Ukážeme, jak vypadají podgrupy $(U_2(15), \cdot)$, $(U_3(15), \cdot)$, $(U_5(15), \cdot)$ a $(U_{15}(15), \cdot)$.
Množina $U(n)$ obsahuje přirozená čísla menší než 15 nesoudělná s 15. Platí $U(n) = \{1, 2, 4, 7, 8, 11, 13, 14\}$. Tabulka operace „$\cdot$“ na množině $U(15)$ je Tabulka 4.3. Pro přehlednost ji uvedeme znovu v Tabulce 10.2.

$\cdot$	1	2	4	7	8	11	13	14
1	1	2	4	7	8	11	13	14
2	2	4	8	14	1	7	11	13
4	4	8	1	13	2	14	7	11
7	7	14	13	4	11	2	1	8
8	8	1	2	11	4	13	14	7
11	11	7	14	2	13	1	8	4
13	13	11	7	1	14	8	4	2
14	14	13	11	8	7	4	2	1

Tabulka 10.2.: *Operace násobení v grupě* $(U(15), \cdot)$.

Podgrupu $(U_2(15), \cdot)$ nemá podle definice smysl sestavovat, protože $2 \nmid 15$. Množinu $U_2(15)$ sestavit můžeme, platí $U_2(15) = \{1, 7, 11, 13\}$, avšak operace „$\cdot$“ nebude na této množině uzavřená. Například $7 \cdot 11 = 77 \equiv 2 \pmod{15}$, avšak $2 \notin U_2(15)$.

Nosič podgrupy $(U_3(15), \cdot)$ obsahuje pouze čísla $(U_3(15), \cdot) = \{x \in U(15) : x \equiv 1 \pmod{3}\}$. Platí $U_3(15) = \{1, 4, 7, 13\}$. Tabulka operace „$\cdot$“ na množině $U_3(15)$ je Tabulka 10.3.

$\cdot$	1	4	7	13
1	1	4	7	13
4	4	1	13	7
7	7	13	4	1
13	13	7	1	4

Tabulka 10.3.: *Operace násobení v grupě* $(U_3(15), \cdot)$.

Nosič podgrupy $(U_5(15), \cdot)$ obsahuje pouze čísla $(U_5(15), \cdot) = \{x \in U(15) : x \equiv 1 \pmod{5}\}$. Platí $U_5(15) = \{1, 11\}$. Tabulka operace „$\cdot$“ na množině $U_5(15)$ je Tabulka 10.4.

$\cdot$	1	11
1	1	11
11	11	1

Tabulka 10.4.: *Operace násobení v grupě* $(U_5(15), \cdot)$.

Nosič podgrupy $(U_{15}(15), \cdot)$ také obsahuje jediné číslo $U_{15}(15) = \{1\}$ a grupa $U_{15}(15)$ je triviální. ✓

Grupa jednotek a vnější součin grup
Na závěr kapitoly uvedeme bez důkazu několik tvrzení, která pěkně ilustrují význam vnějšího součinu grup. Nejprve vyslovíme následující pomocné tvrzení.

Lemma 10.8. *Mějme nesoudělná přirozená čísla p, q. Grupa $(U_p(pq), \cdot)$ je izomorfní s grupou $(U(q), \cdot)$. Symbolicky zapsáno $(U_p(pq), \cdot) \simeq (U(q), \cdot)$.*

Příklad 10.11. Navážeme na Příklad 10.10. Ukážeme, jak vypadá izomorfismus podgrupy $(U_3(15), \cdot)$ do grupy $(U(5), \cdot)$ zaručený v Lemmatu 10.8.

Mějme zobrazení $f : U_3(15) \to U(5)$ dané předpisem $f(x) = x \bmod 3$ pro každé $x \in U_3(15)$, kde operace mod vyjadřuje zbytek po dělení čísla x číslem 3. Dostaneme následující obrazy.

$$f(1) = 1, \quad f(4) = 4 \bmod 5 = 4, \quad f(7) = 7 \bmod 5 = 2, \quad f(13) = 13 \bmod 5 = 3.$$

Zatímco tabulka levé grupy $(U_3(15), \cdot)$ je Tabulka 10.3., tak tabulka pravé grupy je Tabulka 10.5. Tabulka je přeuspořádána tak, aby bylo zřejmé, že zobrazení f je izomorfismus. ✓

$\cdot$	1	4	2	3
1	1	4	2	3
4	4	1	3	2
2	2	3	4	1
3	3	2	1	4

Tabulka 10.5.: *Operace násobení v grupě* $(U(5), \cdot)$.

Následující věta říká, že některé grupy jednotek modulo n můžeme vyjádřit jako vnější součin menších grup.

Věta 10.9. *Mějme nesoudělná přirozená čísla p, q. Grupa jednotek $(U(pq), \cdot)$ je izomorfní se součinem grup $(U(p), \cdot)$ a $(U(q), \cdot)$. Symbolicky zapsáno $(U(pq), \cdot) \simeq (U(p), \cdot) \oplus (U(q), \cdot)$.*

Příklad 10.12. Grupu jednotek $(U(35), \cdot)$ napíšeme jako vnější součin menších grup. Protože $35 = 5 \cdot 7$ a čísla 5 a 7 jsou nesoudělná, tak podle Věty 10.9. můžeme psát $U(35) \simeq (U(5), \cdot) \oplus (U(7), \cdot)$.

Grupu jednotek $(U(25), \cdot)$ však podle Věty 10.9. rozložit nemůžeme, protože číslo 25 nelze rozložit na součin dvou přirozených čísel větších než 1. Můžeme však využít následující větu, kterou dokázal Gauss již v roce 1801. Uvedeme ji opět bez důkazu.

Věta 10.10. *Platí následující tvrzení.*

(i) Grupa $(U(2), \cdot)$ je triviální.
(ii) Grupa $(U(4), \cdot)$ je izomorfní s grupou $(\mathbb{Z}_2, +)$.
(iii) Pro $n \geq 3$ je grupa $(U(2^n), \cdot)$ izomorfní s grupou $(\mathbb{Z}_2, +) \oplus (\mathbb{Z}_{2^{n-2}}, +)$.
(iv) Mějme liché prvočíslo p. Grupa $(U(p^n), \cdot)$ je izomorfní s grupou $(\mathbb{Z}_{p^n - p^{n-1}}, +)$.

Příklad 10.13. Grupu jednotek $(U(25), \cdot)$ napíšeme jako vnější součin menších grup. Protože $25 = 5^2$, tak podle Věty 10.9. můžeme psát $U(25) \simeq (\mathbb{Z}_{5^2 - 5^1}, +) \simeq (\mathbb{Z}_{20}, +)$.

S pomocí Věty 10.9. a Věty 10.10. umíme libovolnou grupu jednotek modulo n vyjádřit jako vnější součin (menších) cyklických grup.

Příklad 10.14. Pro grupu $(U(720), \cdot)$ platí

$$(U(720), \cdot) = (U(2^4 \cdot 3^2 \cdot 5), \cdot) \simeq (U(2^4), \cdot) \oplus (U(3^2), \cdot) \oplus (U(5), \cdot) \simeq (\mathbb{Z}_2, +) \oplus (\mathbb{Z}_4, +) \oplus (\mathbb{Z}_6, +) \oplus (\mathbb{Z}_4, +),$$

přičemž první rovnost odpovídá rozkladu na prvočísla, druhá rovnost vyjadřuje izomorfismus dle Věty 10.9. a třetí rovnost vyjadřuje izomorfismus dle Věty 10.10.

Cvičení

10.3.1.$^{\heartsuit}$ *Napište a) grupu $(U(100), \cdot)$; b) grupu $(U(1000), \cdot)$; c) grupu $(U(10!), \cdot)$ jako vnější součin cyklických grup.*

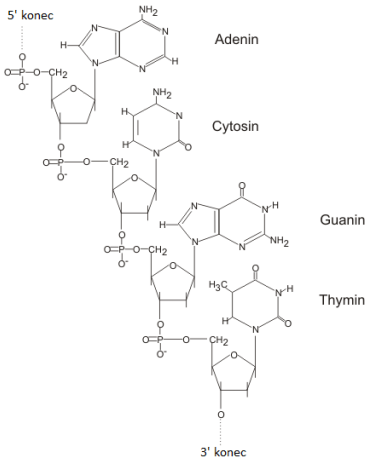
10.3.2. Sestavte podgrupy $(U_k(20), \cdot)$ grupy $(U(20), \cdot)$ pro všechna vhodná k.

10.4. Aplikace

Na závěr kapitoly zmíníme vybrané aplikace, které využívají vnější součin grup.

Zápis DNA

Deoxyribonukleová kyselina, zkráceně označovaná DNA, se skládá z dlouhých řetězů tzv. *nukleotidů*, které jsou navzájem propojené do dlouhého lineárního řetězce (Obrázek 10.1.). Takové řetězce deoxyribonukleové kyseliny mohou existovat jako samostatné jednovláknové molekuly, avšak často vytváří vícevláknové



Obrázek 10.1.: *Chemická struktura úseku DNA.*

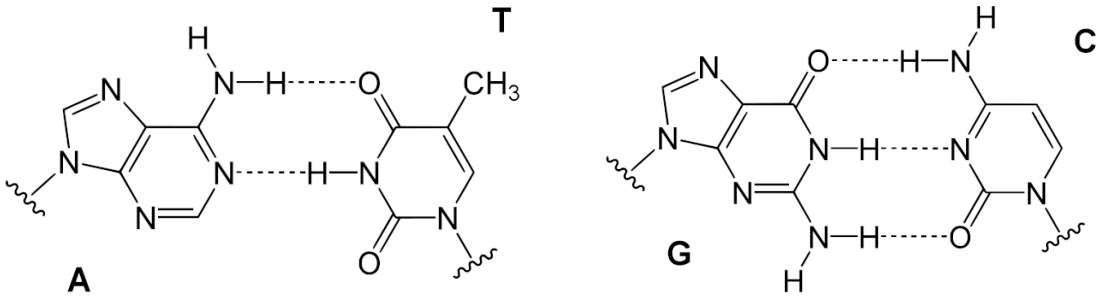
struktury, které jsou složené z několika jednovláknových řetězců spojených tzv. *vodíkovými můstky*. Vodíkové můstky jsou typem slabé vazební interakce mezi dvěma (případně více vlákny DNA), které způsobí, že výsledná vícevláknová struktura je stabilnější.

Ve většině živých organismů je typickým příkladem vícevláknového uspořádání DNA pravotočivá dvoušroubovice, která je tvořená dvěma lineárními řetězci nukleotidů. Každý nukleotid má tři stavební části:

- *deoxyribóza* – pětiuhlíkový cukr (pentóza),
- *fosfát* – vazebný zbytek kyseliny ortofosforečné, který je navázán na jednom uhlíku deoxyribózy daného nukleotidu a jednom uhlíku deoxyribózy předchozího nukleotidu,
- *nukleová báze* – nejčastěji jedna ze čtyř nukleových bází adenin A, guanin G (purinové báze), a thymin T a cytosin C, (pyrimidinové báze).

Protože oba lineární řetězce jsou spojeny velkým množstvím vodíkových můstků, je žádoucí, aby se v dvoušroubovici proti sobě vyskytovaly vždy určité nukleové báze. Zpravidla se

1) A (adenin) propojuje s T (thyminem) dvěma vodíkovými vazbami (Obrázek10.2. vlevo),
2) G (guanin) propojuje s C (cytosinem) třemi vodíkovými vazbami (Obrázek10.2. vpravo).



Obrázek 10.2.: *Chemická struktura úseku DNA.*

Řetězec nukleových bází deoxyribonukleové kyseliny se zpravidla zapisuje jako řetězec písmen značících jednotlivé báze. Mějme například řetězec `TACGGACGGG`. V dvoušroubovici bude protilehlý řetězec `ATGCCTGCCC`.

Řetězce nukleových bází je šikovné modelovat v rámci grupy $(\mathbb{Z}_4,+)\oplus(\mathbb{Z}_4,+)\oplus\cdots\oplus(\mathbb{Z}_4,+)$. Nukleovým bázím přiřadíme prvky grupy $\mathbb{Z}_4$ podle následujícího schématu:

- 0 . . . adenin A,
- 1 . . . guanin G,
- 2 . . . thimin T,
- 3 . . . cytosin C.

Všimněte si, že v grupě $\mathbb{Z}_4$ nyní přičtení prvku 2 odpovídá přechodu k protilehlé bázi $0+2=2$, $2+2=0$, $1+2=3$ a $3+2=1$. Zapíšeme-li řetězec `TACGGACGGG` jako prvek $\underbrace{(\mathbb{Z}_4,+)\oplus(\mathbb{Z}_4,+)\oplus\cdots\oplus(\mathbb{Z}_4,+)}_{10}$, dostaneme 2031103111 (zapsáno bez čárek a závorek). Přičtením prvku 2222222222 dostaneme prvek

$$2031103111+2222222222=0213321333,$$

kterému vskutku odpovídá protilehlý řetězec `ATGCCTGCCC` dvoušroubovice deoxyribonukleové kyseliny.

Odkazy:

- https://cs.wikipedia.org/wiki/DNA

Kapitola 11. Okruhy, obory integrity a tělesa

V předchozích kapitolách jsme pracovali se strukturami s jedinou operací. Měli jsme sice grupu $(\mathbb{Z}, +)$ a pologrupu případně monoid $(\mathbb{Z}, \cdot)$, avšak obě struktury jsme vnímali odděleně. V grupě $(\mathbb{Z}, +)$ můžeme sčítat a také odčítat (s využitím opačných prvků). V monoidu $(\mathbb{Z}, \cdot)$ můžeme násobit, avšak analogie „dělení“ není možná.

Při počítání s racionálními čísly, případně s reálnými čísly však běžně sčítáme, odčítáme, násobíme i dělíme (nenulovými čísly). Navíc jsou tyto operace (obvyklé sčítání a násobení celých, racionálních nebo reálných čísel) provázané: opakované sčítání stejné hodnoty můžeme popsat jako násobek, resp. součin. Součet dvou stejných násobků můžeme vyjádřit jako násobek součtu: $ka + kb = k(a + b)$ a podobně.

Doposud jsme nepožadovali žádnou systematikou souvislost mezi operacemi nad stejnou nosnou množinou. V této kapitole budeme pracovat se strukturami se dvěma operacemi a zavedeme zobecnění celých čísel: tzv. okruh, ve kterém budeme umět provádět tři operace, jež budou analogií sčítání, odčítání a násobení. Podobně zavedeme analogii počítání s racionálními nebo reálnými čísly: tzv. těleso se čtyřmi operacemi, které budou zobecněním sčítání, odčítání, násobení a dělení (nenulovými čísly). Analogické operace je možno popsat i pro jiné množiny, než jsou klasické číselné obory.

Využití struktur se dvěma operacemi je řada. Například v teorii kódování jsou nezastupitelné při konstrukci řady kódů, které pomáhají zajistit bezchybný přenos dat i v případě, že přenosový kanál má nízkou kvalitu a dochází ke zkreslení přenášených dat. V teorii kombinatorických designů se používají pro konstrukci systémů množin se striktně předepsanými průniky a designy se používají například při plánování statisticky vyhodnocovaných experimentů.

11.1. Okruh

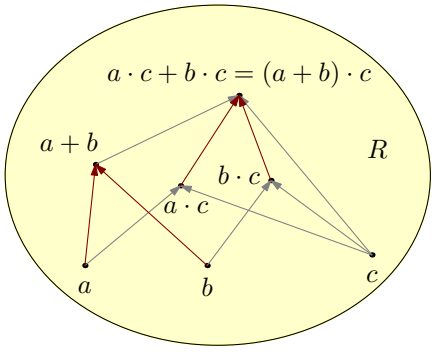
Nejobecnější strukturou se dvěma operacemi je tzv. okruh, který je zobecňuje počítání s celými čísly. Obě operace nad stejnou nosnou množinou prvků budou provázané distributivními zákony.

Definice Mějme neprázdnou množinu R a na R dvě binární operace „$+$“ a „$\cdot$“. Uspořádaná trojice $(R, +, \cdot)$ je *okruh* právě tehdy, když platí

(i) $\forall a, b \in R : a + b = b + a$ (komutativita „$+$“)
(ii) $\forall a, b, c \in R : (a + b) + c = a + (b + c)$ (asociativita „$+$“)
(iii) $\exists 0 \in R\ \forall a \in R : a + 0 = a$ (existence neutrálního prvku vzhledem k „$+$“)
(iv) $\forall a \in R\ \exists - a \in R : a + (-a) = 0$ (existence opačného prvku vzhledem k „$+$“)
(v) $\forall a, b, c \in R : (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (asociativita „$\cdot$“)
(vi) $\forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c$, $(b + c) \cdot a = b \cdot a + c \cdot a$ (distributivita zleva, zprava vhledem k „$+$“)

Poznámka 11.1. Definici bychom mohli vyslovit v kratší formě: okruh $(R, +, \cdot)$ je trojice, kde $(R, +)$ je komutativní grupa (což plyne z položek (i) až (iv)), $(R, \cdot)$ je pologrupa (což plyne z položky (ii)) a obě operace jsou provázány požadavkem na distributivitu zleva i zprava vzhledem k operaci „$+$“ (položka (vi)).

Distributivita operace „$\cdot$“ vzhledem k operaci „$+$“ znamená, že „součin součtu“ je roven „součtu součinů“. Provázanost obou operací je znázorněna na Obrázku 11.1., každá operace jinou barvou.



Obrázek 11.1.: *Distributivita (zprava) provazuje obě operace.*

Operace sice značíme „+“ a „·“, ale nemusí se jednat o sčítání a násobení, ale o jakékoliv operace, které splňují podmínky definice. Popsány mohou být například Cayleyho tabulkou. Podobně jako při počítání s čísly budeme předpokládat, že druhá operace „·“ má přednost před první operací „+“, jestliže priorita není určena závorkami jinak.

Násobení není opakované sčítání
Pozor: prvky na a $n \cdot a$ bychom měli rozlišovat. Zatímco zápis na chápeme ve smyslu úmluvy o opakovaném sčítání na straně 58 a na straně 103, kde $n \in \mathbb{N}$ a $a \in R$, tak zápis $n \cdot a$ chápeme jako operaci prvků $n, a \in R$. Je nutno být opatrný při vynechávání symbolu „·“, aby nedošlo k mýlce, který případ zápis představuje.

Písmenko „R“ používané v označení okruhu pochází z německého slova „der Ring“. Poprvé tento termín použil německý matematik David Hilbert.

Příklad 11.1. Uveďme několik klasických příkladů okruhů.

1) Množina celých čísel s operacemi obvyklého sčítání a násobní $(\mathbb{Z}, +, \cdot)$ je nejjednodušším klasickým příklad okruhu. Pojem okruhu byl zaveden, aby zobecnil právě počítání s celými čísly.
2) Množina reálných čísel s operacemi obvyklého sčítání a násobní $(\mathbb{R}, +, \cdot)$ je okruh.
3) Množina zbytkových tříd s operacemi sčítání a násobní $(\mathbb{Z}_n, +, \cdot)$ je okruh.
4) Označme $R = \{0, 1\}$. Trojice $(R, +, \cdot)$, kde operace jsou určeny Tabulkami 11.1., je okruh (Cvičení 11.1.1.).

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Tabulka 11.1.: *Operace v binárním okruhu* $(\{0, 1\}, +, \cdot)$.

5) *Triviální okruh* je $(R, +, \cdot)$, kde $R = \{0\}$.

Příklad 11.2. Množina přirozených čísel s operacemi obvyklého sčítání a násobní $(\mathbb{N}, +, \cdot)$ okruhem není. Vzhledem k operaci „+“ neexistuje v $\mathbb{N}$ neutrální prvek, navíc k žádnému přirozenému číslu neexistuje v $\mathbb{N}$ opačné číslo. ✓

Příklad 11.3. Množina $U(n)$ přirozených čísel nesoudělných s n s operacemi obvyklého sčítání a násobní modulo n okruh není.
Operace „+“ nemusí být uzavřená na $U(n)$. Stačí si uvědomit, že číslo 1 vždy patří do $U(n)$ a každé číslo k menší než n můžeme napsat ve tvaru $1 + 1 + \cdots + 1$, avšak k do $U(n)$ patřit nemusí. Navíc součet $n \equiv 0 \pmod{n}$ by z uzavřenosti operace sčítání měl do $U(n)$ patřit, avšak z definice množiny $U(n)$ číslo 0 do $U(n)$ nepatří. ✓

Příklad 11.4. Označme $R = \{a, b, c\}$. Trojice $(R, +, \cdot)$, kde operace jsou určeny Tabulkami 11.2., je okruh. Důkaz je ponechán jako Cvičení 11.1.2.

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\cdot$	a	b	c
a	a	a	a
b	a	b	c
c	a	c	b

Tabulka 11.2.: *Operace v okruhu* $(\{a, b, c\}, +, \cdot)$.

Příklad 11.5. Označme $R = \{a, b, c\}$. Trojice $(R, +, \cdot)$, kde operace jsou určeny Tabulkami 11.3. není okruh, neboť operace „·“ není distributivní vzhledem k „+“. Obě operace jsou evidentně komutativní a existuje příslušný neutrální prvek, avšak například $2 \cdot (1 + 2) = 2 \cdot 0 = 1 \neq 2 = 2 + 0 = 2 \cdot 1 + 2 + 2$.

$+$	a	b	c
a	a	b	c
b	b	c	a
c	c	a	b

$\cdot$	a	b	c
a	c	a	b
b	a	b	c
c	b	c	a

Tabulka 11.3.: *Operace v okruhu* $(\{a, b, c\}, +, \cdot)$.

Pro zajímavost zmiňme, že množina *ordinálních čísel* s operacemi sčítání a násobní ordinálních čísel okruhem není, neboť pro ordinální čísla platí pouze levý, nikoliv pravý distributivní zákon. Další příklad najdete ve Cvičení 11.1.11.

Nula a jednička okruhu

Nyní popíšeme některé významné prvky okruhů.

Definice Řekneme, že okruh $(R,+,\cdot)$ je *komutativní* právě tehdy, když je komutativní operace „$\cdot$“, tj. pokud pro každé $a,b\in R$ platí $a\cdot b=b\cdot a$.

Neutrální prvek grupy $(R,+)$ se nazývá *nula okruhu* a značíme jej 0. Pokud existuje neutrální prvek pologrupy $(R,\cdot)$, nazývá se *jednička okruhu* a značí se 1. Dále řekneme, že nenulový prvek $a\in R$ je *jednotkou okruhu* právě tehdy, když k němu existuje inverzní prvek a^{-1} v monoidu $(R\setminus\{0\},\cdot)$.

Připomeňme, že definice je v souladu s úmluvou o aditivní a multiplikativní notaci, kterou jsme zavedli na straně 50. Protože pracujeme se dvěma operacemi, tak budeme pečlivě rozlišovat *nulu*, což je neutrální prvek vzhledem k operaci „$+$“, a *jedničku* což je neutrální prvek vzhledem k operaci „$\cdot$“. Podobně inverzí prvku a vzhledem k operaci „$+$“ bude *opačný* prvek $-a$, zatímco inverzí téhož prvku a vzhledem k operaci „$\cdot$“ bude *inverzní* prvek a^{-1}.

Podobně jako jsme ve Větě 2.2. ukázali, že existuje jediný neutrální prvek monoidu (Věta 2.2.), tak je možno ukázat, že jednička okruhu existuje nejvýše jedna (Cvičení 11.2.2.). Naproti tomu jednotek v okruhu může být více. Například v $(\mathbb{R},+,\cdot)$ jsou jednotkami všechna nenulová čísla. Obecně v každém okruhu jednička je jednotkou, opačná implikace však neplatí (Cvičení 11.1.5.).

Příklad 11.6. Uveďme několik klasických příkladů okruhů včetně určení nuly, jedničky a všech jednotek.

1) $(\mathbb{Z},+,\cdot)$ je komutativní okruh s nulou 0, jedničkou 1 a jednotkami 1 a -1.
2) $(\mathbb{S},+,\cdot)=(2\mathbb{Z},+,\cdot)$ je komutativní okruh s nulou 0, který nemá jedničku ani jednotky.
3) $(\mathbb{R},+,\cdot)$ je komutativní okruh s nulou 0, jedničkou 1. Jednotkami jsou všechna čísla v $\mathbb{R}\setminus\{0\}$.
4) $(\mathbb{Z}_n,+,\cdot)$ je komutativní okruh s nulou $\overline{0}$ (třídou čísel kongruentních s číslem 0) a s jedničkou $\overline{1}$ (třídou čísel kongruentních s číslem 1). Množina jednotek je $U(n)$, což je množina všech čísel nesoudělných s n.
5) Množina polynomů s celočíselnými koeficienty a operacemi obvyklého sčítání a násobení polynomů $(\mathbb{Z}[x],+,\cdot)$ je komutativní okruh s nulou $o(x)=0$ a s jedničkou $p(x)=1$. Jednotkami jsou konstantní polynomy $p_1(x)=1$ a $p_2(x)=-1$.
6) Čtvercové matice řádu 2 s celočíselnými prvky $(M_{2,2}(\mathbb{Z}),+,\cdot)$ tvoří nekomutativní okruh. Nulou je nulová matice $\begin{pmatrix}0&0\\0&0\end{pmatrix}$ a jedničkou je jednotková matice $\begin{pmatrix}1&0\\0&1\end{pmatrix}$. Nalezení jednotek je ponecháno jako Cvičení 11.1.7.
7) Čtvercové matice řádu 2 se sudými celočíselnými prvky $(M_{2,2}(2\mathbb{Z}),+,\cdot)$ tvoří nekomutativní okruh, který nemá jedničku. Nulou je nulová matice řádu 2 a jednotky tento okruh nemá.
8) $(\mathbb{Q},+,\cdot)$ je komutativní okruh s nulou 0 a s jedničkou 1. Jednotky jsou všechna nenulová racionální čísla, neboť pro každé $a\in\mathbb{Q}\setminus\{0\}$ platí $a^{-1}\in\mathbb{Q}$.
9) *Nulový okruh* $(R,+,\cdot)$ sestavíme tak, že pro každé $a,b\in R$ položíme $a\cdot b=0$, kde prvek 0 je nulou grupy $(R,+)$. Jedničku nulový okruh nemá a proto nemá ani jednotky.
10) V triviálním okruhu je jeho jediný prvek a nulou i jedničkou. Prvek a není jednotkou, protože podle definice jednotky jsou nenulové prvky.

Otázky:

- Existuje okruh, který obsahuje jednotky, ale nemá jedničku?
- Existuje okruh, ve kterém nula i jednička jsou totožné prvky?
- Existuje okruh, ve kterém jsou právě tři jednotky?

Příklad 11.7. Uveďme několik dalších příkladů, které okruhem nejsou.

1) Trojice $(\mathbb{Q}^+,+,\cdot)$, okruh netvoří, protože vzhledem k operaci „$+$“ neexistuje v $\mathbb{Q}^+$ neutrální prvek, navíc k žádnému přirozenému číslu neexistuje v $\mathbb{Q}$ opačné číslo.
2) Mějme množinu logických hodnot $\{0,1\}$ a obvyklé logické operace konjunkce „$\wedge$“ a disjunkce „$\vee$“. Ani jedna trojice $(\{0,1\},\wedge,\vee)$, $(\{0,1\},\vee,\wedge)$ netvoří okruh (Cvičení 11.1.4.).

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	b	b
b	a	a

Tabulka 11.4.: *Dvojice operací na množině* $(\{a,b\},+,\cdot)$.

3) Označme $R=\{a,b\}$. Trojice $(R,+,\cdot)$, kde operace jsou určeny Tabulkou 11.4., okruhem není, neboť operace „$\cdot$“ není asociativní. Například $(a\cdot b)\cdot a=b\cdot a=a\neq b=a\cdot a=a\cdot(b\cdot a)$. Pro operaci „$\cdot$“ navíc neplatí ani distributivní vztahy, například $a\cdot(a+b)=a\cdot b=b\neq a=b+b=a\cdot a+a\cdot b$.
4) Označme $R=\{a,b\}$. Trojice $(R,+,\cdot)$, kde operace jsou určeny Tabulkou 11.5., okruhem není, neboť neplatí distributivní vztahy vzhledem k operaci „$+$“, například $a\cdot(a+b)=a\cdot b=a\neq b=b+a=$ $=a\cdot a+a\cdot b$. Přitom evidentně $(R,+)$ je grupa a $(R,\cdot)$ je pologrupa.

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	b	a
b	a	b

Tabulka 11.5.: *Dvojice operací na množině* $(\{a,b\},+,\cdot)$.

5) Označme $R=\{a,b\}$. Trojice $(R,+,\cdot)$, kde operace jsou určeny Tabulkou 11.6., okruhem není, neboť neplatí distributivní vztahy vzhledem k operaci „$+$“, například $b\cdot(a+a)=b\cdot a=b\neq a=b+b=$ $=b\cdot a+b\cdot a$. Přitom evidentně $(R,+)$ i $(R,\cdot)$ jsou grupy.

$+$	a	b
a	a	b
b	b	a

$\cdot$	a	b
a	a	b
b	b	a

Tabulka 11.6.: *Dvojice operací na množině* $(\{a,b\},+,\cdot)$.

Okruhy přirozeným způsobem zobecňují počítání s celými čísly. Celá čísla umíme sčítat i odčítat (přičítat inverzní prvek vzhledem k operace „$+$“. Celá čísla umíme násobit, ale nemáme operaci dělení celých čísel, neboť výsledek nemusí být celé číslo. Stejné vlastnosti má každý okruh. Prvku okruhu můžeme sčítat i „odčítat“, budeme-li přičítat opačné prvky. Prvku okruhu můžeme násobit, avšak inverzní prvky v okruhu nemusí existovat, dokonce v okruhu nemusí existovat ani neutrální prvek vzhledem k operaci „$\cdot$“.

Cvičení

11.1.1.$^{\heartsuit}$ *Ukažte, že trojice* $(R,+,\cdot)$*, kde operace jsou určeny Tabulkou 11.1., je okruh.*

11.1.2. Ukažte, že trojice $(R,+,\cdot)$*, kde operace jsou určeny Tabulkou 11.2., je okruh.*

11.1.3.$^{\heartsuit}$ *Mějme okruh, ve kterém pro každý nenulový prvek* a *a každou dvojici prvků* b,c *platí následující implikace: pokud* $ab=ca$*, potom* $b=c$*. Ukažte, že takový okruh je komutativní.*

11.1.4. Mějme množinu logických hodnot $\{0,1\}$ *a obvyklé logické operace konjunkce „*$\wedge$*“ a disjunkce „*$\vee$*“. Ukažte, že ani jedna trojice* $(\{0,1\},\wedge,\vee)$*,* $(\{0,1\},\vee,\wedge)$ *netvoří okruh (Cvičení 11.1.4.).*

11.1.5.$^{\heartsuit}$ *Ukažte, že v okruhu* $(R,+,\cdot)$ *je jednička jednotkou, avšak opačná implikace neplatí.*

11.1.6. Mějme okruhy $(R_1,+_1,\cdot_1)$*,* $(R_2,+_2,\cdot_2)$*, …,* $(R_n,+_n,\cdot_n)$*. Ukažte, že množina* $R_1\oplus R_2\oplus\ldots\oplus R_n=$ $=\{(a_1,a_2,\ldots,a_n):a_i\in R_i\}$ *s operacemi „*$+$*“ a „*$\cdot$*“ definovanými po složkách, tvoří okruh. Říkáme mu* přímý součet okruhů.

11.1.7. Najděte a popište všechny jednoty okruhu $(M_{2,2}(\mathbb{Z}),+,\cdot)$.

11.1.8. Mějme libovolnou grupu $(G,\oplus)$ *s neutrálním prvkem* e*. Na množině* G *definujeme operaci „*$\odot$*“ předpisem* $\forall a,b\in G:a\odot b=e$*. Ukažte nebo vyvraťte, že* $(G,\oplus,\odot)$ *je okruh.*

11.1.9. Mějme netriviální grupu $(G,\cdot)$*. Ukažte, že trojice* $(G,\cdot,\cdot)$ *(obě operace jsou stejné) není okruh.*

11.1.10. Najděte příklad struktury se dvěma operacemi $(R,+,\cdot)$*, které nejsou okruhem, protože poruší (pokud možno) vždy právě jednu z šesti vlastností v definici okruhu.*

11.1.11. Mějme množinu $F_{\mathbb{R}}$ všech spojitých reálných funkcí $\mathbb{R} \to \mathbb{R}$. Mějme operaci sčítání funkcí „$+$“ a operaci skládání funkcí „$\circ$“. Dokažte nebo vyvraťte, že trojice $(F_{\mathbb{R}}, +, \circ)$ tvoří okruh.

11.2. Vlastnosti okruhů

Nejprve zavedeme obvyklou úmluvu: druhou operaci okruhu budeme místo $a \cdot b$ psát jen ab a místo $a + (-b)$ budeme psát stručněji $a - b$. Pokud by z kontextu nebylo jasné, zda zápisem ab rozumíme součin dvou prvků a a b daného okruhu, nebo zda se jedná o součet a kopií prvku b, tak operaci součinu zapíšeme jako $a \cdot b$.

Věta 11.1. Vlastnosti okruhu
Mějme okruh $(R, +, \cdot)$. Pro každé $a, b, c \in R$ platí následující rovnosti.

(i) $a0 = 0a = 0$
(ii) $a(-b) = (-a)b = -(ab)$
(iii) $(-a)(-b) = ab$
(iv) $a(b-c) = ab - ac$ *a* $(b-c)a = ba - ca$
Jestliže navíc $(R, +, \cdot)$ má jedničku 1, tak platí následující rovnosti.
(v) $(-1)a = -a$
(vi) $(-1)(-1) = 1$

Důkaz.
(i) S využitím levé distributivity operace „$\cdot$“ vzhledem k operaci „$+$“ dostaneme

$$a0 = a(0+0) = a0 + a0,$$

odkud krácením (odečtením opačného prvku k $a0$ podle Věty 2.6.) v grupě $(R, +)$ dostáváme $0 = a0$. Podobně $0a = (0+0)a = 0a + 0a$, odkud krácením (odečtením opačného prvku) dostáváme $0 = 0a$.
(ii) Pro důkaz další rovnosti využijeme neutrální prvek 0, distributivitu operace „$+$“ a předchozí bod (i).

$$a(-b) + ab = a(-b+b) = a0 = 0$$

Odečtením ab od obou stran rovnosti dostaneme $a(-b) = 0 - (ab) = -(ab)$. Analogicky $(-a)b + ab = (-a + a)b = 0b = 0$ a opět odečtením ab dostaneme $(-a)b = 0 - (ab) = -(ab)$.
(iii) Použijeme-li dvakrát předchozí bod (ii), tak dostaneme

$$(-a)(-b) = -(a(-b)) = -(-(ab)) = ab,$$

neboť opačným prvek k opačnému prvku $-(ab)$ je podle Lemmatu 2.5. prvek ab.
(iv) Opět s využitím bodu (ii) dostaneme

$$a(b-c) = ab + a(-c) = ab + -(ac) = ab - ac.$$

Analogicky $(b-c)a = ba + (-c)a = ba + -(ca) = ba - ca$.
(v) Jestliže zvolíme $a = -1$, tak dle bodu (ii) dostaneme $(-1)b = -(1b) = -b$.
(vi) Jestliže navíc zvolíme $b = -1$, tak dle bodu (ii) dostaneme $(-1)(-1) = -(1(-1)) = -(-1) = 1$. □

Zatímco grupa zobecňuje klasické sčítání celých čísel, tak okruh byl zaveden jako zobecnění sčítání a násobení celých čísel. Připomínáme, že pro libovolný prvek a daného okruhu existuje opačný prvek $-a$ vzhledem k operaci „$+$“, avšak inverzní prvek a^{-1} vzhledem k operaci „$\cdot$“ existovat nemusí.

Poznámka 11.2. Časté chyby chápání okruhu
Mějme dán okruh $(R, +, \cdot)$. Je dobré zdůraznit, že zatímco $(R, +)$ tvoří grupu, tak $(R, \cdot)$ grupu *téměř nikdy* netvoří (Cvičení 11.2.1.).

To mimo jiné znamená, že v okruhu obecně nemůžeme krátit: jestliže platí $ab = ac$, tak *nemusí* platit $b = c$. Například v okruhu $(\mathbb{Z}_{12}, +, \cdot)$ platí $\overline{3} \cdot \overline{5} = \overline{3} = \overline{3} \cdot \overline{1}$, ale $\overline{5} \neq \overline{1}$.

Dále v okruhu obecně *nemusí* existovat jednička (neutrální prvek vzhledem k operaci „$\cdot$“). Jestliže například $a^2 = a$, tak nemusí platit $a = 0$ ani $a = 1$. Například v okruhu $(\mathbb{Z}_{10}, +, \cdot)$ platí $\overline{5} = \overline{5}^2$, avšak $\overline{5}$ není ani neutrálním prvkem (nulou) grupy $(\mathbb{Z}_{10}, +)$, ani neutrálním prvkem (jedničkou) pologrupy $(\mathbb{Z}_{10}, \cdot)$.

Okruhům, které mají jedničku vzhledem k operaci „$\cdot$“, se budeme věnovat v Kapitole 11.4. Ukážeme, že ačkoliv druhá operace obecně netvoří grupu, má smysl v některých okruzích krátit (za splnění dalších podmínek).

Cvičení

11.2.1. Najděte (až na izomorfismus) všechny takové okruhy $(R,+,\cdot)$, pro které platí, že $(R,+)$ i $(R,\cdot)$ jsou grupy.

11.2.2.$^{\heartsuit}$ Ukažte, že v okruhu $(R,+,\cdot)$ je nejvýše jedna jednička.

11.2.3. Ukažte, že v netriviálním okruhu $(R,+,\cdot)$ neexistuje k neutrálnímu prvku 0 grupy $(R,+)$ inverzní prvek.

11.2.4. Ukažte, že v netriviálním okruhu nemusí *k danému nenulovému prvku existovat prvek inverzní.*

11.3. Podokruhy

Podobně jako byl v Kapitole 3. zaveden pojem podgrupy dané grupy, má smysl zavést následující podstruktury okruhů.

Definice Mějme okruh $(R,+,\cdot)$ a neprázdnou podmnožinu $S \subseteq R$. Jestliže $(S,+,\cdot)$ je okruh, nazveme jej *podokruh* okruhu $(R,+,\cdot)$.

Podokruh je struktura, která přejímá obě operace okruhu pro všechny své prvky. Operace v okruhu $(S,+,\cdot)$ jsou *restrikcemi* operací okruhu $(R,+,\cdot)$.

Příklad 11.8. Uveďme několik klasických příkladů okruhů a jejich podokruhů.

1) Okruh $(\mathbb{Z},+,\cdot)$ je komutativní podokruh komutativního okruhu $(\mathbb{Q},+,\cdot)$. Okruh $(\mathbb{Q},+,\cdot)$ je komutativní podokruh komutativního okruhu $(\mathbb{R},+,\cdot)$ a okruh $(\mathbb{R},+,\cdot)$ je komutativní podokruh komutativního okruhu $(\mathbb{C},+,\cdot)$.
2) Okruh $(\mathbb{S},+,\cdot)$ je komutativní podokruh komutativního okruhu $(\mathbb{Z},+,\cdot)$.
3) Množina $\{\overline{0},\overline{2},\overline{4}\}$ s příslušnými restrikcemi operací sčítání a násobení modulo 6 je komutativním podokruhem komutativního okruhu $(\mathbb{Z}_6,+,\cdot)$. Nulou okruhu i podokruhu je prvek $\overline{0}$. Je zajímavé si uvědomit, že jedničkou okruhu $(\mathbb{Z}_6,+,\cdot)$ je prvek $\overline{1}$, zatímco jedničkou podokruhu $(\{\overline{0},\overline{2},\overline{4}\},+,\cdot)$ je prvek $\overline{4}$.
4) Množina n násobků celých čísel s operacmi běžného sčítání a násobení $(n\mathbb{Z},+,\cdot)$, kde $n\mathbb{Z} = \{na : a \in \mathbb{Z}\}$, je podokruhem okruhu celých čísel.
5) Množina diagonálních matic (všechny mimodiagonální prvky jsou nulové) s celočíselnými prvky je *komutativním* podokruhem nekomutativního okruhu $(M_{2,2}(\mathbb{Z}),+,\cdot)$.

Má smysl upozornit na příklady podmnožin okruhů, které podokruhem nejsou.

Příklad 11.9. Uveďme několik příkladů okruhů a jejich podmnožin, které podokruh netvoří.

1) $(\mathbb{L},+,\cdot)$ není podokruh komutativního okruhu $(\mathbb{Z},+,\cdot)$, neboť $(\mathbb{L},+)$ není grupa; nemá neutrální prvek a operace $+$ není na $\mathbb{L}$ uzavřená.
2) Množina $\{\overline{0},\overline{1},\overline{2}\}$ s příslušnými restrikcemi operací sčítání a násobení modulo 6 není podokruhem komutativního okruhu $(\mathbb{Z}_6,+,\cdot)$, neboť operace nejsou uzavřené na množině $\{\overline{0},\overline{1},\overline{2}\}$.
3) Okruh $(\mathbb{Z}_n,+,\cdot)$ není podokruhem komutativního okruhu $(\mathbb{Z},+,\cdot)$, neboť se jedná o různé množiny a $\mathbb{Z}_n \not\subseteq \mathbb{Z}$.

Ověření podokruhu

Abychom ověřili, zda daná podmnožina S prvků okruhu $(R,+,\cdot)$ tvoří podokruh stačí podle následující věty ověřit dvě vlastnosti.

Věta 11.2. Test podokruhu
Mějme okruh $(R,+,\cdot)$ a neprázdnou podmnožinu $S \subseteq R$. Potom $(S,+,\cdot)$ je podokruhem okruhu $(R,+,\cdot)$, jestliže platí

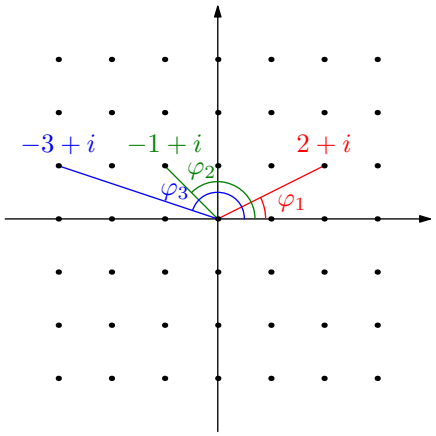
(i) $\forall a,b \in S : a-b \in S$, *($(S,+)$ je podgrupou $(R,+)$)*
(ii) $\forall a,b \in S : a \cdot b \in S$ *(uzavřenost operace „$\cdot$“).*

Důkaz. Protože S je neprázdná podmnožina R, tak podle Věty 3.4. z předpokladu (i) ihned plyne, že grupa $(S,+)$ je podgrupou grupy $(R,+)$. Operace „$\cdot$“ je podle předpokladu (ii) uzavřená na množině S, asociativita operace „$\cdot$“ se podle Cvičení 0.6.6. „zdědí“ z asociativity operace na celém R a proto $(S,\cdot)$ je pologrupa. Distributivita vzhledem k operaci „$+$“ se podle Cvičení 0.6.7. „zdědí“ z distributivity na celém R a z obou předpokladů uzavřenosti (i) a (ii). Podle Poznámky 11.1. je proto $(S,+,\cdot)$ okruhem a podle definice podokruhu je $(S,+,\cdot)$ podokruhem okruhu $(R,+,\cdot)$. □

Příklad 11.10. Ukážeme, že množina gausovských celých čísel s operacmi běžného sčítání a násobení komplexních čísel $(\mathbb{Z}[i],+,\cdot)$, kde $\mathbb{Z}[i]=\{a+bi : a,b\in\mathbb{Z}\}$, je podokruhem okruhu komplexních čísel.
Ověříme předpoklady Věty 11.2. Mějme dvě gaussovská celá čísla $a+bi, c+di \in \mathbb{Z}[i]$. Jejich rozdíl je $(a+bi)-(c+di)=(a-c)+(b-d)i$, a protože $a-c$, $b-d$ jsou celá čísla, tak jistě rozdíl $(a+bi)-(c+di)$ je také gaussovské celé číslo.

Dále ukážeme, že operace násobení gaussovských celých čísel je uzavřená na $\mathbb{Z}[i]$. Součin $(a+bi)\cdot(c+di)=(ac-bd)+(ad+bc)i$. Oba koeficienty $ac-bd$, $ad+bc$ jsou jistě celá čísla, a proto je operace „$\cdot$“ uzavřená na $\mathbb{Z}[i]$. ✓

Připomeňme, že v goniometrickém tvaru odpovídá součin dvou (nebo více) komplexních čísel komplexnímu číslu, jehož velikost je součinem velikostí činitelů a jehož argument je součtem argumentů činitelů. Všimněte si, že operace násobení gaussovských celých čísel je uzavřená v komplexní rovině na množině bodů s celočíselnými složkami. Na Obrázku 11.2. vidíme znázornění součinu $(2+i)\cdot(-1+i)=-3+i$. Zajímavé je rozmyslet si součin stejných komplexních čísel v goniometrickém tvaru. Platí $2+i=\sqrt{5}\left(\frac{2}{\sqrt{5}}+i\frac{1}{\sqrt{5}}\right)$, proto $\varphi_1=\arccos\frac{2}{\sqrt{5}}$. Dále $-1+i=\sqrt{2}\left(\frac{\sqrt{2}}{2}+i\frac{-\sqrt{2}}{2}\right)=\sqrt{2}\left(\cos\frac{3\pi}{4}+i\sin\frac{3\pi}{4}\right)$, kde $\varphi_2=\frac{3\pi}{4}$. A konečně $-3+i=\sqrt{10}\left(-\frac{3}{\sqrt{10}}+i\frac{1}{\sqrt{10}}\right)$, proto $\varphi_3=\arccos\left(-\frac{3}{\sqrt{10}}\right)$. Vskutku platí $\varphi_1+\varphi_2=\arccos\left(\frac{2}{\sqrt{5}}\right)+\frac{3\pi}{4}=$ $=\arccos\left(-\frac{3}{\sqrt{10}}\right)=\varphi_3$ (Cvičení 11.3.6.).



Obrázek 11.2.: *Násobení gaussovských celých čísel.*

Průnik podokruhů

Už víme, že průnik dvou podgrup je vždy také podgrupou (Věta 3.2.). Následující příklad ukáže, že průnik dvou podokruhů tak může být podokruhem.

Příklad 11.11. Mějme okruhy $(2\mathbb{Z},+,\cdot)$ a $(3\mathbb{Z},+,\cdot)$. a) Tvoří $(2\mathbb{Z}\cap 3\mathbb{Z},+,\cdot)$ podokruh $(\mathbb{Z},+,\cdot)$? b) Tvoří $(2\mathbb{Z}\cap 3\mathbb{Z},+,\cdot)$ podokruh $(2\mathbb{Z},+,\cdot)$? c) Pokud ano, jak vypadá podokruh $(2\mathbb{Z}\cap 3\mathbb{Z},+,\cdot)$?
a) Ukážeme, že $(2\mathbb{Z}\cap 3\mathbb{Z},+,\cdot)$ je podokruhem okruhu $(\mathbb{Z},+,\cdot)$. Mějme libovolné dva prvky $a,b\in 2\mathbb{Z}\cap 3\mathbb{Z}$. Protože oba prvky $a-b$, $a\cdot b$ patří jak do $2\mathbb{Z}$ (protože trojice $(2\mathbb{Z},+,\cdot)$ je okruh), tak do $3\mathbb{Z}$ (protože trojice $(3\mathbb{Z},+,\cdot)$ je okruh), tak oba prvky patří i do $(2\mathbb{Z}\cap 3\mathbb{Z},+,\cdot)$. Podle Věty 11.2. je $(2\mathbb{Z}\cap 3\mathbb{Z},+,\cdot)$ podokruhem okruhu $(\mathbb{Z},+,\cdot)$.
b) Stejně jako v předchozím bodu si uvědomíme, že a, b, $a-b$, $a\cdot b$ patří jak do $\mathbb{Z}$, tak dokonce i do $\mathbb{Z}$. Podle Věty 11.2. je $(2\mathbb{Z}\cap 3\mathbb{Z},+,\cdot)$ také podokruhem okruhu $(2\mathbb{Z},+,\cdot)$.
c) Okruh $(2\mathbb{Z},+,\cdot)$ obsahuje všechna sudá celá čísla a okruh $(3\mathbb{Z},+,\cdot)$ obsahuje všechny násobky 3. Jejich průnik proto obsahuje právě násobky čísla 6 a jedná se proto o okruh $(6\mathbb{Z},+,\cdot)$. ✓

Uvedený příklad je možno zobecnit: průnik podokruhů je vždy také podokruhem.

Věta 11.3. *Mějme okruh $(R,+,\cdot)$ a dva jeho podokruhy $(R_1,+,\cdot)$ a $(R_2,+,\cdot)$. Potom $(R_1\cap R_2,+,\cdot)$ je také podokruhem okruhu $(R,+,\cdot)$.*

Důkaz. Dokážeme přímo s využitím Věty 11.2. Mějme podokruhy $(R_1,+,\cdot)$ a $(R_2,+,\cdot)$ jsou okruhy v $(R,+,\cdot)$. Mějme libovolné dva prvky $a,b\in R_1\cap R_2$. Protože $(R_1,+,\cdot)$ je okruh, tak $a-b\in R_1$, a protože $(R_2,+,\cdot)$ je okruh, tak také $a-b\in R_2$. To ale znamená, že $a-b\in R_1\cap R_2$. Dále, protože $(R_1,+,\cdot)$ je okruh, tak $a\cdot b\in R_1$, a protože $(R_2,+,\cdot)$ je okruh, tak také $a\cdot b\in R_2$. To ale znamená, že $a\cdot b\in R_1\cap R_2$. Podle Věty 11.2. je $(R,+,\cdot)$ podokruhem v okruhu $(R,+,\cdot)$. □

Přirozeně se nabízí otázka: může být sjednocení podokruhů také podokruhem? Následující příklad ukazuje, že sjednocení podokruhů nemusí tvořit podokruh.

Příklad 11.12. Mějme okruhy $(2\mathbb{Z},+,\cdot)$ a $(3\mathbb{Z},+,\cdot)$. Zodpovíme otázky. a) Tvoří $(2\mathbb{Z}\cup3\mathbb{Z},+,\cdot)$ podokruh $(\mathbb{Z},+,\cdot)$? b) Tvoří $(2\mathbb{Z}\cup3\mathbb{Z},+,\cdot)$ podokruh $(2\mathbb{Z},+,\cdot)$?
Ukážeme, že sjednocení okruhů $(2\mathbb{Z},+,\cdot)$ a $(3\mathbb{Z},+,\cdot)$ není okruhem. Operace obecně *nejsou* uzavřené na sjednocení dvou nosných množin. Platí sice $2\in2\mathbb{Z}$ a $3\in3\mathbb{Z}$, proto $2,3\in2\mathbb{Z}\cup3\mathbb{Z}$, dále dle „zděděné“ operace je $2+3=5$, avšak $5\notin2\mathbb{Z}\cup3\mathbb{Z}$, neboť 2 není asi sudé číslo, ano násobek 3. Proto $(2\mathbb{Z}\cup3\mathbb{Z},+,\cdot)$ není podokruhem ani $(2\mathbb{Z},+,\cdot)$, ani $(\mathbb{Z},+,\cdot)$. ✓

Otázka: Muže sjednocení okruhů tvořit okruh?

Cvičení

11.3.1.$^\heartsuit$ *Ukažte, že každý podokruh komutativního okruhu je komutativní.*

11.3.2. Ukažte, že sjednocení dvou podokruhů $(R_1,+,\cdot)$ a $(R_2,+,\cdot)$ okruhu $(R,+,\cdot)$ je okruhem právě tehdy, když $R_1\subseteq R_2$ nebo $R_2\subseteq R_1$.

11.3.3. Ukažte, že nula okruhu je současně nulou každého podokruhu.

11.3.4.$^\heartsuit$ *Dokažte nebo vyvraťte následující tvrzení: jednička okruhu (pokud existuje) je současně jedničkou každého podokruhu.*

11.3.5. Zdůvodněte, zda platí následující tvrzení analogické Větě 11.2.: Mějme okruh $(R,+,\cdot)$ a neprázdnou podmnožinu $S\subseteq R$. Jestliže pro každé $a,b\in S$ platí $a+b\in S$ a pro každé $a,b\in S$ platí $a\cdot b\in S$, tak $(S,+,\cdot)$ je podokruhem okruhu $(R,+,\cdot)$.

11.3.6. Odvoďte rovnost komplexních čísel znázorněnou na Obrázku 11.2. algebraicky v goniometrickém tvaru. Tj. ukažte, že platí $\arccos\left(\frac{2}{\sqrt{5}}\right)+\frac{3\pi}{4}=\arccos\left(-\frac{3}{\sqrt{10}}\right)$.

11.3.7. Mějme okruh čtvercových matic řádu 2 s celočíselnými prvky $(M_{2,2}(\mathbb{Z}),+,\cdot)$. Dokažte nebo vyvraťte, že množina $X=\left\{\begin{pmatrix}a&a\\b&b\end{pmatrix}:a,b\in\mathbb{Z}\right\}$ *tvoří podokruh daného okruhu.*

11.3.8. Ve Cvičení 2.2.8. na straně 46 jsme zavedli idempotentní prvky, pro které platí $g\cdot g=g$. Mějme idempotentní prvek g v okruhu $(R,+,\cdot)$. Ukažte, že prvek $1-g$ je také idempotentní.

11.3.9. Mějme nekomutativní okruh $(R,+,\cdot)$ a v něm dvojici prvků a, b, pro které platí $ab=1$, ale $ba\neq1$. Ukažte, že prvek $1-ba$ je idempotentní prvek okruhu $(R,+,\cdot)$ (idempotentní prvky jsme zavedli ve Cvičení 2.2.8. na straně 46).

11.4. Obor integrity

V okruhu můžeme pracovat se třemi klasickými operacemi (resp. jejich analogiemi): sčítání, odčítání a násobení. Dělit nenulovým číslem (násobit inverzní hodnotou) však v okruhu obecně není možné, neboť není zaručena existence inverzních prvků. S využitím násobení však můžeme v okruhu popsat „dělitelnost“, podobně jako pracujeme s dělitelností celých čísel.

V dalším textu se omezíme na komutativní okruhy.

Dělitelnost v okruzích

Dělitelnost jsme zavedli v Kapitole 0.1. na straně 1. Nyní pojem dělitelnosti zobecníme pro operace v obecném okruhu.

Definice Mějme prvek a okruhu $(R,+,\cdot)$. Řekneme, že *prvek a dělí prvek b z R* právě tehdy, když existuje takový prvek c v R, že $a\cdot c=b$. Píšeme $a\mid b$.

Řekneme, že prvek a je (netriviálním) *dělitelem nuly* v okruhu $(R, +, \cdot)$ právě tehdy, když existuje takový nenulový prvek b v R, že $a \cdot b = 0$.

Podle Věty 11.1. pro každý prvek a okruhu $(R, +, \cdot)$ platí $a0 = 0a = 0$. Můžeme proto říci, že každé číslo a je (triviálním) dělitelem nuly, protože pro $c = 0$ je $a \cdot c = 0$. Nás však budou v dalším textu zajímat pouze netriviální dělitelé nuly. Dělitelem nuly budeme rozumět pouze netriviální dělitele nuly a triviální dělitele nebudeme uvažovat.

Při počítání s celými, racionálními nebo reálnými čísly jsme na dělitele nuly nenarazili. Avšak například v $(\mathbb{Z}_{12}, +, \cdot)$ je $\overline{3}_{12} \cdot \overline{4}_{12} = \overline{12}_{12} = \overline{0}_{12}$. Podobně $\overline{2}_{12}$, $\overline{4}_{12}$, $\overline{6}_{12}$, $\overline{8}_{12}$, $\overline{9}_{12}$ a $\overline{10}_{12}$ jsou v $(\mathbb{Z}_{12}, +, \cdot)$ netriviální dělitelé nuly. Jedná se o čísla soudělná s 12. Naproti tomu v $(\mathbb{Z}_{11}, +, \cdot)$ žádní (netriviální) dělitelé nuly nejsou (proč?).

Příklad 11.13. Uveďme několik příkladů dělitelů nuly.

1) V nulovém okruhu je každý prvek dělitelem nuly.
2) V číselných okruzích $(\mathbb{Z}_n, +, \cdot)$, kde n je složené číslo $n = pq$, jsou čísla p i q netriviální dělitelé nuly.
3) V číselných okruzích $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ i $(\mathbb{C}, +, \cdot)$ neexistuje žádný netriviální dělitel nuly.
4) V okruhu matic řádu 2 s celočíselnými prvky $(M_{2,2}(\mathbb{Z}), +, \cdot)$ existuje nekonečně mnoho dělitelů nuly. Například $\begin{pmatrix} 0 & a \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} c & d \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ jsou dělitelé nuly pro libovolné $a, b, c, d \in \mathbb{Z}$.

Jestliže číslo a je dělitelem čísla b, neznamená to, že můžeme číslem a dělit v celém okruhu. Abychom mohli číslem a dělit, potřebujeme existenci inverzního prvku a^{-1}. Například v okruhu $(\mathbb{Z}, +, \cdot)$ je číslo 2 dělitelem čísla 6, avšak číslem 2 nemůžeme dělit žádné liché číslo. Dále, protože pro každé přirozené číslo k platí $0 \cdot k = 0$, tak číslo 0 (i každé číslo k) je dělitelem nuly, avšak nulou nemůžeme dělit ani nulu, neboť není určen „podíl“.

Otázky:

- Má triviální okruh nulu?
- Má triviální okruh jedničku?
- Má triviální okruh jednotku?
- Má triviální okruh dělitele nuly?
- Můžeme v triviálním okruhu dělit nulou?

Obory integrity

Při počítání s reálnými čísly můžeme dělit, při počítání s celými čísly můžeme alespoň krátit. Jestliže v okruhu jsou (netriviální) dělitelé nuly, tak obecně nemůžeme ani dělit, ani krátit. To je nešikovné. Podívejme se na struktury bez (netriviálních) dělitelů nuly.

Definice Netriviální komutativní okruh s jedničkou bez dělitelů nuly se nazývá *obor integrity*.

Celá čísla s operacemi obvyklého sčítání a násobení jsou typickým oborem integrity. Obory integrity byly zavedeny právě jako zobecnění počítání s celými čísly. Všimněte si, že pojem okruhu je oproti celým číslům až příliš zobecněn:

- okruh obecně není komutativní, zatímco celá čísla (a obor integrity) ano,
- okruh obecně nemusí mít jedničku, zatímco celá čísla (a obor integrity) ano,
- v okruhu obecně mohou být dělitelé nuly, zatímco mezi celými čísly (a v oborech integrity) ne.

Příklad 11.14. Uveďme několik příkladů oborů integrity.

1) Celá čísla $(\mathbb{Z}, +, \cdot)$ jsou oborem integrity. Jedničkou je číslo 1.
2) Racionální čísla $(\mathbb{Q}, +, \cdot)$ jsou oborem integrity. Jedničkou je číslo 1.
3) Okruh $(\mathbb{Z}_p, +, \cdot)$, kde p je prvočíslo, je oborem integrity. Jedničkou je třída $\overline{1}$.
4) Okruh polynomů $(\mathbb{Z}[x], +, \cdot)$ s celočíselnými koeficienty je oborem integrity, jedničkou je polynom $0x + 1 = 1$.
5) Množina gausovských celých čísel $(\mathbb{Z}[i], +, \cdot)$ je oborem integrity, neboť jedničkou je číslo $1 + 0i = 1$ a součin dvou nenulových komplexních čísel je nenulový.
6) Množina $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ s operacemi obvyklého sčítání a násobení tvoří obor integrity $(\mathbb{Z}[\sqrt{2}], +, \cdot)$. Jedničkou je číslo $1 + 0i = 1$ (Cvičení 11.4.5.).

Příklad 11.15. Uveďme několik příkladů okruhů, které nejsou oborem integrity.

1) Okruh $(\mathbb{S}, +, \cdot) = (2\mathbb{Z}, +, \cdot)$ není oborem integrity, neboť nemá jedničku.
2) Okruh $(M_{2,2}(\mathbb{Z}), +, \cdot)$ není oborem integrity. Jednak není komutativním okruhem a jednak má dělitele nuly: například $\begin{pmatrix} 1 & 3 \\ 2 & 6 \end{pmatrix} \begin{pmatrix} 6 & 3 \\ -2 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ jsou dělitelé nuly.
3) Okruh $(\mathbb{Z}_6, +, \cdot)$ není oborem integrity, protože má dělitele nuly: $2 \cdot 3 = 0$. Avšak jeho podokruh $(\{0, 2, 4\}, +, \cdot)$ je oborem integrity s jedničkou 4.
4) Okruh $(\mathbb{Z}_n, +, \cdot)$, kde n je složené číslo, není oborem integrity.
5) Množina lichých celých čísel s operacemi obyčejného sčítání a násobení $(\mathbb{L}, +, \cdot)$ není oborem integrity, neboť není ani okruhem.

Otázka: Proč není okruh $(\mathbb{Z}_n, +, \cdot)$, kde n je složené číslo, oborem integrity?

Příklad 11.16. Trojice $(R, +, \cdot)$, kde operace „$+$“ a „$\cdot$“ jsou určeny Tabulkami 11.7., je okruhem (Cvičení 11.4.1.). Ukážeme, že trojice $(R, +, \cdot)$ je oborem integrity.

$+$	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

$\cdot$	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

Tabulka 11.7.: *Operace v okruhu* $(\{a, b, c, d\}, +, \cdot)$.

Protože množina R obsahuje více než 1 prvek a protože operace „$\cdot$“ je podle Tabulky 11.7. komutativní, je trojice $(R, +, \cdot)$ netriviální komutativní okruh. Jedničkou tohoto okruhu je prvek b, neboť pro každé $x \in R$ platí $x \cdot b = x$. Neexistence dělitelů nuly plyne opět z Tabulky 11.7., neboť kromě (nulového) prvku a je pro každou dvojici prvků $x, y \in R \setminus \{a\}$ platí $x \cdot y \neq a$. ✓

Krácení v oboru integrity

Následující věta ukazuje, že v oborech integrity můžeme „krátit“ nenulovými čísly, podobně jako jsme zvyklí krátit celá čísla. Celá čísla můžeme sčítat, odčítat, násobit. Zkoumání dělitelnosti je prvním krokem směrem k dělení (nenulovými) čísly, tj. k hledání inverze vzhledem k (druhé) operaci „$\cdot$“. Je to právě neexistence dělitelů nuly, která možnost krácení nenulovými(!) prvky zajistí.

Věta 11.4. O krácení v oborech integrity

Mějme obor integrity $(R, +, \cdot)$ a mějme prvky $a, b, c \in R$. Jestliže $a \neq 0$ (a není nula oboru integrity) a $ab = ac$, potom $b = c$.

Důkaz. Jestliže $ab = ac$, tak přičtení $-ac$ oběma stranám rovnice a s využitím distributivity vzhledem k operaci „$+$“ dostaneme $0 = ab - ac = a(b - c)$. Protože ale $a \neq 0$ a v oboru integrity neexistují dělitelé nuly, musí platit $b - c = 0$, tedy $b = c$. □

Analogická implikace $ba = ca \Rightarrow b = c$ plyne z komutativity oboru integrity a nemusíme ji dokazovat.

Poznámka 11.3. Uvědomte si, že na rozdíl od grup jsme pro důkaz možnosti krácení v okruhu nepotřebovali existenci inverzních prvků vzhledem k operaci „$\cdot$“. Stačilo využít existence opačných prvků a distributivitu operace „$\cdot$“ vzhledem k operaci „$+$“. Všimněte si, jak byla využita neexistence dělitelů nuly.

Cvičení

11.4.1. Ukažte, že trojice $(R, +, \cdot)$, kde operace „$+$“ a „$\cdot$“ jsou určeny Tabulkami 11.7., je okruhem.

11.4.2. Ukažte, že pokud pro každé dva nenulové prvky okruhu $(R, +, \cdot)$ má alespoň jeden z nich inverzi, tak v okruhu nejsou netriviální dělitelé nuly.

11.4.3.$^{\heartsuit}$ Ukažte, že jednotka okruhu je dělitelem každého prvku okruhu.

11.4.4. Ukažte, že $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ s operacemi obvyklého sčítání a násobení tvoří obor integrity.

11.4.5. Ukažte, že $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$ s operacemi obvyklého sčítání a násobení tvoří obor integrity.

11.4.6. Najděte příklad oboru integrity, jehož nějaký podokruh není oborem integrity. Jestliže takový podokruh neexistuje, dokažte to.

11.4.7. Najděte příklady okruhů, které poruší vždy právě jednu ze čtyř vlastností požadovaných v definici oboru integrity. (Ukažte, že formulace definice oboru integrity není zbytečně přísná).

11.4.8. Najděte příklad okruhu $(R, +, \cdot)$ a takových jeho prvků $a, b \in R$, pro které platí $a \cdot b = 0$, ale $b \cdot a \neq 0$.

11.4.9. Mějme okruhy $(\mathbb{Z}_n, +, \cdot)$ pro $n = 6, 10, 12$. a) Ukažte, že existuje takové přirozené číslo $n > 1$, že $z^n = z$ pro každé $z \in \mathbb{Z}_6$. b) Ukažte, že takové přirozené číslo n existuje i v okruhu $(Z_{10}, +, \cdot)$. c) Ukažte, že v okruhu $(Z_{12}, +, \cdot)$ takové přirozené číslo n neexistuje.

11.4.10. Ukažte, že v okruhu $(Z_n, +, \cdot)$, kde n je dělitelné druhou mocninou některého prvočísla, neexistuje takové přirozené číslo n, že $z^n = z$ pro každé $z \in \mathbb{Z}_n$.*

11.5. Tělesa

Je dobré si uvědomit, že možnost krácení však neznamená automaticky existenci inverzních prvků vzhledem k operaci „$\cdot$“. Například v oboru integrity celých čísel $(\mathbb{Z}, +, \cdot)$ můžeme krátit, avšak inverze k nenulovým prvkům kromě jednotek 1 a -1 neexistují. Dělení nenulovým číslem je možné pouze v případě, že k danému prvku existuje existuje inverze.

Definice Těleso
Netriviální komutativní okruh $(R, +, \cdot)$ s jedničkou se nazývá *těleso* právě tehdy, když ke každému nenulovému prvku existuje inverze.

Alternativně bychom těleso mohli nadefinovat jako takový obor integrity, pro který $(R \setminus \{0\}, \cdot)$ je (komutativní) grupa.

Otázky:

- Kolik jednotek obsahuje těleso řádu n?
- Může nula a jednička tělesa splývat?
- Může nula a jednička okruhu splývat?

Příklad 11.17. Uveďme několik příkladů těles.

1) Klasické číselné obory $(\mathbb{Q}, +, \cdot)$ a $(\mathbb{R}, +, \cdot)$ jsou tělesa. Jedničkou je číslo 1.
2) $(\mathbb{Z}_p, +, \cdot)$, kde p je prvočíslo, je tělesem. Jedničkou je třída $\overline{1}$. Důkaz tohoto tvrzení je ponechán jako Cvičení 11.5.1.
3) $(\mathbb{Z}_3[i], +, \cdot)$ je tělesem s devíti prvky. Jedničkou je prvek $1 + 0i$. Zdůvodnění je ponecháno jako Cvičení 11.5.3.
4) $(\mathbb{Q}(\sqrt{2}), +, \cdot)$, kde $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$ a operace jsou obvyklé sčítání a násobení komplexních čísel, je tělesem. Jedničkou je prvek $1 + 0\sqrt{2}$. Zdůvodnění je ponecháno jako Cvičení 11.5.4.

Příklad 11.18. Uveďme několik okruhů, které tělesem nejsou.

1) Obor integrity $(\mathbb{Z}, +, \cdot)$ není tělesem, například k číslu 2 neexistuje prvek inverzní.
2) Okruh $(\mathbb{S}, +, \cdot)$ není tělesem, neboť nemá jedničku.
3) Okruh $(\mathbb{Z}_6, +, \cdot)$ není tělesem, protože například k prvku 2 neexistuje inverzní prvek vzhledem k násobení (Cayleyho tabulka 0.6.).
4) Okruh $(\mathbb{Z}_n, +, \cdot)$, kde n je složené číslo, není tělesem, protože obsahuje dělitele nuly.
5) $(\mathbb{Z}_2[i], +, \cdot)$ netvoří těleso, protože obsahují dělitele nuly (Cvičení 11.5.5.).
6) Triviální okruh není podle definice tělesem.
7) Nulový okruh není tělesem, neboť obsahuje dělitele nuly.

Některé příklady těles rozebereme podrobněji.

Příklad 11.19. Okruh zbytkových tříd modulo 5 $(\mathbb{Z}_5, +, \cdot)$ je tělesem.

Třídy rozkladu budeme označovat čísly $0, 1, 2, 3, 4$. Už víme, že $(\mathbb{Z}_5, +)$ je grupa. Zbývá ukázat, že $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ je také grupa. Z tabulky 11.8. vpravo vidíme, že operace je uzavřená na neprázdné množině, neutrálním prvkem je 1, inverzí k 1 je 1, inverzí k 2 je 3, inverzí k 3 je 2 a inverzí k 4 je 4. Asociativita operace „$\cdot$“ a distributivita vzhledem ke sčítání plyne z asociativity a distributivity násobení celých čísel. ✓

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\cdot$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Tabulka 11.8.: *Cayleyho tabulky operací „$+$“ a „$\cdot$“ v tělese $(\mathbb{Z}_5, +, \cdot)$ a násobení v grupě $(\mathbb{Z}_5 \setminus \{0\}, +)$.*

Všimněte si, že zatímco $(\mathbb{Z}_5 \setminus \{0\}, \cdot)$ z předchozího příkladu tvoří grupu, tak pokud bychom za nosnou množinu vzali Z_5, nebude $(\mathbb{Z}_5, \cdot)$ grupou, protože prvek 0 nemá inverzi. Později ukážeme, že v každém tělese neutrální prvek první operace nemá inverzi a není možno jej do nosné množiny pro druhou operaci zahrnout, aniž bychom porušili existenci inverze pro prvek 0.

Příklad 11.20. Okruh zbytkových tříd modulo 4 $(\mathbb{Z}_4, +, \cdot)$ *není* tělesem.
Podobně jako v předchozím příkladu budeme třídy rozkladu označovat čísly $0, 1, 2, 3$. Víme, že $(\mathbb{Z}_4, +)$ je grupa. Avšak $(\mathbb{Z}_4 \setminus \{0\}, \cdot)$ není grupa! Z tabulky 11.9. vpravo vidíme, že operace sice má neutrální prvek je 1, ale operace především není uzavřená na (neprázdné) podmnožině $\mathbb{Z}_4 \setminus \{0\}$ a navíc prvek 2 nemá inverzi. ✓

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

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\cdot$	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Tabulka 11.9.: *Cayleyho tabulky operací „$+$“ a „$\cdot$“ v okruhu $(\mathbb{Z}_4, +, \cdot)$ a násobení prvků z množiny $\mathbb{Z}_4 \setminus \{0\}$.*

Tělesa a obory integrity

Následující věta ukazuje, že tělesa jsou speciálním případem oborů integrity.

Věta 11.5. *Každé těleso je oborem integrity.*

Důkaz. Protože každé těleso $(R, +, \cdot)$ je podle definice netriviální, komutativní a má jedničku, tak zbývá ukázat, že v tělese neexistují dělitelé nuly. Mějme libovolné prvky $a, b, \in R$. Jestliže součin $a \cdot b = 0$ a prvek $a \neq 0$, tak musíme ukázat, že $b = 0$. Stačí rovnost roznásobit zleva prvkem inverzním k a, který v tělese existuje. S využitím Věty 11.1. dostaneme

$$\begin{aligned} a^{-1} \cdot a \cdot b &= a^{-1} \cdot 0 \\ 1 \cdot b &= 0 \\ b &= 0. \end{aligned}$$

To znamená, že (netriviální) dělitelé nuly v tělese neexistují a těleso je oborem integrity. □

Naproti tomu ne každý obor integrity je tělesem. Například celá čísla s klasickým sčítáním a násobením tvoří obor integrity, avšak inverze (převrácené hodnoty) existují jen k číslům 1 a -1. Zajímavé však je, že konečné obory integrity tělesem být musí, jak ukazuje následující věta.

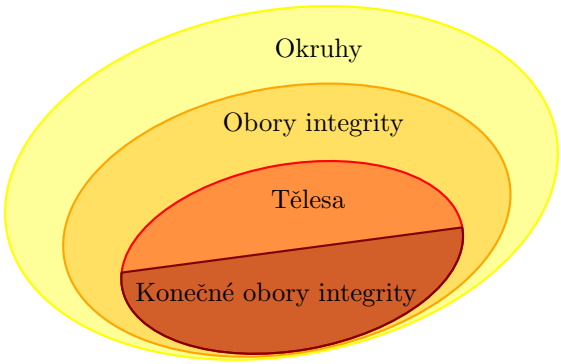
Věta 11.6. *Každý konečný obor integrity je tělesem.*

Důkaz. Ukážeme, že každý nenulový prvek a je v konečném oboru integrity jednotkou (má inverzi). Je-li $a = 1$, tak $a^{-1} = 1 = a$. V konečném oboru integrity je pro $a = a^1 \neq 1$ množina mocnin $a, a^2, \ldots, a^n$ konečná, musí platit $a^j = a^i$ pro nějaké $i > j$. Krácením dostaneme $a^{i-j} = 1$, kde $i - j \neq 0$, a proto prvek a^{i-j-1} je inverzí k a. □

Příklad 11.21. Trojice $(R, +, \cdot)$, kde operace „$+$“ a „$\cdot$“ jsou určeny Tabulkami 11.7., je podle Příkladu 11.16. oborem integrity. Protože nosná množina R je konečná, je tento obor integrity podle Věty 11.6.

současně tělesem. Ihned vidíme, že jedničkou je prvek b a najdeme inverze ke každému prvku různému od a. Platí $b^{-1} = b$, $c^{-1} = d$ a $d^{-1} = c$.

Z definic okruhu, oboru integrity i tělesa a z Vět 11.5. a 11.6. nahlédneme, jaká je hierarchie těchto struktur (Obrázek 11.3.).



Obrázek 11.3.: *Hierarchie okruhů, oborů integrity a těles.*

Ve Cvičení 11.5.1. dokážeme, že okruh zbytkových tříd modulo prvočíslo s operacemi klasického sčítání a násobení zbytkových tříd je tělesem.

Důsledek 11.7. *Je-li p prvočíslo, tak okruh zbytkových tříd $(\mathbb{Z}_p, +, \cdot)$ je tělesem.*

Poznámka 11.4. Pouze v (nevlastním) triviálním okruhu $(\{a\}, +, \cdot)$ může být současně $(\{a\}, +)$ a $(\{a\}, \cdot)$ grupou. Ve vlastích okruzích a oborech integrity $(R, +, \cdot)$ nemůže být $(R, \cdot)$ grupou. Podle Věty 11.1. víme, že pro každé $a \in R$ platí $a0 = 0a = 0 \neq 1$. Prvek 0 proto nemá v grupoidu $(R, \cdot)$ inverzi a $(R, \cdot)$ není grupa.

Cvičení

11.5.1. Ukažte, že pro každé prvočíslo p je okruh zbytkových tříd $(\mathbb{Z}_p, +, \cdot)$ tělesem.

11.5.2. Ukažte, že pro každé složené číslo p okruh zbytkových tříd $(\mathbb{Z}_n, +, \cdot)$ není tělesem.

11.5.3.$^\heartsuit$ Ukažte, že $(\mathbb{Z}_3[i], +, \cdot)$ je tělesem. Množina $(\mathbb{Z}_3[i], +, \cdot) = \{a + bi : a, b \in \mathbb{Z}_3\}$ a operace odpovídají obvyklému sčítání a násobení komplexních čísel.

11.5.4. Ukažte, že $(\mathbb{Q}(\sqrt{2}), +, \cdot)$, kde $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} : a, b \in \mathbb{Q}\}$ a operace jsou obvyklé sčítání a násobení komplexních čísel, je tělesem.

11.5.5. Ukažte, že okruh $(\mathbb{Z}_2[i], +, \cdot)$ není tělesem.

11.5.6. Mějme liché prvočíslo p. Je okruh $(\mathbb{Z}_p[i], +, \cdot)$ je tělesem?

11.5.7. Mějme složené číslo n. Je okruh $(\mathbb{Z}_n[i], +, \cdot)$ je tělesem?

11.5.8. Mějme prvočíslo p. Je okruh $(\mathbb{Z}_p[\sqrt{2}], +, \cdot)$ tělesem?

11.5.9. Dokažte nebo vyvraťte: je-li prvek a dělitelem nuly v okruhu $(R, +, \cdot)$, tak k prvku a neexistuje inverzní prvek.

11.5.10. Mějme netriviální komutativní okruh $(R, +, \cdot)$. Ukažte, že pokud pro každý nenulový prvek $a \in R$ platí $aR = R$, tak $(R, +, \cdot)$ je těleso.

Kapitola 12. Ideály a faktorové okruhy

V kapitole 5. jsme zavedli pojem normální podrgupy, tedy takové podgrupy, které vynásobené kterýmkoliv prvkem grupy zleva nebo zprava dají stejný komplex. Tato vlastnost umožnila posléze pracovat s faktorovými grupami.

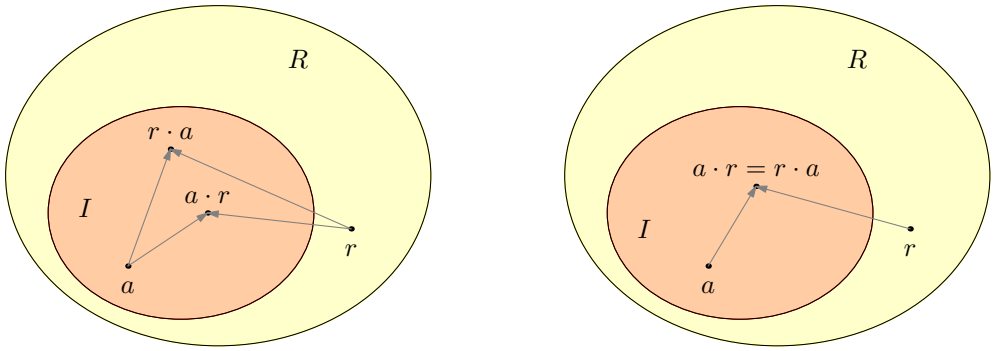
Nyní zavedeme analogický pojem pro strukturu se dvěma operacemi. Místo podgrupy, která je normální, budeme pracovat s podokruhem, který při operaci násobení „pohltí“ všechny prvky celého okruhu.

12.1. Ideál

Nyní zavedeme pojem tzv. ideálu, který v okruhu hraje podobnou roli, jakou má normální podgrupa v grupě.

Definice Ideál okruhu
Mějme okruh $(R,+,\cdot)$. Podokruh $(I,+,\cdot)$ okruhu $(R,+,\cdot)$ se nazývá (oboustranný) *ideál* okruhu $(R,+,\cdot)$ právě tehdy, když pro každé $r\in R$ a každé $a\in I$ platí $r\cdot a\in I$ a současně $a\cdot r\in I$.

Definice říká, že pro každé r z okruhu $(R,+,\cdot)$ platí $rI\subseteq I$, kde $rI=\{ra : a\in I\}$, a současně $Ir\subseteq I$, kde $Ir=\{ar : a\in I\}$. Říkáme, že ideál „pohltí“ nebo „absorbuje“ při násobení prvky celého okruhu (Obrázek 12.1.). Vlastnosti $\forall r\in R$, $\forall a\in I$ platí $r\cdot a\in I\wedge a\cdot r\in I$ se říká *absorpce*.



Obrázek 12.1.: *Ideál „pohltí“ každý prvek okruhu vzhledem k druhé operaci. Vlevo je obecný ideál, vpravo je ideál v komutativním okruhu.*

Příklad 12.1. Uveďme několik jednoduchých příkladů ideálů.

1) Už víme, že $(\mathbb{Z},+,\cdot)$ je okruh a $(\mathbb{S},+,\cdot)$ je jeho podokruh. Jedná se dokonce o ideál, protože libovolný násobek sudého čísla je sudé číslo.
2) Mějme okruh celých čísel s operacemi obvyklého sčítání a násobní $(\mathbb{Z},+,\cdot)$. Okruh $(n\mathbb{Z},+,\cdot)$ pro $n\in\mathbb{N}$ tvoří ideál v $(\mathbb{Z},+,\cdot)$.
3) V okruhu polynomů je ideálem například podokruh polynomů s nulovým absolutním členem.
4) *Triviální okruh* je $(R,+,\cdot)$, kde $R=\{0\}$. Triviální okruh je ideálem v každém okruhu.
5) Okruh $(R,+,\cdot)$ je jistě podokruhem a ideálem sebe sama. Takový ideál najdeme v každém okruhu.

Příklad 12.2. Uveďme několik jednoduchých příkladů, kdy podokruh ideálem není.

1) Například $(\mathbb{Z},+,\cdot)$ je podokruhem v $(\mathbb{Q},+,\cdot)$, avšak není ideálem, protože například $\frac{1}{2}\in\mathbb{Q}$, $1\in\mathbb{Z}$, ale $\frac{1}{2}\cdot 1\notin\mathbb{Z}$.
2) Už víme, že diagonální matice tvoří komutativní podokruh okruhu $(M_{2,2},+,\cdot)$. Diagonální matice však netvoří ideál okruhu $(M_{2,2},+,\cdot)$ (Cvičení 12.1.3.).
3) Množina lichých celých čísel $\mathbb{L}$ není ideálem v okruhu celých čísel $(\mathbb{Z},+,\cdot)$, protože množina $\mathbb{L}$ není uzavřená vzhledem k operaci sčítání a netvoří okruh (zejména ne podokruh $(\mathbb{Z},+,\cdot)$).

Otázka: Je každý podokruh komutativního okruhu ideálem?

Ideál $(I,+,\cdot)$ se nazývá *nevlastní ideál*, jestliže $I=R$ nebo $I=\{0\}$. Tyto ideály existují v každém okruhu. Ostatní ideály se nazývají *vlastní ideály*. Právě vlastní ideály jsou netriviální a zajímavé struktury.

Následující věta říká, jak ověřit, zda nějaký podokruh je ideálem. Znamená to ověřit, zda se jedná o podokruh a zda má vlastnost ideálu (věta říká, že můžeme ušetřit test uzavřenosti.)

Věta 12.1. Test ideálu
Mějme okruh $(R,+,\cdot)$ a neprázdnou podmnožinu $I \subseteq R$. $(I,+,\cdot)$ je ideál okruhu $(R,+,\cdot)$ právě tehdy, když jsou splněny obě následující vlastnosti.

(i) $\forall a,b \in I : a-b \in I$ *(podokruh)*
(ii) $\forall r \in R\ \forall a \in I : ra \in I \wedge ar \in I$ *(absorpce)*

Důkaz. Jedná se o ekvivalenci, dokážeme obě implikace.
„⇒“ Mějme ideál $(I,+,\cdot)$ okruhu $(R,+,\cdot)$. To znamená, že $(I,+,\cdot)$ je podokruh okruhu $(R,+,\cdot)$ a podle Věty 11.2. platí vlastnost (i). A protože $(I,+,\cdot)$ je ideálem, tak je splněna vlastnost (ii).
„⇐“ Předpokládejme, že jsou splněny vlastnosti (i) a (ii). Abychom ukázali, že $(I,+,\cdot)$ je podokruhem okruhu $(R,+,\cdot)$, tak ověříme oba předpoklady Věty 11.2. Předpoklad (i) je stejný ve Větě 11.2. Zbývá ověřit, zda pro každé $a,b \in I$ platí $a \cdot b \in I$, přičemž v předpokladu (ii) stačí zvolit $r = b$. A konečně podle předpokladu (ii) ihned dostáváme, že podokruh $(I,+,\cdot)$ je dle definice ideál okruhu $(R,+,\cdot)$. □

Všimněte si, jak jsou podmínky Věty 12.1. elegantním zpřísněním podmínek Věty 11.2. Následující věta je analogií Věty 11.3.

Věta 12.2. Průnik ideálů je ideál
Mějme ideály $(I_1,+,\cdot)$ a $(I_2,+,\cdot)$ okruhu $(R,+,\cdot)$. Průnik ideálů $(I_1 \cap I_2,+,\cdot)$ je také ideál okruhu $(R,+,\cdot)$.

Důkaz je ponechán jako Cvičení 12.1.1. Platí i následující silnější tvrzení.

Lemma 12.3. *Mějme ideály $(I_j,+,\cdot)$ okruhu $(R,+,\cdot)$, kde $j \in J$. Průnik ideálů $(\bigcap_{j\in J} I_j,+,\cdot)$ je také ideál okruhu $(R,+,\cdot)$.*

Důkaz je opět ponechán jako Cvičení 12.1.2.

Ideál generovaný množinou
Podobně, jako jsme na straně 107 zavedli podgrupu, která je generována množinou prvků, tak můžeme zavést ideál generovaný množinou prvků.

Definice Ideál generovaný množinou
Mějme okruh $(R,+,\cdot)$ a libovolnou podmnožinu $M \subseteq R$. Symbolem $\langle M \rangle$ označíme průnik všech ideálů v okruhu $(R,+,\cdot)$, které obsahují množinu M. Říkáme mu *ideál generovaný množinou M*.

Definice ideálu generovaného množinou je korektní, neboť vždy existuje nějaký ideál, ve kterém je množina M obsažena, a sice samotný okruh $(R,+,\cdot)$. A podle Věty 12.3. je průnik $\langle M \rangle$ všech takových ideálů také ideálem v okruhu $(R,+,\cdot)$.

Cvičení

12.1.1. Mějme ideály $(I_1,+,\cdot)$ a $(I_2,+,\cdot)$ okruhu $(R,+,\cdot)$. Dokažte Větu 12.2., tj. dokažte, že průnik ideálů $(I_1 \cap I_2,+,\cdot)$ je ideálem okruhu $(R,+,\cdot)$.

12.1.2. Mějme ideály $(I_j,+,\cdot)$ okruhu $(R,+,\cdot)$, kde $j \in J$. Dokažte Lemma 12.3., tj. dokažte, že průnik ideálů $(\bigcap_{j\in J} I_j,+,\cdot)$ je ideálem okruhu $(R,+,\cdot)$.

12.1.3. Ukažte, že diagonální matice netvoří ideál okruhu $(M_{2,2},+,\cdot)$ čtvercových matic řádu 2.

12.1.4. Ukažte, že každý podokruh nulového okruhu je ideálem.

12.2. Faktorový okruh

V kapitole 5. jsme zavedli rozklad grupy podle normální podgrupy. Získali jsme faktorovou grupu. Ukázalo se, že faktorové grupy mohou zjednodušit zkoumání dané grupy, neboť faktorová grupa je menšího řádu a přitom stále má některé vlastnosti původní grupy. Podobně můžeme zkoumat faktorové okruhy. Roli normální podgrupy přitom bude hrát ideál.

Nejprve ukážeme, že když se omezíme na první operaci „+“, tak dostáváme klasický koncept normální podgrupy.

Věta 12.4. *Mějme (oboustranný) ideál $(I,+,\cdot)$ okruhu $(R,+,\cdot)$. Potom $(I,+)$ je normální podgrupa grupy $(R,+)$.*

Důkaz. Nejprve si uvědomme, že $(I,+)$ je podle Věty 3.4. podgrupa grupy $(R,+)$. Dále, protože $(I,+,\cdot)$ je podokruh okruhu $(R,+,\cdot)$, tak podle Věty 12.1. pro každé $a,b\in I$ platí $a-b\in I$.

Navíc z komutativity operace „+“ pro každé $x\in R$ platí $x\oplus I=\{x+i : i\in I\}=I\oplus x$, a proto je $(I,+)$ normální podgrupa grupy $(R,+)$. □

Otázka: Věta 12.4. má tvar implikace. Platí opačná implikace? Tj. platí tvrzení: mějme okruh $(R,+,\cdot)$ a normální podgrupu $(I,+)$ grupy $(R,+)$, potom $(I,+,\cdot)$ je ideálem okruhu $(R,+,\cdot)$?

Nyní sestavíme třídy rozkladu daného okruhu podle nějakého ideálu a zavedeme nové operace s třídami tohoto rozkladu. Ukážeme, že výsledná struktura je také okruhem podobně jako faktorová grupa je také grupou.

Věta 12.5. *Mějme je (oboustranný) ideál $(I,+,\cdot)$ okruhu $(R,+,\cdot)$. Definujme množinu $R/I=\{x+I : x\in R\}$. Definujme operaci „$\oplus$“ a operaci „$\odot$“. Pro každé $x,y\in R/I$ položme $(x+I)\oplus(y+I)=(x+y)+I$ and pro každé $x,y\in R/I$ položme $(x+I)\odot(y+I)=(x\cdot y)+I$. Potom $(R/I,\oplus,\odot)$ je okruh.*

Důkaz. Nejprve ukážeme, že $(R/I,\oplus)$ je komutativní grupa. Podle Věty 5.1. se jedná o faktorovou grupu komutativní grupy $(R,+)$ podle normální podgrupy $(I,+)$.

Dále ukážeme korektnost zavedení operace „$\odot$“, tj. výsledná třída součinu nesmí záviset na volbě označení. Jestliže vezmeme různě označené stejné třídy rozkladu $x_1+I=x_2+I$ a $y_1+I=y_2+I$, tak přičtením stejného prvku $-x_2$ dostaneme $-x_2+x_1+I=-x_2+x_2+I=I$. Podle Věty 4.2. je $-x_2+x_1=i\in I$, tedy $x_1=x_2+i$, kde $i\in I$. Analogicky ukážeme, že $y_1=y_2+j$, kde $j\in I$. Nyní

$$(x_1+I)\odot(y_1+I)=(x_2+i+I)\odot(y_2+j+I)=(x_2+I)\odot(y_2+I),$$

neboť $i+I=I$ a $j+I=J$ podle Věty 4.2.

Dále ověříme zbývající vlastnosti okruhu podle Definice 11.1. Operace „$\odot$“ je jistě uzavřená na nosné množině grupy $(R/I,\oplus)$, neboť součin dvou komplexů rozkladu je komplex rozkladu.

Operace „$\odot$“ je asociativní, což lze ukázat s využitím asociativity operace „$\cdot$“. Pro každé tři třídy rozkladu $(a+I),(b+I),(c+I)\in R/I$ platí $(a+I)\odot((b+I)\odot(c+I))=(a+I)\odot((b\cdot c)+I)=a\cdot(b\cdot c)+I=(a\cdot b)\cdot c=((a\cdot b)+I)\odot(c+I)=((a+I)\odot(b+I))\odot(c+I)$.

Zbývá ukázat distributivitu operace „$\odot$“ vzhledem k operaci „$\oplus$“. Analogicky jako v předchozím odstavci využijeme distributivitu operace „$\cdot$“ vzhledem k operaci „+“. Pro každé tři třídy rozkladu $(a+I),(b+I),(c+I)\in R/I$ platí $(a+I)\odot((b+I)\oplus(c+I))=(a+I)\odot((b+c)+I)=a\cdot(b+c)+I=(a\cdot b+a\cdot c)+I=((a\cdot b)+I)\oplus((a\cdot c)+I)=((a+I)\odot(b+I))\oplus((a+I)\odot(c+I))$.

Distributivitu zprava bychom ukázali analogicky, důkaz vynecháme. Ukázali jsme, že třídy rozkladu R/I s operacemi „$\oplus$“ a „$\odot$“ tvoří okruh. □

Nyní můžeme vyslovit následující definici.

Definice Okruh $(R/I,\oplus,\odot)$ budeme nazývat *faktorový okruh* okruhu $(R,+,\cdot)$ podle ideálu $(I,+,\cdot)$.

Příklad 12.3. $(\mathbb{Z}/\mathbb{S},\oplus,\odot)$ tvoří faktorový okruh se dvěma třídami rozkladu.
Protože podle Příkladu 12.1. je $(\mathbb{S},+,\cdot)$ ideálem v okruhu $(\mathbb{Z},+,\cdot)$, tak $(\mathbb{Z}/\mathbb{S},\oplus,\odot)$ je faktorový okruh. Třídy rozkladu jsou $\mathbb{S}$ a $\mathbb{L}$, příslušné operace jsou popsány Tabulkami 12.1.

$\oplus$	$\mathbb{S}$	$\mathbb{L}$
$\mathbb{S}$	$\mathbb{S}$	$\mathbb{L}$
$\mathbb{L}$	$\mathbb{L}$	$\mathbb{S}$

$\odot$	$\mathbb{S}$	$\mathbb{L}$
$\mathbb{S}$	$\mathbb{S}$	$\mathbb{S}$
$\mathbb{L}$	$\mathbb{S}$	$\mathbb{L}$

Tabulka 12.1.: *Operace v binárním okruhu* $(\{\mathbb{S},\mathbb{L}\},\oplus,\odot)$.

Tabulky vyjadřují dobře známé vlastnosti sudých a lichých čísel, například že součet dvou lichých čísel je sudé číslo, nebo že součin sudého a lichého čísla je opět sudé číslo. ✓

Zavedeme klasickou úmluvu, že operace „$\oplus$“ a „$\odot$“ ve faktorovém okruhu $(R/I, \oplus, \odot)$ budeme značit „$+$“ a „$\cdot$“ stejně jako v původním okruhu $(R, +, \cdot)$. Z kontextu (označení prvků) bude vždy zřejmé, zda pracujeme s operací v původním okruhu nebo s operací ve faktorovém okruhu.

Příklad 12.4. Uveďme několik jednoduchých příkladů faktorových okruhů.

1) Protože okruh $(3\mathbb{Z}, +, \cdot)$ je ideál v okruhu $(\mathbb{Z}, +, \cdot)$, tak zbytkové třídy modulo 3

$$\mathbb{Z}/3\mathbb{Z} = \{z + 3\mathbb{Z} : z \in \mathbb{Z}\} = \{\overline{0}_3, \overline{1}_3, \overline{2}_3\}$$

tvoří faktorový okruh se třemi třídami rozkladu. Už víme (Věta 5.1.), že tyto třídy tvoří grupu s operací sčítání tříd. Nyní protože $(3\mathbb{Z}, +, \cdot)$ je ideál v okruhu $(\mathbb{Z}, +, \cdot)$, tak podle Věty 12.5. zbytkové třídy tvoří faktorový okruh. Tento okruh je oborem integrity a dokonce tělesem (Příklad 11.14.).
2) Protože $(4\mathbb{Z}, +, \cdot)$ je ideál v $(\mathbb{Z}, +, \cdot)$, tak $\mathbb{Z}/4\mathbb{Z}$ je faktorový okruh. Tento faktorový okruh se čtyřmi třídami však není oborem integrity, neboť obsahuje dělitele nuly.
3) Mějme okruh $(R, +, \cdot)$ s nulou 0 a jeho triviální podokruh $(\{0\}, +, \cdot)$. Potom $(R/\{0\}, +, \cdot)$ je faktorovým okruhem, jehož třídy rozkladu jsou jednoprvkové množiny s prvky z R.

Příklad 12.5. Uveďme několik jednoduchých příkladů, kdy struktura není faktorovým okruhem.

1) Okruh celých čísel $(\mathbb{Z}, +, \cdot)$ je podokruhem tělesa $(\mathbb{Q}, +, \cdot)$ i tělesa $(\mathbb{R}, +, \cdot)$. Protože však celá čísla netvoří ideál v ani v jednom z uvedených těles, tak faktorový okruh $(\mathbb{Q}/\mathbb{Z}, +, \cdot)$ není definován.
2) Například $(\mathbb{Z}/\mathbb{L}, +, \cdot)$ není faktorový okruh, neboť $(\mathbb{L}, +, \cdot)$ není ideálem. Operace „$\cdot$“ není uzavřená na $\mathbb{L}$, proto ani operace „$\cdot$“ není konzistentní pro příslušné komplexy.

Je dobré si uvědomit, proč při sestavení faktorového okruhu $(R/I), +, \cdot)$ požadujeme, aby $(I, +, \cdot)$ byl ideál, a proč nestačí aby $(I, +, \cdot)$ byl podokruh okruhu $(R, +, \cdot)$. Podívejme se, která vlastnost bude porušena, pokud bychom chtěli sestavit například faktorový okruh $(\mathbb{Q}/\mathbb{Z}, +, \cdot)$. Protože sčítání celých i racionálních čísel je komutativní operace, tak $(\mathbb{Z}, +)$ je normální podgrupou grupy $(\mathbb{Q}, +)$ a můžeme sestavit faktorovou grupu $(\mathbb{Q}/\mathbb{Z}, +)$. Třídy rozkladu budou tvaru $q + \mathbb{Z}$, přičemž dvě třídy $q_1 + \mathbb{Z}$ a $q_2 + \mathbb{Z}$ budou totožné, pokud $q_2 - q_1 \in \mathbb{Z}$. Problém nastane u operace „$\cdot$“, která *nebude dobře definována*. Vezmeme-li například dvě třídy $\frac{1}{2} + \mathbb{Z}$ a $0 + \mathbb{Z} = \mathbb{Z}$, tak čekáme, že jejich součin je třída $\frac{1}{2} \cdot 0 + \mathbb{Z} = 0 + \mathbb{Z} = \mathbb{Z}$. Vezmeme-li však jiné reprezentanty stejných tříd, například $\frac{1}{2} + \mathbb{Z}$ a $\mathbb{Z} = 1 + \mathbb{Z}$ (neboť $1 - 0 = 1 \in \mathbb{Z}$), tak se zdá, že součinem je třída $\frac{1}{2} \cdot 1 + \mathbb{Z} = \frac{1}{2} + \mathbb{Z} \neq \mathbb{Z}$. Výsledné třídy se liší, evidentně $\frac{1}{2} + \mathbb{Z} \neq \mathbb{Z}$. Ve skutečnosti součin není dobře definovaná operace, neboť součin různých reprezentantů dává reprezentanty různých tříd. Právě vlastnost absorpce hlavního ideálu dává jistotu, že nejen součet, ale i součin bude dobře definovaná operace.

Vlastnosti faktorových okruhů

Ukážeme, že komutativita i existence jedničky okruhu $(R, +, \cdot)$ se přenese na každý faktorový okruh tohoto okruhu.

Věta 12.6. *Mějme je (oboustranný) ideál $(I, +, \cdot)$ okruhu $(R, +, \cdot)$. Potom platí následující tvrzení.*

(i) Jestliže je okruh $(R, +, \cdot)$ komutativní, potom je i faktorový okruh $(R/I, +, \cdot)$ komutativní.
(ii) Jestliže okruh $(R, +, \cdot)$ má jedničku, potom i faktorový okruh $(R/I, +, \cdot)$ má jedničku.

Důkaz. Ihned z definice operace násobení dostaneme obě tvrzení. Komutativita plyne z komutativity operace na R.

$$(a + B) \cdot (b + I) = ab + I = ba + I = (b + I) \cdot (a + I)$$

Dále jedničkou je třída $1 + I$, neboť pro každé $a + I \in R/I$ podle definice násobení tříd rozkladu platí

$$(a + I) \cdot (1 + I) = a1 + I = a + I,$$

protože v okruhu $(R, +, \cdot)$ je $a1 = a$. Druhá rovnost $(1 + I) \cdot (a + I) = a + I$ se ukáže analogicky. □

Faktorové okruhy můžeme chápat jako nástroj, jak z větších okruhů (s více prvky) vyrobit podobné menší okruhy (s méně prvky). Má-li okruh více různých ideálů, můžeme vyrobit více různých faktorových okruhů, které částečně zachovávají strukturu původního okruhu. Tomuto aspektu se budeme věnovat v Kapitole 13.

Cvičení

12.2.1. Mějme okruh čtvercových řádu matic s celočíselnými prvky $(M_{2,2}(\mathbb{Z}),+,\cdot)$. Označme I množinu všech čtvercových řádu matic se sudými celočíselnými prvky. Ukažte, že podokruh $(I,+,\cdot)$ je ideálem okruhu $(M_{2,2}(\mathbb{Z}),+,\cdot)$. Kolik prvků má faktorový okruh $(M_{2,2}(\mathbb{Z})/_I,+,\cdot)$?

12.2.2. Ukažte, že okruh $(\mathbb{Z},+,\cdot)$ není ideálem v tělese $(\mathbb{R},+,\cdot)$.

12.2.3. Ukažte, že je-li $(I,+,\cdot)$ ideál v komutativním okruhu $(R,+,\cdot)$ a $a \notin I$, tak množina $J = \{r \in R : a \cdot r \in I\}$ je nosičem ideálu v okruhu $(R,+,\cdot)$.

12.2.4. Mějme okruh $(R,+,\cdot)$ a libovolný prvek $a \in R$. Ukažte, že platí $\langle\{a\}\rangle = \{a \cdot r : r \in R\}$.

12.2.5. Dokažte silnější verzi Věty 12.4. Mějme podokruh $(H,+,\cdot)$ okruhu $(R,+,\cdot)$. Potom $(H,+)$ je normální podgrupa grupy $(R,+)$.

12.2.6. Mějme okruh $(R,+,\cdot)$ a jeho podokruh $(H,+,\cdot)$. Sestavíme rozklad $R/_H$ a definujeme operace „$\oplus$“ a „$\odot$“ jako ve Větě 12.5. Ukažte, že aby byly obě operace dobře definovány, musí podokruh $(H,+,\cdot)$ být (oboustranným) ideálem v okruhu $(R,+,\cdot)$. Tj. ukažte, že vlastnost ideálu je nejen postačují, ale i nutná pro existenci faktorového okruhu $(R/_H,\oplus,\odot)$.*

12.2.7. Dokažte nebo vyvraťte: V okruhu $(\mathbb{Q},+,\cdot)$ neexistuje netriviální vlastní ideál.

12.2.8. Dokažte nebo vyvraťte: V tělese $(R,+,\cdot)$ neexistuje netriviální vlastní ideál.

12.3. Okruh polynomů

Důležitým příkladem faktorových okruhů budou okruhy sestavené z polynomů.

Okruh funkcí
Nejprve si všimneme, že i s funkcemi můžeme pracovat jako s prvky nějakého okruhu.

Příklad 12.6. Mějme R množinu všech reálných funkcí jedné reálné proměnné, jejichž definiční obor jsou všechna reálná čísla. Operace „$+$“ je dána předpisem

$$\forall x \in \mathbb{R} : (f+g)(x) = f(x) + g(x)$$

Operace „$\cdot$“ je dána předpisem

$$\forall x \in \mathbb{R} : (f \cdot g)(x) = f(x) \cdot g(x)$$

Uvedené operace jsou klasické sčítání a násobení funkcí. Potom $(R,+,\cdot)$ je okruh. Nulovým prvkem tohoto okruhu je konstantní funkce $o(x) = 0$ a jedničkou je konstantní funkce $j(x) = 1$.

Polynomy patří mezi funkce s velmi pěknými vlastnostmi. Nyní zavedeme okruh polynomů.

Otázka: Proč není okruh polynomů ideálem v okruhu funkcí?

Definice Mějme netriviální komutativní okruh $(R,+,\cdot)$. Označme

$$R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : n \in \mathbb{N}, a_1, a_2, \ldots, a_n \in R\}.$$

Množinu $R[x]$ nazveme *množinou polynomů nad* R a její prvky jsou *polynomy* v proměnné x. Řekneme, že dva polynomy $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0 \in R[x]$ jsou si *rovny* právě tehdy, když $n = m$ a $a_i = b_i$ pro všechna $0 \leq i \leq n$.

Všimněte si, že symbol „$+$“ se v definici okruhu polynomů používá ve dvou významech. Jednak označuje operaci v okruhu $(R,+,\cdot)$ a jednak v definici množiny $R[x] = \{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 : n \in \mathbb{N}, a_1, a_2, \ldots, a_n \in R\}$ odděluje jednotlivé členy polynomu.

Je důležité si uvědomit, že prvky v $R[x]$ neuvažujeme jako funkce určené předpisem polynomu, ale jako posloupnosti koeficientů. Písmeno x neuvažujeme (nyní) jako proměnnou, za kterou bychom dosazovali číselné hodnoty. Později budeme sice do polynomů z $R[x]$ dosazovat za x prvky okruhu R, avšak při sestavení okruhu polynomů se jedná pouze o symbol, který rozlišuje prvky posloupnosti koeficientů daného polynomu.

Příklad 12.7. Zdůrazněme rozdíl mezi polynomem a polynomickou funkcí.

1) Například v okruhu $(\mathbb{Z}_3[x],+,\cdot)$ jsou $p(x) = x$ a $q(x) = x^3$ různé polynomy, které však určují stejnou funkci $\mathbb{Z}_3 \to \mathbb{Z}_3$, neboť $\mathbb{Z}_3 = \{\overline{0},\overline{1},\overline{2}\}$ a platí $p(\overline{0}) = \overline{0} = q(\overline{0})$, $p(\overline{1}) = \overline{1} = q(\overline{1})$, $p(\overline{2}) = \overline{2} = q(\overline{2})$.

2) Naproti tomu například $p(x) = x$ a $r(x) = x^2$ jsou v okruhu $(\mathbb{Z}_3[x], +, \cdot)$ různé polynomy, které určují různé funkce v okruhu $(\mathbb{Z}_3[x], +, \cdot)$. Platí $p(\overline{0}) = \overline{0} = r(\overline{0})$, $p(\overline{1}) = \overline{1} = r(\overline{1})$, ale $p(\overline{2}) = \overline{2} \neq \overline{1} = r(\overline{2})$.

Uvědomte si, že množina $R[x]$ je vždy nekonečná. Protože číslo n (později zavedeme obvyklou terminologii, dle které n je stupeň polynomu) není pevně zvolené přirozené číslo, tak i v případě, že R je konečná množina, obsahuje $R[x]$ polynomy s libovolnou hodnotou „stupně“ $n \in \mathbb{N}$.

Příklad 12.8. Ukážeme několik jednoduchých příkladů množin polynomů.

1) Množina $\mathbb{Z}[x]$ je množinou polynomů s celočíselnými koeficienty, množina $\mathbb{Q}[x]$ je množinou polynomů s racionálními koeficienty, množina $\mathbb{R}[x]$ je množinou polynomů s reálnými koeficienty, množina $\mathbb{C}[x]$ je množinou polynomů s komplexními koeficienty.
2) Množina $M_{2,2}(\mathbb{Z})[x]$ je množinou polynomů, jejichž koeficienty jsou čtvercové matice řádu 2 s celočíselnými koeficient.
3) Množina $S_n[x]$ je množinou polynomů, jejichž koeficienty jsou permutace řádu n. Nebude však mít smysl sestavovat okruh polynomů nad množinou S_n, neboť k dispozici máme jen jednu přirozenou operaci skládání permutací.
4) Množina $D_n[x]$ je množinou polynomů, jejichž koeficienty jsou permutace řádu n. Opět nemá smysl sestavovat okruh polynomů nad množinou D_n, neboť k dispozici máme jedinou přirozenou operaci skládání zobrazení.

Příklad 12.9. Ukážeme několik příkladů, které množinou polynomů nejsou.

1) $\mathbb{N}[x]$ není množinou polynomů, neboť $\mathbb{N}$ netvoří okruh. Nemáme opačné prvky.
2) $\mathbb{L}[x]$ není množinou polynomů, neboť $\mathbb{L}$ netvoří okruh a operace sčítání není na množině $\mathbb{L}$ uzavřená. Později uvidíme, že by ani operace sčítání polynomů nebyla uzavřená na množině $\mathbb{L}[x]$.

Otázky:

- Kolik existuje různých funkcí $\mathbb{Z}_3 \to \mathbb{Z}_3$?
- Kolik existuje různých polynomů v okruhu $(\mathbb{Z}_3[x], +, \cdot)$?
- Kolik existuje různých polynomů stupně nejvýše tři v okruhu $(\mathbb{Z}_3[x], +, \cdot)$?

Častá chyba při chápání množiny polynomů

V okruzích polynomů $(\mathbb{Z}_n[x], +, \cdot)$ počítáme s koeficienty modulo n, exponenty však zachováváme! Častou chybou je redukce exponentů modulo n. Například v okruhu polynomů $(\mathbb{Z}_3[x], +, \cdot)$ polynom $p(x) = 5x^4 - x + 7 = 2x^4 + 2x + 1$, ale $q(x) = x^5 \neq x^2$. Později ukážeme, že má smysl počítat s konečnými množinami polynomů, avšak nikoliv pouhou redukcí exponentů modulo n. Bude se jednat o faktorové okruhy polynomů.

Operace při počítání s polynomy

S polynomy můžeme provádět klasické operace sčítání a násobení. Operace součtu a součinu polynomů budou definovány „přirozeně“ tak, jak jsme zvyklí s polynomy počítat. Stále však musíme mít na paměti, že se na polynomy díváme jen jako na prvky nějakého okruhu, nikoliv jako na funkce, které číslům přiřazují funkční hodnoty. Následující definice ukazuje, jak obě operace formálně popsat, i když s polynomy nepracujeme jako s funkcemi.

Definice Operace v množině polynomů

Mějme komutativní okruh $(R, +, \cdot)$ a dva polynomy $a(x), b(x) \in R[x]$, kde $a(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $b(x) = b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0$. *Součet polynomů* je

$$a(x) + b(x) = (a_s + b_s)x^s + (a_{s-1} + b_{s-1})x^{s-1} + \cdots + (a_1 + b_1)x + a_0 + b_0,$$

kde $s = \max\{n, m\}$, přičemž $a_i = 0$ pro všechna přirozená čísla $i > n$ a $b_j = 0$ pro všechna přirozená čísla $j > m$. Dále *součin polynomů* je

$$a(x) \cdot b(x) = c_{m+n}x^{m+n} + c_{m+n-1}x^{m+n-1} + \cdots + c_1 x + c_0,$$

kde $c_k = a_k b_0 + a_{k-1}b_1 + \cdots + a_1 b_{k-1} + a_0 b_k$ pro všechna $k = 0, 1, \ldots, m + n$.

Symbol „+“ se v definici operací v okruhu polynomů používá ve třech významech. Jednak označuje první operaci v okruhu $(R,+,\cdot)$, dále odděluje jednotlivé členy polynomu v definici množiny $R[x]=\{a_nx^n+\\+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 : n\in\mathbb{N}, a_1,a_2,\ldots,a_n\in R\}$ a konečně označuje operaci sčítání polynomů $a(x)+b(x)$. Dále symbol „$\cdot$“ se v definici používá ve dvou významech. Jednak označuje druhou operaci v okruhu $(R,+,\cdot)$, kterou v popisu $c_k=a_kb_0+a_{k-1}b_1+\cdots+a_1b_{k-1}+a_0b_k$ podle úmluvy vynecháváme, a dále označuje násobení polynomů $a(x)\cdot b(x)$.

Všimněte si, že takto definované sčítání i násobení polynomů přesně odpovídá klasickým početním operacím, na které jsme zvyklí při práci s polynomickými funkcemi. Hlavním rozdílem je, že koeficienty nejsou nutně reálná čísla, ale pracujeme s prvky nějakého okruhu.

Příklad 12.10. Mějme dva polynomy $a(x)=2x^3+1x^2+2$, $b(x)=2x^2+1x+2$ okruhu polynomů $(\mathbb{Z}_3[x],+,\cdot)$. Vypočítáme součet a součin obou polynomů.
Pro výpočet $a(x)+b(x)$ sečteme koeficienty odpovídajících mocnin. Nesmíme zapomenout, že koeficienty sčítáme nad okruhem $(\mathbb{Z}_3[x],+,\cdot)$.

$$a(x)+b(x)=(2x^3+1x^2+2)+(2x^2+1x+2)=2x^3+0x^2+1x+1=2x^3+1x+1$$

Pro výpočet $a(x)\cdot b(x)$ vypočítáme koeficienty u každé mocniny podle vztahu $c_k=a_kb_0+a_{k-1}b_1+\cdots+\\+a_1b_{k-1}+a_0b_k$ pro všechna $k=0,1,\ldots,m+n$. Dostaneme

$$c_0=2\cdot2=4\equiv1 \pmod 3, c_1=2\cdot1=2, c_2=1\cdot2+2\cdot2=6\equiv0 \pmod 3,$$

$$c_3=2\cdot2+1\cdot1=3\equiv0 \pmod 3, c_4=2\cdot1+1\cdot2=4\equiv1 \pmod 3, c_5=2\cdot2=4\equiv1 \pmod 3.$$

Proto

$$a(x)\cdot b(x)=(2x^3+1x^2+2)\cdot(2x^2+1x+2)=1x^5+1x^4+0x^3+0x^2+2x+1=1x^5+1x^4+2x+1.$$

✓

Okruh polynomů
Nyní můžeme vyslovit následující definici.

Definice Mějme komutativní okruh $(R,+,\cdot)$. Uspořádaná trojice $(R[x],+,\cdot)$, kterou tvoří množina

$$R[x]=\{a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0 : n\in\mathbb{N}, a_1,a_2,\ldots,a_n\in R\}.$$

spolu s operacemi sčítání a násobení polynomů, se nazývá *okruhem polynomů nad R v proměnné x* nebo stručně *okruhem polynomů nad R.*

Nejprve ukážeme, že definice je korektní.

Lemma 12.7. *Jestliže $(R,+,\cdot)$ je komutativní okruh, pak $(R[x],+,\cdot)$ je komutativní okruh.*

Důkaz. Víme, že nosná množina je neprázdná, neboť například nulový polynom $o(x)=0$ je v každém okruhu polynomů. Dále je z definice operací zřejmé, že jak sčítání, tak násobení polynomů jsou operace uzavřené na $R[x]$, neboť výsledek součtu i součinu polynomů jsou polynomy z $R[x]$. Dále násobení i sčítání polynomů jsou komutativní i asociativní operace, protože násobení i sčítání v okruhu $(R,+,\cdot)$ jsou komutativní i asociativní operace, což se ověří dosazením a úpravou (Cvičení 12.3.2.).

Nulou okruhu polynomů je polynom $o(x)=0$. Opačným prvkem k polynomu $a(x)=a_nx^n+a_{n-1}x^{n-1}+\\+\cdots+a_1x+a_0$ je polynom $-a(x)=-a_nx^n+(-a_{n-1})x^{n-1}+\cdots+(-a_1)x+(-a_0)=-a_nx^n-a_{n-1}x^{n-1}-\\\cdots-a_1x-a_0$. Nyní víme, že $(R[x],+)$ je komutativní grupa a že $(R[x],\cdot)$ je komutativní pologrupa.

Dále jedničkou okruhu polynomů je polynom $j(x)=1$, kde 1 je jedničkou okruhu $(R,+,\cdot)$. Ověřit distributivitu operací součinu a součtu polynomů je technicky náročné, využijeme sumy. Mějme $a(x),b(x),c(x)\in$

$R[x]$, kde $a(x)=\sum_{i=0}^{n} a_i x^i$, $b(x)=\sum_{j=0}^{m} b_j x^j$ a $c(x)=\sum_{k=0}^{p} c_k x^k$. Označme $l=\max\{m,n,p\}$ a položme $a_i=0$ pro $n<i\leq l$, $b_j=0$ pro $m<j\leq l$, $c_k=0$ pro $p<k\leq l$. Potom

$$\begin{aligned}
a(x)\,(b(x)+c(x)) &= \sum_{i=0}^{n} a_i x^i \left(\sum_{j=0}^{m} b_j x^j + \sum_{k=0}^{p} c_k x^k\right) = \sum_{i=0}^{l} a_i x^i \left(\sum_{j=0}^{l} b_j x^j + \sum_{k=0}^{l} c_k x^k\right)\\
&= \sum_{i=0}^{l} a_i x^i \sum_{j=0}^{l} \left(b_j x^j + c_j x^j\right) = \sum_{i=0}^{l} a_i x^i \sum_{j=0}^{l} \left(b_j + c_j\right) x^j\\
&= \sum_{i=0}^{2l} \left(\sum_{j=0}^{i} a_j (b_{i-j} + c_{i-j}) x^j\right) = \sum_{i=0}^{2l} \left(\sum_{j=0}^{i} (a_j b_{i-j} + a_j c_{i-j}) x^j\right)\\
&= \sum_{i=0}^{2l} \sum_{j=0}^{i} a_j b_{i-j} x^j + \sum_{i=0}^{2l} \sum_{j=0}^{i} a_j c_{i-j} x^j = \sum_{i=0}^{l} a_i x^i \sum_{j=0}^{l} b_j x^j + \sum_{i=0}^{l} a_i x^i \sum_{k=0}^{l} c_k x^k\\
&= \sum_{i=0}^{n} a_i x^i \sum_{j=0}^{m} b_j x^j + \sum_{i=0}^{n} a_i x^i \sum_{k=0}^{p} c_k x^k = a(x)b(x) + a(x)c(x).
\end{aligned}$$

Druhý distributivní zákon nemusíme díky komutativitě operací ověřovat. Celkem dostáváme, že $(R[x],+,\cdot)$ je okruh, dokonce komutativní okruh. □

Příklad 12.11. Uveďme několik jednoduchých příkladů okruhu polynomů.

1) $(\mathbb{R}[x],+,\cdot)$ je klasický okruh všech polynomů s reálnými koeficienty.
2) $(\mathbb{Z}[x],+,\cdot)$ je okruh všech polynomů s celočíselnými koeficienty.
3) $(\mathbb{Z}_n[x],+,\cdot)$ je okruh všech polynomů s koeficienty z množiny $\mathbb{Z}_n$. Speciálně $(\mathbb{Z}_2[x],+,\cdot)$ je okruh binárních polynomů.

Příklad 12.12. Dále uveďme několik příkladů, kdy okruh polynomů nedostaneme.

1) Trojice $(\mathbb{N}[x],+,\cdot)$ není okruhem polynomů, protože trojice $(\mathbb{N},+,\cdot)$ není okruhem; nemáme opačné prvky vzhledem k operaci „+“.
2) Trojice $(M_{2,2}(\mathbb{Z})[x],+,\cdot)$ není okruhem polynomů, protože operace „$\cdot$“ není komutativní.

V každém okruhu polynomů můžeme zavést některé pojmy, které známe z analýzy polynomických funkcí.

Definice Mějme komutativní okruh $(R,+,\cdot)$ a okruh polynomů $(R[x],+,\cdot)$. Mějme polynom $p(x)=a_n x^n + \\ + a_{n-1}x^{n-1}+\cdots+a_1 x+a_0$. Je-li $a_n\neq 0$ (kde 0 je nula okruhu $(R,+,\cdot)$), tak *stupeň polynomu* $p(x)$ je n. Polynom $o(x)=0$ nazýváme *nulový polynom*. Nulový polynom nemá definovaný stupeň. Dále $a_n x^n$ je *vedoucí člen* polynomu $p(x)$ a a_n je *vedoucí koeficient* polynomu $p(x)$. Polynomy tvaru $p(x)=a_0$ jsou *konstantní polynomy*, které pro $a_0\neq 0$ jsou stupně 0.

Nyní ukážeme, že pokud je okruh $(R,+,\cdot)$ netriviální, komutativní a nemá dělitele nuly, tak tyto vlastnosti bude mít také příslušný okruh polynomů $(R[x],+,\cdot)$.

Věta 12.8. *Jestliže $(D,+,\cdot)$ je obor integrity, pak trojice $(D[x],+,\cdot)$ je obor integrity.*

Důkaz. Protože každý obor integrity $(D,+,\cdot)$ je komutativní okruh, tak podle Lemmatu 12.7. víme, že $(D[x],+,\cdot)$ je komutativní okruh. Tento okruh má jedničku: jedničkou je polynom $j(x)=1$, kde 1 je jedničkou oboru integrity $(D,+,\cdot)$. Protože $o(x)=0\neq 1=j(x)$, je množina $D[x]$ netriviální.

Nyní stačí ukázat, že v okruhu nejsou (netriviální) dělitelé nuly. Mějme dva polynomy $a(x)=a_n x^n + \\ + a_{n-1}x^{n-1}+\cdots+a_1 x+a_0, b(x)=b_m x^m+b_{m-1}x^{m-1}+\cdots+b_1 x+b_0\in D[x]$, kde $a_n\neq 0$ a $b_m\neq 0$. Potom podle definice součinu polynomů je vedoucí koeficient součinu $a(x)\cdot b(x)$ roven $a_n b_m$, a protože $(D,+,\cdot)$ je oborem integrity, tak součin $a_n b_m\neq 0$. To znamená, že součin $a(x)\cdot b(x)\neq o(x)$ a v okruhu $(D[x],+,\cdot)$ nejsou dělitelé nuly. □

Cvičení

12.3.1. Ukažte, že je-li $(R,+,\cdot)$ těleso, tak $(R[x],+,\cdot)$ těleso být nemusí.

12.3.2. Mějme komutativní okruh $(R,+,\cdot)$. Sestavíme okruh polynomů $(R[x],+,\cdot)$. Ukažte, že operace násobení i sčítání polynomů definované na straně 180 jsou komutativní i asociativní operace.

12.3.3. Proveďte operace s polynomy v okruhu $(\mathbb{Z}_3[x],+,\cdot)$.

(i) $(x^3-2x^2+6x+3)+(5x^2-2x+1)$
(ii) $(x^2+2x-1)(x+2)$

12.3.4. Určete zbytek po dělení $(x^5+2x^4-2x^2+x+2):(x^2+x+2)$ v okruhu $(\mathbb{Z}_3[x],+,\cdot)$.

12.3.5. Určete zbytek po dělení $(x^4-2x^3-x^2+2x-1):(x^2+x+2)$ v okruhu $(\mathbb{Z}_3[x],+,\cdot)$.

12.3.6. Nalezněte všechny možné zbytky po dělení polynomu $f(x)$ v okruhu $(\mathbb{Z}_3[x],+,\cdot)$ polynomem x^2+x+2.

12.3.7. Popište množinu všech polynomů $f(x)$, které v okruhu $(\mathbb{Z}_3[x],+,\cdot)$ dávají po dělení polynomem x^2+x+2 zbytek $x+2$.

12.3.8. Dokažte nebo vyvraťte: Mějme těleso $(R,+,\cdot)$. Okruh $(R[x],+,\cdot)$ nikdy není těleso.

12.4. Ideály v okruhu polynomů

Ukážeme, jak konstruovat ideály v okruhu polynomů a pomocí nich budeme sestavovat konečná tělesa různých řádů.

Hlavní ideál

Speciálním případem ideálů jsou ideály, které vzniknou jako množina násobků jednoho prvku.

Definice Mějme komutativní okruh $(R,+,\cdot)$ s jedničkou a nějaký prvek $a\in R$. Označme $\langle a\rangle=\{a\cdot r : r\in R\}$. Trojice $(\langle a\rangle,+,\cdot)$ se nazývá *hlavní ideál* okruhu R.

Nejprve ukážeme, že definice je korektní, tj. množina násobků prvku a spolu s restrikcemi operací okruhu $(R,+,\cdot)$ je ideálem v tomto okruhu.

Věta 12.9. *Mějme komutativní okruh $(R,+,\cdot)$ a nějaký prvek $a\in R$. Potom $(\langle a\rangle,+,\cdot)$ je ideál okruhu $(R,+,\cdot)$.*

Důkaz. Jistě platí, že $\langle a\rangle$ je neprázdná podmnožina v R, neboť podle definice $1\in R$ a $a\cdot 1\in\langle a\rangle$. Dále stačí ověřit předpoklady Věty 12.1. (Test ideálu).

Mějme dva prvky $x,y\in\langle a\rangle$. Ukážeme, že i jejich rozdíl $x-y$ patří do $\langle a\rangle$. Protože $x\in\langle a\rangle$, tak existuje $b\in R$ takové, že $x=a\cdot b$. Podobně, protože $y\in\langle a\rangle$, tak existuje $c\in R$ takové, že $y=a\cdot c$. Nyní s využitím Věty 11.1. dostaneme $x-y=a\cdot b-a\cdot c=a\cdot(b-c)$. Protože $b-c=d\in R$, tak podle definice hlavního ideálu je $x-y=a\cdot d\in\langle a\rangle$ a tvrzení platí.

Zbývá ukázat, že pro každé $b\in R$ a každé $i\in\langle a\rangle$ je také $bi\in\langle a\rangle$. Z definice hlavního ideálu je $i=ar$ pro nějaké $r\in R$. Potom z komutativity a asociativity je $bi=b(ar)=a(rb)=ac$, kde $c=rb$, $c\in R$, což podle definice hlavního ideálu znamená, že $bi\in\langle a\rangle$. □

Příklad 12.13. Uveďme několik jednoduchých příkladů hlavních ideálů.

1) Okruh $(\mathbb{S},+,\cdot)$ je hlavním ideálem $(\langle 2\rangle,+,\cdot)$ okruhu $(\mathbb{Z},+,\cdot)$.
2) Pro každé $n\in\mathbb{N}$ je $(\langle n\rangle,+,\cdot)$ hlavním ideálem okruhu $(\mathbb{Z},+,\cdot)$. Navíc platí $\langle n\rangle=n\mathbb{Z}$.
3) *Triviální okruh* $(\{0\},+,\cdot)$ je hlavním ideálem v každém okruhu, neboť $\langle 0\rangle=\{0\}$.
4) Každý okruh $(R,+,\cdot)$ s jedničkou je svým (nevlastním) hlavním ideálem, neboť $(R,+,\cdot)=(\langle 1\rangle,+,\cdot)$.

Příklad 12.14. Uveďme několik jednoduchých příkladů ideálů, které nejsou hlavním ideálem.

1) Mějme okruh $(T,+,\cdot)$, kde T je taková podmnožina polynomů $T\subseteq\mathbb{Z}[x]$ s celočíselnými koeficienty, které mají sudý absolutní člen. Tento okruh je ideálem v okruhu $(\mathbb{Z}[x],+,\cdot)$ (Cvičení12.4.1.), avšak není hlavním ideálem (Cvičení 12.4.2.)
2) Mějme okruh $(\mathbb{S},+,\cdot)$. Žádný jeho ideál není hlavním ideálem, neboť okruh $(\mathbb{S},+,\cdot)$ nemá jedničku.
3) Mějme okruh $(M_{n,n},+,\cdot)$ čtvercových matic řádu n. Žádný jeho případný ideál není hlavním ideálem, neboť okruh $(M_{n,n},+,\cdot)$ není komutativní.

4) Trojice $(\mathbb{N},+,\cdot)$ není hlavním ideálem okruhu $(\mathbb{Z},+,\cdot)$, neboť trojice $(\mathbb{N},+,\cdot)$ není ideálem, ani podokruhem okruhu $(\mathbb{Z},+,\cdot)$, protože netvoří okruh. Chybí nula i opačné prvky.

Na straně 176 jsme definovali ideál generovaný množinou prvků. Hlavní ideál můžeme analogicky definovat jako průnik všech ideálů, které daný prvek obsahují, neboli jako ideál generovaný jednoprvkovou množinou. Obě struktury: hlavní ideál $(\langle a\rangle,+,\cdot)$ i ideál generovaný množinou $(\langle\{a\}\rangle,+,\cdot)$ jsou totožné, důkaz je ponechán jako Cvičení 12.2.4.

Nyní je zřejmé, proč je součástí definice požadavek, aby okruh obsahoval jedničku. Pokud bychom jedničku nepožadovali, tak hlavní ideál generovaný prvkem by neodpovídal ideálu generovanému jednoprvkovou množinou. Například v okruhu sudých čísel $(\mathbb{S},+,\cdot)$ je podokruh generovaný jednoprvkovou množinou $\{2\}$ právě celý okruh $(\mathbb{S},+,\cdot)$. V Příkladu 12.1. jsme ukázali, že okruh $(\mathbb{S},+,\cdot)$ je dokonce ideálem okruhu $(\mathbb{Z},+,\cdot)$. Hlavní ideál však není definovaný, protože $\mathbb{S}$ neobsahuje jedničku. Pokud bychom existenci jedničky v definici nepožadovali, tak výsledný „hlavní ideál“ by neobsahoval například číslo 2, platilo by $\langle 2\rangle = 4\mathbb{Z}$, nikoliv celé $\langle 2\rangle = \mathbb{S} = 2\mathbb{Z}$.

Ideály v okruhu polynomů

Nyní ukážeme ideály v okruhu polynomů, které mají speciální tvar. Stačí vzít všechny (polynomiální) násobky nějakého pevně zvoleného polynomu. Z Věty 12.9. ihned vyplývá následující tvrzení.

Důsledek 12.10. *Mějme okruh polynomů $(R[x],+,\cdot)$ nad komutativním okruhem $(R,+,\cdot)$ a mějme nějaký polynom $p(x)\in R[x]$. Položme*

$$\langle p(x)\rangle = \{p(x)\cdot f(x) : f(x)\in R[x]\}.$$

Potom trojice $(\langle p(x)\rangle,+,\cdot)$ je ideálem v okruhu polynomů $(R[x],+,\cdot)$.

Důkaz. Protože okruh polynomů je $(R[x],+,\cdot)$ komutativní, tak podle Věty 12.9. tvrzení platí. □

Dá se ukázat, že dokonce všechny ideály v okruhu polynomů jsou tvaru $\langle p(x)\rangle$.

Využití hlavních ideálů

Už víme, že rozkladem okruhu podle ideálu získáme faktorový okruh. Nyní budeme rozkládat okruhy polynomů podle hlavních ideálů a dostaneme tak faktorové okruhy. Některé z takto získaných faktorových okruhů budou navíc tělesem. Ukážeme, jak je možno sestavit faktorový okruh libovolného řádu n^k, kde n, k jsou přirozená čísla.

Příklad 12.15. Sestavíme faktorový okruh $(\mathbb{Z}_3[x]/\langle x^2+1\rangle,+,\cdot)$. Sestavíme tabulky násobení a sčítání.

Abychom sestavili faktorový okruh, najdeme nejprve všechny možné zbytky $r(x)$ po dělení polynomem $p(x)=x^2-1$.

$$0,\quad 1,\quad 2,\quad x,\quad x+1,\quad x+2,\quad 2x,\quad 2x+1,\quad 2x+2$$

Třídy rozkladu faktorového okruhu mají tvar $r(x)+\langle x^2-1\rangle$, budeme je stručně označovat

$$\overline{0},\quad \overline{1},\quad \overline{2},\quad \overline{x},\quad \overline{x+1},\quad \overline{x+2},\quad \overline{2x},\quad \overline{2x+1},\quad \overline{2x+2}.$$

Sestavíme-li tabulku sčítání tříd rozkladu. Dostaneme Tabulku 12.2. Dále sestavíme-li tabulku násobení tříd rozkladu. Dostaneme Tabulku 12.3. ✓

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$	$\overline{x+2}$	$\overline{x}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{x+2}$	$\overline{x+2}$	$\overline{x}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2}$	$\overline{0}$	$\overline{1}$
$\overline{2x}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$
$\overline{2x+1}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{1}$	$\overline{2}$	$\overline{0}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{x}$
$\overline{2x+2}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2}$	$\overline{0}$	$\overline{1}$	$\overline{x+2}$	$\overline{x}$	$\overline{x+1}$

Tabulka 12.2.: *Tabulka operace sčítání ve faktorovém okruhu $(\mathbb{Z}_3[x]/\langle x^2+1\rangle,+,\cdot)$.*

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$	$\overline{2x}$	$\overline{2x+2}$	$\overline{2x+1}$	$\overline{x}$	$\overline{x+2}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{2x}$	$\overline{2}$	$\overline{x+2}$	$\overline{2x+2}$	$\overline{1}$	$\overline{x+1}$	$\overline{2x+1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{x+2}$	$\overline{2x}$	$\overline{1}$	$\overline{2x+1}$	$\overline{2}$	$\overline{x}$
$\overline{x+2}$	$\overline{0}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$	$\overline{2x}$	$\overline{2}$
$\overline{2x}$	$\overline{0}$	$\overline{2x}$	$\overline{x}$	$\overline{1}$	$\overline{2x+1}$	$\overline{x+1}$	$\overline{2}$	$\overline{2x+2}$	$\overline{x+2}$
$\overline{2x+1}$	$\overline{0}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{x+1}$	$\overline{2}$	$\overline{2x}$	$\overline{2x+2}$	$\overline{x}$	$\overline{1}$
$\overline{2x+2}$	$\overline{0}$	$\overline{2x+2}$	$\overline{x+1}$	$\overline{2x+1}$	$\overline{x}$	$\overline{2}$	$\overline{x+2}$	$\overline{1}$	$\overline{2x}$

Tabulka 12.3.: *Tabulka operace násobení ve faktorovém okruhu* $(\mathbb{Z}_3[x]/\langle x^2+1\rangle, +, \cdot)$.

Vyřešíme druhý příklad s velmi podobným zadáním.

Příklad 12.16. Sestavíme faktorový okruh $(\mathbb{Z}_3[x]/\langle x^2-1\rangle, +, \cdot)$. Sestavíme tabulky násobení a sčítání. Opět najdeme nejprve všechny možné zbytky $r(x)$ po dělení polynomem $p(x) = x^2 - 1$.

$$0, \quad 1, \quad 2, \quad x, \quad x+1, \quad x+2, \quad 2x, \quad 2x+1, \quad 2x+2$$

Třídy rozkladu faktorového okruhu mají tvar $r(x) + \langle x^2-1\rangle$, označíme je

$$\overline{0}, \quad \overline{1}, \quad \overline{2}, \quad \overline{x}, \quad \overline{x+1}, \quad \overline{x+2}, \quad \overline{2x}, \quad \overline{2x+1}, \quad \overline{2x+2}.$$

Všimněte si, že třebaže jsou třídy označeny stejně jako v Příkladu 12.15., jedná se o *jiné třídy*. V každé třídě jsou obecně jiné polynomy. Zatímco třída $\overline{1}$ okruhu $(\mathbb{Z}_3[x]/\langle x^2+1\rangle, +, \cdot)$ obsahuje například polynomy $1, x^2+2, 2x^2, \ldots$, tak třída $\overline{1}$ okruhu $(\mathbb{Z}_3[x]/\langle x^2-1\rangle, +, \cdot)$ sice obsahuje polynom 1, avšak neobsahuje polynomy x^2+2 ani $2x^2$.

Sestavíme Cayleyho tabulku sčítání 12.4. v okruhu $(\mathbb{Z}_3[x]/\langle x^2-1\rangle, +, \cdot)$. Tabulka je *stejná* jako Tabulka 12.2. Avšak Cayleyho tabulka násobení 12.5. bude mít jinou strukturu než Tabulka 12.3. Například výrazným rozdílem je, že v okruhu $(\mathbb{Z}_3[x]/\langle x^2-1\rangle, +, \cdot)$ existují dělitelé nuly. Například $(x+2)\cdot(x+1) = x^2+3x+2 = x^2-1 \equiv 0$. Faktorový okruh $(\mathbb{Z}_3[x]/\langle x^2-1\rangle, +, \cdot)$ proto není tělesem ani oborem integrity. ✓

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$	$\overline{x+2}$	$\overline{x}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{x+2}$	$\overline{x+2}$	$\overline{x}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2}$	$\overline{0}$	$\overline{1}$
$\overline{2x}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$
$\overline{2x+1}$	$\overline{2x+1}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{1}$	$\overline{2}$	$\overline{0}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{x}$
$\overline{2x+2}$	$\overline{2x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2}$	$\overline{0}$	$\overline{1}$	$\overline{x+2}$	$\overline{x}$	$\overline{x+1}$

Tabulka 12.4.: *Tabulka operace sčítání ve faktorovém okruhu* $(\mathbb{Z}_3[x]/\langle x^2-1\rangle, +, \cdot)$.

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{x}$	$\overline{x+1}$	$\overline{x+2}$	$\overline{2x}$	$\overline{2x+1}$	$\overline{2x+2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$	$\overline{2x}$	$\overline{2x+2}$	$\overline{2x+1}$	$\overline{x}$	$\overline{x+2}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{2x}$	$\overline{1}$	$\overline{x+1}$	$\overline{2x+1}$	$\overline{2}$	$\overline{x+2}$	$\overline{2x+2}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{0}$	$\overline{2x+2}$	$\overline{0}$	$\overline{x+1}$
$\overline{x+2}$	$\overline{0}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{2x+1}$	$\overline{0}$	$\overline{x+2}$	$\overline{x+2}$	$\overline{2x+1}$	$\overline{0}$
$\overline{2x}$	$\overline{0}$	$\overline{2x}$	$\overline{x}$	$\overline{2}$	$\overline{2x+2}$	$\overline{x+2}$	$\overline{1}$	$\overline{2x+1}$	$\overline{x+1}$
$\overline{2x+1}$	$\overline{0}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{x+2}$	$\overline{0}$	$\overline{2x+1}$	$\overline{2x+1}$	$\overline{x+2}$	$\overline{0}$
$\overline{2x+2}$	$\overline{0}$	$\overline{2x+2}$	$\overline{x+1}$	$\overline{2x+2}$	$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{0}$	$\overline{2x+2}$

Tabulka 12.5.: *Tabulka operace násobení ve faktorovém okruhu* $(\mathbb{Z}_3[x]/\langle x^2-1\rangle, +, \cdot)$.

Je zajímavé srovnat faktorové okruhy z Příkladů 12.15. a 12.16. Faktorový okruh $(\mathbb{Z}_3[x]/\langle x^2+1\rangle, +, \cdot)$ je oborem integrity, neboť je netriviální, komutativní a nemá dělitele nuly. Dokonce se podle Věty 11.6. jedná o těleso řádu 9. Naproti tomu ve faktorovém okruhu $(\mathbb{Z}_3[x]/\langle x^2-1\rangle, +, \cdot)$ existují dělitelé nuly a nejedná se ani o obor integrity.

Ireducibilní a reducibilní polynomy

Ve faktorovém okruhu budou dělitelé nuly vždy, pokud rozkládáme okruh polynomů podle polynomu $p(x)$, který je možno rozložit na dva nekonstantní polynomy $r(x) = a(x) \cdot b(x)$ V takovém případě jsou stupně polynomů $a(x)$, $b(x)$ menší než stupně polynomu $p(x)$, proto oba polynomy najdeme jako reprezentanty tříd $\overline{a(x)}$, $\overline{b(x)}$, a potom $\overline{a(x)} \cdot \overline{b(x)} = \overline{p(x)} = \overline{0}$.

Nyní je zřejmé, že budeme-li chtít sestavit obor integrity nebo dokonce konečné těleso pomocí faktorových okruhů okruhu polynomů, tak musíme rozkládat podle polynomů, které není možné rozložit.

Definice Mějme okruh polynomů $(R[x], +, \cdot)$ nad komutativním okruhem $(R, +, \cdot)$. Mějme nenulový polynom $p(x) \in R[x]$, který není jednotkou v $R[x]$. Řekneme, že $p(x)$ je polynom *ireducibilní* v $R[x]$, jestliže jej není možno napsat jako součin dvou polynomů, které nejsou jednotkou v $R[x]$. Naopak, polynom $p(x)$ je *reducibilní* v $R[x]$, jestliže existují takové polynomy $a(x), b(x) \in R[x]$, kde $a(x)$ ani $b(x)$ nejsou jednotkou v $R[x]$, že platí $p(x) = a(x) \cdot b(x)$.

Příklad 12.17. Uveďme několik příkladů reducibilních i ireducibilních polynomů.

1) Polynom x^2+1 je ireducibilní v $\mathbb{R}[x]$, a proto není ireducibilní ani v $\mathbb{Q}[x]$ ani v $\mathbb{Z}[x]$. Naproti tomu x^2+1 je reducibilní v $\mathbb{C}[x]$, neboť $x^2+1 = (x-i)(x+i)$.
2) Polynom x^2+1 je reducibilní také v $\mathbb{Z}_2[x]$, neboť $x^2+1 = x^2-1 = (x-1)(x+1) = (x+1)(x+1)$. Není reducibilní v $\mathbb{Z}_3[x]$ ani v $\mathbb{Z}_2[x]$, je však reducibilní v $\mathbb{Z}_5[x]$, neboť $(x+2)(x+3) = x^2+0x+1$.
3) Polynom $x^2-9 = (x-3)(x+3)$ je reducibilní v $\mathbb{C}[x]$, v $\mathbb{R}[x]$, v $\mathbb{Q}[x]$ i v $\mathbb{Z}[x]$ a je reducibilním polynomem také v $\mathbb{Z}_{10}[x]$. Kdybychom neměli úmluvu (Poznámka 3.3. na straně 73), že třídy $\mathbb{Z}_2$ můžeme značit libovolným reprezentantem, tak by polynom x^2-9 *nebyl* polynomem v $\mathbb{Z}_2[x]$, neboť $\overline{9} \notin \mathbb{Z}_2$. Na základě úmluvy však můžeme v $\mathbb{Z}_2[x]$ psát $x^2-9 = x^2-1 = (x-1)(x+1)$.
4) Polynom $x^2-\frac{1}{4}$ je reducibilní v $\mathbb{C}[x]$, v $\mathbb{R}[x]$ i v $\mathbb{Q}[x]$, neboť $x^2-\frac{1}{4} = \left(x+\frac{1}{2}\right)\left(x-\frac{1}{2}\right)$. Polynom $x^2-\frac{1}{4}$ však není polynomem v $\mathbb{Z}[x]$ ani v $\mathbb{Z}_n[x]$ a proto nemá smysl uvažovat, zda je reducibilní.
5) Polynom $x^2+\frac{1}{4}$ je reducibilní v $\mathbb{C}[x]$, neboť $x^2+\frac{1}{4} = \left(x+\frac{i}{2}\right)\left(x-\frac{i}{2}\right)$, a je ireducibilní v $\mathbb{R}[x]$ i v $\mathbb{Q}[x]$.
6) Polynom $4x^2-2 = (2x+\sqrt{2})(2x-\sqrt{2})$ je reducibilní v $\mathbb{R}[x]$ i v $\mathbb{C}[x]$ a není reducibilní v $\mathbb{Q}[x]$. Avšak v $\mathbb{Z}[x]$ polynom reducibilní je, neboť $4x^4-2 = 2(2x^2-1)$, přičemž v $\mathbb{Z}[x]$ polynom 2 *není* jednotkou, protože na rozdíl od okruhů $\mathbb{Q}[x]$, $\mathbb{R}[x]$ a $\mathbb{C}[x]$ nemá inverzi.
7) Polynom $p(x) = 10$ není reducibilní ani ireducibilní v $\mathbb{R}[x]$, neboť 10 je jednotkou v $\mathbb{R}[x]$ a definice se na něj nevztahuje. Avšak v $\mathbb{Z}[v]$ polynom $p(x) = 10$ reducibilní je, neboť $10 = 2 \cdot 5$ a ani jeden z polynomů $a(x) = 2$, $b(x) = 5$ není jednotkou v $\mathbb{Z}[x]$, neboť nemají inverzi.
8) Polynom $x^4+1 = (x^2+\sqrt{2}x+1)(x^2-\sqrt{2}x+1)$ je reducibilní v $\mathbb{R}[x]$ i v $\mathbb{C}[x]$ a je ireducibilní v $\mathbb{Q}[x]$a v $\mathbb{Z}[x]$. Naopak, v protože $x^4+1 = (x+1)(x+1)(x+1)(x+1)$ polynom reducibilní je, neboť $4x^4-2 = 2(2x^2-1)$, přičemž v $\mathbb{Z}[x]$ polynom 2 *není* jednotkou, protože na rozdíl od okruhů $\mathbb{Q}[x]$, $\mathbb{R}[x]$ a $\mathbb{C}[x]$ nemá inverzi.

Konečná tělesa můžeme sestavit jako faktorové okruhy podle hlavních ideálů $p(x)$ pouze pokud $p(x)$ je ireducibilní polynom (nelze je rozložit na součin). Pokud je $p(x)$ reducibilní, tak ve faktorovém okruhu určitě budou existovat dělitelé nuly a takový faktorový okruh nebude oborem integrity, ani tělesem.

Rozpoznání reducibilních a ireducibilních polynomů

V konečném faktorovém okruhu lze ireducibilitu polynomu ověřit hrubou silou. Pozor, nemusí stačit hledání lineárních faktorů dosazováním hodnot okruhu R, neboť reducibilní polynom nemusí mít lineární faktory. Například v okruhu $(\mathbb{R}[x], +, \cdot)$ polynom x^4+4 nemá žádné kořeny (ani lineární faktory) a přitom platí

$$x^4+4 = (x^2+2x+2)(x^2-2x+2).$$

Na druhou stranu je možno dokázat, pokud po dosazení prvku c z oboru integrity $(R, +, \cdot)$ za x do polynomu $p(x)$ dostaneme nulu (nulový prvek), tak existuje takový polynom $q(x) \in R[x]$, že $p(x) = (x-c)q(x)$.

Je možno ukázat, že všechna konečná tělesa se dají zkonstruovat jako faktorové okruhy okruhu polynomů podle *vhodných* hlavních ideálů. Důkaz tohoto tvrzení je však nad rámec kurzu.

Cvičení

12.4.1. Ukažte, že okruh polynomů se sudým absolutním členem z Příkladu 12.14. je ideálem okruhu polynomů s celočíselnými koeficienty $(\mathbb{Z}[x],+,\cdot)$.

12.4.2. Ukažte, že okruh polynomů se sudým absolutním členem z Příkladu 12.14. není hlavním ideálem okruhu $(\mathbb{Z}[x],+,\cdot)$.

12.4.3. Ukažte, že $\langle x^2+x+2\rangle$ *je ideál okruhu* $(\mathbb{Z}_3[x],+,\cdot)$.

12.4.4. Ukažte, že $\langle x^2+x+2\rangle$ *je ideál v okruhu* $(\mathbb{Z}_3[x],+,\cdot)$ *bez využití Důsledku 12.10.*

12.4.5. Dokažte Důsledek 12.10. bez použití Věty 12.9.

12.4.6. Ukažte, že $\langle x^2-1\rangle$ *je ideál okruhu* $(\mathbb{Z}_3[x],+,\cdot)$.

12.4.7. Ukažte, že $\langle x^2+1\rangle$ *je ideál okruhu* $(\mathbb{Z}_3[x],+,\cdot)$.

12.4.8. Ukažte, že $\langle x^2+1\rangle$ *je ideál okruhu* $(\mathbb{Z}_2[x],+,\cdot)$.

12.4.9. Ukažte, že $\langle x^2+x+1\rangle$ *je ideál okruhu* $(\mathbb{Z}_2[x],+,\cdot)$.

12.4.10. Popište faktorový okruh $(\mathbb{Z}_3[x]/\langle x^2+x+2\rangle,+,\cdot)$. *Sestavte tabulky operací v tomto okruhu.*

12.4.11. Ukažte, že faktorový okruh $(\mathbb{Z}_3[x]/\langle x^2+x+2\rangle,+,\cdot)$ *ze Cvičení 12.4.10. je obor integrity.*

12.4.12. Ukažte, že faktorový okruh $(\mathbb{Z}_3[x]/\langle x^2+x+2\rangle,+,\cdot)$ *ze Cvičení 12.4.10. je těleso.*

12.4.13. Ověřte, zda faktorový okruh $(\mathbb{Z}_3[x]/\langle 2x^2+1\rangle,+,\cdot)$ *je těleso.*

12.4.14. Ukažte, že faktorový okruh $(\mathbb{Z}_2[x]/\langle x^2+1\rangle,+,\cdot)$ *není obor integrity ani těleso.*

12.4.15. Co by se změnilo, pokud bychom v tabulce násobení faktorového okruhu $(\mathbb{Z}_2[x]/\langle x^2+1\rangle,+,\cdot)$ *z Příkladu 12.4.14. nulu v řádku* $\overline{x+1}$ *a ve sloupci* $\overline{x+1}$ *nahradili jedničkou? Jednalo by se o obor integrity?*

12.4.16. Určete, zda faktorový okruh $(\mathbb{Z}_2[x]/\langle x^2+x+1\rangle,+,\cdot)$ *je těleso.*

12.4.17. Určete, zda faktorový okruh $(\mathbb{Z}_3[x]/\langle x^2+2\rangle,+,\cdot)$ *je těleso.*

12.4.18. Sestavte těleso řádu 8.

Kapitola 13. Homomorfismy okruhů

Homomorfismus okruhů je pojem analogický pojmu homomorfismu grup, kterému jsme se věnovali v Kapitole 8. jedná se o takové zobrazení, které „zachová“ obě operace, tj. obraz součtu je součtem obrazů a navíc obraz součinu je součinen obrazů.

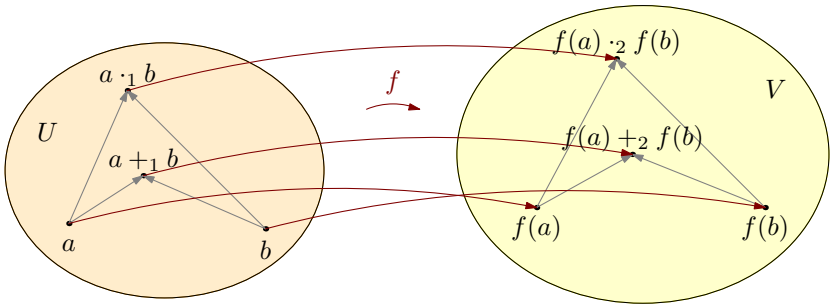
13.1. Homomorfismus okruhů

Existence homomorfismu dvou okruhů říká, že jeden okruh je jako struktura se dvěma operacemi součástí jiného okruhu. Nemusí se jednat přímo o podokruh, ale v druhém okruhu najdeme podokruh s podobnou strukturou. Podobnost chápeme jako „pohled z dálky“, kdy přehlédneme některé detaily.

Definice Mějme okruhy $(U, +_1, \cdot_1)$ a $(V, +_2, \cdot_2)$. *Homomorfismem okruhu* $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$ rozumíme takové zobrazení $f : U \to V$, které zachová obě okruhové operace, tj. že pro každé $x, y \in U$ platí

(i) $f(x +_1 y) = f(x) +_2 f(y)$,
(ii) $f(x \cdot_1 y) = f(x) \cdot_2 f(y)$.

Říkáme, že $(U, +_1, \cdot_1)$ je *první* okruh a $(V, +_2, \cdot_2)$ je *druhý* okruh homomorfismu f. Jestliže je jasné, který okruh je první a který druhý, tak říkáme, f je homomorfismus okruhů $(U, +_1, \cdot_1)$ a $(V, +_2, \cdot_2)$.



Obrázek 13.1.: *Homomorfismus f okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$ zachovává obě operace.*

Příklad 13.1. Uveďme několik jednoduchých příkladů homomorfismů okruhů.

1) Zobrazení $f : \mathbb{Z} \to \mathbb{Q}$, kde pro každé $n \in \mathbb{Z}$ platí $f(n) = n$, je homomorfismus okruhů $(\mathbb{Z}, +, \cdot)$ a $(\mathbb{Q}, +, \cdot)$.
2) Zobrazení $f : \mathbb{Z} \to \mathbb{Z}_n$, ve kterém pro každé $a \in \mathbb{Z}$ položíme $f(a) = \overline{a}_n$ (nebo s využitím úmluvy na straně 73, že třídy $\mathbb{Z}_n$ můžeme značit libovolným reprezentantem můžeme psát $f(a) = r$, kde r je zbytek po dělení čísla a číslem n), je homomorfismus okruhů $(\mathbb{Z}, +, \cdot)$ a $(\mathbb{Z}_n, +, \cdot)$. Tomuto homomorfismu se říká *přirozený homomorfismus $\mathbb{Z}$ do $\mathbb{Z}_n$*.
3) Zobrazení $f : \mathbb{C} \to \mathbb{C}$, kde pro každé $z \in \mathbb{C}$ položíme $f(z) = \overline{z}$, kde $\overline{z}$ je číslo komplexně sdružené, je homomorfismus okruhu $(\mathbb{C}, +, \cdot)$ do sebe.
4) Zobrazení $f : \mathbb{R}[x] \to \mathbb{R}$ dané předpisem $f(p(x)) = p(1)$ (polynomu přiřadíme jeho funkční hodnotu v bodě 1) je homomorfismus okruhů $(\mathbb{R}[x], +, \cdot)$ a $(\mathbb{R}, +, \cdot)$ (Cvičení 13.1.2.).
5) Mějme libovolný okruh $(U, +, \cdot)$ a libovolný okruh $(V, +, \cdot)$ s nulou 0_V. Zobrazení $f : U \to V$ dané předpisem $f(x) = 0_V$ je *nulový homomorfismus*.
6) Zobrazení $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ definované přepisem

$$f(a) = \begin{cases} \overline{0} & \text{pro } a = \overline{0}, \overline{2}, \overline{4} \\ \overline{3} & \text{pro } a = \overline{1}, \overline{3}, \overline{5} \end{cases}$$

je homomorfismem okruhů $(\mathbb{Z}_6, +, \cdot)$ a $(\mathbb{Z}_6, +, \cdot)$. Ověření je ponecháno jako Cvičení 13.1.3.

Příklad 13.2. Uveďme několik jednoduchých příkladů, kdy zobrazení není homomorfismem okruhů.

1) Zobrazení $f : \mathbb{Z} \to \mathbb{Z}$ dané předpisem $f(n) = -n$ pro každé $n \in \mathbb{Z}$ není okruhovým homomorfismem, protože nezachovává operaci „$\cdot$“. Například $f(-1) \cdot f(-1) = 1$, avšak $f((-1) \cdot (-1)) = f(1) = -1$.

2) Mějme zobrazení $f : \mathbb{Z} \to \mathbb{N}_0$, kde pro každé $n \in \mathbb{Z}$ platí $f(n) = |n|$. Zobrazení f není homomorfismus okruhů, neboť nezachovává operaci „+“. Například $f(1)+f(-1) = 1+1 = 2$, avšak $f(1-1) = f(0) = 0$.
3) Zobrazení $f : \mathbb{Z}_n \to \mathbb{Z}$, ve kterém pro každou třídu $\overline{a} \in \mathbb{Z}_n$ položíme $f(\overline{a}) = a$ není homomorfismus okruhů $(\mathbb{Z}_n, +, \cdot)$ a $(\mathbb{Z}, +, \cdot)$. Zobrazení nezachovává operace, například $\overline{n-1} + \overline{n-1} = \overline{n-2}$, avšak $(n-1) + (n-1) = 2n - 2 \neq n - 2$. Podobně $\overline{2} \cdot \overline{n-1} = \overline{n-2}$, avšak $2 \cdot (n-1) = 2n - 2 \neq n - 2$.
4) Mějme přirozené číslo k, $k \neq 1$. Zobrazení $f : \mathbb{Z} \to \mathbb{Q}$, kde pro každé $n \in \mathbb{Z}$ platí $f(n) = kn$ není homomorfismem okruh, neboť $f(a) \cdot f(b) = k^2ab$, avšak $f(a \cdot b) = kab$.
5) Zobrazení $f : M_{2,2}(\mathbb{Z}) \to \mathbb{Z}$ dané předpisem $f(A) = \det(A)$, kde $A \in M_{2,2}(\mathbb{Z})$, není homomorfismus okruhů, neboť $\det(A) + \det(-A) = 2\det(A)$, avšak $\det(A - A) = 0$, což pro regulární matici A není $2\det(A)$.

Otázka: Je zobrazení $f : M_{3,3}(\mathbb{Z}) \to \mathbb{Z}$ dané předpisem $f(A) = \det(A)$, kde $A \in M_{3,3}(\mathbb{Z})$, homomorfismus okruhů?

Poznámka 13.1. Všimněte si, že podle definice homomorfismu okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$ platí rovnost (i), což znamená, že homomorfismus okruhů f je současně homomorfismem grupy $(U, +_1)$ do grupy $(V, +_2)$.

Otázka: Mějme homomorfismus okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$. Podle definice platí také rovnost (ii). Znamená to, že homomorfismus okruhů f je současně homomorfismem grupy $(U, \cdot_1)$ do grupy $(V, \cdot_2)$.

Vlastnosti homomorfismů okruhů

V Kapitole 8. jsme při zkoumání homomorfismu grup ukázali, že obrazem neutrálního prvku grupy je vždy neutrální prvek a obrazem inverzního prvku grupy je inverze obrazu. Analogická tvrzení platí i pro homomorfismy okruhů.

Věta 13.1. Vlastnosti okruhových homomorfismů
Mějme okruh $(U, +_1, \cdot_1)$ s nulou 0_U a okruh $(V, +_2, \cdot_2)$ s nulou 0_V. Jestliže zobrazení $f : U \to V$ je homomorfismus okruhů, pak

(i) $f(0_U) = 0_V$,
(ii) pro každé $x \in U$ platí $f(-x) = -f(x)$.
Jestliže $(U, +_1, \cdot_1)$ a $(V, +_2, \cdot_2)$ jsou navíc tělesa, 1_U je jednička v $(U, +_1, \cdot_1)$, 1_V je jednička v $(V, +_2, \cdot_2)$ a 1_V je obrazem některého prvku z U, pak
(iii) $f(1_U) = 1_V$,
(iv) pro každé $x \in U$, $x \neq 0_U$ platí $f(x^{-1}) = (f(x))^{-1}$.

Důkaz. Ukážeme platnost jednotlivých tvrzení s využitím známých vlastností homomorfismu grup.

(i) Podle Poznámky 13.1. víme, že homomorfismu okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$ je současně homomorfismem grupy $(U, +_1)$ do grupy $(V, +_2)$. Podle Věty 8.1. platí, že neutrální prvek první grupy se zobrazí na neutrální prvek druhé grupy, tj. platí $f(0_U) = 0_V$,
(ii) Podobně jako v důkazu předchozí části využijeme, že f je současně homomorfismem grupy $(U, +_1)$ do grupy $(V, +_2)$. Podle Věty 8.2. platí, že inverze prvku v první grupě se zobrazí na inverzi obrazu v druhé grupě, tj. platí $f(-x) = -f(x)$.
(iii) Jestliže $(U, +_1, \cdot_1)$ a $(V, +_2, \cdot_2)$ jsou tělesa a 1_V je obrazem některého prvku z U, pak z rovnosti (ii) plyne, že homomorfismus okruhů f je současně homomorfismem grup $(U \setminus \{0_U\}, \cdot_1)$ a $(V \setminus \{0_V\}, \cdot_2)$, přičemž množina $V \setminus \{0_V\}$ není prázdná a obsahuje neutrální prvek 1_V. Potom podle Věty 8.1. se neutrální prvek 1_U grupy $(U \setminus \{0_U\}, \cdot_1)$ zobrazí na neutrální prvek 1_V grupy $(V \setminus \{0_V\}, \cdot_2)$, tj. platí $f(1_U) = 1_V$.
(iv) Podobně jako v důkazu předchozí části využijeme, že f je současně homomorfismem grupy $(U \setminus \{0_U\}, \cdot_1)$ na grupu $(V \setminus \{0_V\}, \cdot_2)$. Podle Věty 8.2. platí, že inverze prvku x v první grupě se zobrazí na inverzi obrazu v druhé grupě, tj. platí $f(x^{-1}) = (f(x))^{-1}$.

Ukázali jsme všechna tvrzení a důkaz je ukončen. □

Otázka: Proč ve Větě 13.1. požadujeme u bodů (iii) a (iv) existenci obrazu jedničky 1_V?

Příklad 13.3. Mějme okruh $(\mathbb{Z}, +, \cdot)$. Definujeme zobrazení $f : \mathbb{Z} \to \mathbb{Z}$ předpisem $f(z) = z^2$ pro každé $z \in \mathbb{Z}$. Ukážeme, že se nejedná o homomorfismus.
Stačí si všimnout, že je porušena vlastnost (ii) Věty 13.1. Platí $f(-1) = (-1)^2 = 1$ a nikoliv $f(-1) = -1$. To současně znamená, že zobrazení nezachová některou operaci, případně obě operace. Například $f(2+3) = f(5) = 25$, avšak $f(2) + (3) = 4 + 9 = 13$. ✓

Příklad 13.4. Mějme zobrazení f okruhu $(\mathbb{Z}, +, \cdot)$ do okruhu $(\mathbb{S}, +, \cdot)$ definované předpisem $f(z) = 2z$ pro každé $z \in \mathbb{Z}$. Ukážeme, že se nejedná o homomorfismus.
Zobrazení f *nezachová* operaci násobení. Například $f(2 \cdot 3) = f(6) = 12$, avšak $f(2) \cdot (3) = 4 \cdot 6 = 24$. ✓

Příklad 13.5. Mějme zobrazení f okruhu $(\mathbb{Z}_4, +, \cdot)$ do okruhu $(\mathbb{Z}_6, +, \cdot)$ definované předpisem $f(\overline{x}_4) = \overline{3x}_6$ pro každé $\overline{x}_4 \in \mathbb{Z}_4$. Ukážeme, že f je homomorfismus.
Mějme $a, b \in \mathbb{Z}_4$. Nejprve si uvědomme, že nestačí vycházet z rovnosti $f(a+b) = 3(a+b) = 3a + 3b$, neboť sčítání v prvním okruhu se děje modulo 4, zatímco sčítání v druhém okruhu se děje modulo 6.

Přímo ověříme zachování obou operací. S využitím Věty 0.2. označme $a + b = 4q_1 + r_1$, kde $0 \leq r_1 < 4$. Potom platí $f(a+b) = f(r_1) = 3r_1 = 3(a+b-4q_1) = 3a + 3b - 12q_1 = 3a + 3b = f(a) + f(b)$ a zobrazení f zachovává sčítání.

Podobně označme $a \cdot b = 4q_2 + r_2$, kde $0 \leq r_2 < 4$. Potom platí $f(a+b) = f(r_2) = 3r_2 = 3(a \cdot b - 4q_2) = 3a \cdot b - 12q_2 = 3a \cdot b$. A protože v $\mathbb{Z}_6$ platí $3 \cdot 3 = 9 = 3$, tak s využitím komutativity můžeme psát $3a \cdot b = 3 \cdot 3a \cdot b = (3 \cdot 3a) \cdot (3 \cdot b) = f(a) \cdot f(b)$ a zobrazení f zachovává i násobení. Zobrazení f je homomorfismus okruhu $(\mathbb{Z}_4, +, \cdot)$ do okruhu $(\mathbb{Z}_6, +, \cdot)$. ✓

Příklad 13.6. Ukážeme, že zobrazení f okruhu $(\mathbb{Z}_4, +, \cdot)$ do okruhu $(\mathbb{Z}_6, +, \cdot)$ dané předpisem $f(\overline{x}_4) = \overline{2x}_6$ pro každé $\overline{x}_4 \in \mathbb{Z}_4$ není homomorfismus.
Ukážeme, že takto definované zobrazení nezachovává operaci „$\cdot$“. Pokud například $a = \overline{3}$, $b = \overline{2}$, tak $f(\overline{3}+\overline{2}) = f(\overline{1}) = 2 \cdot \overline{1} = \overline{2}$ v okruhu $(\mathbb{Z}_6, +, \cdot)$. Avšak $f(\overline{3}) + f(\overline{2}) = 2 \cdot \overline{3} + 2 \cdot \overline{2} = \overline{0} + \overline{4} = \overline{4}$ v okruhu $(\mathbb{Z}_6, +, \cdot)$.

Obecně mějme $a, b \in \mathbb{Z}_4$. S využitím Věty 0.2. označme $a + b = 4q_1 + r_1$, kde $0 \leq r_1 < 4$. Potom platí $f(a+b) = f(r_1) = 2r_1 = 2(a+b-4q_1) = 2a + 2b - 8q_1 = 2a + 2b - 2q_1$ v okruhu $(\mathbb{Z}_6, +, \cdot)$. Obecně nemusí platit $f(a) + f(b) = 2a + 2b = 2a + 2b - 2q_1$. ✓

Obraz okruhu je podokruh

V Kapitole 8. jsme ukázali, že množina obrazů homomorfismu grup tvoří spolu s restrikcí operace podgrupu druhé grupy. Analogické tvrzení platí i pro homomorfismus okruhů.

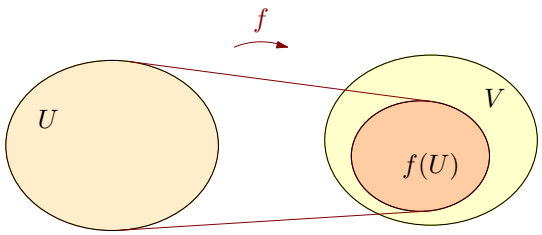
Věta 13.2. *Mějme homomorfismus $f : U \to V$ okruhů $(U, +_1, \cdot_1)$ a $(V, +_2, \cdot_2)$. Pak $(f(U), +_3, \cdot_3)$ je podokruh okruhu $(V, +_2, \cdot_2)$, kde „$+_3$“ je restrikce operace „$+_2$“ na množinu $f(U)$ a „$\cdot_3$“ je restrikce „$\cdot_2$“ na množinu $f(U)$.*

Důkaz. Abychom ukázali, že $(f(U), +_3, \cdot_3)$ je podokruhem okruhu $(V, +_2, \cdot_2)$, tak ověříme předpoklady Věty 11.2. Nejprve si všimneme, že množina $f(U)$ je jistě neprázdná, neboť $f(0_U) = 0_V$ a proto $0_V \in f(U)$. Jistě platí $f(U) \subseteq V$, neboť $f(U)$ je množina prvků z V.

Dále pro každé $f(a), f(b) \in f(U)$ platí $f(a) +_2 (-f(b)) = f(a) +_2 f(-b) = f(a-b)$. Proto pro každé $f(a), f(b) \in f(U)$ platí $f(a) +_3 f(b) = f(a) +_2 f(b) \in f(U)$. A konečně pro každé $f(a), f(b) \in f(U)$ platí $f(a) \cdot_2 f(b) = f(a \cdot_1 b)$. Proto pro každé $a, b \in f(U)$ platí $f(a) \cdot_3 f(b) = f(a) \cdot_2 f(b) \in f(U)$ a operace je uzavřená.

Celkem dostáváme, že $(f(U), +_3, \cdot_3)$ je podokruh okruhu $(V, +_2, \cdot_2)$. □

Připomeňme, že asociativita a distributivita operací okruhu se v podokruhu automaticky „zdědí“, což je ukázáno ve Cvičeních 0.6.6. a 0.6.7.



Obrázek 13.2.: *Podokruh $(f(U), +_3, \cdot_3)$ okruhu $(V, +_2, \cdot_2)$.*

Speciální případy homomorfismů
Jestliže homomorfismus okruhů má nějaké další vlastnosti, zavádíme pro ně pojmenování.

Definice Mějme homomorfismus f okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$. Homomorfismus f je *injektivní homomorfismus* právě tehdy, když pro každé $a, b \in f(U)$ platí implikace $f(a) = f(b) \Rightarrow a = b$. Injektivní homomorfismus nazveme *monomorfismem* okruhů.

Homomorfismus f je *surjektivní homomorfismus* právě tehdy, když pro každé $y \in V$ existuje $x \in U$ takové, že $f(x) = y$. Surjektivní homomorfismus nazveme *epimorfismem okruhů*.

Bijektivní homomorfismus $f : U \to V$ nazveme *izomorfismem okruhů* $(U, +_1, \cdot_1)$ a $(V, +_2, \cdot_2)$. Bijektivní homomorfismus $f : U \to U$ nazveme *automorfismem okruhu* $(U, +, \cdot)$.

Příklad 13.7. Rozebereme několik jednoduchých příkladů homomorfismů okruhů.

1) Zobrazení $f : \mathbb{Z} \to \mathbb{Q}$, kde pro každé $n \in \mathbb{Z}$ platí $f(n) = n$, je monomorfismus okruhů, f však není epimorfismus okruhů.
2) Zobrazení $f : \mathbb{Z} \to \mathbb{Z}_n$, ve kterém pro každé $a \in \mathbb{Z}$ položíme $f(a) = \overline{a}_n = \overline{r}$, kde r je zbytek po dělení čísla a číslem n, je epimorfismus okruhů, avšak ne monomorfismus.
3) Zobrazení $f : \mathbb{C} \to \mathbb{C}$, kde pro každé $z \in \mathbb{C}$ položíme $f(z) = \overline{z}$, kde $\overline{z}$ je číslo komplexně sdružené, je isomorfismus okruhů, který je současně automorfismem.
4) Zobrazení $f : \mathbb{R}[x] \to \mathbb{R}$ dané předpisem $f(p(x)) = p(1)$ (polynomu přiřadíme jeho funkční hodnoty v bodě 1) je epimorfismus okruhů, f však není monomorfismus.
5) Nulový homomorfismus okruhu $(U, +, \cdot)$ do okruhu $(V, +, \cdot)$ je epimorfismus pouze v případě, že V je jednoprvková množina a monomorfismus pouze v případě, že U je jednoprvková množina.
6) Homomorfismus $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ z Příkladu 13.1. není ani monomorfismus ani epimorfismus ani ismorfismus.

Cvičení

13.1.1. Ukažte, že zobrazení $f : \mathbb{Z} \to \mathbb{Z}_n$, ve kterém pro každé $a \in \mathbb{Z}$ položíme $f(a) = \overline{r}$, kde r je zbytek po dělení čísla a číslem n, je homomorfismus.

13.1.2. Ukažte, že zobrazení $f : \mathbb{R}[x] \to \mathbb{R}$ dané předpisem $f(p(x)) = p(1)$ (polynomu přiřadíme jeho funkční hodnoty v bodě 1) je homomorfismus okruhů.

13.1.3. Ukažte, že zobrazení $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ dané předpisem $f(\overline{a}) = \overline{3a \bmod 6}$ (třídě $\overline{a}$ přiřadíme zbytkovou třídu určenou reprezentantem „zbytek po dělení čísla $3a$ číslem 6“) je homomorfismem okruhů $(\mathbb{Z}_6, +, \cdot)$ a $(\mathbb{Z}_6, +, \cdot)$.

13.1.4. Mějme libovolný okruh $(R, +, \cdot)$ s jedničkou 1. Ukažte, že zobrazení $f : \mathbb{Z} \to R$ definované předpisem $f(n) = n1$ (součet n kopií jedničky 1) pro každé $n \in \mathbb{Z}$ je homomorfizmus okruhu $(\mathbb{Z}, +, \cdot)$ do okruhu $(R, +, \cdot)$.

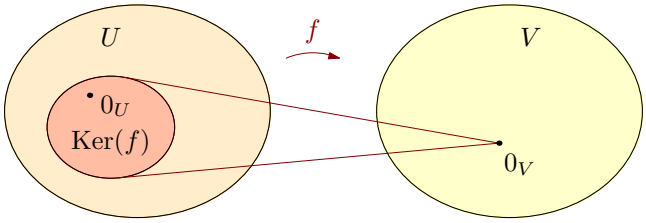
13.1.5. Najděte nějaký homomorfismus okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$, pro který neplatí vlastnosti bodů (iii) a (iv) ve Větě 13.1.

13.1.6. Dokažte nebo vyvraťte. Zobrazení $f : \mathbb{R}[x] \to \mathbb{R}[x]$ definované pro každý polynom $p(x)$ předpisem $f(p(x)) = p'(x)$ (polynomu přiřadíme jeho derivaci) je homomorfismus okruhu $(\mathbb{R}[x], +, \cdot)$ do okruhu $(\mathbb{R}[x], +, \cdot)$.

13.2. Jádro homomorfismu

V Kapitole 8. jsme zavedli jádro homomorfismu grup a ukázali, že se jedná o normální podgrupu první grupy homomorfismu. Nyní zavedeme analogický pojem pro homomorfismus okruhů.

Definice Mějme homomorfismus $f : U \to V$ okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$ s nulou 0_V. *Jádrem homomorfismu* f je množina $\mathrm{Ker}(f) = \{x \in U : f(x) = 0_V\}$.



Obrázek 13.3.: *Jádro homomorfismu okruhů* $(U, +_1, \cdot_1)$ *do okruhu* $(V, +_2, \cdot_2)$.

Příklad 13.8. Rozebereme několik jednoduchých příkladů homomorfismů okruhů.

1) Homomorfismus $f : \mathbb{Z} \to \mathbb{Q}$, kde pro každé $n \in \mathbb{Z}$ platí $f(n) = n$, má jádro $\mathrm{Ker}(f) = \{0\}$.
2) Homomorfismus $f : \mathbb{Z} \to \mathbb{Z}_n$, ve kterém pro každé $a \in \mathbb{Z}$ položíme $f(a) = \overline{a}_n = \overline{r}$, kde r je zbytek po dělení čísla a číslem n, má jádro $\mathrm{Ker}(f) = \{kn : k \in \mathbb{Z}\}$.
3) Isomorfismus $f : \mathbb{C} \to \mathbb{C}$, kde pro každé $z \in \mathbb{C}$ položíme $f(z) = \overline{z}$, má jádro $\mathrm{Ker}(f) = \{0\}$.
4) Jádrem homomorfismu $f : \mathbb{R}[x] \to \mathbb{R}$ dané předpisem $f(p(x)) = p(1)$ (polynomu přiřadíme jeho funkční hodnoty v bodě 1) je množina všech polynomů s reálnými koeficienty, jejichž graf prochází počátkem.
5) Nulový homomorfismus f okruhu $(U, +, \cdot)$ do okruhu $(V, +, \cdot)$ má jádro $\mathrm{Ker}(f) = U$.
6) Homomorfismus $f : \mathbb{Z}_6 \to \mathbb{Z}_6$ z Příkladu 13.1. má jádro $\mathrm{Ker}(f) = \{\overline{0}, \overline{2}, \overline{4}\}$.

Poznámka 13.2. Mějme homomorfismus $f : U \to V$ okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$. Už víme, že f je také homomorfismem grupy $(U, +_1)$ do grupy $(V, +_2)$, a proto je jádro homomorfismu okruhů současně jádrem homomorfismu grupy $(U, +_1)$ do grupy $(V, +_2)$.

Věta 13.3. *Mějme homomorfismus $f : U \to V$ okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$. Pak $(\mathrm{Ker}(f), +_3, \cdot_3)$ je (oboustranný) ideál okruhu $(U, +_1, \cdot_1)$, kde operace „$+_3$“ je restrikce operace „$+_1$“ na množinu $\mathrm{Ker}(f)$ a operace „$\cdot_3$“ je restrikce operace „$\cdot_1$“ na množinu $\mathrm{Ker}(f)$.*

Důkaz. Množina $\mathrm{Ker}(f)$ je jistě neprázdná, neboť podle Věty 13.1. jádro vždy obsahuje neutrální prvek okruhu $(U, +_1, \cdot_1)$.

Operace „$+_3$“ je uzavřená na $\mathrm{Ker}(f)$, protože podle definice homomorfismu a Věty 13.1. pro každé $a, b \in \mathrm{Ker}(f)$ platí $f(a - b) = f(a) +_2 f(-b) = f(a) - f(b) = 0_V - 0_V = 0_V$.

Jádro v součinu absorbuje prvky celého okruhu $(U, +_1, \cdot_1)$, protože pro každé $r \in U$ a každé $i \in \mathrm{Ker}(f)$ platí $f(r \cdot_1 i) = f(r) \cdot_2 f(i) = f(r) \cdot_2 0_V = 0_V$, tedy $r \cdot_1 i \in \mathrm{Ker}(f)$. Podobně pro každé $r \in U$ a každé $i \in \mathrm{Ker}(f)$ platí $f(i \cdot_1 r) = f(i) \cdot_2 f(r) = 0_V \cdot_2 f(r) = 0_V$, tedy také $i \cdot_1 r \in \mathrm{Ker}(f)$.

Podle Věty 12.1. dostáváme, že $\mathrm{Ker}(f)$ je ideál v okruhu $(U, +_1, \cdot_1)$. □

Už víme, že homomorfismus okruhů je současně homomorfismus grup (vzhledem k první operaci) a proto ihned dostáváme následující tvrzení.

Důsledek 13.4. *Mějme homomorfismus $f : U \to V$ okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$. Potom grupa $(\mathrm{Ker}(f), +_3)$ je normální podgrupa grupy $(U, +_1)$, kde „$+_3$“ je restrikce operace „$+_1$“ na množinu $\mathrm{Ker}(f)$.*

Důkaz plyne ihned z předchozí věty a Věty 12.4. z předchozí kapitoly.

Cvičení

13.2.1.$^{\heartsuit}$ *Dokažte, že jádro nulového homomorfismu $f : U \to V$ okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$ je celá množina U.*

13.2.2. Mějme okruhový homomorfismus f okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$. Ukažte, že $\mathrm{Ker}(f) = U$ právě tehdy, když f je nulový homomorfismus.

13.2.3. Mějme homomorfismus okruhu $(\mathbb{Z}[x], +, \cdot)$ do okruhu $(\mathbb{Z}, +, \cdot)$ daný pro každý $p(x) \in \mathbb{Z}[x]$ předpisem $f(x) = p(0)$. Ukažte, že jádro tohoto homomorfismu je $\mathrm{Ker}(f) = \langle x \rangle$.

13.3. Faktorový okruh podle jádra

Protože jádro $\mathrm{Ker}(f)$ tvoří ideál okruhu $(U, +_1, \cdot_1)$ nějakého homomorfismu $f : U \to V$, tak přirozeně můžeme sestavit faktorový okruh okruhu $(U, +_1, \cdot_1)$ podle jádra $\mathrm{Ker}(f)$.

Věta 13.5. *Mějme homomorfismus $f : U \to V$ okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$. Pak $(U/\mathrm{Ker}(f), +, \cdot)$ je okruh, kde „$+$“ je sčítání komplexů a „$\cdot$“ je násobení komplexů.*

Důkaz. Protože $\mathrm{Ker}(f)$ je podle Věty 13.3. ideál okruhu $(U, +_1, \cdot_1)$, tak $(U/\mathrm{Ker}(f), +, \cdot)$ je podle Věty 12.5. faktorový okruh. □

Příklad 13.9. Uveďme několik jednoduchých příkladů homomorfismů okruhů.

1) Jádrem homomorfismu $f : \mathbb{Z} \to \mathbb{Z}_n$, ve kterém pro každé $a \in \mathbb{Z}$ položíme $f(a) = \overline{a}_n$, je $\mathrm{Ker}(f) = \{kn : k \in \mathbb{Z}\}$, přičemž $\overline{a}_n = \overline{r}_n$, kde r je zbytek po dělení čísla a číslem n. Faktorový okruh $(\mathbb{Z}/\mathrm{Ker}(f), +, \cdot)$ je okruh, jehož třídy jsou $\overline{0}$, $\overline{1}$, $\ldots \overline{n-1}$.
2) Jádrem nulového homomorfismu $f : U \to V$ okruh $(U, +, \cdot)$ do okruhu $(V, +, \cdot)$ s nulou 0_V daného předpisem $f(x) = 0_V$ je celá množina U, a proto je faktorový okruh $(U/U, +, \cdot)$ triviální.

Příklad 13.10. Mějme homomorfismus f okruhu $(\mathbb{Z}[x], +, \cdot)$ do okruhu $(\mathbb{Z}, +, \cdot)$ daný pro každý $p(x) \in \mathbb{Z}[x]$ předpisem $f(p(x)) = p(0)$. Jádro homomorfismu f je $\mathrm{Ker}(f) = \langle x \rangle$ (Cvičení 13.2.3.). Sestavíme faktorový okruh $(\mathbb{Z}[x]/\langle x \rangle, +, \cdot)$.
Jádro homomorfismu f je obsahuje všechny polynomy s nulovým absolutním členem. Nula faktorového okruhu $(\mathbb{Z}[x]/\langle x \rangle, +, \cdot)$ proto obsahuje právě polynomy $\mathrm{Ker}(f) = \langle x \rangle$. Další třídy $\overline{z}$ obsahují polynomy, jejichž funkční hodnota v nule je z. Platí $\mathbb{Z}[x]/\langle x \rangle = z + \langle x \rangle$. Pro dva prvky a, b faktorového okruhu platí $(a + \overline{x}) + (b + \overline{x}) = (a + b) + \overline{x}$ a $(a + \overline{x}) \cdot (b + \overline{x}) = (a \cdot b) + \overline{x}$, proto se s třídami počítá stejně jako s celými čísly $\mathbb{Z}$. Každá třída však obsahuje nekonečně mnoho polynomů. ✓

Hlavní věta o homomorfismu okruhů

Následující důsledek je jen přeformulováním Věty 12.4. pro případ, kdy za ideál vezmeme jádro homomorfismu.

Důsledek 13.6. *Mějme homomorfismus $f : U \to V$ okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$. Potom grupa $(U/\mathrm{Ker}(f), +)$ je komutativní grupa, kde „$+$“ je sčítání komplexů.*

Nyní máme všechny nástroje k dispozici a takové faktorové okruhy budeme sestavovat. Máme-li nějaký homomorfismus okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$, tak navíc ukážeme vztah mezi faktorovým okruhem prvního okruhu a podokruhem druhého okruhu.

Věta 13.7. Hlavní věta o homomorfismu okruhů
Mějme homomorfismus $f : U \to V$ okruhu $(U, +_1, \cdot_1)$ do okruhu $(V, +_2, \cdot_2)$. Potom zobrazení $i : U/\mathrm{Ker}(f) \to f(U)$ takové, že

$$\forall a \in U : i(a +_1 \mathrm{Ker}(f)) = f(a)$$

je homomorfismus okruhů $(U/\mathrm{Ker}(f), +, \cdot)$ a $(V, +_2, \cdot_2)$. A dále zobrazení $i : U/\mathrm{Ker}(f) \to f(U)$ je izomorfismus okruhů $(U/\mathrm{Ker}(f), +, \cdot)$ a $(f(U), +_3, \cdot_3)$, kde „$+_3$“ je restrikce operace „$+_2$“ na množinu $f(U)$ a „$\cdot_3$“ je restrikce operace „$\cdot_2$“ na množinu $f(U)$.

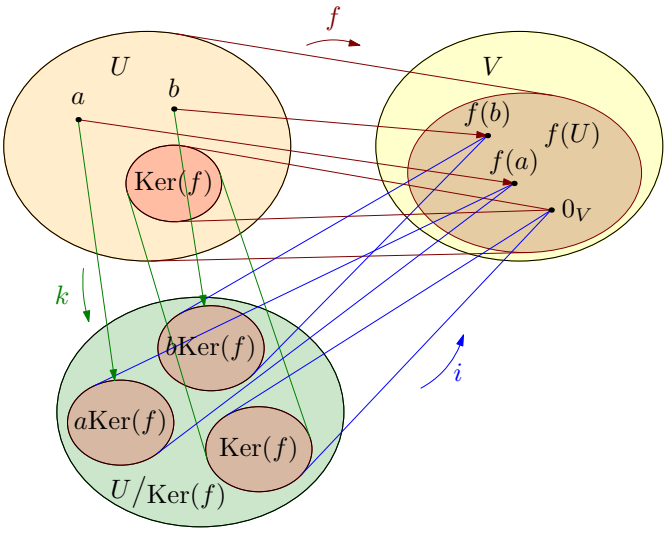
Důkaz. Protože zobrazení f je homomorfismus, tak podle Věty 13.2. víme $(f(U), +_2, \cdot_2)$ je podokruh okruhu $(V, +_2, \cdot_2)$ Dále podle Věty 13.3. víme, že $\mathrm{Ker}(f)$ je (oboustranný) ideál okruhu $(U/\mathrm{Ker}(f), +, \cdot)$.

(i) Pro každé $a, b \in U$ vezmeme třídy $a + \mathrm{Ker}(f)$, $b + \mathrm{Ker}(f)$ a platí $i((a + \mathrm{Ker}(f)) + (b + \mathrm{Ker}(f))) = i((a + b) + \mathrm{Ker}(f)) = f(a + b) = f(a) +_2 f(b) = i(a + \mathrm{Ker}(f)) +_2 i(b + \mathrm{Ker}(f))$. To znamená, že obraz součtu tříd $U/\mathrm{Ker}(f)$ je součet obrazů tříd $U/\mathrm{Ker}(f)$.
(ii) Analogicky ověříme zachování operace násobení. Pro každé $a, b \in U$ platí vezmeme třídy $a + \mathrm{Ker}(f)$, $b + \mathrm{Ker}(f)$ a platí $i((a + \mathrm{Ker}(f)) \cdot (b + \mathrm{Ker}(f))) = i((a \cdot_1 b) + \mathrm{Ker}(f)) = f(a \cdot b) = f(a) \cdot_2 f(b) = i(a + \mathrm{Ker}(f)) \cdot_2 i(b + \mathrm{Ker}(f))$. To znamená, že obraz součinu tříd $U/\mathrm{Ker}(f)$ je součin obrazů tříd $U/\mathrm{Ker}(f)$.

Dostáváme tak, že zobrazení i je homomorfismus okruhu $(U/\mathrm{Ker}(f), +, \cdot)$ do okruhu $(f(U), +_2, \cdot_2)$.

Nepřímo ukážeme, že zobrazení i je injektivní. Je-li $i(a + \mathrm{Ker}(f)) = i(b + \mathrm{Ker}(f))$, tak podle definice zobrazení i platí $f(a) = f(b)$. Potom ale $f(a) - f(b) = f(b) - f(b) = 0_V$. Přitom $f(a) - f(b) = f(a - b)$, proto $f(a - b) = 0_V$ a $a - b = c \in \mathrm{Ker}(f)$. Dostáváme, že $a = b + c$, kde $c \in \mathrm{Ker}(f)$ a $a + \mathrm{Ker}(f) = b + c + \mathrm{Ker}(f) = b + \mathrm{Ker}(f)$.

A konečně ukážeme, že zobrazení i je surjektivní, neboť pro každé $f(x) \in f(U)$ vezmeme $a + \mathrm{Ker}(f) \in U/\mathrm{Ker}(f)$, pro které platí $i(a + \mathrm{Ker}(f)) = f(a)$. Zobrazení i je tedy izomorfismus okruhů $(U/\mathrm{Ker}(f), +, \cdot)$ a $(f(U), +_3, \cdot_3)$. □



Obrázek 13.4.: *Homomorfismu okruhu* $(U/\mathrm{Ker}(f), +_1, \cdot_1)$ *do okruhu* $(V, +_2, \cdot_2)$.

Všimněte si (Obrázek13.4.), že jádro homomorfismu f je ideál okruhu $(U, +_1, \cdot_1)$. Odpovídající třída faktorového okruhu $(U/\mathrm{Ker}(f), +, \cdot)$ se zobrazí na neutrální prvek okruhu $(V, +_2, \cdot_2)$.

Homomorfismus i nám dává nástroj, jak zkoumat okruh $(V, +_2, \cdot_2)$. Místo druhého okruhu $(V, +_2, \cdot_2)$, respektive místo okruhu obrazů $(V, +_2, \cdot_2)$, lze zkoumat faktorový okruh $(U/\mathrm{Ker}(f), +, \cdot)$ prvního okruhu. První okruh $(V, +_1, \cdot_1)$ si můžeme zvolit. Pokud se nám podaří najít vhodný homomorfismus f a jeho jádro, tak faktorový okruh $(U/\mathrm{Ker}(f), +, \cdot)$ okruh je izomorfní s druhým okruhem $(V, +_2, \cdot_2)$.

Cvičení

13.3.1. Ukažte, že každý ideál okruhu $(R, +, \cdot)$ je jádrem nějakého homomorfismu okruhu $(R, +, \cdot)$.

13.3.2. mějme homomorfismus f okruhů $(\mathbb{R}[x], +, \cdot)$ a $(\mathbb{R}, +, \cdot)$. Mějme $a \in \mathbb{R}$. Určete jádro homomorfismu $f : \mathbb{R}[x] \to \mathbb{R}$ dané předpisem $f(p(x)) = p(a)$ (polynomu přiřadíme jeho funkční hodnoty v bodě a).

Rejstřík

Kurzívou jsou v rejstříku označeny stránky, kde najdete definici příslušného pojmu.

2-cyklus, 121

absorbce, *175*
algoritmus
  Euklidův, *3*
alternující grupa, 124, *124*
asociativita, 35, 36
asociativní
  grupoid, *44*
  operace, *19*
asociativní operace, 35, 36
automorfismus
  okruhu, *192*
Avogadrova konstanta, 8

Bézoutovo lemma, *2*
Bézoutovy koeficienty, *2*, 4
bezprostřední následovník, *10*
bijektivní zobrazení, *14*, 84
binární operace, 18

Cayleyho tabulka, *20*, 33, 34
celá čísla
  interval, 31
centrum, *69*
cyklická grupa, 86, 104
cyklus
  délky 2, 121
cykly
  disjunktní, *116*

částečné uspořádání, *10*
čísla
  nesoudělná, 1
  ordinální, 163
číslo
  komplexně sdružené, 189
  složené, *1*
člen
  vedoucí, *182*

definiční obor, 12, 12, *12*
dělení, 1, *168*
  se zbytkem, *2*
dělitel, *1*
  největší společný, 1, 6
  nuly, *169*
dělitelnost, 1
  a dělí b, 1
  a nedělí b, 1
diagonální matice, 175, 176
diagram
  hasseovský, *10*
dihedrální grupa, 37, 51, 84, 84, 85
disjunkce, 20, 26
disjunktní cykly, *116*
distributivní
  operace, 161, 161, 162, 163
distributivní operace, *19*
důkaz
  indukcí, *28*
  nepřímý, *28*
  přímý, *27*
  sporem, *28*
důkazové techniky, 25

ekvivalence, *8*, 26
epimorfismus
  okruhů, *192*
Erdős P., 27
Euklidův algoritmus, *3*, *3*

faktorová grupa, *96*, 176
faktorový okru, 193, 194, 194, 194, 195
faktorový okruh, *177*, 178, 178, 179, 184, 185

gausovská celá čísla, 167, 169
generátor, *104*
grupa, *50*
  alternující, 124, *124*
  cyklická, 86, 104, 119
  dihedrální, 37, 51, 84, 84, 85
  faktorová, *96*, 176
  generátor, *104*
  homomorfismus, *127*
  jednička, *57*
  jednotek, *51*, 54, 84, 85, 86, 113, 113
  Kleinova, 37, *152*
  levá, *127*
  permutací řádků, *148*
  pravá, *127*
  řád, *83*
  symetrická, *116*
grupa permutací, *116*
grupoid, *41*
  abelovský, *42*
  asociativní, *44*
  nekomutativní, *42*

hasseovský diagram, *10*
hlavní ideál, *183*
hodnota operace, *18*
homomorfismus
  grup, *127*
    jádro, *132*
  kanonický, 135, *135*

nulový, *189*, 192, 193, 193
okruhů, *189*
injektivní, *192*
jádro, *192*, 193, 193, 193, 193, 194
surjektivní, *192*
triviální, 128, *129*
hypotéza, *27*

ideál, *175*, 176, 176, 184
generovaný množinou, *176*
hlavní, *183*
nevlastní, *175*
vlastní, *175*
idempotentní
operace, *46*
prvek, *46*, 59
identická permutace, *116*
implikace, 26
indexová množina, 7
index podgrupy, *84*, 85, 85
indukce, 28
indukční krok, 29
injektivní zobrazení, *13*, 84
interval celých čísel, 31
inverzní
matice, 48, 48, 51
inverzní prvek, 103, 163
inverzní zobrazení, *14*
ireducibilní polynom, *186*
izomorfismus
grup, *141*
okruhů, *192*

jádro homomorfismu
grup, *132*, *192*
okruhů, *192*, 193, 193, 193, 193, 194
jednička, *57*, 163, 169
grupy, *57*
okruhu, *163*, 190, *190*, *192*
jednotka
okruhu, *163*
jednotková matice, 42, 44, 46, 48, 64, 69, 70
jednotkový prvek, *57*

kanonický homomorfismus, 135, *135*
kartézská mocnina
množiny, *7*
kartézský součin, 71
množin, *6*
Kleinova grupa, 37, *152*
koeficient
Bézoutův, *2*, 4
vedoucí, *182*
komplex, *70*
násobení, *71*
sčítání, *71*
komplexně sdružené číslo, 189
komutativita, *42*
komutativní
okruh, *163*
operace, *19*
kongruence modulo m, *8*
konjuknce, 26
konjunkce, 20
konstanta
Avogadrova, 8
konstantní polynom, *182*
kvantifikátor, 26

Lagrangeova věta, *87*
lemma
Bézoutovo, *2*
Euklidovo, *3*
levá grupa, *127*
levá množina, *12*, 13, 14, 14
lichá permutace, *122*
logická
disjunkce, 163, 164
konjunkce, 163, 164
logické spojky, 26

matice
diagonální, 175, 176
inverzní, 48, 48, 51
jednotková, 42, 44, 46, 48, 64, 69, 70
množina
indexová, 7
kartézská mocnina, *7*
kartézský součin, *6*
levá, *12*, 13, 14, 14
mohutnost, 31
nosná, *41*, *116*
obrazů, *11*
podmnožina, *6*
polynomů, *179*
potenční, *7*, 70, 71
pravá, *12*, 13, 14, 14
rozklad, *7*
vlastní podmnožina, *6*
vzorů, *11*
množiny
systém, 7
mocnina
prvku, *57*, *103*
mohutnost množiny, 31
monoid, *46*
monomorfismus
okruhů, *192*

následovník, 12
násobek, *1*
nejmenší společný, 2, 6
prvku, *57*
násobení komplexů, *71*
negace, 26
nejmenší společný násobek, 2, 6

největší společný dělitel, 1, 6
nepřímý důkaz, *28*
nesoudělná čísla, 1
netriviální podgrupy, *63*
neutrální prvek, 35, 36, *42*, 43, 43, 46, 46, 47, 103
nevlastní
  ideál, *175*
  podgrupa, *63*
normalizátor, *99*, *99*, *101*
normální podgrupa, *93*, 177, 179
nosič, *41*
nosná množina, *41*, *116*
nukleotid, 157
nula, *57*, 163
  okruhu, *163*, *189*, *190*, *192*, *194*
nulový
  homomorfismus, *189*, 192, 193, 193
  okruh, *163*
  polynom, 181, *182*
  prvek, *57*
nulový okruh, 176
nutná podmínka, *27*

obměna, *28*
obor
  definiční, *12*
  hodnot, *12*
  integrity, *169*, 182
obraz, *11*, 12
okruh, *161*
  automorfismus, *192*
  epimorfismus, *192*
  faktorový, *177*, 178, 178, 179, 184, 185, 193, 194, 194, 194, 195
  homomorfismus, *189*
  izomorfismus, *192*
  jednička, *163*, 190, *190*, *192*
  jednotka, *163*
  komutativní, *163*
  monomorfismus, *192*
  nula, *163*, *189*, *190*, *192*, *194*
  nulový, *163*, 176
  polynomů, 179, *181*, 182
  přímý součet, *164*
  triviální, *162*, 163, 171, 175, 183
opačný prvek, *50*, 103, 163
operace
  asociativní, *19*, 35, 36
  binární, 18
  dělení, 1
  distributivní, *19*, 161, 161, 162, 163
  idempotentní, *46*
  komutativní, *19*
  restrikce, *19*
  ternární, *18*
  unární, *18*
  uzavřená, 23, 24, 41, 41
  výsledek, *18*
operand, *18*
operátor, 33
ordinální čísla, 163
osová symetrie, 33

parita, 121, 121
permutace, *15*, *116*
  identická, *116*
  lichá, *122*
  pevný bod, *115*
  řád, 119
  sudá, *122*
pevný bod permutace, *115*
podgrupa, *62*, 64, 64, 79, 80, 80, 80, 80, 87, 166
  generovaná množinou, *107*
  grupy jednotek, *155*
  index, *84*, 85, 85
  netriviální, *63*
  nevlastní, *63*
  normalizátor, *99*, *99*, *101*
  normální, *93*, 177, 179
  rozklad grupy, *78*
  triviální, *63*
  vlastní, *63*
podíl, *2*, 8
podmínka
  nutná, *27*
  postačující, *27*
podmnožina, *6*
podokruh, 166, 191, 191, 194
pologrupa, *44*
polynom, *179*
  ireducibilní, *186*
  konstantní, *182*
  množina, *179*
  nulový, 181, *182*
  reducibilní, 186, *186*
  součet, *180*
  součin, *180*
  stupeň, *182*
poset, *11*
postačující podmínka, *27*
potenční množina, *7*, 70, 71
pravá grupa, *127*
pravá množina, *12*, 13, 14, 14
pravdivostní hodnota, 26
proměnná, 179, 181
prosté zobrazení, *13*
průnik
  ideálů, 176, 176, 176
  podgrup, 64
  podokruhů, 167
prvek
  fixovaný, *115*
  idempotentní, *46*, 59
  inverzní, 103, 163
  jednotkový, *57*
  mocnina, *57*, *103*

násobek, *57*
neutrální, 35, 36, *42*, 43, 43, 46, 46, 47, 103
nulový, *57*
opačný, *50*, 103, 163
první věta o izomorfismech, *136*
prvočíslo, *1*
předpoklad, *27*
přímý důkaz, *27*
přímý součet
okruhů, *164*
přirozený homomorfismus, 189

reducibilní polynom, 186, *186*
relace, 8
antisymetrická, 10
částečného uspořádání, *10*
dělitelnosti, 1
ekvivalence, *8*
mezi množinami, *8*
na množině, *8*
reflexivní, 8, 10
symetrická, 8
tranzitivní, 8, 10
reprezentant, *91*
restrikce, 12, 166
operace, *19*, 191, 193, 193, 194
rozklad, 93, 94, 176, 177, 184
grupy podle podgrupy, *78*
množiny, *7*
třídy, *7*, 95, 177, 177, 177, 177, 178, 184

řád
grupy, *83*, 104
nekonečný, *83*, *85*, 104
permutace, 119
prvku, *85*, 104

sčítání komplexů, *71*
skalární součin, *31*
složené číslo, *1*
součet
polynomů, *180*
součin
grup
vnější, 151, *151*
polynomů, *180*
skalární, *31*
vektorový, *31*
spor, 28, 28
stupeň polynomu, *182*
sudá permutace, *122*
surjektivní zobrazení, *14*, 84
symetrická grupa, *116*
symetrický objekt, 33
symetrie, 33, 38
n-úhelníka, 37
čtverce, 36
čtyřstěnu, 39
kvádru, 38
osová, 33
symbolu recyklace, 36
trojúhelníka, 34
systém množin, 7

tabulka
Cayleyho, *20*, 33, 34
těleso, 183, 184, 187
transpozice, *121*
triviální
okruh, *162*, 163, 171, 175, 183
podgrupa, *63*
triviální homomorfismus, 128, *129*
třídy rozkladu, *7*
tvrzení, *27*

uzavřená
operace, 23, 24, 41
uzavřená operace, 41
uzavřenost, 35, 36, 41

vedoucí
člen, *182*
koeficient, *182*
vektorový součin, *31*
věta
aritmetiky základní, *5*
Bézoutovo lemma, *2*
Euklidovo lemma, *3*
Euklidův algoritmus, *3*
hlavní o cyklických grupách, *112*
hlavní o homomorfismech, *194*
Lagrangeova, *87*
o jednoznačnosti inverzního prvku v grupě, *52*
o jednoznačnosti neutrálního prvku, *47*
o jednoznačnosti podílu a zbytku, *2*
o krácení v grupě, *55*
o ponožkách a botách, *57*
první věta o izomorfismech, 136
základní věta aritmetiky, *5*
vlastní
ideál, *175*
podgrupy, *63*
vlastní podmnožina, *6*
vnější součin grup, 151, *151*
výrok, *26*
výsledek operace, *18*
vzor, *11*, 12

základ indukce, 28
základní věta aritmetiky, *5*
zbytek, *2*, 8, 189, 192, 192, 193, 194
zbytková třída modulo m, *73*, 107
zobrazení
bijektivní, *14*, 84
injektivní, *13*, 84
inverzní, *14*

množiny, *12*
na, *14*
obraz, *12*
prosté, *13*
surjektivní, *14*, 84
vzájemně jednoznačné, *14*
vzor, *12*
z množiny, *12*
zrcadlení, *33*

Literatura

[G] J.A. Gallian, Contemporary Abstract Algebra, Cengage Learning, 8th edition (2012), ISBN13 978-1133599708.

[P] Ch.C. Pinter, A Book of Abstract Algebra, MacGraw-Hill, 2nd edition (2010), ISBN13 978-0-486-47417-5.

Užitečné tabulky

Zde je uvedeno několik užitečných tabulek, se kterými se často pracuje.

Tabulka skládání symetrií rovnostranného trojúhelníka

$\circ$	R_0	R_{120}	R_{240}	Z_A	Z_B	Z_C
R_0	R_0	R_{120}	R_{240}	Z_A	Z_B	Z_C
R_{120}	R_{120}	R_{240}	R_0	Z_C	Z_A	Z_B
R_{240}	R_{240}	R_0	R_{120}	Z_B	Z_C	Z_A
Z_A	Z_A	Z_B	Z_C	R_0	R_{120}	R_{240}
Z_B	Z_B	Z_C	Z_A	R_{240}	R_0	R_{120}
Z_C	Z_C	Z_A	Z_B	R_{120}	R_{240}	R_0

Tabulka 13.1.: *Dihedrální grupa* $(D_n, \circ)$.

Tabulka skládání symetrií čtyřstěnu

$\circ$	ι	π_{AB}	π_{AC}	π_{AD}	φ_D	φ_A	φ_C	φ_B	φ'_D	φ'_B	φ'_A	φ'_C
$(A) = \iota$	ι	π_{AB}	π_{AC}	π_{AD}	φ_D	φ_A	φ_C	φ_B	φ'_D	φ'_B	φ'_A	φ'_C
$(AB)(CD) = \pi_{AB}$	π_{AB}	ι	π_{AD}	π_{AC}	φ_A	φ_D	φ_B	φ_C	φ'_B	φ'_D	φ'_C	φ'_A
$(AC)(BD) = \pi_{AC}$	π_{AC}	π_{AD}	ι	π_{AB}	φ_C	φ_B	φ_D	φ_A	φ'_A	φ'_C	φ'_D	φ'_B
$(AD)(BC) = \pi_{AD}$	π_{AD}	π_{AC}	π_{AB}	ι	φ_B	φ_C	φ_A	φ_D	φ'_C	φ'_A	φ'_B	φ'_D
$(ABC) = \varphi_D$	φ_D	φ_B	φ_A	φ_C	φ'_D	φ'_C	φ'_B	φ'_A	ι	π_{AD}	π_{AB}	π_{AC}
$(BDC) = \varphi_A$	φ_A	φ_C	φ_D	φ_B	φ'_B	φ'_A	φ'_D	φ'_C	π_{AB}	π_{AC}	ι	π_{AD}
$(ADB) = \varphi_C$	φ_C	φ_A	φ_B	φ_D	φ'_A	φ'_B	φ'_C	φ'_D	π_{AC}	π_{AB}	π_{AD}	ι
$(ACD) = \varphi_B$	φ_B	φ_D	φ_C	φ_A	φ'_C	φ'_D	φ'_A	φ'_B	π_{AD}	ι	π_{AC}	π_{AB}
$(ACB) = \varphi'_D$	φ'_D	φ'_A	φ'_C	φ'_B	ι	π_{AC}	π_{AD}	π_{AB}	φ_D	φ_C	φ_B	φ_A
$(ADC) = \varphi'_B$	φ'_B	φ'_C	φ'_A	φ'_D	π_{AB}	π_{AD}	π_{AC}	ι	φ_A	φ_B	φ_C	φ_D
$(BCD) = \varphi'_A$	φ'_A	φ'_D	φ'_B	φ'_C	π_{AC}	ι	π_{AB}	π_{AD}	φ_C	φ_D	φ_A	φ_B
$(ABD) = \varphi'_C$	φ'_C	φ'_B	φ'_D	φ'_A	π_{AD}	π_{AB}	ι	π_{AC}	φ_B	φ_A	φ_D	φ_C

Tabulka 13.2.: *Alternující grupa* $(A_4, \circ)$.

Tabulka skládání symetrií čtverce

$\circ$	R_0	R_{90}	R_{180}	R_{270}	H	V	E	F
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	E	F
R_{90}	R_{90}	R_{180}	R_{270}	R_0	F	E	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	F	E
R_{270}	R_{270}	R_0	R_{90}	R_{180}	E	F	V	H
H	H	E	V	F	R_0	R_{180}	R_{90}	R_{270}
V	V	F	H	E	R_{180}	R_0	R_{270}	R_{90}
E	E	V	F	H	R_{270}	R_{90}	R_0	R_{180}
F	F	H	E	V	R_{90}	R_{270}	R_{180}	R_0

Tabulka 13.X85.: *Tabulka dihedrální grupy* $(D_4, \circ)$.

Přehled použitých symbolů

Struktury s jednou operací a dvěma operacemi

a^{-1}	inverzní prvek (str. 48)
A^{-1}	inverzní matice (str. 48)
$(G, \circ)$	grupoid s operací „$\circ$“ (str. 41)
$(G, \cdot)$	grupa s operací „$\cdot$“ (str. 50)
$A \boxdot B$	operace s komplexy A, B (str. 71)
$a \odot B$	násobení prvku a a komplexu B (str. 71)
$(G : H)$	index podgrupy $(H, \cdot)$ v grupě $(G, \cdot)$ (str. 84)
$\lvert G \rvert$	řád grupy $(G, \cdot)$ (str. 83)
$Z(G)$	centrum grupy $(G, \cdot)$ (str. 69)
$(\langle a \rangle, \cdot)$	cyklická grupa generovaná prvkem a (str. 104)
$(G, \circ_1) \simeq (H, \circ_2)$	izomorfní grupy $(G, \circ_1)$ a $(H, \circ_2)$ (str. 141)

$(R, +, \cdot)$	okruh s operací sčítání „$+$“ a operací násobení „$\cdot$“ (str. 161)
$(R[x], +, \cdot)$	okruh polynomů s koeficienty z okruhu R (str. 179)
$(\langle a \rangle, +, \cdot)$	hlavní ideál okruhu generovaný prvkem a (str. 183)

Další matematické symboly

2^A	potenční množina množiny A (str. 7)	$A \cup B$	sjednocení množin A a B (str. 6)
$\emptyset$	prázdná množina (str. 6)	$A \setminus B$	rozdíl množin A a B (str. 6)
ε	identická permutace (str. 115)	$A \triangle B$	symetrická diference množin A a B (str. 6)
$\phi(n)$	eulerova $\phi(n)$ funkce (str. ??)	$A \times B$	kartézský součin množin A a B (str. 6)
$E_{n,n}$	jednotková matice řádu n (str. 44)	$A \wedge B$	logická konjunkce „A a současně B“ (str. 20)
$x \in A$	prvek x množiny A (str. 6)	$A \vee B$	logická disjunkce „A nebo B“ (str. 20)
$A \subseteq B$	podmnožina A množiny B (str. 6)	$A \oplus B$	logická operace XOR „A XOR B“ (str. ??)
$A \subset B$	vlastní podmnožina A množiny B (str. 6)	$A \Rightarrow B$	implikace „jestliže platí A, tak platí B“ (str. ??)
$A \cap B$	průnik množin A a B (str. 6)	$A \Leftrightarrow B$	ekvivalence „A platí právě, když B“ (str. ??)

Číselné obory

$\mathbb{N}$	přirozená čísla	$\mathbb{Q}$	racionální čísla	$\mathbb{P}$	prvočísla
$\mathbb{Z}$	celá čísla	$\mathbb{R}$	reální čísla	$\mathbb{S}$	sudá celá čísla
$\mathbb{Z}_n$	zbytkové třídy modulo n	$\mathbb{R}^*$	rozšířená reální čísla	$\mathbb{L}$	lichá celá čísla
$k\mathbb{Z}$	celočíselné násobky čísla k	$\mathbb{C}$	komplexní čísla	$\mathbb{I}$	iracionální čísla

$\mathbb{Z}[i]$	gausovská celá čísla tvaru $a + bi$ (str. 167)
$\mathbb{Z}[\sqrt{2}]$	čísla tvaru $a + b\sqrt{2}$ (str. 169)
$M_{n,n}$	čtvercové matice řádu n s reálnými koeficienty (str. 41)
$M^*_{n,n}$	regulární čtvercové matice řádu n s reálnými koeficienty (str. 51)
$M_{n,n}(F)$	čtvercové matice řádu n s koeficienty z množiny F (str. 62)

Speciální typy algebraických struktur

$(\mathbb{Z}, +)$	grupa celých čísel s operací obyčejného sčítání (str. 50)
$(\mathbb{Z}, \cdot)$	monoid celých čísel s operací obyčejného násobení (str. 46)
$(D_n, \circ)$	dihedrální grupa symetrií n-úhelníka s operací skládání symetrií (str. 37)
$(U(n), \cdot)$	grupa jednotek modulo n s operací obyčejného násobení (str. 51)
$(S_n, \circ)$	symetrická grupa všech permutací n-prvkové množiny (str. 116)
$(S_G, \circ)$	grupa vybraných permutací $\lvert G \rvert$-prvkové množiny dle Cayleho tabulky grupy $(G, \cdot)$ (str. 148)
$(A_n, \circ)$	grupa sudých permutací n-prvkové množiny (str. 124)
$(\mathbb{Z}_n, \cdot)$	grupa zbytkových tříd modulo n (str. 72)
$(M_{n,n}, \cdot)$	monoid násobení čtvercových matic řádu n s reálnými prvky (str. 46)
$(M^*_{n,n}, \cdot)$	grupa násobení regulárních čtvercových matic řádu n s reálnými prvky (str. 51)
$(D_{n,n}, \cdot)$	grupa regulárních diagonálních matic řádu n s reálnými prvky (str. 62)
$(M_{n,n}, +, \cdot)$	okruh čtvercových matic řádu n s reálnými prvky (str. 163)