8. Binární operace

Binární operace je jeden z nejobecnějších pojmů, které v této knize potkáme. Úkolem zkoumat abstraktní struktury z hlediska operací se zabývá obor algebra, tuto kapitolu lze tedy brát jako jemný úvod do algebry.

Podstata binárních operací je jednoduchá, jde o proces, kdy vezmeme dva objekty, zamícháme a dostaneme objekt jiný. Profláklé příklady binárních operací jsou třeba sčítání a násobení čísel, dále jsme potkali skládání zobrazení, binární operací je také násobení matic nebo třeba procedura, kdy vezmeme dva řetězce písmen a vytvoříme z nich třetí tak, že bereme postupně písmena z obou střídavě a řadíme za sebe. Nemusíme se omezovat na matematiku, jako operace můžeme interpretovat i mnoho interakcí v reálném světě, třeba mísení barev.

Jak vyjádříme takovou operaci matematicky? Vždycky nám ze dvou objektů dá třetí, takže je to vlastně přiřazení či posílání. Třeba sčítání dvou čísel v podstatě funguje takto: $(x, y) \mapsto (x + y)$. Vhodným modelem tedy bude zobrazení.

! **Definice.**
Nechť M je množina. Pod pojmem **binární operace** na M rozumíme libovolné zobrazení $\circ\colon M \times M \mapsto M$.

Let M be a set. By a **binary operation** we mean any mapping $\circ\colon M \times M \mapsto M$.

Aby se nám věci lépe psaly, zavedeme speciální značení, takže pro prvky $x, y \in M$ budeme namísto $\circ(x, y)$ psát $x \circ y$. To ostatně známe, sčítání dvou čísel nepíšeme $+(1, 13) = 14$, ale $1+13 = 14$. Někdy používáme i jiné značky, třeba $x \diamond y$, $x * y$ a podobně.

Při práci s operací nám pomáhá, pokud známe rozličná pravidla. Ne každá operace ovšem splňuje věci, které máme rádi. S tím je spojena zásadní otázka, co je třeba k tomu, aby určité pravidlo platilo. Někdy to vyplývá ze speciální podstaty objektů, se kterými pracujeme, ale jindy za tím stojí obecnější principy. Dobrým příkladem je pravidlo, které při přechodu k inverzi převrací pořadí v operaci. Vzoreček $(S \circ T)^{-1} = T^{-1} \circ S^{-1}$ jsme viděli pro skládání zobrazení, později se objevil u skládání relací a čtenář jej potkal v lineární algebře u násobení matic: $(AB)^{-1} = B^{-1}A^{-1}$. Dokonce i důkazy byly vlastně stejné ve všech třech případech. To silně naznačuje, že za platnost tohoto pravidla nevděčíme jakési maticovosti či zobrazeňovosti, ale že vyplývá z nějakého obecného principu. Pokud bychom tento princip dokázali identifikovat a zjistili, co přesně je k jeho platnosti potřebné, tak už platnost tohoto pravidla dostaneme automaticky ve všech situacích, která splňují dotyčné požadavky.

Právě zkoumání prapůvodních příčin různých chování je jednou z náplní matematiky. Vnese se tím pořádek do mnohdy nepřehledných situací, navíc je ekonomické dělat věci jednou, tam, kde na tom opravdu záleží, než stejnou věc dělat stejným způsobem znovu a znovu pro různé inkarnace téhož. Nevýhoda z hlediska začátečníka je, že se tak dostáváme ke zkoumání velice abstraktních struktur, u nichž se často nemužeme odvolat na intuici. Jde tedy obvykle o dosti pokročilou látku.

Když matematici takto obecně přemýšleli o operacích a vlastnostech, které je porůznu zajímají, tak postupně zjistili, že mnoho případů „pěkného“ chování ve skutečnosti vyplývá jen z několika málo základních principů. Právě to je téma této kapitoly. Jako inspiraci si ukažme, jak se poznají ty v zásadě nejlepší operace.

! **Definice.**
Uvažujme binární operaci $\circ$ na množině M. Řekneme, že dvojice $(M, \circ)$ je **grupa**, jestliže splňuje následující axiomy:
(A1) **asociativita**:
pro všechna $x, y, z \in M$ platí $x \circ (y \circ z) = (x \circ y) \circ z$.
(A2) existence **jednotkového prvku**:
existuje $e \in M$ takové, že $x \circ e = e \circ x = x$ pro všechna $x \in M$.
(A3) existence **inverzních prvků**:
pro každé $x \in M$ existuje $y \in M$ takové, že $x \circ y = y \circ x = e$.

Consider a set A with a binary operation $\circ$ on it. We say that the couple $(A, \circ)$ is a **group** if it satisfies the following conditions:
(A1) **associative law**: $\forall x, y, z \in M\colon x \circ (y \circ z) = (x \circ y) \circ z$.
(A2) existence of an **identity element**: $\exists e \in M\ \forall x \in M\colon x \circ e = e \circ x = x$.
(A3) existence of **inverse elements**: $\forall x \in M\ \exists y \in M\colon x \circ y = y \circ x = e$.

Někteří autoři začínají ještě jedním axiomem:
(A0) pro všechna $x, y \in M$ platí, že $x \circ y \in M$. (M je **uzavřená** na $\circ$)

Toto je ale už obsaženo v slovech „binární operace ∘“, takže je to zbytečné tam dávat. Na druhou stranu to nevadí, má to pedagogický efekt, protože to čtenáři připomene tuto důležitou vlastnost binárních operací. Když vymýšlíme operaci, tak si musíme pohlídat, že její výsledky nemohou vyskočit z množiny, na které pracujeme. To se týká zejména případů, kdy už operaci máme, ale rozhodneme se s ní pracovat na nějaké menší množině.

Grupy jsou jedna z nejpopulárnějších obecných struktur v matematice. Pomáhají v mnoha aplikacích, například ve fyzikálních teoriích mikrosvěta i vesmíru, při lámání určitých typů šifer (viz prolomení německého kódování Enigma polským algebraikem před druhou světovou) nebo třeba při analýze Rubikovy kostky.

My se jim ale nebudeme věnovat hned, nejprve se pořádně podíváme na to, jaký dopad vlastně jednotlivé axiomy mají. Ne všechny operace jsou totiž natolik pěkné, aby vytvořily grupy, a pak je dobré vědět, co můžeme čekat, když operaci nějaký axiom chybí. Je navíc zajímavé vidět, jak postupným přibíráním axiomů dokážeme o dané operaci říct stále víc, pochopíme tak lépe souvislosti.

Toto zkoumání také vyjasní některé nejasnosti v definici grupy, kterou jsme zde uvedli. Například v této chvíli nevíme, kolik identit a inverzních prvků vlastně máme, což způsobuje problémy v axiomu (A3). Jak se to vlastně s inverzním prvkem myslí, kdyby těch identit existovalo víc?

Čtenář, který potřebuje jen povšechnou znalost a praktické aplikace grup, může první část přeskočit a jít rovnou na kapitolu 8b, konec konců to tak dělají i někteří autoři. Přesto bych kapitolu 8a doporučil, hlavně část o monoidech, která souvisí s kapitolou 7a.

Než se do toho dáme, poznamenejme, že existují i operace jiné než binární, třeba unární (vezmou objekt a něco s ním udělají, čtenář asi zná konjugaci pro komplexní čísla, vlastně každé zobrazení $A \mapsto A$ je unární operace) nebo naopak obecně n-ární, například v geometrii se používá smíšený součin $\vec{u} \bullet (\vec{v} \times \vec{w})$, který pracuje se třemi objekty. Teď už se ale podívejme na operace binární.

8a. Pologrupy a monoidy

Začneme tím nejjednodušším.

Definice.
Pojmem **grupoid** označujeme každou dvojici $(M, \circ)$, kde M je množina a $\circ$ je binární operace na M.

Tento pojem se příliš nepoužívá, už proto, že zde nepředpokládáme splnění žádných dalších podmínek, tudíž ani nemůžeme čekat, že bychom o takovéto struktuře mohli něco dokázat. I v anglické literatuře vyskytuje zřídka, říkají tomu **groupoid** či častěji **magma**.

Jedna podmínka tam vlastně je: že dotyčná operace je zobrazení do M. Tomu říkáme, že množina M je **uzavřená** na (vzhledem k) operaci $\circ$, čímž se některé případy přece jen vyřadí.

Grupoidy potkáváme pořád, například $(\mathbb{N}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}, -)$, $(\mathbb{R}, \cdot)$.

Grupoidem nebude $(\mathbb{N}, -)$, protože například nemůžeme v množině $\mathbb{N}$ odečítat $13 - 23$. Množina tedy není na odečítání uzavřená a nejde o binární operaci. Podobně není grupoidem $(\mathbb{R}, \div)$, protože neumíme dělit nulou. Ale můžeme si rozmyslet, že $(\mathbb{R} - \{0\}, \div)$ už grupoid je, vydělením dvou nenulových čísel zase získáme nenulové číslo.

Teď už je čas zkusit něco zajímavějšího.

! **Definice.**
Nechť $(M, \circ)$ je grupoid.
Řekneme, že operace $\circ$ je **asociativní**, jestliže pro všechna $x, y, z \in M$ platí $x \circ (y \circ z) = (x \circ y) \circ z$.

Tím jsme zavedli pojem, teď vytvoříme strukturu.

! **Definice.**
Nechť $(M, \circ)$ je grupoid. Řekneme, že je to **pologrupa** (**semigroup**), jestliže $\circ$ je asociativní.

Mnoho autorů začíná touto definicí a grupoid prostě přeskočí. Vidíme, že jsme se omezili pouze na axiom (A1) z definice grupy. Než se podíváme, co se dá s pologrupami dělat, ukážeme si nějaké příklady.

Příklad 8a.a:
1) Klasickými pologrupami jsou $(\mathbb{N}, +)$, $(\mathbb{R}, +)$, vlastně můžeme se sčítáním použít libovolnou známou množinu čísel ($\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$), protože víme snad už od základní školy, že sčítání je asociativní.

Dalšími dobrými příklady je násobení s různými množinami jako $(\mathbb{N}, \cdot)$, $(\mathbb{R}, \cdot)$ a podobně.

Ale $(\mathbb{Z}, -)$ pologrupa není. Sice je splněna uzavřenost množiny vzhledem k odčítání, ale neplatí asociativní zákon: $(5-2)-1 = 2$, zatímco $5-(2-1) = 4$.

Ze stejného důvodu není pologrupou $(\mathbb{R}-\{0\}, \div)$. Operace odečítání a dělení se tedy do této teorie nevejdou. To ukazuje, že nejsou stejného druhu jako sčítání a odčítání. Proto se s nimi v teorii operací vůbec nepracuje, stejně brzy uvidíme, že je vlastně vůbec nepotřebujeme, protože se k nim dostaneme oklikou přes (dobře vychovaná) sčítání a násobení.

Zajímavá poznámka: V reálném světě paradoxně nepracujeme s reálnými čísly, ale jen určitou podmnožinou v závislosti na použité výpočetní technice. Například moje kalkulačka si pamatuje jen 12 míst z každého reálného čísla. To má nečekané dopady, abychom je lépe viděli, trochu zmenšíme rozsah. Nechť M je množina všech reálných čísel s 4 platnými číslicemi. Obsahuje tedy čísla jako 145, -13.76, 1492000 a podobně. Zato neobsahuje číslo 74367, to se v našem světě M automaticky převede na 74360.

Uvažujme prostor $(M, +)$, kde $+$ je teď sčítání „počítačové“, kdy se výsledky automaticky převádějí do M. Tvrdíme, takovéto sčítání není asociativní, tudíž $(M, +)$ není pologrupa. Dokážeme to snadno, porovnejte

$$(11110 + 7) + 7 = 11110 + 7 = 11110,$$
$$11110 + (7 + 7) = 11110 + 14 = 11120.$$

Pokud bychom při převodu výsledku operace do M neořezávali, ale zaokrouhlovali, stejně by to dopadlo jinak:

$$(11110 + 7) + 7 = 11120 + 7 = 11130,$$
$$11110 + (7 + 7) = 11110 + 14 = 11120.$$

Takže sčítání, teoreticky krásná asociativní operace, není v počítačích asociativní (a také není komutativní), což může při výpočtech způsobovat fatální chyby. Lidé, kteří se počítačovými výpočty zaobírají, na toto musí myslet.

2) Ve vícedimenzionálních prostorech umíme sčítat vektory (děláme to po souřadnicích), máme pologrupu $(\mathbb{R}^n, +)$ nebo třeba $(\mathbb{N}^n, +)$, protože sčítáním vektorů se souřadnicemi z $\mathbb{N}$ zase dostaneme vektory se souřadnicemi z $\mathbb{N}$. Dokážeme to pro dvourozměrný případ.

Nechť $(u, v), (x, y) \in \mathbb{N}^2$. Pak $u, v, x, y \in \mathbb{N}$, proto $(u, v) + (x, y) = (u + x, v + y)$ má souřadnice $u + x \in \mathbb{N}$ a $v + y \in \mathbb{N}$. Množina $\mathbb{N}^2$ je tedy opravdu uzavřená na sčítání vektorů.

Teď si ještě přiberme $(s, t) \in \mathbb{N}^2$. Pak pomocí asociativity pro běžné sčítání dostaneme

$$\begin{aligned}[(s,t) + (u,v)] + (x,y) &= (s+u, t+v) + (x,y) = ([s+u]+x, [t+v]+y) \\ &= (s+[u+x], t+[v+y]) = (s,t) + (u+x, v+y) = (s,t) + [(u,v) + (x,y)].\end{aligned}$$

Asociativita je potvrzena, množiny $\mathbb{R}^n$ či $\mathbb{Z}^n$ tvoří se sčítáním vektorů pologrupu. Čtenář si hravě rozmyslí, že totéž lze dokázati o $(\mathbb{Q}^n, +)$, $(\mathbb{Z}^n, +)$ atd.

Standardní násobení na vektorech neexistuje, tak si operaci spojenou s násobením vymyslíme. Necháme se inspirovat klasickým sčítáním a zavedeme násobení po souřadnicích, pro $(u_1, \ldots, u_n), (x_1, \ldots, x_n) \in \mathbb{R}^n$ definujeme $(u_1, \ldots, u_n) \cdot (x_1, \ldots, x_n) = (u_1 \cdot x_1, \ldots, u_n \cdot x_n)$. Podobně jako u sčítání se snadno dokáže, že se vlastnosti obvyklého násobení čísel přenášejí i na tuto operaci, dostáváme tak pologrupy $(\mathbb{R}^n, \cdot)$ či třeba $(\mathbb{N}^n, \cdot)$.

Operací lze na vektorech vymyslet spoustu, viz třeba cvičení 8a.1.

3) Další známá pologrupa je $(M_{m\times n}, +)$, sčítání reálných matic velikosti $m \times n$, podobně je pologrupou $(M_n, \cdot)$ neboli násobení reálných čtvercových matic řádu n. Přinejmenším u sčítání by to nemělo překvapit, protože to funguje po jednotlivých prvcích matic (podobně jako u vektorů jsme sčítali po souřadnicích), takže není problém si matici představit přerovnanou do vektoru, vše funguje stejně.

4) Snadno také dokážeme, že z množiny P všech reálných polynomů dostaneme pologrupy operacemi sčítání i násobení polynomů. Ani to není překvapením, protože polynomy i operace s nimi lze reprezentovat pomocí vektorů čísel (koeficientů polynomu).

△

Příklad 8a.b:

Díky kapitole 7 máme další zajímavý případ, prostory $(\mathbb{Z}_n, +)$ a $(\mathbb{Z}_n, \cdot)$, kde $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Ve Větě 7a.20 jsme dokázali, že sčítání i násobení na $\mathbb{Z}_n$ je asociativní.

△

Příklad 8a.c: Nechť U je libovolná množina, uvažujme $M = P(U)$ (všechny podmnožiny U). Pak $(M, \cap)$ i $(M, \cup)$ jsou pologrupy. Pokud sjednotíme či pronikneme dvě podmnožiny U, pak je výsledná množina zase podmnožinou U, máme tedy uzavřenost M vzhledem k těmto dvěma operacím. Asociativitu průniku i sjednocení dává Věta 2a.7 (vi). Pologrupu ale nedostaneme s operací množinového rozdílu, viz cvičení 2a.2 (iv).

△

Příklad 8a.d:
1) Zvolme nějakou množinu A. Nechť M je množina všech zobrazení z A do A. Pak je M spolu s operací skládání pologrupa, viz Věta 2b.1.

2) Nechť M je množina všech relací na A. Pak je M s operací skládání pologrupa, viz Fakt 3a.3.

3) Vezmeme-li interval I reálných čísel a uvažujeme množinu $F(I)$ všech reálných funkcí na I, pak jsou $(F(I),+)$ a $(F(I),\cdot)$ pologrupy.

Trochu víc práce dá dokázat, že pologrupa je i $(F(\mathbb{R}),\circ)$, kde $\circ$ je operace skládání funkcí.

4) Ukážeme si ještě jednu trochu komplikovanější množinu funkcí. Označíme písmenem F množinu všech funkcí, které mají jako definiční obor nějakou podmnožinu reálných čísel a jdou do reálných čísel. Taková množina už nebude uzavřená ani na sčítání funkcí, protože co dostaneme při sčítání dvou funkcí, které mají disjunktní definiční obory? Vyřešíme to tak, že si zavedeme jako speciální funkci $\emptyset$, to je funkce, která má definiční obor $\emptyset$ a neposílá nic nikam. Ta nám pak pomůže, kdykoliv se pokusíme o něco srandovního, třeba výsledkem $\sqrt{x}+\ln(-x)$ je právě funkce $\emptyset$.

Teď už můžeme funkce z této množiny libovolně kombinovat. Protože se algebraické operace mezi funkcemi definují pomocí běžného sčítání a násobení, které jsou asociativní, tak snadno ukážeme, že $(F,+)$ i $(F,\cdot)$ jsou pologrupy. U skládání se to dokáže také, takže i $(F,\circ)$ je pologrupa.
△

Příklad 8a.e: Uvažujme $A=\mathbb{N}$ a operace $x\circ_l y=\mathrm{lcm}(x,y)$, tj. nejmenší společný násobek, a $x\circ_g y=\gcd(x,y)$, tj. největší společný dělitel.

Například $3\circ_l 7=21$, $3\circ_g 7=1$, $4\circ_l 6=12$, $4\circ_g 6=2$.

Uzavřenost množiny $\mathbb{N}$ na tuto operaci je zjevná, ale ještě potřebujeme dokázat asociativitu obou operací. To dá trochu práce, asi nejjednodušší je ukázat, že $(x\circ_l y)\circ_l z$ odpovídá nejmenšímu společnému násobku x,y,z stejně jako $x\circ_l(y\circ_l z)$, tudíž se musí rovnat. Podobně se dá vyšetřit druhá operace (viz cvičení 6a.19).

Máme tedy pologrupy $(\mathbb{N},\circ_l)$ a $(\mathbb{N},\circ_g)$.
△

Příklad 8a.f: Teď něco trochu exotičtějšího.

1) Uvažujme $A=\mathbb{R}$ a zadefinujeme operaci $\circ_{13}$ takto: Pro reálná čísla x,y je $x\circ_{13}y$ to z čísel x,y, které je blíže číslu 13; pokud jsou obě stejně daleko, dá se přednost tomu levému.

Takže $14\circ_{13}27=27\circ_{13}14=14$, $10\circ_{13}17=17\circ_{13}10=10$, $12\circ_{13}14=12$ ale $14\circ_{13}12=14$ (takže tato operace není komutativní), $\sqrt{8}\circ_{13}(-\pi)=\sqrt{8}$.

Vidíme také, že $13\circ_{13}x=x\circ_{13}13=13$ pro všechna $x\in\mathbb{R}$. U této operace tedy hraje číslo 13 stejnou roli jako číslo 0 u násobení, ale nějaké závěry z toho dělat nebudeme, je to jen zajímavá náhoda.

Asociativita platí, ale dá práci ji dokázat, protože výsledek operace není dán vzorcem. Asi nejjednodušší cesta je si rozmyslet, že výsledkem $(x\circ_{13}y)\circ_{13}z$ je to z čísel x,y,z, které je nejblíže k číslu 13, v případě rovnosti vyhrává to nejvíce vlevo ve výrazu. Výraz $x\circ_{13}(y\circ_{13}z)$ dává totéž, musí se tedy rovnat. Vytvořili jsme tedy pologrupu.

2) Barvu očí určují mimo jiné dva geny, z nichž každý přichází ve dvou formách, H a b. Gen H je dominantní a jakmile se v té dvojici objeví, budou oči hnědé. Gen b je recesivní a převládne jen tehdy, když jsou takové ve dvojici oba, pak jsou oči modré. Můžeme to vyjádřit takto: $H\circ H=H$, $H\circ b=H$, $b\circ H=H$, $b\circ b=b$. Tím vznikla binární operace na množině $M=\{b,H\}$. Rozmyslíme si, že pro tuto operaci platí asociativní zákon.

Máme-li výrazy $(x\circ y)\circ z$ a $x\circ(y\circ z)$, tak jsou dvě možnosti. Jestliže je některý z x,y,z roven H, pak dominantní gen ovládne všechny operace a výsledky obou vzorců jsou H. V opačném případě jsou ve vzorcích samá b a výsledek bude u obou výrazů b.

Takže tento objekt $(M,\circ)$ je pologrupa.
△

Operace na konečných množinách, které nelze definovat vzorcem, se spíš než výčtem možností definují tzv. **Cayleyho tabulkou**. Tabulka pro geny očí z příkladu 8a.f vypadá takto:

$\circ$	H	b
H	H	H
b	H	b

Operace zadané tabulkou jsou nepříjemné, protože chceme-li zjistit, zda platí nějaký zákon, tak musíme vyzkoušet všechny možnosti dosazení, což je docela dost. V případě asociativního volíme na tři pozice, takže u množiny s n prvky to znamená ověřit n^3 možností.

Příklad 8a.g: Uvažujte množinu s dvěma prvky, $M = \{a, b\}$. Vytvoříme na ní binární operaci následující tabulkou.

$\circ$	a	b
a	a	a
b	b	a

Dává to pologrupu? Musíme prozkoumat osm možností. Ukáže se, že tato operace asociativní není, protože $(b \circ b) \circ b = a \circ b = a$, zatímco $b \circ (b \circ b) = b \circ a = b$.

Nedostáváme tedy pologrupu.

△

Příklad 8a.h: Na množině $\mathbb{N}$ definujme následující operaci: Pro $m, n \in \mathbb{N}$ je $m \circ n$ dáno jako největší prvočíslo, které dělí $m + n$. Například $23 + 37 = 60$, to dělí prvočísla $2, 3, 5$, proto $23 \circ 37 = 5$. Evidentně je $\mathbb{N}$ uzavřená na tuto operaci, ale $(\mathbb{N}, \circ)$ není pologrupa, protože selhává asociativita. Například $(3 \circ 5) \circ 10 = 2 \circ 10 = 3$, zatímco $3 \circ (5 \circ 10) = 3 \circ 5 = 2$. Takže tuto operaci už tady znovu nepotkáme.

Mimochodem, všimněte si, že je komutativní, $m \circ n = n \circ m$, ale nikterak jí to nepomůže. V algebře hraje komutativita spíš pomocnou roli.

△

K většině těchto příkladů se budeme opakovaně vracet.

V příkladech jsme se setkali s pologrupami $(\mathbb{Z}, +)$ a $(\mathbb{N}, +)$. Pokud si to čtenář zkusil dokázat, tak zjistil, že důkaz asociativity pro případ $\mathbb{N}$ je zcela stejný jako pro $\mathbb{Z}$, protože jde o stejnou operaci. Patrně jsme tedy dělali zbytečnou práci, selský rozum říká, že když operaci, pro kterou funguje určité pravidlo na množině, používáme na části té množiny, tak se dotyčné pravidlo nemůže pokazit.

Formálně, máme pologrupu a rádi bychom se omezili na nějakou její část, aniž bychom ztratili vlastnost býti pologrupou. To je v matematice častý požadavek, který jsme už ostatně potkali u více pojmů (restrikcí funkce vznikla nová funkce, u uspořádaných množin jsme často ocenili možnost přejít k podmnožinám a zase to byla uspořádaná množina atd.).

Definice.
Nechť $(M, \circ)$ je pologrupa a $N \neq \emptyset$ je podmnožinou M. Řekneme, že N je **podpologrupa** $(M, \circ)$, jestliže $(N, \circ_N)$ je pologrupa, kde $\circ_N$ je restrikce binární operace $\circ$ na množinu $N \times N$.

V našem inspiračním příkladě bychom tedy řekli, že $\mathbb{N}$ je podpologrupa $(\mathbb{Z}, +)$. Operaci u $\mathbb{N}$ není třeba uvádět, protože se automaticky dědí ta původní z větší množiny, v tom je princip pojmu podpologrupy. My jsme si v definici zavedli speciální značení $\circ_N$, ale to je jen dočasně, abychom v důkazu níže jasně ukázali, kde se na operaci $\circ$ díváme v rámci původní množiny a kde v rámci N.

Teď bychom se měli dostat k té úspoře. Představme si, že uvažujeme podmnožinu N pologrupy $(M, \odot)$. Co by se mohlo pokazit, aby to nebyla podpologrupa? Zkoumáme podle definice, zda je $(N, \odot_N)$ pologrupa, a již jsme zmínili intuitivní pocit, že výpočty by měly probíhat stejně v N jako v M, tudíž by asociativita měla platit. Takže jediná podmínka z definice pologrupy, která není zaručena, je uzavřenost operace. Potvrdíme to důkazem.

Věta 8a.1.
Nechť $(M, \circ)$ je pologrupa a $N \neq \emptyset$ je podmnožinou M. Pak N je podpologrupa $(M, \circ)$ právě tehdy, když je N uzavřená na $\circ$.

Důkaz (rutinní)**:** 1) $\Longrightarrow$: Jestliže je N podpologrupa, pak je $(N, \circ_N)$ pologrupa, tudíž již z definice musí platit $x \circ_N y \in N$ pro všechna $x, y \in N$. Protože je $\circ_N$ restrikcí $\circ$ na N, tak pak máme i $x \circ y = x \circ_N y \in N$ pro všechna $x, y \in N$, tedy N je uzavřená vzhledem k $\circ$.

2) $\Longleftarrow$: Předpokládejme, že $x \circ y \in N$ pro všechna $x, y \in N$. Pak má zobrazení $\circ$: $M \times M \mapsto M$ po restrikci na $N \times N$ hodnoty v N, tedy $\circ_N$: $N \times N \mapsto N$. Dvojice $(N, \circ_N)$ je tedy grupoid. Zbývá ověřit asociativní zákon. Použijeme asociativitu $\circ$ na M a faktu, že operace $\circ_N$ coby restrikce splňuje $x \circ_N y = x \circ y$ pro $x, y \in N$.

Vezměme tedy libovolné $x, y, z \in N$. Pak

$$(x \circ_N y) \circ_N z = (x \circ y) \circ z = x \circ (y \circ z) = x \circ_N (y \circ_N z).$$

□

Takže při přechodu k podmnožinám stačí hlídat uzavřenost, což je obvykle snadné. Často tak ze známého příkladu pologrupy vyrábíme další.

S podpologrupami už si rozumíme, tak přestaneme používat $\circ_N$, je to pořád stejná operace $\circ$.

Příklad 8a.i (pokračování 8a.a)**:**
1) Vyjdeme-li z pozorování, že $(\mathbb{C},+)$ a $(\mathbb{C},\cdot)$ jsou pologrupy, dostáváme prakticky okamžitě také pologrupy $(\mathbb{R},+)$, $(\mathbb{N},+)$, $(\mathbb{Z},\cdot)$ a další.

Zkusíme si zajímavější modifikace. Připomeňme, že když je X nějaká známá číselná množina, tak z ní značením X^+ vybereme jen kladná čísla a značením X^- jen záporná čísla, značením X_0 pak přidáme nulu.

Snadno si rozmyslíme, že třeba $(\mathbb{Z}^-,+)$, $(\mathbb{R}^+,+)$, $(\mathbb{Q}_0^+,+)$, $(\mathbb{Q}^+,\cdot)$, $(\mathbb{R}-\{0\},\cdot)$ jsou pologrupy. Stačí například ukázat, že součet dvou záporných celých čísel je záporné celé číslo, a podle Věty to již dokazuje $\mathbb{Z}^+$ coby podpologrupu $(\mathbb{C},+)$, ale také podpologrupu $(\mathbb{Z},+)$, což je zase podpologrupa $(\mathbb{R},+)$. Jak vidíte, můžeme dělat celé řetízky podpologrup.

Naopak $(\mathbb{Z}^-,\cdot)$ pologrupou není, protože to sice je podmnožina pologrupy $(\mathbb{Z},\cdot)$, ale není uzavřená na násobení, vynásobením dvou záporných čísel nedostaneme záporné číslo.

Jiný zajímavý způsob: Zvolme přirozené číslo n a definujme $n\mathbb{Z}=\{nk;\ k\in\mathbb{Z}\}$, například $2\mathbb{Z}$ je množina všech celých násobků 2 čili množina sudých čísel. Ověříme uzavřenost takové množiny na obě známé operace:

Jestliže $x,y\in n\mathbb{Z}$, pak existují $k,l\in\mathbb{Z}$ takové, že $x=nk$ a $y=nl$. Proto $x+y=n(k+l)$ a $k+l\in\mathbb{Z}$, tudíž podle definice $n\mathbb{Z}$ platí $x+y\in n\mathbb{Z}$. Podobně $xy=n(nkl)$ a $nkl\in\mathbb{Z}$, tudíž $x\cdot y\in n\mathbb{Z}$.

Proto jsou $(n\mathbb{Z},+)$ a $(n\mathbb{Z},\cdot)$ pologrupy.

Ukážeme si ještě jednu pěknou pologrupu. Čtenář je jistě obeznámen s pravidly pro interakci znamének v součinech/podílech (dva mínusy jsou plus atd.). Můžeme zavést množinu $M=\{+,-\}$ a pravidla zachytíme tabulkou.

$\circ$	$-$	$+$
$-$	$+$	$-$
$+$	$-$	$+$

Vyhodnocením osmi možností se ukáže, že tato $(M,\circ)$ je pologrupa.

Elegantnější přístup: namísto znamének pracujeme s čísly $+1$ a -1 a násobením. Množina $\{1,-1\}$ je uzavřená na násobení, proto je to podpologrupa $(\mathbb{Z},\cdot)$ a tudíž pologrupa.

2) I ve vícedimenzionálních prostorech teď můžeme utíkat do podmnožin s tím, že si musíme hlídat uzavřenost. Třeba $(\mathbb{Z}^n,+)$, $(\mathbb{Q}^n,+)$, $((\mathbb{R}^+)^n,\cdot)$ nebo $(\mathbb{N}^n,+)$ jsou pologrupy.

Toto je ale docela nudné, zkusme se zamyslet hlouběji nad běžným vektorovým prostorem se sčítáním. Jak vlastně množiny uzavřené na sčítání vypadají? V tom nám pomůže lineární algebra, jsou to například všechny lineární podprostory. Takže v rovině budou takovými podmnožinami všechny přímky procházející počátkem, v třírozměrném prostoru zase všechny přímky či roviny procházející počátkem. Takto je tedy možné vytvářet zajímavé pologrupy, třeba $N=\{(s,t,2s-t);\ s,t\in\mathbb{R}\}$ je rovina procházející počátkem v $\mathbb{R}^3$, proto je $(N,+)$ pologrupa.

3) Uvažujme množinu M_n^R všech regulárních reálných matic $n\times n$, tedy čtvercových matic s nenulovým determinantem. Z lineární algebry víme, že součin dvou regulárních matic je regulární, tudíž je tato množina uzavřená na násobení a $(M_n^R,\cdot)$ je pologrupa.

Tato množina už ale není uzavřená na sčítání. Se sčítáním můžeme zkusit jiné věci, třeba množinu všech matic, jejichž členy jsou kladné.

4) I u polynomů se dají vyrábět zajímavé podmnožiny uzavřené na běžné operace, například množina M všech polynomů, které mají 13 jako kořen, je uzavřená na násobení.
△

Příklad 8a.j (pokračování 8a.c)**:** Máme množinu M všech podmnožin nějakého universa U. Tady už dá trochu práce vybírat množiny z M tak, aby byly uzavřené na sjednocení, popřípadě na průnik.

Pokud si například jako N zkusíme vzít všechny podmnožiny U se sudým počtem prvků, tak to nebude fungovat, je snadné si představit, že průnikem dvou chytře vybraných dvouprvkových možin vznikne jednoprvková a nemáme uzavřenost vzhledem k průniku, sjednocením dvouprvkových množin zase může vzniknout i tříprvková.

Chytřejší nápad: Zvolme si pevně nějaký prvek $u\in U$, nechť N je množina všech podmnožin U, které obsahují u. Pak už jsou $(N,\cap)$ i $(N,\cup)$ pologrupy (rozmyslete si uzavřenost, viz cvičení 8a.2).
△

Příklad 8a.k (pokračování 8a.d)**:**
1) Použijeme-li Fakt 2b.10, tak zjistíme, že množina všech prostých zobrazení z A do A je s operací skládání pologrupa, podobně je uzavřená na skládání i množina všech zobrazení na a množina všech bijekcí.

2) U relací na A a operace skládání se zase z původní pologrupy můžeme omezit například na relace reflexivní (Věta 3c.4) nebo třeba na uspořádání či na ekvivalence.

3) U funkcí můžeme zkusit vzít třeba jen množinu všech funkcí na I, které mají vždy kladné hodnoty, a bude již uzavřená na sčítání a násobení funkcí, dostaneme tak pologrupu.

Zajímavější trik: Vezměme množinu $C(I)$ všech spojitých funkcí na I a množinu $C^1(I)$ všech funkcí na I, které jsou tam spojité, mají první derivaci a i ta je spojitá na I. Věty z matematické analýzy zaručují, že tyto dvě množiny jsou uzavřené jak na sčítání funkcí, tak na jejich násobení, dostáváme tak zajímavé pologrupy $(C(I),+)$, $(C(I),\cdot)$, $(C^1(I),+)$ a $(C^1(I),\cdot)$.

Podobně se ukáže, že pologrupami jsou také $(C(\mathbb{R}),\circ)$ a $(C^1(\mathbb{R}),\circ)$, ani skládání funkcí nezkazí spojitost či diferencovatelnost.

△

Díky asociativitě umíme zavést operaci i pro více prvků a také mocninu.

! **Definice.**
Nechť $(M,\circ)$ je pologrupa.
(i) Pro libovolné $n\in\mathbb{N}$ a $x_1,\dots,x_n\in M$ definujeme $x_1\circ\cdots\circ x_n$ rekurzivním vzorcem
(0) $x_1 = x_1$;
(1) $x_1\circ\cdots\circ x_n\circ x_{n+1} = (x_1\circ\cdots\circ x_n)\circ x_{n+1}$ pro $n\in\mathbb{N}$.
(ii) Pro libovolné $n\in\mathbb{N}$ a $x\in M$ definujeme mocninu x jako
(0) $x^1 = x$;
(1) $x^{n+1} = (x^n)\circ x$ pro $n\in\mathbb{N}$.
Úmluva: Mocnina má prioritu před operací $\circ$, není-li závorkou řečeno jinak.

Díky asociativitě má tato definice smysl a můžeme vynechávat závorky v opakovaných operacích. Například rekurzivním použitím definice získáme

$$x_1\circ x_2\circ x_3\circ x_4 = (x_1\circ x_2\circ x_3)\circ x_4 = ((x_1\circ x_2)\circ x_3)\circ x_4$$

a teď už je operace $\circ$ aplikována vždy jen na dvojici prvků.

Pro začátečníka je mocnina zrádná, protože se podobá běžné mocnině, ale v skutečnosti je to jen zkratka pro opakování operace z uvažované pologrupy. Pokud například pracujeme v pologrupě $(\mathbb{N},+)$, pak výsledek výrazu 2^3 rozhodně není 8, ale je to $2+2+2=6$.

Mocnina je někdy velice užitečná, ale občas se chová zajímavě. V příkladě 8a.e jsme měli operaci gcd, pro celé číslo x pak máme

$$x^3 = x\circ_g x\circ_g x = (x\circ_g x)\circ_g x = \gcd(x,x)\circ_g x = x\circ_g x = \gcd(x,x) = x.$$

Indukcí se snadno dokáže, že $x^n = x$ pro všechna $x\in\mathbb{N}$, takže vlastně mocnina nic nedělá.

Teď si dokážeme pravidlo, které čtenář dobře zná z násobení čísel. Je to tedy typický příklad toho, o čem jsme mluvili v úvodu kapitoly, toto pravidlo platí obecně pro všechny asociativní operace.

! **Fakt 8a.2.**
Nechť $(M,\circ)$ je pologrupa a $x\in M$. Pak pro všechna $m,n\in\mathbb{N}$ platí:
(i) $x^m\circ x^n = x^{m+n}$,
(ii) $(x^m)^n = x^{mn}$.

Důkaz (poučný)**:** (i): Důkaz povedeme indukcí na n. Zvolme tedy pevné $m\in\mathbb{N}$ a dokážeme pro všechna $n\in\mathbb{N}$ následující $V(n)$: $(x^m)\circ(x^n) = x^{m+n}$.

(0) $(x^m)\circ(x^1) = (x^m)\circ x = x^{m+1}$ podle definice mocniny.

(1) Pro nějaké (libovolné) $n\in\mathbb{N}$ předpokládejme, že $(x^m)\circ(x^n) = x^{m+n}$. Pak pomocí vzorců z definice mocniny, asociativního zákona a indukčního předpokladu dostaneme

$$(x^m)\circ(x^{n+1}) = (x^m)\circ(x^n\circ x) = (x^m\circ x^n)\circ x = (x^{m+n})\circ x = x^{(m+n)+1} = x^{m+(n+1)}.$$

Vzhledem k prioritě mocniny byly některé závorky zbytečné, ale při práci v abstraktních prostorech je lepší být opatrný. Všichni jsme totiž zvyklí pracovat s reálnými čísly a běžnými operacemi a mnohé věci děláme skoro bez

přemýšlení, ale u pologrup vůbec nemusí platit. Je proto důležité si každý krok pečlivě rozmyslet, proč vlastně platí.

(ii): Důkaz se nejlépe dělá indukcí na n, použije se i výsledek z (i). Necháme to jako cvičení 8a.3.

□

Abychom se dostali k dalším zajímavým vlastnostem, potřebujeme přidat další z axiomů.

Definice.
Nechť $(M, \circ)$ je grupoid. Řekneme, že prvek $e \in M$ se nazývá **jednotkový prvek** či **identita** (**identity element**), jestliže pro všechna $x \in M$ platí $e \circ x = x \circ e = x$.

Je docela zajímavé, že nemusíme o grupoidu M nic předpokládat a stejně už bude platit, že pokud nějaký jednotkový prvek v M existuje, tak je jediný.

Fakt 8a.3.
Nechť $(M, \circ)$ je grupoid. Jestliže v M existují jednotkové prvky e, f, pak $e = f$.

Důkaz (poučný)**:** Použijeme nejprve to, že f je jednotkový prvek, a pak to, že i e je jednotkový prvek. Dostaneme $e = e \circ f = f$.

□

Podle definice můžeme takový prvek hledat u jakékoliv operace, ale opravdu zajímavé to začne být u pologrup.

Definice.
Nechť $(M, \circ)$ je grupoid. Řekneme, že je to **monoid**, jestliže je to pologrupa a má jednotkový prvek e. Značíme jej pak $(M, \circ, e)$.

Takže přidáváme, teď už se budeme dívat na struktury, které splňují axiomy (A1) a (A2) z definice grupy. Jestliže je dotyčná operace silně podobná sčítání a označená $+$ či podobně, pak se často jednotkový prvek značí také n či 0 a nazývá se **neutrální prvek**. Tady to ale raději dělat nebudeme, aby nebyl zmatek.

Zase si projdeme naše příklady, dá se čekat, že prořídnou.

Příklad 8a.l (pokračování 8a.a)**:**
1) Asi nepřekvapí, že $(\mathbb{R}, +, 0)$ a $(\mathbb{R}, \cdot, 1)$ jsou monoidy, protože vždy platí $x+0 = 0+x = x$ a také $x \cdot 1 = 1 \cdot x = x$.

Teď už ale musíme být opatrní při přechodu k podpologrupám. Například $(\mathbb{N}, \cdot, 1)$ monoid je (obsahuje jednotkový prvek 1), zato $(\mathbb{N}, +)$ už monoid není, protože ztratil jednotkový prvek sčítání 0. Napravíme to například takto: $(\mathbb{N}_0, +, 0)$ je monoid.

Podobně vidíme, že zatímco $(n\mathbb{Z}, +, 0)$ monoidy jsou, protože obsahují jednotkový prvek pro sčítání, s násobením už to fungovat nebude, protože jestliže zvolíme $n > 1$, tak už jednotkový prvek 1 pro násobení nebude v množině $n\mathbb{Z}$. Pak je struktura $(n\mathbb{Z}, \cdot)$ pologrupa, ale ne monoid.

2) Je snadné si rozmyslet, že $(\mathbb{R}^n, +, 0_n)$ je monoid, podobně je i $(\mathbb{R}^n, \circ, 1_n)$ monoid, kde 1_n používáme pro vektor složený ze samých jedniček. Ukážeme to pro $n = 2$: Pro libovolné $(u, v) \in \mathbb{R}^2$ platí

$$(u, v) \circ (1, 1) = (u \cdot 1, v \cdot 1) = (u, v), \qquad (1, 1) \circ (u, v) = (1 \cdot u, 1 \cdot v) = (u, v).$$

3) Připomeňme množinu $M_{m\times n}$ reálných matic. Z lineární algebry víme, že nulová matice $m \times n$ (označíme ji $0_{m\times n}$) je jednotkový prvek pro $(M_{m\times n}, +)$, zatímco jednotková matice E_n je jednotkový prvek pro $(M_n, \cdot)$.

4) Konstantní polynom $p_0(x) = 0$ je jednotkovým prvkem pro $(P, +)$, zatímco konstantní polynom $p_1(x) = 1$ je jednotkovým prvkem pro $(P, \cdot)$.

△

K problematice ztráty jednotkového prvku se po příkladech vrátíme blíže.

Příklad 8a.m (pokračování 8a.b)**:**
V kapitole 7 jsme ukázali (a používali), že $(\mathbb{Z}_n, +, 0)$ a $(\mathbb{Z}_n, \cdot, 1)$ jsou monoidy. Budou to naše oblíbené příklady.
△

Příklad 8a.n (pokračování 8a.c)**:** Nechť U je libovolná množina, víme, že $(P(U), \cap)$ a $(P(U), \cup)$ jsou pologrupy. Ukážeme, že oba jsou i monoidy. Pro první je jednotkovým prvkem množina U, neboť pro libovolnou podmnožinu $A \subseteq U$ platí $A \cap U = U \cap A = A$. Pro tu druhou je jednotkovým prvkem množina $\emptyset$.
△

Příklad 8a.o (pokračování 8a.d)**:**

1) Zde uvažujeme množinu M všech zobrazení z A do A. Fakt 2b.2 říká, že $(M, \circ, i_A)$ je monoid.

Protože je i_A prosté, na a bijekce, budou i množina všech prostých zobrazení, množina všech zobrazení na a množina všech bijekcí s operací skládání monoidy.

2) Podobně díky Faktu 3c.1 víme, že relace $\Delta(A)$ poslouží jako jednotkový prvek pro množinu M všech relací na A a skládání.

3) Konstantní funkce $f_0(x) = 0$ je jednotkovým prvkem pro funkce vzhledem ke sčítání, zatímco konstantní funkce $f_1(x) = 1$ je jednotkovým prvkem pro násobení funkcí. Tyto dvě funkce jsou samozřejmě i spojité a spojitě diferencovatelné, takže vidíme, že i struktury $(F(I), +, f_0)$, $(F(I), \cdot, f_1)$, $(C(I), +, f_0)$, $(C(I), \cdot, f_1)$, $(C^1(I), +, f_0)$ a $(C^1(I), \cdot, f_1)$ jsou monoidy.

Podobně je monoidem $(F, +, f_0)$ a $(F, \cdot, f_1)$.

Jak je tomu se skládáním funkcí? Snadno se rozmyslí, že lineární funkce $i_{\mathbb{R}}(x) = x$ vyhovuje požadavkům (viz Fakt 2b.2), je také spojitá a spojitě diferencovatelná, takže $(F(\mathbb{R}), \circ, i_{\mathbb{R}})$, $(C(\mathbb{R}), \circ, i_{\mathbb{R}})$, $(C^1(\mathbb{R}), \circ, i_{\mathbb{R}})$ a $(F, \circ, i_{\mathbb{R}})$ jsou rovněž monoidy.

△

Příklad 8a.p (pokračování 8a.e)**:** Zde jsme pracovali s operacemi $x \circ_l y = \mathrm{lcm}(x, y)$ a $x \circ_g y = \gcd(x, y)$ na $\mathbb{N}$.

Je snadné si rozmyslet, že $(\mathbb{N}, \circ_l, 1)$ je monoid, ale pro operaci největšího společného dělitele jednotkový prvek nenajdeme. Proč? Zkusíme-li libovolného kandidáta n, pak největším společným dělitelem čísel n a $x = 2n$ je n, tedy $n \circ_g x = n$ a neplatí $n \circ_g x = x$. Toto číslo n tedy jako jednotkový prvek sloužit nemůže.

△

Příklad 8a.q (pokračování 8a.f)**:**

1) Zkusme najít jednotkový prvek e pro operaci „blíž ke 13“. Musí splňovat $e \circ_{13} x = x$, ale výsledek této operace je bližší z čísel e, x ke třináctce, což znamená, že aby to fungovalo, muselo by číslo e být dál od 13 než všechna čísla z $M = \mathbb{R}$. Takové číslo ale neexistuje, tento příklad tedy není monoid.

Zajímavá finta: Uvažujme nějaký konečný interval okolo 13, třeba interval $I = \langle 2, 23\rangle$. Protože je výsledkem operace $x \circ_{13} y$ vždy jedno z čísel x, y, bude libovolná podmnožina $\mathbb{R}$ (i ta naše) uzavřená na tuto operaci. To znamená, že pro libovolnou (neprázdnou) podmnožinu $N \subseteq \mathbb{R}$ je $(N, \circ_{13})$ pologrupa. Zkusme se teď podívat na tu naši I.

Nejvzdálenější bod této množiny od 13 je 2. To znamená, že libovolné jiné číslo x z I je blíže, proto podle definice $x \circ_{13} 2 = 2 \circ_{13} x = x$. No a pro $x = 2$ máme $2 \circ_{13} 2 = 2$. Vidíme tedy, že $(I, \circ_{13}, 2)$ je monoid.

Tento příklad ukazuje, že opravdu děláme velice abstraktní teorii, do které se vejde ledasjaká šílenost.

Zkuste si rozmyslet, že monoidem bude libovolná $(N, \circ_{13})$ taková, že N je nějaká omezená podmnožina $\mathbb{R}$, jejíž supremum a infimum nejsou stejně vzdáleny od 13, přičemž ten vzdálenější z nich musí být v N (bude dělat jednotkový prvek).

2) Interakce genů pro barvu očí obsahuje také rovnosti $b \circ H = H$, $H \circ b = H$ a $b \circ b = b$, což ukazuje, že $(\{b, H\}, \circ, b)$ je monoid.

△

Monoidy jsou docela populární v computer science, například v teorii konečných automatů nebo v teorii jazyků.

Příklad 8a.r: Připomeňme si příklad 5b.g, kde jsme definovali slova Σ^* nad abecedou Σ. Slova se spojují tak, že se prostě dají za sebe, operace se jmenuje konkatenace a značí $x * y$, popřípadě prostě xy. Například konkatenací slov „mate“ a „matika“ je „matematika“. Snadno se ukáže, že jde o asociativní operaci, prázdný řetězec λ pak slouží jako jednotkový prvek. Dostáváme tedy monoid.

△

Vraťme se k problému s přechodem k podmnožině. U pologrup stačilo vyžadovat uzavřenost podmnožiny na operaci a již vznikla pologrupa. Jak to funguje u monoidů? Tam máme o problém víc, musíme se postarat o jednotkový prvek. Co když přejdeme na podmnožinu a jednotkový prvek vynecháme? Kupodivu to může být pořád monoid, pokud se mu podaří najít si nějaký vlastní jednotkový prvek. Jak je to možné? Přechodem na menší množinu se sníží nároky na jednotkový prvek v definici (musí obhospodařit méně prvků), tudíž je naděje, že bude fungovat i prvek, který by v původní množině někde selhával.

Příklad 8a.s (pokračování 8a.a 2)**:** Uvažujme klasickou množinu $\mathbb{R}^2 = \{(x, y);\ x, y \in \mathbb{R}\}$ dvojrozměrných vektorů s naší operací násobení $(u, v) \circ (x, y) = (ux, vy)$. Víme, že $(\mathbb{R}^2, \circ, (1, 1))$ je monoid.

Teď uvažujme podmnožinu $M = \{(x, 0);\ x \in \mathbb{R}\}$ (osa x). Hned vidíme, že je na operaci $\circ$ uzavřená, protože

$$(u, 0) \circ (x, 0) = (u \cdot x, 0 \cdot 0) = (ux, 0) \in M.$$

Je to tedy pologrupa, ale původní jednotkový prvek $(1, 1)$ v ní není. Teď se ovšem podívejme na toto:

$$(u, 0) \circ (1, 0) = (u \cdot 1, 0 \cdot 0) = (u, 0), \qquad (1, 0) \circ (u, 0) = (1 \cdot u, 0 \cdot 0) = (u, 0).$$

Vidíme, že $(M, \circ, (1, 0))$ je monoid, s jiným jednotkovým prvkem, který ovšem v původním $\mathbb{R}^2$ nefungoval vždy správně a proto jím tam nebyl.

△

Je zajímavé si rozmyslet, že tím nedochází ke sporu s Faktem 8a.3, spíš ho to zajímavě ilustruje. Představme si, že máme monoid $(M, \circ, e)$ a uvažujeme jeho podmnožinu N. Kdybychom v podmnožině N původní jednotkový prvek ponechali, tak už si to N svůj vlastní najít nemůže, protože tím by v N byly dva různé a byl by spor s dotyčným Faktem. Teprve tím, že původní e z N odebereme, mu otevíráme dvířka k tomu, aby si našlo své vlastní f, to ale zase podle Faktu nemůže být jednotkovým prvkem v M.

V matematice je ovšem taková změna jednotkového prvku nepříjemná, protože vlastně jde o jinou strukturu, zpřetrhá se tím spojení s původním světem. Pak už se ani nedá čekat, že by se dědily původní vlastnosti, čímž nás to přestane zajímat. Proto budeme trvat v definici podmonoidu na tom, že i menší množina používá původní e.

Definice.
Nechť $(M, \circ, e)$ je monoid a $N \neq \emptyset$ je podmnožina M. Řekneme, že N je **podmonoid** $(M, \circ, e)$, jestliže $e \in N$ a $(N, \circ, e)$ je monoid.

Pomocí Věty 8a.1 dokážeme následující:

Věta 8a.4.
Nechť $(M, \circ, e)$ je monoid a $N \neq \emptyset$ je podmnožina M. Pak je N podmonoid $(M, \circ, e)$ právě tehdy, když $e \in N$ a N je uzavřená na $\circ$.

Důkaz (rutinní)**:** 1) $\Longrightarrow$: Jestliže je $(N, \circ, e)$ podmonoid, pak $e \in N$ už z definice, navíc je $(N, \circ)$ pologrupa a tudíž podle Věty 8a.3 musí být N uzavřená na $\circ$.

2) $\Longleftarrow$: Protože je N uzavřená na $\circ$, je podle Věty 8a.3 $(N, \circ)$ pologrupa. Zbývá ukázat, že prvek $e \in N$ je v ní jednotkový. To je ale jasné, protože prvky z N jsou i prvky z M a operace je stejná, tedy pro $x \in N$ platí $e \circ x = x \circ e = x$.

□

Takže můžeme snadno vyrábět spousty monoidů z těch základních známých, když si dáme pozor, jaké podmnožiny bereme. Například $\mathbb{N}$ je podpologrupa $(\mathbb{Z}, +, 0)$, ale není to podmonoid, protože jsme vynechali nulový prvek. $\mathbb{N}_0$ už podmonoid je, tedy $(\mathbb{N}_0, +, 0)$ je monoid.

Teď si uvedeme další pojem. Inspiraci najdeme u násobení, pro které je 1 jednotkový prvek. Ve výpočtech se často hodí, že k číslu x dokážeme (většinou) najít číslo $\frac{1}{x}$, jehož klíčovou vlastností je $x \cdot \frac{1}{x} = 1$.

! **Definice.**
Nechť $(M, \circ, e)$ je monoid. Řekneme, že prvek $x \in M$ je **invertibilní** (**invertible**), jestliže existuje $y \in M$ takové, že $x \circ y = y \circ x = e$.

Matematika hned zajímá, kolik takových y k invertibilnímu x najdeme.

! **Fakt 8a.5.**
Nechť $(M, \circ, e)$ je monoid, nechť $x \in M$ je invertibilní. Předpokládejme, že $y_1, y_2 \in M$ splňují $x \circ y_1 = y_1 \circ x = e$ a $x \circ y_2 = y_2 \circ x = e$. Pak $y_1 = y_2$.

Důkaz (poučný)**:** Využijeme obě vlastnosti a také asociativitu.

$$y_1 = y_1 \circ e = y_1 \circ (x \circ y_2) = (y_1 \circ x) \circ y_2 = e \circ y_2 = y_2.$$

Důkaz je hotov.

□

Víme tedy, že takové prvky jsou jedinečné, proto pro ně můžeme zavést rozumné značení.

! **Definice.**
Nechť $(M, \circ, e)$ je monoid a $x \in M$ je invertibilní prvek. Pak se prvku $y \in M$ splňujícímu $x \circ y = y \circ x = e$ říká **inverzní prvek** k x a značí se x^{-1}

Abychom ušetřili závorky, dohodneme se, že inverze prvku má vždy **prioritu** před operací $\circ$, není-li závorkou řečeno jinak.

Pokud nějaký autor pracuje s operací, která se chová jako sčítání, značí ji $+$ či podobně a používá názvu neutrální prvek, pak většinou také inverzní prvek značí $(-x)$ a říká mu prvek opačný. Aby v tom nebyl zmatek, zde to dělat nebudeme (s výjimkou kapitoly 8c).

Než se podíváme na příklady, stojí za to se vrátit k předchozímu Faktu. Pozorné čtení důkazu ukáže, že vlastně stačí, aby jeden prvek fungoval zleva (byl „levou inverzí“) a druhý zprava (byl „pravou inverzí“), a už dostáváme, co potřebujeme.

Věta 8a.6.
Nechť $(M, \circ, e)$ je monoid. Jestliže pro $x \in M$ existují prvky $y_1, y_2 \in M$ takové, že $y_1 \circ x = e$ a $x \circ y_2 = e$, pak je x invertibilní a $y_1 = y_2 = x^{-1}$.

Důkaz (poučný)**:** Předpoklady této věty jsou přesně to, co je třeba, aby platil výpočet v předchozím důkazu. Máme tedy $y_1 = y_2$, nazvěme tento prvek y. Když jej pak ale dosadíme do předpokladů místo y_1 a y_2, dostáváme $y \circ x = e = x \circ y$, tedy x je invertibilní a $x^{-1} = y$.

□

Je důležité si všimnout, že „inverze z jedné strany“, třeba levá, ještě nic neznamená. Klidně se může stát, že pro $x \in M$ najdeme prvek y takový, že $y \circ x = e$, ale x je přitom neinvertibilní. Jeden takový příklad ukážeme níže v příkladu 8a.v.

Když ale již dopředu víme, že je prvek invertibilní, pak stačí ověřit jen jednu z rovností, abychom věděli, že jsme našli prvek k němu inverzní.

Fakt 8a.7.
Nechť $(M, \circ, e)$ je monoid. Jestliže je $x \in M$ invertibilní a $y \in M$ splňuje $y \circ x = e$ nebo $x \circ y = e$, pak $y = x^{-1}$.

Důkaz (rutinní)**:** Předpokládejme, že y splňuje $y \circ x = e$. Protože je x invertibilní, pak máme také prvek splňující $x \circ x^{-1} = e$, tudíž podle Věty 8a.6 platí $y = x^{-1}$. Druhá možnost se dokáže stejně.

□

Kolik máme v monoidu invertibilních prvků? Vždy alespoň jeden.

Fakt 8a.8.
Nechť $(M, \circ, e)$ je monoid. Pak e je invertibilní a $e^{-1} = e$.

Důkaz hned plyne z definice e a definice inverzního prvku. Hledáme x tak, aby $x \circ e = e \circ x = e$, prvek $x = e$ vyhovuje.

Teď se již podívejme na příklady. Uvidíme, že některé monoidy v počtu invertibilních prvků s bídou přeskočí laťku nasazenou již tak nízko tímto faktem, zatímco v jiných jsou invertibilní prvky všechny.

! **Příklad 8a.t** (pokračování 8a.a)**:**
1) V monoidu $(\mathbb{R}, +, 0)$ má každý prvek x svou inverzi $-x$, protože pro libovolné x platí $x + (-x) = (-x) + x = 0 = e$.

Naopak v monoidu $(\mathbb{R}_0^+, +, 0)$ je jediným invertibilním prvkem 0 s $-0 = 0$, protože jsme vynechali záporná čísla.

V monoidu $(\mathbb{R},\cdot,1)$ jsou invertibilní všechny prvky $x\neq 0$ a jejich inverze je $x^{-1}=\frac{1}{x}$, neboť pro libovolné nenulové x platí $x\cdot\frac{1}{x}=\frac{1}{x}\cdot x=1=e$.

V monoidu $(\mathbb{N},\cdot,1)$ je jediný invertibilní prvek, a to povinný $x=1$. Podobně v monoidu $(\mathbb{N}_0,+,0)$ je jediný invertibilní prvek $x=0$.

Zajímavější je monoid $(\mathbb{Z},\cdot,1)$, kde jsou invertibilní prvky dva, $x=1$ a $x=-1$, pokaždé $x^{-1}=x$. Jiné tam nenajdeme, pro $x=0$ máme pro libovolného kandidáta y výsledek $xy=0$, takže inverze nejde. Pokud $x\neq 0,\pm 1$, pak $|x|\geq 2$, proto pro libovolné $y\in\mathbb{Z}$ máme buď $xy=0$ pro $y=0$, nebo máme $|xy|=|x|\cdot|y|\geq|x|\geq 2$, takže k jedničce se neostaneme.

2) I v monoidu $(\mathbb{R}^n,+,0)$ má každý prvek x svou inverzi $-x$, protože pro libovolné x platí $x+(-x)=(-x)+x=0_n=e$, zde se sčítají vektory po souřadnicích.

U násobení vektorů po souřadnicích dle očekávání vadí nuly, tentokráte stačí byť jediná nulová souřadnice, aby již vektor nebyl invertibilní. Pokud jsou ale všechny x_i různé od nuly, tak $(x_1,x_2\ldots,x_n)^{-1}=\left(\frac{1}{x_1},\frac{1}{x_2}\ldots,\frac{1}{x_n}\right)$.

3) V monoidu $(M_{m\times n},+,0_{m\times n})$ má každá matice A inverzní prvek $-A$.

V monoidu $(M_n,\cdot,E_n)$ jsou invertibilní regulární matice, neboť pro ně $A\cdot A^{-1}=A^{-1}\cdot A=E_n$.

4) V prostoru polynomů $(P,+,p_0)$ má každý polynom p svou inverzi $-p$, zatímco v prostoru polynomů $(P,\cdot,p_1)$ mají svou inverzi jen nenulové konstantní polynomy $p(x)=a$, pro ně $p^{-1}(x)=\frac{1}{a}$.

△

! Příklad 8a.u (pokračování 8a.b)**:**

Z kapitoly 7 již víme, že v $(\mathbb{Z}_n,+)$ je to s invertibilními prvky jednoduché (jsou to všechny), zatímco v $(\mathbb{Z}_N,\cdot)$ je to zajímavé (jsou to jen taková a, kde $\gcd(a,n)=1$, a hledání a^{-1} dá trochu práce).

Jako příklad si ukážeme $(\mathbb{Z}_{14},\cdot)$, na který se budeme později odkazovat.

$\odot$	0	1	2	3	4	5	6	7	8	9	10	11	12	13
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13
2	0	2	4	6	8	10	12	0	2	4	6	8	10	12
3	0	3	6	9	12	1	4	7	10	13	2	5	8	11
4	0	4	8	12	2	6	10	0	4	8	12	2	6	10
5	0	5	10	1	6	11	2	7	12	3	8	13	4	9
6	0	6	12	4	10	2	8	0	6	12	4	10	2	8
7	0	7	0	7	0	7	0	7	0	7	0	7	0	7
8	0	8	2	10	4	12	6	0	8	2	10	4	12	6
9	0	9	4	13	8	3	12	7	2	11	6	1	10	5
10	0	10	6	2	12	8	4	0	10	6	2	12	8	4
11	0	11	8	5	2	13	10	7	4	1	12	9	6	3
12	0	12	10	8	6	4	2	0	12	10	8	6	4	2
13	0	13	12	11	10	9	8	7	6	5	4	3	2	1

Jednotkový prvek se pozná tak, že se v jeho řádku i sloupci zopakují po řadě všechny prvky (jako v záhlaví), což 1 splňuje.

Invertibilní prvky poznáme podle toho, že mají v řádku i sloupci někde jednotkový prvek, tedy jedničku. Pokud se podíváme na řádek takového prvku x, najdeme v něm jedničku a od ní se podíváme nahoru na hlavičku sloupce, najdeme tam x^{-1}.

Vidíme, že máme invertibilní prvky 1, kde $1^{-1}=1$ (to ostatně plyne z Faktu 8a.8), dále 3, kde $3^{-1}=5$ (kontrola: $3\cdot 5=15\equiv 1$ modulo 14), dále 5, kde je $5^{-1}=3$, dále 9, kde $9^{-1}=11$, také 11, kde $11^{-1}=9$ a nakonec 13, kde $13^{-1}=13$.

Všimněte si zajímavé věci. Začneme třeba s $x=9$, inverzní prvek je 11, a když se podíváme na inverzi k němu, dostaneme zase 9, situace je pěkně symetrická. Funguje to tak u všech dvojic v tomto příkladě a také obecně, za chvíli to dokážeme.

Všimněte si také, že třeba v třetím řádku vidíme zajímavou věc: $2\odot 7=0$. Na to nejsme zvyklí, aby se nám nenulové prvky násobily na nulu, ale jak vidíme, u monoidů (alespoň některých) si na něco takového zvyknout musíme. Existuje na to dokonce teorie, viz kapitola 8c.

△

! Příklad 8a.v (pokračování 8a.d)**:**

1) V monoidu všech zobrazení z množiny A do A se skládáním jsou invertibilní bijekce, inverzní prvky odpovídají inverzním zobrazením.

Zde se na chvíli zastavíme, abychom ilustrovali nebezpečí testování inverze pouze z jedné strany, viz diskuse po Větě 8a.6. Uvažujme zobrazení T a S z $\mathbb{N}$ do $\mathbb{N}$ dané těmito vzorci: $T(n)=n+1$ pro všechna $n\in\mathbb{N}$, zatímco $S(1)=1$ a $S(n)=n-1$ pro $n\geq 2$.

Pak pro každé $n\in\mathbb{N}$ platí $T(n)\geq 2$, proto $(S\circ T)(n)=S(T(n))=T(n)-1=(n+1)-1=n$. Máme tedy $S\circ T=i_{\mathbb{N}}$, ale přesto není S inverzním zobrazením k T, protože neplatí $T\circ S=i_{\mathbb{N}}$. Máme totiž $(T\circ S)(1)=T(S(1))=T(1)=2$.

2) U relací na A to není hned vidět, ale dá se rozmyslet, že i v monoidu všech relací na množině A jsou invertibilní právě ty relace, které jsou zároveň bijektivními zobrazeními.

3) V prostorech funkcí na I (všechny, spojité, spojitě diferencovatelné) jsou všechny funkce invertibilní vůči sčítání, přičemž $f^{-1} = -f$.

Vůči násobení jsou invertibilní jen funkce, které nejsou nikde na I nulové, pro ně $f^{-1} = \frac{1}{f}$.

V prostoru funkcí $F(\mathbb{R})$ se skládáním jsou invertibilní jen bijekce $\mathbb{R}$ na $\mathbb{R}$, pro ně je inverzním prvkem inverzní funkce.

Méně náročné je to v prostoru funkcí F, kde jsou invertibilní všechny prosté funkce. To je jeden z důvodů, proč jsme tuto komplikovanější množinu zaváděli, jsme totiž z matematické analýzy zvyklí invertovat prosté funkce. Například funkce arctg je prostá, má tedy v množině F inverzi, ale v množině $F(\mathbb{R})$ ji nemá, protože to není bijekce $\mathbb{R}$ na $\mathbb{R}$.

△

Příklad 8a.w (pokračování 8a.e)**:** Rozmysleli jsme si, že $\mathbb{N}$ s operací $\circ_l$ danou jako $\mathrm{lcm}(x, y)$ je monoid s $e = 1$. To je také jediný invertibilní prvek, protože pro libovolné $n > 1$ a libovolné $x \in \mathbb{N}$ platí $\mathrm{lcm}(n, x) \geq n > 1$, tedy nedokážeme z n vyrobit operací číslo 1.

△

Příklad 8a.x (pokračování 8a.f)**:**

1) Připomeňme si operaci $\circ_{13}$ určující číslo nejbližší k 13, kde jsme si rozmysleli, že na množině $I = \langle 2, 23\rangle$ spolu $e = 2$ je to monoid.

Jediným invertibilním prvkem je zde 2. Proč? Vezměme si libovolné jiné číslo $x \in I$ a hledejme k němu inverzní prvek. Ať už zkusíme jakékoliv y, tak je vždycky $x \circ_{13} y$ nejvýše tak daleko od 13, jako je x, tudíž to nikdy nemůže být 2, které je ze všech nejdále.

2) Připomeňme si tabulku monoidu genů pro barvy očí, kde je jednotkovým prvkem recesivní gen b. Pak je b automaticky invertibilní, zatímco H díky své dominanci invertibilní není, nikdy z něj nedostaneme b.

△

Jaké jsou základní vlastnosti platící pro inverzní prvky?

! **Věta 8a.9.**
Nechť $(M, \circ, e)$ je monoid.
(i) Jestliže je $x \in M$ invertibilní, pak je také jeho inverze x^{-1} invertibilní a $(x^{-1})^{-1} = x$.
(ii) Jestliže jsou $x, y \in M$ invertibilní, pak je také $x \circ y$ invertibilní a $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$.

Důkaz (rutinní)**:** (i) necháme jako cvičení 8a.4.

(ii): Hledáme prvek z takový, že $(x \circ y) \circ z = e$ a $z \circ (x \circ y) = e$. Dosazením a pomocí asociativního zákona ukážeme, že prvek $y^{-1} \circ x^{-1}$ toto splňuje:

$$(x \circ y) \circ (y^{-1} \circ x^{-1}) = x \circ (y \circ y^{-1}) \circ x^{-1} = x \circ e \circ x^{-1} = (x \circ e) \circ x^{-1} = x \circ x^{-1} = e.$$

Druhá rovnost se dokáže stejně.

□

Kdybychom začali skriptum touto kapitolou, tak jsme Větu 2b.6 ani Větu 3a.4 nemuseli dokazovat, plynuly by okamžitě z tvrzení (ii).

Invertibilní prvky jsou velice užitečné při řešení rovnic.

! **Fakt 8a.10.** (o krácení)
Nechť $(M, \circ, e)$ je monoid. Nechť prvky $c, x, y \in M$ splňují rovnici $c \circ x = c \circ y$ nebo rovnici $x \circ c = y \circ c$. Jestliže je c invertibilní, pak $x = y$.

Důkaz (rutinní)**:** Předpokládejme, že $c \circ x = c \circ y$. Pak

$$x = e \circ x = (c^{-1} \circ c) \circ x = c^{-1} \circ (c \circ x) = c^{-1} \circ (c \circ y) = (c^{-1} \circ c) \circ y = e \circ y = y.$$

Druhý případ se dělá obdobně, viz cvičení 8a.5.

□

Prvky, které nejsou invertibilní, pak v rovnicích krátit nemůžeme, což přináší komplikace, jak jsme to již viděli třeba v kapitole 7b.

Pomocí krácení se snadno dokáže jeden užitečný způsob, jak poznat jednotkový prvek:

Lemma 8a.11.
Nechť $(M, \circ, e)$ je monoid a $g \in M$ je invertibilní prvek. Jestliže $g^2 = g$, pak $g = e$.

Důkaz necháváme jako snadné cvičení 8a.6. Poznamenejme, že obecně z $g^2 = g$ nic neplyne, například v $(\mathbb{Z}_6, \cdot)$ máme $3^2 = 3$ (neboť $3 \cdot 3 = 9 \equiv 3 \pmod 6$), ale není to jednotkový prvek. Také tam ovšem 3 není invertibilní, proto se na něj naše Lemma nevztahuje.

Mocniny prvků jsme definovali pro pologrupy. V monoidech se tato definice dá rozšířit.

! **Definice.**
Nechť $(M, \circ, e)$ je monoid a $x \in M$. Definujeme **mocniny** následovně:
- pro $n \in \mathbb{N}$ definujeme x^n dle původní definice;
- pro $n = 0$ definujeme $x^0 = e$;
- jestliže je x invertibilní, pak pro $n \in \mathbb{N}$ definujeme $x^{-n} = (x^{-1})^n$.

Pořád platí, že je třeba být ostražitý. Například v monoidu $(\mathbb{Z}, +, 0)$ je operací sčítání, proto 2^{-1} je -2 a tudíž $2^{-3} = (2^{-1})^3 = (-2)^3 = (-2) + (-2) + (-2) = -6$. Stojí za zopakování, že x^n není běžná mocnina, ale symbol pro opakování operace $\circ$.

Je snadné ale pracné dokázat (musí se rozebrat všechny kombinace kladných, záporných a nulových exponentů), že vzorce pro mocninu stále platí:

! **Věta 8a.12.**
Nechť $(M, \circ, e)$ je monoid, nechť $x \in M$. Pak vzorce $(x^m) \circ (x^n) = x^{m+n}$ a $(x^m)^n = x^{mn}$ platí pro všechna $m, n \in \mathbb{N}_0$.
Jestliže je x invertibilní, pak tyto vzorce platí pro všechna $m, n \in \mathbb{Z}$.

Platí i další rozumné pravido.

! **Fakt 8a.13.**
Nechť $(M, \circ, e)$ je monoid, nechť $x \in M$ je invertibilní. Pak je invertibilní i x^n pro každé $n \in \mathbb{Z}$ a $(x^n)^{-1} = x^{-n}$.

Důkaz (rutinní)**:** 1) Nejprve to dokážeme pro $n \in \mathbb{N}$. Důkaz povedeme indukcí.

(0) Evidentně $(x^1)^{-1} = x^{-1}$.

(1) Předpokládejme, že pro nějaké $n \in \mathbb{N}$ je x^n invertibilní a $(x^n)^{-1} = x^{-n}$. Pak je podle Věty 8a.9 (ii) invertibilní i $x^n \circ x = x^{n+1}$ a podle téže věty je

$$(x^{n+1})^{-1} = (x^n \circ x)^{-1} = x^{-1} \circ (x^n)^{-1} = x^{-1} \circ (x^{-n}) = x^{-n-1} = x^{-(n+1)}.$$

2) Pro $n = 0$ tvrzení evidentně platí, $(x^0)^{-1} = e^{-1} = e = e^{-0}$.

3) Jestliže je $n \in \mathbb{Z}$ a $n < 0$, pak $m = -n \in \mathbb{N}$. Připomeňme, že pro invertibilní prvek y se záporná mocnina definuje jako $(y^{-1})^{-n} = (y^{-1})^m$, budeme to dále aplikovat na x i x^{-1}.

Protože je x invertibilní, je podle Věty 8a.9 (i) invertibilní i x^{-1}, tudíž je podle části 1) tohoto důkazu invertibilní i $(x^{-1})^m = x^n$. Opět podle části 1) máme

$$(x^n)^{-1} = ((x^{-1})^m)^{-1} = (x^{-1})^{-m} = ((x^{-1})^{-1})^m = x^{-n}.$$

Důkaz je hotov.

□

! 8a.14 Mocniny

Mocniny prvku jsou zajímavý objekt. Zvolme si pevně prvek g z monoidu $(M, \circ, e)$ a začněme jej kombinovat samý se sebou, tedy uvažujme g, $g \circ g = g^2$, $g \circ g \circ g = g^3$, g^4, g^5, … Co se může stát? Jsou dvě možnosti.

a) U některých prvků tak dostaneme nekonečnou posloupnost $\{g^n\}_{n=1}^{\infty}$ *různých* prvků množiny M.

Například prvek 2 v monoidu $(\mathbb{Z}, +, 0)$ dává $2^1 = 2$, $2^2 = 2 + 2 = 4$, $2^3 = 2 + 2 + 2 = 6$, snadno se nahlédne, že 2^n (ve smyslu mocniny monoidu) je číslo $2n$.

b) U jiných prvků se stane, že se nějaký prvek po čase zopakuje, tedy pro jisté n se najde menší k takové, že $g^n = g^k$. Pak se již nic nového nestane a pořád dokola se budou opakovat prvky $g^k, g^{k+1}, \ldots, g^{n-1}$, protože $g^{n+1} = g^n \circ g = g^k \circ g = g^{k+1}$, $g^{n+2} = g^n \circ g^2 = g^k \circ g^2 = g^{k+2}$ a tak dále.

Příklad 8a.y: Zajímavé případy nabízí $(\mathbb{Z}_{12}, \cdot, 1)$.

Mocniny prvku $g = 3$ se zacyklí na začátek: $3^1 = 3$, $3^2 = 3 \cdot 3 = 9$, $3^3 = 9 \cdot 3 = 27 \bmod 12 = 3$, zacyklili jsme se, pak $3^4 = 3^3 \cdot 3 = 3 \cdot 3 = 9$, atd. Dostáváme řetízek $3 \mapsto 9 \mapsto 3 \mapsto 9 \mapsto \dots$.

Mocniny prvku $g = 2$ se na začátek nevrátí: $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 4$, $2^5 = 8$ atd., tedy máme $2 \mapsto 4 \mapsto 8 \mapsto 4 \mapsto 8 \mapsto \dots$

To zacyklení může být extrémně krátké: $g = 4$ má mocniny $4 \mapsto 4 \mapsto 4 \mapsto \dots$. Lze k tomu dorazit i později: $g = 6$ nabízí mocniny $6 \mapsto 0 \mapsto 0 \mapsto 0 \mapsto \dots$.

Pro trochu delší řetězec se podíváme do monoidu $(\mathbb{Z}_{14}, \cdot, 1)$. Volba $g = 3$ dává $3^1 = 3$, $3^2 = 9$, $3^3 = 13$, $3^4 = 11$, $3^5 = 5$, $3^6 = 1$, $3^7 = 3$, vidíme cyklus $3 \mapsto 9 \mapsto 13 \mapsto 11 \mapsto 5 \mapsto 1 \mapsto 3 \mapsto \dots$

△

Případy, kdy cyklení začne později, nejsou až tak přínosné, mnohem raději máme prvky, u kterých se mocnina vrátí na začátek ke g. Ukážeme, že pro invertibilní prvky je to zaručeno, příklad výše nicméně ukazuje, že to není podmínka nutná. Měli jsme $g = 3 = g^3$, ale 3 není invertibilní v $\mathbb{Z}_{12}$. Následující tvrzení tedy bude mít formu implikace.

Fakt 8a.15.
Nechť $(M, \circ, e)$ je monoid, nechť $g \neq e$ je invertibilní prvek z M. Předpokládejme, že množina $A = \{n \in \mathbb{N};\ \exists k \in \{1, 2, \dots, n-1\}\colon g^n = g^k\}$ je neprázdná, a označme její nejmenší prvek jako m. Pak $g^m = g$.

Důkaz (poučný)**:** Protože $m \in A$, existuje $k \in \{1, 2, \dots, m-1\}$ takové, že $g^m = g^k$. Prvek g je invertibilní, tudíž můžeme podle Faktu 8a.13 najít také inverzní prvek g^{-k} k g^k. Pomocí tohoto prvku a rovnosti $g^m = g^k$ pak odvodíme, že

$$g^{m-k+1} = [g^m \circ g^{-k}] \circ g = [g^k \circ ((g^k)^{-1})] \circ g = e \circ g = g.$$

To znamená, že se mocnina g^{m-k+1} zacyklila k předchozí množině, a tedy $m - k + 1$ leží v množině A. Zároveň je m její nejmenší prvek, což je možné jen tehdy, když $k = 1$, tedy $g^m = g^k$ je vlastně $g^m = g$, přesně jak jsme potřebovali dokázat.

□

Všimněte si, že pak $g^{m-1} = g^m \circ g^{-1} = g \circ g^{-1} = e$. Invertibilní prvky, které se cyklí, se tedy o mocninu dříve dostanou k e, jak ostatně ukázal případ $g = 3$ v $(\mathbb{Z}_{14}, \cdot, 1)$. To nám umožňuje udělat následující definici:

! **Definice.**
Nechť $(M, \circ, e)$ je monoid a $g \in M$ je invertibilní prvek. Definujeme **řád** (**order**) prvku g, značeno $\mathrm{ord}(g)$, jako nejmenší prvek množiny $\{n \in \mathbb{N};\ g^n = e\}$, jestliže je neprázdná, jinak definujeme $\mathrm{ord}(g) = \infty$.

Řád se také někdy značí $|g|$, ale raději to nebudeme používat, ať se to neplete s absolutní hodnotou. Snadno se nahlédne, že v každém monoidu je $\mathrm{ord}(e) = 1$. Je to jediný takový prvek, je to vidět přímo z definice, $\mathrm{ord}(g) = 1$ znamená, že $g^1 = e$ neboli $g = e$. Z našich příkladů vidíme, že v monoidu $(\mathbb{Z}, +, 0)$ je $\mathrm{ord}(2) = \infty$ a v $(\mathbb{Z}_{14}, \cdot, 1)$ je $\mathrm{ord}(3) = 6$.

Teď jsme připraveni na jednu užitečnou větu.

! **Věta 8a.16.**
Nechť $(M, \circ, e)$ je monoid a $g \in M$ je invertibilní prvek takový, že $\mathrm{ord}(g) < \infty$. Pak platí následující:
(i) Pro $n \in \mathbb{Z}$ platí $g^n = e$ právě tehdy, když n je násobek $\mathrm{ord}(g)$.
(ii) Pro $m, n \in \mathbb{Z}$ platí $g^m = g^n$ právě tehdy, když $m - n$ je násobek $\mathrm{ord}(g)$.

Důkaz (poučný)**:** (i): Označme $o = \mathrm{ord}(g)$. Podle Věty 6a.6 existují čísla $r \in \mathbb{N}_0$ a $k \in \mathbb{Z}$ taková, že $n = ok + r$ a $r < o$, tedy $r = n \bmod o$ je zbytek po dělení n číslem o. Pak máme $e = g^n = g^{ok+r} = (g^o)^k \circ g^r = e^k \circ g^r = g^r$. Takže $g^r = e$, ale zároveň je o nejmenší přirozené číslo s touto vlastností a $r < o$. Jediná možnost, jak se vyhnout sporu, je $r = 0$, tedy $n = ko$.

(ii): Jestliže $g^m = g^n$, pak $e = g^m \circ (g^m)^{-1} = g^m \circ (g^n)^{-1} = g^m \circ g^{-n} = g^{m-n}$, podle (i) je tedy $m - n$ násobkem řádu.

Nechť naopak $m - n = ko$ pro nějaké $k \in \mathbb{Z}$. Pak podle (i) $g^{m-n} = e$ a $g^m = g^{n+m-n} = g^n \circ g^{m-n} = g^n \circ e = g^n$.

□

Teď uděláme další zajímavou věc, všechny mocniny včetně záporných sesypeme do jedné množiny.

! **Definice.**
Nechť g je nějaký invertibilní prvek v monoidu $(M, \circ, e)$. Definujeme **monoid generovaný prvkem** g jako množinu

$$\langle g \rangle = \{g^n;\ n \in \mathbb{Z}\}.$$

Díky našim předchozím zkoumáním už dobře víme, jak takový generovaný monoid vypadá. Pro prvky nekonečného řádu je to množina $\{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$, kde jsou všechny mocniny různé. Pro prvky konečného řádu je to množina $\{e, g, g^2, \dots, g^{\mathrm{ord}(g)-1}\}$.

Sice tomu říkáme „monoid generovaný“, ale ještě vlastně nevíme, že je to monoid. Hned to napravíme.

! **Věta 8a.17.**
Nechť $(M, \circ, e)$ je monoid a $g \in M$ nějaký invertibilní prvek. Pak $\langle g \rangle$ je podmonoid $(M, \circ, e)$.
Jestliže $\mathrm{ord}(g) < \infty$, pak $\langle g \rangle = \{e, g, g^2, \dots, g^{\mathrm{ord}(g)-1}\}$ a $|\langle g \rangle| = \mathrm{ord}(g)$.

Důkaz (rutinní)**:** Podle Věty 8a.4 musíme ukázat dvě věci. Jednak že $e \in \langle g \rangle$, ale to je snadné, $e = g^0$. Pak musíme ukázat uzavřenost na $\circ$, ale to je také snadné. Nechť $x, y \in \langle g \rangle$. Pak existují $k, l \in \mathbb{Z}$ takové, že $x = g^k$ a $y = g^l$, proto $x \circ y = g^k \circ g^l = g^{k+l} \in \langle g \rangle$.

Druhá část: Označme $N = \{e, g, g^2, \dots, g^{\mathrm{ord}(g)-1}\}$. Již z této definice platí $N \subseteq \{g^n;\ n \in \mathbb{N}\} = \langle g \rangle$. Teď ukážeme, že $\langle g \rangle \subseteq N$. Pro libovolné $n \in \mathbb{Z}$ vyjádříme $n = k\,\mathrm{ord}(g) + r$, kde $k \in \mathbb{Z}$ a $r \in \mathbb{N}_0$ je zbytek splňující $r < \mathrm{ord}(g)$. Pak je $n - r$ násobkem $\mathrm{ord}(g)$, proto dle Věty 8a.16 (ii) je $g^n = g^r \in N$. Rovnost množin dokázána.

Nakonec ukážeme, že vypsané prvky N jsou navzájem různé. I to plyne z Věty 8a.16 (ii) a z toho, že čísla $0 < m, n < \mathrm{ord}(g)$ splňují podmínku $m - n = k\,\mathrm{ord}(g)$ jen tehdy, když $m = n$. Tato množina má tedy $\mathrm{ord}(g)$ různých prvků.

□

Množinu $\langle g \rangle$ lze definovat i pro prvky, které nejsou invertibilní, ale pak už obecně nedostáváme podmonoid, takže to přestává být zajímavé. V příkladě výše jsme třeba viděli, že volba $g = 2$ v monoidu $(\mathbb{Z}_{12}, \cdot, 1)$ dává $\langle 2 \rangle = \{2, 4, 8\}$.

V poslední části této kapitoly se budeme věnovat zajímavému úkazu, když máme prvek g v monoidu $(M, \circ, e)$ a necháme jej působit prostřednictvím operace $\circ$ nikoliv na různé jednotlivé prvky, ale rovnou na celý kus množiny M. Inspirace pochází například z geometrie. Představme si nějaký útvar v rovině, třeba jistý kruh. Matematicky to znamená, že máme určitou množinu K vektorů. Teď si vezmeme ještě jiný vektor $\vec{v}$ a přičteme jej ke všem vektorům množiny K. Geometricky to znamená, že jsme celý kruh posunuli, přičemž směr a velikost posunu jsou dány vektorem $\vec{v}$.

Matematicky bychom tento posunutý kruh nazvali $\vec{v} + K$ a je dán jako $\vec{v} + K = \{\vec{v} + \vec{u};\ \vec{u} \in K\}$.

Tato operace je v geometrii často používaná, například z přímek procházejících počátkem (které jsou docela výjimečné, například tvoří podprostory) dostáváme ostatní přímky právě posunem.

Stejnou fintu lze provést i obecně, přičemž ale představa zůstává stejná, máme množinu objektů N, a když na všechny z nich provedeme operaci $\circ$ s účastí nějakého prvku g, tak jakoby množinu N posouváme.

Definice.
Nechť $(M, \circ, e)$ je monoid. Pro libovolnou podmnožinu $N \subseteq M$ a prvek $c \in M$ definujeme cN jako $\{c \circ x;\ x \in N\}$.

Klíčová otázka je, co se s takovou množinou po posunu stane. Geometrické posouvání z našeho inspiračního příkladu zachovává tvar i velikost, ale obecně nemá smysl o tvaru mluvit, zato otázka velikosti (u množin tedy mohutnosti) může mít velký význam. Zajímat nás někdy mohou i další vlastnosti.

Příklad 8a.z: Uvažujme $(\mathbb{R}^2, \cdot, 1_2)$, tedy pracujeme s dvourozměrnými vektory, které mezi sebou násobíme po souřadnicích, jak jsme vymysleli v příkladě 8a.a 2).

Zvolme nějakou množinu N v $\mathbb{R}^2$. Jak si představujeme $(2, -1)N$? Je to množina $\{(2, -1) \cdot (u, v);\ (u, v) \in N\} = \{(2u, -v);\ (u, v) \in N\}$. Geometricky to znamená, že jsme vzali útvar daný množinou N, přetočili okolo osy x, takže vznikl zrcadlový obraz, a pak jej roztáhli dvakrát ve směru osy x (oběma směry od počátku). V zásadě se dá říct, že základní tvar zůstal do velké míry zachován (protažení udělá ze čtverce kosodélník či z kružnice elipsu, ale hlavní prvky se nezmění), zůstala i dimenze tohoto útvaru (pokud byla N dvourozměrná, třeba bramboroid, tak i $(2, -1)N$ je pořád dvourozměrná) a rovněž mohutnost množiny je stejná.

Teď se podíváme na $(0,1)N = \{(0,y);\ (x,y) \in N\}$. Toto je takzvaná projekce na osu y, všechny body z množiny N jsme nahradili jejich nejbližšími sousedy z osy y. Pokud byla N trochu tučnější (třeba kruh), tak už výsledný útvar rozhodně nevypadá podobně, protože se celý nachází na ose y, z kruhu či čtverce by vznikla úsečka. Ztratili jsme tedy jednu dimenzi, útvar N se nám „posunem“ $(0,1)N$ podstatně změnil.

Ke stejnému jevu může docházet i v dalších monoidech. Uvažujme množinu $N = \{0,1,2,3,4,5\}$ v našem oblíbeném $(\mathbb{Z}_{12}, \cdot, 1)$. Pak $5N = \{0,5,10,3,8,1\}$, zde zůstala velikost zachována, zatímco $4N = \{0,4,8,0,4,8\} = \{0,4,8\}$, množina se smrskla na polovinu.

△

Mizení části množin je při posunech velice nepříjemné, tak se podíváme, kdy se toho nemusíme bát.

Věta 8a.18.
Nechť $(M, \circ, e)$ je monoid a $N \subseteq M$. Pro $c \in M$ definujme zobrazení $T\colon N \mapsto cN$ předpisem $T(x) = c \circ x$ pro $x \in N$. Jestliže je c invertibilní, pak je T bijekce.

Důkaz (poučný)**:** T je na: Vezměme libovolné $y \in cN$. Pak pro nějaké $x \in N$ platí $y = c \circ x$. Máme $x \in N$ a $T(x) = c \circ x = y$, tedy T je na.

T je prosté: Nechť pro $x, y \in N$ platí $T(x) = T(y)$. Pak $c \circ x = c \circ y$, c je invertibilní a podle Faktu 8a.10 tedy $x = y$.

□

Tato věta nám říká dvě věci. Jedna je, že pro invertibilní c mají množiny N a cN stejnou mohutnost, to ještě použijeme. Stejně užitečný bude i druhý poznatek: Pokud máme v monoidu dva různé prvky a vynásobíme je invertibilním prvkem, pak musí být výsledky rovněž různé (to nám říká prostota toho T).

Je zajímavé aplikovat závěr Věty přímo na samotnou množinu M. Pokud vezmeme invertibilní prvek $c \in M$, pak je cM zase množina M. Podívejme se do příkladu 8a.b na tabulku. Vidíme, že v řádcích u invertibilních prvků $1, 3, 5, 9, 11, 13$ se vždy opravdu vyskytnou všechny prvky $\mathbb{Z}_{14}$, bez opakování, jen někdy v jiném pořadí.

V závěru této kapitoly si spojíme dva posledně zkoumané pojmy, tedy $\langle g \rangle$ a cN. Opět něco pro inspiraci: Budeme pracovat v rovině, což je teď pro nás množina vektorů s operací sčítání. Typickým podmonoidem je tam přímka procházející počátkem. Jednu takovou si zvolme, nazvěme ji p. Už jsme si rozmysleli, že pro vektor $\vec{v}$ dává $\vec{v}p$ přímku p posunutou o vektor $\vec{v}$, ta je s tou původní rovnoběžná.

Všimněme si dvou věcí. Jedna je, že pokud provedeme dva takové posuny, neboli pokud uvažujeme $\vec{u}p$ a $\vec{v}p$, tak buď budou výsledné přímky totožné, nebo naopak disjunktní. To by mělo čtenáři připomenout situaci s třídami ekvivalence. Druhá věc je, že celý prostor dokážeme získat tak, že sjednotíme různé posuny této konkrétní přímky. To už opravdu zavání rozkladem a taky tam je, pod tímto povídáním je ve skutečnosti schovaná relace. Nás v této chvíli ale mnohem více zajímá, že to funguje úplně stejně i v obecných monoidech.

Věta 8a.19.
Nechť $(M, \circ, e)$ je monoid a $g \in M$ invertibilní prvek. Pak platí následující:
(i) Pro libovolné invertibilní $x \in M$ je zobrazení $T(g^k) = x \circ g^k$ bijekce z $\langle g \rangle$ na $x\langle g \rangle$. Proto také $|\langle g \rangle| = |x\langle g \rangle|$.
(ii) Pro každé $x \in M$ platí: $x\langle g \rangle = \langle g \rangle$ právě tehdy, když $x \in \langle g \rangle$.
(iii) Pro všechna $x, y \in M$ platí: $x\langle g \rangle = y\langle g \rangle$ právě tehdy, když $y = x \circ g^k$ pro nějaké $k \in \mathbb{Z}$.
(iv) Množina $\{x\langle g \rangle\}_{x \in M}$ je rozklad množiny M.

Důkaz (poučný)**:** (i) je vlastně Věta 8a.18.

(ii): Předpokládejme, že $x\langle g \rangle = \langle g \rangle$. Protože $e \in \langle g \rangle$, pak i $x = x \circ e \in x\langle g \rangle$ neboli $x \in \langle g \rangle$.

Nechť naopak $x \in \langle g \rangle$. Pak $x = g^n$ pro nějaké $n \in \mathbb{Z}$. Proto pro každé $x \circ g^k \in x\langle g \rangle$ máme $x \circ g^k = g^{n+k} \in \langle g \rangle$ a naopak pro každé $g^k \in \langle g \rangle$ máme $g^k = g^{n+k-n} = g^n \circ g^{k-n} = x \circ g^{k-n} \in x\langle g \rangle$.

(iii): Jestliže $y\langle g \rangle = x\langle g \rangle$, pak $y \in x\langle g \rangle$ a tedy $y = x \circ g^k$. Důkaz opačným směrem je podobný důkazu (ii).

(iv): Protože $x \in x\langle g \rangle$, evidentně platí $M = \bigcup_{x \in M} x\langle g \rangle$. Teď potřebujeme druhou podmínku.

Předpokládejme, že $x\langle g \rangle \cap y\langle g \rangle \neq \emptyset$. Pak najdeme prvek z takový, že $z = x \circ g^m$ a $z = y \circ g^n$ pro nějaká $m, n \in \mathbb{Z}$. Pak dostáváme

$$x = x \circ e = x \circ (g^m \circ g^{-m}) = (x \circ g^m) \circ g^{-m} = z \circ g^{-m} = (y \circ g^n) \circ g^{-m} = y \circ g^{n-m},$$

a podle (iii) je $x\langle g \rangle = y\langle g \rangle$.

□

Dostáváme docela zajímavý obrázek. Máme monoid $(M, \circ, e)$ a vybereme si invertibilní prvek g. Pak $\langle g \rangle$ dává podmnožinu M, která si s operací $\circ$ rozumí tak dobře, že sama tvoří monoid, je to tedy velice pěkný kousek množiny M. Množinu M pak dokážeme poskládat z posunů onoho pěkného kousku $\langle g \rangle$. Pokud se k posouvání používaly invertibilní prvky, tak dokonce všechny ty kousky mají stejný „tvar" jako původní $\langle g \rangle$. Tato představa je tak žádoucí, že se omezíme jen na tyto situace, což nás přinutí jít do další kapitoly.

Cvičení

Cvičení 8a.1 (rutinní, poučné, zkouškové)**:** Uvažujme následující grupoidy. Pro každý z nich rozhodněte, zda je $\circ$ asociativní (tedy zda je M pologrupa). Pokud ano, zjistěte, zda existuje jednotkový prvek. Pokud půjde o monoid, vyšetřete, které jeho prvky jsou invertibilní, a najděte předpis pro inverzní prvky.

(i) $M = \mathbb{Z}$, $x \circ y = x + y + 13$;
(ii) $M = \mathbb{R}$, $x \circ y = \sqrt{x^2 + y^2}$;
(iii) $M = \mathbb{R}$, $x \circ y = x^2 y$;
(iv) $M = \mathbb{Q}$, $x \circ y = |xy|$;
(v) $M = \mathbb{R} - \{0\}$, $x \circ y = \frac{1}{\frac{1}{x} + \frac{1}{y}}$ (takto se sčítají paralelní rezistory v obvodech);
(vi) $M = \mathbb{R}^2$, $(u, v) \circ (x, y) = (u + x, v \cdot y)$;
(vii) $M = \mathbb{Z}^2$, $(u, v) \circ (x, y) = (u + x, v \cdot y)$;
(viii) $M = \mathbb{Z}^2$, $(u, v) \circ (x, y) = (u^x, v + y)$;
(ix) $M = \mathbb{Q}^2$, $(u, v) \circ (x, y) = (uy, vx)$.

Cvičení 8a.2 (rutinní, poučné)**:** Nechť U je množina, zvolme pevně prvek $u \in U$. Ukažte, že následující množiny N jsou uzavřené na operace $\cap$ a $\cup$, viz příklad 8a.j.

(i) $N = \{X \subseteq U; u \in X\}$;
(ii) $N = \{X \subseteq U;\ u \notin X\}$.

Cvičení 8a.3 (dobré, poučné)**:** Dokažte, že když je x prvek v pologrupě $(M, \circ)$, pak pro všechna $m, n \in \mathbb{N}$ platí $(x^m)^n = x^{mn}$ (viz Fakt 8a.2).

Cvičení 8a.4 (rutinní, poučné)**:** Dokažte, že když je x invertibilní prvek v monoidu $(M, \circ, e)$, pak je invertibilní i x^{-1} a $(x^{-1})^{-1} = x$ (viz Věta 8a.9).

Cvičení 8a.5 (rutinní, poučné)**:** Nechť $(M, \circ, e)$ je monoid a prvky $c, x, y \in M$ splňují rovnici $x \circ c = y \circ c$. Dokažte, že jestliže je c invertibilní, pak $x = y$ (viz Fakt 8a.10).

Cvičení 8a.6 (rutinní, poučné)**:** Nechť $(M, \circ, e)$ je monoid a prvek $g \in M$ je invertibilní. Dokažte, že když $g^2 = g$, tak $g = e$.

Cvičení 8a.7 (rutinní)**:** Dokažte, že když je g prvek v monoidu $(M, \circ, e)$, pak pro $m, n \in \mathbb{N}$ platí $g^m \circ g^n = g^n \circ g^m$.

Řešení:

8a.1: (i): $(x \circ y) \circ z = (x + y + 13) \circ z = (x + y + 13) + z + 13 = x + y + z + 26$ a $x \circ (y \circ z) = x \circ (y + z + 13) = x + (y + z + 13) + 13 = x + y + z + 26$. Rovno, je asociativní.
Jednotka: rovnice $x \circ e = x$ dává $x + e + 13 = x$, tedy $e = -13$. Zkouška: $x \circ e = x \circ (-13) = x + (-13) + 13 = x$, $e \circ x = (-13) \circ x = (-13) + x + 13 = x$, ano, máme monoid.
Inverzní prvky: Dáno $x \in M = \mathbb{Z}$, hledáme $x \circ y = e$, tedy $x + y + 13 = -13$. Řešení: $y = -26 - x$. Závěr: Všechny prvky jsou invertibilní, $x^{-1} = -x - 26$.
(ii): $(x \circ y) \circ z = \sqrt{x^2 + y^2} \circ z = \sqrt{x^2 + y^2 + z^2}$, $x \circ (y \circ z) = x \circ \sqrt{y^2 + z^2} = \sqrt{x^2 + y^2 + z^2}$, rovno. Rovnice $x \circ e = x$ dá po umocnění $e = 0$, ale to bohužel není řešením, protože pro $x < 0$ to neřeší původní rovnici. Je totiž jasné, že pro x záporné se k němu nemůžeme dostat pomocí odmocniny. Jednotkový prvek tedy není.
Kdybychom pozměnili zadání úlohy a uvažovali dotyčnou operaci na $\mathbb{R}_0^+$, pak už by $e = 0$ bylo identitou. Jak by pak tomu bylo s inverzními prvky? Žádné $x > 0$ není invertibilní, protože pro libovolné y platí $x \circ y = \sqrt{x^2 + y^2} \geq |x| > 0$.
(iii): Není asociativní, $(x \circ y) \circ z = x^4 y^2 z$, zatímco $x \circ (y \circ z) = x^2 y^2 z$. Protipříklad: třeba $x = 2$, $y = 1$, $z = 1$, aby byl vidět rozdíl mezi těmi dvěma vzorci, pak $(2 \circ 1) \circ 1 = 4 \circ 1 = 16$, zatímco $2 \circ (1 \circ 1) = 2 \circ 1 = 4$.
(iv): Je asociativní, $(x \circ y) \circ z = |xy| \circ z = ||xy|z| = |xyz| = x \circ (y \circ z)$.
Nemá jednotkový prvek, pro $x = -1$ hledáme e takové, aby $x \circ e = x$, tedy $|-e| = -1$, což nelze. Není to monoid.
(v): Kupodivu asociativní, $(x \circ y) \circ z = \frac{1}{\frac{1}{x} + \frac{1}{y}} \circ z = \frac{1}{\frac{1}{x} + \frac{1}{y} + \frac{1}{z}} = x \circ (y \circ z)$.
Jednotkový prvek e by musel splňovat $x = \frac{1}{\frac{1}{x} + \frac{1}{e}}$, tedy $\frac{1}{e} = 0$, takový není. Neexistuje tedy rezistor s odporem, který by při paralelním zapojení nic nezměnil. Pokud bychom ale povolili $e = \infty$, už by to fungovalo, takže dát jako paralelní rezistor s nekonečným odporem (třeba rozstřihnutý drát) dá původní odpor.
(vi): $[(s, t) \circ (u, v)] \circ (x, y) = (s + u, tv) \circ (x, y) = (s + u + x, tvy)$ a $(s, t) \circ [(u, v) \circ (x, y)] = (s, t) \circ (u + x, vy) = (s + u + x, tvy)$. Rovno, je asociativní.

Identita: $(x,y)\circ(e_1,e_2)=(x,y)$ dává $x+e_1=x$ a $ye_2=y$ pro všechna x,y, vyhovuje $e_1=0$ a $e_2=1$. Kontrola: $(x,y)\circ(0,1)=(0,1)\circ(x,y)=(x,y)$.
Inverze: dáno (x,y), chceme $(x+u,yv)=(0,1)$. Pak $u=-x$ a $v=\frac{1}{y}$, pokud to jde. Závěr: pro $y\neq 0$ je (x,y) invertibilní a $(x,y)^{-1}=\left(-x,\frac{1}{y}\right)$.
(vii): Asociativita a jednotkový prvek viz (vi).
Inverze: dáno (x,y), chceme $(x+u,yv)=(0,1)$. Pak $u=-x$ a $v=\frac{1}{y}$, pokud to jde. Závěr: pro $y=\pm1$ je (x,y) invertibilní a $(x,y)^{-1}=(-x,y)$.
(viii): $[(s,t)\circ(u,v)]\circ(x,y)=(s^u,t+v)\circ(x,y)=((s^u)^x,t+v+y)$ a $(s,t)\circ[(u,v)\circ(x,y)]=(s,t)\circ(u^x,v+y)=(s^{u^x},t+v+y)$. Není to stejné, protože $(s^u)^x=s^{ux}$ se liší od $s^{(u^x)}$, takže není asociativní, protipříklad vyrobíme snadno pomocí té mocniny. Třeba $[(2,0)\circ(2,0)]\circ(3,0)=(4,0)\circ(3,0)=(64,0)$, zatímco $(2,0)\circ[(2,0)\circ(3,0)]=(2,0)\circ(8,0)=(256,0)$.
(ix): $[(s,t)\circ(u,v)]\circ(x,y)=(sv,tu)\circ(x,y)=(svy,tux)$ a $(s,t)\circ[(u,v)\circ(x,y)]=(s,t)\circ(uy,vx)=(svx,tuy)$. Není to stejné, takže není asociativní, protipříklad vyrobíme snadno, musíme odlišit x a y, třeba $[(1,1)\circ(1,1)]\circ(1,2)=(1,1)\circ(1,2)=(2,1)$, zatímco $(1,1)\circ[(1,1)\circ(1,2)]=(1,1)\circ(2,1)=(1,2)$.
8a.2: (i): $A,B\in N \implies A,B\subseteq U\wedge u\in A\wedge u\in B$. Pak $A\cap B\subseteq U\wedge u\in A\cap B$, tedy $A\cap B\in N$.
Pro *cup* a (ii) obdobně.
8a.3: Indukce na n, (1) $(x^m)^{n+1}=(x^m)^n\circ(x^m)=x^{mn}\circ x^m=x^{mn+m}=x^{m(n+1)}$.
8a.4: Ověřte, že $y=x$ splňuje podmínku $x^{-1}\circ y=y\circ x^{-1}=e$.
8a.5: $x=x\circ e=x\circ(c\circ c^{-1})$ tak dále.
8a.6: Napište si to jako $g\circ g=g\circ e$ a použijte vhodný Fakt.
8a.7: Využijte Fakt 8a.2.

8b. Grupy

Definice.
Monoid $(M,\circ,e)$ se nazývá **grupa**, jestliže je každý jeho prvek invertibilní.

Tím jsme se vrátili k původní definici s jejími axiomy (A1) až (A3). Abychom si to oddělili i graficky, budeme grupy značit G. Nejprve se podívejme na příklady. Projdeme si známé monoidy z předchozí kapitoly a zamyslíme se, jak to v nich chodí s invertibilními prvky.

Příklad 8b.a (pokračování 8a.a)**:**
1) Opačný prvek k číslu a vzhledem ke sčítání je $-a$. Je tedy jasné, že reálná čísla se sčítáním $(\mathbb{R},+,0)$ tvoří grupu, stejně jako vhodné podmnožiny, třeba $(\mathbb{Q},+,0)$ či $(\mathbb{Z},+,0)$. Naopak $(\mathbb{N}_0,+)$ grupu netvoří.

Grupami jsou také $(n\mathbb{Z},+,0)$ pro všechna $n\in\mathbb{N}$.

Žádné monoidy postavené na standardních číselných množinách a násobení nebudou grupy, máme problém s inverzí pro nulu, u celých čísel s inverzemi vůbec. Je tedy potřeba trochu množiny změnit. Podle Věty 8b.4 či selským rozumem dovodíme, že $(\mathbb{R}-\{0\},\cdot,1)$ je grupa, $(\mathbb{Q}-\{0\},\cdot,1)$ je grupa. To byl nejpřímočařejší způsob, zbavili jsme se problémového prvku. Jde to i jinak, například $(\mathbb{R}^+,\cdot,1)$ je grupa či $(\{-1,1\},\cdot,1)$ je grupa.

2) U vektorů je to podobné, $(\mathbb{R}^n,+,0_n)$ je grupa, zato u „našeho násobení“ $\cdot$ je problém s vektory s nulami. Vyhnout se jim umíme, například $((\mathbb{R}-\{0\})^n,\cdot,1_n)$ či $((\mathbb{R}^+)^n,\cdot,1_n)$ jsou grupy.

Rozmyslete si, že neprojde pokus $(\mathbb{R}^n-\{0_n\},\cdot,1_n)$; které vektory tam leží a nejsou invertibilní?

3) Matice se sčítáním tvoří grupu $(M_{m\times n},+,0_{m\times n})$, ale u násobení matic máme problém se singulárními maticemi. Vyhneme se jim a dopadne to dobře, $(M_n^R,\cdot,E_n)$ je grupa.

4) Reálné polynomy jsou s operací sčítání grupy. U násobení je problémových polynomů hodně. Jakmile $\mathrm{st}(p)\geq 1$, tak už nutně $\mathrm{st}(pq)\geq 1$ pro libovolný nenulový polynom q, takže takový p nemůže být invertibilní. Jediné invertibilní polynomy jsou tedy nenulové konstanty, $p(x)=a$, čímž ale vlastně dostáváme $(\mathbb{R}-\{0\},\cdot)$, takže rozumnou grupu z reálných polynomů udělat nelze.
△

Příklad 8b.b (pokračování 8a.c)**:** Vůči průniku a sjednocení na množinách inverzi nenajdeme s výjimkou (povinného) jednotkového prvku, tedy nejde o grupy.
△

! **Příklad 8b.c** (pokračování 8a.d)**:**
V kapitole 7 jsme vlastně ukázali, že $(\mathbb{Z}_n, +, 0)$ jsou grupy pro všechna $n \in \mathbb{N}$, zatímco $(\mathbb{Z}_n, \cdot, 1)$ jsou grupy jen v případě, že n je prvočíslo.
△

! **Příklad 8b.d** (pokračování 8a.d)**:**
1) Nechť A je množina. Množina všech zobrazení $A \mapsto A$ s operací skládání obecně není grupa (výjimkou jsou extrémní případy, kdy je A jednoprvková).
Zato množina všech bijekcí na množině A je s operací skládání grupa.
2) Nechť A je množina. Množina všech relací na A s operací skládání obecně není grupa, vyjde to zase jen u jednoprvkové A.
3) Funkce na intervalu I jsou s operací sčítání grupy. U násobení je zase problém s nulami, u skládání s funkcemi, které nejsou bijekce či prosté.
△

Příklad 8b.e (pokračování 8a.e)**:** Ani operace $\mathrm{lcm}(x, y)$ nedá na $\mathbb{N}$ grupu.
△

Příklad 8b.f (pokračování 8a.f)**:**
1) Už jsme zjistili dříve, že v prostoru $(\langle 2, 23\rangle, \circ_{13}, 2)$ je inverzní jen jednotkový prvek 2. Takže grupa to není ani náhodou.
2) Monoid genů pro barvu očí není grupa.
△

Docela nám to prořídlo, to se dalo čekat. Zkusíme něco nového.

Příklad 8b.g: Uvažujme uspořádanou množinu X, nechť M je množina všech permutací této množiny. Jako operaci bereme skládání, tedy jsou-li π_1, π_2 permutace, pak $\pi_2 \circ \pi_1$ je permutace, jejíž akce na množinu X funguje tak, že nejprve X zpermutujeme pomocí π_1, pak výslednou množinu zpermutujeme pomocí π_2.
Dá se ukázat, že tímto vznikne pologrupa (ověříme asociativní zákon). Permutace, která nechá množinu na místě, je jednotkovým prvkem množiny všech permutací na X, a každou permutaci množiny X je možné zase zamíchat na původní stav, takže máme i inverze. Množina permutací množiny X je tedy grupa. Právě věty o grupách permutací výrazně pomohly při zlomení německé šifry Enigma, což podle některých odhadů uspíšilo porážku Německa v druhé světové až od dva roky.
Formálně se permutace definuje jako bijekce množiny, pak už nám to vyplyne z příkladu 8a.d.
△

Pro grupy samozřejmě platí vše, co jsme si řekli o monoidech, ale s tím, že už nemusíme dělat předpoklady o inverzních prvcích, to už je zabudováno v grupě. Shrneme si to nejdůležitější, začneme základními vlastnostmi.

! **Věta 8b.1.**
Nechť $(G, \circ, e)$ je grupa. Pak platí následující:
(i) Jednotkový prvek e je jediný, stejně jako jsou jednoznačně určeny všechny inverzní prvky x^{-1}.
(ii) (o krácení) Nechť $c \in G$. Jestliže pro prvky $x, y \in G$ platí $c \circ x = c \circ y$ nebo $x \circ c = y \circ c$, pak už $x = y$.
(iii) Pro každé $x \in G$ existují mocniny x^n pro všechna $n \in \mathbb{Z}$, platí pro ně $x^m \circ x^n = x^{m+n}$ a $(x^m)^n = x^{mn}$ pro všechna $m, n \in \mathbb{Z}$.

Uvedeme teď pro úplnost ještě jeden axiom.

! **Definice.**
Nechť $(M, \circ)$ je grupoid. Řekneme, že je **komutativní** či **Abelův** (**commutative** or **Abelian**), jestliže pro všechna $x, y \in M$ platí $x \circ y = y \circ x$.

Můžeme tedy uvažovat komutativní pologrupy, komutativní monoidy a komutativní grupy. Čtenář se možná divil, že se tato vlastnost neobjevila dříve, ale pravda je taková, že jsme ji nepotřebovali, na vlastnosti zkoumaného prostoru má komutativita řádově menší dopad než naše axiomy. Potvrdí se to i ve zbytku této části, komutativitu potřebovat nebudeme. Její hlavní význam na této úrovni je praktický, mnohé výpočty (a důkazy) se v případě

komutativní operace silně zjednoduší a my jsme proto samozřejmě rádi, když ji máme. (Při hloubějším ponoru do teorie grup začne být komutativita významná, ale v této knize tak daleko nedojdeme.)

Velká část našich příkladů jsou komutativní monoidy či grupy, ale pro některé to neplatí, třeba pro skládání zobrazení, funkcí a permutací, známý je také problém s prohazováním u maticového násobení. Takové příklady máme také rádi, protože se zajímavěji chovají.

Existuje jedna situace, kdy máme komutativitu zaručenu, a to je podmonoid generovaný prvkem. Pravidla pro počítání s mocninami g^k zaručují, že spolu komutují, viz cvičení 8a.7. Pro invertibilní prvky g tak $\langle g\rangle$ vždy tvoří komutativní grupu.

Je čas na další teorii. Pojem podgrupy vytvoříme stejným způsobem jako předtím, tedy nechceme, abychom přechodem k podmnožině o něco přišli.

Definice.
Nechť $(G,\circ,e)$ je grupa a $N\neq\emptyset$ je podmnožina G. Řekneme, že N je **podgrupou** G, jestliže je $(N,\circ,e)$ je grupa.

Oproti podmonoidům je zde jedno velké zjednodušení, ta specifikace e u $(N,\circ,e)$ není podstatná. Podmnožina grupy, která chce zůstat grupou, si totiž nemůže vybrat svůj vlastní jednotkový prvek a musí také mít stejné inverzní prvky.

Fakt 8b.2.
Nechť $N\neq\emptyset$ je podmnožina grupy $(G,\circ,e)$. Předpokládejme, že pro nějaký prvek e_N je $(N,\circ,e_N)$ grupa. Pak platí následující:
(i) $e_N=e$.
(ii) Nechť $x\in N$. Jestliže nějaký prvek $y\in N$ splňuje $x\circ y=y\circ x=e_N$, pak je y inverzní prvek k x v grupě G.

Důkaz (poučný)**:** (i): Prvek e_N splňuje $e_N=e_N\circ e_N$ v N, tedy i v G. Každý prvek v G je invertibilní, tudíž podle Lemma 8a.11 aplikovaného na G a e_N platí $e_N=e$.

(ii): Teď už víme, že $e_N=e$, takže se předpoklad dá napsat jako $x\circ y=y\circ x=e$ a z jednoznačnosti inverze v grupě G máme $y=x^{-1}$.

□

To má zajímavý dopad na to, jak poznávat, zda nějaká podmnožina N grupy $(G,\circ,e)$ je její podmnožinou. Víme už, že není třeba kontrolovat přítomnost e, ale učitě zůstává nutnost ověřit, že je množina N uzavřená vůči operaci $\circ$. Přibude ještě něco navíc, ještě je třeba zajistit, aby každý prvek z N také našel v této množině svou inverzi (která určitě existuje, když je G grupa, jen ty inverze nesmíme při výběru N vynechat). Dostaneme tak kritérium pro vlastnost býti podgrupou, následující věta to potvrdí a navíc ukáže, že se dva testy dají spojit do jednoho.

Věta 8b.3.
Nechť $(G,\circ,e)$ je grupa a $N\neq\emptyset$ podmnožina G. Následující tvrzení jsou ekvivalentní:
(i) N je podgrupa $(G,\circ,e)$;
(ii) pro všechna $x,y\in N$ platí $x\circ y\in N$ a pro všechna $x\in N$ platí $x^{-1}\in N$;
(iii) pro všechna $x,y\in N$ platí $x\circ y^{-1}\in N$.

Důkaz (poučný)**:** (i)$\Longrightarrow$(iii): Předpokládáme, že $(N,\circ,e)$ je grupa. Nechť $x,y\in N$. Pak musí mít y inverzní prvek v N, víme, že je to totéž jako inverze y^{-1} vůči G. Prvky x,y^{-1} jsou z N, tudíž i $x\circ y^{-1}\in N$ podle uzavřenosti N na $\circ$.

(iii)$\Longrightarrow$(ii): Protože je $N\neq\emptyset$, můžeme si vzít nějaké $x\in N$. Když aplikujeme (iii) na $y=x$, dostaneme, že $e=x\circ x^{-1}\in N$. Proto můžeme aplikovat (iii) na prvky e a x a dostaneme, že $x^{-1}=e\circ x^{-1}\in N$.

Jestliže $x,y\in N$, tak jsme právě ukázali, že i $y^{-1}\in N$, tudíž podle (iii) zase $x\circ y=x\circ(y^{-1})^{-1}\in N$.

(ii)$\Longrightarrow$(i): Vezměme $x\in N$, pak podle (ii) $x^{-1}\in N$, tedy zase podle (ii) $e=x\circ x^{-1}\in N$.

Protože N splňuje $e\in N$ a $x\circ y\in N$ pro $x,y\in N$, je podle Věty 8a.4 $(N,\circ,e)$ podmonoid $(G,\circ,e)$, tedy monoid. Podle podmínky o x^{-1} má každý prvek $x\in N$ v množině svou inverzi, proto je $(N,\circ,e)$ grupa.

□

V praxi se nejčastěji používá (iii), ale i (ii) se občas hodí, třeba teď.

! **Věta 8b.4.**
Nechť je $(M, \circ, e)$ monoid. Označme $N = \{x \in M;\ x \text{ invertibilní}\}$. Pak je $(N, \circ, e)$ grupa.

Důkaz (rutinní)**:** Tvrzení plyne z Věty 8b.3 (ii) a Věty 8a.9.

□

Díky této větě snadno vyrobíme rozličné grupy. Můžeme například u čtvercových matic s maticovým násobením vybrat ty regulární neboli invertibilní a podle Věty 8b.4 tak dostaneme grupu. Víme také, že mezi zobrazeními z A na A jsou invertibilní jen bijekce, takže automaticky dostáváme, že množina bijekcí na určité množině A spolu se skládáním je grupa.

V předchozí kapitole jsme si ukázali zajímavé vlastnosti podmonoidů generovaných invertibilními prvky. V grupách jsou invertibilní všechny, čímž se situace pročistí. Shrňme si to nejpodstatnější.

! **Věta 8b.5.**
Nechť $(G, \circ, e)$ je grupa a $g \in G$.
(i) Buď $\mathrm{ord}(g) = \infty$ a $\langle g\rangle = \{g^n;\ n \in \mathbb{Z}\}$, kde jsou všechny prvky různé,
nebo $\mathrm{ord}(g) < \infty$ a $\langle g\rangle = \{e, g, g^2, \dots, g^{\mathrm{ord}(g)-1}\}$, kde jsou všechny prvky různé.
(ii) Pro každé $x \in G$ platí $|x\langle g\rangle| = |\langle g\rangle|$.
(iii) Pro všechna $x \in G$ platí: $x \in x\langle g\rangle$.
(iv) Pro všechna $x, y \in G$ platí: $x\langle g\rangle = y\langle g\rangle$ právě tehdy, když $x^{-1} \circ y \in \langle g\rangle$, a to právě tehdy když $y^{-1} \circ x \in \langle g\rangle$.
(v) Množina $\{x\langle g\rangle\}_{x\in G}$ je rozklad množiny G.

Důkaz: (i) plyne z Věty 8a.17.
(ii) plyne z Věty 8a.19.
(iii): $x = x \circ e = x \circ g^0 \in x\langle g\rangle$.
(iv): Nejprve ukážeme ekvivalenci posledních dvou tvrzení. Nechť $x^{-1} \circ y \in \langle g\rangle$. Pak pro nějaké $k \in \mathbb{Z}$ je $x^{-1} \circ y = g^k$, proto také $[x^{-1} \circ y]^{-1} = [g^k]^{-1}$. Podle rozličných pravidel pro inverzi pak $y^{-1} \circ x = g^{-k} \in \langle g\rangle$. Opačný směr je zjevně obdobný.
Nyní předpokládejme, že $x\langle g\rangle = y\langle g\rangle$. Protože $y \in y\langle g\rangle = x\langle g\rangle$, existuje $k \in \mathbb{Z}$ takové, že $y = x \circ g^k$. Pak ovšem $x^{-1} \circ y = x^{-1} \circ x \circ g^k = e \circ g^k = g^k \in \langle g\rangle$.
Zbývá ukázat, že z předpokladů $x^{-1} \circ y \in \langle g\rangle$ a $y^{-1} \circ x \in \langle g\rangle$ plyne rovnost oněch dvou množin.
Z první inkluze máme $x^{-1} \circ y = g^k$ pro nějaké $k \in \mathbb{Z}$. Odtud $y = x \circ g^k$, proto pro všechna $z \in y\langle g\rangle$ platí:

$$z = y \circ g^m = x \circ g^k \circ g^m = x \circ g^{k+m} \in x\langle g\rangle.$$

Takže $y\langle g\rangle \subseteq x\langle g\rangle$.
Obdobně z $y^{-1} \circ x \in \langle g\rangle$ odvodíme $x\langle g\rangle \subseteq y\langle g\rangle$ a rovnost je dokázána.
(v) Každý $x \in G$ leží v $x\langle g\rangle$, proto $G = \bigcup_{x\in G} x\langle g\rangle$. Zbývá ukázat, že dotyčné množiny jsou buď shodné, nebo disjunktní. Vezměme tedy libovolné $x, y \in G$.
Jestliže $x\langle g\rangle \cap y\langle g\rangle = \emptyset$, jsme hotovi. Předpokládejme tedy, že existuje $z \in x\langle g\rangle \cap y\langle g\rangle$. Pak musí existovat $k, m \in \mathbb{Z}$ takové, že $z = x \circ g^k$ a $z = y \circ g^m$. Pak ovšem $x \circ g^k = y \circ g^m$, proto $x^{-1} \circ x \circ g^k = x^{-1} \circ y \circ g^m$ neboli $g^k = x^{-1} \circ y \circ g^m$, následně $g^k \circ g^{-m} = x^{-1} \circ y$ neboli $x^{-1} \circ y = g^{k-m}$. Podle (iv) z toho již plyne $x\langle g\rangle = y\langle g\rangle$.

□

Čtenář si možná pomyslel, že některé kroky byly zbytečně složité. Proč jsme prostě rovnici $x \circ g^k = y \circ g^m$ nevynásobili prvkem $x^{-1} \circ g^{-m}$ a pak nepokrátili? Protože by to nefungovalo. V grupách obecně nelze jen tak násobit a krátit v rovnicích. Ještě se k tomu vrátíme.

Podívejme se teď blíže na ten rozklad. U monoidů jsme komentovali, že si množinu G vlastně umíme poskládat z rozličných posunutí jedné $\langle g\rangle$. V případě grupy navíc víme, že všechny tyto posuny jsou stejné velikosti. U konečných grup z toho dostaneme zajímavý a užitečný výsledek.

! **Důsledek 8b.6.**
Nechť $(G, \circ, e)$ je grupa, kde G je konečná množina. Pak pro každé $g \in G$ platí, že $\mathrm{ord}(g)$ dělí $|G|$.

Důkaz (poučný)**:** Pokud je G konečná, tak nemůže být $\langle g\rangle$ nekonečná množina, tudíž $\mathrm{ord}(g) < \infty$ a jde o čísla, se kterými jde dále počítat.

Podle (iv) se G rozloží na několik disjunktních množin, díky konečnosti G jich bude konečně mnoho, řekněme k, všechny mají podle (ii) stejnou mohutnost $\mathrm{ord}(g)$. Dostáváme tedy $|G| = k \cdot \mathrm{ord}(g)$.

□

Tento výsledek hrál klíčovou roli v kapitole 7, jmenovitě v důkazu Eulerovy věty 7a.22. Ukážeme si ještě jeden praktický dopad, viz Věta 8a.16.

Důsledek 8b.7.
Nechť $(G, \circ, e)$ je grupa, kde G je konečná množina, označme $n = |G|$. Pak pro každé $g \in G$ platí $g^n = e$.
Je-li navíc n prvočíslo a $g \neq e$, pak $g^k = e$ právě tehdy, když k je násobek n.

! **Příklad 8b.h** (pokračování 8a.b)**:** Víme, že $(\mathbb{Z}_{14}, \odot, 1)$ je jen monoid. Podle Věty 8b.4 bychom měli dostat grupu tak, že si vybereme invertibilní prvky, tedy $G = \{1, 3, 5, 9, 11, 13\}$. Její multiplikativní tabulku získáme tak, že z původní tabulky pro $\mathbb{Z}_{14}$ vyškrtáme nepoužité řádky a sloupce.

$\odot$	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	11
13	13	11	9	5	3	1

Jaké řády dokážeme získat? Pro $g = 1$ máme evidentně $1^k = 1$ a tedy $\langle 1 \rangle = \{1\}$, proto $\mathrm{ord}(1) = 1$, což dělí $|G| = 6$.

Řetízek mocnin pro $g = 3$ nám již dříve ukázal, že $\langle 3 \rangle = G$ a $\mathrm{ord}(3) = 6$, což opravdu dělí $|G| = 6$.

Případ $g = 5$ dává $5^2 = 11$, $5^3 = 13$, $5^4 = 9$, $5^5 = 3$, $5^6 = 1$, zase $\langle 5 \rangle = G$ a $\mathrm{ord}(5) = 6$.

Pro $g = 9$ máme $9^1 = 9$, $9^2 = 9 \odot 9 = 11$, $9^3 = 9^2 \odot 9 = 11 \odot 9 = 1$. Proto $\langle 9 \rangle = \{9, 11, 1\}$ a $\mathrm{ord}(9) = 3$, což zase dělí $|G| = 6$.

Ověřte si sami, že $\langle 11 \rangle = \{1, 9, 11\}$ a $\mathrm{ord}(11) = 3$, také $\langle 13 \rangle = \{1, 13\}$ a $\mathrm{ord}(13) = 2$.

Každý dělitel čísla 6 našel svůj prvek, ale obecně to nemusí být pravda.

Pro zajímavost se ještě podíváme na $(\mathbb{Z}_4, \oplus, 0)$, což je grupa.

Zvolme $g = 3$, pak $3^1 = 3$, $3^2 = 3 \oplus 3 = 2$, $3^3 = 3 \oplus 3 \oplus 3 = 2 \oplus 3 = 1$, $3^4 = 3^2 \oplus 3^2 = 2 \oplus 2 = 0 = e$. Máme tedy $\langle 3 \rangle = \{3, 2, 1, 0\} = \mathbb{Z}_4$ a $\mathrm{ord}(3) = 4$.

Teď zvolme $g = 2$, pak $2^1 = 2$, $2^2 = 2 \oplus 2 = 0 = e$. Máme tedy $\langle 2 \rangle = \{2, 0\}$ a $\mathrm{ord}(2) = 2$.

△

8b.8 Poznámka: Ukázali jsme zajímavou souvislost mezi velikostí grupy a velikostí speciálních podgrup. Přesně stejný postup se dá udělat pro libovolnou podgrupu. Zkuste si znovu přečíst úvahy, které k našemu výsledku vedly, ale s takovouto změnou:

- Nechť H je podgrupa G. Pak pro libovolné $x \in G$ je $T(h) = x \circ h$ bijekce z H na xH, mimo jiné tedy $|H| = |xH|$, viz Věta 8a.19 a Věta 8b.5 (ii).
- Pro libovolné $x, y \in G$ platí $xH = yH$ právě tehdy, když $x^{-1} \circ y \in H$, viz Věta 8b.5 (iii).
- Množina $\{xH\}_{x \in G}$ je rozklad množiny G, viz Věta 8b.5 (iv).

Důsledek: Jestliže je G konečná grupa a H její podgrupa, tak nutně $|H|$ dělí $|G|$.

Tomuto se říká Lagrangeova věta. Jak vidíte, dostáváme se zde již blízko k teorii grup, ale v našem dalším textu to nebudeme potřebovat. Pokud vás to zaujalo, přečtěte si nějakou pěknou knížku o algebře.

△

Ve zbytku kapitoly se podíváme na alternativní způsoby, jak poznat, že je pologrupa vlastně grupou. První kritérium říká, že to lze poznávat podle toho, zda v rámci dotyčného prostoru umíme řešit lineární rovnice.

Věta 8b.9.
Nechť $(M, \circ)$ je pologrupa. Je to grupa právě tehdy, když pro libovolné $a, b \in M$ existují řešení $x, y \in M$ rovnic $a \circ x = b$ a $y \circ a = b$.
Ta řešení jsou pak jednoznačná.

Důkaz (poučný)**:** 1) $\Longrightarrow$: Jestliže je M grupa, pak existuje jednotkový prvek e a inverzní prvek a^{-1}. Proto lze definovat $x = a^{-1} \circ b$ a snadno ověříme, že řeší první rovnici: $a \circ x = a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$.

Podobně ověříme, že $y = b \circ a^{-1}$ řeší druhou rovnici. Jsou ta řešení jednoznačná? Nechť x je nějaké řešení první rovnice. Pak už nutně $x = e \circ x = (a^{-1} \circ a) \circ x = a^{-1} \circ (a \circ x) = a^{-1} \circ b$.

Podobně pro tu druhou rovnici.

2) $\Longleftarrow$: Zvolme si nějaké $a \in M$. Pak v M existuje řešení rovnice $a \circ x = a$, označme ho e_r, a řešení $x \circ a = a$ označme e_l. Chceme ukázat, že jde o jediný prvek, a to jednotkový.

Na to ještě potřebujeme řešení rovnice $x \circ a = e_l$ označené $a_{l,-1}$ a řešení rovnice $a \circ x = e_r$ označené $a_{r,-1}$. Pak máme

$e_l = a_{l,-1} \circ a = a_{l,-1} \circ (a \circ e_r) = (a_{l,-1} \circ a) \circ e_r = e_l \circ e_r = e_l \circ (a \circ a_{r,-1}) = (e_l \circ a) \circ a_{r,-1} = a \circ a_{r,-1} = e_r$.

Označme tedy tento prvek e. Ukážeme, že je to jednotkový prvek.

Začneme tím, že $e^2 = e$. Máme totiž $e^2 \circ a = e \circ (e \circ a) = e \circ a = a$, proto také e^2 řeší rovnici $x \circ a = a$ a podle předchozího výpočtu s $e_l = e^2$ a $e_r = e$ máme $e^2 = e$.

Teď vezměme libovolné $b \in M$. Pak existuje řešení rovnice $x \circ e = b$, označme jej c. Máme

$b \circ e = (c \circ e) \circ e = c \circ e^2 = c \circ e = b$. Podobně ukážeme, že $e \circ b = b$. Máme potvrzeno, že $(M, \circ, e)$ je monoid.

Předpoklad o řešení rovnic pak umožňuje pro libovolné $a \in A$ najít řešení rovnic $a \circ x = e$ a $y \circ a = e$, tedy podle Věty 8a.6 získáme inverzní prvek k a.

□

Toto vede na zajímavý závěr. Mějme pologrupu $(M, \circ)$ a uvažujme lineární rovnice. Věta říká, že když jsou takové rovnice řešitelné všechny, tak už jsou řešitelné jednoznačně. Z toho vyplývá, že když má nějaká rovnice více řešení, pak už musí také existovat rovnice, která řešení nemá.

Kapitolu ukončíme dalším způsobem, jak poznat grupu. Je to spíš taková kuriozitka.

V kapitole o monoidech jsme čtenáře varovali, že když zkoumáme, zda je nějaké x invertibilní, tak ještě nestačí, když najdeme „jednostrannou inverzi“, existence prvku y s vlastností $y \circ x = e$ nic neznamená. Musíme také vyzkoušet platnost $x \circ y = e$ a teprve pak jásat.

Když testujeme, zda je nějaký monoid $(M, \circ, e)$ grupou, tak testujeme všechny prvky $x \in M$, zda jsou invertibilní. Ukáže se, že při takovémto hromadném testování už stačí zkoušet jen z jedné strany. Dokonce se to týká nejen axiomu (A3), ale i (A2).

Věta 8b.10.
Uvažujme množinu M s binární operací $\circ$. Předpokládejme, že následující podmínky jsou splněny:
(A1) pro všechny $x, y, z \in M$ platí $x \circ (y \circ z) = (x \circ y) \circ z$;
(A2') existuje $e \in M$ takové, že $e \circ x = x$ pro všechna $x \in M$;
(A3') pro každé $x \in M$ existuje $y \in M$: $y \circ x = e$.
Pak už je $(M, \circ, e)$ grupa.

Důkaz (poučný)**:** 1) Nechť $x \in M$ a y je levá inverze k x dle (A3'). Ukážeme, že je to i pravá inverze. K tomu ještě najdeme prvek z jako levou inverzi prvku y dle (A3'). Pak pomocí (A2') počítáme

$x \circ y = e \circ (x \circ y) = (z \circ y) \circ (x \circ y) = z \circ (y \circ x) \circ y = z \circ e \circ y = z \circ (e \circ y) = z \circ y = e$.

Máme tedy podmínky $y \circ x = e$ a $x \circ y = e$, což bude znamenat, že libovolné $x \in M$ je invertibilní, ale až ve chvíli, kdy ukážeme, že e je opravdu jednotkový prvek.

2) Nechť $x \in M$ je libovolné. Podmínka (A2') dává $e \circ x = x$, potřebujeme to ještě zprava. Pro toto x najdeme levou inverzi y dle (A3'), která je dle 1) i pravou inverzí, a počítáme $x \circ e = x \circ (y \circ x) = (x \circ y) \circ x = e \circ x = x$.

□

Je samozřejmě možné udělat verze (A2") a (A3") s pravou identitou a pravou inverzí, zase by to stačilo na grupu. Tím končí kapitola o grupách.

Cvičení

Cvičení 8b.1 (rutinní, poučné)**:** Uvažujte $G = \mathbb{Q} - \{0\}$ a operaci $x \circ y = 2xy$. Dokažte, že je to grupa, a najděte vzorec pro inverzní prvky.

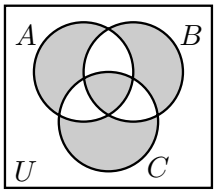
Cvičení 8b.2 (rutinní, poučné)**:** Nechť U je množina, uvažujme $G = P(U)$ a operaci **symetrický rozdíl** definovanou jako $A \div B = (A - B) \cup (B - A)$ (nakreslete si Vennův diagram).
Dokažte, že $(G, \div)$ je grupa, identifikujte jednotkový prvek a inverzní prvky.
Nápověda: asociativita stačí Vennovým diagramem.

Cvičení 8b.3 (rutinní, poučné)**:** Uvažujte monoid $(\mathbb{Z}_9, \cdot)$.
(i) Najděte grupu N jeho invertibilních prvků. Ověřte, že je opravdu uzavřená na násobení modulo 9.
(ii) Pro všechny prvku $x \in N$ určete $\langle x \rangle$ a $\mathrm{ord}(x)$.
(iii) Nechť $g = 7$. Pro všechna $x \in N$ určete $x\langle g \rangle$, najděte odpovídající rozklad grupy N.

Cvičení 8b.4 (rutinní, poučné)**:** Uvažujte matici $A = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ v monoidu $(M_{2\times 2}, \cdot)$.

Určete $\langle A \rangle$ a $\mathrm{ord}(A)$.

Řešení:
8b.1: $(x \circ y) \circ z = 4xyz = x \circ (y \circ z)$, $e = \frac{1}{2}$, $x^{-1} = \frac{1}{4x}$.
8b.2:
Vennův diagram $(A \div B) \div C = A \div (B \div C)$ je „květinka“, viz vpravo.
Ověřte: $A \div \emptyset = A$ a $A^{-1} = A$ pro libovolnou množinu.



8b.3: (i): $N = \{1, 2, 4, 5, 7, 8\}$. Ověření: třeba $7 \cdot 8 = 56 \bmod 9 = 2 \in N$, atd.
(ii) $\langle 1 \rangle = \{1\}$ a $\mathrm{ord}(1) = 1$; $\langle 2 \rangle = \{2, 2^2 = 4, 2^3 = 8, 2^4 = 7, 2^5 = 5, 2^6 = 1\} = N$ a $\mathrm{ord}(2) = 6$;
$\langle 4 \rangle = \{4, 4^2 = 7, 4^3 = 1\}$ a $\mathrm{ord}(4) = 3$; $\langle 5 \rangle = \{5, 5^2 = 7, 5^3 = 8, 5^4 = 4, 5^5 = 2, 5^6 = 1\} = N$ a $\mathrm{ord}(5) = 6$;
$\langle 7 \rangle = \{7, 7^2 = 4, 7^3 = 1\}$ a $\mathrm{ord}(7) = 3$; $\langle 8 \rangle = \{8, 8^2 = 1\}$ a $\mathrm{ord}(8) = 2$;
(iii) $1\langle 7 \rangle = \langle 7 \rangle = \{1, 4, 7\}$; $2\langle 7 \rangle = \{2, 8, 5\}$; $4\langle 7 \rangle = \{4, 7, 1\}$; $5\langle 7 \rangle = \{5, 2, 8\}$; $7\langle 7 \rangle = \{7, 1, 4\}$; $8\langle 7 \rangle = \{8, 5, 2\}$.
$N = \{1, 4, 7\} \cup \{2, 5, 8\}$.
8b.4: $\langle A \rangle = \left\{ A, A^2 = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}, A^3 = E_2 \right\}$; $\mathrm{ord}(A) = 3$.

8c. Další struktury

Tato kapitola je z větší části nepovinná a zbytek knihy lze bez ní číst, ale zajímavě doplňuje kapitolu 7c o polynomech a vůbec nabídne trochu nadhled. Víc ani nebylo cílem, tématy jen prolétneme, aby měl čtenář základní orientaci, oč vůbec jde.

Pokročilejší struktury vznikají například tak, že se přidá další operace.

Definice.
Uvažujme binární operace $\oplus$ a $\odot$ na množině R. Řekneme, že $(R, \oplus, \odot)$ je **okruh** (**ring**), jestliže splňuje následující axiomy:
(A1) pro všechna $x, y, z \in R$ platí $x \oplus (y \oplus z) = (x \oplus y) \oplus z$, (asociativita $\oplus$)
(A2) existuje $n \in R$ takové, že $x \oplus n = n \oplus x = x$ pro všechna $x \in R$, (jednotkový prvek pro $\oplus$)
(A3) pro každé $x \in R$ existuje $y \in R$ takové že $x \oplus y = y \oplus x = n$, (inverzní prvky pro $\oplus$)
(A4) pro každé $x, y \in R$ platí $x \oplus y = y \oplus x$, (komutativita $\oplus$)
(A5) pro všechna $x, y, z \in R$ platí $x \odot (y \odot z) = (x \odot y) \odot z$, (asociativita $\odot$)
(A6) existuje $e \in R$ takové, že $x \odot e = e \odot x = x$ pro všechna $x \in R$, (jednotkový prvek pro $\odot$)
(A7) pro všechna $x, y, z \in R$ platí
$x \odot (y \oplus z) = (x \odot y) \oplus (x \odot z)$ a $(y \oplus z) \odot x = (y \odot x) \oplus (z \odot y)$. (distributivní zákon)

Řekneme, že okruh $(R, \oplus, \odot)$ je **komutitativní okruh** (**commutative ring**), jestliže navíc splňuje axiom
(A8) pro každé $x, y \in R$ platí $x \odot y = y \odot x$. (komutativita $\odot$)

I zde někteří autoři přidávají
(A0) pro všechna $x, y \in R$ platí $x \oplus y \in R$ a $x \odot y \in R$.
I zde je to zbytečné, ale nezaškodí to. Když se na ty podmínky pro okruh podíváme, vidíme, že je lze zkrátit následovně: $(R, \oplus, n)$ je komutativní grupa, $(R, \odot, e)$ je monoid a operace jsou spoly svázány distributivním zákonem.

Z toho vyplývá, že jednotkové prvky i inverzní prvky jsou jednoznačně určeny. Inverzní prvky vzhledem k $\oplus$ se tradičně značí $-x$, zatímco inverzní prvky vzhledem k $\odot$ (alespoň ty, které náhodou existují) se značí x^{-1}. Víme z kapitoly 8a, že přinejmenším jeden existuje, $e^{-1} = e$. Mnoho autorů používá mnemotechnickou pomůcku a značí jednotkové prvky pomocí 0 a 1, někteří dokonce používají pro okruh značení $(R, +, \cdot)$, ale je třeba si uvědomit, že pak „0“ nemusí být číslo 0 a „1“ nemusí být číslo 1, jak ostatně hned uvidíme.

Nejjednodušší okruh je $R = \{0\}$ s operacemi $0 \oplus 0 = 0 \odot 0 = 0$. Pak také $n = e = 0$. Zrovna toto se některým autorům nelíbí a přidávají do definice okruhu podmínku, že $n \neq e$, čímž vznikne okruh s více prvky. Dá se mimochodem ukázat, že jakmile má okruh víc než jeden prvek, tak už nutně $n \neq e$ (viz poznámka po Faktu 8c.1). Tím se dostáváme k tomu, že autoři definuje okruhy různě, někteří třeba vynechávají axiom (A6), naše definice patří k těm nejobvyklejším.

Klasickým příkladem okruhů jsou samozřejmě naši staří známí $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{Z}, +, \cdot)$ a $(\mathbb{Z}_n, +, \cdot)$. Okruhy se v matematice používají docela hodně, protože jejich vlastnosti jsou vyváženým kompromisem mezi snahou mít co nejvíce axiomů, aby platilo hodně vlastností, a snahou mít jich co nejméně, aby se do výsledné formy vešlo co nejvíce aplikací.

O okruzích se toho dá říct velice mnoho. Tato kapitola je spíš uzavírací a přehledová, tak jen jako ukázku uvedeme pár vlastností, které máme u nám známých číselných množin (představujte si $n = 0$, $e = 1$) a fungují i obecně.

Fakt 8c.1.
Nechť $(R, \oplus, \odot, n, e)$ je okruh. Pak platí následující:
(i) pro každé $x \in R$ platí $n \odot x = x \odot n = n$;
(ii) pro každé $x \in R$ platí $(-e) \odot x = (-x)$;
(iii) pro každé $x, y \in R$ platí $(-x) \odot y = x \odot (-y) = -(x \odot y)$.

Důkaz (poučný)**:** (i): Pro neutrální prvek platí $n = n \oplus n$. Pak máme díky distributivnímu zákonu rovnost $x \odot n = x \odot (n \oplus n) = (x \odot n) \oplus (x \odot n)$. Podle Lemma 8a.11 aplikovaného na invertibilní prvek $x \odot n$ v monoidu $(R, \oplus, n)$ tedy $x \odot n = n$. Druhá rovnost se dokazuje obdobně.

(ii): Ověříme, že výraz nalevo splňuje definici inverzního prvku x vůči $\oplus$, použijeme $x = e \odot x$ a distributivní zákon:

$$x \oplus [(-e) \odot x] = [e \odot x] \oplus [(-e) \odot x] = [e \oplus (-e)] \odot x = n \odot x = n.$$

(iii): Ověříme, že výraz zcela nalevo splňuje definici inverzního prvku $x \odot y$ vůči $\oplus$:
$[(-x) \odot y] \oplus [x \odot y] = [(-x) \oplus x] \odot y = n \odot y = n$. Pro druhý výraz zleva se to dělá obdobně.

□

Část (i) má zajímavý důsledek. Kdyby platilo $n = e$, tak už pro libovolné $x \in R$ máme $x = x \odot e = x \odot n = n$, tedy $R = \{n\}$. To potvrzuje naši poznámku výše, že jakmile má R víc než jeden prvek, tak už nutně $n \neq e$. Platí pak obecně i další věc, kterou známe z běžného násobení čísel.

Fakt 8c.2.
Nechť $(R, \oplus, \odot, n, e)$ je okruh a $|R| \geq 2$. Pak n není invertibilní.

Důkaz (poučný)**:** Sporem: Nechť existuje $y = n^{-1}$. Pak $y \odot n = e$, ale podle (i) výše také $y \odot n = n$. Dostáváme $e = n$, což ale platí jen pro jednoprvkové R.

□

Jsou ale také věci, které známe z $\mathbb{R}$ či $\mathbb{Z}$, ale v obecných okruzích nefungují. V zásadě jsou okruhy dostatečně bohaté na to, abychom na nich zkusili vybudovat celou teorii dělitelnosti z kapitoly 6a (prvočísla atd.), a podle toho, jak daleko se dostaneme (funguje v nich Euklidův algoritmus? funguje v nich jednoznačnost rozkladu na prvočísla?), se okruhy klasifikují. Jsou o tom tlusté knihy z oboru algebra, takže do toho nebudeme šťourat, nicméně na jednu zajímavou vlastnost jsme tu už narazili.

Definice.
Nechť $(R, \oplus, \odot)$ je okruh. Řekneme, že prvek $x \in R$ je **dělitelem nuly** (**zero divisor**), jestliže $x \neq n$ a existuje $y \neq n$ takový, že $x \odot y = n$.

Na takové prvky nejsme zvyklí, naopak rádi v algebraických úpravách z rovnice $x \cdot y = 0$ usuzujeme, že jeden z prvků musí být nula, ale obecně v okruzích to neplatí. Příklady už jsme potkali v kapitole 7, například při násobení modulo 4 platí $2 \cdot 2 = 0$, neboli v okruhu $(\mathbb{Z}_4, +, \cdot)$ je 2 dělitelem nuly. Podobně jsme v příkladě 8a.b viděli, že v okruhu $\mathbb{Z}_{14}$ platí $2 \cdot 7 = 0$, $7 \cdot 10 = 0$ a podobně.

To je v mnoha situacích velice nepříjemné, takže se vyplatí zavést speciální kategorii okruhů, kde toto nehrozí.

Definice.
Řekneme, že okruh $(R, \oplus, \odot)$ je **obor integrity** (**integral domain**), jestliže je to komutativní okruh bez dělitelů nuly.

Takže $(\mathbb{R}, +, \cdot)$ a $(\mathbb{Z}, +, \cdot)$ jsou dozajista obory integrity, zajímavé je, že jsme v kapitole 7a zjistili, že pro prvočísla p jsou i $(\mathbb{Z}_p, +, \cdot)$ obory integrity. V těch se hned lépe pracuje. Jeden způsob, jak se dělitelů nuly zbavit, je mít co nejvíce invertibilních prvků.

Fakt 8c.3.
Nechť je $(R, \oplus, \odot)$ okruh. Jestliže je $x \in R$ invertibilní vůči $\odot$, pak není dělitelem nuly.

Důkaz (rutinní, poučný)**:** Nechť $y \in R$ splňuje podmínku $x \odot y = n$. Ukážeme, že pak už nutně $y = n$.

$$y = e \odot y = (x^{-1} \odot x) \odot y = x^{-1} \odot (x \odot y) = x^{-1} \odot n = n.$$

□

Neplatí to ale naopak: Prvky, které nejsou děliteli nuly, nemusí být automaticky invertibilní. Pro příklad se stačí podívat na $(\mathbb{Z}, +, \cdot)$, třeba $x = 13$ není dělitelem nuly, ale ani nemá v $\mathbb{Z}$ inverzní prvek vůči násobení.

Měli jsme Fakt 8a.10, který říkal, že invertibilní prvky je možno v rovnicích krátit. Platí to i pro prvky, které nejsou dělitelé nuly. Jak jsme právě viděli, je jich potencionálně více, čímž se vysvětluje, proč můžeme krátit nenulová čísla v rovnicích, i když pracujeme v $\mathbb{Z}$. Poučný je způsob, kterým se toto dokazuje, protože to výstižně ukazuje mechanismus práce v okruzích.

Normálně bychom v rovnici $cx = cy$ přesunuli oba prvky na levou stranu odečtením pravé strany, získáme $cx - cy = 0$, vytkneme na $c(x - y) = 0$ a pak vydělíme. V okruhu ovšem nemáme ani odčítání, ani dělení, takže se vše musí odehrávat přes inverzní prvky. Jdeme na to.

Předpokládejme tedy, že máme rovnici $c \odot x = c \odot y$ a c není dělitel nuly. Přičteme k obou stranám opačný prvek k pravé straně vůči $\oplus$ a dostaneme $(c \odot x) \oplus [-(c \odot y)] = n$. Teď použijeme (iii) z Faktu 8c.1, máme $(c \odot x) \oplus (c \odot (-y)) = n$ a jsme zralí na distributivní zákon: $c \odot (x \oplus (-y)) = n$. Protože c není dělitel nuly, musí být nutně $x \oplus (-y) = n$, takže $-y$ splňuje podmínku inverzního prvku vůči x. Z jeho jednoznačnosti máme $-x = -y$. Pak také $-(-x) = -(-y)$, tedy $x = y$, zde jsme použili Větu 8a.9.

Nejlepší jsou ale stejně prvky invertibilní. Ideální je stav, kdy jsou invertibilní všechny kromě n, kde to nejde již z principu (s výjimkou triviálního jednoprvkového okruhu).

Definice.
Uvažujme binární operace $\oplus$ a $\odot$ na množině F. Řekneme, že $(F, \oplus, \odot)$ je **těleso** (**field**), jestliže je to komutativní okruh, tedy splňuje axiomy (A1) až (A8), a navíc splňuje axiom
(A9) pro každé $x \in F$, $x \neq n$ existuje $y \in F$ takové, že $x \odot y = y \odot x = e$. (inverzní prvky pro $\odot$)

Jinak řečeno, $(F, \oplus, n)$ je komutativní grupa, $(F - \{n\}, \odot, e)$ je komutativní grupa a operace jsou svázány distributivním zákonem. Klasickými příklady těles jsou $\mathbb{C}$, $\mathbb{R}$ či $\mathbb{Q}$, teď už $\mathbb{Z}$ vypadává. V kapitole 7a jsme viděli, že pro prvočísla p je $\mathbb{Z}_p$ těleso, pro computer science je samozřejmě velice zajímavé těleso $\mathbb{Z}_2$. Díky existenci inverzních prvků vůči $\odot$ už nejsou v tělesech žádní dělitelé nuly, takže těleso je i okruh integrity. Dobře se proto s nimi pracuje, s tělesy se dá dělat v zásadě všechno, co s $\mathbb{R}$, například lineární algebra.

Příklad 8c.a: Máme-li těleso F, můžeme nad ním definovat matice obvyklým způsobem, pro každé $n \in \mathbb{N}$ tak vznikne množina $M_n(F)$ matic o rozměru $n \times n$. Když ji vybavíme operacemi maticového sčítání a násobení, které se definuje běžným způsobem, jen namísto $+$ a $\cdot$ používáme operace $\oplus$ a $\odot$ z tělesa, dostáváme tak okruh, který je nekomutativní pro $n \geq 2$. Asi není překvapením, že v computer science jsou zajímavé matice nad $\mathbb{Z}_p$ pro prvočísla p, zejména okruh $M_n(\mathbb{Z}_2)$. Blíže viz kapitola 7c.

8c.4 Okruhy polynomů

Běžně pracujeme s polynomy nad $\mathbb{R}$, značenými $\mathbb{R}[x]$, setkali jsme se již také s polynomy nad $\mathbb{Z}_n$. Zde vybudujeme polynomy nad obecným okruhem $(R, \oplus, \odot)$. Pro účely této části se vyplatí značit jeho neutrální prvek 0 a jednotkový prvek 1, protože to zjednoduší zápis a čtenář už je snad dost zkušený na to, aby věděl, že „0“ nemusí být zrovna číslo 0, ale třeba matice ze samých nul či jiný neutrální prvek. Zavedeme také pro zjednodušení zápisu prioritu $\odot$ před $\oplus$.

! **Definice.**
Uvažujme okruh $(R, \oplus, \odot)$.
Termínem **polynom** (**polynomial**) nad R označujeme abstraktní výraz

$$p = \sum_{k=0}^{n} a_k x^k = a_0 x^0 + a_1 x^1 + \cdots + a_{n-1} x^{n-1} + a_n x^n,$$

kde $n \in \mathbb{N}_0$ a $a_i \in R$ pro všechna i.
Jako $R[x]$ označíme množinu všech polynomů nad R.

! **Poznámka (velice důležitá):** Je třeba si uvědomit, že to x má v polynomu ryze symbolický charakter. Sice mu říkáme **proměnná**, ale to je jen jméno pro symbol, klidně tam místo x může být hvězdička nebo třeba srdíčko: $p = 13 + 2\heartsuit^2$ by mohl být polynom nad $\mathbb{Z}_{14}$. Tento symbol, stejně jako symbol „+“ nemající nic společného se sčítáním, slouží k oddělení jednotlivých koeficientů polynomu. Když vidíme x^2, tak víme, že ten prvek z R před ním je v pořadí třetí koeficient polynomu. Šlo by to i jinak, klidně jsme namísto $a_0x^0 + a_1x^1 + a_2x^2$ mohli zavést zápis „$a_0\heartsuit, a_1\diamondsuit, a_2\bullet$“ a celá teorie by dál fungovala. Jinak řečeno, to podstatné jsou koeficienty a ostatní symboly slouží jen jako připomínka, kde který koeficient je.

V některých aplikacích si proto množinu $R[x]$ ztotožníme s množinou $\bigcup_{n=0}^{\infty} R^k$ vektorů s koeficienty z R libovolné délky, například $p = 13 + 2x^2$ je jen pohodlný zápis pro vektor $(13, 0, 2)$. Zde je třeba přijmout úmluvu, že každý vektor lze prodloužit nulami na vektor libovolné délky a bude to pořád stejný vektor. Tím do nového jazyka zahrneme obvyklou úmluvu, že $p = 13 + 2x^2$ je totéž jako $p = 13 + 2x^2 + 0x^3 + 0x^4$, takže potřebujeme, aby i vektory $(13, 0, 2)$ a $(13, 0, 2, 0, 0)$ byly považovány za stejné. Celou teorii polynomů je pak možné vybudovat čistě v jazyce vektorů a nebude to ani o moc těžší.

Takovéto polynomy lze vlastně zavést nad libovolnou množinou M, která ani nemusí mít nějaké operace. Pak se toho ale moc nedá vymyslet. Zajímavé to je právě u množin s operacemi. Brzy ukážeme, že oněm speciálním symbolům + a x^k můžeme dát určitý význam, který odpovídá tomu, co známe z reálných polynomů. Jsou tedy vhodnější než srdíčka, ale dá trochu práce to všechno udělat pořádně.

△

Polynomy nad reálnými čísly zná každý, ukážeme zajímavější příklad.

! **Příklad 8c.b:** Uvažujme $R = M_2(\mathbb{Z})$, okruh všech matic 2×2 s celočíselnými prvky. Pak třeba

$$p = \begin{pmatrix} 3 & -23 \\ 1 & 14 \end{pmatrix} x^0 + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} x^1 + \begin{pmatrix} 1 & 0 \\ 0 & 13 \end{pmatrix} x^2 + \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} x^3$$

je polynom nad R.

△

! Abychom zjednodušili zápis, uděláme následující úmluvy:
- členy $0x^k$, kde 0 je nulový prvek okruhu R, můžeme ze zápisu vynechat,
- mocninu $1x^k$, kde 1 je jednotkový prvek okruhu R, budeme psát jako x^k,
- mocninu x^1 budeme psát jako x,
- mocninu $x^0 = 1$ nebudeme při psaní uvádět.

Samozřejmě tato úmluva úzce souvisí s významem, který symbolu x^k později přiřadíme.

Při této příležitosti uděláme malou poznámku o zápisu. Každý autor řeší při zavádění polynomů dilema, zda řadit mocniny od nejmenší k největší nebo naopak. Obojí má své pro i proti. Já jsem se v definici rozhodl brát členy od nejmenších, protože jsme si rozmysleli, že polynomy můžeme „prodlužovat“, a přišlo mi dobré začínat od části, která je pro polynom důležitá, případné prodloužení o nulové členy pak dělat ke konci. Této konvence se budu držet v teoretických úvahách. Na druhou stranu jsme u reálných polynomů zvyklí začínat nejvyšší mocninou, což budu také dělat často v příkladech. Konec konců, je to v zásadě jedno.

Příklad 8c.c: Polynom z předchozího příkladu lze zapsat i jako

$$p = \begin{pmatrix} 3 & -23 \\ 1 & 14 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 13 \end{pmatrix} x^2.$$

Mimo jiné jsme použili pravidlo o nulovém prvku $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ okruhu $R = M_2(\mathbb{Z})$.

△

!

Definice.
Nechť R je okruh, nechť $p = \sum_{k=0}^{n} a_k x^k \in R[x]$.
Definujeme **stupeň** (**degree**) polynomu p jako $\mathrm{st}(p) = -\infty$ jestliže pro všechna $k = 1, \ldots, n$ je $a_k = 0$ (tedy $p = 0$), jinak jako $\mathrm{st}(p) = \max\{k;\ a_k \neq 0\}$.

Takže třeba pro polynom p s maticemi z příkladu výše máme $\mathrm{st}(p) = 2$. Definice stupně pro nulový polynom možná překvapí, ale když si ještě zavedeme pravidlo, že $-\infty + a = -\infty$ a $\max(-\infty, a) = a$ pro libovolné a (včetně $-\infty$), tak nám to bude skvěle fungovat.

Teď se naučíme s polynomy pracovat. Nejprve si zadefinujeme klasické operace. Budou samozřejmě inspirovány tím, co dobře známe, připomeneme násobení reálných polynomů:
$(a_0+a_1x+\cdot+a_nx^n)\cdot(b_0+b_1x+\cdots+b_mx^m)=[a_0b_0]+[a_0b_1+a_1b_0]x+[a_0b_2+a_1b_1+a_2b_0]x^2+\cdots+[a_nb_m]x^{n+m}$.
Jenže my teď nemáme sčítání ani násobení, ale nějaké neznámé operace z okruhu R, takže musíme zapisovat opatrněji.

! **Definice.**
Nechť $(R,\oplus,\odot)$ je okruh. Pro polynomy $p=\sum_{k=0}^{n}a_kx^k$ a $q=\sum_{k=0}^{m}b_kx^k$ a $c\in R$ definujeme operace takto:
3) Definujeme **skalární násobek polynom** jako

$$c\boxdot p=\sum_{k=0}^{n}(c\odot a_i)x^k.$$

2) Doplněním mocnin typu $0x^i$ můžeme předpokládat, že $m=n$, pak definujeme **součet polynomů** jako

$$p\boxplus q=\sum_{k=0}^{n}(a_k\oplus b_k)x^k.$$

3) Definujeme **součin polynomů** jako

$$p\boxdot q=\sum_{k=0}^{m+n}\Big(\sum_{i+j=k}a_i\odot b_j\Big)x^k.$$

Zavedli jsme značení $\boxplus$ a $\boxdot$ pro operace mezi polynomy, abychom mohly ve výpočtech a důkazech správně indikovat, kterou operaci používáme. Jakmile nabereme trochu zkušenosti, přejdeme k obvyklé úmluvě, že se operace mezi polynomy značí stejnou značkou jako operace v R.

Význam definice vynikne v dlouhém zápise. Jestliže $p=a_0+a_1x+\cdots+a_{n-1}x^{n-1}+a_nx^n$ a $q=b_0+b_1x+\cdots+b_{m-1}x^{m-1}+b_mx^m$, pak pro $m=n$ máme

$$p\boxplus q=[a_0\oplus b_0]+[a_1\oplus b_1]x+\cdots+[a_{n-1}\oplus b_{n-1}]x^{n-1}+[a_n\oplus b_n]x^n,$$

pro libovolná m,n pak máme

$$p\boxdot q=[a_0\odot b_0]+[(a_0\odot b_1)\oplus(a_1\odot b_0)]x+[(a_0\odot b_2)\oplus(a_1\odot b_1)\oplus(a_2\odot b_0)]x^2+\cdots$$
$$\cdots+[(a_{n-1}\odot b_m)\oplus(a_n\odot b_{m-1})]x^{n-1}+[a_n\odot b_m]x^{n+m}.$$

Všimněte si, že jde zase jen o manipulaci s koeficienty, takže tyto operace bychom mohli stejně tak definovat pro vektory koeficientů:

$$c\boxdot(a_0,a_1,\dots,a_n)=(c\odot a_0,c\odot a_1,\dots,c\odot a_n)$$
$$(a_0,a_1,\dots,a_n)\boxplus(b_0,b_1,\dots,b_n)=(a_0\oplus b_0,a_1\oplus b_1,\dots,a_n\oplus b_n)$$
$$(a_0,a_1,\dots,a_n)\boxdot(b_0,b_1,\dots,b_m)=(a_0\odot b_0,(a_0\odot b_1)\oplus(a_1\odot b_0),\dots,a_n\odot b_m).$$

Sice to funguje stejně, ale museli bychom si to pamatoval jako pravidla, zatímco ten zápis s „mocninami“ nám napovídá, jak operace dělat. Má tedy své výhody, jak ukáže příklad.

Příklad 8c.d: Uvažujme polynomy $p=\begin{pmatrix}0&-23\\1&0\end{pmatrix}+\begin{pmatrix}1&0\\0&13\end{pmatrix}x$ a $q=\begin{pmatrix}3&13\\0&14\end{pmatrix}+\begin{pmatrix}3&-6\\1&7\end{pmatrix}x$ z okruhu polynomů $M_2(\mathbb{Z})[x]$ a $c=\begin{pmatrix}2&0\\-1&0\end{pmatrix}\in M_2(\mathbb{Z})$. Pak máme

$$c\boxdot q=\begin{pmatrix}2&0\\-1&0\end{pmatrix}\boxdot\Big[\begin{pmatrix}0&-23\\1&0\end{pmatrix}+\begin{pmatrix}1&0\\0&13\end{pmatrix}x\Big]=\Big[\begin{pmatrix}2&0\\-1&0\end{pmatrix}\begin{pmatrix}0&-23\\1&0\end{pmatrix}\Big]+\Big[\begin{pmatrix}2&0\\-1&0\end{pmatrix}\begin{pmatrix}1&0\\0&13\end{pmatrix}\Big]x$$
$$=\begin{pmatrix}0&-46\\-1&0\end{pmatrix}+\begin{pmatrix}2&0\\0&-13\end{pmatrix}x,$$
$$p\boxplus q=\Big[\begin{pmatrix}0&-23\\1&0\end{pmatrix}+\begin{pmatrix}3&13\\0&14\end{pmatrix}\Big]+\Big[\begin{pmatrix}1&0\\0&13\end{pmatrix}+\begin{pmatrix}3&-6\\1&7\end{pmatrix}\Big]x$$
$$=\begin{pmatrix}3&-10\\1&14\end{pmatrix}+\begin{pmatrix}4&-6\\1&20\end{pmatrix}x$$

a

$$\begin{aligned} p \boxdot q &= \left[\begin{pmatrix} 0 & -23 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 13 \end{pmatrix} x\right] \boxdot \left[\begin{pmatrix} 3 & 13 \\ 0 & 14 \end{pmatrix} + \begin{pmatrix} 3 & -6 \\ 1 & 7 \end{pmatrix} x\right] \\ &= \left[\begin{pmatrix} 0 & -23 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & 13 \\ 0 & 14 \end{pmatrix}\right] + \left[\begin{pmatrix} 0 & -23 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 3 & -6 \\ 1 & 7 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 13 \end{pmatrix}\begin{pmatrix} 3 & 13 \\ 0 & 14 \end{pmatrix}\right] x + \left[\begin{pmatrix} 1 & 0 \\ 0 & 13 \end{pmatrix}\begin{pmatrix} 3 & -6 \\ 1 & 7 \end{pmatrix}\right] x^2 \\ &= \begin{pmatrix} 0 & -322 \\ 3 & 13 \end{pmatrix} + \begin{pmatrix} -20 & -148 \\ 3 & -1086 \end{pmatrix} x + \begin{pmatrix} 3 & -6 \\ 13 & 91 \end{pmatrix} x^2. \end{aligned}$$

Protože víme, že násobení matic není komutativní, je třeba být opatrný na správné pořadí matic při roznásobování závorek. Z toho pak usoudíme, že násobení polynomů nebude obecně komutativní.
△

Vytvářením polynomů neztratíme základní vlastnosti.

Věta 8c.5.
Nechť $(R, \oplus, \odot)$ je okruh. Pak je $(R[x], \boxplus, \boxdot)$ také okruh.
Jestliže je $(R, \oplus, \odot)$ komutativní, pak je také $(R[x], \boxplus, \boxdot)$ komutativní.

Důkaz si v této přehledové kapitole odpustíme, je snadný, ale dlouhý, než se ověří všech 7 až 8 axiomů.
Teď se podíváme, které z vlastností známých pro běžné reálné polynomy platí i obecně. Začneme stupněm.

Fakt 8c.6.
Nechť R je okruh a $p, q \in R[x]$. Pak $\mathrm{st}(p \boxplus q) \leq \max(\mathrm{st}(p), \mathrm{st}(q))$ a $\mathrm{st}(p \boxdot q) \leq \mathrm{st}(p) + \mathrm{st}(q)$.

To první tvrzení nepřekvapí, sečtením polynomů se nemůže stupeň navýšit, zato se vyšší mocniny mohou ztratit, když se pokrátí, například $(x+1) + (-x+1) = 2$. Zato u násobení asi čtenář čekal rovnost, jenže tady je zádrhel s děliteli nuly. Například v okruhu $\mathbb{Z}_4$ máme $(2x+1) \cdot (2x+1) = 4x^2 + 4x + 1 = 0x^2 + 0x + 1 = 1$.
Takovýmto problémům se dá vyhnout, když se jako základ použije těleso.

Věta 8c.7.
Je-li R těleso, pak $R[x]$ je okruh integrity a pro $p, q \in R[x]$ platí $\mathrm{st}(p \boxdot q) = \mathrm{st}(p) + \mathrm{st}(q)$.

Vůbec se dá říct, že pokud chceme, aby se polynomy chovaly tak, jak jsme zvyklí, tak potřebujeme začít s tělesem. Jako příklad si dokážeme, že funguje dělení polynomů se zbytkem.

Věta 8c.8.
Nechť F je těleso a p, d jsou polynomy z $F[x]$, nechť $d \neq 0$.
Pak existují polynomy $q, r \in F[x]$ takové, že $p = q \boxdot d \boxplus r$ a $\mathrm{st}(r) < \mathrm{st}(d)$.

Důkaz (drsný, poučný)**:** Důkaz povedeme silnou indukcí na $\mathrm{st}(p)$ a zároveň tím ukážeme algoritmus. Zkuste si rozmyslet, že je to pořád náš starý známý algoritmus na dělení polynomů se zbytkem, jen obecně nemůžeme mluvit o odčítání a dělení, místo toho používáme opačné a inverzní prvky.

(0) Nechť $\mathrm{st}(p) = 0$. Pak je $p = a_0$ konstantní polynom. Jestliže $\mathrm{st}(d) > 0$, pak $p = 0 \boxdot d \boxplus p$ a $\mathrm{st}(p) < \mathrm{st}(d)$, tedy lze vzít $r = p$. Jestliže $\mathrm{st}(d) = 0$, tak je $d = b_0$ konstantní polynom a díky našemu předpokladu není nulový. b_0 má tedy inverzi vůči násobení v F a můžeme psát $a_0 = a_0 \odot b_0^{-1} \odot b_0 \oplus 0$ neboli $p = (a_0 \odot b_0^{-1}) \boxdot d \boxplus r$, kde $r = 0$, proto $\mathrm{st}(r) = -\infty < 0 = \mathrm{st}(d)$.

(1) Předpokládejme, že tvrzení platí pro všechny polynomy stupně nejvýše n. Mějme polynom p stupně $n+1$ a nenulový polynom d. Jestliže $\mathrm{st}(d) > \mathrm{st}(p)$, pak položíme $p = 0 \boxdot d \boxplus p$ a je to.

Jinak nechť a_{n+1} je nejvyšší nenulový koeficient p a b_m je nejvyšší nenulový koeficient d, máme $m \leq n+1$. Pak polynom

$(-a_{n+1} \odot b_m^{-1}) x^{n+1-m} \boxdot d$ má nejvyšší koeficient rovný $-a_{n+1}$ a je u mocniny $x^{m+n+1-m} = x^{n+1}$, takže po přičtení k p dostaneme, že polynom $h = p \boxplus (-a_{n+1} \odot b_m^{-1}) x^{n-m} \boxdot d$ má určitě stupeň menší než $n+1$. To znamená, že na něj můžeme aplikovat indukční předpoklad a dostáváme polynomy q', r takové, že $\mathrm{st}(r) < \mathrm{st}(d)$ a $h = q' \boxdot d \boxplus r$. Pak

$$\begin{aligned} p &= h \boxplus (-a_{n+1} \odot b_m^{-1}) x^{n+1-m} \boxdot d = (-a_{n+1} \odot b_m^{-1}) x^{n+1-m} \boxdot d \boxplus q' \boxdot d \boxplus r \\ &= [(-a_{n+1} \odot b_m^{-1}) x^{n+1-m} \boxplus q'] \boxdot d \boxplus r \end{aligned}$$

a pořád $\mathrm{st}(r) < \mathrm{st}(d)$. Rozklad je hotov.

□

Když umíme dělit, můžeme také zavést pojem dělitelnosti, hledat společné násobky a dělitele a další věci, jako se to dělá v kapitole 6a. Obecně se dá říct, že když máme polynomy nad tělesem, tak vše funguje v zásadě stejně, a to dokonce včetně Bezoutovy věty a rozšířeného Euklidova algoritmu, i když si asi umíte představit, že dělit v Euklidovi polynomy se zbytkem, přičemž koeficienty jsou z nějakého exotického tělesa, je poněkud dobrodružnější, než když se to dělá s čísly.

Můžeme také zavést pojem inspirovaný prvočísly.

Definice.
Nechť R je okruh. Řekneme, že polynom $p \in R[x]$ je **ireducibilní** (**irreducible**), jestliže neexistují polynomy $q, r \in R[x]$ takové, že $p = q \boxdot r$, $\mathrm{st}(q) < \mathrm{st}(p)$ a $\mathrm{st}(r) < \mathrm{st}(p)$.

Pro reálné polynomy jsou ireducibilními polynomy všechny konstantní, lineární a pak ty kvadratické, které nemají reálné kořeny. Pokud máme polynomy nad tělesem, jsme schopni každý polynom rozložit na součin ireducibilních faktorů, podobně jako prvočíselný rozklad celých čísel.

Teď se podíváme na poslední velké téma, z formálních polynomů vytvoříme zobrazení (či funkci, chcete-li) z R do R. Není v tom žádné překvapení, pro polynom $p = a_n x^n + \cdots + a_1 x + a_0$ definujeme ono zobrazení předpisem

$$r \mapsto (a_n \odot r^n) \oplus \cdots \oplus (a_1 \odot r) \oplus a_0.$$

Říkáme, že do polynomu dosazujeme $r \in R$, hodnotu značíme $p(r)$.

Příklad 8c.e: Uvažujme polynom $p = \begin{pmatrix} 1 & 0 \\ 0 & 13 \end{pmatrix} x + \begin{pmatrix} 0 & -23 \\ 1 & 0 \end{pmatrix}$ z prostoru $M_2(\mathbb{Z})[x]$. Můžeme do něj dosadit třeba $x = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \in M_2(\mathbb{Z})$ a dostaneme

$$p(x) = \begin{pmatrix} 1 & 0 \\ 0 & 13 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 0 & -23 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -22 \\ 1 & 0 \end{pmatrix}.$$

△

Pro toto dosazování platí běžná pravidla, dá se například dokázat, že pro polynomy p, q získáme dosazením do $p \boxplus q$ stejnou hodnotu, jako kdybychom dosadili do p a q zvlášť a výsledky spojili pomocí $\oplus$. Formálně řečeno: $(p \boxplus q)(r) = p(r) \oplus q(r)$, podobně $(p \boxdot q)(r) = p(r) \odot q(r)$.

Je třeba si ale uvědomit, že zobrazení daná polynomy jsou obecně jinými objekty než polynomy, které jim daly vzniknout. Čtenář je samozřejmě zvyklý na polynomy reálné, kde se polynom a funkce z něj vzniklá berou jako totéž. To je odůvodněno základním faktem, že když dva polynomy dávají stejné hodnoty coby reálné funkce, tak už musí jít o stejné polynomy coby výrazy, tedy musejí se rovnat všechny koeficienty. Bohužel, toto neplatí u polynomů nad obecnými tělesy. Může se stát, že dva polynomy, které mají různé koeficienty, dávají při dosazování $r \in R$ tvrdošíjně stále stejné hodnoty, takže z nich vzniká stejné zobrazení. Pro případ není třeba chodit daleko, viz kapitola 7c.

Proto je třeba obecně dbát na rozdíl mezi polynomem jako výrazem a zobrazením vzniklým pomocí onoho polynomu.

Definice.
Nechť R je okruh, uvažujme polynom $p \in R[x]$. Řekneme, že prvek $r \in R$ je **kořen** (**root**) polynomu p, jestliže po dosazení do p platí $p(r) = 0$.

Pro tělesa pak máme povědomé tvrzení.

Věta 8c.9.
Nechť F je těleso, uvažujme polynom $p \in F[x]$.
Prvek $r \in F$ je kořenem p právě tehdy, když polynom $x + (-r)$ dělí p.

Znamená to, že polynom, který má kořen, již nemůže být ireducibilní. Obměna tedy říká, že ireducibilní polynom nemá kořeny. Platí to i naopak? Obecně ne, dokonce ani u reálných polynomů, například polynom $(1+x^2)(1+x^2)$ reálné kořeny nemá, ale rozložit jej lze. Pro polynomy nižšího stupně už ale ireducibilita a neexistence kořenů souhlasí dokonce obecně.

Fakt 8c.10.
Nechť F je těleso, p je polynom z $F[x]$ stupně 2 nebo 3.
p je ireducibilní v $F[x]$ právě tehdy, když nemá kořeny v F.

Důkaz (poučný)**:** Neexistenci kořenů pro ireducibilní polynomy jsme už ukázali výše.

Předpokládejme naopak, že polynom p není ireducibilní, tedy $p = s \odot t$, kde s, t jsou polynomy se stupni menšími než $\mathrm{st}(p)$. Protože $\mathrm{st}(p) \leq 3$, musí být alespoň jeden z polynomů s, t stupně jedna, čili polynom ve tvaru $x + r$. Pak je $(-r) \in F$ jeho kořenem, tedy i kořenem p.

□

Tímto končíme stručný přehled vlastností polynomů nad okruhy.

8d. Bonus: Racionální čísla

Zde si položíme zdánlivě jednoduchou otázku: Co jsou to racionální čísla? Je svůdné odpovědět, že to jsou zlomky, jenže co je to vlastně za objekt? Zdá se přirozené definovat zlomek jako uspořádanou dvojici čísel, pro kterou jsme zvolili speciální zápis, jenže tento nápad má zásadní problém. Pokud přijmeme, že $\frac{1}{2}$ je zápis pro dvojici $(1, 2)$, co je pak $\frac{2}{4}$? Jako dvojice $(2, 4)$ je to zcela jiný objekt než $(1, 2)$, ale my bychom to rádi brali jako jednu věc. Je vidět, že to nebude tak snadné, ale s trochou práce se s tím vypořádáme.

V této kapitole korektně vybudujeme množinu racionálních čísel, přičemž si krásně ukážeme v akci pojmy z několika kapitol této knihy. Protože důkazy jsou často spíš technické (nahání se triviální rovnosti a nerovnosti), čtenář je případně může přeskočit a soustředit se na tok myšlenek.

8d.1 Budujeme zlomky

Začneme množinou, která se nabízí, provizorně si ji nazveme $\mathbb{F}$ jako „fractions“:

$$\mathbb{F} = \big\{(p, q);\ p, q \in \mathbb{Z} \wedge q \neq 0\big\}.$$

Pro ušetření místa a znaků se domluvíme, že místo dvojic (p, q) budeme psát $\frac{p}{q}$.

Teď potřebujeme matematicky zachytit, že například zlomky $\frac{4}{6}$ a $\frac{6}{9}$ jsou vlastně stejná věc. Na to se přesně hodí pojem relace.

Definice 8d.2.
Definujeme relaci $\sim$ na množině $\mathbb{F}$ předpisem $\frac{p}{q} \sim \frac{u}{v}$ právě tehdy, když $pv = uq$.

Protože $4 \cdot 9 = 6 \cdot 6$, máme $\frac{4}{6} \sim \frac{6}{9}$, přesně jak bychom chtěli. Tato ekvivalence má geometrický význam. Každý zlomek $\frac{p}{q}$ neboli (p, q) reprezentuje určitou délku na reálné ose, tuto délku získáme tak, že si vezmeme úsek délky p a rozdělíme jej na q shodných částí (zde je nutno precizovat, co toto znamená, když je jedno či obě čísla záporné, vzniká tím orientace). Není obtížné si rozmyslet, že dva zlomky jsou v relaci $\sim$ právě tehdy, když dávají stejnou geometrickou délku.

Čtenář již možná tuší, co od naší relace očekáváme.

Fakt 8d.3.
Relace $\sim$ je na $\mathbb{F}$ ekvivalence.

Důkaz (rutinní)**:** 1) reflexivita: Nechť $\frac{p}{q} \in \mathbb{F}$. Protože určitě $pq = pq$, je i $\frac{p}{q} \sim \frac{p}{q}$.

2) symetrie: Nechť $\frac{p}{q}, \frac{u}{v} \in \mathbb{F}$ a předpokládejme, že $\frac{p}{q} \sim \frac{u}{v}$. Pak $pv = uq$, proto i $uq = pv$ a tedy $\frac{u}{v} \sim \frac{p}{q}$.

3) tranzitivita: Nechť $\frac{p}{q}, \frac{u}{v}, \frac{s}{t} \in \mathbb{F}$ a předpokládejme, že $\frac{p}{q} \sim \frac{u}{v}$ a $\frac{u}{v} \sim \frac{s}{t}$. Podle definice to znamená $pv = uq$ a $ut = vs$. Protože $t \neq 0$ a $q \neq 0$, můžeme obě rovnice vynásobit na tvar $pvt = uqt$ a $utq = vsq$, což dává $pvt = vsq$. Protože také $v \neq 0$, zkrátíme a dostáváme $pt = sq$ neboli $\frac{p}{q} \sim \frac{s}{t}$.

□

Množina $\mathbb{F}$ se tedy rozpadne na třídy ekvivalence. Každá třída ekvivalence obsahuje všechny zlomky, které geometricky vyjadřují jednu konkrétní délku neboli určitou kvantitu.

Definice 8d.4.
Definujeme množinu $\mathbb{Q}$ racionálních čísel jako množinu všech tříd ekvivalence relace $\sim$,
značíme $\mathbb{Q} = \{[f];\ f \in F\}$.

Teď můžeme přesně říct, jak vlastně v praxi fungují racionální čísla. Když si vezmeme třeba $\frac{4}{6}$, tak ve skutečnosti myslíme na celou třídu ekvivalence, tedy jakoby bereme i ostatní zlomky ekvivalentní k $\frac{4}{6}$, protože víme, že z hlediska praxe je jedno, kterého zástupce dotyčné třídy ekvivalence si vybereme. To jsme ovšem ještě nedokázali, máme co dohánět. Zatím díky kapitole 4a víme, že když si pro dotyčnou třídu vybereme jiného zástupce, dá nám stejnou třídu ekvivalence, tedy dosáhneme z něj na stejné zlomky. Ještě jsme ale nedokázali, že si můžeme zástupce vybírat i v případech, kdy se zlomky provádíme rozličné běžné věci jako porovnávání, operace a podobně. Nejprve si samozřejmě musíme tyto věci zadefinovat.

Poznámka doplňující: V řeči faktorových množin můžeme napsat $\mathbb{Q} = \mathbb{F}/\sim$.

8d.5 Porovnáváme zlomky

Jak porovnáváme zlomky v praxi? Porovnáme kvantity, které reprezentují. Abychom to udělali správně matematicky, musíme toto porovnávání vyjádřit čistě pomocí zúčastněných čísel a známých matematických operací, což ale není problém, například $\frac{3}{5} < \frac{7}{8}$ se dá hravě přepsat na $3 \cdot 8 < 7 \cdot 5$. Tím je inspirována definice. Je v tom ale háček, my jsme se od $\frac{3}{5} < \frac{7}{8}$ k $3 \cdot 8 < 7 \cdot 5$ dostali vynásobením, ale to funguje jen v případech, kdy jsou jmenovatelé kladní. Vyřešíme to jednoduše, prostě si vezmeme vhodné zástupce ze tříd.

Definice 8d.6.
Definujeme uspořádání $<$ na $\mathbb{Q}$ následujícím předpisem: třídy $x, y \in \mathbb{Q}$ splňují $x < y$ právě tehdy, když existují $\frac{p}{q} \in x$ a $\frac{u}{v} \in y$ takoví, že $p > 0$, $v > 0$ a $pv < uq$.

Dále budeme namísto „$p > 0$, $v > 0$“ zkráceně psát jen $p, v > 0$.

Protože u každé třídy dokážeme vybrat zástupce $\frac{p}{q}$ tak, aby $q > 0$, vztahuje se tato definice na všechny třídy a dokážeme tedy vždy rozhodnout, zda je nějaká dvojice tříd v relaci nebo ne. Aby byla definice korektní, musíme ještě ukázat, že toto rozhodnutí nezáleží na volbě zástupců.

Frac 8d.7.
Nechť $\frac{p}{q}, \frac{u}{v}, \frac{P}{Q}, \frac{U}{V} \in \mathbb{F}$, předpokládejme, že $q, Q, v, V > 0$, $\left[\frac{p}{q}\right] = \left[\frac{P}{Q}\right]$ a $\left[\frac{u}{v}\right] = \left[\frac{U}{V}\right]$. Pak $\left[\frac{p}{q}\right] < \left[\frac{u}{v}\right]$ právě tehdy, když $\left[\frac{P}{Q}\right] < \left[\frac{U}{V}\right]$.

Důkaz (rutinní)**:** Díky symetrii situace stačí ukázat jeden směr, druhý se dokazuje obdobně (zkuste si to).

Předpokládejme tedy, že $\left[\frac{p}{q}\right] < \left[\frac{u}{v}\right]$ neboli $pv < uq$, po vynásobení číslem $Q > 0$ dostáváme $pvQ < uqQ$. Z předpokladu $\left[\frac{p}{q}\right] = \left[\frac{P}{Q}\right]$ máme $pQ = Pq$, po vynásobení číslem $v \neq 0$ dostáváme $pQv = Pqv$. Spojením s odvozenou nerovností máme $Pqv < uqQ$, po zkrácení číslem $q > 0$ máme $Pv < uQ$ a jsme v polovině cesty.

Obdrženou nerovnost vynásobíme číslem $V > 0$, dostáváme $PvV < uQV$. Z předpokladu $\left[\frac{u}{v}\right] = \left[\frac{U}{V}\right]$ máme $uV = Uv$, po vynásobení číslem $Q \neq 0$ vyjde $uVQ = UvQ$. Spojením dostáváme $PvV < UvQ$, a když zkrátíme číslem $v > 0$, máme $PV < UQ$ neboli $\left[\frac{P}{Q}\right] < \left[\frac{U}{V}\right]$.

Všimněte si, že jsme v důkazu silně závislí na předpokladu $q, Q, v, V > 0$.

□

Dokázali jsme, že naše definice porovnávání nezáleží na volbě zástupců (s kladnými druhými složkami) ze tříd ekvivalence. Umíme tedy porovnávat zlomky. K naší úplné spokojenosti chybí ještě dvě věci.

Definice 8d.8.
Definujeme relaci $>$ na $\mathbb{Q}$ jako $<^{-1}$.
Definujem relaci $\leq$ na $\mathbb{Q}$ předpisem $x \leq y$ právě tehdy, když $[x < y$ nebo $x = y]$.
Definujeme relaci $\geq$ na $\mathbb{Q}$ jako $\leq^{-1}$.

Teď už máme k dispozici všechna porovnávání, na která jsme zvyklí, a dokážeme, že fungují dle očekávání.

Fakt 8d.9.
Relace $\leq$ a $\geq$ jsou lineární částečná uspořádání na $\mathbb{Q}$.
Relace $<$ a $>$ jsou ostrá uspořádání na $\mathbb{Q}$.

Důkaz (z povinnosti)**:** 1) $<$ je ostré uspořádání:

Asymetrie: Nechť $x, y \in \mathbb{Q}$ splňují $x < y$. Zvolme $\frac{p}{q} \in x$, $\frac{u}{v} \in y$ tak, aby $q, v > 0$. Předpoklad dává $pv < uq$, pak ovšem nemůže zároveň platit $pv < uq$ a tedy ani $y < x$.

Tranzitivita: Nechť $x, y, z \in \mathbb{Q}$ splňují $x < y$ a $y < z$. Zvolme $\frac{p}{q} \in x$, $\frac{u}{v} \in y$ a $\frac{s}{t} \in y$ tak, aby $q, v, t > 0$. Dle předpokladu pak $pv < uq$ a $ut < sv$. Vynásobíme první nerovnost číslem $t > 0$ a druho číslem $q > 0$, vyjde $pvt < uqt$ a $utq < svq$ neboli $pvt < svq$. Vydělíme číslem $v > 0$ a dostáváme $pt < sq$, tedy $x < z$ neboli $x \leq z$.

2) Z části 1) a Věty 4b.5 vyplývá, že $\leq$ je částečné uspořádání.

Linearita: Mějme libovolné $x, y \in \mathbb{Q}$. Zvolme zástupce $\frac{p}{q} \in x$, $\frac{u}{v} \in y$ tak, aby $q, v > 0$. Jestliže $pv = uq$, tak $x = y$ a proto dle definice $x \leq y$. Jinak máme dvě různá celá čísla pv, uq, proto buď $pv < uq$, pak $x < y$ a tedy i $x \leq y$, nebo $pv > uq$, což znamená $uq < pv$ neboli $y < x$ neboli $y \leq x$. Ukázali jsme, že prvky x, y jsou porovnatelné.

3) Z 1), 2) a Věty 3c.3 vyplývá, že i $>$ je ostré a $\geq$ je částečné uspořádání, důkaz linearity je obdobný.

□

Doporučujeme čtenáři, aby si jako cvičení zkusil dokázat přímo, že $\leq$ je částečné uspořádání.

8d.10 Počítáme se zlomky

V praxi zlomky sčítáme tak, že sečteme libovolně zvolené zástupce. Podobně funguje odčítání, násobení i dělení.

Definice 8d.11.
Nechť $x, y \in \mathbb{Q}$. Definujeme

$$x + y = \left[\frac{pv + uq}{qv}\right],$$
$$x - y = \left[\frac{pv - uq}{qv}\right],$$
$$x \cdot y = \left[\frac{pu}{qv}\right],$$
$$x/y = \left[\frac{pv}{qu}\right],$$

kde $\frac{p}{q} \in x$ a $\frac{u}{v} \in y$ jsou zvoleny libovolně.

I zde musíme začít důkazem, že výsledek operací nezáleží na volbě zástupců.

Věta 8d.12.
Nechť $\frac{p}{q}, \frac{u}{v}, \frac{P}{Q}, \frac{U}{V} \in \mathbb{F}$, předpokládejme, že $\left[\frac{p}{q}\right] = \left[\frac{P}{Q}\right]$ a $\left[\frac{u}{v}\right] = \left[\frac{U}{V}\right]$. Pak

$$\left[\frac{p}{q}\right] + \left[\frac{u}{v}\right] = \left[\frac{P}{Q}\right] + \left[\frac{U}{V}\right],$$
$$\left[\frac{p}{q}\right] - \left[\frac{u}{v}\right] = \left[\frac{P}{Q}\right] - \left[\frac{U}{V}\right],$$
$$\left[\frac{p}{q}\right] \cdot \left[\frac{u}{v}\right] = \left[\frac{P}{Q}\right] \cdot \left[\frac{U}{V}\right],$$
$$\left[\frac{p}{q}\right] \Big/ \left[\frac{u}{v}\right] = \left[\frac{P}{Q}\right] \Big/ \left[\frac{U}{V}\right].$$

Důkaz (z povinnosti)**:** 1) Sčítání: Z předpokladu máme $pQ = Pq$ a $uV = Uv$. Pak
$(pv + uq)(QV) = pvQV + uqQV = (pQ)vV + (uV)qQ = PqvV + UvqQ = PVqv + UQqv = (PV + UQ)(qv)$,
tedy $\frac{pv+uq}{qv} \sim \frac{PV+UQ}{QV}$. Proto $\left[\frac{pv+uq}{qv}\right] = \left[\frac{PV+UQ}{QV}\right]$.

2) Ostatní operace si čtenář jistě rád dokáže, je to snadné, ale únavné.

□

Již tradičně konstatujeme, že operace odčítání a dělení ve skutečnosti nejsou plnoprávné operace, ale jen zkratky pro jiné činnosti, jmenovitě pro výpočty $\left[\frac{p}{q}\right]+\left(-\left[\frac{u}{v}\right]\right)$ a $\left[\frac{p}{q}\right]\cdot\left[\frac{u}{v}\right]^{-1}$. Klíčové operace sčítání a násobení samozřejmě splňují všechna pravidla, na která jsme zvyklí, viz kapitola 8c.

Věta 8d.13.
Prostor $\left(\mathbb{Q},+,\cdot,\left[\frac{0}{1}\right],\left[\frac{1}{1}\right]\right)$ je těleso.

Důkaz (rutinní)**:** Důkazy jsou snadné, vycházejí z toho, že v definicích operací pro $\mathbb{Q}$ jsme použili tradiční operace pro reálná čísla, která všechny potřebné vlastnosti mají. Ukážeme dvě vlastnosti jako inspiraci, čtenář si dodělá zbytek.

Komutativita ščítání: Nechť $x,y\in\mathbb{Q}$, zvolme zástupce $\frac{p}{q}\in x$, $\frac{u}{v}\in y$. Pak díky komutativitě sčítání a násobení v $\mathbb{R}$ dostáváme

$$x+y=\left[\frac{pv+uq}{qv}\right]=\left[\frac{vp+qu}{vq}\right]=y+x.$$

Jednotkový prvek pro sčítání a násobení: Označme $0_Q=\left[\frac{0}{1}\right]$ a $1_Q=\left[\frac{1}{1}\right]$. Pak pro libovolné $x\in\mathbb{Q}$ zvolíme zástupce $\frac{p}{q}\in x$ a počítáme

$$x+0_Q=\left[\frac{p\cdot 1+0\cdot q}{q\cdot 1}\right]=\left[\frac{p}{q}\right]=x,$$
$$x\cdot 1_Q=\left[\frac{p\cdot 1}{q\cdot 1}\right]=\left[\frac{p}{q}\right]=x.$$

Obdobně $0_Q+x=x$ a $1_Q\cdot x=x$.

Invertibilita pro násobení: Nechť $x\in\mathbb{Q}$, $x\neq 0_Q$. Zvolme libovolného zástupce $\frac{p}{q}\in x$. Pak jistě $p,q\neq 0$ (jinak by $x=0_Q$), můžeme tedy uvažovat $y=\left[\frac{q}{p}\right]$. Dostáváme

$$x\cdot y=\left[\frac{pq}{qp}\right]=\left[\frac{1}{1}\right]=1_Q.$$

Obdobně $y\cdot x=1_Q$, proto je x invertibilní vůči násobení a $y=x^{-1}$.

□

8d.14 Zlomky a celá/reálná čísla

Pro zlomky coby třídy jsme definovali srovnání a operace. My jsme ovšem zvyklí vnímat zlomky jako rozšíření celých čísel, jinak řečeno, celá čísla by měla být obsažena v racionálních a operace by si měly odpovídat. Podobně by si měly odpovídat operace na zlomcích s operacemi a porovnáním u reálných čísel, protože bychom rádi vnímali zlomky coby podmnožinu reálných čísel. Jak se toto dá zařídit? Začneme čísly celými.

Zde je myšlenka jednoduchá, ztotožníme si celá čísla se zlomky, které označují celočíselné kvantity, tedy se zlomky typu $\frac{p}{1}$. Pro takovéto ztotožnění se v matematice používá pojem zobrazení.

Definujme T: $\mathbb{Z}\mapsto\mathbb{Q}$ předpisem $T(z)=\left[\frac{z}{1}\right]$. Množina $\mathbb{Z}$ se tímto zobrazením spojí s množinou $Z=T[\mathbb{Z}]\subseteq\mathbb{Q}$, jinak řečeno, když ze všech celých čísel vyrobíme zlomky a uvažujeme jejich třídy ekvivalence, pak dostáváme jistou podmnožinu Z množiny $\mathbb{Q}$. Na této podmnožině pak máme srovnání a operace tak, jak jsme je definovali pro třídy ekvivalence.

Tvrdíme ovšem, že tato množina Z je věrnou kopií celých čísel $\mathbb{Z}$, takže vyjde nastejno, jestli pracujeme s čísly $x,y\in\mathbb{Z}$ nebo jejich kopiemi $\left[\frac{z}{1}\right],\left[\frac{y}{1}\right]\in\mathbb{Q}$. Matematicky se tím dostáváme k isomorfismům, viz kapitola 13. Nebudeme se na tento jazyk odvolávat a raději řekneme přesně a otevřeně, co tím míníme.

Věta 8d.15.
Zobrazení T je bijekce $\mathbb{Z}\mapsto Z$. Dále pro všechna $x,y\in\mathbb{Z}$ platí:
(i) $x=y$ právě tehdy, když $T(x)=T(y)$;
(ii) $x\leq y$ právě tehdy, když $T(x)\leq T(y)$;
(iii) $x<y$ právě tehdy, když $T(x)<T(y)$;
(iv) $T(x+y)=T(x)+T(y)$;
(v) $T(x-y)=T(x)-T(y)$;
(vi) $T(x\cdot y)=T(x)\cdot T(y)$;
(vii) $T(x/y)=T(x)/T(y)$.

Čtenář jistě vidí, že na levé straně jsou srovnání/operace ze $\mathbb{Z}$ a na pravé z $\mathbb{Q}$ coby množiny tříd ekvivalence. Vlastnosti (i) až (iii) říkají, že když porovnáváme dvě celá čísla, pak vyjde nastejno, jestli je porovnáváme jako celá čísla, nebo si porovnáme jejich kopie v $\mathbb{Q}$ „po zlomkovsku“ dle naší definice.

U vlastností (iv) až (vii) pomůže, když si je vyjádříme ještě jinak. Protože T je bijekce, máme k dispozici i inverzní zobrazení $T^{-1}\colon Z \mapsto \mathbb{Z}$. Když jej aplikujeme třeba na (iv), dostáváme $T^{-1}(T(x+y)) = T^{-1}(T(x)+T(y))$ neboli $x+y = T^{-1}(T(x)+T(y))$. Jaká je interpretace? Jestliže chceme sečíst dvě celá čísla, tak to můžeme udělat přímo, nebo si představíme, že jsou to zlomky, sečteme je „po zlomkovsku“ a výsledek pak zase vezmeme jako celé číslo, vyjde to nastejno.

Všimněte si mimochodem, že jsme při aplikování T^{-1} na třídu $T(x)+T(y) \in \mathbb{Q}$ mlčky předpokládali, že to jde, tedy že ten součet je zase z množiny Z. To vůbec není samozřejmé a musí se to u všech operací dokázat. Jazykem binárních operací má platit, že množina Z je uzavřená na sčítání, násobení a přechod k opačným a inverzním prvkům.

Důkaz (z povinnosti, možná poučný)**:**

(i): $x = y \iff x\cdot 1 = y\cdot 1 \iff \left[\frac{x}{1}\right] = \left[\frac{y}{1}\right] \iff T(x) = T(y)$.

(iii): Protože $1 > 0$, je $\frac{x}{1}$ vhodným zástupcem pro $\left[\frac{x}{1}\right]$ při porovnávání, podobně u y. Proto

$$x < y \iff x\cdot 1 < y\cdot 1 \iff \left[\frac{x}{1}\right] < \left[\frac{y}{1}\right] \iff T(x) < T(y).$$

(ii): Je to kombinace (i) a (iii).

(iv): $T(x+y) = \left[\frac{x+y}{1}\right] = \left[\frac{x\cdot 1 + y\cdot 1}{1\cdot 1}\right] = \left[\frac{x}{1}\right] + \left[\frac{y}{1}\right] = T(x)+T(y)$.

Při čtení zprava vidíme, že třída $T(x)+T(y)$ je dána zástupcem $\frac{x+y}{1}$, patří tedy zase do Z, množina Z je tedy uzavřená na sčítání.

Zbytek důkazu je obdobný.

□

Shrneme-li naše poznatky, tak množina $\mathbb{Z}$ a její kopie Z mají i stejnou algebraickou strukturu, lze je tedy z praktického pohledu považovat za totéž. Více jsme o tom psali v kapitole 13.

Zapojení zlomků mezi reálná čísla probíhá podobně, v rámci reálných čísel si vytvoříme kopii našeho $\mathbb{Q}$ pomocí přirozeného kandidáta, zobrazení $\left[\frac{p}{q}\right] \mapsto (p/q)$. Pak se ukáže obdoba věty výše o porovnání a operacích. Nebudeme to zde dělat, je to rutiní práce a důkazy jsou obdobné. Abychom knihu nenatahovali, necháme to zvídavému (a pilnému) čtenáři, cíl kapitoly už byl dosažen: Nahlédli jsme do matematické kuchyně a viděli jsme některé probrané pojmy v akci.