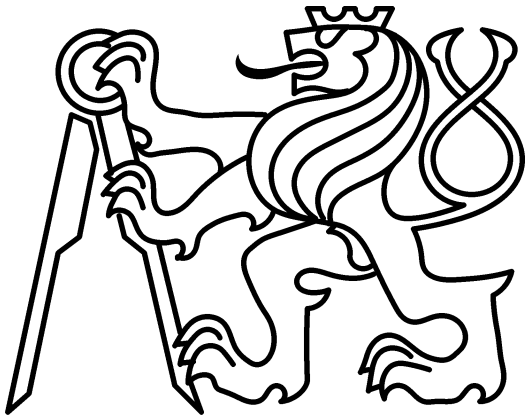
České Vysoké Učení Technické v Praze
Fakulta elektrotechnická

Diskrétní matematika

Sbírka řešených příkladů

Jiří Velebil
katedra matematiky
Praha, 2007

velebil@math.feld.cvut.cz
http://math.feld.cvut.cz/velebil



Obsah

Úvod

Text, který máte před sebou, by měl posloužit jako sbírka řešených příkladů k předmětu *Diskrétní matematika* Y01DMA pro druhý ročník. Jde o jeho první variantu, proto přivítám jakékoli reakce.

Řazení textu. Text je rozdělen do kapitol zhruba podle témat syllabu přednášky *Diskrétní matematika*. Většinu příkladů doprovází komentáře, upozorňující na důležité momenty řešení nebo na časté chyby v postupu řešení.

Důležité upozornění. Řadu dalších řešených příkladů lze najít ve skriptech *Diskrétní matematika*, viz stránky http://math.feld.cvut.cz/velebil.

Text je zveřejněn jako „klikací PDF“, tj. jako soubor s hypertextovými odkazy. Přesto nejde o „klikací knihu“, takový text bych psal a řadil úplně jinak. Hypertextové odkazy jsou vytvořeny jen pro zpříjemnění prohlížení elektronické podoby dokumentu.

Poděkování. K napsání byl použit systém LaTeX Leslieho Lamporta, hypertextové odkazy byly vytvořeny balíkem hyperref Sebastiana Rahtze a Heiko Oberdiek, obrázky byly nakresleny pomocí maker XY-pic Kristoffera H. Rose a Rosse Moorea.

Přeji Vám příjemnou četbu.

Jiří Velebil
V Praze, v červenci 2007

Kapitola 1

Matematická indukce

V odstavci 1.1 je vyřešeno několik klasických příkladů principy matematické indukce. Není možné postihnout všechny možné způsoby, kterými lze indukcí dokazovat. Přesto je možné říci, co *musí* každý korektní důkaz matematickou indukcí obsahovat:

1. Přesnou formulaci tvrzení, které dokazujeme. Toto tvrzení musí vždy mít tvar *Pro všechna přirozená čísla* $n \geq n_0$ *platí V(n).*

   Vlastnost $V(n)$ může být komplikovaná a vždy se vyplatí si uvědomit přesné znění $V(n)$, viz například 1.1.3.

2. Oznámení, podle čeho indukci provádíme. Pro tvrzení tvaru *Pro všechna přirozená čísla* $n \geq n_0$ *platí V(n)* je to n, pro tvrzení tvaru *Pro všechna přirozená čísla* $m \geq m_0$ *platí W(m)* je to m, a tak dále.

3. Jasný důkaz základního kroku indukce. Někdy musí být takových základních kroků více, viz příklad 1.1.3.

4. Indukční krok: zde musíme oznámit tvrzení, které chceme v indukčním kroku dokázat. Toto tvrzení pak musíme jasně dekomponovat a to nám umožní zformulovat a poté správně použít indukční předpoklad. Indukční předpoklad je zapotřebí přesně zformulovat.

   Soustružnické postupy (viz komentář k příkladu 1.1.1) při důkazu indukčního kroku nás většinou zavedou do slepých uliček. Mějte neustále na paměti, že korektní důkaz indukcí je dynamický: běží jako rekursivní algoritmus. Jste-li na pochybách o korektnosti svého důkazu, důkaz spusťte.

5. Dekompozice a formulace indukčního předpokladu signalisují, který z principů indukce náš důkaz využívá.

Dále jsou v odstavci 1.2 spočteny příklady na použití principu strukturální indukce. Použití tohoto principu je extrémně jednoduché: jde vždy o to, zda je jistá vlastnost invariantní na průchod zadanými pravidly. Přesto je i zde nutno jasně oddělit základní krok indukce a indukční krok.

1.1 Klasická matematická indukce

1.1.1 Příklad Dokažte, že pro všechna přirozená čísla $n \geq 1$ platí rovnost $\sum_{k=1}^{n} (-1)^{k+1} \cdot k^2 = \frac{(-1)^{n+1} n(n+1)}{2}$.

Řešení. Budeme využívat některý princip indukce a indukci povedeme podle n.

> **Komentář.** Fakt, že můžeme zkusit využít princip indukce plyne z toho, že námi dokazované tvrzení má tvar *Pro všechna přirozená čísla* $n \geq 1$ *platí* $V(n)$., kde vlastnost $V(n)$ je platnost rovnosti $\sum_{k=1}^{n} (-1)^{k+1} \cdot k^2 = \frac{(-1)^{n+1} n(n+1)}{2}$ pro pevné číslo n. Nevíme ovšem zatím, který z principů indukce použijeme. To nám řekne až dekomposice problému.

1. **Základní krok:** pro $n = 1$ ověříme platnost $V(n)$ přímým výpočtem. Levá strana rovnosti je:

$$\sum_{k=1}^{1} (-1)^{k+1} \cdot k^2 = (-1)^{1+1} \cdot 1^2 = 1$$

a pravá strana rovnosti je

$$\frac{(-1)^{1+1}1\cdot(1+1)}{2}=\frac{2}{2}=1.$$

Ověřili jsme, že $V(1)$ platí.

2. **Indukční krok:** zvolíme libovolné, ale pevné číslo $n\geq 1$. Máme ukázat platnost $V(n+1)$, neboli platnost rovnosti

$$\sum_{k=1}^{n+1}(-1)^{k+1}\cdot k^2=\frac{(-1)^{(n+1)+1}(n+1)\cdot((n+1)+1)}{2}.$$

Všimneme si, že levou stranu rovnosti lze přirozeným způsobem dekomponovat:

$$\sum_{k=1}^{n+1}(-1)^{k+1}\cdot k^2=\sum_{k=1}^{n}(-1)^{k+1}\cdot k^2+(-1)^{(n+1)+1}\cdot(n+1)^2$$

To nám dává návod, jak zformulovat **indukční předpoklad:** pro libovolné pevné $n\geq 1$ platí rovnost

$$\sum_{k=1}^{n}(-1)^{k+1}\cdot k^2=\frac{(-1)^{n+1}n(n+1)}{2}.$$

Komentář. Tento postup je typický: dekomposice nám dává návod, jak zformulovat indukční předpoklad a jak jej použít. Zároveň se dozvídáme, který princip indukce budeme používat (v tomto případě jde o slabý princip indukce, protože dekomposice sahá o jeden krok zpátky do historie).

Indukční předpoklad nyní použijeme na levou (dekomponovanou) stranu rovnice:

$$\sum_{k=1}^{n}(-1)^{k+1}\cdot k^2+(-1)^{(n+1)+1}\cdot(n+1)^2=\frac{(-1)^{n+1}n(n+1)}{2}+(-1)^{(n+1)+1}\cdot(n+1)^2$$

V součtu napravo už můžeme použít normální aritmetiku f a dostáváme tak rovnost

$$\frac{(-1)^{n+1}n(n+1)}{2}+(-1)^{(n+1)+1}\cdot(n+1)^2=\frac{(-1)^{(n+1)+1}(n+1)\cdot((n+1)+1)}{2}.$$

Indukční krok je u konce, dokázali jsme platnost rovnosti

$$\sum_{k=1}^{n+1}(-1)^{k+1}\cdot k^2=\frac{(-1)^{(n+1)+1}(n+1)\cdot((n+1)+1)}{2}.$$

Komentář. Častou chybou při důkazu indukčního kroku je „soustružení“ dokazovaného vztahu. V našem případě by takový postup mohl vypadat takto:

$$\begin{aligned}\sum_{k=1}^{n+1}(-1)^{k+1}\cdot k^2 &= \frac{(-1)^{(n+1)+1}(n+1)\cdot((n+1)+1)}{2}\\ (-1)^{(n+1)+1}\cdot(n+1)^2 &= \frac{(-1)^{(n+1)+1}(n+1)\cdot((n+1)+1)}{2}-\frac{(-1)^{n+1}n(n+1)}{2}\\ &\vdots\\ 0 &= 0\end{aligned}$$

Proč je tento postup nesprávný? Především: rovnost $0=0$ jsme jistě dokázat nechtěli. Předchozí řádky máme tedy číst *odspodu nahoru*, abychom z platnosti rovnosti $0=0$ odvodili platnost rovnosti $\sum_{k=1}^{n+1}(-1)^{k+1}\cdot k^2=\frac{(-1)^{(n+1)+1}(n+1)\cdot((n+1)+1)}{2}$. K tomu je zapotřebí vědět, že všechny použité úpravy jsou reversibilní. Často tomu tak skutečně může být (v našem příkladě jsme při přechodu z prvního na druhý řádek „odčítali rovnost“), často je reversibilita velmi problematická (příklady 1.1.2 a 1.1.3) a často je zcela nemožná (příklad 1.1.4). Závěr? Soustružení nepoužívejte!

Důkaz indukcí je u konce, použili jsme slabý princip matematické indukce. ■

1.1.2 Příklad Dokažte, že nerovnost $\frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{2n}>\frac{1}{2}$ platí pro všechna přirozená čísla $n\geq 2$.

Řešení. Budeme postupovat nějakým principem indukce podle $n\geq 2$.

1. **Základní krok:** pro $n=2$ je levá strana nerovnosti výraz $\frac{1}{2+1}+\frac{1}{4}$ neboli číslo $\frac{7}{12}$. Pravá strana nerovnosti je $\frac{1}{2}$. Protože $\frac{7}{12}>\frac{1}{2}$ platí, je základní krok u konce.

2. **Indukční krok:** zvolíme libovolné, ale pevné číslo $n\geq 2$. Máme ukázat platnost nerovnosti

$$\frac{1}{(n+1)+1}+\frac{1}{(n+1)+2}+\ldots+\frac{1}{2(n+1)}>\frac{1}{2} \tag{1.1}$$

Pokusíme se o dekomposici a zřejmě máme dekomponovat levou stranu. Protože smyslem dekomposice je objevit „problém menších rozměrů“, pokoušíme se v levé straně objevit výraz

$$\frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{2n}. \tag{1.2}$$

Levá strana (1.1) však „začíná a končí později“ než výraz (1.2). Použijeme tedy obvyklého triku přičtení a odečtení a levou stranu (1.1) dekomponujeme takto:

$$\frac{1}{(n+1)+1}+\frac{1}{(n+1)+2}+\ldots+\frac{1}{2(n+1)}=\frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{2n}+\left(\frac{1}{2n+1}+\frac{1}{2n+2}-\frac{1}{n+1}\right) \tag{1.3}$$

Na základě této dekomposice můžeme zformulovat **indukční předpoklad:** pro libovolné pevné $n\geq 2$ platí nerovnost

$$\frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{2n}>\frac{1}{2}.$$

Dekomposice (1.3) dává návod, jak indukční předpoklad použít:

$$\begin{aligned}\frac{1}{(n+1)+1}+\frac{1}{(n+1)+2}+\ldots+\frac{1}{2(n+1)} &= \frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{2n}+\left(\frac{1}{2n+1}+\frac{1}{2n+2}-\frac{1}{n+1}\right)\\ &> \frac{1}{2}+\left(\frac{1}{2n+1}+\frac{1}{2n+2}-\frac{1}{n+1}\right)\end{aligned}$$

Nyní by k ukončení důkazu indukčního kroku stačilo ukázat, že platí nerovnost

$$\frac{1}{2n+1}+\frac{1}{2n+2}-\frac{1}{n+1}\geq 0$$

neboli, že platí nerovnost

$$\frac{1}{2n+1}\geq\frac{1}{n+1}-\frac{1}{2n+2} \tag{1.4}$$

To je ale snadné: pravá strana (1.4) je rovna výrazu $\frac{1}{2n+2}$ a nerovnost

$$\frac{1}{2n+1}\geq\frac{1}{2n+2}$$

jistě pro $n\geq 2$ platí. Celkový důkaz indukčního kroku tedy vypadá takto:

$$\begin{aligned}\frac{1}{(n+1)+1}+\frac{1}{(n+1)+2}+\ldots+\frac{1}{2(n+1)} &= \frac{1}{n+1}+\frac{1}{n+2}+\ldots+\frac{1}{2n}+\left(\frac{1}{2n+1}+\frac{1}{2n+2}-\frac{1}{n+1}\right)\\ &> \frac{1}{2}+\left(\frac{1}{2n+1}+\frac{1}{2n+2}-\frac{1}{n+1}\right)\\ &\geq \frac{1}{2}\end{aligned}$$

Použili jsme slabý princip indukce. ■

1.1.3 Příklad Dokažte, že nerovnost $\left|\sum_{i=1}^{n} x_i\right| \leq \sum_{i=1}^{n} |x_i|$ platí pro libovolné $n \geq 1$ a libovolná reálná čísla $x_1, \ldots, x_n$.

Řešení. Budeme postupovat nějakým principem indukce podle $n \geq 1$.

Komentář. Vyplatí se si přesně uvědomit, že dokazujeme tvrzení tvaru *Pro všechna přirozená čísla $n \geq 1$ platí $V(n)$*, kde $V(n)$ znamená platnost nerovnosti $\left|\sum_{i=1}^{n} x_i\right| \leq \sum_{i=1}^{n} |x_i|$ pro libovolná reálná čísla $x_1, \ldots, x_n$. Tento dodatek (pro libovolná reálná…) budeme muset „tahat s sebou“!

1. **Základní krok:** pro $n = 1$ máme ukázat platnost nerovnosti $\left|\sum_{i=1}^{1} x_i\right| \leq \sum_{i=1}^{1} |x_i|$ pro libovolné reálné číslo x_1.

   Levá strana této nerovnosti je $|x_1|$ a pravá strana této nerovnosti je opět $|x_1|$.

   Nerovnost $\left|\sum_{i=1}^{1} x_i\right| \leq \sum_{i=1}^{1} |x_i|$ pro libovolné reálné číslo x_1 je dokázána.

2. **Indukční krok:** pro libovolné pevné $n \geq 1$ máme dokázat platnost nerovnosti

   $$\left|\sum_{i=1}^{n+1} x_i\right| \leq \sum_{i=1}^{n+1} |x_i|$$

   pro libovolná reálná čísla $x_1, \ldots, x_n, x_{n+1}$. Dekomponovat budeme zřejmě levou stranu:

   $$\left|\sum_{i=1}^{n+1} x_i\right| = \left|\left(\sum_{i=1}^{n} x_i\right) + x_{n+1}\right|$$

   což nám dovoluje zformulovat **indukční předpoklad:** pro libovolné pevné $n \geq 1$ platí nerovnost

   $$\left|\sum_{i=1}^{n} x_i\right| \leq \sum_{i=1}^{n} |x_i|$$

   pro libovolná reálná čísla $x_1, \ldots, x_n$.

   Co ale máme dělat dál? Jak indukční předpoklad použít? Nabízí se tento další postup:

   $$\left|\left(\sum_{i=1}^{n} x_i\right) + x_{n+1}\right| \leq \left(\left|\sum_{i=1}^{n} x_i\right|\right) + |x_{n+1}| \leq \left(\sum_{i=1}^{n} |x_i|\right) + |x_{n+1}| = \sum_{i=1}^{n+1} |x_i| \tag{1.5}$$

   který v první nerovnosti využívá platnost tvrzení $V(2)$ a ve druhé nerovnosti indukční předpoklad. Tvrzení $V(2)$ totiž říká: nerovnost $|A + B| \leq |A| + |B|$ platí pro libovolná reálná čísla A, B. (Přejmenovali jsme vázané proměnné x_1 a x_2 na A a B, víme z logiky, že se to smí, říká se tomu α-konverse.) My jsme tvrzení $V(2)$ použili pro

   $$A = \left(\sum_{i=1}^{n} x_i\right) \qquad B = x_{n+1}.$$

   Komentář. Zde se naplno projevuje nutnost tahat s sebou dodatek *pro všechna reálná…* Bez tohoto dodatku by náš důkaz nebyl korektní.

   Protože tvrzení $V(2)$ jsme ale nedokázali, přerušíme důkaz indukčního kroku a dokážeme druhou část kroku základního pro $n = 2$.

   Komentář. To je nutné udělat: příslušný rekursivní algoritmus by totiž neběžel. Náš algoritmus totiž platnost (například) $V(4)$ redukuje na platnost $V(3)$, platnost $V(3)$ redukuje na platnost $V(2)$ a tam se zastaví s chybovým hlášením. Platnost $V(2)$ jsme zatím nedokázali.

3. **Základní krok (druhá část):** máme dokázat platnost nerovnosti

$$|x_1 + x_2| \leq |x_1| + |x_2| \tag{1.6}$$

pro libovolná reálná čísla x_1, x_2. Nejjednodušší je postupovat odstraňováním absolutních hodnot:

(a) V případě, že $x_1 + x_2 \geq 0$, je pravá strana nerovnosti (1.6) rovna $x_1 + x_2$. Protože pro (jakákoli) reálná čísla x_1, x_2 platí nerovnosti $x_1 \leq |x_1|$ a $x_2 \leq |x_2|$, dostáváme nerovnost (1.6)

$$|x_1 + x_2| = x_1 + x_2 \leq |x_1| + |x_2|$$

(b) V případě, že $x_1 + x_2 < 0$, je pravá strana nerovnosti (1.6) rovna $-x_1 - x_2$. Protože pro (jakákoli) reálná čísla x_1, x_2 platí nerovnosti $-x_1 \leq |x_1|$ a $-x_2 \leq |x_2|$, dostáváme nerovnost (1.6)

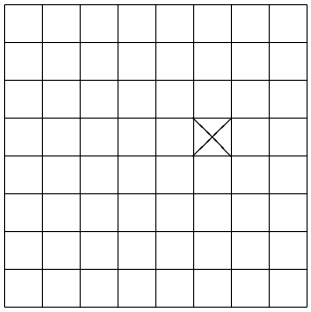
$$|x_1 + x_2| = -x_1 - x_2 \leq |x_1| + |x_2|$$

Důkaz tvrzení $V(2)$ je u konce.

4. **Indukční krok (druhá část):** nyní je již postup v (1.5) v pořádku a indukční krok je dokázán.

Použili jsme slabý princip indukce. ■

1.1.4 Příklad *Místností rozměru n* budeme rozumět šachovnici rozměru $2^n \times 2^n$, kde $n \geq 1$, ze které je jedno (libovolné) pole vyjmuto. Toto je příklad místnosti rozměru 3:



Trimino je parketa následujícího tvaru:

Vyřešte následující problémy:

1. Sestavte rekursivní algoritmus, který vyparketuje libovolnou místnost rozměru $n \geq 1$ triminy. Vyparketováním triminy rozumíme rozložení trimin po místnosti tak, aby žádné pole nezbylo volné. Trimina se přitom mohou pouze dotýkat hranou a nesmí pokrýt vyjmuté pole.

2. Ukažte (indukcí) totální korektnost tohoto algoritmu.

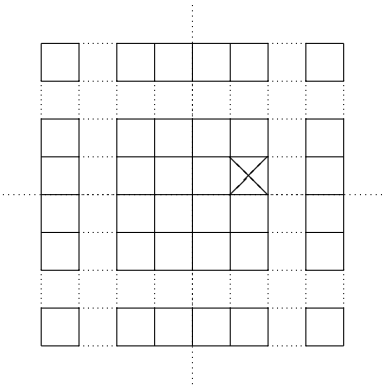
Řešení. Nejprve sestavíme rekursivní algoritmus, který vyparketuje libovolnou místnost rozměrů $n \geq 1$ triminy. Důkaz korektnosti algoritmu okamžitě poplyne z návrhu algoritmu.

> **Komentář.** Zde naplno uvidíme, proč je důkaz indukcí totéž jako rekursivní algoritmus. Uvidíme také, že důkaz indukcí pracuje „směrem dolů“, tj., že indukční krok redukuje úlohu velkých rozměrů na úlohy rozměrů menších (tento rozklad je přesně dekomposice problému) a že rekursivní volání odpovídá přesně použití indukčního předpokladu.

1. **Základní krok algoritmu:** pro $n = 1$ náš algoritmus nebude pracovat rekursivně. Místnost rozměrů 1 totiž vypadá (až na rotaci) takto:

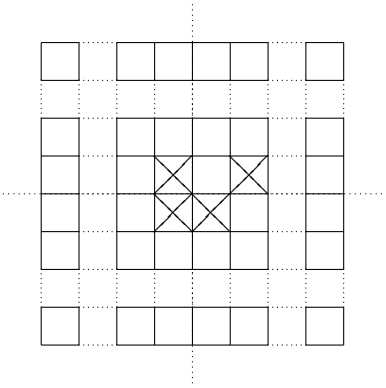
a my ji tudíž vyparketujeme jedním triminem.

2. **Rekursivní práce algoritmu:** Máme vyparketovat místnost rozměrů $n+1$. Protože $2^{n+1} = 2 \cdot 2^n$, nabízí se stranu příslušného čtverce rozpůlit a získat tak čtyři čtverce rozměrů $2^n \times 2^n$:



Komentář. Všimněme si, že *nevznikly* čtyři místnosti rozměrů n, dekomposice tudíž ještě není u konce.

Nyní položíme na střed místnosti jedno trimino a dostaneme tak:



(1.7)

V tento okamžik je dekomposice u konce: máme vyparketovat čtyři místnosti rozměrů n. To uděláme rekursivně.

Korektnost algoritmu dokážeme indukcí podle $n \geq 1$:

1. **Základní krok:** Místnost rozměrů $n = 1$ náš algoritmus vyparketuje.

2. **Indukční krok:** Máme ukázat, že náš algoritmus vyparketuje místnost rozměrů $n+1$. Provedeme dekomposici výše uvedeným způsobem a zformulujeme **indukční předpoklad** takto: každou místnost rozměrů n náš algoritmus vyparketuje. Indukční předpoklad použijeme *čtyřikrát*: jednou na každou místnost rozměrů n v dekomposici na obrázku (1.7).

   Důkaz indukčního kroku je skončen.

Podle principu slabé indukce je důkaz korektnosti u konce. ■

1.2 Strukturální indukce

1.2.1 Příklad Ať $\Sigma = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ je konečná abeceda. Zadejte induktivně množinu L všech slov nad Σ, která representují nenulová přirozená čísla.

Řešení. Nejprve popíšeme charakteristickou vlastnost prvků množiny L. Pro slovo $w \in \Sigma^*$ zavedeme značení: $V(w)$ platí právě když platí $|w| \geq 1$ a první znak zleva ve w není 0. Potom platí rovnost $L = \{w \in \Sigma^* \mid V(w)\}$. Tuto množinu L zadáme induktivně.

Naše gramatika bude mít devět axiomů

$$\frac{}{1}\ (1) \quad | \quad \frac{}{2}\ (2) \quad | \quad \frac{}{3}\ (3) \quad | \quad \frac{}{4}\ (4) \quad | \quad \frac{}{5}\ (5) \quad | \tag{1.8}$$

$$\frac{}{6}\ (6) \quad | \quad \frac{}{7}\ (7) \quad | \quad \frac{}{8}\ (8) \quad | \quad \frac{}{9}\ (9)$$

a deset deduktivních pravidel

$$\frac{w}{w0}\ (10) \quad | \quad \frac{w}{w1}\ (11) \quad | \quad \frac{w}{w2}\ (12) \quad | \quad \frac{w}{w3}\ (13) \quad | \quad \frac{w}{w4}\ (14) \quad | \tag{1.9}$$

$$\frac{w}{w5}\ (15) \quad | \quad \frac{w}{w6}\ (16) \quad | \quad \frac{w}{w7}\ (17) \quad | \quad \frac{w}{w8}\ (18) \quad | \quad \frac{w}{w9}\ (19)$$

Tato gramatika induktivně zadává jistou množinu slov G. Naším úkolem je dokázat rovnost $G = L$.

Úkol rozdělíme na dvě části:

1. $G \subseteq L$: máme ukázat: jestliže $w \in G$, potom $w \in L$, a to pro libovolné slovo w.

   Zvolme libovolné slovo w z množiny G. To znamená, že slovo w je vygenerováno koonečným použitím pravidel (1.8) a (1.9). To znamená, že máme k disposici syntaktický strom T_w slova w a slovo w je kořenem stromu T_w.

   Chceme dokázat, že platí $V(w)$. K tomu nám postačí ukázat, že platnost vlastnosti $V(w)$ je invariantní na průchod gramatikou (1.8) a (1.9). (Používáme tedy princip strukturální indukce.)

   > **Komentář.** To je zcela typický postup. V tomto směru ($G \subseteq L$) je vždy vhodný princip strukturální indukce.

   (a) **Základní krok:** závěr každého axiomu z (1.8) má vlastnost $V(w)$, jde o slovo délky jedna a první znak zleva není nula.

   Důkaz základního kroku strukturální indukce je ukončen.

   (b) **Indukční krok:** vězměme libovolné deduktivní pravidlo ze seznamu (1.9). Máme ukázat, že závěr tohoto deduktivního pravidla má vlastnost V, jestliže předpoklad tohoto pravidla má vlastnost V.

   Důkaz provedeme pro pravidlo (19), pro ostatní deduktivní pravidla je důkaz analogický.

   Předpokládáme tedy platnost $V(w)$ a chceme dokázat platnost $V(w9)$. To je triviální: $w9$ je slovo délky alespoň 1 a první znak zleva slova $w9$ není znak 0, protože víme, že slovo w nezačíná znakem 0.

   Důkaz indukčního kroku je u konce.

   Dokázali jsme $G \subseteq L$.

2. $L \subseteq G$: máme dokázat: jestliže $w \in L$, potom $w \in G$, a to pro libovolné slovo w.

   Zvolme libovolné slovo w z množiny L. To znamená, že $V(w)$ platí. Naším úkolem je sestavit syntaktický strom slova w. Jediné, co lze využít, je znalost délky $|w|$ slova w.

   Zkusíme tedy (klasickou) indukcí dokázat toto tvrzení: pro všechna $n \geq 1$ platí: jestliže platí $V(w)$ pro slovo w délky n, potom existuje syntaktický strom T_w vytvořený podle pravidel (1.8) a (1.9).

   > **Komentář.** V tomto směru ($L \subseteq G$) se pro konstrukci syntaktického stromu musí vždy použít některý klasický princip indukce. Nejobtížnější tu bývá zjistit, podle čeho indukci provádět.

   (a) **Základní krok:** máme dokázat, že každé slovo w délky 1 takové, že $V(w)$ platí, má syntaktický strom T_w vytvořený podle pravidel (1.8) a (1.9).

   Protože slovo w má délku jedna a platí $V(w)$, je slovo w některým ze znaků 1, 2, 3, 4, 5, 6, 7, 8, 9.

   Důkaz provedme pro případ $w = 7$, pro ostatní případy je důkaz analogický.

   Hledaný syntaktický strom T_w je $\frac{}{7}\ (7)$.

   Důkaz základního kroku je u konce.

(b) **Indukční krok:** máme slovo w délky $n+1$ a víme, že $V(w)$ platí. Chceme ukázat, že existuje syntaktický strom T_w vytvořený podle pravidel (1.8) a (1.9).

Protože postupujeme klasickou indukcí, hledáme nějakou dekomposici. Protože slovo w má délku $n+1$, nabízí se dekomposice $w = w'a$, kde w' má délku n a $a \in \Sigma$. Navíc zjevně platí $V(w')$.

Indukční předpoklad tedy zformulujeme takto: každé slovo w' délky n, pro které platí $V(w')$, má syntaktický strom $T_{w'}$ vytvořený podle pravidel (1.8) a (1.9).

Budeme předpokládat, že poslední znak a slova w je znak 3, pro ostatní případy se důkaz vede analogicky.

Hledaný syntaktický strom T_w je $\dfrac{T_{w'}}{w'3}$ (13) .

Důkaz indukčního kroku je u konce.

Slabým principem indukce jsme dokázali, že $L \subseteq G$.

■

1.2.2 Příklad Ať At je množina atomických formulí. Množina $F(At)$ všech formulí výrokové logiky je induktivně zadána následujícími axiomy

$$\frac{}{\mathtt{tt}}\ (\text{true}) \quad | \quad \frac{}{a}\ (a) \quad \text{kde } a \in At \tag{1.10}$$

a deduktivními pravidly

$$\frac{\varphi}{(\neg\varphi)}\ (\neg) \quad | \quad \frac{\varphi_1 \quad \varphi_2}{(\varphi_1 \wedge \varphi_2)}\ (\wedge) \quad | \quad \frac{\varphi_1 \quad \varphi_2}{(\varphi_1 \vee \varphi_2)}\ (\vee) \quad | \tag{1.11}$$

$$\frac{\varphi_1 \quad \varphi_2}{(\varphi_1 \Rightarrow \varphi_2)}\ (\Rightarrow) \quad | \quad \frac{\varphi_1 \quad \varphi_2}{(\varphi_1 \Leftrightarrow \varphi_2)}\ (\Leftrightarrow)$$

Dokažte, že v každé formuli $\varphi \in F(At)$ je počet levých a pravých závorek shodný.

Řešení. Protože množina $F(At)$ je induktivně vytvořena, zkusíme k důkazu využít princip strukturální indukce. Na množině všech slov nad abecedou $\Sigma = \{\neg, \wedge, \vee, \Rightarrow, \Leftrightarrow, \mathtt{tt}, (,)\} \cup At$ zavedeme následující vlastnost: $V(w)$ platí, pokud je ve slovu w počet levých a pravých závorek stejný.

Komentář. Samozřejmě: ne každé slovo w nad Σ je formule. Například slovo $\wedge\wedge()$ není formule, ale má vlastnost V.

Chceme dokázat, že platí $V(w)$, a to pro každé slovo z množiny $F(At)$. Podle principu strukturální indukce stačí ukázat, že vlastnost V je invariantní na průchod pravidly (1.10) a (1.11).

1. **Základní krok:** máme ukázat, že závěr každého axiomu z (1.10) má vlastnost V.

   To je zřejmé: závěr každého axiomu má nula pravých a nula levých závorek.

   Důkaz základního kroku je u konce.

2. **Indukční krok:** máme ukázat, že pro každé deduktivní pravidlo z (1.11) platí: jestliže všechny předpoklady pravidla mají vlastnost V, má vlastnost V i závěr tohoto pravidla.

   To je zřejmé: vezměme například pravidlo $(\Leftrightarrow)$, pro ostatní pravidla proběhne důkaz analogicky.

   Pokud platí $V(\varphi_1)$ a $V(\varphi_2)$, platí zřejmě i $V((\varphi_1 \Leftrightarrow \varphi_2))$.

   Důkaz indukčního kroku je u konce.

Podle principu strukturální indukce je důkaz ukončen. ■

Kapitola 2

Binární relace na množině

V odstavci 2.1 jsou vyřešeny standardní příklady týkající se vlastností binárních relací na množině, v odstavci 2.2 pak jsou řešeny některé složitější příklady.

Připomeňme některé definice a značení, použitá ve skriptech *Diskrétní matematika*:

1. *Binární relace R na množině A* je podmnožina $R \subseteq A \times A$. Místo $(x, y) \in R$ píšeme $x\ R\ y$.

   Komentář. Slovo *relace* znamená česky *vztah*. Nejrozumnější je představit si relaci R jako seznam dvojic, kde první položka má (jakýsi) vztah s druhou položkou.
   Zápis $x\ R\ y$ *není* totéž jako relace R. Zápis $x\ R\ y$ je *tvrzení*, že x má vztah R s y. Takové tvrzení může být pravdivé nebo nepravdivé. Jde o podobné rozlišení jako u funkcí: zápis $\sin x$ *není funkce*, ale funkční hodnota. Příslušnou funkcí je sin.

2. *Identická relace* Δ_A na množině A je definována vlastností: $x\ \Delta_A\ y$ právě když $x = y$.

3. *Relace opačná* k R je relace značená R^{op} s vlastností: $x\ R^{op}\ y$ právě když $y\ R\ x$.

4. *Složení relací R a S* je relace značená $R; S$ s vlastností: $x\ R; S\ y$ právě když existuje $z \in A$ tak, že platí $x\ R\ z$ a $z\ S\ y$ současně.

2.1 Vlastnosti konkrétních relací

2.1.1 Příklad Na množině $\mathbb{Z}$ celých čísel je zadána relace T vlastností: $a\ T\ b$ právě když $a + b$ je dělitelné třemi. Rozhodněte, zda relace T je:

1. Reflexivní. 2. Symetrická. 3. Transitivní. 4. Antisymetrická.

Komentář. V definici relace T je použita vlastnost *dělitelnost třemi*, nikoli operace *dělení třemi*. Mezi těmito pojmy je zásadní rozdíl! Zaměňování těchto pojmů vede k nesprávným úvahám.

Řešení.

1. **Reflexivita:** máme ukázat, že pro všechna $a \in \mathbb{Z}$ platí $a\ T\ a$. Neboli: máme rozhodnout, zda číslo $a + a$ je dělitelné třemi pro všechna $a \in \mathbb{Z}$.

   To není pravda: číslo $a = 1$ je celé a číslo $a = 1 + 1 = 2$ není dělitelné třemi.

   Zadaná relace T není reflexivní.

   Komentář. Častou chybou je tvrzení: pro $a = 24$ je $a + a = 48$ a to je číslo dělitelné třemi. *Relace T je reflexivní pro $a = 24$.* Pozor! Nic takového jako *reflexivita pro nějakou hodnotu* nebylo definováno! Relace buď reflexivní je nebo není. Pokud máme dojem, že relace reflexivní je, musíme podmínku reflexivity dokázat pro *všechny* prvky zadané množiny, pokud máme dojem, že relace reflexivní není, stačí najít (co nejjednodušší) protipříklad na podmínku reflexivity.

2. **Symetrie:** máme ukázat, že z platnosti $a\ T\ b$ plyne platnost $b\ T\ a$, a to pro *všechna* celá čísla a, b.

   Pokud $a + b$ je dělitelné třemi, znamená to, že umíme najít celé číslo k tak, že $a + b = 3k$. Protože sčítání celých čísel je komutativní, víme, že $b + a = 3k$. Proto platí $b\ T\ a$.

   Zadaná relace T je symetrická.

Komentář. Nejspíš není možné popsat všechny možné chyby, které se u práce se symetrií mohou vyskytnout. Zde je výčet dvou nejčastějších:

(a) Symetrie naší relace T *není* vlastnost $a\ T\ b$ *a současně* $b\ T\ a$ pro všechna $a, b \in \mathbb{Z}$. Viz příklad 2.2.3. Tuto podmínku relace T *nesplňuje*: zvolte $a = 1$, $b = 2$. Neplatí ani $a\ T\ b$, ani $b\ T\ a$.

(b) Pokud jsme ukázali, že nějaká relace je symetrická, *neplyne* z toho automaticky, že není antisymetrická. Relace, které jsou symetrické a antisymetrické současně, existují. Podívejte se na příklad 2.2.2.

3. **Transitivita:** máme ukázat, že z platnosti $a\ T\ b$ a současně $b\ T\ c$ plyne $a\ T\ c$, a to pro libovolná celá čísla a, b, c.

   Tato podmínka splněna není: pro $a = 1$, $b = 2$, $c = 1$ platí $a\ T\ b$ a současně $b\ T\ c$, ale $a\ T\ c$ neplatí.

   Zadaná relace T není transitivní.

4. **Antisymetrie:** máme ukázat, že z platnosti $a\ T\ b$ a současně $b\ T\ a$ plyne $a = b$, a to pro libovolná celá čísla a, b.

   Tato podmínka splněna není: pro $a = 1$, $b = 2$ platí $a\ T\ b$ a současně $b\ T\ a$, ale $a = b$ neplatí.

   Zadaná relace T není antisymetrická.

■

2.1.2 Příklad Na množině $\mathbb{R}$ reálných čísel je zadána relace S takto: $x\ S\ y$ právě když $x^2 + 2xy \leq y^4$. Rozhodněte, zda platí $(-1)\ S^{op}; S\ 1$.

Řešení. Vztah $(-1)\ S^{op}; S\ 1$ platí právě tehdy, když existuje $z \in \mathbb{R}$ tak, že platí $(-1)\ S^{op}\ z$ a $z\ S\ 1$ současně. A to platí právě tehdy, když existuje $z \in \mathbb{R}$ tak, že platí $z\ S\ (-1)$ a $z\ S\ 1$ současně.

Jinými slovy: hledáme $z \in \mathbb{R}$ tak, že platí $z^2 - 2z \leq 1$ a $z^2 + 2z \leq 1$. Takovým z je třeba číslo 0.

Komentář. Častou chybou u příkladů tohoto typu je snaha nějak definiční vztah relace upravovat. Často je to téměř nemožné a skoro vždy to vůbec není zapotřebí. Správná strategie tu je *lazy evaluation*: pracujte s nepříjemnými výrazy teprve tehdy, když to situace skutečně vyžaduje.

Protože jsme číslo z s požadovanými vlastnostmi našli, vztah $(-1)\ S^{op}; S\ 1$ platí. ■

2.1.3 Příklad Na množině $\mathbb{R}$ reálných čísel je zadána relace W takto: $x\ W\ y$ právě když $x \geq y$. Rozhodněte, zda platí $(-5)\ W; W\ 1$.

Řešení. Vztah $(-5)\ W; W\ 1$ platí právě tehdy, když existuje $z \in \mathbb{R}$ tak, že platí $(-5)\ W\ z$ a $z\ W\ 1$ současně.

Jinými slovy: hledáme $z \in \mathbb{R}$ tak, že platí $-5 \geq z$ a $z \geq 1$. Takové reálné číslo z neexistuje.

Protože číslo z s požadovanými vlastnostmi neexistuje, vztah $(-5)\ W; W\ 1$ neplatí. ■

2.1.4 Příklad Ukažte, že relace $\mid$ (dělitelnost) na množině $\mathbb{N}$ je uspořádání.

Řešení. Máme ukázat, že relace $\mid$ je reflexivní, transitivní a antisymetrická.

Komentář. Je dobré si uvědomit, že jde o *dělitelnost*. Vztah $a \mid b$ znamená: existuje přirozené číslo k tak, že $b = k \cdot a$.

1. **Reflexivita:** Máme ukázat, že $a \mid a$ pro všechna přirozená čísla a.

   Vezměme tedy libovolné přirozené číslo a. *Hledáme* přirozené číslo k takové, že platí rovnost $a = k \cdot a$. Hledaným číslem k je číslo 1.

   Důkaz reflexivity je u konce.

2. **Transitivita:** Máme ukázat, že z platnosti $a \mid b$ a $b \mid c$ plyne vlastnost $a \mid c$, a to pro všechna přirozená čísla a, b, c.

   Protože $a \mid b$, existuje přirozené číslo k tak, že platí $b = k \cdot a$. S tímto číslem k můžeme dále pracovat.

   Protože $b \mid c$, existuje přirozené číslo l tak, že platí $b = l \cdot a$. S tímto číslem l můžeme dále pracovat.

Komentář. Všimněme si, že jsme k označení svědků dělitelnosti použili různá písmena. Úvaha $b = k \cdot a$ a $c = k \cdot b$ (stejní svědci dělitelnosti) je častou chybou.

Chceme-li ukázat, že $a \mid c$, stačí najít nějaké přirozené číslo m tak, aby platilo $c = m \cdot a$. Zjevně pro $m = k \cdot l$ rovnost $c = m \cdot a$ platí: $c = l \cdot b = l \cdot k \cdot a$.

Důkaz transitivity je u konce.

3. **Antisymetrie:** Máme ukázat, že z platnosti $a \mid b$ a $b \mid a$ plyne vlastnost $a = b$, a to pro všechna přirozená čísla a, b.

   Protože $a \mid b$, existuje přirozené číslo k tak, že platí $b = k \cdot a$. S tímto číslem k můžeme dále pracovat.

   Protože $b \mid a$, existuje přirozené číslo l tak, že platí $a = l \cdot b$. S tímto číslem l můžeme dále pracovat.

   Dostáváme tedy rovnosti

   $$a = l \cdot b = l \cdot k \cdot a \tag{2.1}$$

   V případě, že $a \neq 0$, můžeme rovnosti (2.1) číslem a vydělit a dostaneme tak rovnost $l \cdot k = 1$. Protože k i l jsou přirozená čísla, musí platit $k = l = 1$. Proto $a = l \cdot b = b$.

   V případě, že $a = 0$, tak rovnost $b = 0$ okamžitě plyne z rovnosti $b = k \cdot a$. Proto v tomto případě platí $a = b$.

   Další možnost nastat nemůže, důkaz antisymetrie je u konce.

Komentář. V tomto příkladu jsme ukázali, že $\langle \mathbb{N}, | \rangle$ je poset. Viz také příklad 6.2.1.

■

2.1.5 Příklad Ukažte, že relace U na množině komplexních čísel $\mathbb{C}$, definovaná vztahem

$$x \; U \; y \quad \text{právě když} \quad |x| = |y|$$

je relace ekvivalence a popište třídu ekvivalence čísla $1 + i$.

Komentář. Připomeňme, že relace ekvivalence musí být reflexivní, symetrická a transitivní.

Řešení. Nejprve dokážeme, že U je relace ekvivalence:

1. **Reflexivita:** máme ukázat, že $|x| = |x|$ pro všechna komplexní čísla x. To jistě platí.

   Ukázali jsme, že U je reflexivní relace.

2. **Symetrie:** máme ukázat, že z platnosti $|x| = |y|$ plyne platnost $|y| = |x|$, a to pro všechna komplexní čísla x, y. To je pravda díky vlastnostem rovnosti.

   Ukázali jsme, že U je symetrická relace.

3. **Transitivita:** máme ukázat, že z platnosti $|x| = |y|$ a $|y| = |z|$ plyne platnost $|x| = |z|$, a to pro všechna komplexní čísla x, y, z. To je pravda díky vlastnostem rovnosti.

   Ukázali jsme, že U je transitivní relace.

Třída ekvivalence čísla $1 + i$ je množina

$$U[1 + i] = \{z \in \mathbb{C} \mid |1 + i| = |z|\} = \{z \in \mathbb{C} \mid \sqrt{2} = |z|\},$$

což je kružnice v Gaussově rovině se středem v počátku a poloměrem $\sqrt{2}$.

Komentář. Zřejmě může být vůbec každá třída ekvivalence relace U příslušná komplexnímu číslu z chápána jako kružnice v Gaussově rovině se středem v počátku a poloměrem $r = |z|$.

Tento popis tříd ekvivalence dává popis rozkladu $\mathbb{C}$ podle U: množina $\mathbb{C}/U$ „je“ množina nezáporných reálných čísel, protože každou třídu ekvivalence můžeme representovat nezáporným reálným číslem (poloměrem příslušné kružnice).

■

2.2 Práce s relacemi

2.2.1 Příklad Ať R, S a T jsou binární relace na množině A. Ať navíc platí $R \subseteq S$. Ukažte, že potom platí $R;T \subseteq S;T$.

Řešení. Chceme ukázat, že z platnosti vztahu $a\ R;T\ b$ plyne platnost vztahu $a\ S;T\ b$, a to pro všechna a, b z A.

Vezměme tedy libovolná a a b taková, že platí $a\ R;T\ b$.
Vztah $a\ R;T\ b$ znamená existenci $c \in A$ tak, že platí $a\ R\ c$ a současně $c\ T\ b$.
Protože předpokládáme $R \subseteq S$, víme, že platí $a\ S\ c$. Celkově tedy platí $a\ S\ c$ a současně $c\ T\ b$.
Ukázali jsme, že $a\ S;T\ b$ platí. ■

2.2.2 Příklad Ukažte, že pro binární relaci R na množině A jsou následující podmínky ekvivalentní:

1. R je symetrická a antisymetrická současně.
2. R je *koreflexivní*, tj. platí $R \subseteq \Delta_A$.

Řešení. Máme dokázat, že z 1. plyne 2. a naopak.

1. Ať R je symetrická a antisymetrická současně. To znamená, že platí $R = R^{op}$ (symetrie) a $R \cap R^{op} \subseteq \Delta_A$ (antisymetrie).

   Potom platí $R = R \cap R = R \cap R^{op} \subseteq \Delta_A$. Relace R je koreflexivní, to jsme chtěli dokázat.

2. Ať platí $R \subseteq \Delta_A$. Potom zjevně platí $R = R^{op}$ a relace R je tudíž symetrická.

   Dále platí $R = R \cap R^{op} \subseteq \Delta_A$ a relace R je antisymetrická.

■

2.2.3 Příklad Ať A je neprázdná množina. Ať R je binární relace na A, která splňuje $x\ R\ y$ a současně $y\ R\ x$ pro všechna x, y z množiny A. Ukažte, že potom platí $R = A \times A$.

Řešení. Máme ukázat platnost $R \subseteq A \times A$ a platnost $A \times A \subseteq R$ současně.

1. Inkluse $R \subseteq A \times A$ samozřejmě platí, protože R je binární relace na množině A.
2. Dokážeme inklusi $A \times A \subseteq R$. Zvolme libovolný prvek $(x, y) \in A \times A$. Máme dokázat, že platí $x\ R\ y$.

   To je ale triviální: podle našich předpokladů o relaci R víme, že platí $x\ R\ y$ a současně $y\ R\ x$. Speciálně tedy platí $x\ R\ y$.

Dokázali jsme, že platí $R = A \times A$. ■

2.2.4 Příklad Řekneme, že binární relace R na množině A je *funkcionální*, pokud pro každé $x \in A$ existuje právě jedno $y \in A$ tak, že platí $x\ R\ y$. Dokažte, že relace R je funkcionální právě tehdy, když platí $\Delta_A \subseteq R;R^{op}$ a současně $R^{op};R \subseteq \Delta_A$.

> **Komentář.** Máme tedy dokázat, že R je funkcionální právě tehdy, když $R;R^{op}$ je reflexivní a $R^{op};R$ je koreflexivní (viz příklad 2.2.2).

Řešení.

1. Budeme předpokládat, že relace R je funkcionální. Chceme ukázat, že platí $\Delta_A \subseteq R;R^{op}$ a současně $R^{op};R \subseteq \Delta_A$.

(a) Budeme dokazovat platnost $\Delta_A \subseteq R; R^{op}$.

Zvolíme libovolné $x \in A$. Chceme dokázat, že platí $x\ R; R^{op}\ x$. Hledáme tudíž $y \in A$ tak, že platí $x\ R\ y$ a současně $y\ R^{op}\ x$. Jinými slovy: hledáme $y \in A$ tak, že platí $x\ R\ y$ a současně $x\ R\ y$. Toto y jistě existuje: relace R je totiž funkcionální.

Dokázali jsme, že $\Delta_A \subseteq R; R^{op}$ platí.

(b) Budeme dokazovat platnost $R^{op}; R \subseteq \Delta_A$.

Zvolíme libovolná y a y' tak, že platí $y\ R^{op}; R\ y'$. Chceme ukázat, že platí $y\ \Delta_A\ y'$, neboli, že platí $y = y'$.

Z platnosti $y\ R^{op}; R\ y'$ plyne existence $x \in A$ tak, že platí $y\ R^{op}\ x$ a současně $x\ R\ y'$. Neboli platí $x\ R\ y$ a současně $x\ R\ y'$. Protože relace R je funkcionální, platí $y = y'$.

Dokázali jsme, že $R^{op}; R \subseteq \Delta_A$ platí.

Ukázali jsme, že platí $\Delta_A \subseteq R; R^{op}$ a současně $R^{op}; R \subseteq \Delta_A$.

2. Budeme předpokládat, že platí $\Delta_A \subseteq R; R^{op}$ a současně $R^{op}; R \subseteq \Delta_A$. Chceme dokázat, že R je funkcionální relace.

Zvolme libovolné $x \in A$.

(a) Nejprve dokážeme, že existuje $y \in A$ tak, že platí $x\ R\ y$. K tomu využijeme platnost inkluse $\Delta_A \subseteq R; R^{op}$.

Platnost inkluse zaručuje, že platí $x\ R; R^{op}\ x$. Tudíž existuje $y \in A$ tak, že platí $x\ R\ y$ a současně $y\ R^{op}\ x$.

Speciálně jsme dokázali, že existuje $y \in A$ tak, že platí $x\ R\ y$.

(b) Nyní dokážeme, že z platnosti $x\ R\ y$ a současně $x\ R\ y'$ plyne $y = y'$.

Protože platí $x\ R\ y$ a současně $x\ R\ y'$, platí $y\ R^{op}\ x$ a současně $x\ R\ y'$. Neboli platí $y\ R^{op}; R\ y'$.

Protože platí $R^{op}; R \subseteq \Delta_A$, plyne z výše uvedeného, že $y = y'$. To jsme chtěli dokázat.

Relace R je funkcionální.

Komentář. Fukcionální binární relace R na množině A může být *ztotožněna* s funkcí $f_R : A \longrightarrow A$ takto: $y = f_R(x)$ platí právě tehdy, když platí $x\ R\ y$. Obráceně každá funkce $f : A \longrightarrow A$ dává vznikout funkcionální binární relaci R_f na množině A: definujte, že $x\ R_f\ y$ platí právě tehdy, když platí $y = f(x)$.

Samozřejmě, *ne každá* binární relace je funkcionální: buď

pro nějaké x existují *různá* y, y' tak, že platí $x\ R\ y$ a současně $x\ R\ y'$.
Příklad: $A = \{a, b\}$, $R = \{(a, a), (a, b)\}$. Existuje totiž $x \in A$ (sice $x = a$) tak, že platí $x\ R\ y$ a současně $x\ R\ y'$ pro *různá* y, y', sice pro $y = a$ a $y' = b$.

nebo

pro nějaké x *neexistuje žádné* y tak, že platí $x\ R\ y$.
Příklad: $A = \{a, b\}$, $R = \{(a, a), (a, b)\}$. Existuje totiž $x \in A$ (sice $x = b$) tak, že neexistuje žádné y tak, že platí $x\ R\ y$. Oba možní kandidáti, totiž $y = a$ a $y = b$, selhávají.

Pojem relace je *obecnější* než pojem funkce!

■

2.2.5 Příklad Rozhodněte, zda průnik dvou symetrických relací na téže množině je opět symetrická relace.

Řešení. Označme jako S_1 a S_2 dvě symetrické na množině A. Dále označme $P = S_1 \cap S_2$. Máme rozhodnout, zda P je opět symetrická relace.

Protože $S_1 = S_1^{op}$ (symetrie S_1) a $S_2 = S_2^{op}$ (symetrie S_2), platí $S_1 \cap S_2 = S_1^{op} \cap S_2^{op} = (S_1 \cap S_2)^{op}$.

Protože $S_1 \cap S_2 = P$, je symetrie P dokázána. ■

2.2.6 Příklad Rozhodněte, zda sjednocení dvou antisymetrických relací na téže množině je opět antisymetrická relace.

Řešení. Označme jako R_1 a R_2 dvě antisymetrické na množině A. Dále označme $S = R_1 \cup R_2$. Máme rozhodnout, zda S je opět antisymetrická relace.

> **Komentář.** Protože nemáme nejmenší ponětí, zda tvrzení je pravdivé nebo ne, použijeme optimistickou metodu. Budeme se pokoušet tvrzení dokázat. Buď se nám to povede, nebo se důkaz na nějakém místě zadrhne. Toto místo pak bude zdrojem protipříkladu, který tvrzení vyvrátí.

Víme, že platí $R_1 \cap R_1^{op} \subseteq \Delta_A$ (antisymetrie R_1) a také platí $R_2 \cap R_2^{op} \subseteq \Delta_A$ (antisymetrie R_2). Chceme dokázat, že platí $S \cap S^{op} \subseteq \Delta_A$ (antisymetrie S).

Protože $S = R_1 \cup R_2$, platí rovnosti

$$\begin{aligned} S \cap S^{op} = (R_1 \cup R_2) \cap (R_1 \cup R_2)^{op} &= (R_1 \cup R_2) \cap (R_1^{op} \cup R_2^{op}) \\ &= (R_1 \cap R_1^{op}) \cup (R_1 \cap R_2^{op}) \cup (R_2 \cap R_1^{op}) \cup (R_2 \cap R_2^{op}) \end{aligned}$$

První a čtvrtý člen pravé strany rovnosti jsou podmnožiny Δ_A díky antisymetrii R_1 a R_2. Jsou i druhý a třetí člen pravé strany rovnosti podmnožiny Δ_A? Obecně se nezdá, že by tomu tak být mělo.

> **Komentář.** To je místo, kde se důkaz zadrhává, začínáme konstruovat protipříklad. Pokud se podaří zařídit to tak, aby některý z prostředních dvou členů *nebyl* podmnožinou Δ_A, bude protipříklad hotov.

Zvolme $A = \{a, b\}$, $R_1 = \{(a, b)\}$, $R_2 = \{(b, a)\}$. Potom $R_1 \cap R_2^{op} = \{(a, b)\}$ a $R_2 \cap R_1^{op} = \{(b, a)\}$, což jistě nejsou podmnožiny $\Delta_A = \{(a, a), (b, b)\}$.

Jsou relace R_1 a R_2 antisymetrické? Jsou. Platí totiž $R_1 \cap R_1^{op} = \emptyset$ a $R_2 \cap R_2^{op} = \emptyset$ a prázdná množina je podmnožinou jakékoli množiny, tedy i množiny Δ_A.

Závěr: uvedené tvrzení neplatí. Nalezli jsme množinu A a dvě antisymetrické relace R_1 a R_2 na A takové, že $R_1 \cup R_2$ není antisymetrická relace na A. ■

2.2.7 Příklad Popište všechny relace ekvivalence na množině $A = \{a, b, c\}$.

Řešení. Stačí popsat nejrůznější možnosti „slepení“ prvků množiny A.

1. Slepí se všechny prvky a, b, c.

   To odpovídá relaci E_1, definované vztahem $x\ E_1\ y$ právě když $x, y \in A$.

   Relace E_1 je zjevně relace ekvivalence.

2. Slepí se prvky a a b, prvkek c se slepí pouze sám se sebou.

   To odpovídá relaci E_2, definované vztahem $x\ E_2\ y$ právě když $x, y \in \{a, b\}$ nebo $x, y \in \{c\}$.

   Relace E_2 je zjevně relace ekvivalence.

3. Slepí se prvky a a c, prvkek b se slepí pouze sám se sebou.

   To odpovídá relaci E_3, definované vztahem $x\ E_3\ y$ právě když $x, y \in \{a, c\}$ nebo $x, y \in \{b\}$.

   Relace E_3 je zjevně relace ekvivalence.

4. Slepí se prvky b a c, prvkek a se slepí pouze sám se sebou.

   To odpovídá relaci E_4, definované vztahem $x\ E_4\ y$ právě když $x, y \in \{b, c\}$ nebo $x, y \in \{a\}$.

   Relace E_4 je zjevně relace ekvivalence.

5. Každý z prvků a, b, c se slepí pouze sám se sebou.

   To odpovídá relaci E_5, definované vztahem $x\ E_5\ y$ právě když $x = y$.

   Relace E_5 je zjevně relace ekvivalence.

Žádné další relace ekvivalence na množině $\{a, b, c\}$, než výše popsané relace E_1 až E_5, nejsou.

> **Komentář.** Ukázali jsme užitečnou techniku: relaci ekvivalence na množině A můžeme popsat rozkladem množiny A na disjunktní části. Tento rozklad jsou pak jednotlivé třídy ekvivalence. Například pro výše uvedenou relaci E_3 platí $E_3[a] = E_3[c] = \{a, c\}$ a $E_3[b] = \{b\}$.

■

Kapitola 3

Počítání modulo číslo

V odstavci 3.1 jsou řešeny příklady ze základní teorie lineárních rovnic v $\mathbb{Z}_m$. Jádrem všech příkladů je bezpečné zvládnutí běhu rozšířeného Eukleidova algoritmu a sestavení příslušné Bezoutovy rovnosti.

V odstavci 3.2 pak jsou řešeny příklady pomocí hlubších výsledků modulární aritmetiky: čínské věty o zbytcích a Eulerovy věty.

3.1 Inverse, lineární rovnice a diofantické rovnice

3.1.1 Příklad Pokud existuje, nalezněte inversi k číslu 51 v $\mathbb{Z}_{501}$.

Řešení. Víme, že inverse existuje právě když $\gcd(501, 51) = 1$. Největšího společného dělitele nalezneme rozšířeným Eukleidovým algoritmem:

a	b	q	r	α_2	α_1	β_2	β_1
501	51			1	0	0	1
501	51	9	42	0	1	1	-9
51	42	1	9	1	-1	-9	10
42	9	4	6	-1	35	10	-49
9	6	1	3	35	-36	-49	59
6	3	2	0				

Spočetli jsme, že $\gcd(501, 51) = 3$, inverse čísla 51 v $\mathbb{Z}_{501}$ neexistuje.

> **Komentář.** Jako vedlejší produkt jsme rozšířeným Eukleidovým algoritmem získali příslušnou Bezoutovu rovnost $3 = -36 \cdot 501 + 59 \cdot 51$ v $\mathbb{Z}$. Pro naši úlohu tato rovnost získá obrovský význam v případě, kdy nám vyjde největší společný dělitel 1, viz příklad 3.1.2.

■

3.1.2 Příklad Pokud existuje, nalezněte inversi k číslu 17 v $\mathbb{Z}_{851}$.

Řešení. Víme, že inverse existuje právě když $\gcd(851, 17) = 1$. Největšího společného dělitele nalezneme rozšířeným Eukleidovým algoritmem:

a	b	q	r	α_2	α_1	β_2	β_1
851	17			1	0	0	1
851	17	50	1	0	1	1	-50
17	1	17	0				

Spočetli jsme, že $\gcd(851, 17) = 1$, inverse čísla 51 v $\mathbb{Z}_{501}$ existuje.

Rozšířený Eukleidův algoritmus nám dodal i příslušnou Bezoutovu rovnost:

$$1 = 1 \cdot 851 + (-50) \cdot 17 \quad \text{v } \mathbb{Z}$$

Přečteme-li Bezoutovu rovnost v $\mathbb{Z}_{851}$, dostaneme $1 = (-50) \cdot 17$. Zjistili jsme, že inverse k číslu 17 v $\mathbb{Z}_{851}$ je číslo $-50 = 801$. ■

3.1.3 Příklad Vyřešte rovnici $51x = 36$ v $\mathbb{Z}_{501}$.

Řešení. Způsobem, předvedeným v příkladu 3.1.1, nalezneme $\gcd(501, 51) = 3$. Protože $3 \mid 36$, má zadaná rovnice právě tři různá řešení v $\mathbb{Z}_{501}$ podle věty o klasifikaci řešení lineárních rovnic.

Danou rovnici nejprve „zkrátíme“ třemi, tj. zaměříme se na rovnici $17x = 12$ v $\mathbb{Z}_{167}$. Víme, že $\gcd(167, 17) = 1$, a proto má rovnice $17x = 12$ jednoznačné řešení v $\mathbb{Z}_{167}$. K nalezení tohoto řešení potřebujeme nalézt inversi k 17 v $\mathbb{Z}_{167}$. Tuto inversi nalezneme rozšířeným Eukleidovým algoritmem:

a	b	q	r	α_2	α_1	β_2	β_1
167	17			1	0	0	1
167	17	9	14	0	1	1	-9
17	14	1	3	1	-1	-9	10
14	3	4	2	-1	5	10	-49
3	2	1	1	5	-6	-49	59
2	1	2	0				

Bezoutova rovnost má tedy tvar $1 = -6 \cdot 167 + 59 \cdot 17$, proto je inverse k 17 v $\mathbb{Z}_{167}$ číslo 59. Řešení rovnice $17x = 12$ v $\mathbb{Z}_{167}$ je číslo $x = 17^{-1} \cdot 12 = 59 \cdot 12 = 708 = 40$ v $\mathbb{Z}_{167}$. Volbou $k = 0, 1, 2$ dostaneme pak tři různá řešení $x_k = x + k \cdot 167$ v $\mathbb{Z}_{501}$:

$$x_0 = 40, \quad x_1 = 40 + 1 \cdot 167 = 207, \quad x_2 = 40 + 2 \cdot 167 = 374 \quad \text{v } \mathbb{Z}_{501}$$

■

3.1.4 Příklad Vyřešte rovnici $15x + 81y = 195$ v $\mathbb{Z}$.

Řešení. Jedná se o diofantickou rovnici. Nejprve zjistíme, zda řešení existuje. Spočteme $\gcd(15, 81) = 3$ (rozšířeným Eukleidovým algoritmem). Protože $3 \mid 195$, řešení existuje. Původní rovnici číslem tři můžeme zkrátit: ekvivalentním problémem tedy je vyřešit rovnici $5x + 27y = 65$ v $\mathbb{Z}$. Ta má tu výhodu, že $\gcd(5, 27) = 1$.

Hledání řešení rozdělíme do dvou kroků:

1. Partikulární řešení je jakákoli dvojice, která problém $5x + 27y = 65$ řeší. Můžeme jako partikulární řešení zvolit například dvojici $(13, 0)$.

   Komentář. Pokud se nám nepovede partikulární řešení uhodnout, pomůže opět rozšířený Eukleidův algoritmus, spuštěný na koeficienty 5 a 27:

a	b	q	r	α_2	α_1	β_2	β_1
27	5			1	0	0	1
27	5	5	2	0	1	1	-5
5	2	2	1	1	-2	-5	11
2	1	2	0				

   Proto má Bezoutova rovnost tvar $5 \cdot 11 + 27 \cdot (-2) = 1$. Když ji vynásobíme 65, dostaneme rovnost $5 \cdot 715 + 27 \cdot (-130) = 65$. Získali jsme partikulární řešení $(715, -130)$.

2. Řešení homogenní rovnice $5x + 27y = 0$ jsou dvojice $t \cdot (27, -5)$, kde $t \in \mathbb{Z}$.

Celkové řešení je přímka $(13, 0) + t \cdot (27, -5)$, kde $t \in \mathbb{Z}$. ■

3.1.5 Příklad Dokažte, že v $\mathbb{Z}_m$ platí: *Jestliže mají a a b inversi, má inversi i součin $a \cdot b$.*

Řešení. Hledáme číslo x v $\mathbb{Z}_m$, které jednoznačně řeší rovnici $(a \cdot b) \cdot x = 1$ v $\mathbb{Z}_m$.

Nejprve ukážeme, že takové x je určeno jednoznačně. Předpokládejme, že platí $(a \cdot b) \cdot u = 1$ a $(a \cdot b) \cdot v = 1$ v $\mathbb{Z}_m$. Díky asociativitě násobení v $\mathbb{Z}_m$ potom platí $a \cdot (b \cdot u) = 1$ a $a \cdot (b \cdot v) = 1$ v $\mathbb{Z}_m$. Protože a^{-1} existuje, platí i rovnosti $b \cdot u = a^{-1}$ a $b \cdot v = a^{-1}$ v $\mathbb{Z}_m$. Protože b^{-1} existuje, platí i rovnosti $u = b^{-1} \cdot a^{-1}$ a $v = b^{-1} \cdot a^{-1}$ v $\mathbb{Z}_m$. Dokázali jsme, že $u = v$ v $\mathbb{Z}_m$.

Nyní stačí ukázat, že číslo $b^{-1} \cdot a^{-1}$ je řešením rovnice $(a \cdot b) \cdot x = 1$ v $\mathbb{Z}_m$. Stačí za x dosadit: využijeme asociativitu násobení a vlastnosti inversí:

$$(a \cdot b) \cdot (b^{-1} \cdot a^{-1}) = a \cdot (b \cdot b^{-1}) \cdot a^{-1} = a \cdot a^{-1} = 1 \quad \text{v } \mathbb{Z}_m$$

■

3.2 Čínská věta o zbytcích a Eulerova věta

3.2.1 Příklad Nalezněte řešení soustavy

$$x = 2 \text{ v } \mathbb{Z}_6 \quad x = 2 \text{ v } \mathbb{Z}_7 \quad x = 6 \text{ v } \mathbb{Z}_{25}$$

Řešení. Protože $\gcd(6,7) = \gcd(6,25) = \gcd(7,25) = 1$, můžeme použít čínskou větu o zbytcích. Řešení bude určeno jednoznačně v $\mathbb{Z}_M$, kde $M = 6 \cdot 7 \cdot 25 = 1\,050$. Řešení napíšeme ve tvaru

$$x \;=\; 2 \cdot \boxed{7 \cdot 25 \cdot ?} + 2 \cdot \boxed{6 \cdot 25 \cdot ?} + 6 \cdot \boxed{6 \cdot 7 \cdot ?}$$

Čísla v jednotlivých obdélnících zajišťují jejich nulovost: například první obdélník se anuluje při čtení v $\mathbb{Z}_7$ a v $\mathbb{Z}_{25}$. Zbývá dopočítat otazníky: ty zajistí jedničkovost obdélníků.

1. První obdélník: spočteme $7 \cdot 25 = 175 = 1$ v $\mathbb{Z}_6$. Protože $1^{-1} = 1$ v $\mathbb{Z}_6$, obsahuje první obdélník součin $7 \cdot 25 \cdot 1$.
2. Druhý obdélník: spočteme $6 \cdot 25 = 150 = 3$ v $\mathbb{Z}_7$. Protože $3^{-1} = 5$ v $\mathbb{Z}_7$, obsahuje druhý obdélník součin $6 \cdot 25 \cdot 5$.
3. Třetí obdélník: spočteme $6 \cdot 7 = 42 = 17$ v $\mathbb{Z}_{25}$. Protože $17^{-1} = 3$ v $\mathbb{Z}_{25}$, obsahuje třetí obdélník součin $6 \cdot 7 \cdot 3$.

Řešení je

$$x = 2 \cdot 7 \cdot 25 \cdot 1 + 2 \cdot 6 \cdot 25 \cdot 5 + 6 \cdot 6 \cdot 7 \cdot 3 = 350 + 1\,500 + 756 = 2\,606 = 506 \quad \text{v } \mathbb{Z}_{1\,050}$$

■

3.2.2 Příklad Rozhodněte, zda 107 je prvočíslo.

Řešení. Stačí vyzkoušet dělitelnost čísla 107 všemi prvočísly $\leq \sqrt{107} \doteq 10,34$. Pokud vyjdou vždy nenulové zbytky, bude číslo 107 prvočíslo.

> **Komentář.** Tomuto postupu se říká *Eratosthenovo síto*. Jde vlastně o test prvočíselnosti hrubou silou. Pro lepší testy prvočíselnosti nemáme vybudovannou patřičnou teorii.

Takovými prvočísly jsou 2, 3, 5 a 7.

Protože platí

$$\begin{aligned} 107 &= 2 \cdot 53 + 1 \\ 107 &= 3 \cdot 35 + 2 \\ 107 &= 5 \cdot 21 + 2 \\ 107 &= 7 \cdot 15 + 2 \end{aligned}$$

je číslo 107 prvočíslo. ■

3.2.3 Příklad Spočítejte $\varphi(856)$.

Řešení. Pro zjištění hodnoty Eulerovy funkce potřebujeme znát prvočíselný rozklad čísla 856. Nemáme jiné prostředky než nalézt tento rozklad hrubou silou:

$$856 = 2 \cdot 428 = 2^2 \cdot 214 = 2^3 \cdot 107$$

Protože 107 je podle příkladu 3.2.2 prvočíslo, nalezli jsme prvočíselný rozklad čísla 856.

Protože $\gcd(2^3, 107) = 1$, platí $\varphi(856) = \varphi(2^3) \cdot \varphi(107) = (2^3 - 2^2) \cdot (107 - 1) = 4 \cdot 106 = 424$. ■

3.2.4 Příklad Spočtěte $28\,457^{297\,917}$ v $\mathbb{Z}_{856}$.

Řešení. Nejprve upravíme základ mocniny v $\mathbb{Z}_{856}$: $28\,457 = 209$. Víme tedy, že v $\mathbb{Z}_{856}$ platí $28\,457^{297\,917} = 209^{297\,917}$.

Spočteme $\gcd(856, 209)$ rozšířeným Eukleidovým algoritmem:

a	b	q	r	α_2	α_1	β_2	β_1
856	209			1	0	0	1
856	209	4	20	0	1	1	-4
209	20	10	9	1	-10	-4	41
20	9	2	2	-10	21	41	-86
9	2	4	1	21	-94	-86	385
2	1	2	0				

Tudíž $\gcd(856, 209) = 1$, můžeme použít Eulerovu větu, která nám říká, že $209^{\varphi(856)} = 209^{424} = 1$. (Hodnotu $\varphi(856) = 424$ jsme spočetli v příkladu 3.2.3.) Spočteme exponent modulo $\varphi(856)$: $297\,917 = 424 \cdot 702 + 269$.

Proto platí v $\mathbb{Z}_{856}$ následující rovnosti:

$$28\,457^{297\,917} = 209^{297\,917} = 209^{424 \cdot 702 + 269} = (209^{424})^{702} \cdot 209^{269} = 1^{702} \cdot 209^{269} = 209^{269}$$

Dále musíme postupovat algoritmem opakovaných čtverců. Převedeme exponent 269 do binárního zápisu:

$$(269)_2 = 100001101$$

což nám dá řídící slovo $XSSSSSXSXSSX$ pro algoritmus opakovaných čtverců (následující výpočty jsou v $\mathbb{Z}_{856}$):

$$\begin{array}{ll}
X & 209 = 1 \cdot 209 = 209 \\
S & 209^2 = 209^2 = 43\,681 = 25 \\
S & 209^4 = 25^2 = 625 \\
S & 209^8 = 625^2 = 390\,625 = 289 \\
S & 209^{16} = 289^2 = 83\,521 = 489 \\
S & 209^{32} = 489^2 = 239\,121 = 297 \\
X & 209^{33} = 297 \cdot 209 = 62\,073 = 441 \\
S & 209^{66} = 441^2 = 194\,481 = 169 \\
X & 209^{67} = 169 \cdot 209 = 35\,321 = 225 \\
S & 209^{134} = 225^2 = 50\,625 = 121 \\
S & 209^{268} = 121^2 = 14\,641 = 89 \\
X & 209^{269} = 89 \cdot 209 = 18\,601 = 625
\end{array}$$

Spočtali jsme $28\,457^{297\,917} = 209^{269} = 625$ v $\mathbb{Z}_{856}$. ■

Kapitola 4

RSA a lineární kódy

V odstavci 4.1 je spočteno několik příkladů na útok na protokol RSA. V každém z těchto příkladů se několikrát využívá rozšířený Eukleidův algoritmus, algoritmus opakovaných čtverců a čínská věta o zbytcích. Příklady na zvládnutí těchto technik jsou v kapitole 3.

V odstavci 4.2 jsou řešeny příklady na nalezení kontrolní matice z generující matice a naopak. Na spočtení složitějších příkladů z teorie lineárních kódů nebyla odpřednesena teorie.

4.1 Útoky na RSA

4.1.1 Příklad Dešifrujte hrubou silou zprávu 21 pro Alici, znáte-li Alicin veřejný klíč $(703, 53)$ v protokolu RSA.

Řešení. Nejprve nalezneme faktorizaci Alicina modulu 703. Použijeme k tomu faktorizaci hrubou silou: musíme vyzkoušet všechna prvočísla menší nebo rovna číslu $\sqrt{703} \leq 27$. Dostaneme rozklad $703 = 19 \cdot 37$.

> **Komentář.** Rozklad modulu RSA na prvočísla hrubou silou je nejslabším článkem útoku na RSA hrubou silou. Takový rozklad je totiž výpočetně velmi náročný: trvá *exponenciálně* dlouho.

Nyní potřebujeme najít Alicin dešifrovací exponent. K tomu potřebujeme spočítat $\varphi(703) = 18 \cdot 36 = 648$ a v $\mathbb{Z}_{648}$ invertovat šifrovací exponent 53. Spustíme rozšířený Eukleidův algoritmus:

a	b	q	r	α_2	α_1	β_2	β_1
648	53			1	0	0	1
648	53	12	12	0	1	1	-12
53	12	4	5	1	-4	-12	49
12	5	2	2	-4	9	49	-110
5	2	2	1	9	-22	110	269
2	1	2	0				

Inverse k 53 v $\mathbb{Z}_{648}$ je tedy 269. Alicin soukromý klíč je $(703, 269)$.

Pro dešifrování zprávy je zapotřebí spočítat mocninu 21^{269} v $\mathbb{Z}_{703}$. Využijeme k tomu algoritmus opakovaných čtverců a čínskou větu o zbytcích.

> **Komentář.** Tato technika je rozumná: modul RSA máme rozložen na dvě (nesoudělná) prvočísla, která jsou řádově menší než původní modul. Budeme tak pracovat s relativně malými čísly.

V každém případě musíme zjistit binární hodnotu exponentu:

$$(269)_2 = 100001101$$

Řídící slovo pro algoritmus opakovaných čtverců tedy je $XSSSSSXSXSSX$.

1. Výpočet 21^{269} v $\mathbb{Z}_{19}$:

$$\begin{array}{ll} X & 21 = 1 \cdot 21 = 2 \\ S & 21^2 = 2^2 = 4 \\ S & 21^4 = 4^2 = 16 = -3 \\ S & 21^8 = (-3)^2 = 9 \\ S & 21^{16} = 9^2 = 81 = 5 \\ S & 21^{32} = 5^2 = 25 = 6 \\ X & 21^{33} = 6 \cdot 21 = 126 = 12 \\ S & 21^{66} = 12^2 = 144 = 11 \\ X & 21^{67} = 11 \cdot 21 = 231 = 3 \\ S & 21^{134} = 3^2 = 9 \\ S & 21^{268} = 9^2 = 81 = 5 \\ X & 21^{269} = 5 \cdot 21 = 105 = 10 \end{array}$$

Spočítali jsme, že $21^{269} = 10$ v $\mathbb{Z}_{19}$.

2. Výpočet 21^{269} v $\mathbb{Z}_{37}$:

$$\begin{array}{ll} X & 21 = 1 \cdot 21 = 21 = -16 \\ S & 21^2 = (-16)^2 = 256 = 34 = -3 \\ S & 21^4 = (-3)^2 = 9 \\ S & 21^8 = 9^2 = 81 = 7 \\ S & 21^{16} = 7^2 = 49 = 12 \\ S & 21^{32} = 12^2 = 144 = 33 \\ X & 21^{33} = 33 \cdot 21 = 693 = 27 = -10 \\ S & 21^{66} = (-10)^2 = 100 = 26 = -11 \\ X & 21^{67} = (-11) \cdot 21 = -231 = -9 \\ S & 21^{134} = (-9)^2 = 81 = 7 \\ S & 21^{268} = 7^2 = 49 = 12 \\ X & 21^{269} = 12 \cdot 21 = 252 = 30 \end{array}$$

Spočítali jsme, že $21^{269} = 30$ v $\mathbb{Z}_{37}$.

Připravíme si koeficienty pro čínskou větu o zbytcích. Potřebujeme 37^{-1} v $\mathbb{Z}_{19}$ a 19^{-1} v $\mathbb{Z}_{37}$.

1. Inverse 37 v $\mathbb{Z}_{19}$. Využijeme rovnosti $37 = -1$ v $\mathbb{Z}_{19}$. Proto je $37^{-1} = -1 = 18$ v $\mathbb{Z}_{19}$.

   Komentář. Tento způsob nalezení inverse (všimnutí si speciálního vztahu) je samozřejmě legální. Pochopitelně tato cesta bývá nejrychlejší, nejde ale použít vždy.

2. Inversi k 19 v $\mathbb{Z}_{37}$ spočítáme opět rozšířeným Eukleidovým algoritmem:

a	b	q	r	α_2	α_1	β_2	β_1
37	19			1	0	0	1
37	19	1	18	0	1	1	-1
19	18	1	1	1	-1	-1	2
18	1	18	0				

   Spočetli jsme $19^{-1} = 2$ v $\mathbb{Z}_{37}$.

Z čínské věty o zbytcích dostáváme rovnost

$$21^{269} = 10 \cdot 37 \cdot 18 + 30 \cdot 19 \cdot 2 = 6\,660 + 1\,140 = 7\,800 = 67 \quad \text{v } \mathbb{Z}_{703}$$

Dešifrovaná zpráva je 67. ■

4.1.2 Příklad Dvěma účastníkům s veřejnými klíči $(403, 13)$ a $(403, 11)$ byla zaslána stejná zpráva z. Eve zachytila $c_1 = 47$ a $c_2 = 70$. Nalezněte zprávu z metodou útoku outsidera.

Řešení. Vidíme, že šifrovací exponenty obou účastníků jsou nesoudělné. Rozšířeným Eukleidovým algoritmem spočteme Bezoutovu rovnost:

a	b	q	r	α_2	α_1	β_2	β_1
13	11			1	0	0	1
13	11	1	2	0	1	1	-1
11	2	5	1	1	-5	-1	6
2	1	2	0				

Bezoutova rovnost má tvar $1 = -5 \cdot 13 + 6 \cdot 11$, neboli $1 + 5 \cdot 13 = 6 \cdot 11$. Proto platí i rovnost

$$z \cdot 47^5 = z \cdot (z^{13})^5 = z^{1+5\cdot 13} = z^{6\cdot 11} = (z^{11})^6 = 70^6 \quad \text{v } \mathbb{Z}_{403}$$

Protože platí $47^5 = 125$ a $70^6 = 194$ v $\mathbb{Z}_{403}$ (to spočteme algoritmem opakovaných čtverců jako v příkladu 4.1.1), máme vyřešit lineární rovnici

$$z \cdot 125 = 194 \quad \text{v } \mathbb{Z}_{403} \tag{4.1}$$

Zjistíme, zda existuje inverse k 125 v $\mathbb{Z}_{403}$. Opět rozšířeným Eukleidovým algoritmem:

a	b	q	r	α_2	α_1	β_2	β_1
403	125			1	0	0	1
403	125	3	28	0	1	1	-3
125	28	4	13	1	-4	-3	13
28	13	2	2	-4	2	13	-29
13	2	6	1	2	-76	-29	187
2	1	2	0				

Inverse k 125 v $\mathbb{Z}_{403}$ je 187. Řešení rovnice (4.1) je $z = 125^{-1} \cdot 194 = 187 \cdot 194 = 166$ v $\mathbb{Z}_{403}$ a číslo 166 je původně odeslaná zpráva. ■

4.1.3 Příklad Dvěma účastníkům s veřejnými klíči $(391, 17)$ a $(391, 13)$ byla zaslána stejná zpráva z. Eve zachytila $c_1 = 34$ a $c_2 = 102$. Nalezněte zprávu z metodou útoku outsidera.

Řešení. Protože evidentně platí $\gcd(17, 13) = 1$, spočítáme rozšířeným Eukleidovým algoritmem Bezoutovu rovnost:

a	b	q	r	α_2	α_1	β_2	β_1
17	13			1	0	0	1
17	13	1	4	0	1	1	-1
13	4	3	1	1	-3	-1	4
3	1	3	0				

Bezoutova rovnost má tvar $1 = -3 \cdot 17 + 4 \cdot 13$, neboli $1 + 3 \cdot 17 = 4 \cdot 13$. Proto platí i rovnost

$$z \cdot 34^3 = z \cdot (z^{17})^3 = z^{1+3\cdot 17} = z^{4\cdot 13} = (z^{13})^4 = 102^4 \quad \text{v } \mathbb{Z}_{391}$$

Protože platí $34^3 = 204$ a $102^4 = 340$ v $\mathbb{Z}_{391}$ (to spočteme algoritmem opakovaných čtverců jako v příkladu 4.1.1), máme vyřešit lineární rovnici

$$z \cdot 204 = 340 \quad \text{v } \mathbb{Z}_{391} \tag{4.2}$$

Zjistíme, zda existuje inverse k 204 v $\mathbb{Z}_{391}$. Opět rozšířeným Eukleidovým algoritmem:

a	b	q	r	α_2	α_1	β_2	β_1
391	204			1	0	0	1
391	204	1	187	0	1	1	-1
204	187	1	17	1	-1	-1	2
187	17	11	0				

Zjistili jsme, že $\gcd(391, 204) = 17$, tudíž inverse k 204 v $\mathbb{Z}_{391}$ neexistuje a rovnice (4.2) má přesně 17 různých řešení, pokud navíc platí $17 \mid 340$.

Komentář. Jedna možnost je nyní zjistit, zda $17 \mid 340$ a pak případně 17 různých řešení rovnice (4.2) najít způsobem předvedeným v příkladu 3.1.3 a každé z těchto řešení vyzkoušet. Předvedeme jiný postup: právě jsme totiž *nalezli dělitele* čísla 391, sice číslo 17.

Protože jsme zjistili, že platí $17 \mid 391$, můžeme modul 391 faktorizovat: $391 = 17 \cdot 23$. Zprávu z nalezneme způsobem, popsaným v příkladu 4.1.1.

1. Platí $\varphi(391) = 16 \cdot 22 = 352$. Nalezneme soukromý klíč účastníka s veřejným klíčem $(391, 17)$. To znamená spočítat inversi k 17 v $\mathbb{Z}_{352}$. Spustíme rozšířený Eukleidův algoritmus:

a	b	q	r	α_2	α_1	β_2	β_1
352	17			1	0	0	1
352	17	20	12	0	1	1	-20
17	12	1	5	1	-1	-20	21
12	5	2	2	-1	3	21	-62
5	2	2	1	3	-7	-62	145
2	1	2	0				

   Zjistili jsme, že $17^{-1} = 145$ v $\mathbb{Z}_{352}$. Proto je příslušný soukromý klíč $(391, 145)$.

2. Hledaná zpráva je $z = 34^{145}$ v $\mathbb{Z}_{391}$. Tuto mocninu spočítáme způsobem uvedeným v příkladu 4.1.1.

   Protože $(145)_2 = 10010001$, je řídící slovo pro algoritmus opakovaných čtverců $XSSSXSSSSX$. Spočítáme 34^{145} v $\mathbb{Z}_{17}$ a $\mathbb{Z}_{23}$ a poté použijeme čínskou větu o zbytcích. Protože $34 = 0$ v $\mathbb{Z}_{17}$, je $34^{145} = 0$ v $\mathbb{Z}_{17}$.

   Výpočet $34^{145} = 11^{145}$ v $\mathbb{Z}_{23}$:

$$\begin{array}{ll} X & 11 = 1 \cdot 11 = 11 \\ S & 11^2 = 121 = 6 \\ S & 11^4 = 6^2 = 36 = 13 \\ S & 11^8 = 13^2 = 169 = 8 \\ X & 11^9 = 8 \cdot 11 = 88 = 19 = -4 \\ S & 11^{18} = (-4)^2 = 16 = -7 \\ S & 11^{36} = (-7)^2 = 49 = 3 \\ S & 11^{72} = 3^2 = 9 \\ S & 11^{144} = 9^2 = 81 = 12 \\ X & 21^{145} = 12 \cdot 11 = 132 = 17 \end{array}$$

   Spočetli jsme, že $34^{145} = 17$ v $\mathbb{Z}_{23}$.

   Podle čínské věty o zbytcích platí:

$$34^{145} = 0 \cdot 23 \cdot 3 + 17 \cdot 17 \cdot 19 = 5\,491 = 17 \quad \text{v } \mathbb{Z}_{391}$$

   protože $23^{-1} = 6^{-1} = 3$ v $\mathbb{Z}_{17}$ a $17^{-1} = (-6)^{-1} = -4 = 19$ v $\mathbb{Z}_{23}$

Odeslaná zpráva je $z = 17$.

Komentář. Upozorněme, že časová složitost právě předvedeného útoku se podstatně liší od útoku hrubou silou z příkladu 4.1.1. V příkladu 4.1.1 jsme museli faktorizovat modul RSA hrubou silou, a to trvá exponenciálně dlouho. V právě dopočteném příkladu jsme faktorizaci modulu RSA zjistili z Eukleidova algoritmu, který má polynomiální složitost.

■

4.2 Generující a kontrolní matice

4.2.1 Příklad Víme, že generující matice $\mathbb{G}$ lineárního kódu nad $\mathbb{Z}_{11}$ je

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

Nalezněte (nějakou) příslušnou kontrolní matici $\mathbb{H}$.

Řešení.

Komentář. Danou úlohu můžeme vyřešit dvěma různými způsoby. Předvedeme oba způsoby.

1. **První způsob řešení:** spustíme GEM.

$$\begin{pmatrix} 5 & 4 & 3 & 2 & 7 \\ 7 & 6 & 4 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 5 & 4 & 3 & 2 & 7 \\ 0 & 6 & 8 & 2 & 0 \end{pmatrix} \begin{matrix} R_1 \\ R_1 + 4 \cdot R_2 \end{matrix}$$

Komentář. Používáme „zdravotní značení“, abychom neztratili přehled o tom, co se děje.
Všechny výpočty jsou samozřejmě v $\mathbb{Z}_{11}$. Značka R_1 znamená: nový první řádek je opsaný starý první řádek. Značka $R_1 + 4 \cdot R_2$ znamená: nový druhý řádek je starý první řádek, ke kterému jsme přičetli 4-násobek starého druhého řádku. To je totiž úprava, nulující první pozici na druhém řádku: v $\mathbb{Z}_{11}$ platí $5 + 4 \cdot 7 = 33 = 0$.

Gaussova eliminace skončila, hodnost matice $\mathbb{G}$ (tj. počet nenulových řádků po skončení Gaussovy eliminace) je 2.

V řádcích hledané matice $\mathbb{H}$ budou prvky fundamentálního systému homogenní rovnice

$$\left(\begin{array}{ccccc|c} 5 & 4 & 3 & 2 & 7 & 0 \\ 0 & 6 & 8 & 2 & 0 & 0 \end{array}\right) \tag{4.3}$$

Počet prvků tohoto fundamentálního systému je $5 - 2 = 3$, to plyne z Frobeniovy věty. Prvky fundamentálního systému nalezneme metodou organisovaného hádání.

Vektory fundamentálního systému mají tvar

$$(a_1, a_2, 1, 0, 0) \quad (b_1, b_2, 0, 1, 0) \quad (c_1, c_2, 0, 0, 1)$$

Volbou nul a jedniček v posledních třech položkách jsme totiž zajistili lineární nezávislost hledaných vektorů a nyní dopočítáme v každém vektoru první dvě položky pomocí soustavy (4.3).

(a) První vektor: dosazení vektoru $(a_1, a_2, 1, 0, 0)$ do druhé rovnice v (4.3) dává $6a_2 + 8 = 0$ v $\mathbb{Z}_{11}$ a po vyřešení je $a_2 = 6$.
Dosazení vektoru $(a_1, 6, 1, 0, 0)$ do první rovnice v (4.3) dává $5a_1 + 24 + 3 = 0$ v $\mathbb{Z}_{11}$ a po vyřešení je $a_1 = 10$.
První vektor fundamentálního systému je $(10, 6, 1, 0, 0)$.

(b) Druhý vektor: dosazení vektoru $(b_1, b_2, 0, 1, 0)$ do druhé rovnice v (4.3) dává $6b_2 + 2 = 0$ v $\mathbb{Z}_{11}$ a po vyřešení je $b_2 = 7$.
Dosazení vektoru $(b_1, 7, 0, 1, 0)$ do první rovnice v (4.3) dává $5b_1 + 28 + 2 = 0$ v $\mathbb{Z}_{11}$ a po vyřešení je $b_1 = 5$.
Druhý vektor fundamentálního systému je $(5, 7, 0, 1, 0)$.

(c) Třetí vektor: dosazení vektoru $(c_1, c_2, 0, 0, 1)$ do druhé rovnice v (4.3) dává $6c_2 + 0 = 0$ v $\mathbb{Z}_{11}$ a po vyřešení je $c_2 = 0$.
Dosazení vektoru $(b_1, 0, 0, 0, 1)$ do první rovnice v (4.3) dává $5c_1 + 7 = 0$ v $\mathbb{Z}_{11}$ a po vyřešení je $c_1 = 3$.
Třetí vektor fundamentálního systému je $(3, 0, 0, 0, 1)$.

Kontrolní matice $\mathbb{H}$ je (například)

$$\begin{pmatrix} 10 & 6 & 1 & 0 & 0 \\ 5 & 7 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 1 \end{pmatrix}$$

2. **Druhý způsob řešení:** původní matici budeme upravovat tak, abychom dostali na začátku jednotkovou matici.

$$\begin{pmatrix} 5 & 4 & 3 & 2 & 7 \\ 7 & 6 & 4 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 5 & 4 & 3 & 2 & 7 \\ 0 & 6 & 8 & 2 & 0 \end{pmatrix} \begin{matrix} R_1 \\ R_1 + 4 \cdot R_2 \end{matrix} \sim$$

$$\begin{pmatrix} 5 & 0 & 5 & 8 & 7 \\ 0 & 6 & 8 & 2 & 0 \end{pmatrix} \begin{matrix} R_1 + 3 \cdot R_2 \\ R_2 \end{matrix} \sim \begin{pmatrix} 1 & 0 & 1 & 6 & 8 \\ 0 & 1 & 5 & 4 & 0 \end{pmatrix} \begin{matrix} 9 \cdot R_1 \\ 2 \cdot R_2 \end{matrix}$$

Nyní použijeme větu z přednášky: generující matice je v blokovém tvaru

$$\left(\begin{array}{cc|ccc} 1 & 0 & 1 & 6 & 8 \\ 0 & 1 & 5 & 4 & 0 \end{array}\right)$$

a proto je příslušná kontrolní matice $\mathbb{H}$

$$\left(\begin{array}{cc|ccc} -1 & -5 & 1 & 0 & 0 \\ -6 & -4 & 0 & 1 & 0 \\ -8 & -0 & 0 & 0 & 1 \end{array}\right) = \begin{pmatrix} 10 & 6 & 1 & 0 & 0 \\ 5 & 7 & 0 & 1 & 0 \\ 3 & 0 & 0 & 0 & 1 \end{pmatrix}$$

■

4.2.2 Příklad Víme, že kontrolní matice $\mathbb{H}$ lineárního kódu nad $\mathbb{Z}_{13}$ je

$$\begin{pmatrix} 5 & 4 & 3 & 2 & 7 \end{pmatrix}$$

Nalezněte (nějakou) příslušnou generující matici $\mathbb{G}$.

Řešení. GEM končí po nula krocích, matice $\mathbb{H}$ má hodnost 1 a matice $\mathbb{G}$ bude obsahovat prvky fundamentálního systému homogenní rovnice

$$\left(\begin{array}{ccccc|c} 5 & 4 & 3 & 2 & 7 & 0 \end{array}\right) \tag{4.4}$$

Počet vektorů ve fundamentálním systému je $5 - 1 = 4$ podle Frobeniovy věty a my je nalezneme metodou organizovaného hádání.

Označme čtyři vektory fundamentálního systému následovně:

$$(a, 1, 0, 0, 0) \quad (b, 0, 1, 0, 0) \quad (c, 0, 0, 1, 0) \quad (d, 0, 0, 0, 1)$$

Požadavky na jednotlivé první položky dostaneme dosazováním jednotlivých vektorů do homogenní rovnice (4.4):

$$5a + 4 = 0 \quad 5b + 3 = 0 \quad 5c + 2 = 0 \quad 5d + 7 = 0 \quad \text{v } \mathbb{Z}_{13}$$

neboli

$$a = 7 \quad b = 2 \quad c = 10 \quad d = 9 \quad \text{v } \mathbb{Z}_{13}$$

Generující matice $\mathbb{G}$ je (například)

$$\begin{pmatrix} 7 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 0 & 0 \\ 10 & 0 & 0 & 1 & 0 \\ 9 & 0 & 0 & 0 & 1 \end{pmatrix}$$

■

Kapitola 5

Počítání modulo polynom

Počítání modulo polynom se řídí stejnými zákonitostmi jako počítání modulo číslo. Celá čísla jsou ovšem systematicky nahrazena polynomy nad $\mathbb{Z}_p$, kde p je prvočíslo. Snad pomůže následující tabulka:

	modulo číslo	modulo polynom
základní množina „čísel“	$\mathbb{Z}$	$\mathbb{Z}_p[x]$, p prvočíslo
„prvočíslo“	prvočíslo	ireducibilní polynom
množina „čísel modulo“	$\mathbb{Z}_m$	$\mathbb{Z}_p[x]/m(x)$

V odstavci 5.1 jsou vyřešeny základní úlohy lineární algebry modulo polynom a v odstavci 5.2 příklady týkající se konečných těles.

5.1 Lineární algebra modulo polynom

5.1.1 Příklad Pokud existuje, nalezněte řešení lineární rovnice $p(x)\cdot(x^2+1)=(x+2)$ v $\mathbb{Z}_3[x]/(x^3+1)$.

Řešení. Nejprve zjistíme, zda má polynom x^2+1 v $\mathbb{Z}_3[x]/(x^3+1)$ inversi. Použijeme k tomu rozšířený Eukleidův algoritmus pro polynomy. Všechny výpočty v tomto algoritmu jsou v $\mathbb{Z}_3[x]$.

$a(x)$	$b(x)$	$q(x)$	$r(x)$	$\alpha_2(x)$	$\alpha_1(x)$	$\beta_2(x)$	$\beta_1(x)$
x^3+1	x^2+1			1	0	0	1
x^3+1	x^2+1	x	$2x+1$	0	1	1	$2x$
x^2+1	$2x+1$	$2x+2$	2	1	$x+1$	$2x$	$2x^2+2x+1$
$2x+1$	2	$x+2$	0				

Zjistili jsme, že Bezoutova rovnost má tvar

$$(x+1)\cdot(x^3+1)+(2x^2+2x+1)\cdot(x^2+1)=2 \quad \text{v } \mathbb{Z}_3[x]$$

neboli platí

$$(2x+2)\cdot(x^3+1)+(x^2+x+2)\cdot(x^2+1)=1 \quad \text{v } \mathbb{Z}_3[x]$$

(vynásobili jsme celou v Bezoutovu rovnost číslem $2^{-1}=2$ v $\mathbb{Z}_3$).

Zjistili jsme tedy, že $\gcd(x^3+1,x^2+1)=1$, proto $(x^2+1)^{-1}$ v $\mathbb{Z}_3[x]/(x^3+1)$ existuje a jde o polynom x^2+x+2.

Rovnice $p(x)\cdot(x^2+1)=(x+2)$ má v $\mathbb{Z}_3[x]/(x^3+1)$ právě jedno řešení, a to

$$p(x)=(x^2+1)^{-1}\cdot(x+2)=(x^2+x+2)\cdot(x+2)=x^3+x+1=x \quad \text{v } \mathbb{Z}_3[x]/(x^3+1)$$

■

5.1.2 Příklad Pokud existuje, nalezněte řešení lineární rovnice $p(x)\cdot(2x+1)=(x+2)$ v $\mathbb{R}[x]/(x^2+1)$.

Řešení.

Komentář. Jsou možné dva způsoby řešení, ukážeme oba dva.

1. **První způsob:** nalezneme (pokud existuje) inversi k $2x+1$ v $\mathbb{R}[x]/(x^2+1)$. Protože polynom x^2+1 je ireducibilní v $\mathbb{R}[x]$, je $\mathbb{R}[x]/(x^2+1)$ těleso. Protože $2x+1$ není nulový prvek, inverse k $2x+1$ v $\mathbb{R}[x]/(x^2+1)$ existuje.

   K nalezení inverse k $2x+1$ použijeme rozšířený Eukleidův algoritmus pro polynomy. Všechny výpočty v tomto algoritmu jsou v $\mathbb{R}[x]$.

$a(x)$	$b(x)$	$q(x)$	$r(x)$	$\alpha_2(x)$	$\alpha_1(x)$	$\beta_2(x)$	$\beta_1(x)$
x^2+1	$2x+1$			1	0	0	1
x^2+1	$2x+1$	$\frac{1}{2}x-\frac{1}{4}$	$\frac{5}{4}$	0	1	1	$-\frac{1}{2}x+\frac{1}{4}$
$2x+1$	$\frac{5}{4}$	$\frac{8}{5}x+\frac{4}{5}$	0				

   Bezoutova rovnost má tudíž tvar

$$1\cdot(x^2+1)+(-\frac{1}{2}x+\frac{1}{4})\cdot(2x+1)=\frac{5}{4} \quad \text{v } \mathbb{R}[x]$$

   neboli

$$\frac{4}{5}\cdot(x^2+1)+(-\frac{2}{5}x+\frac{1}{5})\cdot(2x+1)=1 \quad \text{v } \mathbb{R}[x]$$

   (původní Bezoutovu rovnost jsme vynásobili $(\frac{5}{4})^{-1}=\frac{4}{5}$ v $\mathbb{R}[x]$).

   Zjistili jsme, že $\gcd(x^2+1,2x+1)=1$, proto $(2x+1)^{-1}$ v $\mathbb{R}[x]/(x^2+1)$ existuje a jde o polynom $-\frac{2}{5}x+\frac{1}{5}$.

   Zadaná rovnice má tedy jediné řešení:

$$p(x)=(2x+1)^{-1}\cdot(x+2)=(-\frac{2}{5}x+\frac{1}{5})\cdot(x+2)=-\frac{2}{5}x^2-\frac{3}{5}x+\frac{2}{5}=-\frac{3}{5}x+\frac{4}{5} \quad \text{v } \mathbb{R}[x]/(x^2+1)$$

2. **Druhý způsob:** z přednášky víme, že platí $\mathbb{R}[x]/(x^2+1)$ je těleso, které je isomorfní tělesu $\mathbb{C}$ komplexních čísel, tudíž jde o obyčejnou lineární rovnici $p\cdot(2i+1)=i+2$ v komplexním oboru. Proto je řešení tvaru

$$p=\frac{i+2}{2i+1}=\frac{i+2}{2i+1}\cdot\frac{-2i+1}{-2i+1}=\frac{-3i+4}{5}=-\frac{3}{5}i+\frac{4}{5} \quad \text{v } \mathbb{C}$$

   neboli (po ztotožnění $i=x$)

$$p(x)=-\frac{3}{5}x+\frac{4}{5} \quad \text{v } \mathbb{R}[x]/(x^2+1)$$

■

5.1.3 Příklad Nad tělesem $\mathbb{Z}_2[x]/(x^2+x+1)$ vyřešte (použitím GEM) soustavu lineárních rovnic:

$$\begin{array}{rcrcrcrl} ax_1 & + & x_2 & + & x_3 & + & ax_4 & = b \\ x_1 & + & bx_2 & + & ax_3 & + & ax_4 & = 1 \end{array} \tag{5.1}$$

kde značíme $a=x$, $b=x+1$, tj. tabulky sčítání a násobení v $\mathbb{Z}_2[x]/(x^2+x+1)$ vypadají takto:

$+$	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

(5.2)

Řešení. Přepíšeme soustavu do matice

$$\left(\begin{array}{cccc|c} a & 1 & 1 & a & b \\ 1 & b & a & a & 1 \end{array}\right)$$

a matici upravujeme pomocí GEM:

$$\left(\begin{array}{cccc|c} a & 1 & 1 & a & b \\ 1 & b & a & a & 1 \end{array}\right) \sim \left(\begin{array}{cccc|c} a & 1 & 1 & a & b \\ 0 & 0 & a & 1 & 1 \end{array}\right) \begin{array}{l} R_1 \\ R_2 - a \cdot R_2 \end{array}$$

Komentář. Používáme „zdravotní značení“, abychom neztratili přehled o tom, co se děje. Viz příklad 4.2.1. Značka R_1 znamená: nový první řádek je opsaný starý první řádek. Značka $R_1 - a \cdot R_2$ znamená: nový druhý řádek je starý první řádek, od kterého jsme odečetli a-násobek starého druhého řádku.

GEM skončila: hodnost matice soustavy je rovna hodnosti rozšířené matice soustavy (a je rovna 2). Podle Frobeniovy věty řešení soustavy (5.1) existuje.

Nalezneme partikulární řešení a fundamentální systém.

1. Partikulární řešení je jakákoli čtveřice, která soustavu řeší. Použijeme zápis soustavy po skončení eliminace

$$\left(\begin{array}{cccc|c} a & 1 & 1 & a & b \\ 0 & 0 & a & 1 & 1 \end{array}\right)$$

Zvolíme-li $(x_1, 0, 0, 1)$, bude náš vektor jistě řešit druhou rovnici. První položku dopočítáme z první rovnice: musí platit $ax_1 + a = b$, a tedy $ax_1 = b - a = 1$, neboli $x_1 = b$.

Partikulární řešení je čtveřice $(b, 0, 0, 1)$.

2. Fundamentální systém musí mít $4 - 2 = 2$ prvky, protože soustava má 4 neznámé a hodnost matice soustavy je 2. Použijeme maticový zápis homogenní soustavy

$$\left(\begin{array}{cccc|c} a & 1 & 1 & a & 0 \\ 0 & 0 & a & 1 & 0 \end{array}\right) \tag{5.3}$$

První vektor ve fundamentálním systému napíšeme ve tvaru $(x_1, 0, x_2, 1)$ a druhý vektor ve tvaru $(y_1, 1, y_2, 0)$. Volba nul a jedniček ve druhé a čtvrté položce zajistí lineární nezávislost.

Komentář. Tvar soustavy (5.3) nám nedovoluje volit jedničky a nuly na posledních dvou položkách. Metoda organizovaného hádání nám přikazuje pozici jedniček a nul posunout směrem doleva.

Další položky musíme dopočítat.

Dopočtení x_2: ze druhé rovnice v (5.3) dostáváme požadavek $ax_2 + 1 = 0$, neboli $ax_2 = -1 = 1$, tudíž $x_2 = b$.

Dopočtení x_1: z první rovnice v (5.3) dostáváme požadavek $ax_1 + b + a = 0$, neboli $ax_1 = -b - a = b + a = 1$, tudíž $x_1 = b$.

Dopočtení y_2: ze druhé rovnice v (5.3) dostáváme požadavek $ay_2 + 0 = 0$, neboli $ay_2 = 0$, tudíž $y_2 = 0$.

Dopočtení y_1: z první rovnice v (5.3) dostáváme požadavek $ay_1 + 1 + 0 + 0 = 0$, neboli $ay_1 = -1 = 1$, tudíž $y_1 = b$.

Fundamentální systém je tvořen vektory $(b, 0, b, 1)$ a $(b, 1, 0, 0)$.

Celkové řešení soustavy (5.1) je

$$(b, 0, 0, 1) + \alpha \cdot (b, 0, b, 1) + \beta \cdot (b, 1, 0, 0)$$

kde α, β jsou libovolné prvky ze $\mathbb{Z}_2[x]/(x^2 + x + 1)$. ■

5.2 Konečná tělesa

5.2.1 Příklad Označte jako $\mathbb{Z}_3(i)$ množinu $\{a+bi \mid a,b \in \mathbb{Z}_3\}$. (Připomeňme, že i je komplexní jednotka splňující $i^2=-1$.) Na množině $\mathbb{Z}_3(i)$ definujte zřejmým způsobem sčítání a násobení:

$$(a+bi)+(a'+b'i)=(a+a')+(b+b')i, \quad (a+bi)\cdot(a'+b'i)=(aa'-bb')+(ab'+a'b)i.$$

Je $\langle \mathbb{Z}_3(i),+,\cdot\rangle$ těleso?

Řešení.

> **Komentář.** Existuje přímý způsob, jak příklad vyřešit, tj. ověřit axiomy tělesa. Předvedeme způsob jiný: množina $\mathbb{Z}_3(i)$ totiž připomíná komplexní čísla, takže by mohlo platit $\mathbb{Z}_3(i) \cong \mathbb{Z}_3[x]/(x^2+1)$. Připomeňme, že prvky množiny $\mathbb{Z}_3[x]/(x^2+1)$ jsou všechny výrazy tvaru $bx+a$, kde a, b jsou prvky množiny $\mathbb{Z}_3$. Tyto polynomy se sčítají a násobí následovně: $(bx+a)+(b'x+a')=(b+b')x+(a+a')$, $(bx+a)\cdot(b'x+a')=(ab'+a'b)x+(aa'-bb')$.

Zobrazení $f:\mathbb{Z}_3(i) \longrightarrow \mathbb{Z}_3[x]/(x^2+1)$ definované předpisem $f(a+bi)=bx+a$ je zřejmě bijekce:

1. Zobrazení f je prosté. Ať platí $f(a+bi)=f(a'+b'i)$. Chceme dokázat, že platí $a+bi=a'+b'i$.

   Jestliže $bx+a=b'x+a'$, potom platí $b=b'$ a současně $a=a'$. K tomu jsme použili fakta o rovnosti dvou polynomů. Ukázali jsme, že rovnost $a+bi=a'+b'i$ platí.

   Dokázali jsme, že zobrazení f je prosté.

2. Zobrazení f je na. Ať $bx+a$ je libovolný prvek $\mathbb{Z}_3[x]/(x^2+1)$. Hledáme prvek $a'+b'i$ v $\mathbb{Z}_3(i)$ tak, že platí $f(a'+b'i)=bx+a$.

   Stačí zvolit $b=b'$ a $a=a'$.

   Dokázali jsme, že zobrazení f je na.

   > **Komentář.** Právě jsme ukázali, že *množiny* $\mathbb{Z}_3(i)$ a $\mathbb{Z}_3[x]/(x^2+1)$ jsou z abstraktního hlediska stejné. Zobrazení f slouží jako „přemalování“ prvků množiny $\mathbb{Z}_3(i)$ na prvky množiny $\mathbb{Z}_3[x]/(x^2+1)$.
   >
   > Na obou množinách je však definována jistá struktura sčítání a násobení. Musíme ukázat, že zobrazení f tuto strukturu respektuje.

Zobrazení f respektuje sčítání a násobení.

1. Zobrazení f respektuje sčítání: máme dokázat, že platí $f((a+bi)+(a'+b'i))=f(a+bi)+f(a'+b'i)$, a to pro libovolné prvky $a+bi$, $a'+b'i$ z množiny $\mathbb{Z}_3(i)$.

   Levá, stejně jako pravá strana požadované rovnosti je $(b+b')x+(a+a')$, to jsme chtěli dokázat.

   Dokázali jsme, že zobrazení f respektuje sčítání.

2. Zobrazení f respektuje násobení: máme dokázat, že platí $f((a+bi)\cdot(a'+b'i))=f(a+bi)\cdot f(a'+b'i)$, a to pro libovolné prvky $a+bi$, $a'+b'i$ z množiny $\mathbb{Z}_3(i)$.

   Levá, stejně jako pravá strana požadované rovnosti je $(ab'+a'b)x+(aa'-bb')$, to jsme chtěli dokázat.

   Dokázali jsme, že zobrazení f respektuje násobení.

   > **Komentář.** Právě jsme ukázali, že struktury $\langle \mathbb{Z}_3(i),+,\cdot\rangle$ a $\langle \mathbb{Z}_3[x]/(x^2+1),+,\cdot\rangle$ jsou isomorfní. Isomorfismem je zobrazení f.

Zbývá dokázat, že $\mathbb{Z}_3[x]/(x^2+1)$ je těleso. K tomu je zapotřebí dokázat, že polynom x^2+1 je ireducibilní v $\mathbb{Z}_3[x]$. Stačí vyzkoušet dělitelnost polynomu x^2+1 všemi polynomy stupně přesně 1.

> **Komentář.** To připomíná Eratosthenovo síto pro test prvočíselnosti, viz příklad 3.2.2. Chceme-li testovat ireducibilitu polynomu $p(x)$ stupně n, stačí testovat dělitelnost všemi polynomy $q(x)$ stupně alespoň 1 a nanejvýš $\frac{n}{2}$.

Polynom nad $\mathbb{Z}_3$ stupně přesně 1 lze zakódovat dvojicí koeficientů (a_1,a_0), kde a_1, a_0 jsou prvky $\mathbb{Z}_3$ a $a_1 \neq 0$. Proto je polynomů stupně právě 1 přesně $2\cdot 3=6$. Jsou to polynomy

$$x, \quad 2x, \quad x+1, \quad x+2, \quad 2x+1, \quad 2x+2.$$

Po vydělení se zbytkem (všechny výpočty jsou v $\mathbb{Z}_3[x]$) dostáváme

$$x^2+1=x\cdot x+1, \quad x^2+1=2x\cdot 2x+1, \quad x^2+1=(x+1)\cdot(x+2)+2, \quad x^2+1=(2x+1)\cdot(2x+2)+2,$$

proto je polynom x^2+1 ireducibilní v $\mathbb{Z}_3[x]$ a $\langle \mathbb{Z}_3[x]/(x^2+1), +, \cdot \rangle$ je těleso.

Protože $\langle \mathbb{Z}_3(i), +, \cdot \rangle$ a $\langle \mathbb{Z}_3[x]/(x^2+1), +, \cdot \rangle$ jsou isomorfní, je těleso i $\langle \mathbb{Z}_3(i), +, \cdot \rangle$. ■

5.2.2 Příklad Existuje těleso, které má přesně 76 různých prvků?

Řešení. Podle věty o klasifikaci konečných těles je každé konečné těleso (až na isomorfismus) některé Galoisovo těleso $GF(p^n)$, kde p je prvočíslo a $n \geq 1$ je přirozené číslo. Navíc těleso $GF(p^n)$ pak má přesně p^n různých prvků.

Protože číslo 76 nelze napsat ve tvaru p^n, kde p je prvočíslo a $n \geq 1$ je přirozené číslo ($76 = 2^2 \cdot 19$), konečné těleso s přesně 76 prvky neexistuje. ■

5.2.3 Příklad Nalezněte těleso o 16 prvcích.

Řešení. Protože $16 = 2^4$, hledáme podle věty o klasifikaci konečných těles Galoisovo těleso $GF(2^4)$. K tomu stačí najít ireducibilní polynom $m(x)$ stupně 4 nad $\mathbb{Z}_2$. Hledané těleso $GF(2^4)$ pak je $\mathbb{Z}_2[x]/m(x)$.

Polynom $a_4x^4 + a_3x^3 + a_2x^2 + a_1x + a_0$ stupně 4 nad $\mathbb{Z}_2$ můžeme zakódovat jako pětici $(a_4, a_3, a_2, a_1, a_0)$ jeho koeficientů, kde $a_i \in \mathbb{Z}_2$ a $a_4 \neq 0$. Takových pětic je přesně $1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 = 16$.

Jediná možnost je prohledat množinu 16 polynomů hrubou silou, protože žádný algoritmus hledající ireducibilní polynomy nemáme k disposici. Přesto lze onu množinu zredukovat: žádný polynom kódovaný pěticí, která obsahuje sudý počet jedniček, není ireducibilní. Každý takový polynom totiž musí mít kořen 1 a proto je dělitelný příslušným kořenovým faktorem $x+1$. Projdeme tedy pouze polynomy kódované pěticemi s lichým počtem jedniček. Navíc pro ireducibilitu stačí testovat dělitelnost polynomy x, $x+1$, x^2, x^2+x, x^2+x+1 a x^2+1.

1. Pětice $(1,0,0,0,0)$: polynom x^4 není ireducibilní, platí $x^4 = x^2 \cdot x^2$.
2. Pětice $(1,0,0,1,1)$: polynom x^4+x+1 je ireducibilní. Není totiž dělitelný žádným z polynomů x (zbytek 1), $x+1$ (zbytek 1), x^2 (zbytek $x+1$), x^2+x (zbytek 1), x^2+x+1 (zbytek 1) a x^2+1 (zbytek x).

   Komentář. Tady bychom mohli příklad ukončit. Stačilo najít alespoň jeden ireducibilní polynom stupně 4. Jak uvidíme, je takových polynomů více.

3. Pětice $(1,0,1,0,1)$: polynom x^4+x^2+1 není ireducibilní, platí $x^4+x^2+1 = (x^2+x+1) \cdot (x^2+x+1)$.
4. Pětice $(1,0,1,1,0)$: polynom x^4+x^2+x není ireducibilní, platí $x^4+x^2+x = x \cdot (x^3+x+1)$.
5. Pětice $(1,1,0,0,1)$: polynom x^4+x^3+1 je ireducibilní. Není totiž dělitelný žádným z polynomů x (zbytek 1), $x+1$ (zbytek 1), x^2 (zbytek 1), x^2+x (zbytek 1), x^2+x+1 (zbytek x) a x^2+1 (zbytek x).
6. Pětice $(1,1,0,1,0)$: polynom x^4+x^3+x není ireducibilní, platí $x^4+x^3+x = x \cdot (x^3+x^2+1)$.
7. Pětice $(1,1,1,0,0)$: polynom $x^4+x^3+x^2$ není ireducibilní, platí $x^4+x^3+x^2 = x^2 \cdot (x^2+x+1)$.
8. Pětice $(1,1,1,1,1)$: polynom $x^4+x^3+x^2+x+1$ je ireducibilní. Není totiž dělitelný žádným z polynomů x (zbytek 1), $x+1$ (zbytek 1), x^2 (zbytek $x+1$), x^2+x (zbytek 1), x^2+x+1 (zbytek $x+1$) a x^2+1 (zbytek 1).

Nalezli jsme dokonce tři ireducibilní polynomy stupně 4 nad $\mathbb{Z}_3$.

Hledané těleso je kterékoli ze tří těles $\mathbb{Z}_2[x]/(x^4+x+1)$, $\mathbb{Z}_2[x]/(x^4+x^3+1)$, $\mathbb{Z}_2[x]/(x^4+x^3+x^2+x+1)$.

Komentář. Tělesa $\mathbb{Z}_2[x]/(x^4+x+1)$, $\mathbb{Z}_2[x]/(x^4+x^3+1)$ a $\mathbb{Z}_2[x]/(x^4+x^3+x^2+x+1)$ jsou (podle věty o klasifikaci konečných těles) navzájem isomorfní. To dokazovat nebudeme.

■

Kapitola 6

Abstraktní výpočty

V této kapitole jsou spočteny některé příklady z teorie jednoduchých algebraických struktur a rovnicových algebraických specifikací. Nejde dát obecný návod, jak takové příklady řešit. Obecně platná je jediná rada: postupujte vždy formálně a používejte rovnicové vlastnosti jako přepisovací pravidla.

Úlohy uvedené v odstavci 6.3 navíc vyžadují statečnou kreativitu: specifikovat můžeme téměř cokoli, měli bychom ale umět napsanou specifikaci obhájit.

6.1 Grupoidy, pologrupy, monoidy a grupy

6.1.1 Příklad Na množině reálných čísel $\mathbb{R}$ je definována binární operace $\star$ následovně:

$$x \star y = x + y + x^2 y$$

Ukažte, že platí:

1. Operace $\star$ má neutrální prvek e.
2. Pro každé x existuje právě jedno y tak, že $x \star y = e$. Tomuto jednoznačně určenému y říkáme *pravá inverse k* x.
3. Existuje x tak, že rovnost $y \star x = e$ neplatí pro žádné y. To znamená, že *levá inverse k* x obecně neexistuje.

Řešení. Vyřešíme jednotlivé body:

1. Neutrální prvek e: chceme najít reálné číslo e tak, aby platily rovnosti $x \star e = x$ a $e \star x = x$, a to pro všechna reálná čísla x.

   V první rovnosti $x \star e = x$ přepíšeme levou stranu pomocí definice $\star$: požadujeme rovnost $x + e + x^2 e = x$, neboli $e + x^2 e = e \cdot (1 + x^2) = 0$. Proto $e = 0$.

   Pokud ukážeme, že $0 \star x = x$ platí pro všechna x, ukážeme, že $e = 0$ je neutrální prvek operace $\star$. Přepíšeme levou stranu pomocí definice $\star$: dostáváme rovnost $0 + x + 0^2 x = x$.

   Ukázali jsme, že číslo 0 je neutrální prvek operace $\star$.

2. Zvolme libovolné x. Hledáme jednoznačně určené y tak, aby platilo $x \star y = e$. Tuto rovnost přepíšeme pomocí definice $\star$ a znalosti prvku e na $x + y + x^2 y = 0$. Ta má jednoznačné řešení vzhledem k y: $y = \dfrac{-x}{1 + x^2}$.

3. Hledáme takové číslo x, aby rovnice $y \star x = e$ neměla žádné řešení v $\mathbb{R}$. Rozepišme rovnici $y \star x = e$ podle definice $\star$: $y + x + y^2 x = 0$. Pro pevné x se zjevně jedná o kvadratickou rovnici pro y. Ta nebude mít řešení v $\mathbb{R}$ například pro $x = 1$, protože její diskriminant pak bude záporný.

   Závěr: pro $x = 1$ neexistuje y tak, že $y \star x = e$.

■

6.1.2 Příklad Rozhodněte, zda $\langle \mathbb{R}, \star \rangle$ je pologrupa, kde operace $\star$ na množině reálných čísel $\mathbb{R}$ je definována takto: $x \star y = x + y + xy$.

Řešení. Máme rozhodnout, zda rovnost $(x \star y) \star z = x \star (y \star z)$ platí pro všechna reálná čísla x, y, z.
Upravíme levou a pravou stranu požadované rovnice podle definice $\star$.

1. Levá strana: $(x \star y) \star z = (x+y+xy) \star z = x+y+xy+z+(x+y+xy)z = x+y+z+xy+xz+yz+xyz$.
2. Pravá strana: $x \star (y \star z) = x \star (y+z+yz) = x+y+z+yz+x(y+z+yz) = x+y+z+xy+xz+yz+xyz$.

Protože levá strana je rovna pravé straně, pro libovolná reálná čísla x, y, z, dokázali jsme asociativitu operace $\star$.
Závěr: $\langle \mathbb{R}, \star \rangle$ je pologrupa. ■

6.1.3 Příklad Rozhodněte, zda $\langle \mathbb{N}, \star \rangle$ je pologrupa, kde operace $\star$ na množině přirozených čísel $\mathbb{N}$ je definována takto: $x \star y = x^y$.

Řešení. Máme rozhodnout, zda rovnost $(x \star y) \star z = x \star (y \star z)$ platí pro všechna přirozená čísla x, y, z.
Upravíme levou a pravou stranu požadované rovnice podle definice $\star$.

1. Levá strana: $(x \star y) \star z = (x^y)^z = x^{yz}$.
2. Pravá strana: $x \star (y \star z) = x \star (y^z) = x^{(y^z)}$.

   Komentář. Nezdá se, že by (obecně) byla levá strana rovnosti byla stejná jako pravá strana. Tento pocit musíme ospravedlnit svědky, kteří dosvědčí, že levá strana je různá od pravé strany.

Levá strana pro $x = 3$, $y = 3$, $z = 3$ je $3^9 = 19\,683$ a pravá strana pro $x = 3$, $y = 3$, $z = 3$ je $3^{27} = 7\,625\,597\,484\,987$.
Asociativní zákon pro $\star$ neplatí a proto $\langle \mathbb{N}, \star \rangle$ není pologrupa. ■

6.1.4 Příklad Označte jako $t : \{a, b\} \longrightarrow \{a, b\}$ funkci $t(a) = b$, $t(b) = a$. Dále označte $S = \{t, t \circ t\}$. Dokažte, že $\langle S, \circ \rangle$ je grupa.

Řešení. Především je $\circ$ skutečně operace na S: to plyne z toho, že $t \circ t = \mathrm{id}$ (identická funkce), takže platí rovnosti

$$\mathrm{id} \circ \mathrm{id} = \mathrm{id} \quad \mathrm{id} \circ t = t \quad t \circ \mathrm{id} = t \quad t \circ t = \mathrm{id}$$

Ukázali jsme, že $\langle S, \circ \rangle$ je grupoid.

1. **Asociativita $\circ$:** skládání funkcí je vždy asociativní.
   Ukázali jsme, že $\langle S, \circ \rangle$ je pologrupa.
2. **Neutrální prvek:** označíme $e = \mathrm{id}$. Potom platí rovnosti $e \circ f = f \circ e = f$, a to pro všechna $f \in S$.
   Ukázali jsme, že $\langle S, \circ, e \rangle$ je monoid.
3. **Inverse:** definujeme $t^{-1} = t$ a $\mathrm{id}^{-1} = \mathrm{id}$. Definovali jsme unární operaci a zjevně platí rovnosti $f^{-1} \circ f = f \circ f^{-1} = e$, a to pro všechna $f \in S$.
   Ukázali jsme, že $\langle S, \circ, e, (-)^{-1} \rangle$ je grupa.

■

6.1.5 Příklad Centrum grupy $\langle G, \star, e, (-)^{-1} \rangle$ je množina

$$Z(G) = \{a \in G \mid a \star g = g \star a \text{ pro všechna } g \in G\}.$$

Ukažte, že množina $Z(G)$ je v G uzavřena na všechny operace, a tvoří tudíž podgrupu grupy $\langle G, \star, e, (-)^{-1} \rangle$.

Řešení. Máme dokázat uzavřenost centra na binární operaci, neutrální prvek a inversi.

1. **Uzavřenost na binární operaci:** máme dokázat, že $a_1 \star a_2 \in Z(G)$, a to pro všechna a_1, a_2 ze $Z(G)$.
   Zvolíme libovolný prvek $g \in G$. Chceme ukázat, že platí rovnost
   $$(a_1 \star a_2) \star g = g \star (a_1 \star a_2). \tag{6.1}$$
   Budeme přepisovat levou stranu požadované rovnosti a budeme při tom využívat axiomů grupy:
   $$\begin{array}{rcll} (a_1 \star a_2) \star g & = & a_1 \star (a_2 \star g) & (\text{asociativita } \star) \\ & = & a_1 \star (g \star a_2) & (\text{protože } a_2 \in Z(G)) \\ & = & (a_1 \star g) \star a_2 & (\text{asociativita } \star) \\ & = & (g \star a_1) \star a_2 & (\text{protože } a_1 \in Z(G)) \\ & = & g \star (a_1 \star a_2) & (\text{asociativita } \star) \end{array}$$
   Levou stranu rovnosti (6.1) jsme přepsali na pravou, proto je množina $Z(G)$ uzavřena na operaci $\star$.
2. **Uzavřenost na neutrální prvek:** máme dokázat, že $e \in Z(G)$.
   Zvolíme libovolný prvek $g \in G$. Chceme ukázat, že platí $e \star g = g \star e$. Tato rovnost ale platí, protože e je neutrální prvek grupy $\langle G, \star, e, (-)^{-1} \rangle$.
3. **Uzavřenost na inversi:** máme dokázat, že $a^{-1} \in Z(G)$, a to pro všechna a ze $Z(G)$.
   Zvolíme libovolný prvek $g \in G$. Chceme ukázat, že platí rovnost
   $$a^{-1} \star g = g \star a^{-1}. \tag{6.2}$$
   Stačí dokázat, že platí rovnost
   $$g = a \star (g \star a^{-1}), \tag{6.3}$$
   protože z (6.3) plyne (6.2) vynásobením zleva prvkem a^{-1}. Budeme upravovat pravou stranu rovnosti (6.3) a využívat při tom axiomů grupy:
   $$\begin{array}{rcll} a \star (g \star a^{-1}) & = & (a \star g) \star a^{-1} & (\text{asociativita } \star) \\ & = & (g \star a) \star a^{-1} & (\text{protože } a \in Z(G)) \\ & = & g \star (a \star a^{-1}) & (\text{asociativita } \star) \\ & = & g \star e & (\text{axiom pro } (-)^{-1}) \\ & = & g & (\text{axiom pro } e) \end{array}$$
   Pravou stranu rovnosti (6.3) jsme přepsali na levou, proto je množina $Z(G)$ uzavřena na operaci $(-)^{-1}$.

■

6.1.6 Příklad Ať $\langle X, / \rangle$ je grupoid a $e \in X$ je prvek takový, že platí následující čtyři axiomy

$$\text{(i) } x/e = x \qquad \text{(ii) } x/x = e \qquad \text{(iii) } e/(x/y) = y/x \qquad \text{(iv) } (x/z)/(y/z) = x/y$$

pro všechny prvky x, y, z z X.

Definujte $x \star y = x/(e/y)$ a $x^{-1} = e/x$. Dokažte, že e je neutrální prvek operace $\star$ a že x^{-1} je inverse k x.

Řešení. Nejprve si uvědomme, že $\star$ a $(-)^{-1}$ jsou skutečně operace. To plyne z toho, že $\langle X, / \rangle$ je grupoid. Žádané axiomy ověříme v tomto pořadí:

1. **Neutralita e:** máme ověřit rovnosti $x \star e = e \star x = x$, a to pro libovolné $x \in X$.
   Rovnost $x \star e = x$ dokážeme tak, že budeme přepisovat její levou stranu a budeme při tom využívat definici $\star$ a axiomy (i)–(iv):
   $$\begin{array}{rcll} x \star e & = & x/(e/e) & (\text{definice } \star) \\ & = & x/e & (\text{axiom (ii), aplikovaný na } e) \\ & = & x & (\text{axiom (i)}) \end{array}$$

Rovnost $e \star x = x$ dokážeme tak, že budeme přepisovat její levou stranu a budeme při tom využívat definici $\star$ a axiomy (i)–(iv):

$$\begin{array}{rcll} e \star x & = & e/(e/x) & \text{(definice } \star\text{)} \\ & = & x/e & \text{(axiom (iii))} \\ & = & x & \text{(axiom (i))} \end{array}$$

Ukázali jsme, že e je neutrální prvek operace $\star$.

2. **Axiomy pro inverse:** máme dokázat, že platí rovnosti $x^{-1} \star x = x \star x^{-1} = e$, a to pro libovolné $x \in X$.

   Rovnost $x^{-1} \star x = e$ dokážeme tak, že budeme přepisovat její levou stranu a budeme při tom využívat definici $\star$, $(-)^{-1}$ a axiomy (i)–(iv):

$$\begin{array}{rcll} x^{-1} \star x & = & (e/x)/(e/x) & \text{(definice } \star \text{ a } (-)^{-1}\text{)} \\ & = & e & \text{(axiom (ii), aplikovaný na } e/x\text{)} \end{array}$$

   Rovnost $x \star x^{-1} = e$ dokážeme tak, že budeme přepisovat její levou stranu a budeme při tom využívat definici $\star$, $(-)^{-1}$ a axiomy (i)–(iv):

$$\begin{array}{rcll} x \star x^{-1} & = & x/(e/(e/x)) & \text{(definice } \star \text{ a } (-)^{-1}\text{)} \\ & = & x/(x/e) & \text{(axiom (iii), aplikovaný na } e/x\text{)} \\ & = & x/x & \text{(axiom (i))} \\ & = & e & \text{(axiom (ii))} \end{array}$$

Komentář. Povšimněme si, že pro důkaz požadovaných tvrzení jsme *nepoužili* axiom (iv). Podobnou technikou však lze dokázat, že operace $\star$ je asociativní, a tudíž, že $\langle X, \star, e, (-)^{-1}\rangle$ je grupa. To ale není úplně triviální, je zapotřebí dokázat řadu pomocných tvrzení. Zde už axiom (iv) budeme skutečně pořebovat.

■

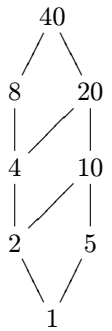
6.2 Posety, svazy a Booleovy algebry

6.2.1 Příklad Označte jako X množinu všech dělitelů čísla 40. Pro x, y z množiny X definujte $x \sqsubseteq y$ právě tehdy, když číslo y je dělitelné číslem x. Ukažte, že $\langle X, \sqsubseteq\rangle$ je poset, ve kterém existují suprema a infima všech dvojic.

Řešení. Protože platí $40 = 2^3 \cdot 5$, má množina X celkem $(3+1)\cdot(1+1) = 8$ různých prvků. Platí $X = \{1, 2, 4, 5, 8, 10, 20, 40\}$.

K tomu, že $\langle X, \sqsubseteq\rangle$ je poset, stačí ukázat, že relace $\sqsubseteq$ je reflexivní, transitivní a antisymetrická. To se dokáže analogicky jako v příkladu 2.1.4.

Nakreslíme Hasseho diagram $\langle X, \sqsubseteq\rangle$:



(6.4)

Z tohoto obrázku je vidět, že suprema a infima všech dvojic existují: $\sup_{\sqsubseteq}\{x, y\} = \mathrm{lcm}(x, y)$ (nejmenší společný násobek x a y) a $\inf_{\sqsubseteq}\{x, y\} = \gcd(x, y)$ (největší společný dělitel x a y). ■

6.2.2 Příklad Rozhodněte, zda v obecném svazu $\langle X, \wedge, \vee\rangle$ platí nerovnost $x \wedge y \sqsubseteq x \wedge (y \vee z)$.

Řešení.

> **Komentář.** Připomínáme, že svazy jsou přesně posety, ve kterých existují suprema a infima všech dvojic. Přitom platí $x \wedge y = \inf_{\sqsubseteq}\{x, y\}$ a $x \vee y = \sup_{\sqsubseteq}\{x, y\}$ pro všechna x a y. Této korespondence budeme využívat.

Nerovnost $x \wedge y \sqsubseteq x \wedge (y \vee z)$ platí přesně když platí

$$x \wedge y \sqsubseteq x \quad \text{a současně} \quad x \wedge y \sqsubseteq y \vee z \tag{6.5}$$

pro všechna x, y, z. To plyne z toho, že $x \wedge (y \vee z)$ je infimum x a $y \vee z$ v uspořádání $\sqsubseteq$.

Levá část požadavku (6.5) je splněna pro všechna x, y: platí totiž $\inf_{\sqsubseteq}\{x, y\} \sqsubseteq x$.

Pravá strana požadavku (6.5) je splněna díky transitivitě uspořádání $\sqsubseteq$. Platí totiž

$$x \wedge y \sqsubseteq y \quad \text{a současně} \quad y \sqsubseteq y \vee z \tag{6.6}$$

a to pro všechna x, y, z.

Levá strana požadavku (6.6) je splněna pro všechna x, y: platí totiž $\inf_{\sqsubseteq}\{x, y\} \sqsubseteq y$.

Pravá strana požadavku (6.6) je splněna pro všechna y, z: platí totiž $y \sqsubseteq \sup_{\sqsubseteq}\{y, z\}$.

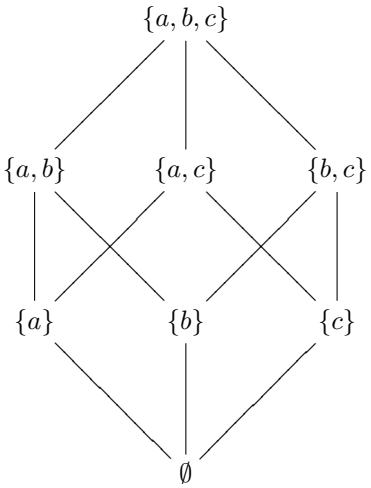
Závěr: nerovnost $x \wedge y \sqsubseteq x \wedge (y \vee z)$ platí pro všechna x, y, z v libovolném svazu $\langle X, \wedge, \vee\rangle$. ■

6.2.3 Příklad Ukažte, že poset $\langle X, \sqsubseteq\rangle$ z příkladu 6.2.1 není Booleova algebra.

Řešení. Připomeňme, že $X = \{1, 2, 4, 5, 8, 10, 20, 40\}$. Množina X má tudíž 8 prvků. Podle věty o klasifikaci konečných Booleových algeber by poset $\langle X, \sqsubseteq\rangle$ z příkladu 6.2.1 musel být isomorfní Booleově algebře

$$\langle \exp\{a, b, c\}, \cap, \cup, \emptyset, \{a, b, c\}, \{a, b, c\} \setminus (-)\rangle,$$

která má $2^3 = 8$ prvků. Hasseho diagram takové Booleovy algebry vypadá následovně:



což je Hasseho diagram, který není isomorfní s Hasseho diagramem z obrázku (6.4). Proto $\langle X, \sqsubseteq\rangle$ z příkladu 6.2.1 není Booleova algebra. ■

6.2.4 Příklad Ať $\langle X, \wedge, \vee, \top, \bot, (-)'\rangle$ je Booleova algebra. Definujte $x \Rightarrow y$ jako zkratku za $x' \vee y$. Dokažte, že $x \wedge y \sqsubseteq z$ platí právě tehdy, když platí $x \sqsubseteq y \Rightarrow z$, a to pro všechna x, y, z z množiny X.

Řešení.

> **Komentář.** Využijeme faktu, že Booleova algebra je přesně distributivní, komplementární svaz s největším a nejmenším prvkem. Zvlášť budeme používat definice uspořádání: $x \sqsubseteq y$ platí právě tehdy, když $x \vee y = y$, což platí právě tehdy, když $x \wedge y = x$, a to pro všechna x a y.

1. Předpokládejme, že platí $x \wedge y \sqsubseteq z$, čili $(x \wedge y) \vee z = z$. Chceme dokázat platnost $x \sqsubseteq y \Rightarrow z$, neboli platnost rovnosti $x \vee (y' \vee z) = y' \vee z$. Budeme přepisovat $y' \vee z$ pomocí zákonů Booleovy algebry:

$$\begin{array}{rcll}
y' \vee z & = & y' \vee ((x \wedge y) \vee z) & (\text{platí } (x \wedge y) \vee z = z) \\
& = & y' \vee ((x \vee z) \wedge (y \vee z)) & (\text{distributivní zákon}) \\
& = & (y' \vee (x \vee z)) \wedge (y' \vee (y \vee z)) & (\text{distributivní zákon}) \\
& = & (y' \vee (x \vee z)) \wedge ((y' \vee y) \vee z) & (\text{asociativní zákon}) \\
& = & (y' \vee (x \vee z)) \wedge (\top \vee z) & (\text{vlastnost doplňku}) \\
& = & (y' \vee (x \vee z)) \wedge \top & (\text{axiom pro největší prvek}) \\
& = & y' \vee (x \vee z) & (\text{axiom pro největší prvek}) \\
& = & (y' \vee x) \vee z & (\text{asociativní zákon}) \\
& = & (x \vee y') \vee z & (\text{komutativní zákon}) \\
& = & x \vee (y' \vee z) & (\text{asociativní zákon})
\end{array}$$

2. Předpokládejme, že platí $x \sqsubseteq y \Rightarrow z$, čili $x \wedge (y' \vee z) = x$. Chceme dokázat platnost $x \wedge y \sqsubseteq z$, čili $(x \wedge y) \vee z = z$. Budeme upravovat výraz $(x \wedge y) \vee z$ a využívat při tom zákonů Booleovy algebry:

$$\begin{array}{rcll}
(x \wedge y) \vee z & = & ((x \wedge (y' \vee z)) \wedge y) \vee z & (\text{platnost } x \wedge (y' \vee z) = x) \\
& = & (x \wedge ((y' \vee z) \wedge y)) \vee z & (\text{asociativní zákon}) \\
& = & (x \wedge ((y' \wedge y) \vee (z \wedge y)) \vee z & (\text{distributivní zákon}) \\
& = & (x \wedge (\bot \vee (z \wedge y)) \vee z & (\text{vlastnost doplňku}) \\
& = & (x \wedge (z \wedge y)) \vee z & (\text{vlastnost nejmenšího prvku}) \\
& = & (x \wedge (y \wedge z)) \vee z & (\text{komutativní zákon}) \\
& = & ((x \wedge y) \wedge z) \vee z & (\text{asociativní zákon}) \\
& = & ((x \wedge y) \vee z) \wedge (z \vee z) & (\text{distributivní zákon}) \\
& = & ((x \wedge y) \vee z) \wedge z & (\text{idempotence}) \\
& = & z & (\text{absorpce})
\end{array}$$

■

6.3 Jednoduché rovnicové specifikace

6.3.1 Příklad Napište rovnicovou specifikaci komutativních pologrup. Jednotlivé části specifikace krátce okomentujte.

Řešení. Naše specifikace bude jednosortová (komutativní pologrupa je totiž množina s jednou asociativní a komutativní binární operací).

Specifikace tedy může vypadat následovně:

```
1 spec KOM_POLOGRUPA is
2   sorts: elt
3   operations: _*_ : elt,elt --> elt
4   variables: x,y, z: elt
5   equations: (x*y)*z=x*(y*z)
6              x*y=y*x
7 endspec
```

Komentář:

1. Řádky `1` a `7` jsou otevírací a zavírací příkazy specifikace.
2. Na řádku `2` specifikujeme jedinou sortu: sorta `elt` representuje prvky naší komutativní pologrupy.
3. Na řádku `3` specifikujeme `_*_` jako binární operaci, psanou infixně.
4. Na řádku `4` deklarujeme proměnné: `x`, `y` a `z`.

5. Na řádku 5 specifikujeme asociativní zákon a na řádku 6 specifikujeme komutativní zákon.

■

6.3.2 Příklad Dejte příklad *confusion* modelu specifikace

```
1 spec POLOGRUPA is
2   sorts: elt
3   operations: _*_ : elt,elt --> elt
4   variables: x,y, z: elt
5   equations: (x*y)*z=x*(y*z)
6 endspec
```

Komentář. Confusion model je takový model dané specifikace, ve kterém jsou splněny některé rovnice, které nejsou specifikací vynuceny.

Řešení. Struktura $\langle \mathbb{N}, + \rangle$ je modelem specifikace `POLOGRUPA`, protože sčítání přirozených čísel splňuje asociativní zákon. V $\langle \mathbb{N}, + \rangle$ ovšem platí i rovnice $x + y = y + x$ pro všechna x, y z množiny $\mathbb{N}$. Komutativní zákon ovšem obecně asociativním zákonem vynucen není. ■

6.3.3 Příklad Dejte příklad *junk* modelu specifikace

```
1 spec POINTED is
2   sorts: elt
3   operations: p : --> elt
4 endspec
```

Komentář. Junk model je takový model dané specifikace, ve kterém se vyskytují některé prvky, které nejsou specifikací vynuceny.

Řešení. Struktura $\langle \mathbb{N}, 0 \rangle$ je modelem specifikace `POINTED`, kde nulární operace `p` je interpretována jako číslo 0. Protože množina $\mathbb{N}$ obsahuje i jiné prvky (například číslo 12), jde o junk model. ■

6.3.4 Příklad Specifikujte konstrukci `if _ then _ else _ fi` nějakého imperativního programovacího jazyka jako vícesortovou operaci a dejte příklad jedné rovnice, kterou by tato operace měla splňovat. Každou deklarovanou sortu, operaci a rovnici krátce okomentujte.

Řešení. Hledaná specifikace bude vícesortová: do operace `if _ then _ else _ fi` totiž jako první operand vstupuje Booleovský výraz a další dva operandy jsou příkazy.

Specifikace tedy může vypadat následovně:

```
1 spec IF is
2   sorts: bexp, comm
3   operations: if _ then _ else _ fi : bexp,comm,comm --> comm
4   variables: e: bexp, c: comm
5   equations: if e then c else c fi = c
6 endspec
```

Komentář:

1. Řádky 1 a 6 jsou otevírací a zavírací příkazy specifikace.
2. Na řádku 2 specifikujeme dvě sorty: sorta `bexp` jsou Booleovské výrazy a sorta `comm` jsou příkazy.
3. Na řádku 3 specifikujeme `if _ then _ else _ fi` jako operaci, která má vstupní argumenty po řadě sort `bexp`, `comm`, `comm` a výstupní sortu `comm`.

4. Na řádku `4` deklarujeme proměnné: `e` sorty `bexp` a `c` sorty `comm`.

5. Konečně na řádku `5` specifikujeme rovnici, která říká, že pokud napíšeme stejný (ale libovolný) příkaz do obou větví, pak je to totéž jako napsat pouze tento příkaz, a to nezávisle na testovaném (libovolném) Booleovském výrazu.

Komentář. Je pochopitelně možné napsat celou řadu jiných specifikací, které vyhovují zadání. Jiná možnost je například

```
1 spec IF2 is
2   sorts: bexp, comm
3   operations: if _ then _ else _ fi : bexp,comm,comm --> comm
4               true: --> bexp
6               not _ : bexp --> bexp
7   variables: e: bexp, c1, c2: comm
8   equations: if not e then c1 else c2 fi = if e then c2 else c1 fi
9 endspec
```

Specifikace `IF2` je ovšem složitější než specifikace `IF` a obhajoba specifikace `IF2` bude jistě složitější než obhajoba specifikace `IF`.

■