Algebra (studijní opora)

Martin Kuřil

Obsah

1 Úvod

Jednotlivé kapitoly (části) této studijní opory jsou zpracovány dvojím či vlastně trojím způsobem. V některé kapitole je probíraná látka v textu přímo vyložena a výklad je doplněn několika cvičeními. Jindy je čtenáři (studentovi) po krátkém úvodu do problematiky uloženo, kde a co přesně má nastudovat. Někdy dokonce tento úvod do problematiky chybí a čtenáři je přímo

uloženo samostudium, avšak takto postupuji pouze v tom případě, kdy čtenáře odkazuji na svůj studijní text [3]. Někdy následují další doporučení, například co dalšího by bylo dobré si přečíst. Ve většině případů je uloženo studium z textu [3]:

Martin Kuřil: *Základy algebry.*
`https://kma.ujep.cz/administrace/uploads/85ac80c.pdf`

Jde o studijní text, který je zatím ve fázi přípravy, avšak některé kapitoly jsou již hotové, například je hotová celá část věnovaná grupám (pochopitelně, i hotové části ještě mohou být změněny – hlavně budou opravovány případné chyby). Text je vhodný pro samostudium a jako studijní opora (nejen) pro studenty distanční a kombinované formy studia. Výklad je veden ve volném tempu a je provázen mnoha příklady. Důkazy tvrzení a vět jsou až nezvykle podrobné. Výhodou také jistě je, že studijní text je volně dostupný na internetu, a to na mé stránce na stránkách Katedry matematiky Přírodovědecké fakulty UJEP.

Ve třech případech je čtenáři uloženo studium z vysokoškolské učebnice [1]:

Jaroslav Blažek, Milan Koman, Blanka Vojtášková: *Algebra a teoretická aritmetika, II. díl.* Státní pedagogické nakladatelství, Praha, 1985.

Jde sice o knihu starší, avšak stále (jak se domnívám) dobře dostupnou – například Vědecká knihovna UJEP má ve svém fondu celkem 11 exemplářů této učebnice (stav ke dni 30.10.2020). Kniha byla v roce 1985 vydána jako celostátní vysokoškolská učebnice pro studenty matematicko-fyzikálních, přírodovědeckých a pedagogických fakult studijního oboru Učitelství všeobecně vzdělávacích předmětů aprobačního předmětu matematika.

Ve dvou případech je čtenáři uloženo studium z knihy (skript) [5]:

David Stanovský: *Základy algebry.* **matfyz**press, Praha, 2010.

Je to moderní text, který byl sepsán jako učební pomůcka k úvodnímu kursu obecné algebry na MFF UK. Skripta obsahují mnoho příkladů (nikoli cvičení) a aplikací mimo abstraktní algebru.

V jednom případě je čtenáři uloženo studium z textu [2]:

Martin Kuřil: *Lineární algebra.* Studijní text.
`https://kma.ujep.cz/administrace/uploads/144f052.pdf`

Jedná se o přepis poznámek, na jejichž základě jsem několikrát přednášel lineární algebru na UJEP. Látku probíranou v tomto studijním textu lze samozřejmě najít v mnoha učebnicích a knihách věnovaných lineární algebře. Výhodou samozřejmě je, že tento studijní text je volně dostupný na internetu na mé stránce na stránkách Katedry matematiky Přírodovědecké fakulty UJEP.

Je jasné, že budete také potřebovat úlohy k procvičení probírané látky. Zde v této studijní opoře najdete řadu cvičení, a to především v těch kapitolách, ve kterých je látka přímo vyložena.

Před chvíli jsem uvedl, že bude uloženo samostudium ze čtyř výše uvedených textů. Z nich se úlohy k procvičení vyskytují pouze v učebnici [1]. Kde vzít další cvičení (úlohy)? Jistě vám úlohy dá přímo váš vyučující nebo vám doporučí konkrétní (doufejme, že dobře dostupné) zdroje úloh. Já vám rozhodně doporučuji sbírku [4]:

David Stanovský: *Příklady z algebry.* Pracovní verze sbírky příkladů k základní přednášce z obecné algebry.
`https://www2.karlin.mff.cuni.cz/~stanovsk/vyuka/sbirka.pdf`

Ve sbírce najdete celkem 741 úloh. K některým jsou na konci uvedeny návody, k mnohým jsou uvedena řešení. Sbírka je volně dostupná na internetu na stránkách jejího autora.

Existují také další dobré a rozsáhlé sbírky úloh z algebry, například

A. K. Faddejev, J. S. Sominskij: *Zbierka úloh z vyššej algebry.* ALFA, Bratislava 1968.

Jde o slovenský překlad z ruského originálu. Sbírka obsahuje 1184 cvičení a také návody a výsledky k většině uvedených příkladů. Bohužel se však k této sbírce pravděpodobně dostanete jen s velkými obtížemi, například ve fondu Vědecké knihovny UJEP se nachází pouze jediný výtisk.

Někteří z vás možná rádi čtou anglicky psanou literaturu. Těm mohu doporučit následující text – jednak je dobrý, jednak se k němu snadno dostanete:

Frederick M. Goodman: *Algebra: abstract and concrete.* Edition 2.6. SemiSimple Press, Iowa City, IA, 2015.
`https://homepage.divms.uiowa.edu/~goodman/algebrabook.dir/book.2.6.pdf`

Text poskytuje důkladný úvod do abstraktní algebry. Kniha se věnuje tématům grupy, okruhy, tělesa. Kniha obsahuje spoustu cvičení. První a druhé vydání textu bylo publikováno nakladatelstvím Prentice-Hall. Současná verze je volně dostupná na internetu na stránkách autora knihy.

Prosím čtenáře, aby vzal v úvahu, že toto je první verze studijní opory – v budoucnu bude ještě opravována, upravována, vylepšována.

Jednotlivé číselné obory budeme značit následovně:

- $\mathbb{N}$ – množina všech přirozených čísel, $\mathbb{N} = \{0, 1, 2, 3, \dots\}$
- $\mathbb{Z}$ – množina všech celých čísel, $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$
- $\mathbb{Q}$ – množina všech racionálních čísel, $\mathbb{Q} = \{\frac{a}{b} |\ a, b \in \mathbb{Z}, b \neq 0\}$
- $\mathbb{R}$ – množina všech reálných čísel
- $\mathbb{C}$ – množina všech komplexních čísel, $\mathbb{C} = \{a + bi |\ a, b \in \mathbb{R}\}$

Připomeňme: Pro množiny A, B zápis $A \subseteq B$ znamená, že množina A je podmnožinou množiny B (tedy: pro každý prvek $x \in A$ platí, že $x \in B$). Zápis $A \subset B$ znamená, že $A \subseteq B$ a současně $A \neq B$.

Platí:

$$\emptyset \subset \mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

Také budeme používat následující značení:

- $\mathbb{Z}^+$ – množina všech kladných celých čísel, $\mathbb{Z}^+ = \{x \in \mathbb{Z} |\ x > 0\}$
- $\mathbb{Z}^-$ – množina všech záporných celých čísel, $\mathbb{Z}^- = \{x \in \mathbb{Z} |\ x < 0\}$
- $\mathbb{Q}^+$ – množina všech kladných racionálních čísel, $\mathbb{Q}^+ = \{x \in \mathbb{Q} |\ x > 0\}$
- $\mathbb{Q}^-$ – množina všech záporných racionálních čísel, $\mathbb{Q}^- = \{x \in \mathbb{Q} |\ x < 0\}$
- $\mathbb{R}^+$ – množina všech kladných reálných čísel, $\mathbb{R}^+ = \{x \in \mathbb{R} |\ x > 0\}$
- $\mathbb{R}^-$ – množina všech záporných reálných čísel, $\mathbb{R}^- = \{x \in \mathbb{R} |\ x < 0\}$

2 Základní pojmy teorie grup

Na počátku oddílu, věnovaného grupám, bych rád zmínil knihu, do které by mohli nahlédnout případní zájemci o hlubší studium teorie grup. Zmiňuji se o ní mimo jiné proto, že kniha je psaná česky a je volně dostupná na internetu. Jedná se o starší knihu vynikajícího českého matematika:

Otakar Borůvka: *Základy teorie grupoidů a grup*. Nakladatelství Československé akademie věd, Praha, 1962.
`https://dml.cz/handle/10338.dmlcz/401378`

2.1 Definice grupy

Úkol. Prostudujte kapitolu 1.1 Definice grupy v [3].

2.2 Mocniny

Úkol. Prostudujte kapitolu 1.2 Mocniny v [3].

2.3 Homomorfismy

Úkol. Prostudujte kapitolu 1.3 Homomorfismy v [3].

2.4 Podgrupy

Úkol. Prostudujte kapitolu 1.4 Podgrupy v [3].

2.5 Součiny grup

Úkol. Prostudujte kapitolu 1.5 Součiny grup v [3].

3 Příklady grup

3.1 Aditivní grupa okruhu

Úkol. Prostudujte kapitolu 2.1 Aditivní grupa okruhu v [3].

3.2 Grupa jednotek okruhu

Úkol. Prostudujte kapitolu 2.2 Grupa jednotek okruhu v [3].

3.3 Symetrická grupa

Úkol. Prostudujte kapitolu 2.3 Symetrická grupa v [3].

3.4 Alternující grupa

Úkol. Prostudujte kapitolu 2.4 Alternující grupa v [3].

3.5 Obecná lineární grupa

Úkol. Prostudujte kapitolu 2.5 Obecná lineární grupa v [3].

3.6 Grupa symetrií obrazce

Úkol. Prostudujte kapitolu 2.6 Grupa symetrií obrazce v [3].

3.7 Kvaterniony

Úkol. Prostudujte kapitolu 2.7 Kvaterniony v [3].

4 Lagrangeova věta a její důsledky

4.1 Lagrangeova věta

Úkol. Prostudujte kapitolu 3.1 Lagrangeova věta v [3].

4.2 Věty Fermatova a Eulerova

Úkol. Prostudujte kapitolu 3.2 Věty Fermatova a Eulerova v [3].

5 Cyklické grupy

5.1 Popis všech cyklických grup

Úkol. Prostudujte kapitolu 4.1 Popis všech cyklických grup v [3].

5.2 Podgrupy cyklických grup

Úkol. Prostudujte kapitolu 4.2 Podgrupy cyklických grup v [3].

6 Základní pojmy teorie okruhů

6.1 Definice okruhu

Úkol. Prostudujte kapitolu 8.1 Definice okruhu v [3].

6.2 Homomorfismy

Úkol. Prostudujte kapitolu 8.2 Homomorfismy v [3].

6.3 Podokruhy a ideály

Úkol. Prostudujte kapitolu 8.3 Podokruhy a ideály v [3].

7 Příklady okruhů

7.1 Okruh kvadratických celých čísel

Úkol. Prostudujte kapitolu 9.1 Okruh kvadratických celých čísel v [3].

7.2 Okruh zbytkových tříd

Pod názvem "okruh zbytkových tříd"se skrývají okruhy $\mathbb{Z}_m$, s nimiž jste se již setkali v části 3.1 Aditivní grupa okruhu. Jak již víte (právě z části 3.1), okruhy $\mathbb{Z}_m$ těsně souvisí s kongruencemi modulo m v oboru integrity $\mathbb{Z}$. V části 8.5 Počítání modulo pak zařadíte okruhy zbytkových tříd do širšího rámce – v části 8.5 budete zkoumat počítání modulo v libovolném oboru integrity.

Úkol. Prostudujte část 1.2 Operace na množině ve studijním textu [2]. Zopakujete si základní fakta o kongruencích v $\mathbb{Z}$ a také o okruzích $\mathbb{Z}_m$, a to včetně důkazů. Alternativně můžete studovat paragraf 2 Kongruence v $\mathbb{Z}$ v kapitole XIV Dělitelnost ve speciálních strukturách a její užití v knize [1] – najdete tam mnohem více informací.

7.3 Maticový okruh

Matice jsou základním matematickým objektem. Znáte je dobře z Lineární algebry. Pokud si chcete matice zopakovat, podívejte se například do studijního textu [2] a projděte si v něm kapitolu 5 Matice (nad tělesem).

Omezíme se zde (stejně jako v textu [2]) pouze na matice nad tělesem. Nechť m, n jsou kladná celá čísla. Množinu všech matic typu (m, n) nad tělesem T značíme $T_{m,n}$ (v souladu s [2]). Symbolem O značíme nulovou matici, tj. matici, která má všechny prvky rovny 0 (kde 0 je neutrální prvek operace sčítání v tělese T).

Dobře víte, že matice téhož typu je možno sčítat (a jistě také víte jak). Je snadné ukázat (udělejte si to jako cvičení!), že množina $T_{m,n}$ spolu s operací sčítání matic je komutativní grupa s neutrálním prvkem O.

Nechť m, n, p jsou kladná celá čísla. Připomeňme si, že pro všechna $A \in T_{m,p}$ a $B \in T_{p,n}$ lze vypočítat součin $A \cdot B$; přitom bude $AB \in T_{m,n}$.

Pro libovolné dvě čtvercové matice stupně n nad tělesem T lze tedy určit jejich součet i součin. Takže sčítání matic a násobení matic jsou binární operace na množině $T_{n,n}$. Již jsme hovořili o tom, že množina $T_{n,n}$ spolu s operací sčítání matic je komutativní grupa. Pro všechna $A, B, C \in T_{n,n}$ je $A(B + C) = AB + AC$ a také $(B + C)A = BA + CA$ (pokuste se to dokázat jako cvičení; v případě nutnosti, když se důkaz nevydaří, se podívejte do [2] na větu 5.2.5.). Můžeme tedy konstatovat, že $T_{n,n}$ spolu s operacemi sčítání a násobení matic je okruh. Tento okruh budeme značit $M_n(T)$.

Navíc, operace násobení čtvercových matic stupně n nad tělesem T je asociativní (zopakujte si důkaz!) a má neutrální prvek E, kde E je jednotková matice splňující $e_{ii} = 1$ (neutrální prvek operace $\cdot$ v tělese T) pro všechna $i \in \{1, \ldots, n\}$ a $e_{ij} = 0$ (neutrální prvek operace $+$ v tělese T) pro všechna $i, j \in \{1, \ldots, n\}$, $i \neq j$. Můžeme tedy říci, že

$$M_n(T) \text{ je asociativní okruh s jednotkovým prvkem}$$

Jaké kvality má okruh $M_n(T)$? Pro $n = 1$ máme $M_1(T) \cong T$ (viz cvičení).

Nechť n je celé číslo, $n > 1$. Definujme matice $A, B \in T_{n,n}$ takto:

$$a_{ij} = \begin{cases} 1 & \text{pokud } i = 1 \wedge j = 1 \\ 0 & \text{pokud } i \neq 1 \vee j \neq 1 \end{cases}$$

$$b_{ij} = \begin{cases} 1 & \text{pokud } i = n \wedge j = 1 \\ 0 & \text{pokud } i \neq n \vee j \neq 1 \end{cases}$$

Pak máme

$$A \neq O,\ B \neq O,\ AB = O,\ BA = B,\ AB \neq BA$$

Vidíme, že pro $n > 1$ okruh $M_n(T)$ není obor integrity a není komutativní, a to bez ohledu na těleso T.

Cvičení.

1. Nechť T je těleso, m, n jsou kladná celá čísla. Dokažte, že množina $T_{m,n}$ spolu s operací sčítání matic je komutativní grupa s neutrálním prvkem O.
2. Nechť n je kladné celé číslo, T je těleso. Dokažte, že pro všechna $A, B, C \in T_{n,n}$ platí:

$$A(B + C) = AB + AC,\ (B + C)A = BA + CA$$

3. Nechť n je kladné celé číslo, T je těleso. Dokažte, že pro všechna $A, B, C \in T_{n,n}$ platí:

$$A(BC) = (AB)C$$

4. Nechť T je těleso. Dokažte, že $M_1(T) \cong T$ (tj. okruh $M_1(T)$ je isomorfní s tělesem T).
5. Určete počet prvků okruhu $M_2(\mathbb{Z}_2)$. Sestrojte tabulky operací + a $\cdot$ v okruhu $M_2(\mathbb{Z}_2)$.

7.4 Okruh polynomů

Jistě jste již pracovali s polynomy a máte o nich tudíž nějakou představu. Zde se především naučíte, jak lze formálně přesně vybudovat pojem polynomu s koeficienty z libovolného předem daného oboru integrity.

Úkol. Prostudujte paragraf 1 Úvodní poznámky a paragraf 2 Algebraická definice polynomů v kapitole XI Polynomy v učebnici [1]. Najdete tam také několik cvičení.

Cvičení. Hodně cvičení týkajících se polynomů najdete v [4] na stranách 9 – 12. Upozorňuji však, že ne všechny tam uvedené příklady jsou určeny k procvičení látky, se kterou se seznámíte v této části (například některá cvičení jsou o kořenech polynomů, jimž je věnována až poslední část tohoto studijního textu).

8 Základní pojmy teorie dělitelnosti

Jistě jste se již setkali s dělitelností v celých číslech. Například s výroky "3 dělí 12", "3 nedělí 10", "3 je největší společný dělitel čísel 12 a 15", "11 je prvočíslo", "12 je číslo složené", atd.

Budeme se teď věnovat studiu dělitelnosti v obecnější situaci, a to v oborech integrity. Připomínám, že obor integrity je asociativní a komutativní okruh, v němž pro každé dva prvky x, y platí

$$x \cdot y = 0 \Longrightarrow x = 0 \vee y = 0$$

8.1 Relace dělitelnosti

8.1.1. Definice. Nechť I je obor integrity, $a, b \in I$. Říkáme, že a **dělí** b (b **je násobkem** a, b **je dělitelné** a), pokud existuje $c \in I$, $b = ac$. Fakt, že a dělí b, zapisujeme $a|b$.

V následujících dvou tvrzeních jsou uvedeny základní vlastnosti relace $|$, které budeme v dalším zcela běžně používat.

Připomínám, že kvaziuspořádání množiny A je relace na A, která je reflexivní a tranzitivní.

8.1.2. Tvrzení. *Nechť I je obor integrity s jednotkovým prvkem. Pak relace $|$ je kvaziuspořádání množiny I.*

Důkaz.

1. Relace $|$ je reflexivní: Nechť $a \in I$. Chceme: $a|a$. Stačí si uvědomit, že $a = a \cdot 1$.
2. Relace $|$ je tranzitivní: Nechť $a, b, c \in I$, $a|b$, $b|c$. Chceme: $a|c$. Protože $a|b$, existuje $u \in I$, $b = au$. Protože $b|c$, existuje $v \in I$, $c = bv$. Pak $c = bv = (au)v = a(uv)$ a tedy $a|c$.

Povšimněte si, že existenci jednotkového prvku v oboru integrity I jsme potřebovali pouze k důkazu reflexivity relace $|$, nikoli k důkazu tranzitivity.

8.1.3. Tvrzení. *Nechť I je obor integrity, $a, b, c \in I$. Platí:*

1. *Jestliže $c \neq 0$, pak $a|b$ právě tehdy, když $ca|cb$.*
2. *Jestliže $c|a$ a $c|b$, pak $c|ua + vb$ pro všechna $u, v \in I$.*

Důkaz.

1. Nechť $c \neq 0$. Předpokládejme, že $a|b$. Ukážeme, že $ca|cb$. Je $b = ad$ pro nějaké $d \in I$. Pak $cb = c(ad) = (ca)d$, $cb = (ca)d$ a tedy $ca|cb$. Nyní naopak. Předpokládejme, že $ca|cb$. Ukážeme, že $a|b$. Je $cb = (ca)e$ pro nějaké $e \in I$. Pak $cb = (ca)e = c(ae)$, $cb = c(ae)$. Je $c \neq 0$ a v oboru integrity lze krátit nenulovým prvkem. Dostáváme tedy $b = ae$, $a|b$.

2. Důkaz proveďte jako cvičení.

Relace $|$ nemusí být antisymetrická – může se stát, že $a|b$ a $b|a$ a přitom $a \neq b$. Například v $\mathbb{Z}$ máme $5|-5$ (jelikož $-5 = 5 \cdot (-1)$) a $-5|5$ (jelikož $5 = (-5) \cdot (-1)$) a přitom samozřejmě $5 \neq -5$.

8.1.4. Definice. Nechť I je obor integrity, $a, b \in I$. Říkáme, že prvek a **je asociován** s prvkem b, pokud $a|b$ a současně $b|a$. Fakt, že prvek a je asociován s prvkem b, zapisujeme $a \| b$.

8.1.5. Tvrzení. *Nechť I je obor integrity s jednotkovým prvkem. Pak relace $\|$ je ekvivalence na množině I.*

Důkaz. Cvičení.

8.1.6. Tvrzení. *Nechť I je obor integrity. Nechť $a, b, c, d \in I$, $a \| c$, $b \| d$. Platí: $a|b$ právě tehdy, když $c|d$.*

Důkaz.

1. Nechť $a|b$. Chceme: $c|d$. Protože $a \| c$, máme $c|a$. Protože $b \| d$, máme $b|d$. Celkem tedy $c|a$, $a|b$, $b|d$. Relace $|$ je tranzitivní, takže $c|d$.

2. Nechť $c|d$. Chceme: $a|b$. Protože $a \| c$, máme $a|c$. Protože $b \| d$, máme $d|b$. Celkem tedy $a|c$, $c|d$, $d|b$. Relace $|$ je tranzitivní, takže $a|b$.

Tvrzení 8.1.6. nám sděluje, že přechod k asociovaným prvkům nemá vliv na vztah dělitelnosti. Pokud $a \| c$ a $b \| d$, pak je otázka "Je prvek b násobkem prvku a?"ekvivalentní otázce "Je prvek d násobkem prvku c?"– dostaneme stejné odpovědi.

V části 3.2 jste se seznámili s pojmem jednotka okruhu. Nechť R je asociativní okruh s jednotkovým prvkem 1. Pak prvek $x \in R$ se nazývá jednotka okruhu R, pokud existuje prvek $y \in R$ takový, že $xy = 1$ a $yx = 1$. Množinu všech jednotek okruhu R značíme $U(R)$. Také již víte, že $U(R)$ spolu s operací násobení je grupa. Nepleťte pojmy jednotka a jednotkový prvek! Jednotkový prvek je vždy jednotka (protože $1 \cdot 1 = 1$), avšak jednotka nemusí být jednotkovým prvkem – například -1 je jednotka v $\mathbb{Z}$ (protože $(-1) \cdot (-1) = 1$) a přitom $-1 \neq 1$.

8.1.7. Tvrzení. *Nechť I je obor integrity s jednotkovým prvkem. Nechť $a, b \in I$. Následující tvrzení jsou ekvivalentní:*

1. $a \| b$

2. $b = aj$ pro nějaké $j \in U(I)$

3. $a = bk$ *pro nějaké* $k \in U(I)$

Důkaz.
Z 1 plyne 2:
Nechť $a \| b$. Pak $a|b$, takže $b = aj$ pro nějaké $j \in I$. Také $b|a$, takže $a = bk$ pro nějaké $k \in I$. Pak $b = aj = (bk)j = b(kj)$, $b = b(kj)$, $b \cdot 1 = b \cdot (kj)$. Pokud $b \neq 0$, můžeme krátit prvkem b (jsme totiž v oboru integrity) a dostaneme $1 = kj$, což dává $j \in U(I)$; připomeňme teď, že $b = aj$. Pokud $b = 0$, je $a = bk = 0 \cdot k = 0$, $a = 0$, takže $b = a$, $b = a \cdot 1$ a stačí si uvědomit, že $1 \in U(I)$.
Z 2 plyne 3:
Nechť $b = aj$, kde $j \in U(I)$. Protože $j \in U(I)$, existuje $k \in I$, $jk = 1$. Pak $bk = (aj)k = a(jk) = a \cdot 1 = a$, $a = bk$; uvědomme si, že $k \in U(I)$.
Z 3 plyne 1:
Nechť $a = bk$, kde $k \in U(I)$. Pak $b|a$. Protože $k \in U(I)$, existuje $j \in I$, $kj = 1$. Pak $aj = (bk)j = b(kj) = b \cdot 1 = b$, $b = aj$, $a|b$. Celkem máme $a|b$ a $b|a$, takže $a \| b$.

Cvičení.

1. Dokažte druhou část Tvrzení 8.1.3.
2. Dokažte Tvrzení 8.1.5.
3. Rozhodněte, zda $5|12$ v $\mathbb{Z}$. Rozhodnutí zdůvodněte.
4. Rozhodněte, zda $5|12$ v $\mathbb{Q}$. Rozhodnutí zdůvodněte.
5. Najděte všechny jednotky v $\mathbb{Z}$.
6. Najděte všechny jednotky v $\mathbb{Z}[i]$.
7. Najděte všechny prvky asociované s prvkem 9 v $\mathbb{Z}$.
8. Najděte všechny prvky asociované s prvkem $17 + 9i$ v $\mathbb{Z}[i]$.
9. Nechť I je obor integrity s jednotkovým prvkem, v němž $1 + 1 \neq 0$. Dokažte, že relace $|$ není antisymetrická.
10. Nechť f, g jsou nenulové polynomy nad oborem integrity I. Jestliže $f|g$, pak $deg(f) \leq deg(g)$. Dokažte.
11. Nechť f, g jsou nenulové polynomy nad oborem integrity I. Jestliže $f \| g$, pak $deg(f) = deg(g)$. Dokažte.

8.2 Největší společný dělitel

Chceme teď vymezit, co to znamená, že prvek d je největším společným dělitelem prvků a a b. Pojmenování prvku d, totiž "největší společný dělitel prvků a a b", nám hodně napovídá. Předně je to společný dělitel prvků a a b, což má samozřejmě ten význam, že $d|a$ a současně $d|b$. No a dále d má být ze všech společných dělitelů prvků a a b ten největší. Označíme-li S množinu všech společných dělitelů prvků a a b, má být prvek d největším prvkem množiny S, tj. má být $d = \max S$. Zde máme problém, protože na množině I (pohybujeme se v oboru integrity I) nemusí být předem dáno žádné uspořádání. Tak nějaké uspořádání na I definujeme. Ale jaké? Jestliže má být definice největšího společného dělitele obecná, nemůže využívat speciální vlastnost konkrétního oboru integrity (takovou, kterou jeden obor integrity má a jiný zase nemá). Napadne vás třeba vzít diagonální relaci Δ_I na množině I (relace Δ_A je uspořádání na množině A, a to pro každou množinu A). Pak ovšem $\max S$ nebude existovat, kdykoli S bude mít více než jeden prvek. Vzpomeňte si však, že v každém oboru integrity s jednotkovým prvkem máme k dispozici kvaziuspořádání $|$. Budeme tedy největší společný dělitel prvků a a b definovat jako "největší"prvek množiny S vzhledem ke kvaziuspořádání $|$, tj. prvek d je největší společný dělitel prvků a a b, pokud $d \in S$ a pro každé $x \in S$ platí $x|d$. Výsledkem našich úvah je následující definice.

8.2.1. Definice. Nechť I je obor integrity, $a, b, d \in I$. Prvek d se nazývá **největší společný dělitel** prvků a a b, pokud platí:

1. $d|a$ a $d|b$
2. Jestliže $s \in I$, $s|a$ a $s|b$, pak $s|d$.

Největší společný dělitel prvků a a b budeme značit $NSD(a, b)$. Používá se také jiné značení, například $GCD(a, b)$ (greatest common divisor).

Jestliže $(A, \leq)$ je uspořádaná množina a $S \subseteq A$, pak S má nejvýše jeden největší prvek. Zdůvodnění je jednoduché. Nechť d, e jsou největší prvky množiny S. Pak $d, e \in S$. Protože d je největší prvek množiny S, máme $e \leq d$. Protože e je největší prvek množiny S, máme $d \leq e$. Celkem tedy $e \leq d$ a $d \leq e$. Protože relace uspořádání je antisymetrická, dostáváme $d = e$.

Relace $|$ nemusí být antisymetrická a nelze tedy očekávat, že pro každé dva prvky existuje nejvýše jeden největší společný dělitel. Vskutku, například v oboru integrity $\mathbb{Z}$ je $1 = NSD(0, 1)$ a také $-1 = NSD(0, 1)$ (zdůvodněte!). Platí aspoň následující tvrzení.

8.2.2. Tvrzení. *Nechť I je obor integrity, $a, b, d, e \in I$. Jestliže d je největší společný dělitel prvků a a b a také e je největší společný dělitel prvků a a b, pak $d \| e$.*

Důkaz. Protože $d = NSD(a, b)$, platí:
(I) $d|a$ a $d|b$
(II) Jestliže $s \in I$, $s|a$ a $s|b$, pak $s|d$.

Protože $e = NSD(a, b)$, platí
(III) $e|a$ a $e|b$
(IV) Jestliže $s \in I$, $s|a$ a $s|b$, pak $s|e$.
Z (I) a (IV) plyne, že $d|e$. Z (III) a (II) plyne, že $e|d$. Celkem tedy $d|e$, $e|d$, $d\|e$.

8.2.3. Tvrzení. *Nechť I je obor integrity, $a, b, d, a', b', d' \in I$. Nechť $a\|a'$, $b\|b'$, $d\|d'$. Jestliže $d = NSD(a, b)$, pak $d' = NSD(a', b')$.*

Důkaz. Cvičení.

V některých oborech integrity lze zaručit, že pro každé dva prvky existuje jejich největší společný dělitel. Je tomu tak například v eukleidovských oborech a gaussovských oborech (seznámíte se s nimi v další fázi studia tohoto předmětu). V eukleidovských oborech lze dokonce největší společný dělitel dvou prvků vypočítat Eukleidovým algoritmem, který je jednoduchý a efektivní. A jak uvidíte, mezi eukleidovské obory patří $\mathbb{Z}$, $\mathbb{Z}[i]$ (gaussova celá čísla), $T[x]$ (polynomy nad tělesem T).

V některých oborech integrity však existují dvojice prvků, pro které neexistuje jejich největší společný dělitel. Je tomu tak například v oboru integrity $\mathbb{Z}[\sqrt{-5}]$. Tento obor integrity patří mezi okruhy kavadratických celých čísel, o kterých si můžete více přečíst v [3], a to v části 9.1. Nám postačí vědět, že $\mathbb{Z}[\sqrt{-5}]$ je podokruh tělesa $\mathbb{C}$ a dále

$$\mathbb{Z}[\sqrt{-5}] = \{a + b \cdot \sqrt{-5} |\ a, b \in \mathbb{Z}\}$$

přičemž vyjádření prvků okruhu $\mathbb{Z}[\sqrt{-5}]$ ve tvaru $a + b \cdot \sqrt{-5}$, kde a, b jsou celá čísla, je jednoznačné (viz [3], 8.3.12., 8.3.24.).

8.2.4. Příklad. Ukážeme, že v $\mathbb{Z}[\sqrt{-5}]$ neexistuje největší společný dělitel prvků 9 a $6+3\sqrt{-5}$. Využijeme přitom zobrazení $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}_0$ definované následovně: pro celá čísla a, b je

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

Zobrazení N má důležitou vlastnost: pro všechna $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ je

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

O tom se můžete snadno přesvědčit přímým výpočtem, případně se můžete podívat na příklad 8.3.24. v [3].

Nechť $\alpha \in \mathbb{Z}[\sqrt{-5}]$. Jestliže $N(\alpha) = 1$, pak $\alpha \in \{1, -1\}$. Zdůvodnění: Nechť $\alpha = a + b\sqrt{-5}$, kde a, b jsou celá čísla. Je $a^2 + 5b^2 = 1$. Protože $5b^2 \leq a^2 + 5b^2$, je $5b^2 \leq 1$, $b^2 \leq \frac{1}{5}$, $b^2 = 0$, $b = 0$. Pak $a^2 = 1$, $a \in \{1, -1\}$, $\alpha \in \{1, -1\}$.

Určíme teď všechny společné dělitele prvků 9 a $6 + 3\sqrt{-5}$.

Nechť $\alpha \in \mathbb{Z}[\sqrt{-5}]$, $\alpha|9$. Pak $9 = \alpha\beta$ pro nějaké $\beta \in \mathbb{Z}[\sqrt{-5}]$. Je $N(\alpha\beta) = N(9)$, $N(\alpha)N(\beta) = 81$. Nechť $\alpha = a + b\sqrt{-5}$, kde a, b jsou celá čísla. Protože $N(\alpha)N(\beta) = 81$ a $N(\alpha), N(\beta) \in \mathbb{N}_0$, máme pro hodnotu $N(\alpha) = a^2 + 5b^2$ pouze pět možností:

1. $N(\alpha) = 1$:
   Víme již, že $\alpha \in \{1, -1\}$.

2. $N(\alpha) = 3$:
   Je $a^2 + 5b^2 = 3$. Protože $5b^2 \leq a^2 + 5b^2$, je $5b^2 \leq 3$, $b^2 \leq \frac{3}{5}$, $b^2 = 0$, $b = 0$. Pak $a^2 = 3$. Ovšem čtverec celého čísla nikdy není roven číslu 3, takže $\alpha \in \emptyset$.

3. $N(\alpha) = 9$:
   Je $a^2 + 5b^2 = 9$. Protože $5b^2 \leq a^2 + 5b^2$, je $5b^2 \leq 9$, $b^2 \leq \frac{9}{5}$, $b^2 \in \{0, 1\}$. Pro $b^2 = 0$ máme $b = 0$, $a^2 = 9$, $a \in \{3, -3\}$, $\alpha \in \{3, -3\}$. Pro $b^2 = 1$ máme $b \in \{1, -1\}$, $a^2 = 4$, $a \in \{2, -2\}$, $\alpha \in \{2 + \sqrt{-5}, 2 - \sqrt{-5}, -2 + \sqrt{-5}, -2 - \sqrt{-5}\}$. Celkem tedy $\alpha \in \{3, -3, 2 + \sqrt{-5}, 2 - \sqrt{-5}, -2 + \sqrt{-5}, -2 - \sqrt{-5}\}$.

4. $N(\alpha) = 27$:
   Je $a^2 + 5b^2 = 27$. Protože $5b^2 \leq a^2 + 5b^2$, je $5b^2 \leq 27$, $b^2 \leq \frac{27}{5}$, $b^2 \in \{0, 1, 4\}$. Pro $b^2 = 0$ je $a^2 = 27$. Pro $b^2 = 1$ je $a^2 = 22$. Pro $b^2 = 4$ je $a^2 = 7$. Ovšem čtverec celého čísla nikdy není roven číslu 27, ani není roven číslu 22, ani není roven číslu 7. Takže $\alpha \in \emptyset$.

5. $N(\alpha) = 81$:
   Je $N(\alpha)N(\beta) = 81$, takže $N(\beta) = 1$, $\beta \in \{1, -1\}$. Připomeňme, že $\alpha\beta = 9$. Pro $\beta = 1$ máme $\alpha = 9$, pro $\beta = -1$ máme $\alpha = -9$. Celkem tedy $\alpha \in \{9, -9\}$.

Pro α máme tedy 10 kandidátů:

$$1, -1, 3, -3, 2 + \sqrt{-5}, 2 - \sqrt{-5}, -2 + \sqrt{-5}, -2 - \sqrt{-5}, 9, -9$$

.

Nyní určíme, kteří kandidáti dělí číslo 9 (v $\mathbb{Z}[\sqrt{-5}]$).
$1|9$, $-1|9$, $3|9$, $-3|9$, $2 + \sqrt{-5}|9$ (jelikož $9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$), $2 - \sqrt{-5}|9$, $-2 + \sqrt{-5}|9$ (jelikož $9 = (-2 + \sqrt{-5})(-2 - \sqrt{-5})$), $-2 - \sqrt{-5}|9$, $9|9$, $-9|9$.
Zde je seznam všech dělitelů čísla 9:

$$1, -1, 3, -3, 2 + \sqrt{-5}, 2 - \sqrt{-5}, -2 + \sqrt{-5}, -2 - \sqrt{-5}, 9, -9$$

Určíme nyní, kteří dělitelé čísla 9 také dělí prvek $6 + 3\sqrt{-5}$.
Jistě $1|6 + 3\sqrt{-5}$, $-1|6 + 3\sqrt{-5}$.
Je $6 + 3\sqrt{-5} = 3(2 + \sqrt{-5}) = (-3)(-2 - \sqrt{-5})$, takže $3|6 + 3\sqrt{-5}$, $-3|6 + 3\sqrt{-5}$, $2 + \sqrt{-5}|6 + 3\sqrt{-5}$, $-2 - \sqrt{-5}|6 + 3\sqrt{-5}$.
Předpokládejme, že $2 - \sqrt{-5}|6 + 3\sqrt{-5}$. Existují tedy celá čísla x, y taková, že $(2 - \sqrt{-5})(x + y\sqrt{-5}) = 6 + 3\sqrt{-5}$. Je $(2 - \sqrt{-5})(x + y\sqrt{-5}) = 2x + 2y\sqrt{-5} - x\sqrt{-5} + 5y = (2x + 5y) + (-x + 2y)\sqrt{-5}$, takže $2x + 5y = 6$, $-x + 2y = 3$. Z toho plyne, že $y = \frac{4}{3}$, spor (číslo y je totiž celé). Takže $2 - \sqrt{-5}$ není dělitelem čísla $6 + 3\sqrt{-5}$. Protože $2 - \sqrt{-5} \| -2 + \sqrt{-5}$, také $-2 + \sqrt{-5}$ není dělitelem čísla $6 + 3\sqrt{-5}$.

Předpokládejme, že $9|6+3\sqrt{-5}$. Pak $6+3\sqrt{-5}=9\epsilon$ pro nějaké $\epsilon \in \mathbb{Z}[\sqrt{-5}]$. Pak $N(6+3\sqrt{-5}) = N(9\epsilon) = N(9)N(\epsilon)$, $81 = 81N(\epsilon)$, $N(\epsilon) = 1$, $\epsilon \in \{1,-1\}$, $6+3\sqrt{-5} = 9$ nebo $6+3\sqrt{-5} = -9$, spor. Takže 9 není dělitelem čísla $6+3\sqrt{-5}$. Protože $-9\|9$, také -9 není dělitelem čísla $6+3\sqrt{-5}$.

Nyní můžeme konečně napsat seznam všech společných dělitelů prvků 9 a $6+3\sqrt{-5}$:

$$1, -1, 3, -3, 2+\sqrt{-5}, -2-\sqrt{-5}$$

Připomeňme, že největší společný dělitel dvojice prvků je dělitelný všemi společnými děliteli dané dvojice.

Protože 1 není násobek čísla 3 (v $\mathbb{Z}[\sqrt{-5}]$), není 1 největší společný dělitel prvků 9 a $6+3\sqrt{-5}$. Jelikož $-1\|1$, není také -1 největší společný dělitel prvků 9 a $6+3\sqrt{-5}$.

Předpokládejme, že 3 je největším společným dělitelem prvků 9 a $6+3\sqrt{-5}$. Pak $2+\sqrt{-5}|3$, $3 = (2+\sqrt{-5})\gamma$ pro nějaké $\gamma \in \mathbb{Z}[\sqrt{-5}]$. Pak $N(3) = N((2+\sqrt{-5})\gamma) = N(2+\sqrt{-5})N(\gamma)$, $N(3) = N(2+\sqrt{-5})N(\gamma)$, $9 = 9N(\gamma)$, $N(\gamma) = 1$, $\gamma \in \{1,-1\}$, $3 = 2+\sqrt{-5}$ nebo $3 = -2-\sqrt{-5}$, spor. Není tedy 3 největším společným dělitelem prvků 9 a $6+3\sqrt{-5}$. Jelikož $-3\|3$, není také -3 největší společný dělitel prvků 9 a $6+3\sqrt{-5}$.

Předpokládejme, že $2+\sqrt{-5}$ je největším společným dělitelem prvků 9 a $6+3\sqrt{-5}$. Pak $3|2+\sqrt{-5}$, $2+\sqrt{-5} = 3\delta$ pro nějaké $\delta \in \mathbb{Z}[\sqrt{-5}]$. Pak $N(2+\sqrt{-5}) = N(3\delta)$, $N(2+\sqrt{-5}) = N(3)N(\delta)$, $9 = 9N(\delta)$, $N(\delta) = 1$, $\delta \in \{1,-1\}$, $2+\sqrt{-5} = 3$ nebo $2+\sqrt{-5} = -3$, spor. Není tedy $2+\sqrt{-5}$ největším společným dělitelem prvků 9 a $6+3\sqrt{-5}$. Jelikož $-2-\sqrt{-5}\|2+\sqrt{-5}$, není také $-2-\sqrt{-5}$ největší společný dělitel prvků 9 a $6+3\sqrt{-5}$.

Ukázali jsme tedy podrobně, že v $\mathbb{Z}[\sqrt{-5}]$ neexistuje největší společný dělitel prvků 9 a $6+3\sqrt{-5}$.

Jak uvidíte později, v eukleidovských oborech a gaussovských oborech pro každé dva prvky existuje jejich největší společný dělitel. Takže $\mathbb{Z}[\sqrt{-5}]$ je příklad oboru integrity, který není eukleidovský ani gaussovský.

Na závěr této části ještě definujeme, co to znamená, že dva prvky jsou nesoudělné. Nechť I je obor integrity s jednotkovým prvkem, $a, j \in I$, j je jednotka. Pak $j|1$ a $1|a$, takže $j|a$. Vidíme, že jednotka dělí každý prvek oboru integrity I. Z toho plyne, že každé dva prvky $a, b \in I$ mají vždy nějaké společné dělitele, a to minimálně všechny jednotky oboru integrity I. Jestliže nemají již žádné další společné dělitele, pak říkáme, že prvky a, b jsou nesoudělné.

8.2.5. Definice. Nechť I je obor integrity s jednotkovým prvkem, $a, b \in I$. Říkáme, že prvky a, b jsou **nesoudělné**, pokud pro všechna $d \in I$ platí: jestliže $d|a$ a $d|b$, pak $d|1$. Fakt, že prvky a, b jsou nesoudělné, zapisujeme jako $a \perp b$.

8.2.6. Tvrzení. *Nechť I je obor integrity s jednotkovým prvkem, $a, b \in I$. Platí:*

$$a \perp b \iff NSD(a,b) = 1$$

Důkaz. Cvičení.

Cvičení.

1. Dokažte Tvrzení 8.2.3.
2. Nechť I je obor integrity s jednotkovým prvkem, $a, b, j \in I$, j je jednotka oboru integrity I (tedy $j \in U(I)$). Dokažte, že $NSD(a, 0) = a$, $NSD(a, a) = a$, $NSD(a, ab) = a$, $NSD(j, a) = 1$.
3. Dokažte Tvrzení 8.2.6.

8.3 Ireducibilní prvky

Jak víte, celá čísla větší než jedna se dělí na prvočísla a čísla složená. Přitom celé číslo p, $p > 1$, se nazývá prvočíslo, pokud pro všechna kladná celá čísla d platí: jestliže $d|p$, pak $d = 1$ nebo $d = p$.

Jaké dělitele má prvočíslo p v rámci celého oboru integrity $\mathbb{Z}$? Nechť d je celé číslo, $d|p$. Pak existuje celé číslo e takové, že $p = de$. Jistě $d \neq 0$ ($d = 0$ by dalo $p = 0$). Dostáváme $p = |p| = |de| = |d||e|$ a vidíme, že $|d|$ dělí číslo p. Ovšem $|d|$ je kladné celé číslo (protože d je nenulové celé číslo) a p je prvočíslo, což dává $|d| = 1$ nebo $|d| = p$, $d \in \{1, -1\}$ nebo $d \in \{p, -p\}$, takže $d \| 1$ nebo $d \| p$. Úvahu teď shrneme. Jestliže p je prvočíslo a d je celé číslo takové, že $d|p$, pak $d \| 1$ nebo $d \| p$.

Roli prvočísel v oborech integrity hrají ireducibilní prvky a roli složených čísel hrají prvky reducibilní. Zde je definice:

8.3.1. Definice. Nechť I je obor integrity s jednotkovým prvkem, $q \in I$, $q \neq 0$, $q \notin U(I)$. Pak q se nazývá **ireducibilní prvek** (oboru integrity I), pokud pro všechna $d \in I$ platí: jestliže $d|q$, pak $d \| 1$ nebo $d \| q$. Jestliže q není ireducibilní prvek, pak se q nazývá **reducibilní prvek** (oboru integrity I).

8.3.2. Poznámka. Odpověď na otázku, zda číslo (prvek) je ireducibilní, velmi závisí na tom, v jakém oboru integrity jsme. Například 5 je prvočíslo, takže 5 je ireducibilní prvek v $\mathbb{Z}$. Avšak 5 je reducibilní prvek v $\mathbb{Z}[i]$. Proč? Vzpomeňte si, že ve cvičení číslo 6 v části 8.1. jste našli (pokud jste správně hledali) všechny jednotky v $\mathbb{Z}[i]$: $1, -1, i, -i$. Pro číslo 5 v $\mathbb{Z}[i]$ platí: $5 \neq 0$, $5 \notin U(\mathbb{Z}[i])$, $2 + i | 5$ (jelikož $5 = (2 + i)(2 - i)$) a přitom číslo $2 + i$ není asociováno s 1 (jelikož s 1 jsou asociována čísla $1, -1, i, -i$) a také $2 + i$ není asociováno s 5 (protože s 5 jsou asociována čísla $5, -5, 5i, -5i$).

Uvedeme nyní dvě jednoduchá, avšak užitečná tvrzení (dále je budeme zcela běžně používat, již bez odkazu na tato tvrzení).

8.3.3. Tvrzení. *Nechť I je obor integrity s jednotkovým prvkem. Nechť $q, r \in I$. Jestliže prvek q je ireducibilní a $r \| q$, pak prvek r je také ireducibilní.*

Důkaz. Důkaz je snadný, udělejte jej jako cvičení.

8.3.4. Tvrzení. *Každý lineární polynom nad tělesem T je ireducibilní prvek oboru integrity $T[x]$.*

Důkaz. Určíme nejprve, jak vypadají jednotky oboru integrity $T[x]$. Nechť f je jednotka. Pak existuje $g \in T[x]$, $fg = 1$. Nutně $f \neq 0$, $g \neq 0$. Platí: $deg(fg) = deg(1)$, $deg(f) + deg(g) = 0$. Protože stupně polynomů jsou nezáporná celá čísla, $deg(f)+deg(g) = 0$ dává $deg(f) = deg(g) = 0$. Ovšem $deg(f) = 0$ znamená, že f je nenulový konstantní polynom. Ukázali jsme zatím, že každá jednotka je nenulový konstantní polynom. Naopak, každý nenulový konstantní polynom c je jednotka, protože $cc^{-1} = 1$ (zde je podstatné, že T je těleso a tedy každý nenulový prvek z T má prvek inverzní). Ukázali jsme, že jednotky v $T[x]$ jsou právě všechny nenulové konstantní polynomy. Buď nyní f lineární polynom nad tělesem T. Chceme ukázat, že f je ireducibilní prvek oboru integrity $T[x]$. Jistě $f \neq 0$, $f \notin U(T[x])$. Nechť g je polynom nad tělesem T, $g|f$. Je třeba ukázat, že $g \| 1$ nebo $g \| f$. Protože $g|f$, je $f = gh$ pro nějaký polynom h nad tělesem T. Zřejmě $g \neq 0$, $h \neq 0$. Platí: $deg(f) = deg(gh)$, $1 = deg(g) + deg(h)$. Případ $deg(g) \geq 2$ dává $deg(g) + deg(h) \geq 2$ (protože $deg(h) \geq 0$). Nutně tedy $deg(g) = 0$ nebo $deg(g) = 1$. Pokud $deg(g) = 0$, je g nenulový konstantní polynom a tedy g je jednotka oboru integrity $T[x]$, $g \| 1$. Pokud $deg(g) = 1$, je $deg(h) = 0$, h je nenulový konstantní polynom, h je jednotka, $g \| f$.

8.3.5. Příklad. Polynom $3x + 6$ je ireducibilní v $\mathbb{Q}[x]$, avšak je reducibilní v $\mathbb{Z}[x]$. Dle Tvrzení 8.3.4. je polynom $3x + 6$ ireducibilní v $\mathbb{Q}[x]$. Jaká je situace v $\mathbb{Z}[x]$? Nejdříve určíme jednotky v $\mathbb{Z}[x]$. Protože $1 \cdot 1 = (-1) \cdot (-1) = 1$, jsou $1, -1$ jednotky. Zjistíme, zda jsou v $\mathbb{Z}[x]$ ještě nějaké další jednotky. Buď f jednotka. Pak existeje $g \in \mathbb{Z}[x]$, $fg = 1$. Pak $deg(fg) = deg(1)$, $deg(f) + deg(g) = 0$. Z toho plyne (protože stupně polynomů jsou nezáporná celá čísla), že $deg(f) = deg(g) = 0$ a tedy f, g jsou nenulová celá čísla. Pak ovšem $f = 1, g = 1$ nebo $f = -1, g = -1$. Tudíž $f \in \{1, -1\}$. Vidíme, že $U(\mathbb{Z}[x]) = \{1, -1\}$. Ukážeme nyní, že polynom $3x+6$ je reducibilní v $\mathbb{Z}[x]$. Je $3x+6 \neq 0$, $3x+6$ není jednotka, $3|3x+6$, protože $3x+6 = 3(x+2)$. Jelikož 3 není jednotka, není konstantní polynom 3 asociován s 1. Také 3 není asociován s $3x+6$, protože s $3x + 6$ jsou asociovány pouze polynomy $3x + 6$ a $-3x - 6$. Tento příklad opět ukazuje, že odpověď na otázku, zda nějaký prvek je ireducibilní či reducibilní, závisí podstatně na tom, v jakém oboru integrity zrovna jsme.

Samozřejmě je dobré, pokud víme, jak přesně vypadají ireducibilní prvky daného oboru integrity. Pro $\mathbb{Z}$ je odpověď jednoduchá a je obsažena v následujícím tvrzení.

8.3.6. Tvrzení. *Nechť q je celé číslo. Pak q je ireducibilní v $\mathbb{Z}$ právě tehdy, když q je prvočíslo nebo $-q$ je prvočíslo.*

Důkaz.

1. Nechť q je ireducibilní v $\mathbb{Z}$. Chceme: q je prvočíslo nebo $-q$ je prvočíslo. Protože q je ireducibilní, je $q \neq 0$, $q \notin \{1, -1\}$ (připomeňte si, že $U(\mathbb{Z}) = \{1, -1\}$).
   Případ (I): $q > 1$. Ukážeme, že q je prvočíslo. Nechť d je kladné celé číslo, $d|q$. Je třeba ukázat, že $d = 1$ nebo $d = q$. Protože q je ireducibilní, je $d \| 1$ nebo $d \| q$. První případ dává $d \in \{1, -1\}$; ovšem $d > 0$, takže $d = 1$. Druhý případ dává $d \in \{q, -q\}$; ovšem $d > 0$, takže $d = q$.
   Případ (II): $q < -1$. Ukážeme, že $-q$ je prvočíslo. Protože $-q \| q$ a q je ireducibilní, je také $-q$ ireducibilní. Je $-q > 1$ a postupem obdobným jako v případě (I) dokážeme, že $-q$ je prvočíslo.

2. Nechť q je prvočíslo nebo $-q$ je prvočíslo. Chceme: q je ireducibilní v $\mathbb{Z}$.
   Případ (I): q je prvočíslo. Nechť d je celé číslo, $d|q$. Víme již (viz počátek části 8.3.), že $d \| 1$ nebo $d \| q$. Je tedy q ireducibilní.
   Případ (II): $-q$ je prvočíslo. Je tedy $-q$ ireducibilní (viz případ (I)). Protože $q \| -q$, je q ireducibilní.

Víte již, že lineární polynomy v $T[x]$, kde T je těleso, jsou ireducibilní. Takže také lineární polynomy v $\mathbb{C}[x]$ jsou ireducibilní. Zajímavé je, že v $\mathbb{C}[x]$ již žádné další ireducibilní polynomy neexistují – to se naučíte v kapitole číslo 11; bude to důsledek Základní věty algebry, která tvrdí, že každý nekonstantní polynom s komplexními koeficienty má aspoň jeden komplexní kořen.

Je také znám úplný popis všech ireducibilních polynomů v $\mathbb{R}[x]$. Jsou to polynomy lineární a polynomy kvadratické se záporným diskriminantem. Je nám již jasné, že lineární polynomy v $\mathbb{R}[x]$ jsou ireducibilní. Jako cvičení zkuste dokázat, že kvadratický polynom s reálnými koeficienty a se záporným diskriminantem je ireducibilní v $\mathbb{R}[x]$. No a žádné další ireducibilní polynomy v $\mathbb{R}[x]$ neexistují - to se opět naučíte v kapitole 11.

Je zajímavé, že v $\mathbb{Q}[x]$ je situace úplně jiná – existují tam ireducibilní polynomy libovolného stupně n, kde n je celé číslo, $n \geq 1$ (viz Větu 7 na straně 202 v učebnici [1]).

Cvičení.

1. Dokažte Tvrzení 8.3.3.

2. Nechť T je těleso. Najděte všechny ireducibilní prvky v T.

3. Nechť f je polynom s reálnými koeficienty, f je kvadratický, f má záporný diskriminant. Dokažte, že polynom f je ireducibilní v $\mathbb{R}[x]$.

4. Rozhodněte, zda prvek $2 + 3i$ je ireducibilní v $\mathbb{Z}[i]$. Své rozhodnutí zdůvodněte.

8.4 Prvočísla

Na počátku předchozí části jsme si připomněli, že celá čísla větší než jedna se dělí na prvočísla a čísla složená. Přitom celé číslo p, $p > 1$, se nazývá prvočíslo, pokud pro všechna kladná celá čísla d platí: jestliže $d|p$, pak $d = 1$ nebo $d = p$.

Vzhledem k Tvrzení 8.3.6. můžeme prvočísla také vymezit jako kladné ireducibilní prvky oboru integrity $\mathbb{Z}$.

Zkoumání prvočísel je velmi zajímavá a také oblíbená činnost, která spíše než do algebry patří do teorie čísel.

Existuje velké množství knih, které se zabývají teorií čísel.

Z vlastní zkušenosti mohu doporučit knihu

Kenneth Ireland, Michael Rosen: *A Classical Introduction to Modern Number Theory.* Second Edition. Springer, New York 1990.

Následující kniha je sice stará, avšak dobrá a na internetu volně bez omezení dostupná:

Robert D. Carmichael: *The Theory of Numbers.* John Wiley & Sons, New York 1914.
`https://www.gutenberg.org/files/13693/13693-pdf.pdf`

Z česky psané literatury o teorii čísel doporučím také jen knížečky či knihy volně dostupné.

Základní poučení o teorii čísel najdete v knížečce

Jiří Sedláček: *Co víme o přirozených číslech.* Mladá fronta, Praha 1961.
`https://dml.cz/handle/10338.dmlcz/403433`

Zájemce o česky psané podrobnější poučení o teorii čísel mohu odkázat na

Karel Rychlík: *Úvod do elementární teorie číselné.* Jednota čs. matematiků a fysiků, Praha 1931.
`https://dml.cz/handle/10338.dmlcz/402936`

Na ukázku vyslovím jednu známou větu o prvočíslech a podám její klasický důkaz. Mimochodem, ten důkaz byste se měli naučit (pokud ho již neznáte).

8.4.1. Věta. *Existuje nekonečně mnoho prvočísel.*

Důkaz. Důkaz provedeme sporem. Předpokládejme, že existuje pouze konečně mnoho prvočísel. Celkový počet prvočísel označme k. Jistě existuje aspoň jedno prvočíslo, například číslo 2. Je tedy $k \geq 1$. Buď $p_1, p_2, \ldots, p_k$ seznam všech prvočísel. Uvažme číslo $c = p_1 p_2 \cdots p_k + 1$. Číslo c je celé a navíc $c > 1$. Nechť $M = \{d \in \mathbb{Z};\ d|c \wedge d > 1\}$. Je $M \neq \emptyset$, protože například $c \in M$. Položme $q = \min M$. Číslo q je celé, $q|c$ a $q > 1$. Ukážeme, že q je prvočíslo. Nechť d je kladné celé číslo, $d|q$. Chceme: $d = 1$ nebo $d = q$. Jestliže $d = 1$, pak jsme hotovi. Nechť tedy $d \neq 1$.

Pak $d > 1$ a také $d|c$ (protože $d|q$ a $q|c$). Vidíme, že $d \in M$. Protože $q = \min M$, máme $q \leq d$. Jelikož d a q jsou kladná celá čísla a $d|q$, je $d \leq q$. Celkem $q \leq d$, $d \leq q$, $d = q$. Ukázali jsme tedy, že q je prvočíslo. Pak ovšem $q = p_i$ pro nějaké celé číslo i, $1 \leq i \leq k$. Víme, že $q|c$, čili $p_i|c$. Je $1 = c - p_1 p_2 \cdots p_k$. Ovšem $p_i|c$ a také $p_i|p_1 p_2 \cdots p_k$, protože $p_i \in \{p_1, p_2, \ldots, p_k\}$. Z toho plyne, že $p_i|1$. Pak $p_i \in \{1, -1\}$, spor (každé prvočíslo je větší než 1).

Cvičení.

1. Dokažte, že každé celé číslo větší než jedna lze napsat jako součin několika prvočísel.

2. Najděte dvanáct po sobě jdoucích složených čísel.

8.5 Počítání modulo

Již jste se setkali s počítáním modulo v oboru integrity celých čísel, a to při konstrukci okruhů $\mathbb{Z}_m$ (kde m je kladné celé číslo, tzv. modul). Nyní budeme počítat modulo v libovolném oboru integrity I, přičemž modulem bude nějaký zvolený nenulový prvek m oboru integrity I. Sestrojíme tak nový okruh $I/(m)$. Bude se jednat o provedení konstrukce známé ze $\mathbb{Z}$ v oboru integrity I (který již nemusí být $\mathbb{Z}$), takže pro $I = \mathbb{Z}$, $m \in \mathbb{Z}$, $m \neq 0$, bude okruh $\mathbb{Z}/(m)$ totožný se $\mathbb{Z}_m$. Mohli byste si říci, že se jedná o zobecnění, které se dělá jen proto, aby se nějaké zobecnění udělalo. Avšak tak tomu není. Uvedu příklad. Nechť p je prvočíslo, n je kladné celé číslo. Vezmeme polynom f nad tělesem $\mathbb{Z}_p$ a to takový, aby byl ireducibilní v $\mathbb{Z}_p[x]$ a měl stupeň n (lze dokázat, že takový polynom opravdu existuje). Pak $\mathbb{Z}_p[x]/(f)$ bude konečné těleso, které má přesně p^n prvků. Právě zmíněným postupem lze dokonce sestrojit všechna konečná tělesa.

Přejděme tedy k počítání modulo v libovolném oboru integrity. Doporučuji vám, ať si napřed připomenete počítání modulo v $\mathbb{Z}$ – pokud si to nepamatujete, můžete se třeba podívat do kapitoly 2.1 v [3] či do kapitoly 1.2 v [2].

8.5.1. Definice. Nechť I je obor integrity, $a, b, m \in I$, $m \neq 0$. Říkáme, že a je **kongruentní** s b **modulo** m, pokud m dělí $b - a$. Tento vztah zapisujeme $a \equiv b\ (m)$, případně $a \equiv b \mod m$ či $a \equiv_m b$. Bude-li z kontextu jasné, o jaké m se jedná, můžeme psát pouze $a \equiv b$.

8.5.2. Tvrzení. *Nechť I je obor integrity, $m \in I$, $m \neq 0$. Platí: $\equiv_m$ je relace ekvivalence na množině I.*

Důkaz. Důkaz je jednoduchý, udělejte jej jako cvičení.

Faktorovou množinu $I/\equiv_m$ budeme značit $I/(m)$. Připomínám, že $I/(m)$ je rozklad množiny I, v němž pro všechna $a, b \in I$ platí: a a b leží ve stejné třídě rozkladu tehdy a jen tehdy, když $a \equiv b$.

Nechť $a \in I$. Třídu rozkladu $I/(m)$, v níž leží prvek a, budeme značit $[a]_m$. Bude-li z kontextu jasné, o jaké m se jedná, můžeme psát pouze $[a]$; v [3] a také v [2] se používá značení

$\overline{a}$ (ovšem v uvedených dvou textech se uvažují pouze kongruence v $\mathbb{Z}$). Je $[a] = \{x \in I;\ x \equiv a\}$.

8.5.3. Tvrzení. *Nechť I je obor integrity, $a, b, c, d, m \in I$, $m \neq 0$. Jestliže $a \equiv c\ (m)$, $b \equiv d\ (m)$, pak $a + b \equiv c + d\ (m)$, $a \cdot b \equiv c \cdot d\ (m)$.*

Důkaz. Nechť $a \equiv c$, $b \equiv d$. Víme tedy, že $m|c-a$, $m|d-b$. Ukážeme nejprve, že $a+b \equiv c+d$. Je $(c+d)-(a+b) = (c-a)+(d-b)$. Z toho je patrné, že $m|(c+d)-(a+b)$, takže $a+b \equiv c+d$. Nyní ukážeme, že $ab \equiv cd$. Je $cd - ab = cd - ad + ad - ab = (c-a)d + a(d-b)$. Z toho je patrné, že $m|cd - ab$, takže $ab \equiv cd$.

Na množině $I/(m)$ nyní definujeme sčítání a násobení takto:

$$[a] + [b] = [a + b],\ [a] \cdot [b] = [a \cdot b]$$

$(a, b \in I)$

Je dobré si uvědomit, že ve výrazu $[a] + [b] = [a + b]$ symbol + na levé straně nemá stejný význam jako + na pravé straně. Na levé straně + označuje definované sčítání tříd rozkladu $I/(m)$, kdežto + na pravé straně označuje již dané (známé) sčítání v oboru integrity I. Takže jeden symbol označuje dvě věci. Obdobný komentář bychom mohli učinit o symbolu $\cdot$ ve výrazu $[a] \cdot [b] = [a \cdot b]$.

Je třeba dát pozor. Operace sčítání a násobení na množině $I/(m)$ jsou definovány pomocí reprezentantů. Co se tím myslí? Nechť $\alpha, \beta \in I/(m)$. Chceme určit $\alpha+\beta$ a také $\alpha\cdot\beta$. Postupujme podle definice. Vezmeme nějaký prvek $a \in \alpha$ (je tedy $\alpha = [a]$)– takový prvek vždy existuje, protože třídy rozkladu jsou neprázdné množiny; prvek a je reprezentantem třídy α. Obdobně vezmeme nějaký prvek $b \in \beta$ (je tedy $\beta = [b]$); prvek b je reprezentantem třídy β. No a pak bude $\alpha + \beta = [a] + [b] = [a + b]$, $\alpha \cdot \beta = [a] \cdot [b] = [a \cdot b]$. Kde by mohl být problém? Třída α může mít více prvků, takže jako reprezentanta třídy α můžeme vzít prvek $c \in \alpha$ (tj. $[c] = \alpha$), který může být jiný, než prvek a (definice součtu a součinu neobsahují žádná pravidla pro výběr reprezentantů). Obdobně můžeme vzít prvek $d \in \beta$ (tj. $[d] = \beta$), který bude jiný, než prvek b. Pomocí reprezentantů c, d pak bude $\alpha + \beta = [c] + [d] = [c + d]$, $\alpha \cdot \beta = [c] \cdot [d] = [c \cdot d]$. Výsledný součet $\alpha + \beta$ a součin $\alpha \cdot \beta$ však musí být určeny jednoznačně, čili, jak se říká, nesmí záviset na volbě reprezentantů. Musí tedy být $[a + b] = [c + d]$ a $[a \cdot b] = [c \cdot d]$. Máme $a, c \in \alpha$, takže $a \equiv c$. Dále $b, d \in \beta$, takže $b \equiv d$. Dle Tvrzení 8.5.3. je $a + b \equiv c + d$, $a \cdot b \equiv c \cdot d$. To dává $[a + b] = [c + d]$, $[a \cdot b] = [c \cdot d]$. To právě jsme potřebovali. Problém nenastal, operace sčítání a násobení na množině $I/(m)$ jsou definovány korektně.

8.5.4. Tvrzení. *Nechť I je obor integrity, $m \in I$, $m \neq 0$. Na $I/(m)$ definujeme operace sčítání a násobení takto: $[a] + [b] = [a + b]$, $[a] \cdot [b] = [a \cdot b]$ $(a, b \in I)$. Pak $I/(m)$ je komutativní asociativní okruh. Navíc, pokud I má jednotkový prvek 1, pak $I/(m)$ má jednotkový prvek $[1]$.*

Důkaz. Nejprve ukážeme, že $I/(m)$ s operací + je komutativní grupa.
operace + je asociativní: Nechť $a, b, c \in I$. Chceme: $[a] + ([b] + [c]) = ([a] + [b]) + [c]$. Počítejme:

$[a] + ([b] + [c]) = [a] + [b + c] = [a + (b + c)] = [(a + b) + c] = [a + b] + [c] = ([a] + [b]) + [c]$.
operace $+$ je komutativní: Nechť $a, b \in I$. Chceme: $[a] + [b] = [b] + [a]$. Počítejme: $[a] + [b] = [a + b] = [b + a] = [b] + [a]$.
operace $+$ má nulový prvek $[0]$: Nechť $a \in I$. Chceme: $[a] + [0] = [a]$. Počítejme: $[a] + [0] = [a + 0] = [a]$.
ke každému prvku množiny $I/(m)$ existuje prvek opačný: Nechť $a \in I$. Stačí ukázat, že $[a] + [-a] = [0]$. Počítejme: $[a] + [-a] = [a + (-a)] = [0]$.
Právě jsme ukázali, že $I/(m)$ spolu s operací $+$ je komutativní grupa.
Nyní ukážeme, že operace $\cdot$ je distributivní vzhledem k operaci $+$. Nechť $a, b, c \in I$. Chceme: $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$ a $([b] + [c]) \cdot [a] = [b] \cdot [a] + [c] \cdot [a]$. Počítejme: $[a] \cdot ([b] + [c]) = [a] \cdot [b + c] = [a \cdot (b + c)] = [a \cdot b + a \cdot c] = [a \cdot b] + [a \cdot c] = [a] \cdot [b] + [a] \cdot [c]$ a $([b] + [c]) \cdot [a] = [b + c] \cdot [a] = [(b + c) \cdot a] = [b \cdot a + c \cdot a] = [b \cdot a] + [c \cdot a] = [b] \cdot [a] + [c] \cdot [a]$.
Právě jsme ukázali, že $I/(m)$ s operacemi $+$ a $\cdot$ je okruh.
Zbytek důkazu již určitě doděláte snadno jako cvičení.

8.5.5. Poznámka. Ačkoli I je obor integrity, $I/(m)$ nemusí být obor integrity (i když je to vždy asociativní komutativní okruh). Tento fakt znáte již z dřívějška. Například $\mathbb{Z}_{10}$ není obor integrity. Je $[2], [5] \in \mathbb{Z}_{10}$, $[2] \neq [0]$ ($[0] = [2]$ by dávalo $0 \equiv 2$ (10), $10|2 - 0$, $10|2$, což však v $\mathbb{Z}$ neplatí), $[5] \neq [0]$, a přitom $[2] \cdot [5] = [2 \cdot 5] = [10] = [0]$. Někdy však speciální kvalita oboru integrity I a modulu m poskytne speciální kvalitu okruhu $I/(m)$ (o tom snad později). Vlastně trochu to již znáte – víte, že pro prvočíslo p je $\mathbb{Z}_p$ těleso.

Cvičení.

1. Dokažte Tvrzení 8.5.2.
2. Dokončete důkaz Tvrzení 8.5.4.
3. Nechť I je obor integrity s jednotkovým prvkem, $j \in U(I)$, tj. j je jednotka okruhu I. Popište přesně, jak vypadá množina $I/(j)$.

9 Eukleidovské obory

Volně řečeno, eukleidovské obory jsou obory integrity, ve kterých se dá dělit se zbytkem nenulovými prvky. To není samoúčelné. V eukleidovských oborech totiž pak lze k výpočtu největšího společného dělitele použít Eukleidův algoritmus, každý nenulový prvek, který není jednotkou, lze jednoznačně rozložit na součin ireducibilních prvků, atd.

9.1 Definice eukleidovského oboru

Ve škole jste se učili, jak se kladná celá čísla dělí se zbytkem. Někdy vyjde dělení beze zbytku (zbytek je nulový), například $55 : 11 = 5$ (protože $55 = 11 \cdot 5$). Někdy vyjde dělení s nenulovým

zbytkem, například $50 : 11 = 4$, zbytek 6 (protože $50 = 11 \cdot 4 + 6$ a $6 < 11$). Zbytek musí být menší než dělitel! Abychom mohli v oboru integrity I dělit se zbytkem, musíme mít možnost nějak porovnat velikost zbytku a velikost dělitele (připomínám: zbytek má být menší než dělitel). S tím jsme neměli problém v kladných celých číslech – použili jsme obvyklé uspořádání celých čísel (které, jak víte, je lineární). Jak budeme postupovat v případě obecného oboru integrity I? Na množině I přece nemusí být předem dáno žádné uspořádání, dány jsou pouze operace sčítání a násobení. Každému nenulovému prvku i oboru integrity I přiřadíme nezáporné celé číslo $N(i)$, kterému budeme říkat norma prvku i. Dělit prvek a nenulovým prvkem b pak bude znamenat najít v oboru integrity I prvek q (zvaný podíl nebo neúplný podíl) a prvek r (zvaný zbytek) tak, aby platilo: $a = bq + r$ a přitom $r = 0$ nebo $r \neq 0$ a $N(r) < N(b)$. Ještě si všimněme jedné věci. V kladných celých číslech z $a|b$ plyne $a \leq b$ ($a|b$ znamená, že existuje kladné celé číslo c takové, že $b = ac$; pak $1 \leq c$, $a \cdot 1 \leq a \cdot c$, $a \leq b$). V obecném oboru integrity I budeme požadovat, aby pro všechna $a, b \in I$, $a \neq 0$, $b \neq 0$, platilo: jestliže $a|b$, pak $N(a) \leq N(b)$. Nyní vyslovíme přesnou definici eukleidovského oboru.

9.1.1. Definice. Nechť I je obor integrity s jednotkovým prvkem. Pak I se nazývá **eukleidovský obor**, pokud existuje zobrazení $N : I - \{0\} \to \mathbb{N}_0$ (zvané **norma** nebo **eukleidovská norma**) takové, že platí

1. pro všechna $a, b \in I$, $b \neq 0$, existují $q, r \in I$ takové, že $a = bq + r$ a přitom $r = 0$ nebo $r \neq 0$ a $N(r) < N(b)$ (q se nazývá **podíl** nebo **neúplný podíl**, r se nazývá **zbytek**)
2. pro všechna $a, b \in I$, $a \neq 0$, $b \neq 0$, platí: jestliže $a|b$ pak $N(a) \leq N(b)$.

V eukleidovských oborech mají každé dva prvky a, b největší společný dělitel, který se dá vyjádřit ve tvaru $ua + vb$. V následující větě tento fakt přesně vyslovíme a podáme důkaz, který bude existenční. V části 9.3. pak uvedeme algoritmus, který největší společný dělitel prvků a, b vypočítá a také vypočítá prvky u, v.

9.1.2. Věta. *Nechť I je eukleidovský obor. Pak platí:*

1. *Pro každé dva prvky z I existuje v I jejich největší společný dělitel.*
2. *Nechť $a, b, d \in I$. Jestliže d je největší společný dělitel prvků a, b, pak existují $u, v \in I$ tak, že $d = ua + vb$.* **(Bézoutova rovnost)**

Důkaz.

1. Nechť $a, b \in I$. Jestliže $a = 0$, je $b = NSD(0, b) = NSD(a, b)$. Nechť $a \neq 0$. Položme

$$M = \{xa + yb; x \in I, y \in I, xa + yb \neq 0\}$$

Je $M \neq \emptyset$, protože $a \in M$ (je totiž $a = 1 \cdot a + 0 \cdot b$, $a \neq 0$). Buď $m \in M$ prvek takový, že pro všechna $e \in M$ je $N(m) \leq N(e)$. Protože $m \in M$, je $m \neq 0$, $m = ua + vb$ pro nějaká $u, v \in I$. Ukážeme, že $m = NSD(a, b)$. Je třeba ukázat dvě věci:

(a) $m|a$, $m|b$: Existují $q, r \in I$, $a = mq + r$ a přitom $r = 0$ nebo $r \neq 0$ a $N(r) < N(m)$. Předpokládejme, že $r \neq 0$. Pak $N(r) < N(m)$. Je $r = a - mq = a - (ua + vb)q = a - (uaq + vbq) = a - uaq - vbq = (1 - uq)a + (-vq)b$, $r = (1 - uq)a + (-vq)b$. Jelikož $1 - uq, -vq \in I$, $r \neq 0$, je $r \in M$. Pak $N(m) \leq N(r)$. Celkem $N(m) \leq N(r)$ a $N(r) < N(m)$, spor. Nutně tedy $r = 0$, $a = mq$, $m|a$. Obdobně lze ukázat, že $m|b$.

(b) Nechť $e \in I$, $e|a$, $e|b$. Chceme: $e|m$. Stačí si připomenout, že $m = ua + vb$.

2. Předpokládejme, že $d = NSD(a, b)$. Chceme: existují $u, v \in I$, $d = ua + vb$. Pokud $a = 0$, je $NSD(a, b) = NSD(0, b) = b$ a tedy $d \| b$. Pak $d = jb$, kde $j \in U(I)$, a $d = 0 \cdot a + j \cdot b$ a vezmeme $u = 0$, $v = j$. Nechť $a \neq 0$. V důkazu první části věty jsme dokázali, že existuje $m \in I$, $m = NSD(a, b)$, $m = ua + vb$ pro nějaká $u, v \in I$. Jelikož také $d = NSD(a, b)$, je $d \| m$ a tedy $d = km$ pro nějaké $k \in U(I)$. Pak $d = km = k(ua + vb) = kua + kvb = (ku)a + (kv)b$. Stačí si uvědomit, že $ku, kv \in I$.

9.1.3. Důsledek. *Nechť I je eukleidovský obor, $a, b, c \in I$. Jestliže $a|bc$ a $a \perp b$, pak $a|c$.*

Důkaz. Předpokládejme, že $a|bc$ a $a \perp b$. Chceme: $a|c$. Protože $a \perp b$, je $NSD(a, b) = 1$. Dle 9.1.2. existují $u, v \in I$ tak, že $1 = ua + vb$. Pak $1 \cdot c = (ua + vb)c$, $c = uac + vbc$. Zřejmě $a|uac$ a také $a|vbc$, jelikož $a|bc$. Pak $a|uac + vbc$, $a|c$.

9.1.4. Důsledek. *Nechť I je eukleidovský obor, $i, b, c \in I$. Jestliže $i|bc$ a i je ireducibilní, pak $i|b$ nebo $i|c$.*

Důkaz. Předpokládejme, že $i|bc$ a i je ireducibilní. Chceme: $i|b$ nebo $i|c$. Pokud $i|b$, jsme hotovi. Nechť tedy $\neg(i|b)$. Musíme ukázat, že $i|c$. Ukážeme nejprve, že $i \perp b$. Buď $d \in I$, $d|i$ a $d|b$. Chceme: $d|1$. Jelikož prvek i je ireducibilní, je $d \| 1$ nebo $d \| i$. Případ $d \| i$ by dal $i|b$, což neplatí. Takže $d \| 1$, $d|1$. Máme tedy tuto situaci: $i|bc$ a $i \perp b$. Dle 9.1.3. pak $i|c$.

9.1.5. Příklad. Uvažme obor integrity $\mathbb{Z}[\sqrt{-5}]$. Tímto oborem integrity jsme se zabývali v příkladu 8.2.4. Doporučuji vám: Podívejte se znovu na příklad 8.2.4. Porozumíte pak lépe tomuto příkladu. Připomínám, že $\mathbb{Z}[\sqrt{-5}]$ je podokruh tělesa $\mathbb{C}$ a dále

$$\mathbb{Z}[\sqrt{-5}] = \{a + b \cdot \sqrt{-5} |\ a, b \in \mathbb{Z}\}$$

přičemž vyjádření prvků okruhu $\mathbb{Z}[\sqrt{-5}]$ ve tvaru $a + b \cdot \sqrt{-5}$, kde a, b jsou celá čísla, je jednoznačné.

Využijeme zobrazení $N : \mathbb{Z}[\sqrt{-5}] \to \mathbb{N}_0$ definované následovně: pro celá čísla a, b je

$$N(a + b\sqrt{-5}) = a^2 + 5b^2.$$

Zobrazení N má důležitou vlastnost: pro všechna $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$ je

$$N(\alpha\beta) = N(\alpha)N(\beta).$$

Pokud $N(\alpha) = 1$, je $\alpha \in \{1, -1\}$ – tento fakt jsme podrobně zdůvodnili v příkladu 8.2.4. a bude se nám hodit také v tomto příkladu.

Povšimněme si, že $N(\alpha) = 1$ dává $\alpha \in U(\mathbb{Z}[\sqrt{-5}])$, protože z $N(\alpha) = 1$ plyne $\alpha \in \{1, -1\}$ a $1 \cdot 1 = (-1) \cdot (-1) = 1$.

Zdůvodníme teď, že 3 je ireducibilní prvek v $\mathbb{Z}[\sqrt{-5}]$. Je $N(3) = 9$. Jistě $3 \neq 0$. Také 3 není jednotka v $\mathbb{Z}[\sqrt{-5}]$, protože pro každou jednotku ι v $\mathbb{Z}[\sqrt{-5}]$ je $N(\iota) = 1$. Proč? Je-li ι jednotka, pak existuje $\kappa \in \mathbb{Z}[\sqrt{-5}]$ tak, že $\iota\kappa = 1$. Pak $N(\iota\kappa) = N(1)$, $N(\iota)N(\kappa) = 1$, $N(\iota) = 1$ (jelikož $N(\iota), N(\kappa) \in \mathbb{N}_0$). Buď $\alpha \in \mathbb{Z}[\sqrt{-5}]$, $\alpha|3$. Je třeba ukázat, že $\alpha \| 1$ nebo $\alpha \| 3$. Existuje $\beta \in \mathbb{Z}[\sqrt{-5}]$, $3 = \alpha\beta$. Pak $N(3) = N(\alpha\beta)$, $9 = N(\alpha)N(\beta)$. Protože $N(\alpha), N(\beta) \in \mathbb{N}_0$, máme pouze tři možnosti:

1. $N(\alpha) = 1$, $N(\beta) = 9$: Je $\alpha \in U(\mathbb{Z}[\sqrt{-5}])$, takže $\alpha \| 1$.
2. $N(\alpha) = 3$, $N(\beta) = 3$: Situace $N(\alpha) = 3$ nemůže nastat – viz Příklad 8.2.4.
3. $N(\alpha) = 9$, $N(\beta) = 1$: Je $\beta \in U(\mathbb{Z}[\sqrt{-5}])$, takže $\alpha \| 3$.

Zdůvodnili jsme tedy, že 3 je ireducibilní prvek v $\mathbb{Z}[\sqrt{-5}]$.

Platí: $3|(2 + \sqrt{-5})(2 - \sqrt{-5})$, protože $(2 + \sqrt{-5})(2 - \sqrt{-5}) = 9$.

Ovšem $\neg(3|2+\sqrt{-5})$. Zdůvodnění: Předpokládejme, že $3|2+\sqrt{-5}$. Pak existuje $\gamma \in \mathbb{Z}[\sqrt{-5}]$, $3\gamma = 2 + \sqrt{-5}$. Je $\gamma = x + y\sqrt{-5}$ pro nějaká celá čísla x, y. Pak $3(x + y\sqrt{-5}) = 2 + \sqrt{-5}$, $3x+3y\sqrt{-5} = 2+\sqrt{-5}$, $3x = 2$, spor (je totiž x celé číslo). Nutně tedy $\neg(3|2+\sqrt{-5})$. Obdobně lze ukázat, že $\neg(3|2 - \sqrt{-5})$.

Shrnutí: V oboru integrity $\mathbb{Z}[\sqrt{-5}]$ platí:

$$3|(2 + \sqrt{-5})(2 - \sqrt{-5}),\ 3 \text{ je ireducibilní prvek},\ \neg(3|2 + \sqrt{-5}),\ \neg(3|2 - \sqrt{-5})$$

Z toho mimochodem plyne, že obor integrity $\mathbb{Z}[\sqrt{-5}]$ není eukleidovský – viz Důsledek 9.1.4.

Druhý požadavek z definice eukleidovských oborů stanoví vztah mezi relací $|$ a normou N: jestliže $a \neq 0$, $b \neq 0$, $a|b$, pak $N(a) \leq N(b)$. Prozkoumáme teď vztah mezi $|$ a N trochu podrobněji.

9.1.6. Tvrzení. *Nechť I je eukleidovský obor, $a, b \in I$, $a \neq 0$, $b \neq 0$. Platí:*

1. *Jestliže $a \| b$, pak $N(a) = N(b)$.*
2. *Jestliže $a|b$ a $\neg(b|a)$, pak $N(a) < N(b)$.*

Důkaz.

1. Toto je velmi jednoduché, jistě to zvládnete dokázat sami jako cvičení.

2. Předpokládejme, že $a|b$ a $\neg(b|a)$. Chceme: $N(a) < N(b)$. Jelikož $a|b$, máme $N(a) \leq N(b)$. Předpokládejme, že $N(a) = N(b)$. Existují $q, r \in I$, $a = bq + r$ a přitom $r = 0$ nebo $r \neq 0$ a $N(r) < N(b)$. Protože $\neg(b|a)$, máme $r \neq 0$ a tedy $N(r) < N(b)$. Ovšem $N(a) = N(b)$, takže $N(r) < N(a)$. Je $r = a + (-q)b$. Protože $a|b$, máme $a|r$. Pak $N(a) \leq N(r)$. Celkem $N(r) < N(a)$ a současně $N(a) \leq N(r)$. To je spor. Nutně tedy $N(a) \neq N(b)$. Víme teď, že $N(a) \leq N(b)$, $N(a) \neq N(b)$. Tudíž $N(a) < N(b)$.

V poznámce 8.5.5. jsme zmínili, že speciální kvalita oboru integrity I a speciální kvalita modulu m poskytne někdy speciální kvalitu okruhu $I/(m)$. O tom něco říká následující tvrzení.

9.1.7. Tvrzení. *Jestliže I je eukleidovský obor a $m \in I$, m je ireducibilní, pak okruh $I/(m)$ je těleso.*

Důkaz. Protože m je ireducibilní prvek, je $m \neq 0$. Tvrzení 8.5.4. nám říká, že $I/(m)$ je komutativní asociativní okruh s jednotkovým prvkem. Jednotkovým prvkem okruhu $I/(m)$ je prvek $[1]$, kde 1 je jednotkový prvek oboru integrity I, a nulovým prvkem okruhu $I/(m)$ je prvek $[0]$, kde 0 je nulový prvek oboru integrity I. Chceme, aby pro každé $\alpha \in I/(m)$, $\alpha \neq [0]$, existovalo $\beta \in I/(m)$ takové, že $\beta\alpha = [1]$. Zvolme tedy libovolně $\alpha \in I/(m)$, $\alpha \neq [0]$. Je $\alpha = [a]$ pro nějaké $a \in I$. Předpokládejme, že $m|a$. Pak $0 \equiv a\ (m)$, $[0] = [a]$, $[0] = \alpha$, spor. Nutně tedy $\neg(m|a)$. Protože prvek m je ireducibilní a $\neg(m|a)$, máme $NSD(a, m) = 1$. Dle věty 9.1.2. existují $u, v \in I$, $1 = ua + vm$. Pak $1 - ua = vm$, $m|1 - ua$, $ua \equiv 1\ (m)$, $[ua] = [1]$, $[u][a] = [1]$, $[u]\alpha = [1]$. Stačí vzít $\beta = [u]$. Dle definice tělesa musíme ještě ukázat, že $I/(m)$ má aspoň dva prvky. Postačí tedy ukázat, že $[0] \neq [1]$. Předpokládejme, že $[0] = [1]$. Pak $0 \equiv 1\ (m)$, $m|1 - 0$, $m|1$, $m \in U(I)$, spor (ireducibilní prvek dle definice nikdy není jednotka). Proto $[0] \neq [1]$.

Cvičení.

1. Dokažte první část Tvrzení 9.1.6.

2. Nechť I je eukleidovský obor, k je kladné celé číslo, $i, a_1, \ldots, a_k \in I$. Jestliže $i|a_1 \cdots a_k$ a i je ireducibilní, pak existuje celé číslo j, $1 \leq j \leq k$, $i|a_j$. Dokažte. Poznámka: jedná se o zobecnění důsledku 9.1.4.

9.2 Příklady eukleidovských oborů

V této části uvedeme základní příklady eukleidovských oborů, a to $\mathbb{Z}$, $\mathbb{Z}[i]$, $T[x]$, kde T je libovolné těleso.

9.2.1. Příklad. Obor integrity celých čísel $\mathbb{Z}$ je eukleidovský obor s eukleidovskou normou $|\ |$ (absolutní hodnota).

Zdůvodnění:

Zřejmě $|\ |:\mathbb{Z}-\{0\}\to\mathbb{N}_0$. Nechť $a,b\in\mathbb{Z}$, $b\neq 0$. Hledáme $q,r\in\mathbb{Z}$ tak, aby $a=bq+r$ a přitom $r=0$ nebo $r\neq 0$ a $|r|<|b|$. Je $|b|>0$ a tedy $\ldots,-2\cdot|b|<-1\cdot|b|<0\cdot|b|<1\cdot|b|<2\cdot|b|<\ldots$. Existuje přesně jedno celé číslo k takové, že $k|b|\leq a<(k+1)|b|$. Položme $r=a-k|b|$. Pak r je celé číslo, $0\leq a-k|b|=r$, $r=a-k|b|<(k+1)|b|-k|b|=|b|$, čili $0\leq r<|b|$. Rozlišíme dva případy:

- $b>0$: Je $a=k|b|+r=kb+r$ a položíme $q=k$. Pak q je celé číslo, $a=qb+r$ a přitom $r=0$ nebo $r\neq 0$ a $|r|<|b|$ (uvědomme si, že $r=|r|$).
- $b<0$: Je $a=k|b|+r=k(-b)+r=(-k)b+r$ a položíme $q=-k$. Pak q je celé číslo, $a=qb+r$ a přitom $r=0$ nebo $r\neq 0$ a $|r|<|b|$.

Zbývá ještě ukázat, že pro všechna nenulová celá čísla a,b z $a|b$ plyne $|a|\leq|b|$. Předpokládejme, že $a|b$. Existuje tedy celé číslo c takové, že $b=ac$. Musí být $c\neq 0$, protože $c=0$ by dalo $b=0$. Je $|a|>0$, $|b|>0$, $|c|>0$. Protože c je celé číslo, je $1\leq|c|$. Pak $|a|\cdot 1\leq|a|\cdot|c|$, $|a|\leq|ac|$, $|a|\leq|b|$.

Povšimněte si, že při dělení se zbytkem v $\mathbb{Z}$ s eukleidovskou normou $|\ |$ nejsou podíl a zbytek určeny jednoznačně. Například $29:9=3$, zbytek 2, jelikož $29=9\cdot 3+2$ a $|2|<|9|$; také však $29:9=4$, zbytek -7, jelikož $29=9\cdot 4+(-7)$ a $|-7|<|9|$. Je dobré si uvědomit, že definice eukleidovského oboru nepožaduje, aby podíl a zbytek byly určeny jednoznačně.

9.2.2. Příklad. Obor integrity Gaussových celých čísel $\mathbb{Z}[i]$ je eukleidovský obor s eukleidovskou normou N definovanou takto: pro celá čísla a,b je $N(a+bi)=a^2+b^2$.

Zdůvodnění:

Zřejmě $N:\mathbb{Z}[i]-\{0\}\to\mathbb{N}_0$. Nechť $\alpha,\beta\in\mathbb{Z}[i]$, $\beta\neq 0$. Hledáme $\delta,\epsilon\in\mathbb{Z}[i]$ tak, aby $\alpha=\beta\delta+\epsilon$ a přitom $\epsilon=0$ nebo $\epsilon\neq 0$ a $N(\epsilon)<N(\beta)$. Nejprve rozšíříme definiční obor zobrazení N na celou množinu $\mathbb{C}$: pro reálná čísla u,v položíme $N(u+vi)=u^2+v^2$. Přímým výpočtem se lze snadno přesvědčit o tom, že pro všechna komplexní čísla ϕ,ψ je $N(\phi\psi)=N(\phi)N(\psi)$ (viz cvičení). Provedeme dělení v tělese komplexních čísel: $\frac{\alpha}{\beta}=\gamma$. Nechť $\gamma=u+vi$, kde u,v jsou reálná čísla. Nechť e je celé číslo, které je nejblíže reálnému číslu u. Pak $|u-e|\leq\frac{1}{2}$ (číslo e nemusí být určeno jednoznačně; například pro $u=3,5$ můžeme vzít $e=3$ nebo také $e=4$). Obdobně nechť f je celé číslo, které je nejblíže číslu v. Pak $|v-f|\leq\frac{1}{2}$. Položme $\delta=e+fi$. Je $\delta\in\mathbb{Z}[i]$. Dále položme $\epsilon=\alpha-\beta\delta$. Jsou $\alpha,\beta,\delta\in\mathbb{Z}[i]$, takže také $\epsilon\in\mathbb{Z}[i]$. Zřejmě $\alpha=\beta\delta+\epsilon$. Pokud $\epsilon=0$ jsme hotovi. Nechť tedy $\epsilon\neq 0$. Je třeba ukázat, že $N(\epsilon)<N(\beta)$. Je $\epsilon=\alpha-\beta\delta=\beta\gamma-\beta\delta=\beta(\gamma-\delta)$. Takže $\epsilon=\beta(\gamma-\delta)$, $N(\epsilon)=N(\beta(\gamma-\delta))$, $N(\epsilon)=N(\beta)N(\gamma-\delta)$. Máme $\gamma-\delta=(u+vi)-(e+fi)=(u-e)+(v-f)i$, $\gamma-\delta=(u-e)+(v-f)i$ a tedy $N(\gamma-\delta)=(u-e)^2+(v-f)^2=|u-e|^2+|v-f|^2\leq(\frac{1}{2})^2+(\frac{1}{2})^2=\frac{1}{4}+\frac{1}{4}=\frac{1}{2}<1$, $N(\gamma-\delta)<1$. Pak $N(\beta)N(\gamma-\delta)<N(\beta)\cdot 1$ (zde bylo důležité, že $\beta\neq 0$ a tedy $N(\beta)>0$), $N(\epsilon)<N(\beta)$. To jsme chtěli.

Zbývá ještě ukázat, že pro $\alpha,\beta\in\mathbb{Z}[i]$, $\alpha\neq 0,\beta\neq 0$, z $\alpha|\beta$ plyne $N(\alpha)\leq N(\beta)$. Předpokládejme, že $\alpha|\beta$. Pak existuje $\gamma\in\mathbb{Z}[i]$, $\beta=\alpha\gamma$. Pak $N(\beta)=N(\alpha\gamma)$, $N(\beta)=N(\alpha)N(\gamma)$. Jelikož

$\beta \neq 0$, také $\gamma \neq 0$. Pak $N(\gamma) > 0$. Protože $\gamma \in \mathbb{Z}[i]$, je $N(\gamma) \geq 1$. Z $\alpha \neq 0$ dostáváme $N(\alpha) > 0$. Platí: $1 \leq N(\gamma)$, $N(\alpha) \cdot 1 \leq N(\alpha)N(\gamma)$, $N(\alpha) \leq N(\beta)$.

9.2.3. Poznámka. V příkladu 9.2.2. jsme ukázali, jak se v eukleidovském oboru $\mathbb{Z}[i]$ s eukleidovskou normou $N(a+bi) = a^2 + b^2$ (a, b jsou celá čísla) dělí se zbytkem. Ukážeme to na příkladě. Číslo $\alpha = 4 - 5i$ vydělíme se zbytkem číslem $\beta = 2 + 3i$. Neúplný podíl označme δ, zbytek označme ϵ. Vypočítáme nejprve $\frac{\alpha}{\beta}$ v tělese $\mathbb{C}$. Počítejme:

$$\frac{\alpha}{\beta} = \frac{4-5i}{2+3i} = \frac{(4-5i)(2-3i)}{(2+3i)(2-3i)} = \frac{8-12i-10i-15}{13} = \frac{-7-22i}{13} = -\frac{7}{13} + \left(-\frac{22}{13}\right) i$$

Najdeme celé číslo e, které je nejblíže číslu $-\frac{7}{13}$, a celé číslo f, které je nejblíže číslu $-\frac{22}{13}$. Je $e = -1$ a $f = -2$. Položíme $\delta = e + fi$, $\delta = -1 - 2i$. Chceme, aby bylo $\alpha = \beta\delta + \epsilon$. Proto položíme

$$\epsilon = \alpha - \beta\delta = 4 - 5i - (2+3i)(-1-2i) = 4 - 5i + (2+3i)(1+2i) = 4 - 5i + 2 + 4i + 3i - 6 = 2i$$

Je $\epsilon \neq 0$. V příkladu 9.2.2. jsme ukázali, že zvolený postup vždy pro $\epsilon \neq 0$ zaručí $N(\epsilon) < N(\beta)$. Můžeme to teď ještě zkontrolovat pro naše konkrétní hodnoty:

$$N(\epsilon) = N(2i) = 2^2 = 4, \; N(\beta) = N(2+3i) = 2^2 + 3^2 = 4 + 9 = 13$$

Závěr: $4 - 5i : 2 + 3i = -1 - 2i$, zbytek $2i$.

9.2.4. Příklad. Nechť T je těleso. Obor integrity $T[x]$ všech polynomů nad tělesem T je eukleidovský obor s eukleidovskou normou deg (stupeň polynomu).

Zdůvodnění:

Zřejmě $deg : T[x] - \{0\} \to \mathbb{N}_0$. Nechť $f, g \in T[x]$, $g \neq 0$. Hledáme polynomy q, r nad tělesem T tak, aby $f = gq + r$ a přitom $r = 0$ nebo $r \neq 0$ a $deg(r) < deg(g)$. Polynomy q, r určíme pomocí rekurze.

1. Pokud $f = 0$ nebo $f \neq 0$ a $deg(f) < deg(g)$, položíme $q = 0$ a $r = f$. Pak $gq + r = g \cdot 0 + f = f$, $r = 0$ nebo $r \neq 0$ a $deg(r) < deg(g)$.

2. Nechť $f \neq 0$ a $deg(f) \geq deg(g)$. Připomeňme, že pro nenulový polynom h označuje $lc(h)$ vedoucí koeficient polynomu h, tedy koeficient u $x^{deg(h)}$. Položme

$$g1x^* = lc(f)lc(g)^{-1}x^{deg(f)-deg(g)}g$$

Zde bylo důležité, že pracujeme s polynomy nad tělesem T a tedy pro $lc(g) \neq 0$ existuje v T prvek $lc(g)^{-1}$. Polynom g^* je opět polynom nad T, $g^* \neq 0$, $deg(g^*) = deg(f)$, $lc(g^*) = lc(f)$. Položme nyní

$$f^* = f - g^*$$

Také f^* je polynom nad tělesem T. Protože $deg(g^*) = deg(f)$, $lc(g^*) = lc(f)$, je $f^* = 0$ nebo $f^* \neq 0$ a $deg(f^*) < deg(f)$. Nyní budeme pracovat s dvojicí polynomů f^*, g (v tom právě je ta rekurze). Určíme polynomy q^* a r^* nad tělesem T takové, že $f^* = gq^* + r^*$, přičemž $r^* = 0$ nebo $r^* \neq 0$ a $deg(r^*) < deg(g)$. Pak

$$\begin{aligned} f - g^* &= gq^* + r^* \\ f &= gq^* + g^* + r^* \\ f &= gq^* + lc(f)lc(g)^{-1}x^{deg(f)-deg(g)}g + r^* \\ f &= g(q^* + lc(f)lc(g)^{-1}x^{deg(f)-deg(g)}) + r^* \end{aligned}$$

Nyní stačí vzít $q = q^* + lc(f)lc(g)^{-1}x^{deg(f)-deg(g)}$ a $r = r^*$.

Zbývá ještě ukázat, že pro $f, g \in T[x]$, $f \neq 0$, $g \neq 0$, z $f|g$ plyne $deg(f) \leq deg(g)$. Předpokládejme, že $f, g \in T[x]$, $f \neq 0$, $g \neq 0$, $f|g$. Existuje tedy polynom h nad tělesem T takový, že $g = fh$. Protože $g \neq 0$, je také $h \neq 0$. Pak $deg(g) = deg(fh) = deg(f) + deg(h)$, $deg(g) = deg(f) + deg(h)$. Jelikož $deg(h) \geq 0$, je $deg(f) \leq deg(g)$.

9.2.5. Poznámka. V příkladu 9.2.4. jsme ukázali, jek se v eukleidovském oboru $T[x]$, kde T je těleso, s eukleidovskou normou deg dělí se zbytkem. Toto dělení provádíme pomocí rekurze. Uvědomte si, že je to přesně ten postup, který znáte již ze školy (pokud jste tam ovšem prováděli dělení polynomu nenulovým polynomem se zbytkem). Nechť například $T = \mathbb{Q}$, $f = 12x^3 - 8x^2 + 7x - 6$, $g = 3x^2 + 4x - 5$. Provedeme tedy dělení se zbytkem $12x^3 - 8x^2 + 7x - 6 : 3x^2 + 4x - 5$. Nejprve vypočítáme $12x^3 : 3x^2 = 4x$ a to je právě $lc(f)lc(g)^{-1}x^{deg(f)-deg(g)}$. Pak od $12x^3 - 8x^2 + 7x - 6$ odečteme $4x(3x^2 + 4x - 5) = 12x^3 + 16x^2 - 20x$, tj. od f odečteme $lc(f)lc(g)^{-1}x^{deg(f)-deg(g)}g = g^*$. Získáme polynom $-24x^2+27x-6$, tj. polynom f^*. V dalším pak dělíme polynom $-24x^2 + 27x - 6$ opět polynomem $3x^2 + 4x - 5$, tj. polynom f^* polynomem g. Dostaneme podíl q^* a zbytek r^*. Celkově bude neúplný podíl při dělení polynomu f polynomem g roven $4x + q^*$, tj. $lc(f)lc(g)^{-1}x^{deg(f)-deg(g)} + q^*$, a zbytek bude roven r^*.

9.2.6. Příklad. Nechť p je prvočíslo. $\mathbb{Z}$ je eukleidovský obor (viz 9.2.1.) sa p je ireducibilní prvek v $\mathbb{Z}$ (viz 8.3.6.). Pak $\mathbb{Z}/(p) = \mathbb{Z}_p$ je těleso dle Tvrzení 9.1.7. To jen tak pro připomenutí.

9.2.7. Tvrzení. *Jestliže T je konečné těleso s k prvky a m je ireducibilní polynom nad tělesem T, $deg(m) = n$, pak $T[x]/(m)$ je konečné těleso s k^n prvky. Přitom*

$$T[x]/(m) = \{[f]; f \in T[x], f = 0 \vee f \neq 0 \wedge deg(f) < n\}$$

Důkaz. Jsou k, n celá čísla, $k \geq 2$ (každé těleso má aspoň dva prvky), $n \geq 1$ (ireducibilní polynom nemůže mít stupeň 0, protože by pak byl nenulový konstantní polynom a tedy jednotka). Víme již, že $T[x]$ je eukleidovský obor (viz Příklad 9.2.4.). Pak $T[x]/(m)$ je těleso podle Tvrzení 9.1.7. Položme

$$M = \{[f]; f \in T[x], f = 0 \vee f \neq 0 \wedge deg(f) < n\}$$

Ukážeme, že $M = T[x]/(m)$. Jistě $M \subseteq T[x]/(m)$. Nechť f je libovolný polynom nad tělesem T. Dokážeme, že $[f] \in M$. Pak bude dokázáno také, že $T[x]/(m) \subseteq M$. Provedeme dělení se zbytkem v eukleidovském oboru $T[x]$ s eukleidovskou normou deg. Je $f = mq + r$ pro nějaké polynomy nad tělesem T, přičemž $r = 0$ nebo $r \neq 0$ a $deg(r) < deg(m) = n$. Uvědomme si, že $f - r = mq$, $m|f - r$, $r \equiv f\ (m)$, $[f] = [r]$. Zřejmě $[r] \in M$, protože $r = 0$ nebo $r \neq 0$ a $deg(r) < n$. Takže $[f] \in M$.

Teď je již dokázáno, že $T[x]/(m) = M$. Polynomy nad tělesem T, které mají stupeň menší než n (včetně polynomu nultého) mají tvar $a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$; počet takových polynomů je roven k^n, neboť pro každé a_i máme celkem k možností (uvažujeme polynomy nad tělesem T, jež má k prvků). Z toho plyne, že $|M| \leq k^n$. Ukážeme ještě, že pro všechna $f, g \in T[x]$, $f = 0$ nebo $f \neq 0$ a $deg(f) < n$, $g = 0$ nebo $g \neq 0$ a $deg(g) < n$, platí: jestliže $[f] = [g]$, pak $f = g$. Jako důsledek pak dostaneme $k^n \leq |M|$, $k^n = |M|$, $|T[x]/(m)| = k^n$.

Nechť tedy $f, g \in T[x]$, $f = 0$ nebo $f \neq 0$ a $deg(f) < n$, $g = 0$ nebo $g \neq 0$ a $deg(g) < n$, $[f] = [g]$. Chceme: $f = g$. Protože $[f] = [g]$, je $f \equiv g\ (m)$, $m|g - f$. Předpokládejme, že $f \neq g$. Pak $g - f \neq 0$ a z $m|g - f$ dostáváme $deg(m) \leq deg(g - f)$. Ovšem $deg(g - f) < n$, takže $deg(m) < n$, $n < n$, spor. Nutně tedy $f = g$.

9.2.8. Příklad. Uvažme těleso $\mathbb{Z}_2$. Toto těleso má prvky $[0]_2$ a $[1]_2$; pro stručnost pišme pouze 0 a 1. Uvažme polynom m nad tělesem $\mathbb{Z}_2$, $m = x^2 + x + 1$. Polynom m je ireducibilni v $\mathbb{Z}_2[x]$ (zdůvodněte!). Dle Tvrzení 9.2.7. je $\mathbb{Z}_2[x]/(x^2+x+1)$ konečné těleso se 4 prvky, $\mathbb{Z}_2[x]/(x^2+x+1) = \{[0], [1], [x], [x+1]\}$. Není obtížné sestavit tabulky sčítání a násobení v tělese $\mathbb{Z}_2[x]/(x^2 + x + 1)$ (cvičení 2).

Cvičení.

1. Definujme zobrazení $N : \mathbb{C} \to \mathbb{R}$ takto: pro libovolná reálná čísla u, v je $N(u+vi) = u^2+v^2$. Dokažte, že pro všechna komplexní čísla ϕ, ψ je $N(\phi\psi) = N(\phi)N(\psi)$.

2. Uvažme těleso $\mathbb{Z}_2$. Toto těleso má prvky $[0]_2$ a $[1]_2$; pro stručnost pišme pouze 0 a 1. Uvažme polynom m nad tělesem $\mathbb{Z}_2$, $m = x^2 + x + 1$.

   - Dokažte, že polynom m je ireducibilni v $\mathbb{Z}_2[x]$.
   - Sestavte tabulky operací + a $\cdot$ v tělese $\mathbb{Z}_2[x]/(x^2 + x + 1)$.

3. Proveďte dělení se zbytkem v eukleidovském oboru $\mathbb{Z}$ s eukleidovskou normou $|\ |$: $11 : 3$, $11 : -3$, $-11 : 3$, $-11 : -3$. Udělejte zkoušku.

4. Proveďte dělení se zbytkem v eukleidovském oboru $\mathbb{Z}[i]$ s eukleidovskou normou $N(a + bi) = a^2 + b^2$ (pro $a, b \in \mathbb{Z}$): $13 + 3i : 23 - 8i$. Udělejte zkoušku.

5. Proveďte dělení se zbytkem v eukleidovském oboru $\mathbb{Z}_3[x]$ s eukleidovskou normou deg: $x^3 + 2x^2 + 1 : 2x^2 + 1$ (pro stručnost píšeme 0 místo $[0]_3$, 1 místo $[1]_3$ a 2 místo $[2]_3$). Udělejte zkoušku.

9.3 Eukleidův algoritmus

Už víte (viz větu 9.1.2.), že v eukleidovském oboru mají každé dva prvky a, b největší společný dělitel, který jde vyjádřit ve tvaru $ua + vb$, kde u, v jsou vhodné prvky daného eukleidovského oboru. V této části se seznámíte s Eukleidovým algoritmem, který vypočítá největší společný dělitel prvků a, b a také (bude-li to potřeba) vypočítá prvky u, v.

Nechť tedy I je eukleidovský obor s eukleidovskou normou N. Nechť $a, b \in I$. Chceme určit $d = NSD(a, b)$ a případně také prvky $u, v \in I$, $ua + vb = d$.

Eukleidův algoritmus počítá $d = NSD(a, b)$ a je založen na transformaci

$$E : (a_1, a_2) \mapsto (a_2, r)$$

kde $a_1, a_2, r \in I$, $a_2 \neq 0$, $a_1 = a_2q + r$ pro nějaké $q \in I$, $r = 0$ nebo $r \neq 0$ a $N(r) < N(a_2)$.

Výpočet začneme s dvojicí (a, b). Na uspořádané dvojice opakovaně aplikujeme transformaci E, a to tak dlouho, dokud je to možné, tj, dokud druhá složka dvojice je nenulová. Vzhledem k tomu, že normy druhých složek jsou nezáporná celá čísla a postupně klesají (pro $r \neq 0$ je $N(r) < N(a_2)$), skončíme po konečně mnoha krocích s dvojicí $(d, 0)$. Pak bude opravdu $d = NSD(a, b)$.

Zdůvodnění:

Pro $s, t \in I$ označme $S(s, t)$ množinu všech společných dělitelů prvků s, t v I. Ukážeme, že $S(a_1, a_2) = S(a_2, r)$ (transformace E nemění množiny všech společných dělitelů). Z toho pak vyplyne, že $S(a, b) = S(d, 0)$. Ovšem $S(d.0) = \{x \in I;\ x|d\}$, takže

$$S(a, b) = \{x \in I;\ x|d\}$$

a specielně $d = NSD(a, b)$.

$S(a_1, a_2) \subseteq S(a_2, r)$: Buď $x \in I$, $x|a_1$ a $x|a_2$. Chceme: $x|a_2$ a $x|r$. Je zřejmé, že $x|a_2$. Je $r = a_1 - a_2q$. Protože $x|a_1$, $x|a_2$, máme $x|r$.

$S(a_2, r) \subseteq S(a_1, a_2)$: Buď $x \in I$, $x|a_2$ a $x|r$. Chceme: $x|a_1$ a $x|a_2$. Je zřejmé, že $x|a_2$. Je $a_1 = a_2q + r$. Protože $x|a_2$, $x|r$, máme $x|a_1$.

9.3.1. Příklad. Pomocí Eukleidova algoritmu vypočítáme největšího společného dělitele celých čísel 1971, 1965.

$$(1971, 1965) \mapsto (1965, 6) \mapsto (6, 3) \mapsto (3, 0)$$

Závěr: $NSD(1971, 1965) = 3$.

Proč výpočet proběhl tak, jak je uvedeno? Byla totiž provedena tato dělení se zbytkem:

$$\begin{aligned} 1971 &= 1965 \cdot 1 + 6 \\ 1965 &= 6 \cdot 327 + 3 \\ 6 &= 3 \cdot 2 + 0 \end{aligned}$$

9.3.2. Příklad. Pomocí Eukleidova algoritmu vypočítáme největšího společného dělitele Gaussových celých čísel $13+3i$ a $11+3i$.

$$(13+3i, 11+3i) \mapsto (11+3i, 2) \mapsto (2, 1+i) \mapsto (1+i, 0)$$

Závěr: $NSD(13+3i, 11+3i) = 1+i$.

Proč výpočet proběhl tak, jak je uvedeno? Byla totiž provedena tato dělení se zbytkem:

$$\begin{aligned} 13+3i &= (11+3i)\cdot 1 + 2 \\ 11+3i &= 2\cdot(5+i) + (1+i) \\ 2 &= (1+i)\cdot(1-i) + 0 \end{aligned}$$

Rozšířený Eukleidův algoritmus počítá $d = NSD(a,b)$ a také $u, v \in I$ taková, že $ua+vb = d$ a je založen na třech paralelních transformacích

$$E_r : (a_1, a_2)_1 \mapsto (a_2, r)_1, (p_1, p_2)_2 \mapsto (p_2, p_1 - p_2 q)_2, (q_1, q_2)_3 \mapsto (q_2, q_1 - q_2 q)_3$$

kde $a_1, a_2, p_1, p_2, q_1, q_2, q, r \in I$, $a_2 \neq 0$, $a_1 = a_2 q + r$, $r = 0$ nebo $r \neq 0$ a $N(r) < N(a_2)$.

Všimněte si, že $r = a_1 - a_2 q$, takže $(a_1, a_2)_1 \mapsto (a_2, a_1 - a_2 q)_1$ a všechny tři transformace mají stejný výtvarný zákon, totiž $(w_1, w_2) \mapsto (w_2, w_1 - w_2 q)$.

Výpočet začneme s dvojicemi $(a,b)_1$, $(1,0)_2$ a $(0,1)_3$. Na uspořádané dvojice opakovaně aplikujeme transformace E_r, a to tak dlouho, dokud je to možné, tj, dokud druhá složka první dvojice je nenulová. Vzhledem k tomu, že normy druhých složek první dvojice jsou nezáporná celá čísla a postupně klesají (pro $r \neq 0$ je $N(r) < N(a_2)$), skončíme po konečně mnoha krocích s dvojicemi $(d,0)_1$, $(u,u^*)_2$ a $(v,v^*)_3$. Pak bude opravdu $d = NSD(a,b)$ a $ua + vb = d$.

Zdůvodnění:

Již víme, že

$$S(a,b) = \{x \in I;\ x|d\}$$

a specielně $d = NSD(a,b)$.

Ukážeme: (A) $(p_1 - p_2 q)a_2 - p_2(a_1 - a_2 q) = -(p_2 a_1 - p_1 a_2)$, tj. druhá složka druhé dvojice $\times$ první složka první dvojice $-$ první složka druhé dvojice $\times$ druhá složka první dvojice provedením E_r změní znaménko, nikoli však absolutní hodnotu. Počítejme:

$$(p_1 - p_2 q)a_2 - p_2(a_1 - a_2 q) = p_1 a_2 - p_2 q a_2 - p_2 a_1 + p_2 a_2 q = p_1 a_2 - p_2 a_1 = -(p_2 a_1 - p_1 a_2)$$

Ukážeme: (B) $(q_1 - q_2 q)a_2 - q_2(a_1 - a_2 q) = -(q_2 a_1 - q_1 a_2)$, tj. druhá složka třetí dvojice $\times$ první složka první dvojice $-$ první složka třetí dvojice $\times$ druhá složka první dvojice provedením E_r změní znaménko, nikoli však absolutní hodnotu. Počítejme:

$$(q_1 - q_2 q)a_2 - q_2(a_1 - a_2 q) = q_1 a_2 - q_2 q a_2 - q_2 a_1 + q_2 a_2 q = q_1 a_2 - q_2 a_1 = -(q_2 a_1 - q_1 a_2)$$

Ukážeme: (C) $(q_1 - q_2q)p_2 - q_2(p_1 - p_2q) = -(q_2p_1 - q_1p_2)$, tj. druhá složka třetí dvojice $\times$ první složka druhé dvojice $-$ první složka třetí dvojice $\times$ druhá složka druhé dvojice provedením E_r změní znaménko, nikoli však absolutní hodnotu. Počítejme:

$$(q_1 - q_2q)p_2 - q_2(p_1 - p_2q) = q_1p_2 - q_2qp_2 - q_2p_1 + q_2p_2q = q_1p_2 - q_2p_1 = -(q_2p_1 - q_1p_2)$$

Předpokládejme, že výpočet skončil po n krocích (n krát se aplikovala transformace E_r); může být $n = 0$.

Z (A) dostáváme $u^*d - u \cdot 0 = (-1)^n \cdot (0 \cdot a - 1 \cdot b)$, (A') $u^*d = (-1)^{n+1} \cdot b$.

Z (B) dostáváme $v^*d - v \cdot 0 = (-1)^n \cdot (1 \cdot a - 0 \cdot b)$, (B') $v^*d = (-1)^n \cdot a$.

Z (C) dostáváme: $v^*u - vu^* = (-1)^n(1 \cdot 1 - 0 \cdot 0)$, (C') $v^*u - vu^* = (-1)^n$.

Rovnost (C') teď budeme upravovat:

$$\begin{aligned}
v^*u - vu^* &= (-1)^n \\
(v^*u - vu^*)d &= (-1)^n \cdot d \\
v^*ud - vu^*d &= (-1)^n \cdot d \\
u(v^*d) - v(u^*d) &= (-1)^n \cdot d \text{ (aplikujeme (A'), (B'))} \\
u \cdot (-1)^n \cdot a - v \cdot (-1)^{n+1} \cdot b &= (-1)^n \cdot d \\
u \cdot (-1)^n \cdot a + v \cdot (-1)^{n+2} \cdot b &= (-1)^n \cdot d \\
u \cdot (-1)^n \cdot a + v \cdot (-1)^n \cdot b &= (-1)^n \cdot d \\
(-1)^n(ua + vb) &= (-1)^n \cdot d \\
ua + vb &= d
\end{aligned}$$

9.3.3. Příklad. Pomocí Rozšířeného Eukleidova algoritmu vypočítáme největšího společného dělitele d celých čísel 1971, 1965 a také celá čísla u, v splnující $u \cdot 1971 + v \cdot 1965 = d$.

$$\begin{array}{ccccccc}
(1971, 1965)_1 & \mapsto & (1965, 6)_1 & \mapsto & (6, 3)_1 & \mapsto & (3, 0)_1 \\
(1, 0)_2 & \mapsto & (0, 1)_2 & \mapsto & (1, -327)_2 & \mapsto & (-327, 655)_2 \\
(0, 1)_3 & \mapsto & (1, -1)_3 & \mapsto & (-1, 328)_3 & \mapsto & (328, -657)_3
\end{array}$$

Závěr: $NSD(1971, 1965) = 3$, $-327 \cdot 1971 + 328 \cdot 1965 = 3$.

Proč výpočet proběhl tak, jak je zaznamenáno? První řádek je nám již jasný, je to řádek z Eukleidova algoritmu (viz příklad 9.3.1.). Věnujme se druhému a třetímu řádku. Prvnímu kroku odpovídá dělení se zbytkem $1971 = 1965 \cdot 1 + 6$ a tedy $q = 1$, $(1, 0)_2 \mapsto (0, 1 - 0 \cdot 1)_2 = (0, 1)_2$, $(0, 1)_3 \mapsto (1, 0 - 1 \cdot 1)_3 = (1, -1)_3$. Druhému kroku odpovídá dělení se zbytkem $1965 = 6 \cdot 327 + 3$ a tedy $q = 327$, $(0, 1)_2 \mapsto (1, 0 - 1 \cdot 327)_2 = (1, -327)_2$, $(1, -1)_3 \mapsto (-1, 1 - (-1) \cdot 327)_3 = (-1, 328)_3$. Třetímu kroku odpovídá dělení se zbytkem $6 = 3 \cdot 2 + 0$ a tedy $q = 2$, $(1, -327)_2 \mapsto (-327, 1 - (-327) \cdot 2)_2 = (-327, 655)_2$, $(-1, 328)_3 \mapsto (328, -1 - 328 \cdot 2)_3 = (328, -657)_3$.

9.3.4. Příklad. Pomocí Rozšířeného Eukleidova algoritmu vypočítáme největšího společného dělitele d Gaussových celých čísel $13 + 3i$, $11 + 3i$ a také Gaussova celá čísla u, v splnující $u \cdot (13 + 3i) + v \cdot (11 + 3i) = d$.

$$\begin{array}{ccccccc} (13+3i,11+3i)_1 & \mapsto & (11+3i,2)_1 & \mapsto & (2,1+i)_1 & \mapsto & (1+i,0)_1 \\ (1,0)_2 & \mapsto & (0,1)_2 & \mapsto & (1,-5-i)_2 & \mapsto & (-5-i,7-4i)_2 \\ (0,1)_3 & \mapsto & (1,-1)_3 & \mapsto & (-1,6+i)_3 & \mapsto & (6+i,-8+5i)_3 \end{array}$$

Závěr: $NSD(13+3i,11+3i) = 1+i$, $(-5-i)\cdot(13+3i)+(6+i)\cdot(11+3i) = 1+i$.

Proč výpočet proběhl tak, jak je zaznamenáno? První řádek je nám již jasný, je to řádek z Eukleidova algoritmu (viz příklad 9.3.2.). Věnujme se druhému a třetímu řádku. Prvnímu kroku odpovídá dělení se zbytkem $13+3i = (11+3i)\cdot 1+2$ a tedy $q=1$, $(1,0)_2 \mapsto (0,1-0\cdot 1)_2 = (0,1)_2$, $(0,1)_3 \mapsto (1,0-1\cdot 1)_3 = (1,-1)_3$. Druhému kroku odpovídá dělení se zbytkem $11+3i = 2\cdot(5+i)+(1+i)$ a tedy $q = 5+i$, $(0,1)_2 \mapsto (1,0-1\cdot(5+i))_2 = (1,-5-i)_2$, $(1,-1)_3 \mapsto (-1,1-(-1)\cdot(5+i))_3 = (-1,6+i)_3$. Třetímu kroku odpovídá dělení se zbytkem $2 = (1+i)\cdot(1-i)+0$ a tedy $q = 1-i$, $(1,-5-i)_2 \mapsto (-5-i,1-(-5-i)\cdot(1-i))_2 = (-5-i,7-4i)_2$, $(-1,6+i)_3 \mapsto (6+i,-1-(6+i)\cdot(1-i))_3 = (6+i,-8+5i)_3$.

Cvičení.

1. Pomocí Rozšířeného Eukleidova algoritmu vypočtěte největší společný dělitel d celých čísel 456, 123 a určete celá čísla u, v taková, že $u\cdot 456 + v\cdot 123 = d$.

2. Pomocí Rozšířeného Eukleidova algoritmu vypočtěte největší společný dělitel d Gaussových celých čísel $24+8i$, $18+2i$ a určete Gaussova celá čísla u, v taková, že $u\cdot(24+8i) + v\cdot(18+2i) = d$.

3. Uvažme Eukleidovský obor $\mathbb{Z}_3[x]$ všech polynomů nad tříprvkovým tělesem. Místo $[0]_3$, $[1]_3$, $[2]_3$ pišme stručně 0, 1, 2. Pomocí Rozšířeného Eukleidova algoritmu vypočtěte největší společný dělitel d polynomů $x^5+2x^4+2x^2+1$, x^4+2 a určete polynomy u, v takové, že $u\cdot(x^5+2x^4+2x^2+1) + v\cdot(x^4+2) = d$.

9.4 Jednoznačný rozklad na součin ireducibilních prvků

Jistě víte, že každé celé číslo větší než jedna lze napsat jako součin několika prvočísel. Obdobně lze ukázat, že každé celé číslo n, které není 0 a není jednotka oboru integrity $\mathbb{Z}$, lze zapsat jako součin několika ireducibilních prvků oboru integrity $\mathbb{Z}$. Proč? Víme, že v $\mathbb{Z}$ jsou právě dvě jednotky, a to 1 a -1 (viz cvičení 5 v části 8.1.). Je tedy $n \neq 0$, $n \neq 1$, $n \neq -1$. Pak $|n|$ je celé číslo větší než 1. Existují tedy prvočísla $p_1, p_2, \ldots, p_k$ tak, že $|n| = p_1 p_2 \ldots p_k$. Pro $n > 0$ máme $|n| = n$ a tedy

$$n = p_1 \ldots p_k$$

Pro $n < 0$ máme $|n| = -n$ a tedy

$$-n = p_1 \ldots p_k,\ n = (-p_1)p_2 \ldots p_k$$

Víme, že $p_1, -p_1, p_2, \ldots, p_k$ jsou ireducibilní prvky v $\mathbb{Z}$ (viz 8.3.6.). Tudíž n lze zapsat jsko součin několika ireducibilních prvků oboru integrity $\mathbb{Z}$.

Právě zdůvodněný fakt (každé celé číslo, které není 0 a není jednotka, lze zapsat jako součin několika ireducibilních prvků oboru integrity $\mathbb{Z}$) není specialitou eukleidovského oboru $\mathbb{Z}$, ale platí dokonce v každém eukleidovském oboru.

9.4.1. Tvrzení. *Nechť I je eukleidovský obor. Nechť $a \in I$, $a \neq 0$, $a \notin U(I)$. Pak a lze zapsat jako součin několika ireducibilních prvků oboru I. (Přitom ireducibilní prvek také považujeme za součin několika ireducibilních prvků, totiž jednoho.)*

Důkaz. Nechť $S = \{x \in I;\ x \neq 0, x \notin U(I)\}$. Nechť $T \subseteq S$, T je množina všech prvků z množiny S, které nelze vyjádřit ve tvaru součinu několika ireducibilních prvků oboru integrity I. Chceme: $T = \emptyset$. Postupujme sporem. Předpokládejme, že $T \neq \emptyset$. Nechť $m \in T$, $N(m) \leq N(x)$ pro všechna $x \in T$. Takový prvek existuje, protože $N : I - \{0\} \to \mathbb{N}_0$. Protože $m \in T$, $m \neq 0$, $m \notin U(I)$, m nelze vyjádřit jako součin několika ireducibilních prvků a specielně tedy prvek m není ireducibilní. Existuje tedy $d \in I$, $d|m$, $\neg(d\|1)$, $\neg(d\|m)$. Je $m = de$, kde $e \in I$. Je $m \neq 0$, takže $d \neq 0$, $e \neq 0$. Protože $\neg(d\|1)$, máme $d \notin U(I)$. Takže $d \in S$. Kdyby e byla jednotka, bylo by $d\|m$, což neplatí. Takže $e \notin U(I)$ a $e \in S$. Jelikož $d \neq 0$, $m \neq 0$, $d|m$, $\neg(m|d)$ ($m|d$ by dalo $d\|m$), máme $N(d) < N(m)$ (viz Tvrzení 9.1.6.). Takže $d \in S$, $d \notin T$ ($d \in T$ by dalo $N(m) \leq N(d)$). Předpokládejme, že $m|e$. Pak $e = mf$ pro nějaké $f \in I$ a $m = dmf$, $1 = df$ (v oboru integrity lze krátit nenulovým prvkem), $d \in U(I)$, spor. Nutně tedy $\neg(m|e)$. Máme: $e \neq 0$, $m \neq 0$, $e|m$, $\neg(m|e)$. Dle 9.1.6. pak $N(e) < N(m)$. Takže $e \in S$, $e \notin T$ ($e \in T$ by dalo $N(m) \leq N(e)$). Protože $d \in S$, $d \notin T$, existují ireducibilní prvky $p_1, \ldots, p_k$ oboru integrity I tak, že $d = p_1 \cdots p_k$. Protože $e \in S$, $e \notin T$, existují ireducibilní prvky $q_1, \ldots, q_l$ oboru integrity I tak, že $e = q_1 \cdots q_l$. Pak $m = p_1 \cdots p_k q_1 \cdots q_l$, m lze vyjádřit jako součin několika ireducibilních prvků, spor.

Ukázali jsme, že každý nenulový prvek eukleidovského oboru, který není jednotkou tohoto oboru, lze zapsat jako součin několika ireducibilních prvků. Platí dokonce víc – tento rozklad je jednoznačný. Řeknete si možná, že to přece není pravda, například v eukleidovském oboru $\mathbb{Z}$ je $6 = 2 \cdot 3$ a také $6 = 3 \cdot 2$. Vzhledem k tomu, že eukleidovský obor je komutativní, nelze požadovat jednoznačnost absolutní. Takže to opravíme: rozklad na součin ireducibilních prvků je jednoznačný až na pořadí činitelů (tj. dva rozklady lišící se pouze pořadím činitelů považujeme za rozklad jeden). Takovou jednoznačnost však také nedokážeme zaručit: máme nejen $6 = 2 \cdot 3$, ale také $6 = (-2) \cdot (-3)$. Přece však jsou rozklady $6 = 2 \cdot 3$ a $6 = (-2) \cdot (-3)$ hodně podobné, totiž $2\| - 2$ a $3\| - 3$.

9.4.2. Tvrzení. *Nechť I je eukleidovský obor. Nechť k, l jsou kladná celá čísla, $p_1, \ldots, p_k$ a také $q_1, \ldots, q_l$ jsou ireducibilní prvky oboru I. Nechť*

$$p_1 \cdots p_k = q_1 \cdots q_l$$

Pak $k = l$ a existuje permutace π množiny $\{1, \ldots, k\}$ taková, že

$$p_1 \| q_{\pi(1)} \ \wedge \cdots \wedge \ p_k \| q_{\pi(k)}$$

Důkaz. Všimněme si nejprve, že pokud p, q jsou ireducibilní prvky a $p|q$, pak $p\|q$. Zdůvodnění: Protože q je ireducibilní, máme $p\|1$ nebo $p\|q$. Ovšem $p\|1$ by znamenalo, že p je jednotka, což by byl spor – ireducibilní prvek dle definice není jednotka. Nutně tedy $p\|q$. Konec zdůvodnění. Je $k \leq l$ nebo $l \leq k$. Nechť například $k \leq l$. Vidíme, že $p_1|q_1 \cdots q_l$. Dle 9.1.4. (viz také cvičení 2 v části 9.1) existuje $j_1 \in \{1, \ldots, l\}$, $p_1|q_{j_1}$. Prvky p_1 a q_{j_1} jsou ireduciblní, takže $p_1\|q_{j_1}$. Pak existuje jednotka u_1 tak, že $q_{j_1} = u_1 p_1$. Počítejme:

$$\begin{aligned} p_1 p_2 \cdots p_k &= q_1 \cdots q_{j_1-1} q_{j_1} q_{j_1+1} \cdots q_l \\ p_1 p_2 \cdots p_k &= q_1 \cdots q_{j_1-1} u_1 p_1 q_{j_1+1} \cdots q_l \\ p_2 \cdots p_k &= q_1 \cdots q_{j_1-1} u_1 q_{j_1+1} \cdots q_l \\ p_2 \cdots p_k &= u_1 q_1 \cdots q_{j_1-1} q_{j_1+1} \cdots q_l \end{aligned}$$

Vidíme, že $p_2|u_1 q_1 \cdots q_{j_1-1} q_{j_1+1} \cdots q_l$. Dle 9.1.4. $p_2|u_1$ nebo $p_2|q_{j_2}$ pro nějaké $j_2 \in \{1, \ldots, l\}$, $j_2 \neq j_1$. Ovšem $p_2|u_1$ by dalo $p_2|1$, p_2 je jednotka, což by byl spor. Takže $\neg(p_2|u_1)$ a $p_2|q_{j_2}$ pro nějaké $j_2 \in \{1, \ldots, l\}$, $j_2 \neq j_1$. Pak $p_2\|q_{j_2}$, $q_{j_2} = u_2 p_2$ pro nějakou jednotku u_2. Počítejme:

$$\begin{aligned} p_2 p_3 \cdots p_k &= u_1 q_1 \cdots q_{j_1-1} q_{j_1+1} \cdots q_l \\ p_2 p_3 \cdots p_k &= u_1 \prod_{j \in \{1,\ldots,l\}, j \neq j_1} q_j \\ p_2 p_3 \cdots p_k &= u_1 q_{j_2} \prod_{j \in \{1,\ldots,l\}, j \neq j_1, j \neq j_2} q_j \\ p_2 p_3 \cdots p_k &= u_1 u_2 p_2 \prod_{j \in \{1,\ldots,l\}, j \neq j_1, j \neq j_2} q_j \\ p_3 \cdots p_k &= u_1 u_2 \prod_{j \in \{1,\ldots,l\}, j \neq j_1, j \neq j_2} q_j \end{aligned}$$

Vidíme, že $p_3|u_1 u_2 \prod_{j \in \{1,\ldots,l\}, j \neq j_1, j \neq j_2} q_j$. Dle 9.1.4. $p_3|u_1$ nebo $p_3|u_2$ nebo $p_3|q_{j_3}$ pro nějaké $j_3 \in \{1, \ldots, l\}$, $j_3 \neq j_1$, $j_3 \neq j_2$. Ovšem p_3 je ireducibilní prvek a u_1, u_2 jsou jednotky, takže $\neg(p_3|u_1)$, $\neg(p_3|u_2)$ a $p_3|q_{j_3}$ pro nějaké $j_3 \in \{1, \ldots, l\}$, $j_3 \neq j_1$, $j_3 \neq j_2$. Pak $p_3\|q_{j_3}$, $q_{j_3} = u_3 p_3$ pro nějakou jednotku u_3. Počítejme:

$$\begin{aligned} p_3 p_4 \cdots p_k &= u_1 u_2 \prod_{j \in \{1,\ldots,l\}, j \neq j_1, j \neq j_2} q_j \\ p_3 p_4 \cdots p_k &= u_1 u_2 u_3 p_3 \prod_{j \in \{1,\ldots,l\}, j \neq j_1, j \neq j_2, j \neq j_3} q_j \\ p_4 \cdots p_k &= u_1 u_2 u_3 \prod_{j \in \{1,\ldots,l\}, j \neq j_1, j \neq j_2, j \neq j_3} q_j \end{aligned}$$

Z poslední rovnosti plyne, že existuje $j_4 \in \{1,\dots,l\}$, $j_4 \neq j_1$, $j_4 \neq j_2$, $j_4 \neq j_3$, $p_4 \| q_{j_4}$, $q_{j_4} = u_4 p_4$, $u_4 \in U(I)$. Atd.

Po k krocích nakonec zjistíme: Existují $j_1,\dots,j_k \in \{1,\dots,l\}$, $j_1,\dots,j_k$ vzájemně různá, $u_1,\dots,u_k \in U(I)$, přičemž $p_s \| q_{j_s}$, $q_{j_s} = u_s p_s$ pro $s = 1,\dots,k$. Pak

$$\begin{aligned} p_1 \cdots p_k &= q_{j_1} \cdots q_{j_k} \prod_{j \in \{1,\dots,l\} - \{j_1,\dots,j_k\}} q_j \\ p_1 \cdots p_k &= u_1 p_1 \cdots u_k p_k \prod_{j \in \{1,\dots,l\} - \{j_1,\dots,j_k\}} q_j \\ p_1 \cdots p_k &= u_1 \cdots u_k p_1 \cdots p_k \prod_{j \in \{1,\dots,l\} - \{j_1,\dots,j_k\}} q_j \\ 1 &= u_1 \cdots u_k \prod_{j \in \{1,\dots,l\} - \{j_1,\dots,j_k\}} q_j \end{aligned}$$

Předpokládejme, že $k \neq l$. Pak $k < l$, $\{1,\dots,l\} - \{j_1,\dots,j_k\} \neq \emptyset$. Zvolme $j_0 \in \{1,\dots,l\} - \{j_1,\dots,j_k\}$. Z rovnosti

$$1 = u_1 \cdots u_k \prod_{j \in \{1,\dots,l\} - \{j_1,\dots,j_k\}} q_j$$

plyne, že $q_{j_0} | 1$. Pak q_{j_0} je jednotka, spor (uvědomte si, že prvek q_{j_0} je ireducibilní). Nutně tedy $k = l$.

Nyní stačí pro $s \in \{1,\dots,k\}$ položit $\pi(s) = j_s$. Je π permutace množiny $\{1,\dots,k\}$, jelikož $j_1,\dots,j_k \in \{1,\dots,k\}$, $j_1,\dots,j_k$ jsou vzájemně různá čísla. Na závěr si uvědomte, že $p_s \| q_{j_s}$, $p_s \| q_{\pi(s)}$ pro $s = 1,\dots,k$.

Všimněte si, že pro důkaz tvrzení 9.4.2. je podstatný důsledek 9.1.4., tj. důsledek věty 9.1.2.

Tvrzení 9.4.1. a 9.4.2. můžeme shrnout do následující věty:

9.4.3. Věta. *V eukleidovském oboru má každý nenulový prvek, který není jednotkou, jednoznačný rozklad na součin ireducibilních prvků. Jednoznačností rozkladu rozumíme jednoznačnost až na pořadí a asociovanost.*

Cvičení.

1. Uvažme obor integrity $\mathbb{Z}[\sqrt{-5}]$ – zabývali jsme se jím v příkladech 8.2.4. a také 9.1.5. Je $9 = 3 \cdot 3 = (2+\sqrt{-5}) \cdot (2-\sqrt{-5})$. Ukažte, že prvky 3, $2+\sqrt{-5}$, $2-\sqrt{-5}$ jsou ireducibilní v $\mathbb{Z}[\sqrt{-5}]$ a přitom číslo 3 není asociováno s $2+\sqrt{-5}$ ani není asociováno s $2-\sqrt{-5}$. Dále ukažte, že 9 není jednotka v $\mathbb{Z}[\sqrt{-5}]$. V oboru integrity $\mathbb{Z}[\sqrt{-5}]$ tedy neplatí, že každý nenulový prvek, který není jednotkou, má jednoznačný rozklad na součin irducibilních prvků.

9.5 Základní věta aritmetiky

Základním poznatkem teorie čísel je fakt, že každé celé číslo větší než jedna lze jednoznačně vyjádřit jako součin několika prvočísel. Uvidíme, že se jedná o důsledek věty 9.4.3.

9.5.1. Věta. (**Základní věta aritmetiky**) *Nechť n je celé číslo, $n > 1$. Pak existují prvočísla $p_1, p_2, \ldots, p_k$ splňující*

$$n = p_1 p_2 \cdots p_k$$

Toto vyjádření je jednoznačné až na pořadí činitelů.

Důkaz. Využijeme toho, že $\mathbb{Z}$ je eukleidovský obor. Připomeňme si, že $U(\mathbb{Z}) = \{1, -1\}$. Nechť $n \in \mathbb{Z}$, $n > 1$. Tvrzení 9.4.1. dává: existují ireducibilní prvky $q_1, \ldots, q_k \in \mathbb{Z}$, $n = q_1 \cdots q_k$. Z 8.3.6. dostáváme: pro $i = 1, \ldots, k$ je $q_i = \varepsilon_i p_i$, kde p_i je prvočíslo, $\varepsilon_i \in \{1, -1\}$. Pak $n = \varepsilon_1 \cdots \varepsilon_k p_1 \cdots p_k$. Protože $n > 0$, $p_i > 0$ pro $i = 1, \ldots, k$, je $\varepsilon_1 \cdots \varepsilon_k > 0$ a tedy $\varepsilon_1 \cdots \varepsilon_k = 1$. Takže $n = p_1 \cdots p_k$.

Nechť nyní $u_1, \ldots, u_k$, $v_1, \ldots, v_l$ jsou prvočísla, $n = u_1 \cdots u_k$, $n = v_1 \cdots v_l$. Chceme: $k = l$, existuje permutace π množiny $\{1, \ldots, k\}$ tak, že $u_s = v_{\pi(s)}$ pro $s = 1, \ldots, k$.

Podle 8.3.6. jsou $u_1, \ldots, u_k$, $v_1, \ldots, v_l$ ireducibilní prvky v $\mathbb{Z}$. Z 9.4.2. dostáváme: $k = l$, existuje permutace π množiny $\{1, \ldots, k\}$, $u_s \| v_{\pi(s)}$ pro $s = 1, \ldots, k$. Stačí si uvědomit toto: Jestliže p, q jsou prvočísla, $p \| q$, pak $p = q$. Proč to tak je? $p \| q$ znamená, že $p = iq$, kde $i \in U(\mathbb{Z})$, takže $p = q$ nebo $p = -q$. Protože $p > 0$, $q > 0$, musí být $p = q$.

Cvičení.

1. Najděte prvočíselný rozklad čísla 1234567890.

9.6 Čínská věta o zbytcích

Zformulujeme nyní Čínskou větu o zbytcích, která patří mezi základní věty teorie čísel.

9.6.1. Věta. (**Čínská věta o zbytcích**) *Nechť $m_1, \ldots, m_k$ jsou kladná celá čísla, která jsou po dvou nesoudělná (tj. $m_i \perp m_j$ pro všechna $i, j \in \{1, \ldots, k\}$, $i \neq j$). Nechť $a_1, \ldots, a_k$ jsou libovolná celá čísla. Uvažme následující systém kongruencí v $\mathbb{Z}$:*

$$(S) \begin{cases} x & \equiv & a_1 & (m_1) \\ & \vdots & & \\ x & \equiv & a_k & (m_k) \end{cases}$$

Platí:

1. *Systém (S) má řešení v $\mathbb{Z}$.*

2. *Buď $M = m_1 \cdots m_k$. Nechť x_0 je celé číslo, které je řešením sytému (S). Pak pro všechna celá čísla x_1 platí:*

$$x_1 \text{ je řešením systému } (S) \text{ právě tehdy, když } x_1 \equiv x_0 \ (M)$$

Zájemci si mohou o Čínské větě o zbytcích přečíst například v učebnici [5] – tam je větě věnována kapitolka 3.5. na stranách 21 až 23.

Zformulujeme teď a dokážeme Čínskou větu o zbytcích pro libovolný eukleidovský obor. Věta 9.6.1. pak bude jejím důsledkem. Pro jednoduchost se v zobecněné Čínské větě o zbytcích omezíme na případ $k = 2$, tedy na systémy dvou kongruencí.

9.6.2. Věta. (**Čínská věta o zbytcích**) *Nechť I je eukleidovský obor. Nechť $m_1, m_2 \in I$, $m_1 \neq 0$, $m_2 \neq 0$, $m_1 \perp m_2$. Nechť $a_1, a_2 \in I$. Uvažme následující systém kongruencí v I:*

$$(S') \begin{cases} x & \equiv & a_1 & (m_1) \\ x & \equiv & a_2 & (m_2) \end{cases}$$

Platí:

1. *Systém (S') má řešení v I.*
2. *Buď $M = m_1 m_2$. Nechť $x_0 \in I$, x_0 je řešením sytému (S'). Pak pro všechna $x_1 \in I$ platí:*

$$x_1 \text{ je řešením systému } (S') \text{ právě tehdy, když } x_1 \equiv x_0 \ (M)$$

Důkaz.

1. Protože $m_1 \perp m_2$, je $NSD(m_1, m_2) = 1$ (viz 8.2.6.). Dle věty 9.1.2. existují $u, v \in I$, $um_1 + vm_2 = 1$ (Bézoutova rovnost). Položme $x_0 = a_1 v m_2 + a_2 u m_1$. Ukážeme, že x_0 je řešení systému (S').

   Všimněme si nejprve, že $um_1 = 1 - vm_2$, takže $m_1 | 1 - vm_2$, $vm_2 \equiv 1 \ (m_1)$. Dále $vm_2 = 1 - um_1$, takže $m_2 | 1 - um_1$, $um_1 \equiv 1 \ (m_2)$.

   Je $x_0 - a_1 v m_2 = a_2 u m_1$, takže $m_1 | x_0 - a_1 v m_2$ a $x_0 \equiv a_1 v m_2 \ (m_1)$. Z $vm_2 \equiv 1 \ (m_1)$ dostáváme $a_1 v m_2 \equiv a_1 \cdot 1 \ (m_1)$, $a_1 v m_2 \equiv a_1 \ (m_1)$. Celkem $x_0 \equiv a_1 v m_2 \ (m_1)$ a $a_1 v m_2 \equiv a_1 \ (m_1)$, což dává $x_0 \equiv a_1 \ (m_1)$. Ukázali jsme, že x_0 vyhovuje první kongruenci systému (S').

   Je $x_0 - a_2 u m_1 = a_1 v m_2$, takže $m_2 | x_0 - a_2 u m_1$ a $x_0 \equiv a_2 u m_1 \ (m_2)$. Z $um_1 \equiv 1 \ (m_2)$ dostáváme $a_2 u m_1 \equiv a_2 \cdot 1 \ (m_2)$, $a_2 u m_1 \equiv a_2 \ (m_2)$. Celkem $x_0 \equiv a_2 u m_1 \ (m_2)$ a $a_2 u m_1 \equiv a_2 \ (m_2)$, což dává $x_0 \equiv a_2 \ (m_2)$. Ukázali jsme, že x_0 vyhovuje druhé kongruenci systému (S').

2. Nechť $M = m_1 m_2$. Předpokládejme, že $x_0 \in I$, x_0 je řešením systému (S'). Nechť $x_1 \in I$. Chceme:

$$x_1 \text{ je řešením systému } (S') \text{ právě tehdy, když } x_1 \equiv x_0 \ (M)$$

Předpokládejme nejprve, že x_1 je řešením systému (S'). Chceme: $x_1 \equiv x_0 \ (M)$. Je $x_0 \equiv a_1 \ (m_1)$, $x_1 \equiv a_1 \ (m_1)$, což dává $x_1 \equiv x_0 \ (m_1)$, $m_1 | x_0 - x_1$. Obdobně $x_0 \equiv a_2 \ (m_2)$, $x_1 \equiv a_2 \ (m_2)$, což dává $x_1 \equiv x_0 \ (m_2)$, $m_2 | x_0 - x_1$. Protože $m_1 | x_0 - x_1$, je $x_0 - x_1 = m_1 s$ pro nějaké $s \in I$. Takže $m_2 | m_1 s$ a připomeňme, že $m_1 \perp m_2$. Dle důsledku 9.1.3. pak $m_2 | s$. Z toho máme $s = m_2 t$ pro nějaké $t \in I$, $x_0 - x_1 = m_1 m_2 t$, $x_0 - x_1 = Mt$, $M | x_0 - x_1$, $x_1 \equiv x_0 \ (M)$.

Nyní naopak předpokládejme, že $x_1 \equiv x_0 \ (M)$. Chceme: x_1 je řešením systému (S'). Z $x_1 \equiv x_0 \ (M)$ dostáváme $M | x_0 - x_1$. Ovšem $m_1 | M$ a proto $m_1 | x_0 - x_1$, $x_1 \equiv x_0 \ (m_1)$. Jelikož x_0 je řešení systému (S'), máme $x_0 \equiv a_1 \ (m_1)$. Celkem $x_1 \equiv x_0 \ (m_1)$, $x_0 \equiv a_1 \ (m_1)$ a tedy $x_1 \equiv a_1 \ (m_1)$. Také $m_2 | M$ a proto $m_2 | x_0 - x_1$, $x_1 \equiv x_0 \ (m_2)$. Jelikož x_0 je řešení systému (S'), máme $x_0 \equiv a_2 \ (m_2)$. Celkem $x_1 \equiv x_0 \ (m_2)$, $x_0 \equiv a_2 \ (m_2)$ a tedy $x_1 \equiv a_2 \ (m_2)$.

9.6.3. Poznámka. Důkaz věty 9.6.2. dává návod, jak získat počáteční řešení x_0 systému (S'): Určíme $u, v \in I$ taková, že $um_1 + vm_2 = NSD(m_1, m_2) = 1$. Pak vezmeme $x_0 = a_1 v m_2 + a_2 u m_1$. Důležité je, že pro určení u, v můžeme použít Rozšířený Eukleidův algoritmus (je popsán v části 9.3).

Je také dobré si všimnout, že u, v nezávisí na a_1, a_2 – k jejich určení potřebujeme znát pouze m_1, m_2. Jestliže tedy v soustavě (S') jenom vyměníme a_1 za b_1 a a_2 za b_2 (kde $b_1, b_2 \in I$), pak při určení počátečního řešení nemusíme znovu počítat u a v, postačí pouze místo $a_1 v m_2 + a_2 u m_1$ vzít $b_1 v m_2 + b_2 u m_1$.

9.6.4. Příklad. V $\mathbb{Z}$ najděte všechna řešení následujícího systému kongruencí:

$$(S_1) \begin{cases} x & \equiv & 10 & (11) \\ x & \equiv & 12 & (13) \end{cases}$$

Řešení: Máme $a_1 = 10$, $a_2 = 12$, $m_1 = 11$, $m_2 = 13$, $M = m_1 m_2 = 11 \cdot 13 = 143$. Určíme počáteční řešení x_0 soustavy (S_1). Nejprve najdeme celá čísla u, v taková, že $um_1 + vm_2 = NSD(m_1, m_2)$, tj. $u \cdot 11 + v \cdot 13 = NSD(11, 13) = 1$. Použijeme Rozšířený Eukleidův algoritmus:

$$\begin{array}{ccccccccc} (11,13)_1 & \mapsto & (13,11)_1 & \mapsto & (11,2)_1 & \mapsto & (2,1)_1 & \mapsto & (1,0)_1 \\ (1,0)_2 & \mapsto & (0,1)_2 & \mapsto & (1,-1)_2 & \mapsto & (-1,6)_2 & \mapsto & (6,-13)_2 \\ (0,1)_3 & \mapsto & (1,0)_3 & \mapsto & (0,1)_3 & \mapsto & (1,-5)_3 & \mapsto & (-5,11)_3 \end{array}$$

Je tedy $u = 6$, $v = -5$ a $x_0 = a_1 v m_2 + a_2 u m_1 = 10 \cdot (-5) \cdot 13 + 12 \cdot 6 \cdot 11 = 142$.
Závěr: Pro $x_1 \in \mathbb{Z}$ platí:

x_1 řeší soustavu (S_1) právě tehdy, když $x_1 \equiv 142\ (143)$

9.6.5. Příklad. V $\mathbb{Z}$ najděte nejmenší nezáporné řešení následujícího systému kongruencí:

$$(S_2)\left\{\begin{array}{rcll} x & \equiv & 1903 & (11) \\ x & \equiv & 1931 & (13) \end{array}\right.$$

Všimněme si, že v soustavě (S_2) jsou stejné moduly m_1, m_2 jako v soustavě (S_1) v předchozím příkladě. To nám usnadní další výpočet. Pokud vám to není jasné, přečtěte si poznámku 9.6.3. Lze totiž vzít hodnoty u, v z předchozího příkladu, tj. $u = 6$ a $v = -5$. Počáteční řešení soustavy (S_2) pak bude $1903 \cdot (-5) \cdot 13 + 1931 \cdot 6 \cdot 11 = 3751$. Pro $x_1 \in \mathbb{Z}$ platí:

$$x_1 \text{ řeší soustavu } (S_2) \text{ právě tehdy, když } x_1 \equiv 3751\ (143)$$

Víme, že $x_1 \equiv 3751\ (143)$ znamená $x_1 - 3751 = k \cdot 143$ pro nějaké $k \in \mathbb{Z}$, tj. $x_1 = k \cdot 143 + 3751$ pro nějaké $k \in \mathbb{Z}$.

Řešení x_1 je nezáporné právě tehdy, když $k \cdot 143 + 3751 \geq 0$, tj. $k \geq \frac{-3751}{143}$. Nejmenší nezáporné řešení soustavy (S_2) dostáváme pro $k = \left\lceil \frac{-3751}{143} \right\rceil$, $k = -26$. Je $-26 \cdot 143 + 3751 = 33$.

Závěr: Nejmenším nezáporným řešením systému kongruencí (S_2) je celé číslo 33.

Cvičení.

1. V $\mathbb{Z}$ najděte všechna řešení následujícího systému kongruencí:

$$\begin{array}{rcll} x & \equiv & 17 & (14) \\ x & \equiv & 10 & (15) \end{array}$$

2. V $\mathbb{Z}$ najděte nejmenší nezáporné řešení následujícího systému kongruencí:

$$\begin{array}{rcll} x & \equiv & 10 & (14) \\ x & \equiv & 7 & (15) \end{array}$$

3. V $\mathbb{Z}[i]$ najděte všechna řešení následujícího systému kongruencí:

$$\begin{array}{rcll} x & \equiv & 5 - 6i & (-1 + 2i) \\ x & \equiv & 7 + 8i & (3 - 4i) \end{array}$$

10 Gaussovské obory

Volně řečeno, gaussovské obory jsou obory integrity, v nichž každý nenulový prvek, který není jednotkou, má jednoznačný rozklad na součin ireducibilních prvků.

10.1 Definice gaussovského oboru

10.1.1. Definice. Nechť I je obor integrity s jednotkovým prvkem. Pak I se nazývá **gaussovský obor**, pokud platí:

1. Nechť $a \in I$, $a \neq 0$, $a \notin U(I)$. Pak a lze zapsat jako součin několika ireducibilních prvků oboru I. (Přitom ireducibilní prvek také považujeme za součin několika ireducibilních prvků, totiž jednoho.)

2. Nechť k, l jsou kladná celá čísla, $p_1, \ldots, p_k$ a také $q_1, \ldots, q_l$ jsou ireducibilní prvky oboru I. Nechť
$$p_1 \cdots p_k = q_1 \cdots q_l$$
Pak $k = l$ a existuje permutace π množiny $\{1, \ldots, k\}$ taková, že
$$p_1 \| q_{\pi(1)} \ \wedge \cdots \wedge \ p_k \| q_{\pi(k)}$$

10.2 Příklady gaussovských oborů

Z definice 10.1.1. a z věty 9.4.3. (případně z tvrzení 9.4.1. a 9.4.2.) je ihned vidět, že každý eukleidovský obor je také gaussovský obor. Otázkou je, zda existují gaussovské obory, které nejsou eukleidovské. Za chvíli uvidíme, že existují (a uvidíme také konkrétní příklad).

Připomeňme, že $\mathbb{Z}[x]$ označuje obor integrity všech polynomů s celočíselnými koeficienty.

10.2.1. Věta. *Obor integrity $\mathbb{Z}[x]$ je gaussovský obor.*

Úkol. Prostudujte paragraf 3 Dělitelnost v $\mathbb{Z}[x]$ na stranách 160 – 167 v knize [1]. Mimo jiné tam najdete důkaz věty 10.2.1. a také pár cvičení.

Alternativně můžete prostudovat část 9.1. Gaussovo lemma v učebnici [5] (strany 45 – 47).

10.2.2. Příklad. $\mathbb{Z}[x]$ je gaussovský obor, který není eukleidovský.

Zdůvodnění: Věta 10.2.1. říká, že obor integrity $\mathbb{Z}[x]$ je gaussovský.

Předpokládejme, že $\mathbb{Z}[x]$ je eukleidovský obor. Položme $f = x$, $g = 2$. Zřejmě f a g jsou polynomy s celočíselnými koeficienty.

Ukážeme teď, že $f \perp g$. Nechť d je polynom s celočíselnými koeficienty, $d|f$, $d|g$. Chceme: $d \| 1$. Protože $d|g$, existuje $e \in \mathbb{Z}[x]$, $g = de$. Je $g \neq 0$, takže také $d \neq 0$, $e \neq 0$. Máme $deg(g) = deg(de)$, $0 = deg(d) + deg(e)$. Z toho plyne, že $deg(d) = deg(e) = 0$. Jsou tedy d, e celá čísla splňující $2 = de$. Tudíž $d \in \{1, -1, 2, -2\}$. Uvažme libovolný polynom $h \in \mathbb{Z}[x]$. Polynomy $2h$ a $-2h$ mají všechny koeficienty sudé. Proto $2h \neq f$, $-2h \neq f$, $\neg(2|f)$, $\neg(-2|f)$. Nutně tedy $d \in \{1, -1\}$ a $d \| 1$.

Jelikož $f \perp g$, je $NSD(f, g) = 1$ (viz 8.2.6.). Z předpokladu, že $\mathbb{Z}[x]$ je eukleidovský obor, dostáváme: $uf + vg = 1$ pro nějaké polynomy $u, v \in \mathbb{Z}[x]$ (Bézoutova rovnost, 9.1.2.). Tudíž $ux + v \cdot 2 = 1$. Porovnáním absolutních členů (připomínka: absolutní člen polynomu je koeficient u x^0) dostaneme $2v_0 = 1$, kde v_0 je absolutní člen polynomu v. Je tedy číslo 1 sudé, spor.

Ke sporu vedl předpoklad, že $\mathbb{Z}[x]$ je eukleidovský obor. Tudíž obor integrity $\mathbb{Z}[x]$ není eukleidovský.

Cvičení.

1. Gaussova věta říká: *Buď I gaussovský obor. Pak $I[x]$ je také gaussovský obor.* Najděte v literatuře důkaz této věty.

10.3 Největší společný dělitel prvků gaussovského oboru

Když jste chodili do školy, tak jste největší společný dělitel čísel $a = 2^1 \cdot 3^9 \cdot 5^6$ a $b = 2^{10} \cdot 3^4 \cdot 5^7$ počítali (pravděpodobně) takto:

$$NSD(a,b) = NSD(2^1 \cdot 3^9 \cdot 5^6, 2^{10} \cdot 3^4 \cdot 5^7) = 2^{\min(1,10)} \cdot 3^{\min(9,4)} \cdot 5^{\min(6,7)} = 2^1 \cdot 3^4 \cdot 5^6$$

Ze Základní věty aritmetiky (Věta 9.5.1.) plyne, že obdobně lze spočítat největší společný dělitel libovolných dvou celých čísel a, b, $a > 1$, $b > 1$ (pokud ovšem známe či jsme schopni určit jejich prvočíselný rozklad).

No a obdobně lze určit největší společný dělitel dvou prvků a, b ($a \neq 0$, $b \neq 0$, a není jednotka, b není jednotka) v libovolném gaussovském oboru, a to díky existenci jednoznačného rozkladu prvku a a také prvku b na součin ireducibilních prvků.

Nyní tuto záležitost prozkoumáme podrobněji.

Připomeňme si tradiční značení: Jestliže I je obor integrity, $a \in I$, n je kladné celé číslo, pak

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

Dále klademe $a^0 = 1$. Není obtížné dokázat, že pro všechna nezáporná celá čísla k, l je

$$a^k a^l = a^{k+l}$$

(proveďte důkaz jako cvičení).

10.3.1. Tvrzení. *Nechť I je gaussovský obor. Nechť $a \in I$, $a = p_1^{n_1} \cdots p_k^{n_k}$, kde k je kladné celé číslo, $p_1, \ldots, p_k$ jsou navzájem neasociované ireducibilní prvky oboru I (tj. $\neg(p_i \| p_j)$ pro všechna $i, j \in \{1, \ldots, k\}$, $i \neq j$), $n_1, \ldots, n_k$ jsou nezáporná celá čísla. Pak pro všechna $d \in I$ platí:*

$$d|a \iff d = s p_1^{u_1} \cdots p_k^{u_k}$$

pro nějaká $s \in U(I)$, $u_i \in \mathbb{Z}$, $0 \leq u_i \leq n_i$ pro $i = 1, \ldots, k$.

Důkaz.
$\Rightarrow$: Existuje $e \in I$, $a = de$. Protože $a \neq 0$, máme $d \neq 0$, $e \neq 0$. Pokud d je jednotka, položíme $s = d$, $u_i = 0$ pro $i = 1, \ldots, k$. Pokud e je jednotka, existuje jednotka f, $ef = 1$. Pak $af = def$,

$fa = d \cdot 1$, $fp_1^{n_1} \cdots p_k^{n_k} = d$ a položíme $s = f$, $u_i = n_i$ pro $i = 1, \ldots, k$. Nechť nyní d, e nejsou jednotky. Existují ireducibilní prvky $q_1, \ldots, q_l \in I$, $r_1, \ldots, r_m \in I$, $d = q_1 \cdots q_l$, $e = r_1 \cdots r_m$. Pak

$$p_1^{n_1} \cdots p_k^{n_k} = q_1 \cdots q_l r_1 \cdots r_m$$

Protože jsme v gaussovském oboru, je $n_1 + \cdots + n_k = l + m$ a existují $j_1, \ldots, j_l \in \{1, \ldots, k\}$ taková, že $q_1 \| p_{j_1}, \ldots, q_l \| p_{j_l}$. Pak $q_1 = s_1 p_{j_1}, \ldots, q_l = s_l p_{j_l}$ pro nějaké jednotky $s_1, \ldots, s_l$. Dostáváme

$$d = q_1 \cdots q_l = s_1 p_{j_1} \cdots s_l p_{j_l} = s_1 \cdots s_l p_{j_1} \cdots p_{j_l}$$

Položme $s = s_1 \cdots s_l$. Jelikož $s_1, \ldots, s_l$ jsou jednotky v I, je také s jednotka v oboru I. Dále $p_{j_1} \cdots p_{j_l} = p_1^{u_1} \cdots p_k^{u_k}$ pro nějaká nezáporná celá čísla $u_1, \ldots, u_k$. Vidíme, že

$$d = s p_1^{u_1} \cdots p_k^{u_k}$$

Zbývá ukázat, že $u_i \leq n_i$ pro $i = 1, \ldots, k$. Předpokládejme naopak, že pro nějaké $i \in \{1, \ldots, k\}$ je $u_i > n_i$. Máme

$$\begin{aligned} a &= de \\ p_1^{n_1} \cdots p_k^{n_k} &= s p_1^{u_1} \cdots p_k^{u_k} e \end{aligned}$$

V poslední rovnosti budeme krátit prvkem $p_i^{n_i}$ – to lze, protože jsme v oboru integrity I a $p_i \neq 0$ (je totiž p_i ireducibilní prvek). Pro $k = 1$ je také $i = 1$ a dostáváme $1 = s p_1^{u_1 - n_1} e$; jelikož $u_1 - n_1 > 0$, máme $p_1 | 1$, p_1 je jednotka, spor (připomínám, že p_1 je ireducibilní prvek). Nechť nyní $k > 1$. Po krácení dostáváme

$$\begin{aligned} p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k} &= s p_1^{u_1} \cdots p_{i-1}^{u_{i-1}} p_i^{u_i - n_i} p_{i+1}^{u_{i+1}} \cdots p_k^{u_k} e \\ p_1^{n_1} \cdots p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdots p_k^{n_k} &= p_1^{u_1} \cdots p_{i-1}^{u_{i-1}} (s p_i) p_i^{u_i - n_i - 1} p_{i+1}^{u_{i+1}} \cdots p_k^{u_k} r_1 \cdots r_m \end{aligned}$$

Jelikož s je jednotka, je $sp_i \| p_i$ a prvek sp_i je také ireducibilní (viz 8.3.3.). Poslední rovnost dává (díky tomu, že jsme v gaussovském oboru): $sp_i \| p_j$ pro nějaké $j \in \{1, \cdots, k\} - \{i\}$. Pak také $p_i \| p_j$. To je však spor, protože prvky $p_1, \ldots, p_k$ jsou navzájem neasociované. Spor jsme dostali pro $k = 1$ i $k > 1$. Nutně tedy $u_i \leq n_i$ pro $i = 1, \ldots, k$.
$\Leftarrow$: Pro všechna $i = 1, \ldots, k$ existuje nezáporné celé číslo v_i takové, že $u_i + v_i = n_i$. Jelikož s je jednotka, existuje $t \in I$, $st = 1$. Položme $e = t p_1^{v_1} \cdots p_k^{v_k}$. Platí:

$$de = s p_1^{u_1} \cdots p_k^{u_k} t p_1^{v_1} \cdots p_k^{v_k} = st p_1^{u_1 + v_1} \cdots p_k^{u_k + v_k} = 1 \cdot p_1^{n_1} \cdots p_k^{n_k} = p_1^{n_1} \cdots p_k^{n_k} = a$$

Vidíme, že $de = a$, $d | a$.

10.3.2. Tvrzení. *Nechť I je gaussovský obor. Nechť k je kladné celé číslo, $p_1, \ldots, p_k$ jsou navzájem neasociované ireducibilní prvky oboru integrity I. Nechť $s, t \in U(I)$, $u_1, \ldots, u_k, v_1, \ldots, v_k$ jsou nezáporná celá čísla. Platí:*

$$s p_1^{u_1} \cdots p_k^{u_k} = t p_1^{v_1} \cdots p_k^{v_k} \Longrightarrow s = t \ \wedge \ u_1 = v_1 \ \wedge \cdots \wedge u_k = v_k$$

Důkaz. Nechť $sp_1^{u_1}\cdots p_k^{u_k} = tp_1^{v_1}\cdots p_k^{v_k}$. Buď $i \in \{1,\ldots,k\}$. Chceme: $u_i = v_i$.
Předpokládejme, že $u_i \neq v_i$. Nechť například $u_i < v_i$. Jestliže $k = 1$, je $i = 1$ a po krácení máme $s = tp_1^{v_1-u_1}$. Z toho plyne, že $p_1|s$, p_1 je jednotka. To je spor (prvek p_1 je ireducibilní).
Předpokládejme, že $k > 1$. Protože s je jednotka, existuje $w \in I$, $ws = 1$. Pak $sp_1^{u_1}\cdots p_k^{u_k} = tp_1^{v_1}\cdots p_k^{v_k}$, $wsp_1^{u_1}\cdots p_k^{u_k} = wtp_1^{v_1}\cdots p_k^{v_k}$, $1\cdot p_1^{u_1}\cdots p_k^{u_k} = wtp_1^{v_1}\cdots p_k^{v_k}$, $p_1^{u_1}\cdots p_k^{u_k} = wtp_1^{v_1}\cdots p_k^{v_k}$.
Po krácení prvkem $p_i^{u_i}$ dostaneme

$$\begin{aligned} p_1^{u_1}\cdots p_{i-1}^{u_{i-1}}p_{i+1}^{u_{i+1}}\cdots p_k^{u_k} &= wtp_1^{v_1}\cdots p_{i-1}^{v_{i-1}}p_i^{v_i-u_i}p_{i+1}^{v_{i+1}}\cdots p_k^{v_k} \\ p_1^{u_1}\cdots p_{i-1}^{u_{i-1}}p_{i+1}^{u_{i+1}}\cdots p_k^{u_k} &= p_1^{v_1}\cdots p_{i-1}^{v_{i-1}}(wtp_i)p_i^{v_i-u_i-1}p_{i+1}^{v_{i+1}}\cdots p_k^{v_k} \end{aligned}$$

Je $wt \in U(I)$, takže $wtp_i \| p_i$ a prvek wtp_i je ireducibilní (uvědomte si, že p_i je ireducibilní prvek a použijte tvrzení 8.3.3.). Uvažme poslední odvozenou rovnost. Jsou dvě možnosti:

- $u_j = 0$ pro všechna $j \in \{1,\ldots,k\} - \{i\}$: Je $1 = p_1^{v_1}\cdots p_{i-1}^{v_{i-1}}(wtp_i)p_i^{v_i-u_i-1}p_{i+1}^{v_{i+1}}\cdots p_k^{v_k}$, $wtp_1|1$, wtp_i je jednotka, spor.
- $u_j \neq 0$ pro nějaké $j \in \{1,\ldots,k\} - \{i\}$: Protože jsme v gaussovském oboru, existuje $j \in \{1,\ldots,k\} - \{i\}$ tak, že $wtp_i \| p_j$. Ovšem $p_i \| wtp_i$, takže $p_i \| p_j$, spor (je totiž $i \neq j$).

Spor jsme dostali v obou případech. Co nás zavedlo ke sporu? Byl to předpoklad, že $u_i \neq v_i$. Protože tedy $u_i = v_i$ pro $i = 1,\ldots,k$, je $sp_1^{u_1}\cdots p_k^{u_k} = tp_1^{u_1}\cdots p_k^{u_k}$. Jsme v oboru integrity a prvky $p_1,\ldots,p_k$ jsou ireducibilní a tedy nenulové. Můžeme tedy krátit a dostáváme $s = t$.

Nyní již konečně podáme důkaz toho, že pro každé dva prvky gaussovského obor existuje jejich největší společný dělitel.

10.3.3. Věta. *Nechť I je gaussovský obor, a, b jsou libovolné prvky oboru I. Pak v I existuje největší společný dělitel prvků a, b.*

Důkaz. Je-li $a = 0$ je $NSD(a,b) = NSD(0,b) = b$ (zdůvodněte!). Je-li a jednotka, je $NSD(a,b) = 1$ (zdůvodněte!). Obdobně existuje největší společný dělitel prvků a, b v případech, kdy $b = 0$ nebo b je jednotka.

Předpokládejme tedy dále, že $a \neq 0$, a není jednotka, $b \neq 0$, b není jednotka. Pak existují ireducibilní prvky $q_1,\ldots,q_l$, $r_1,\ldots,r_m$ oboru integrity I (l, m jsou kladná celá čísla) tak, že $a = q_1\cdots q_l$, $b = r_1\cdots r_m$. Buď $M = \{q_1,\ldots,q_l,r_1,\ldots,r_m\}$. Je M konečná neprázdná množina. Relace $\|$ je ekvivalence na množině M. Z každé třídy rozkladu $M/\|$ vybereme jeden prvek a takto vybrané prvky dáme do množiny P. Pak $P \subseteq M$, P je konečná neprázdná množina, prvky množiny P jsou navzájem neasociované (pokud $y, z \in P$, $y \neq z$, je $\neg(y\|z)$, protože z každé třídy rozkladu $M/\|$ jsme do množiny P vybrali jeden prvek) a pro každé $z \in M$ existuje

přesně jeden prvek $p \in P$ takový, že $z \| p$ (je to ten prvek, který jsme do P vybrali z té třídy rozkladu $M/\|$, v níž leží z). Počet prvků množiny P označme k. Nechť $P = \{p_1, \ldots, p_k\}$.

Zvolme libovolně $i \in \{1, \ldots, l\}$. Pak $q_i \in M$ a $q_i \| p_{j_i}$ pro nějaké $j_i \in \{1, \ldots, k\}$; jelikož $q_i \| p_{j_i}$ je $q_i = e_i p_{j_i}$ pro nějakou jednotku e_i. Položme $e = e_1 \cdots e_l$. Prvek e je jednotka oboru integrity I (je součinem jednotek). Máme

$$a = q_1 \cdots q_l = e_1 p_{j_1} \cdots e_l p_{j_l} = e_1 \cdots e_l p_{j_1} \cdots p_{j_l} = e p_{j_1} \cdots p_{j_l}$$

Existují nezáporná celá čísla $n_1, \ldots, n_k$ tak, že $p_{j_1} \cdots p_{j_l} = p_1^{n_1} \cdots p_k^{n_k}$. Celkem

$$a = e p_1^{n_1} \cdots p_k^{n_k}$$

Obdobně lze ukázat, že prvek b má vyjádření ve tvaru

$$b = f p_1^{o_1} \cdots p_k^{o_k}$$

kde f je jednotka a $o_1, \ldots, o_k$ jsou nezáporná celá čísla.

Položme $a' = p_1^{n_1} \cdots p_k^{n_k}$, $b' = p_1^{o_1} \cdots p_k^{o_k}$. Zřejmě $a' \| a$ a $b' \| b$.

Položme dále $D = p_1^{\min(n_1, o_1)} \cdots p_k^{\min(n_k, o_k)}$. Ukážeme, že $D = NSD(a', b')$. Pak bude také $D = NSD(a, b)$ (viz 8.2.3.) a důkaz věty bude hotov. Je třeba ukázat dvě věci:

- $D|a'$, $D|b'$: Všimneme si, že pro $i = 1, \ldots, k$ je $0 \leq \min(n_i, o_i) \leq n_i$; dle 10.3.1. pak $D|a'$. Dále si všimneme, že pro $i = 1, \ldots, k$ je $0 \leq \min(n_i, o_i) \leq o_i$; dle 10.3.1. pak $D|b'$.

- Nechť $d \in I$, $d|a'$, $d|b'$. Chceme: $d|D$. Protože $d|a'$, z 10.3.1. dostáváme $d = s p_1^{u_1} \cdots p_k^{u_k}$, kde $s \in U(I)$, $u_i \in \mathbb{Z}$, $0 \leq u_i \leq n_i$ pro $i = 1, \ldots, k$. Protože $d|b'$, z 10.3.1. dostáváme $d = t p_1^{v_1} \cdots p_k^{v_k}$, kde $t \in U(I)$, $v_i \in \mathbb{Z}$, $0 \leq v_i \leq o_i$ pro $i = 1, \ldots, k$. Vidíme, že $s p_1^{u_1} \cdots p_k^{u_k} = t p_1^{v_1} \cdots p_k^{v_k}$. Podle 10.3.2. je $u_i = v_i$ pro $i = 1, \ldots, k$. Pak pro $i = 1, \ldots, k$ platí: $0 \leq u_i \leq n_i$ a také $0 \leq u_i \leq o_i$. Z toho plyne, že pro $i = 1, \ldots, k$ je $0 \leq u_i \leq \min(n_i, o_i)$. Shrnutí: $d = s p_1^{u_1} \cdots p_k^{u_k}$, $s \in U(I)$, $0 \leq u_i \leq \min(n_i, o_i)$ pro $i = 1, \ldots, k$. Připomeňme ještě, že $D = p_1^{\min(n_1, o_1)} \cdots p_k^{\min(n_k, o_k)}$. Z 10.3.1. plyne, že $d|D$.

10.3.4. Poznámka. Nechť I je eukleidovský obor, $p_1, \ldots, p_k$ jsou vzájemně neasociované ireducibilní prvky oboru integrity I, $n_1, \ldots n_k, o_1, \ldots, o_k$ jsou nezáporná celá čísla. V důkazu věty 10.3.3. jsme spočítali, že

$$p_1^{\min(n_1, o_1)} \cdots p_k^{\min(n_k, o_k)} = NSD(p_1^{n_1} \cdots p_k^{n_k}, p_1^{o_1} \cdots p_k^{o_k})$$

A to je právě formulka známá z počítání největšího společného dělitele dvou celých čísel větších než jedna, známe-li jejich prvočíselné rozklady.

Cvičení.

1. Nechť I je obor integrity, $a \in I$, k, l jsou nezáporná celá čísla. Pak

   $$a^k a^l = a^{k+l}$$

   Dokažte.

11 Kořeny polynomů

Čím se budeme zabývat v poslední části tohoto textu? To je přece jasné, čekají nás kořeny polynomů (a problematika s nimi související). Nechť f je polynom nad oborem integrity I. Co je to kořen polynomu f? Je to takový prvek $c \in I$, pro který je $f(c) = 0$. Co je to $f(c)$? Pro

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

je

$$f(c) = a_n c^n + \cdots + a_1 c + a_0$$

Hledat kořeny polynomu f tedy znamená řešit rovnici

$$a_n x^n + \cdots + a_1 x + a_0 = 0$$

s neznámou x. (Rovnice tohoto typu se nazývají algebraické.)

11.1 Násobnost a počet kořenů polynomu

Již na střední škole jste hledali kořeny kvadratických polynomů (tj. řešili jste kvadratické rovnice). Zjistili jste tehdy, že kvadratický polynom s reálnými koeficienty nemá žádný reálný kořen, nebo má jeden reálný kořen, nebo má dva reálné kořeny, avšak nikdy nemá více než dva kořeny. V této části (mimo jiné) dokážeme obecné tvrzení: Jestliže f je polynom nad oborem integrity I a f má stupeň n, pak f má nejvýše n kořenů v I.

11.1.1. Věta. *Nechť I je obor integrity, f je polynom nad I, $c \in I$. Platí:*

$$f(c) = 0 \iff x - c | f(x)$$

Důkaz.
$\Longleftarrow$: Nechť $x-c|f(x)$. Existuje $g \in I[x]$, $f(x) = (x-c)g(x)$. Pak $f(c) = (c-c)g(c) = 0 \cdot g(c) = 0$.
$\Longrightarrow$: Nechť $f(c) = 0$. Předpokládejme nejprve, že polynom f je konstantní. Pak $f(x) = a$, kde $a \in I$. Je $f(c) = a$, takže $a = 0$ a f je nulový polynom. Pak je jasné, že $x - c|f(x)$. Předpokládejme nyní, že polynom f není konstantní. Pak $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, kde n je celé číslo, $n \geq 1$, $a_0, \ldots, a_n \in I$, $a_n \neq 0$. Počítejme:

$$\begin{aligned} f(x) &= f(x) - 0 \\ &= f(x) - f(c) \\ &= (a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0) - (a_n c^n + a_{n-1} c^{n-1} + \cdots + a_1 c + a_0) \\ &= a_n x^n - a_n c^n + a_{n-1} x^{n-1} - a_{n-1} c^{n-1} + \cdots + a_1 x - a_1 c + a_0 - a_0 \\ &= a_n (x^n - c^n) + a_{n-1} (x^{n-1} - c^{n-1}) + \cdots + a_1 (x - c) \end{aligned}$$

Nyní si stačí uvědomit, že pro každé kladné celé číslo k platí $x-c|x^k-c^k$. Pak totiž $x-c$ dělí každý sčítanec v $a_n(x^n-c^n)+a_{n-1}(x^{n-1}-c^{n-1})+\cdots+a_1(x-c)$ a tedy $x-c$ dělí součet, čili $x-c$ dělí $f(x)$.

Proč $x-c|x^k-c^k$? Pro $k=1$ je to jasné, pro $k>1$ uvažte rovnost

$$x^k-c^k=(x-c)(x^{k-1}+x^{k-2}c+\cdots+xc^{k-2}+c^{k-1})$$

Nyní již dokážeme větu o počtu kořenů polynomu.

11.1.2. Věta. *Nechť f je nenulový polynom nad oborem integrity I. Jestliže f má stupeň n, pak f má nejvýše n kořenů v I.*

Důkaz. Postupujme indukcí vzhledem k n.
$n=0$: Nechť f má stupeň 0. Je $f(x)=a$, kde $a\in I$, $a\neq 0$. Pro každé $c\in I$ je $f(c)=a\neq 0$, takže f nemá v I žádný kořen a tedy má v I nejvýše n kořenů.
$n>0$: Nechť f má stupeň n. Množinu všech kořenů polynomu f v oboru integrity I označme A. Chceme: $|A|\leq n$. Jsou dvě možnosti:

- $A=\emptyset$: Je $|A|=0$, takže $|A|<n$.
- $A\neq\emptyset$: Zvolme $c\in A$. Je $f(c)=0$ a dle věty 11.1.1. pak $x-c|f(x)$. Potom $f(x)=(x-c)g(x)$ pro nějaký polynom g nad I. Množinu všech kořenů polynomu g v oboru integrity I označme B. Protože polynom f je nenulový, je také polynom g nenulový. Platí: $n=deg(f(x))=deg((x-c)g(x))=deg(x-c)+deg(g(x))=1+deg(g(x))$. Vidíme, že polynom g má stupeň $n-1$. Dle indukčního předpokladu $|B|\leq n-1$. Ukážeme teď, že $A\subseteq\{c\}\cup B$. Zvolme libovolně $d\in A$. Musíme ukázat, že $d\in\{c\}\cup B$. Protože $d\in A$, je $f(d)=0$. Ovšem $f(x)=(x-c)g(x)$, takže $f(d)=(d-c)g(d)$, $(d-c)g(d)=0$. Jelikož g je polynom nad I a $d\in I$, je $g(d)\in I$. Tudíž $d-c\in I$, $g(d)\in I$, $(d-c)g(d)=0$. Protože I je obor integrity, dostáváme $d-c=0$ nebo $g(d)=0$. Pokud $d-c=0$, je $d=c$ a tedy $d\in\{c\}\cup B$. Pokud $g(d)=0$, je $d\in B$ a tedy také $d\in\{c\}\cup B$. Nyní víme: $|B|\leq n-1$ a $A\subseteq\{c\}\cup B$. Proto

$$|A|\leq|\{c\}\cup B|\leq|\{c\}|+|B|=1+|B|\leq 1+(n-1)=n,\ |A|\leq n$$

11.1.3. Poznámka.

1. Samozřejmě se může stát, že polynom má méně kořenů, než je jeho stupeň. Například kvadratický polynom x^2+1 je polynom nad tělesem $\mathbb{R}$, který nemá žádný kořen v $\mathbb{R}$.

2. V důkazu věty 11.1.2. bylo podstatné, že I byl obor integrity. Z $(d-c)g(d)=0$ jsme mohli odvodit, že $d-c=0$ nebo $g(d)=0$. Pokud bychom uvažovali polynomy nad komutativními asociativními okruhy s jednotkovým prvkem, nebude Věta 11.1.2. platit – například kvadratický polynom x^2+x nad $\mathbb{Z}_6$ má 4 kořeny v $\mathbb{Z}_6$.

Nakonec ještě budeme definovat násobnost kořene (neboť je slíbeno v názvu, že se v této části o násobnosti kořene aspoň něco řekne).

11.1.4. Definice. Nechť f je polynom nad oborem integrity I, $c\in I$, k je nezáporné celé číslo. Říkáme, že prvek c je k-násobným kořenem polynomu f, pokud

$$(x-c)^k|f(x)\ \wedge\ \neg((x-c)^{k+1}|f(x))$$

11.1.5. Poznámka. O násobnosti kořene polynomu si můžete přečíst v paragrafu 1 Násobnost kořene polynomu. Hornerovo schéma v kapitole XV Vlastnosti kořenů polynomů v učebnici [1]. Přečtete si tam například to, jak můžete násobnost kořene zjistit pomocí Hornerova schématu.

Cvičení.

1. Zjistěte násobnost kořenů $c_1=\frac{1}{2}$, $c_2=-2$ polynomu

$$f(x)=8x^7+4x^6-2x^5+3x^4-6x^3-2x^2+4x-1\in\mathbb{Q}[x]$$

2. Nechť f je polynom nad oborem integrity I, $c\in I$, k je nezáporné celé číslo. Dokažte: c je k-násobným kořenem polynomu f právě tehdy, když existuje $g\in I[x]$ takový, že

$$f(x)=(x-c)^k g(x)\ \wedge\ g(c)\neq 0$$

11.2 Základní věta algebry a její důsledky

Pod názvem Základní věta algebry se skrývá následující tvrzení:

11.2.1. Věta. (**Základní věta algebry**) *Každý nekonstantní polynom s komplexními koeficienty má aspoň jeden komplexní kořen.*

Základní větu algebry dokazovat nebudeme. Větu poprvé přesvědčivě dokázal C. F. Gauss v roce 1799. Přestože tvrzení Základní věty algebry je snadno pochopitelné i pro středoškolského studenta, pro její důkazy to v žádném případě neplatí.

Základní věta algebry má zajímavé a významné důsledky. Dva z nich uvedeme a také dokážeme.

11.2.2. Důsledek. *Nechť $f \in \mathbb{C}[x]$. Pak polynom f je ireducibilní v $\mathbb{C}[x]$ právě tehdy, když f je lineární.*

Důkaz. Jestliže f je lineární, pak f je ireducibilní – viz 8.3.4. Předpokládejme naopak, že f je ireducibilní. Dle definice ireducibilního prvku je f nenulový a také f není jednotka, z čehož plyne, že polynom f není konstantní. Podle Základní věty algebry existuje komplexní číslo c takové, že $f(c) = 0$. Pak $x - c|f(x)$ (viz 11.1.1.). Protože polynom f je ireducibilní, máme $x - c \| 1$ nebo $x - c \| f(x)$. Předpokládejme, že $x - c \| 1$. Pak $deg(x - c) = deg(1)$ (viz cvičení 11 v části 8.1 nebo také tvrzení 9.1.6.), čili $1 = 0$, spor. Nutně tedy $x - c \| f(x)$, což dává $deg(x - c) = deg(f(x))$, $1 = deg(f)$, f je lineární.

Důsledek 11.2.2. tedy přesně popisuje, jak vypadají ireducibilní prvky v $\mathbb{C}[x]$.
Připomeňme, že pro komplexní číslo $c = s + ti$ $(s, t \in \mathbb{R})$ je $\overline{c} = s - ti$.
Zavedeme následující označení:
Nechť f je polynom nad komplexními čísly,

$$f(x) = a_n x^n + \cdots + a_1 x + a_0$$

Polynom $\overline{f}$ definujeme takto:

$$\overline{f}(x) = \overline{a}_n x^n + \cdots + \overline{a}_1 x + \overline{a}_0$$

11.2.3. Tvrzení. *Nechť f je polynom s komplexními koeficienty, c je komplexní číslo. Pak $\overline{f(c)} = \overline{f}(\overline{c})$.*

Důkaz. Pro libovolná dvě komplexní čísla c, d je $\overline{c + d} = \overline{c} + \overline{d}$, $\overline{cd} = \overline{c}\,\overline{d}$. Jako cvičení proveďte důkaz uvedených dvou rovností – je to jednoduché (stačí jen pozorně počítat). Nechť $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Počítejme:

$$\overline{f(c)} = \overline{a_n c^n + \cdots + a_1 c + a_0} = \overline{a_n c^n} + \cdots + \overline{a_1 c} + \overline{a_0} = \overline{a_n}(\overline{c})^n + \cdots + \overline{a_1}(\overline{c}) + \overline{a_0} = \overline{f}(\overline{c})$$

11.2.4. Důsledek. *Necht $f \in \mathbb{R}[x]$. Pak polynom f je ireducibilní v $\mathbb{R}[x]$ právě tehdy, když f je lineární nebo f je kvadratický se záporným diskriminantem.*

Důkaz.

1. Jestliže f je lineární, pak f je ireducibilní – viz 8.3.4.
   Jestliže f je kvadratický se záporným diskriminantem, pak f je ireducibilní – viz cvičení 3 v části 8.3.

2. Nechť f je ireducibilní polynom v $\mathbb{R}[x]$. Pak f není konstantní (kdyby byl konstantní, byl by nulový nebo by byl jednotkou v $\mathbb{R}[x]$, což u ireducibilního prvku nepřipadá v úvahu). Dle Základní věty algebry existuje komplexní číslo c takové, že $f(c) = 0$. Jsou dvě možnosti:
Číslo c je reálné:
Dle 11.1.1. $x - c|f(x)$ v $\mathbb{R}[x]$. Protože polynom f je ireducibilní, máme $x - c\|1$ nebo $x - c\|f(x)$. Předpokládejme, že $x - c\|1$. Pak $deg(x - c) = deg(1)$ (viz cvičení 11 v části 8.1 nebo také tvrzení 9.1.6.), čili $1 = 0$, spor. Nutně tedy $x - c\|f(x)$, což dává $deg(x - c) = deg(f(x))$, $1 = deg(f)$, f je lineární.
Číslo c není reálné:
Je $c = s+ti$, kde s, t jsou reálná čísla, $t \neq 0$. Dle 11.1.1. máme $x-c|f(x)$ v $\mathbb{C}[x]$. Existuje tedy polynom $h \in \mathbb{C}[x]$ takový, že $f(x) = (x-c)h(x)$. Dle 11.2.3. je $\overline{f(c)} = \overline{f}(\overline{c})$, $\overline{0} = \overline{f}(\overline{c})$, $0 = \overline{f}(\overline{c})$. Ovšem $\overline{f} = f$, takže $f(\overline{c}) = 0$. Potom $(\overline{c} - c)h(\overline{c}) = 0$. Jelikož $\overline{c} - c \neq 0$, je $h(\overline{c}) = 0$. Dle 11.1.1. máme $x - \overline{c}|h(x)$ v $\mathbb{C}[x]$. Existuje tedy polynom $u \in \mathbb{C}[x]$ takový, že $h(x) = (x - \overline{c})u(x)$. Pak $f(x) = (x - c)(x - \overline{c})u(x)$. Je $(x - c)(x - \overline{c}) = x^2 - (c + \overline{c})x + c\overline{c}$. Vidíme, že polynom $(x-c)(x-\overline{c})$ má reálné koeficienty – je totiž $c+\overline{c} = 2s$ a $c\overline{c} = s^2+t^2$. Ukážeme, že $(x - c)(x - \overline{c})|f(x)$ v $\mathbb{R}[x]$. Využijeme teď toho, že $\mathbb{R}[x]$ je eukleidovský obor s normou deg: existují polynomy $v, w \in \mathbb{R}[x]$, $f(x) = (x - c)(x - \overline{c})v(x) + w(x)$ a přitom $w = 0$ nebo $w \neq 0$ a $deg(w) < 2$. Chceme: $w = 0$. Předpokládejme naopak, že $w \neq 0$. Pak $deg(w) < 2$. Je $(x - c)(x - \overline{c})u(x) = (x - c)(x - \overline{c})v(x) + w(x)$. Z toho plyne, že $(x - c)(x - \overline{c})|w(x)$ v $\mathbb{C}[x]$. Pak $deg((x - c)(x - \overline{c})) \leq deg(w(x))$, $2 \leq deg(w)$. Víme také, že $deg(w) < 2$. Dostáváme $2 < 2$, spor. Nutně tedy $w = 0$, $f(x) = (x - c)(x - \overline{c})v(x)$, $(x - c)(x - \overline{c})|f(x)$v $\mathbb{R}[x]$. Protože f je ireducibilní v $\mathbb{R}[x]$, platí $(x - c)(x - \overline{c})\|1$ nebo $(x-c)(x-\overline{c})\|f(x)$. Předpokládejme, že $(x-c)(x-\overline{c})\|1$. Pak $deg((x-c)(x-\overline{c})) = deg(1)$, $2 = 0$, spor. Nutně tedy $(x - c)(x - \overline{c})\|f(x)$. Z toho plyne, že $deg((x - c)(x - \overline{c})) = deg(f(x))$, $2 = deg(f)$. Zjistili jsme tedy, že polynom f je kvadratický. Zbývá ještě ukázat, že polynom f má záporný diskriminant. Protože $(x - c)(x - \overline{c})\|f(x)$, existuje $r \in \mathbb{R}[x]$, $f(x) = r(x)(x - c)(x - \overline{c})$. Pak $r \neq 0$, $deg(f(x)) = deg(r(x)(x - c)(x - \overline{c}))$, $deg(f(x)) = deg(r(x)) + deg((x - c)(x - \overline{c}))$, $2 = deg(r) + 2$, $deg(r) = 0$. Je tedy $r(x) = d$, kde d je nenulové reálné číslo. Takže $f(x) = d(x^2 - 2sx + (s^2 + t^2)) = dx^2 - 2dsx + d(s^2 + t^2)$. Diskriminant polynomu f označme D. Je $D = 4d^2s^2-4dd(s^2+t^2) = 4d^2s^2-4d^2s^2-4d^2t^2 = -4d^2t^2 < 0$ (připomeňme, že $d \neq 0$, $t \neq 0$).

Důsledek 11.2.4. přesně popisuje, jak vypadají ireducibilní prvky v $\mathbb{R}[x]$.

11.2.5. Poznámka. Připomeňte si větu 9.4.3.: *V eukleidovském oboru má každý nenulový prvek, který není jednotkou, jednoznačný rozklad na součin ireducibilních prvků. Jednoznačností rozkladu rozumíme jednoznačnost až na pořadí a asociovanost.* Polynomy nad tělesem tvoří eukleidovský obor. Takže $\mathbb{R}[x]$ a $\mathbb{C}[x]$ jsou eukleidovské obory a všechny jejich nekonstantní polynomy mají rozklad na součin ireducibilních polynomů. Důsledky 11.2.2. a 11.2.4. pak sa-

mozřejmě poskytují informace o tom, jak rozklady na součin ireducibilních polynomů v $\mathbb{R}[x]$ a $\mathbb{C}[x]$ vypadají. O tom více ve cvičeních.

Cvičení.

1. Nechť c, d jsou komplexní čísla. Dokažte: $\overline{c+d} = \overline{c} + \overline{d}$, $\overline{cd} = \overline{c}\,\overline{d}$.

2. Nechť f je nekonstantní monický polynom s komplexními koeficienty. Pak f lze v $\mathbb{C}[x]$ rozložit na součin monických lineárních polynomů, přičemž tento rozklad je jednoznačný až na pořadí. Dokažte. Poznámka: Monickým polynomem se rozumí nenulový polynom s vedoucím koeficientem 1.

3. Nechť f je nekonstantní monický polynom s reálnými koeficienty. Pak f lze v $\mathbb{R}[x]$ rozložit na součin několika monických lineárních polynomů a několika monických kvadratických polynomů se záporným diskriminantem, přičemž tento rozklad je jednoznačný až na pořadí. Dokažte.

11.3 Algebraické a transcendentní prvky

Nechť T je těleso, $S \subseteq T$, S je podtěleso tělesa T (tj. S je podokruh okruhu T, $1 \in S$ a pro všechna $s \in S$, $s \neq 0$, je $s^{-1} \in S$). Nechť $a \in T$. Prvek a se nazývá **algebraický** nad S, pokud existuje nenulový plynom $f \in S[x]$ takový, že $f(a) = 0$. V opačném případě se prvek a nazývá **transcendentní** nad S.

V této části se omezíme pouze na případ $T = \mathbb{R}$ a $S = \mathbb{Q}$. Jestliže reálné číslo a je algebraické nad $\mathbb{Q}$, pak stručně říkáme pouze, že číslo a je algebraické. Obdobně, jestliže reálné číslo a je transcendentní nad $\mathbb{Q}$, pak říkáme stručně pouze, že číslo a je transcendentní.

Není obtížné dokázat, že pro reálné číslo a platí:

číslo a je algebraické právě tehdy, když existuje nenulový polynom $f \in \mathbb{Z}[x]$ takový, že $f(a) = 0$

Dokažte to jako cvičení!

Úkol. Prostudujte část 10.2 Algebraická a transcendentní čísla v učebnici [5] (strany 49 a 50).

Cvičení.

1. Nechť a je reálné číslo. Pak platí:

   číslo a je algebraické právě tehdy, když existuje nenulový polynom $f \in \mathbb{Z}[x]$ takový, že $f(a) = 0$

   Dokažte.

2. Nechť a je komplexní číslo. Dokažte, že číslo a je algebraické nad $\mathbb{R}$

11.4 Binomické rovnice

Rovnice

$$x^n - \alpha = 0$$

kde n je kladné celé číslo a α je nenulové komplexní číslo, se nazývá **binomická rovnice**. Chceme najít všechna řešení binomické rovnice v oboru komplexních čísel. Řešení rovnice $x^n - \alpha = 0$ nazýváme n-té odmocniny z α.

Úkol. Prostudujte paragraf 1 Binomické rovnice v kapitole XVII Algebraické řešení algebraických rovnic v knize [1].

Cvičení.

1. Najděte všechna řešení binomické rovnice $x^4 - 1 = 0$ v oboru komplexních čísel.
2. Najděte všechna řešení binomické rovnice $x^3 - 1 = 0$ v oboru komplexních čísel.

11.5 Kvadratické a kubické rovnice

Jak víte, **kvadratická rovnice** je rovnice

$$ax^2 + bx + c = 0$$

kde a, b, c jsou komplexní čísla, $a \neq 0$.

Kubická rovnice pak je rovnice

$$ax^3 + bx^2 + cx + d = 0$$

kde a, b, c, d jsou komplexní čísla, $a \neq 0$.

Chceme najít všechny kořeny kvadratické rovnice i kubické rovnice v oboru komplexních čísel.

Již na střední škole jste se naučili, jak postupovat při řešení kvadratické rovnice. Teď si tento postup zopakujete a také se naučíte tzv. Cardanovy vzorce pro výpočet kořenů polynomů stupně třetího.

Úkol. Prostudujte část 10.4. Cardanovy vzorce v knize [5]; zaměřte se především na strany 51 a 52, na nichž je popsáno řešení kvadratických rovnic a Tartagliův postup na řešení kubické rovnice. Můžete si také přečíst paragraf 2 Algebraická řešitelnost rovnic 2., 3. a 4. stupně v kapitole XVII Algebraické řešení algebraických rovnic v učebnici [1]; tento paragraf je značně rozsáhlejší než část 10.4. v [5] a jeho látka je také pokročilejší (obtížnější).

Cvičení.

1. Vyřešte rovnici $x^2 + 2x + 3 = 0$ v oboru komplexních čísel.
2. Vyřešte rovnici $x^3 - 6x - 9 = 0$ v oboru komplexních čísel.

11.6 Kořeny polynomů nad celými čísly

Zde vyslovíme a dokážeme jednoduché tvrzení, které lze použít k nalezení všech racionálních kořenů polynomu s celočíselnými koeficienty.

11.6.1. Tvrzení. *Nechť n je kladné celé číslo. Nechť*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

je polynom nad celými čísly, tj. $a_0, \ldots, a_n$ jsou celá čísla. Nechť r, s jsou celá čísla, $s > 0$, r a s jsou nesoudělná. Jestliže $f(\frac{r}{s}) = 0$, pak $r|a_0$ a $s|a_n$.

Důkaz. Předpokládejme, že $f(\frac{r}{s}) = 0$. Pak

$$a_n \left(\frac{r}{s}\right)^n + a_{n-1}\left(\frac{r}{s}\right)^{n-1} + \cdots + a_1\left(\frac{r}{s}\right) + a_0 = 0$$

Rovnost vynásobíme číslem s^n. Dostaneme

$$a_n r^n + a_{n-1}r^{n-1}s + \cdots + a_1 r s^{n-1} + a_0 s^n = 0$$

Číslo r dělí všechny sčítance $a_n r^n, a_{n-1}r^{n-1}s, \ldots, a_1 r s^{n-1}$, takže $r|a_0 s^n$. Jelikož $r \perp s$, máme $r|a_0$.

Číslo s dělí všechny sčítance $a_{n-1}r^{n-1}s, \ldots, a_1 r s^{n-1}, a_0 s^n$, takže $s|a_n r^n$. Jelikož $r \perp s$, máme $s|a_n$.

Jak nám pomůže Tvrzení 11.6.1. při hledání racionálních kořenů polynomu $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$? Jistě lze předpokládat, že $a_n \neq 0$. Předpokládejme také, že $a_0 \neq 0$. Jestliže $f(\frac{r}{s}) = 0$ ($r, s \in \mathbb{Z}$, $s > 0$, $r \perp s$), pak dle 11.6.1. máme $r|a_0$ a $s|a_n$. Ovšem $r|a_0$ dává $|r| \leq |a_0|$ a $s|a_n$ dává $|s| \leq |a_n|$. Dostaneme tak konečný počet kandidátů na racionální kořen polynomu $f(x)$ a dosazením zjistíme, který z kandidátů opravdu je kořenem.

Možná namítnete, že může být $a_0 = 0$. Pak pro každé celé číslo r máme $r|a_0$ a máme nekonečně mnoho kandidátů na kořen polynomu $f(x)$. Ano, avšak i v případě $a_0 = 0$ nám Tvrzení 11.6.1. pomůže získat pouze konečný počet kandidátů na kořen. Jak? Na to jistě přijdete sami.

Cvičení.

1. Najděte všechny racionální kořeny polynomu $2x^6 - 3x^4 + 2x^3 - x + 1$.

2. Nechť n je kladné celé číslo. Nechť

   $$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

   je polynom nad celými čísly, tj. $a_0, \ldots, a_n$ jsou celá čísla. Nechť r, s jsou celá čísla, $s > 0$, r a s jsou nesoudělná. Jestliže $f(\frac{r}{s}) = 0$, pak $r - ms|f(m)$ pro libovolné celé číslo m. Specielně $r - s|f(1)$ a $r + s|f(-1)$. Dokažte.

3. Najděte všechny racionální kořeny polynomu $x^3 - 6x^2 + 15x - 14$.

11.7 Hornerovo schéma

Nechť n je kladné celé číslo, I je obor integrity. Nechť

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

je polynom nad oborem integrity I, tj. $a_0, \ldots, a_n \in I$.

Hornerovo schéma je efektivní algoritmus pro určení hodnoty $f(c)$, kde $c \in I$. Kdy se nám to bude hodit? Například tehdy, když budeme chtít zjistit, zda c je kořenem polynomu $f(x)$.

Myšlenku, na níž je Hornerovo schéma založeno, ukážeme nejprve pro $n = 4$. Máme

$$f(x) = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0$$

Při naivním výpočtu hodnoty $f(c)$ postupujeme takto:

$$f(c) = a_4 cccc + a_3 ccc + a_2 cc + a_1 c + a_0$$

Vidíme, že potřebujeme provést 10 násobení a 4 sčítání. Při chytřejším počítání postupně vypočítáme $cc = c^2$, $c^2 c = c^3$ a $c^3 c = c^4$ – k tomu potřebujeme 3 násobení. No a pak spočteme $a_4 c^4 + a_3 c^3 + a_2 c^2 + a_1 c + a_0 = f(c)$ - teď jsme potřebovali 4 násobení a 4 sčítání. Celkem jsme tedy pro výpočet $f(c)$ potřebovali 7 násobení a 4 sčítání.

Můžeme postupovat ještě chytřeji? Ano, a to s využitím vztahu

$$f(x) = a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = (((a_4 x + a_3)x + a_2)x + a_1)x + a_0$$

Tento vztah je základem Hornerova schématu pro $n = 4$. Vidíme, že k výpočtu $f(c)$ teď potřebujeme 4 násobení a 4 sčítání.

Obecně, základem Hornerova schématu je vztah

$$f(x) = (\ldots(((a_n x + a_{n-1})x + a_{n-2})x + a_{n-3})x + \cdots + a_1)x + a_0$$

Dle Hornerova schématu pro výpočet hodnoty $f(c)$ je potřeba n násobení a n sčítání.

Lze dokonce dokázat, že Hornerovo schéma je nejlepší algoritmus pro vyhodnocení polynomu – neexistuje žádný algoritmus, který by používal méně než n sčítání a také neexistuje žádný algoritmus, který by používal méně než n násobení.

Na závěr si ještě povšimněte, že při naivním výpočtu $f(c)$ (pouhým dosazením za x) je potřeba $\frac{n(n+1)}{2}$ násobení a n sčítání, a při výpočtu, v němž si nejdříve postupně určíme hodnoty $c^2, c^3, \ldots, c^n$, pak použijeme $2n - 1$ násobení a n sčítání.

11.7.1. Poznámka. Můžete si přečíst poměrně podrobné pojednání o Hornerově schématu v paragrafu 1 Násobnost kořene polynomu. Hornerovo schéma v kapitole XV Vlastosti kořenů polynomů v knize [1]. Tam se také dočtete, jak lze Hornerovo schéma využít při určování násobnosti kořene.

Reference

[1] Blažek, J., Koman, M., Vojtášková, B.: *Algebra a teoretická aritmetika, II díl.* Státní pedagogické nakladatelství, Praha, 1985.

[2] Kuřil, M.: *Lineární algebra.* Studijní text.
`https://kma.ujep.cz/administrace/uploads/144f052.pdf`

[3] Kuřil, M.: *Základy algebry.*
`https://kma.ujep.cz/administrace/uploads/85ac80c.pdf`

[4] Stanovský, D.: *Příklady z algebry.* Pracovní verze sbírky příkladů k základní přednášce z obecné algebry.
`https://www2.karlin.mff.cuni.cz/~stanovsk/vyuka/sbirka.pdf`

[5] Stanovský, D.: *Základy algebry.* **matfyz**press, Praha, 2010.