VYBRANÉ KAPITOLY Z ALGEBRY

Jaroslav Beránek

Brno 2011

Obsah

Úvod

Tento text je určen pro studenty pedagogického asistentství matematiky pro základní školy. Jedná se o přehledný studijní materiál doplňující základní studijní literaturu v disciplíně Algebra 3. Jelikož se jedná o text doplňující a osvětlující základní studijní literaturu ([2], [5], [6], [12], [15], [16]), nejsou v tomto textu v zájmu zachování lepší čtivosti a plynulosti textu uváděny důkazy jednotlivých tvrzení. Všechny důkazy lze nalézt ve studijní literatuře. Text je psán pro přehlednost velmi stručně a často se (na rozdíl od základní studijní literatury) omezuje pouze na případy, s nimiž se může student v praxi setkat (např. kapitola o polynomech je omezena pouze na polynomy nad tělesem reálných čísel). Pro studium textu je nutno předpokládat znalosti základů algebry (množinové operace a jejich vlastnosti, binární relace a jejich vlastnosti, relace uspořádání a uspořádané množiny, relace ekvivalence a rozklad množiny, binární algebraické operace a jejich vlastnosti, algebraické struktury a jejich homomorfismy). Standardní je rovněž označení základních číselných množin:
$\boldsymbol{N}$ – množina všech přirozených čísel (samozřejmě včetně čísla nula)
$\boldsymbol{Z}$ – množina všech celých čísel
$\boldsymbol{Q}$ – množina všech racionálních čísel
$\boldsymbol{R}$ – množina všech reálných čísel
$\boldsymbol{C}$ – množina všech komplexních čísel.
U množin $\boldsymbol{Z, Q, R}$ budeme v případě potřeby užívat i označení $\boldsymbol{Z^+, Q^+, R^+}$ a $\boldsymbol{Z^-, Q^-, R^-}$, označující podmnožinu všech kladných, resp. záporných čísel daného číselného oboru. Bude-li do této podmnožiny zařazena i nula, doplníme označení indexem nula, např. $\boldsymbol{Z_0^+, Q_0^-}$.

1. Přirozená čísla

Jednou ze základních charakteristik množiny všech přirozených čísel je to, že každé přirozené číslo má svého bezprostředního následovníka (pro každé $n \in \boldsymbol{N}$ je to číslo $n + 1$). Tento „fakt“ znají už žáci na 1. stupni ZŠ a je často didakticky využíván při výuce. Existence následovníka využijeme při teoretickém zavedení množiny přirozených čísel. Nejprve axiomaticky definujeme tzv. Peanovu množinu a potom ukážeme, že tato množina je univerzálním modelem množiny všech přirozených čísel. Poznamenejme ještě, že většinu důkazů v částech 1 - 5 lze nalézt v publikacích [12], resp. [2], z nichž je převzata i podstatná část textu.

Axiomy Peanovy množiny *P*

(A1) Ke každému prvku x množiny P existuje jeho následovník, který budeme označovat $x^{'}$.
(A2) V množině P existuje prvek $e \in P$, který není následovníkem žádného prvku množiny P.
(A3) Různé prvky mají různé následovníky.
(A4) *Axiom úplné indukce*. Nechť $M \subseteq P$. Jestliže platí:

a) $e \in M$,
b) $(\forall x \in P)\ x \in M \Rightarrow x^{'} \in M$,

pak $M = P$.

Věta 1.1. Nechť $x \in P$, pak platí:
(1) $x \neq x^{'}$ **,**
(2) $x \neq e \Rightarrow (\exists u \in P)\ x = u^{'}$**.**

Část (1) předchozí věty říká, že každý prvek je různý od svého následovníka. Ze druhé části pak plyne, že každý prvek x Peanovy množiny s výjimkou prvku e je následovníkem nějakého prvku $u \in P$. Tento prvek u budeme nazývat předchůdce prvku x a značit ${}^{/}x$.

Věta 1.2. Peanova množina je nekonečná množina.

Definice 1.3: Nechť $a \in P$ je libovolný prvek. Nechť množina $U(a) \subseteq P$ je pro každý prvek $a \in P$ definována takto:
(1) $a \in U(a)$,
(2) $x \in U(a) \Rightarrow {}^{/}x \in U(a)$ (pokud ${}^{/}x$ existuje).
Pak množinu $U(a)$ budeme nazývat úsek Peanovy množiny příslušný k prvku a .

Poznámka 1.4. Je zřejmé, že pro každé $a \in P$ je příslušný úsek $U(a)$ konečná množina.

Poznámka 1.5. Z předchozího plyne, že Peanovu množinu můžeme považovat za teoretický model množiny přirozených čísel. V tomto případě prvek e je roven číslu 1, následovník $x^{'}$ je roven číslu $x + 1$ a modely úseků příslušných ke každému přirozenému číslu chápanému jako prvek množiny P si lze představit takto: $U(1) = \{1\}$, $U(2) = \{1, 2\}$, $U(3) = \{1, 2, 3\}$, $U(4) = \{1, 2, 3, 4\}$ atd. Je zřejmé, že počet prvků každého úseku je určen přirozeným číslem, jemuž daný úsek přísluší. Proto i v dalším textu je možné představit si porovnávání prvků Peanovy množiny (relaci uspořádání v množině P) a následně i operace sčítání a násobení v množině P pomocí množiny přirozených čísel. I když teoretický postup je opačný (z obecné teorie v množině P plynou speciální vlastnosti v množině přirozených čísel), je pro pochopení podstaty vhodné už na tomto místě využít množiny přirozených čísel jako modelu Peanovy množiny P. Poznamenejme dále, že existuje i možnost vybudovat axiomaticky Peanovu množinu tak, že prvek e je roven číslu 0 (viz např. [2]). V tom případě je samozřejmě nutné

všechny definice a tvrzení přeformulovat. Protože ale číslo nula není prvkem množiny přirozených čísel, budeme se držet běžnější verze, v níž prvek *e* je roven číslu *1*.

Relace uspořádání v množině *P*

Definice 1.6: Nechť $a, b \in P$. Pak platí: $a \leq b \Leftrightarrow a \in U(b)$.

Poznámka 1.7. Je zřejmé, že relace $\leq$ z definice 1.6. je reflexivní, antisymetrická a tranzitivní, jedná se tedy skutečně o uspořádání v množině *P*. Pro každé dva různé prvky *a, b* množiny *P* vždy platí právě jeden ze vztahů $a \in U(b)$, $b \in U(a)$, proto je uspořádání $\leq$ lineární. Hasseovským diagramem lineárně uspořádané množiny $(P, \leq)$ je řetězec s nejmenším prvkem *e*. Dále poznamenejme, že zápis $a < b$ označuje tzv. ostré uspořádání, tedy $a \leq b$ a současně $a \neq b$.

Věta 1.8. Nechť $a, b \in P$. Pak platí:
(1) $(\forall\, a \in P)\ a < a^{|}$**;**
(2) Mezi prvky $a, a^{|}$ neexistuje žádný prvek *x* množiny *P* s vlastností $a < x < a^{|}$;
(3) Množina $(P, \leq)$ je dobře uspořádaná množina.

Operace sčítání v množině *P*

Věta 1.9. Na množině *P* existuje právě jedna operace + taková, že pro každou dvojici *x, y* prvků množiny *P* platí:
(1) $x + e = x^{|}$ **,**
(2) $x + y^{|} = (x + y)^{|}$ **.**

Definice 1.10. Operace + z předchozí věty se nazývá operace sčítání v množině *P* .

Věta 1.11. Operace + je v množině *P* asociativní a komutativní.

Věta 1.12. V grupoidu $(P, +)$ platí zákony o odečítání, tj. pro každé tři prvky *x, y, z* množiny *P* platí implikace $x + y = x + z \Rightarrow y = z$.

Věta 1.13. Nechť $x, y \in P$. Pak nastane právě jeden z následujících tří případů:
(1) $x = y$,
(2) existuje $p \in P$ s vlastností $x = y + p$,
(3) existuje $q \in P$ s vlastností $y = x + q$.

Operace sčítání je spojena s relací uspořádání řadou vztahů. Některé z nich jsou uvedeny v následující větě.

Věta 1.14. Nechť $x, y, z, u, v \in P$. Pak platí:
(1) $x < y \Leftrightarrow x + z < y + z$,
(2) $x \leq y \Leftrightarrow x + z \leq y + z$,
(3) $x \leq y,\ u \leq v \Rightarrow x + u \leq y + v$,
(4) $x < y \Rightarrow x^{|} \leq y$ **.**

Operace násobení v množině *P*

Věta 1.15. Na množině P existuje právě jedna operace $\cdot$ taková, že pro každou dvojici x, y prvků množiny P platí:

(1) $x \cdot e = x$,

(2) $x \cdot y^{|} = x \cdot y + x$.

Definice 1.16. Operace $\cdot$ z předchozí věty se nazývá operace násobení v množině P .

Poznámka 1.17. Pokud v zápise početních operací v množině P nepoužijeme závorky, má operace násobení přednost před operací sčítání. Rovněž se v zápisech velmi často vynechává označení $\cdot$ operace násobení, tj. místo $x \cdot y$ píšeme jenom xy.

Věta 1.18. Operace $\cdot$ je v množině P asociativní, komutativní, má neutrální prvek (prvek e) a s operací sčítání je svázána distributivním zákonem:

$$x, y, z \in P: \; x \cdot (y + z) = x \cdot y + x \cdot z \; .$$

Operace násobení je spojena s relací uspořádání řadou vztahů. Některé z nich jsou uvedeny v následující větě (zajímavá je analogie s obdobnými vztahy pro sčítání). Poznamenejme ještě, že tvrzení (3) následující věty říká, že v grupoidu $(P, \cdot)$ platí zákony o krácení.

Věta 1.19. Nechť $x, y, z, u, v \in P$. Pak platí:

(1) $x < y \Leftrightarrow x \cdot z < y \cdot z$,

(2) $x \leq y \Leftrightarrow x \cdot z \leq y \cdot z$,

(3) $x \cdot z = y \cdot z \Rightarrow x = y$

(4) $x \leq y, u \leq v \Rightarrow x \cdot u \leq y \cdot v$.

Důsledek 1.20. Algebraická struktura $(P, +, \cdot)$ je komutativní polookruh s jedničkou.

Poznámka 1.21. Z definice množiny P a popsaných vlastností relace uspořádání a operací sčítání a násobení v této množině vyplývá, že polookruh všech přirozených čísel $(\boldsymbol{N}, +, \cdot)$ je jedním z možných modelů polookruhu $(P, +, \cdot)$. Roli prvku e hraje číslo 1, následovníkem čísla x je číslo $x + 1$, úsek množiny $\boldsymbol{N}$ příslušný číslu n obsahuje všechna přirozená čísla od čísla 1 po číslo n atd.

Poznámka 1.22. Jako problémová se jeví otázka, kolik modelů polookruhu $(P, +, \cdot)$ existuje, tzn. zda jsou přirozená čísla určena jednoznačně, resp. zda vůbec nějaký model množiny P existuje. Existenci modelu množiny P a tím i existenci přirozených čísel lze snadno ukázat; jde o kardinální čísla konečných množin. Těm se budeme věnovat v dalším textu. Odpovědí na otázku počtu modelů Peanovy množiny je tvrzení, že těchto modelů je nekonečně mnoho, všechny jsou ale navzájem izomorfní. Proto lze tvrdit, že přirozená čísla lze definovat až na izomorfismus jediným možným způsobem. Důležitou větu o tomto izomorfismu nyní uvedeme:

Věta 1.23. (O jednoznačnosti přirozených čísel) Nechť $\boldsymbol{N_1}, \boldsymbol{N_2}$ jsou dvě množiny přirozených čísel (dva modely Peanovy množiny). Pak existuje právě jedna bijekce $f: \boldsymbol{N_1} \to \boldsymbol{N_2}$ s vlastností

$$\forall \, x \in \boldsymbol{N_1} : f\,(x^{|}) = [\,f(x)]^{|} \; .$$

Přirozená čísla jako kardinální čísla konečných množin

V této části se omezíme pouze na konečné množiny. I když v obecné teorii množin jsou studována i kardinální čísla nekonečných množin, pro účely konstrukce oboru všech přirozených čísel se nekonečnými množinami nemusíme zabývat.

Víme, že dvě množiny jsou ekvivalentní, jestliže existuje bijekce (vzájemně jednoznačné zobrazení) jedné na druhou. Tato relace ekvivalence na systému všech konečných množin $\mathcal{M}$ (označujeme ji $\sim$) je ekvivalencí v relačním smyslu (zřejmě je reflexivní, symetrická a tranzitivní). Proto generuje jednoznačným způsobem rozklad $\mathcal{M}|_{\sim}$ na systému všech konečných množin $\mathcal{M}$. Třídy rozkladu $\mathcal{M}|_{\sim}$ se nazývají kardinální čísla. Kardinálním číslem konečné množiny M tedy rozumíme třídu rozkladu $\mathcal{M}|_{\sim}$, která obsahuje množinu M. Místo označení kardinální číslo množiny M se často užívá též pojmu mohutnost množiny M (píšeme card M). Nyní definujeme přirozená čísla jako kardinální čísla konečných množin.

Popíšeme-li výše uvedenou konstrukci populárně (a matematicky ne zcela přesně), pak kardinální číslo konečné množiny M je systém množin, který kromě dané množiny M obsahuje všechny množiny (nekonečně mnoho), které mají tentýž počet prvků jako množina M. Tato jediná společná vlastnost všech těchto množin, tj. stejný počet prvků, je vyjádřena přirozeným číslem, které je kardinálním číslem množiny M definováno. Ve školské matematice na ZŠ proto říkáme, že přirozená čísla vyjadřují počty prvků konečných množin.

Přechod od struktury $(P, +, \cdot)$ k jejímu modelu $(\mathbf{N}, +, \cdot)$ lze popsat takto: Nechť $n \in P$ je libovolný prvek Peanovy množiny. Úsek množiny P příslušný k prvku n je množina $U(n) = \{e, e^{|}, e^{||}, e^{|||}, \ldots, {}^{/}n, n\}$. Tato množina je konečná, proto jistě náleží do některé třídy rozkladu $\mathcal{M}|_{\sim}$. Tato třída rozkladu je kardinálním číslem konečné množiny $U(n)$ a odpovídající přirozené číslo je číslo n. Lze tedy tvrdit, že úsek $U(n)$ obsahuje právě n prvků. Odtud prvku e odpovídá číslo *1,* prvku $e^{|}$ číslo *2,* prvku $e^{||}$ číslo *3* atd. Přirozené uspořádání množiny přirozených čísel lze pak definovat ve shodě s definicí porovnávání prvků Peanovy množiny (každé číslo náležející do $U(n)$ je menší nebo rovno číslu n).

Jiná situace je u definice obou základních operací sčítání a násobení. I když lze tyto operace definovat stejným způsobem jako v abstraktní Peanově množině, z metodických důvodů se obě operace zavádějí odlišně, na základě množinových operací.

Definice 1.24. (Sčítání kardinálních čísel) Nechť A, B jsou konečné množiny, nechť platí $A \cap B = \phi$. Pak definujeme

$$\text{card } A + \text{card } B = \text{card } (A \cup B) .$$

Definice 1.25. (Násobení kardinálních čísel) Nechť A, B jsou konečné množiny.
Pak definujeme

$$\text{card } A \cdot \text{card } B = \text{card } (A \times B) .$$

Poznámka 1.26. Lze ukázat, že obě operace definované definicemi 1.24. a 1.25. mají všechny vlastnosti, které očekáváme od operací sčítání a násobení přirozených čísel. Povšimněme si nyní omezující podmínky $A \cap B = \phi$ v definici 1.24. V případě jejího vypuštění bude pro součet kardinálních čísel množin A, B platit vztah card A + card $B \geq$ card $(A \cup B)$, přičemž číslo na levé straně této neostré nerovnosti je obecně větší než číslo na pravé straně o počet prvků průniku obou množin. Platí tedy rovnost

$$\text{card } A + \text{card } B - \text{card } (A \cap B) = \text{card } (A \cup B) .$$

Z teoretického hlediska se jedná o princip inkluze a exkluze pro $n = 2$. Pokud jsou tedy množiny A, B disjunktní, pak card $(A \cap B) = 0$ a předchozí rovnost přejde v definici sčítání kardinálních čísel podle definice 1.24.

2. Celá čísla

Obecná teorie

Definice 2.1. Nechť *(G, ·), (H, ·)* jsou grupoidy (dále budeme k označení grupoidů užívat pouze symbol nosné množiny). Řekneme, že grupoid *G* lze vnořit do grupoidu *H,* jestliže existuje injektivní homomorfismus *f* grupoidu *G* do grupoidu *H.*

Věta 2.2. Nechť *G* je komutativní grupoid. Pak jsou následující výroky ekvivalentní:
(1) Grupoid *G* je asociativní a platí v něm zákony o krácení.
(2) Grupoid *G* lze vnořit do nějaké grupy.

Poznámka 2.3. Důkaz této věty je konstruktivní, obsahuje konstrukci tzv. podílové grupy Γ grupoidu *G.* Tuto konstrukci nyní popíšeme:

Vyjdeme z kartézského součinu $G \times G$. Nechť na $G \times G$ je definována binární relace $\sim$ definovaná takto:

$$[a, b] \sim [c, d] \Rightarrow a \cdot d = b \cdot c \text{ pro každé dvě dvojice z } G \times G. \quad (1)$$

Tato relace $\sim$ je ekvivalence, existuje tedy rozklad $G \times G \,|_{\sim}$. Množinu tříd rozkladu $G \times G \,|_{\sim}$ označme Γ. Na množinovém systému Γ definujme nyní binární operaci *o* následujícím způsobem. Nechť *[a, b], [c, d]* jsou reprezentanti dvou tříd systému Γ. Pak platí

$$[a, b] \, o \, [c, d] = [a \cdot c, b \cdot d]. \quad (2)$$

Grupoid *(Γ, o)* je faktoroidem grupoidu *(G, ·).* Lze dokázat, že algebraická struktura *(Γ, o)* je dokonce grupa. Tato grupa se nazývá podílová grupa grupoidu *(G, ·).* Vnoření $\psi : G \to \Gamma$ grupoidu *G* do grupy Γ je definováno pro každý prvek $g \in G$ předpisem

$$\psi(g) = \{[g \cdot x, x]; x \in G\}. \quad (3)$$

Je-li místo multiplikativního označení (operace $\cdot$) užito označení aditivního (operace +), pak definiční vztahy (1), (2), (3) přejdou do tvaru:

$$[a, b] \sim [c, d] \Rightarrow a + d = b + c \text{ pro každé dvě dvojice z } G \times G, \quad (4)$$

$$[a, b] \, o \, [c, d] = [a + c, b + d] \ , \quad (5)$$

$$\psi(g) = \{[g + x, x]; x \in G\}. \quad (6)$$

Místo označení podílová grupa pak říkáme rozdílová grupa.

Celá čísla

Definice 2.4. Rozdílová grupa pologrupy $(\boldsymbol{N}, +)$ se nazývá aditivní grupa celých čísel $(\boldsymbol{Z}, +)$.

Poznámka 2.5. Při konstrukci grupy $(\boldsymbol{Z}, +)$ postupujeme podle obecné konstrukce. Výchozím kartézským součinem je $\boldsymbol{N} \times \boldsymbol{N}$, relace $\sim$ je definována vztahem (4) pro $G = \boldsymbol{N}$; operace *o,* kterou budeme označovat symbolem +, tj. stejně jako sčítání čísel přirozených (zřejmě nebude docházet k nedorozumění), je pak definována pomocí vztahu (5), tedy

$$[a, b] + [c, d] = [a + c, b + d]. \quad (7)$$

Celá čísla jsou podle této konstrukce třídami rozkladu $\boldsymbol{N} \times \boldsymbol{N} \,|_{\sim}$. Vnoření $\psi : \boldsymbol{N} \to \boldsymbol{Z}$ grupoidu $\boldsymbol{N}$ do grupy $\boldsymbol{Z}$ je definováno analogicky jako v (6), tedy pro každý prvek $n \in \boldsymbol{N}$ předpisem

$$\psi(n) = \{[n + x, x]; x \in \boldsymbol{N}\}.$$

Poznámka 2.6. V dalším textu o celých číslech je nutno rozlišovat mezi případem, kdy *[a, b]* bude označovat tuto jednu konkrétní uspořádanou dvojici přirozených čísel a případem, kdy bude hrát roli reprezentující dvojice nějakého celého čísla. V tomto druhém případě budeme užívat tučného označení ***[a, b]***. Platí tedy např. ***[4, 2]*** = *{[3, 1], [4, 2], [5, 3], [6, 4], ...}*. Celé

číslo je vždy reprezentováno nekonečnou množinou navzájem ekvivalentních uspořádaných dvojic přirozených čísel. Podle dohodnutého označení je nutno také rozlišovat následující vztahy: Např. pro uspořádané dvojice *[5, 3], [6, 4]* platí $[5, 3] \neq [6, 4]$, $[5, 3] \sim [6, 4]$, pro dvě celá čísla ***[5, 3]***, ***[6, 4]*** ale platí rovnost ***[5, 3]*** = ***[6, 4],*** protože obě tyto dvojice jsou reprezentanty téže třídy rozkladu systému $\boldsymbol{N \times N}$ $|_{\sim}$. Poznamenejme, že v dalším textu budeme pro zjednodušení označovat celá čísla velkými tučnými písmeny, např. ***A, B,*** .... Toto označení není v rozporu s uvedenou konstrukcí; vždy lze přejít k reprezentaci pomocí uspořádaných dvojic, např. $\boldsymbol{A = [a_1, a_2]}$, $\boldsymbol{B = [b_1, b_2]}$, ...

Operace s celými čísly a jejich vlastnosti

Poznámka 2.7. Sčítání celých čísel je, jak již bylo zmíněno v poznámce 2.2., definováno předpisem

$$\boldsymbol{[a, b] + [c, d] = [a + c, b + d].}$$

Věta 2.8. Operace + z předchozí poznámky 2.7. je komutativní, asociativní, má neutrální prvek ***0*** reprezentovaný dvojicí ***[n, n]*** pro libovolné $\boldsymbol{n \in N}$ a ke každému celému číslu $\boldsymbol{A = [a, b]}$ existuje právě jedno opačné číslo $\boldsymbol{-A = [b, a].}$

Věta 2.9. Algebraická struktura *(**Z**, +)* je komutativní grupa, ve které platí zákony o dělení, tj rovnice $\boldsymbol{A + X = B}$ má vždy řešení v množině ***Z*** pro každá dvě celá čísla ***A, B.***

Důsledek 2.10. V grupě *(**Z**, +)* platí zákony o krácení (v aditivní symbolice zákony o odečítání) a existuje právě jedna inverzní operace k operaci sčítání. Tato operace se nazývá odčítání a je definována vztahem $\boldsymbol{A - B = A + (-B).}$

Poznámka 2.11. Z předchozí věty a věty 2.1. lze odvodit početní pravidlo pro operaci odčítání:

$$\boldsymbol{[a, b] - [c, d] = [a + d, b + c].}$$

Povšimněme si, že v definici odčítání vystupují na pravé straně pouze součty přirozených čísel, tzn. operace odčítání je neomezeně definovaná a tedy algebraická struktura *(**Z**, –)* je grupoid. Tento grupoid není pologrupou, protože operace odčítání zřejmě není asociativní ani komutativní.

Definice 2.12. Na množině ***Z*** definujme binární operaci $\cdot$ následujícím způsobem:

$$\boldsymbol{[a, b] \cdot [c, d] = [ac + bd, ad + bc].}$$

Tuto operaci nazveme násobením v množině celých čísel. Tato operace je v množině ***Z*** neomezeně definovaná, struktura *(**Z**, $\cdot$)* je tedy grupoid.

Věta 2.13. Grupoid *(**Z**, $\cdot$)* je asociativní, komutativní a má neutrální prvek ***1*** reprezentovaný dvojicí ***[n+1, n]*** pro libovolné $\boldsymbol{n \in N}$.

Věta 2.14. V grupoidu *(**Z**, $\cdot$)* platí omezený zákon o krácení, tzn. pro každá tři celá čísla $x, y, z, x \neq 0$ platí implikace $x \cdot y = x \cdot z \Rightarrow y = z$.

Věta 2.15. Operace násobení je v množině celých čísel svázána s operací sčítání distributivním zákonem, tj.

$$\boldsymbol{A, B, C \in Z:\ A \cdot (B + C) = A \cdot B + A \cdot C.}$$

Důsledek 2.16. Algebraická struktura $(\boldsymbol{Z},+,\cdot)$ je komutativní okruh s jedničkou charakteristiky nula, který není tělesem. V tomto okruhu neexistují vlastní dělitelé nuly, je to tedy obor integrity.

Poznámka 2.17. V oboru integrity všech celých čísel $(\boldsymbol{Z},\ +,\ \cdot)$ platí řada tvrzení, běžně užívaných při výpočtech. Uveďme některé příklady.

Věta 2.18. Nechť $\boldsymbol{A, B, C \in Z}$. Pak platí:
(1) $-(-\boldsymbol{A}) = \boldsymbol{A}$;
(2) $-(\boldsymbol{A + B}) = (-\boldsymbol{A}) + (-\boldsymbol{B})$;
(3) $-(\boldsymbol{A - B}) = \boldsymbol{B - A}$;
(4) $(\boldsymbol{A - (B - C)} = (\boldsymbol{A + C}) - \boldsymbol{B}$;
(5) $(-\boldsymbol{A}) \cdot \boldsymbol{B} = \boldsymbol{A} \cdot (-\boldsymbol{B}) = -(\boldsymbol{A} \cdot \boldsymbol{B})$.

Relace uspořádání v množině celých čísel

Definice 2.19. Nechť $\boldsymbol{A} = \boldsymbol{[a, b]}$ je celé číslo. Řekneme, že toto číslo je kladné a píšeme $\boldsymbol{A} > 0$, právě když platí $a > b$. Je-li $a = b$, pak číslo $\boldsymbol{A} = \boldsymbol{0}$; ve zbývajícím případě pro $a < b$ říkáme, že celé číslo $\boldsymbol{A}$ je záporné a píšeme $\boldsymbol{A} < 0$.

Poznámka 2.20. Je zřejmé, že jeden z předchozích případů vždy musí nastat. Každé celé číslo je tedy buďto kladné nebo záporné nebo je rovno nule. Existuje tedy rozklad množiny všech celých čísel na čísla kladná, nulu a čísla záporná. Ve shodě s běžnou terminologií zavádíme i označení $\boldsymbol{A} \leq 0$ a říkáme, že číslo $\boldsymbol{A}$ je nekladné, resp. v případě $\boldsymbol{A} \geq 0$ je toto číslo nezáporné.

Definice 2.21. Nechť $\boldsymbol{A, B}$ jsou celá čísla. Řekneme, že $\boldsymbol{A} < \boldsymbol{B}$, právě když platí $\boldsymbol{A} - \boldsymbol{B} < 0$. Je-li $\boldsymbol{A} - \boldsymbol{B} = 0$, pak $\boldsymbol{A} = \boldsymbol{B}$; ve zbývajícím případě pro $\boldsymbol{A} - \boldsymbol{B} > 0$ pak platí $\boldsymbol{A} > \boldsymbol{B}$.

Poznámka 2.22. Je zřejmé, že i v předchozí definici jeden z případů vždy musí nastat. Relace uspořádání všech celých čísel je tedy lineární. I zde se běžně užívá i neostrá nerovnost $\boldsymbol{A} \leq \boldsymbol{B}$ pro případ $\boldsymbol{A} - \boldsymbol{B} \leq 0$ a analogicky $\boldsymbol{A} \geq \boldsymbol{B}$ pro případ $\boldsymbol{A} - \boldsymbol{B} \geq 0$.

Věta 2.23. Nechť $\boldsymbol{A}$ je celé číslo. Pak platí:
(1) $\boldsymbol{A} > 0 \Rightarrow -\boldsymbol{A} < 0$.
(2) $\boldsymbol{A} < 0 \Rightarrow -\boldsymbol{A} > 0$.

Věta 2.24. Nechť $\boldsymbol{A},\ \boldsymbol{B}$ jsou kladná celá čísla. Potom jejich součet $\boldsymbol{A} + \boldsymbol{B}$ i součin $\boldsymbol{A} \cdot \boldsymbol{B}$ jsou také kladná celá čísla.

Poznámka 2.25. Výše definovaná relace uspořádání v množině všech celých čísel je spojena s operacemi v této množině řadou vztahů. Uveďme alespoň některé.

Věta 2.26. Nechť $\boldsymbol{A},\ \boldsymbol{B},\ \boldsymbol{C},\ \boldsymbol{D}$ jsou libovolná celá čísla. Pak platí:
(1) Jestliže $\boldsymbol{A} > \boldsymbol{B}$ a $\boldsymbol{C} < 0$, potom $\boldsymbol{AC} < \boldsymbol{BC}$;
(2) Jestliže $\boldsymbol{A} + \boldsymbol{C} > \boldsymbol{B} + \boldsymbol{C}$, potom $\boldsymbol{A} > \boldsymbol{B}$;
(3) Jestliže $\boldsymbol{AC} > \boldsymbol{BC}$ a $\boldsymbol{C} > 0$, potom $\boldsymbol{A} > \boldsymbol{B}$;

(4) Jestliže $AC > BC$ a $C < 0$, potom $A < B$;
(5) Jestliže $A > B$ a $C > D$, potom $A + C > B + D$;
(6) Jestliže $A > B$ a $C > D$ a $C > 0$ a $B > 0$, potom $A \cdot C > B \cdot D$.

Věta 2.27. Nechť A, B jsou libovolná celá čísla, přičemž $B \neq 0$. Pak existuje jednoznačně určená dvojice celých čísel Q, R (přičemž $0 \leq R < |B|$) s vlastností $A = B \cdot Q + R$. Číslo A se nazývá dělenec, číslo B dělitel, číslo Q je podíl (někdy též neúplný podíl) a číslo R je zbytek. Proces nalezení čísel Q, R se nazývá dělení se zbytkem v množině celých čísel.

Definice 2.28. Absolutní hodnotu $|A|$ celého čísla A definujeme takto:
(1) Je-li $A \geq 0$, pak $|A| = A$;
(2) Je-li $A < 0$, pak $|A| = -A$.

Věta 2.29. Nechť A, B jsou libovolná celá čísla, pak platí:
(1) $|A| = |-A|$;
(2) $A \leq |A|$;
(3) $|A|^2 = A^2$;
(4) $|A \cdot B| = |A| \cdot |B|$;
(5) $|A + B| \leq |A| + |B|$;
(6) $|A - B| \geq |A| - |B|$.

Poznámka 2.30. Vnoření $\psi : N \to Z$ grupoidu N do grupy Z je definováno podle poznámky 2.2. pro každý prvek $n \in N$ předpisem $\psi(n) = \{[n + x, x]; x \in N\}$. Každé celé kladné (tj. přirozené) číslo n je tedy reprezentováno dvojicí $[n + x, x]$, číslo nula je reprezentováno dvojicí $[x, x]$ a každé celé záporné číslo $-n$ je reprezentováno dvojicí $[x, n + x]$.

3. Racionální čísla

Obecná teorie

Definice 3.1. Nechť $R = (R, +, \cdot)$, $S = (S, +, \cdot)$ jsou okruhy. Řekneme, že okruh R lze vnořit do okruhu S, jestliže existuje injektivní homomorfismus f okruhu R do okruhu S.

Věta 3.2. Nechť $(R, +, \cdot)$ je komutativní okruh. Pak jsou následující výroky ekvivalentní:
(1) V okruhu $(R, +, \cdot)$ platí omezený zákon o krácení, tzn.

$$\forall x, y, z \in R, x \neq 0: \; x \cdot y = x \cdot z \Rightarrow y = z \, .$$

(2) Okruh R lze vnořit do tělesa.

Poznámka 3.3. Důkaz této věty je konstruktivní, obsahuje konstrukci tzv. podílového tělesa T okruhu R. Tuto konstrukci nyní popíšeme:

Vyjdeme z kartézského součinu $R \times R - \{0\}$, který označíme M a budeme nazývat množina všech zlomků okruhu R. Nechť na M je definována binární relace $\sim$ definovaná takto:

$$[a, b] \sim [c, d] \Rightarrow a \cdot d = b \cdot c \text{ pro každé dvě dvojice z množiny } M. \qquad (8)$$

Tato relace $\sim$ je ekvivalence na M, existuje tedy rozklad $M|_{\sim}$. Množinu tříd rozkladu $M|_{\sim}$ označme T. Na množinovém systému T definujme nyní binární operace sčítání a násobení následujícím způsobem. Nechť $[a, b], [c, d]$ jsou reprezentanti dvou tříd systému T. Pak platí

$$[a, b] + [c, d] = [ad + bc, bd], \quad [a, b] \cdot [c, d] = [ac, bd] \qquad (9)$$

Lze dokázat, že algebraická struktura $(T, +, \cdot)$ je těleso. Toto těleso se nazývá podílové těleso okruhu R. Nulou tohoto tělesa je třída $\{[0, r]; r \in R\}$, jedničkou třída $\{[r, r]; r \in R\}$. Vnoření $\psi: R \to T$ okruhu R do tělesa T je definováno pro každý prvek $r \in R$ předpisem

$$\psi(r) = \{[r \cdot x, x]; x \in R\}. \qquad (10)$$

Racionální čísla

Definice 3.4. Podílové těleso okruhu $(\boldsymbol{Z}, +, \cdot)$ se nazývá těleso racionálních čísel $(\boldsymbol{Q}, +, \cdot)$.

Poznámka 3.5. Při konstrukci tělesa $(\boldsymbol{Q}, +, \cdot)$ postupujeme podle obecné konstrukce. Výchozím kartézským součinem je $M = \boldsymbol{Z} \times \boldsymbol{Z} - \{0\}$, relace $\sim$ je definována vztahem (8) pro $R = \boldsymbol{Z}$. Protože se podle obecné teorie jedná o zlomky, budeme uspořádané dvojice z množiny M zapisovat jako zlomky, tedy místo $[a, b]$ budeme psát $\frac{a}{b}$. Odtud je také zřejmé, proč se v množině M pro druhé složky všech dvojic nepřipouští číslo nula. Operace sčítání a násobení jsou definovány vztahy (9); po vyjádření pomocí zlomků tedy

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \, .$$

Racionální čísla jsou podle této konstrukce třídami rozkladu $M|_{\sim}$. Vnoření $\psi: \boldsymbol{Z} \to \boldsymbol{Q}$ okruhu $\boldsymbol{Z}$ do tělesa $\boldsymbol{Q}$ je definováno analogicky jako v (10), tedy pro každý prvek $z \in \boldsymbol{Z}$ předpisem

$$\psi(z) = \{\frac{z \cdot x}{x}; x \in \boldsymbol{Z} - \{0\}\}.$$

Analogicky jako u celých čísel budeme rozlišovat jeden konkrétní zlomek od racionálního čísla. Tučným označením $\frac{\boldsymbol{a}}{\boldsymbol{b}}$ budeme označovat stav, kdy tento zlomek bude reprezentovat racionální číslo, zatímco běžným způsobem $\frac{a}{b}$ budeme označovat tento jeden konkrétní

zlomek. Platí tedy např. $\frac{3}{4} = \{\frac{3}{4}, \frac{6}{8}, \frac{3}{12}, \frac{-21}{-28}, ...\}$. Poznamenejme, že v dalším textu budeme pro zjednodušení označovat racionální čísla velkými tučnými písmeny, např. ***A, B,*** .... Toto označení není, tak jako u celých čísel, v rozporu s uvedenou konstrukcí; vždy lze přejít k reprezentaci pomocí uspořádaných dvojic, např. $\boldsymbol{A} = \frac{a_1}{a_2}$, $\boldsymbol{B} = \frac{b_1}{b_2}$, ... Obě operace sčítání a násobení lze pak užitím tohoto označení psát jako

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} .$$

Věta 3.6. Operace sčítání v množině všech racionálních čísel je komutativní, asociativní, má neutrální prvek, ke každému racionálnímu číslu existuje právě jedno číslo opačné a platí zákony o dělení. Algebraická struktura *(**Q**, +)* je tedy komutativní grupa.

Poznámka 3.7. V grupě *(**Q**, +)* platí analogické vlastnosti a vztahy jako v grupě *(**Z**, +),* není tedy nutné je na tomto místě znovu uvádět. Poznamenejme jen, že neutrálním prvkem je číslo ***0*** reprezentované třídou $\frac{0}{b}$ a opačným racionálním číslem k číslu $\frac{a}{b}$ je číslo $-\frac{a}{b}$, které lze reprezentovat buďto třídou $\frac{-a}{b}$ nebo třídou $\frac{a}{-b}$.

Poznámka 3.8. Analogicky jako pro celá čísla lze zavést operaci odčítání jako přičtení opačného prvku, tedy $\boldsymbol{A} - \boldsymbol{B} = \boldsymbol{A} + (-\boldsymbol{B})$. Takto lze snadno odvodit běžně užívaný vztah pro odčítání zlomků:

$$\frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} .$$

Poznámka 3.9. Operace odčítání má v množině všech racionálních čísel tytéž vlastnosti jako v množině celých čísel (tj. není komutativní ani asociativní).

Poznámka 3.10. Nyní se budeme věnovat operaci násobení v množině všech racionálních čísel. Připomeneme definici: $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$.

Věta 3.11. Operace násobení v množině ***Q*** je komutativní, asociativní a má neutrální prvek. Tímto neutrálním prvkem je číslo ***1*** reprezentované třídou zlomků $\frac{a}{a}$. Algebraická struktura *(**Q**, ·)* je komutativní monoid. Operace násobení je distributivní vzhledem k operaci sčítání v množině všech racionálních čísel.

Poznámka 3.12. Budeme-li zkoumat i existenci inverzních prvků a platnost zákonů o dělení vzhledem k operaci násobení v množině ***Q,*** snadno zjistíme, že jediným prvkem, který neumožňuje obecnou platnost těchto vlastností, je číslo *0.* Po jeho odstranění z množiny ***Q*** můžeme vyslovit následující větu.

Věta 3.13. (1) Algebraická struktura *(**Q** − {0}, ·)* je komutativní grupa.
(2) Algebraická struktura *(**Q** ,+, ·)* je komutativní těleso.

Poznámka 3.14. Inverzním prvkem k racionálnímu číslu $\frac{a}{b}$ je číslo $\frac{b}{a}$ (předpokládáme, že $a \neq 0$). Toto číslo vždy jednoznačně existuje ($b \neq 0$ podle konstrukce racionálních čísel a $a \neq 0$ podle předpokladu), nazývá se převrácené číslo k číslu $\frac{a}{b}$ a označuje $\left(\frac{a}{b}\right)^{-1}$. Při označení racionálního čísla A se převrácené číslo kromě zápisu A^{-1} zapisuje též $\frac{1}{A}$. V množině $Q - \{0\}$ jsme nyní připraveni k definici operace dělení.

Definice 3.15. Dělení v množině $Q - \{0\}$ je definováno jako násobení převráceným číslem, tj. $A : B = A \cdot B^{-1}$. Vyjádřeno pomocí definice operace násobení a převráceného čísla dostáváme

$$\frac{a}{b} : \frac{c}{d} = \frac{ad}{bc} .$$

Poznámka 3.16. Připomeňme znovu, že existence převráceného čísla i operace dělení jsou neomezeně definovány v množině $Q - \{0\}$, tedy že skutečně nemůže dojít k „dělení nulou“. Pro operace dělení a násobení platí rovněž řada vlastností, z nichž uvedeme např.:

Věta 3.17. Nechť $A, B, C \in Q$. Pak platí:
(1) $(A^{-1})^{-1} = A$;
(2) $(A \cdot B)^{-1} = A^{-1} \cdot B^{-1}$;
(3) $(A \cdot B^{-1})^{-1} = B \cdot A^{-1}$;
(4) $(A \cdot B^{-1}) \cdot C^{-1} = A \cdot (B \cdot C)^{-1}$;
(5) $A \cdot (B \cdot C^{-1})^{-1} = (A \cdot C) \cdot B^{-1}$.

Relace uspořádání v množině racionálních čísel

Definice 3.18. Nechť $A = \frac{a}{b}$ je racionální číslo. Řekneme, že toto číslo je kladné a píšeme $A > 0$, právě když platí a i b jsou buďto obě současně kladná celá čísla nebo obě současně záporná celá čísla. . Je-li $a = 0$, pak číslo $A = 0$; ve zbývajícím případě (jedno z čísel a, b je kladné celé číslo a jedno záporné) říkáme, že racionální číslo A je záporné a píšeme $A < 0$.

Poznámka 3.19. Je zřejmé, že jeden z předchozích případů vždy musí nastat. Každé racionální číslo je tedy buďto kladné nebo záporné nebo je rovno nule. Existuje tedy rozklad množiny všech racionálních čísel na čísla kladná, nulu a čísla záporná. Ve shodě s běžnou terminologií zavádíme i označení $A \leq 0$ a říkáme, že číslo A je nekladné, resp. v případě $A \geq 0$ je toto číslo nezáporné.

Definice 3.20. Nechť A, B jsou racionální čísla. Řekneme, že $A < B$, právě když platí $A - B < 0$. Je-li $A - B = 0$, pak $A = B$; ve zbývajícím případě pro $A - B > 0$ pak platí $A > B$.

Poznámka 3.21. Je zřejmé, že i v předchozí definici jeden z případů vždy musí nastat. Relace uspořádání všech racionálních čísel je tedy lineární. I zde se běžně užívá i neostrá nerovnost $A \leq B$ pro případ $A - B \leq 0$ a analogicky $A \geq B$ pro případ $A - B \geq 0$.

Poznámka 3.22. Pro relaci uspořádání v množině racionálních čísel a její spojení s operacemi v množině $\boldsymbol{Q}$ platí analogické vztahy jako v množině celých čísel, stejně je definována i absolutní hodnota racionálního čísla. Vzhledem k tomu, že $(\boldsymbol{Q}, +, \cdot)$ je komutativní těleso, nemá smysl v množině racionálních čísel zavádět dělení se zbytkem. Platí však zajímavá vlastnost relace uspořádání racionálních čísel, která v množinách přirozených ani celých čísel nemá analogii.

Definice 3.23. Uspořádání v množině racionálních čísel je husté (tj. $(\boldsymbol{Q}, <)$ je hustě uspořádaná množina), jestliže platí

$$\forall x, y \in \boldsymbol{Q}, x \neq y; \exists z \in \boldsymbol{Q}: x < z < y .$$

Poznámka 3.24. Definice hustého uspořádání říká, že „mezi každá dvě různá racionální čísla lze vložit další racionální číslo“. Z teorie uspořádaných množin z toho plyne, že uspořádaná množina $\boldsymbol{Q}$ nemá skoky. Vysvětlení této skutečnosti ponecháme na teorii konstrukce reálných čísel.

Desetinné rozvoje racionálních čísel

Poznámka 3.25. Je zřejmé, že racionální čísla nevyjadřujeme výlučně ve tvaru zlomku, např. velmi často se setkáváme s jejich vyjádřením pomocí desetinných rozvojů.

Věta 3.26. Každé racionální číslo lze vyjádřit pomocí desetinného rozvoje, přičemž tento desetinný rozvoj je buďto ukončený nebo je periodický. Ukončený je právě tehdy, je-li dané racionální číslo tvaru $\frac{a}{2^p \cdot 5^q}$, tj. obsahuje-li rozklad jeho jmenovatele na prvočinitele pouze prvočísla *2* nebo *5*.

Nástin důkazu. Při dělení čitatele zlomku jeho jmenovatelem mohou nastat pouze dvě možnosti. Buďto je zbytek od jistého kroku dělení roven nule, pak je desetinný rozvoj ukončený. Nenastane-li tento případ, je rozvoj neukončený. Protože však počet všech možných nenulových zbytků musí být menší než jmenovatel zlomku, musí se nutně od jistého kroku zbytky opakovat.

Definice 3.27. Zlomek, jehož jmenovatel je roven některé mocnině čísla deset, se nazývá desetinný zlomek. Racionální číslo, jehož desetinný rozvoj je ukončený, se nazývá v rozvinutém tvaru desetinné číslo.

Poznámka 3.28. Převod zápisu racionálního čísla ze zlomku na desetinný rozvoj provádíme dělením čitatele jmenovatelem; opačný převod buďto přechodem na desetinný zlomek a úpravou (v případě konečného rozvoje) nebo užitím součtu konvergentní geometrické řady.

4. Reálná čísla

Poznámka 4.1. Protože $(\boldsymbol{Q}, +, \cdot)$ je komutativní těleso, tzn. ze strukturálního hlediska „nejbohatší“ strukturou, nelze již provést její „zlepšení“. Proto konstrukce reálných čísel

nemůže být provedena pomocí podílových struktur; lze dokázat, že konstrukcí podílového tělesa racionálních čísel nedostaneme již nic nového. Těleso reálných čísel musí být konstruováno na jiné bázi. K tomu lze využít uspořádaných množin; buďto teorii řezů pocházející od R. Dedekinda nebo teorii úplných metrických prostorů. Zde využijeme Dedekindových řezů. Nejprve opět základní přehled teorie.

Obecná teorie

Definice 4.2. Nechť $(E, \leq)$ je lineárně uspořádaná množina. Dvojice $\alpha = (A, B)$, $A \subseteq E$, $B \subseteq E$ se nazývá řez v množině E, jestliže platí:
(1) $A \cup B = E$, $A \neq \emptyset$, $B \neq \emptyset$,
(2) $x \in A \wedge y \in B \Rightarrow x < y$,
(3) $A \cap B = \emptyset$.

Poznámka 4.3. Systém $\{A, B\}$ tvoří tedy rozklad množiny E; množina A je dolní skupina řezu α a množina B je horní skupina řezu α.

Poznámka 4.4. (Typy řezů). Nechť $\alpha = (A, B)$ je řez v množině E. Pak mohou nastat následující čtyři případy.
Řez 1. druhu: Množina A obsahuje největší prvek a množina B neobsahuje nejmenší prvek;
Řez 2. druhu: Množina A neobsahuje největší prvek a množina B obsahuje nejmenší prvek;
Řez 3. druhu: Množina A neobsahuje největší prvek a množina B neobsahuje nejmenší prvek;
Řez 4. druhu: Množina A obsahuje největší prvek a množina B obsahuje nejmenší prvek.

Protože řezy 1. a 2. druhu popisují v podstatě tutéž situaci, budeme je v dalším textu ztotožňovat. Každá lineárně uspořádaná množina proto může mít pouze řezy 1., 3. a 4. druhu.

Definice 4.5. Řez 3. druhu z poznámky 4.4. se nazývá mezera v lineárně uspořádané množině, řez 4. druhu z poznámky 4.4. se nazývá skok v lineárně uspořádané množině.

Věta 4.6. Lineárně uspořádaná množina, která obsahuje alespoň dva prvky, je hustě uspořádaná, právě když nemá skoky.

Příklady: a) řez 1. druhu: $E = \boldsymbol{Q}$; $A = \{x \in \boldsymbol{Q}: x \leq 1\}$, $B = \{x \in \boldsymbol{Q}: x > 1\}$;
b) řez 3. druhu: $E = \boldsymbol{Q}$; $A = \{x \in \boldsymbol{Q}: x^2 < 2\}$, $B = \{x \in \boldsymbol{Q}: x^2 > 2\}$;
c) řez 4. druhu: $E = \boldsymbol{Z}$; $A = \{x \in \boldsymbol{Z}: x \leq 1\}$, $B = \{x \in \boldsymbol{Z}: x \geq 2\}$.

Definice 4.7. Lineárně uspořádaná množina se nazývá spojitě uspořádaná, právě když nemá skoky ani mezery.

Definice 4.8. Nechť $(R, \leq)$, $(S, \leq)$ jsou lineárně uspořádané množiny. Zobrazení $f : R \to S$ se nazývá vnoření $(R, \leq)$ do $(S, \leq)$, jestliže platí:
(1) f je injektivní;
(2) $\forall x, y \in R: x \leq y \Rightarrow f(x) \leq f(y)$.
Někdy se pro toto zobrazení f užívá též označení izotonní zobrazení.

Věta 4.9. Každou lineárně uspořádanou množinu lze vnořit do lineárně uspořádané množiny bez mezer.

Věta 4.10. Nechť $(R, \leq)$ je lineárně uspořádaná množina. Označme S množinu všech řezů 1. a 3. druhu v množině R. Nechť na S je definováno uspořádání takto:

$$\alpha=(A, B),\ \beta=(C, D),\ \alpha, \beta \in S:\ \alpha \leq \beta \Leftrightarrow A \subseteq C.$$

Pak S je lineárně uspořádaná množina, která neobsahuje mezery.

Definice 4.11. Lineárně uspořádaná množina $(S, \leq)$ z předchozí věty se nazývá normální obal lineárně uspořádané množiny $(R, \leq)$.

Poznámka 4.12. Ztotožníme-li prvky množiny R s řezy 1. druhu v R, pak normální obal množiny R se skládá z prvků množiny R a mezer v R.

Označení 4.13. Nechť $(E, \leq)$ je lineárně uspořádaná množina. Pro každý prvek $m \in E$ budeme její podmnožinu $\{x \in E: x \leq m\}$ označovat $(m]$.

Věta 4.14. Nechť $(R, \leq)$ je lineárně uspořádaná množina a nechť $(S, \leq)$ je její normální obal. Uvažujme všechny řezy 1. druhu v množině R (podle poznámky 4.4. je každému prvku $r \in R$ přiřazen právě jeden řez 1. druhu, kde prvek r je největším prvkem dolní skupiny příslušného řezu). Označme $\alpha = (A, B)$ libovolný řez 1. druhu v množině R, nechť $r \in R$ je největší prvek množiny A. Definujme nyní zobrazení $f: R \to S$ takto: Pro každý prvek $r \in R$ nechť je jeho obrazem řez $f(r)$ v množině S definovaný takto:

$$f(r) = (\ (r],\ R - (r]\ ).$$

Pak zobrazení $f: R \to S$ je vnoření $(R, \leq)$ do $(S, \leq)$.

Reálná čísla

Poznámka 4.15. Z teorie racionálních čísel víme, že $(\boldsymbol{Q}, <)$ je lineárně uspořádaná množina, která nemá skoky (uspořádání je husté). Lze však snadno dokázat, že obsahuje mezery, např. $\sqrt{2}$ je zcela jistě číslo, které není racionální (nelze ho vyjádřit pomocí zlomku).

Věta 4.16. V lineárně uspořádané množině $(\boldsymbol{Q}, <)$ existují pouze řezy 1. a 3. druhu. Řezy 1. druhu odpovídají racionálním číslům a řezy 3. druhu mezerám v uspořádané množině $(\boldsymbol{Q}, <)$.

Definice 4.17. Normální obal lineárně uspořádané množiny $(\boldsymbol{Q}, <)$ je lineárně uspořádaná množina $(\boldsymbol{R}, <)$. Podle věty 4.10. lineárně uspořádaná množina $(\boldsymbol{R}, <)$ neobsahuje mezery, existují v ní tedy pouze řezy 1. druhu.

Věta 4.18.

(1) Lineárně uspořádaná množina $(\boldsymbol{R}, <)$ je spojitě uspořádaná (neobsahuje mezery).

(2) $\forall x, y \in \boldsymbol{R}, x < y;\ \exists z \in \boldsymbol{Q}: x < z < y$.

Definice 4.19. V uspořádané množině $(\boldsymbol{Q}, <)$ odpovídají řezy 1. druhu racionálním číslům a řezy 3. druhu (tj. mezery) odpovídají číslům iracionálním. Každá mezera v uspořádané množině $(\boldsymbol{Q}, <)$ tedy určuje právě jedno iracionální číslo. Označíme-li množinu všech iracionálních čísel $\boldsymbol{I}$, pak platí $\boldsymbol{R} = \boldsymbol{Q} \cup \boldsymbol{I}$.

Poznámka 4.20. Protože lineárně uspořádaná množina $(\boldsymbol{R}, <)$ neobsahuje mezery, lze konstatovat, že každý bod číselné osy je obrazem právě jednoho reálného čísla a naopak, každé reálné číslo lze jednoznačně znázornit na číselné ose. Uvedené skutečnosti plynou i

z axiomů spojitosti, známých z axiomatické teorie výstavby geometrie. Tyto axiomy jsou dva, Archimédův a Cantorův. Zejména Cantorův axiom, podle něhož průnik do sebe zařazených úseček je neprázdný, podstatně přispívá k představě obrazů reálných čísel na číselné ose.

Uspořádání v množině reálných čísel

Poznámka 4.21. Připomeňme, že reálná čísla jsou sjednocením racionálních řezů 1. a 3. druhu, tj. každé reálné číslo je racionálním řezem. V případě řezu 1. druhu jde o číslo racionální, v případě řezu 3. druhu jde o číslo iracionální.

Definice 4.22. Nechť $\alpha = (A, B)$, $\beta = (C, D)$ jsou řezy v množině $\boldsymbol{Q}$ (tj. dvě reálná čísla). Pak platí:

$$\alpha \leq \beta \Leftrightarrow A \subseteq C .$$

Definice 4.23. Nechť $\boldsymbol{Q}^+ = \{r \in \boldsymbol{Q}: r > 0\}$, tj. $\boldsymbol{Q}^+$ označuje množinu všech kladných racionálních čísel. Pak řez $(\boldsymbol{Q} - \boldsymbol{Q}^+, \boldsymbol{Q}^+)$ je reálné číslo, které označíme symbolem 0 a nazýváme nulou. Číslo $a \in \boldsymbol{R}$ je kladné, je-li $a > 0$, číslo $a \in \boldsymbol{R}$ je záporné, je-li $a < 0$.

Operace v množině reálných čísel

Definice 4.24. Nechť $a = (A, B)$, $b = (C, D)$ jsou libovolná reálná čísla. Položme nyní $C_2 = \{\alpha + \beta ;\ \alpha \in B, \beta \in D\}$, $C_1 = \boldsymbol{Q} - C_2$. Pak $C = (C_1, C_2)$ je reálné číslo, které nazveme součtem reálných čísel a, b a značíme $a + b$.

Věta 4.25. Nechť $a, b, c,$ jsou libovolná reálná čísla. Nechť platí $a < b$. Potom platí také nerovnost $a + c < b + c$. (Uspořádání reálných čísel je monotonní vzhledem ke sčítání).

Věta 4.26. Operace sčítání je v množině všech reálných čísel komutativní, asociativní, má neutrální prvek a platí zákony o dělení (rovnice $a + x = b$ má řešení pro libovolná reálná čísla a, b). Algebraická struktura $(\boldsymbol{R}, +)$ je komutativní grupa.

Definice 4.27. Z předchozí věty plyne, že rovnice $a + x = b$ má řešení pro libovolná reálná čísla a, b. Toto řešení píšeme ve tvaru $x = b - a$ a nazveme rozdílem reálných čísel a, b. příslušná operace se nazývá odčítání reálných čísel.

Definice 4.28. Nechť $a = (A, B)$, $b = (C, D)$ jsou libovolná reálná čísla. Položme nyní: $C_2 = \{\alpha \cdot \beta ;\ \alpha \in B, \beta \in D\}$, $C_1 = \boldsymbol{Q} - C_2$. Pak $C = (C_1, C_2)$ je reálné číslo, které nazveme součinem reálných čísel a, b a značíme $a \cdot b$.

Věta 4.29. Nechť $a, b, c,$ jsou libovolná reálná čísla. Pak platí:
(1) $(-a) \cdot b = a \cdot (-b) = -(a \cdot b)$;
(2) $(-a) \cdot (-b) = a \cdot b$;
(3) $a \cdot b = 0$ právě tehdy, je-li $a = 0$ nebo $b = 0$.

Věta 4.30.
(1) Algebraická struktura $(\boldsymbol{R} - \{0\}, \cdot)$ je komutativní grupa.
(2) Algebraická struktura $(\boldsymbol{R}, +, \cdot)$ je komutativní těleso.

Věta 4.31. (Věta o supremu a infimu) Nechť M je libovolná neprázdná podmnožina množiny reálných čísel. Pak platí:
(1) Je-li M zdola ohraničená, existuje $inf_{\boldsymbol{R}} M$;
(2) Je-li M shora ohraničená, existuje $sup_{\boldsymbol{R}} M$.

Věta 4.32. (Vnoření racionálních čísel do čísel reálných)
Nechť $a \in \boldsymbol{Q}$. Označme $\boldsymbol{R_a} = \{x \in \boldsymbol{R}: x \leq a\}$. Pak zobrazení $f: \boldsymbol{Q} \to \boldsymbol{R}$ definované předpisem

$$f(a) = (\boldsymbol{R_a}, \boldsymbol{R} - \boldsymbol{R_a})$$

je izomorfní vnoření lineárně uspořádané množiny $\boldsymbol{Q}$ do lineárně uspořádané množiny $\boldsymbol{R}$.

Poznámka 4.33. Z matematické analýzy jsou známy následující definice:
(1) Posloupnost $\{a_n\}_{n=1}^{\infty}$ je cauchyovská, jestliže ke každému $\varepsilon > 0$ existuje přirozené číslo n_0 s vlastností, že pro každou dvojici přirozených čísel $m, n > n_0$ platí $|a_m - a_n| < \varepsilon$.
(2) Posloupnost $\{a_n\}_{n=1}^{\infty}$ je konvergentní s limitou L, jestliže ke každému $\varepsilon > 0$ existuje přirozené číslo n_0 s vlastností, že pro každé přirozené číslo $n > n_0$ platí $|a_n - L| < \varepsilon$.

Je zřejmé, že každá konvergentní posloupnost je cauchyovská, opak obecně neplatí. V metrickém prostoru $\boldsymbol{R}$ je ale každá cauchyovská posloupnost konvergentní, to znamená, že $\boldsymbol{R}$ je úplným metrickým prostorem. Této teorie úplných prostorů lze využít též ke konstrukci tělesa reálných čísel místo teorie řezů. Nyní následuje několik didaktických poznámek. Následující poznámka je převzata z publikace [4], s. 90 – 92.

Poznámka 4.34. Již na střední škole se setkají studenti s důkazem, že číslo $\sqrt{2}$ nelze vyjádřit ve tvaru zlomku, tzn. že kromě čísel racionálních existují ještě čísla iracionální, přičemž iracionálními čísly jsou téměř všechny odmocniny, hodnoty goniometrických funkcí, logaritmů atd. Studentům však většinou chybí názorná geometrická představa; velmi těžko odlišují pojmy mezera a skok na číselné ose. Tyto pojmy, známé již ze starověké matematiky, jsou přitom ke správnému pochopení reálných čísel nezbytné. Nyní uvedeme dva modely reálných čísel, aritmetický a geometrický. S oběma se setká již žák základní školy. Aritmetickým modelem je pro něj množina všech čísel, geometrickým modelem číselná osa. Izomorfismus obou modelů umožňuje nerozlišovat mezi číslem a jeho obrazem na číselné ose. Aritmetický model je častější, geometrický model je přitom názornější a pro zavádění reálných čísel na školách vhodnější.

Množina $\boldsymbol{R}$ je:
- *uspořádaná* , tj. pro každá dvě $x, y \in \boldsymbol{R}$ nastane právě jeden z případů $x < y, x = y, x > y$;
- *hustá*, tj. $\forall x, y \in \boldsymbol{R}, x < y, \exists z \in \boldsymbol{R}: x < z < y$;
- *archimedovská*, tj. $\forall x, y \in \boldsymbol{R}, 0 < x < y, \exists n \in \boldsymbol{N}: x(n-1) \leq y < xn$;
- *spojitá*, tj. každá neprázdná shora ohraničená množina $M \subset \boldsymbol{R}$ má supremum.

V geometrickém modelu lze předchozí čtyři tvrzení formulovat názorněji:

- Jsou-li X, Y dva body na ose o, nastává právě jeden z případů: $X = Y$, X leží vlevo od Y, Y leží vlevo od X.
- Mezi každými dvěma různými body existuje bod.
- Jestliže B je vnitřním bodem úsečky AX a jestliže na polopřímce AX sestrojíme posloupnost bodů $B_1 = B, B_2, B_3$, ... tak, že postupně nanášíme úsečku AB (tedy úsečka

AB_n je n-násobek úsečky AB), pak po jistém počtu kroků překročíme bod X (bod X bude prvkem jisté úsečky $B_{k-1}B_k$).

- Na číselné ose nejsou skoky (díry).

Aritmetický model množiny $\boldsymbol{R}$ je méně přehledný, lze v něm však uskutečňovat všechny aritmetické operace a dobře rozlišovat mezi racionálním a iracionálním číslem.

Od historie k dnešku

Poznámka 4.35. Problém důkazu existence iracionálních čísel je velmi starý. Již v antickém Řecku se objevila tzv. první krize matematického myšlení, která se týkala „nesouměřitelnosti úseček“. V tehdejší matematice byla známá racionální čísla i to, že jakékoliv racionální číslo lze přesnou geometrickou konstrukcí zobrazit na číselné ose. Společně se znalostí hustoty uspořádání racionálních čísel byl tehdy všeobecně přijímán názor, že jiná čísla než racionální neexistují, že každé číslo lze vyjádřit zlomkem a že každý bod číselné osy je obrazem nějakého racionálního čísla. Objev faktu, že v jakémkoliv čtverci jsou jeho strana a úhlopříčka tzv. nesouměřitelné a že délku úhlopříčky nelze vyjádřit zlomkem (má-li strana čtverce délku a, má úhlopříčka délku $\sqrt{2}\,a$), způsobil v tehdejší době doslova pozdvižení, neboť nebylo známo, jak vzniklý problém vyřešit. Z teorie už víme, že princip nesouměřitelnosti znamená to, že lineárně uspořádaná množina racionálních čísel obsahuje mezery. Vyřešení problému nesouměřitelnosti, tj. zavedení iracionálních čísel, mohlo být úspěšně teoreticky ukončeno až mnohem později, po uznání aktuálního nekonečna v díle Bernarda Bolzana.

Připomeneme nyní Cantorův axiom spojitosti, známý z geometrie. Podle něj je průnik do sebe zařazených úseček neprázdný. Po uznání aktuálního nekonečna a s tím souvisejícím zavedení limitních procesů do matematiky lze dokázat, že při nekonečném počtu do sebe zařazených úseček je průnikem pouze jednoprvková množina. Při nekonečném počtu do sebe zařazených úseček na číselné ose je tedy průnikem jediné číslo. Proto je možné iracionální číslo, které je mezerou na číselné ose (racionálním řezem 3. druhu), definovat jako průnik nekonečně mnoha do sebe zařazených úseček na číselné ose. Levé krajní body těchto úseček tvoří rostoucí shora ohraničenou posloupnost racionálních čísel, která proto musí mít limitu. Analogicky pravé krajní body tvoří klesající zdola ohraničenou posloupnost racionálních čísel, která musí mít rovněž limitu. Obě tyto limity se rovnají a jejich hodnota je hledané iracionální číslo. Uvedeme dva příklady:

a) Nechť (A, B), $A = \{x \in \boldsymbol{Q}: x^2 < 2\}$, $B = \{x \in \boldsymbol{Q}: x^2 > 2\}$ je řez třetího druhu v množině $\boldsymbol{Q}$. Budeme postupně volit čísla z množiny A i B tak, aby čísla množiny A tvořila rostoucí posloupnost a čísla z množiny B klesající posloupnost. Tyto dvojice čísel budou krajními body vnořených intervalů, kterými budeme postupně stále přesněji aproximovat hodnotu zvolené mezery (řezu 3. druhu).

$1^2 = 1;$	$2^2 = 4,$	tedy	$1 < \sqrt{2} < 2$
$(1,4)^2 = 1,96;$	$(1,5)^2 = 2,25\ ,$	tedy	$1,4 < \sqrt{2} < 1,5$
$(1,41)^2 = 1,9881;$	$(1,42)^2 = 2,0164\ ,$	tedy	$1,41 < \sqrt{2} < 1,42$
$(1,414)^2 = 1,999396;$	$(1,415)^2 = 2,002225\ ,$	tedy	$1,414 < \sqrt{2} < 1,415$
$(1,4141)^2 = 1,99967881;$	$(1,4143)^2 = 2,00024449\ ,$	tedy	$1,4141 < \sqrt{2} < 1,4143$

atd.

Uvedený proces aproximace je nekonečný a číslo $\sqrt{2}$ je tak postupně určováno se stále větší přesností. Při praktickém počítání v praxi se spokojíme s přesností, která postačuje k řešení daného matematického problému.

b) Proces postupné aproximace iracionálního čísla lze i programovat. Příkladem může být přibližné určení čísla Eulerova čísla *e*. Víme, že $2 < e < 4$. Dále z matematické analýzy víme, že platí: $\lim_{n\to\infty} (1+\frac{1}{n})^n = e$, $\lim_{n\to\infty} (1+\frac{1}{n})^{n+1} = e$, přičemž první z těchto posloupností $\left\{\left(1+\frac{1}{n}\right)^n\right\}_{n=1}^{\infty}$ je rostoucí s prvním členem *2*, druhá z těchto posloupností $\left\{\left(1+\frac{1}{n}\right)^{n+1}\right\}_{n=1}^{\infty}$ je klesající s prvním členem *4*. Obecně tedy můžeme Eulerovo číslo aproximovat pro $n \in \boldsymbol{N}$ pomocí nerovností

$$(1+\frac{1}{n})^n < e < (1+\frac{1}{n})^{n+1} .$$

Závěrečné poznámky k reálným číslům

A) Surdické výrazy

Poznámka 4.36. Surdické výrazy jsou reálná čísla tvaru $a \pm \sqrt{b}$, kde *a, b* jsou nezáporná racionální čísla, *b* není druhou mocninou žádného racionálního čísla. Jedná o velmi starou problematiku - vzorce pro úpravu surdických výrazů znal již ve 12. století indický matematik Bháskara. Pro úpravu surdických výrazů platí vztahy: (předpokládáme, že $a > \sqrt{b} \geq 0$)

$$\sqrt{a+\sqrt{b}} \pm \sqrt{a-\sqrt{b}} = \sqrt{2(a \pm \sqrt{a^2-b})} , \qquad \sqrt{a \pm \sqrt{b}} = \sqrt{\frac{a+\sqrt{a^2-b}}{2}} \pm \sqrt{\frac{a-\sqrt{a^2-b}}{2}} .$$

Pomocí uvedených dvou vztahů se některé výrazy s odmocninami téměř „zázračně“ upraví, např. výraz $\sqrt{3+2\sqrt{2}} - \sqrt{3-2\sqrt{2}}$. Zde $a = 3, b = 8$, podle prvního ze vzorců je výsledek roven *2*. Takto lze upravovat i odmocniny z vyšších čísel, např. $\sqrt{100-2\sqrt{2499}} = \sqrt{51} - 7$, $\sqrt{31+\sqrt{600}} = 5 + \sqrt{6}$, $\sqrt{x+y+2\sqrt{xy}} + \sqrt{x+y-2\sqrt{xy}} = 2\sqrt{x}$.

Poznámka 4.37. Nyní se budeme věnovat úpravám výrazu $X = \sqrt[3]{\sqrt{a}+b} - \sqrt[3]{\sqrt{a}-b}$. Pokud $\sqrt[3]{a-b^2}$ je racionální číslo, pak lze po umocnění výrazu *X* na třetí a úpravě psát $X^3 = 2b - 3\sqrt[3]{a-b^2}\,X$, což je rovnice, ze které lze hodnota *X* vypočítat. Např. ve výrazu $\sqrt[3]{\sqrt{5}+2} - \sqrt[3]{\sqrt{5}-2}$ je $a = 5, b = 2$. Rovnice je potom tvaru $X^3 = 4 - 3X$, odkud je jeden kořen $X = 1$ ihned patrný včetně toho, že další reálná řešení tato rovnice nemá. Dodejme ještě, že obdobný rozbor lze provést i v případě, kdy ve výrazu *X* je mezi odmocninami znaménko plus.

B) Algebraická a transcendentní čísla

Definice 4.38. Algebraické číslo je takové reálné číslo, které je kořenem nějakého polynomu s racionálními koeficienty. Z množiny všech polynomů, jejichž je dané algebraické číslo kořenem, vybereme polynom s nejnižším stupněm. Tento stupeň polynomu je také stupněm tohoto algebraického čísla.

Poznámka 4.39. Každé racionální číslo je algebraické. Algebraická je však i řada iracionálních čísel. Např. číslo $\sqrt{2}$ je algebraické, neboť je řešením rovnice $x^2-2 = 0$. Z poznatků algebry a geometrie plyne, že pomocí kružítka a pravítka (bez stupnice) lze sestrojit právě a jen ty úsečky, jejichž délky jsou algebraická čísla stupně mocniny dvou. Z toho plyne neřešitelnost některých geometrických úloh jako je kvadratura kruhu, trisekce úhlu či duplikace krychle (tři klasické problémy antické matematiky).

Věta 4.40.
(1) Označme A množinu všech algebraických čísel. Pak $(A, +, \cdot)$ je komutativní těleso.
(2) Kořeny polynomu, jehož koeficienty jsou algebraická čísla, jsou opět algebraická čísla.

Definice 4.41. Transcendentní číslo je takové reálné číslo, které není kořenem žádné algebraické rovnice s racionálními koeficienty.

Poznámka 4.42. (Viz [3]) Důkaz existence transcendentních čísel přinesl v roce 1844 francouzský matematik Joseph Liouville. Je zřejmé, že transcendentní čísla musí být iracionální, jejich iracionalita je však „jiného typu“ než např. u surdických čísel, která jsou algebraická. I když od roku 1840 byla známa existence transcendentních čísel, po řadu let se nedařilo dokázat transcendentnost dvou významných iracionálních čísel π a e. Až v roce 1873 dokázal Hermite transcendentnost čísla e a v roce 1882 Ferdinand von Lindemann transcendentnost čísla π.

Poznámka 4.43. Lze dokázat, že v jistém smyslu většina iracionálních čísel je transcendentních. Abychom si udělali alespoň obecnou představu o transcendentních číslech, uvedeme výsledek, který dokázali v roce 1934 Gelfand a Schneider. (Viz [3], s. 100).

Věta 4.44. Nechť α, β jsou algebraická reálná čísla, nechť β je iracionální číslo a nechť $\alpha \neq 0$, $\alpha \neq 1$. Potom všechna čísla tvaru α^{β} jsou transcendentní.

Příklad 4.45. Podle předchozí věty 4.44. mezi transcendentní čísla patří například čísla $2^{\sqrt{2}}$, $3^{\sqrt{5}}$, $\left(\sqrt[3]{7}\right)^{(2+\sqrt{3})}$, $\left(1+\sqrt{3}\right)^{\sqrt{2}}$, ...

5. Komplexní čísla

Věta 5.1. Těleso reálných čísel lze vnořit do tělesa, ve kterém má rovnice $x^2 + 1 = 0$ řešení.

Poznámka 5.2. Důkaz je konstruktivní. Konstrukci tohoto tělesa popíšeme. Označme $\boldsymbol{C}$ kartézský součin $\boldsymbol{R} \times \boldsymbol{R}$, tzn. $\boldsymbol{C} = \boldsymbol{R} \times \boldsymbol{R} = \{[a, b]; a \in \boldsymbol{R}, b \in \boldsymbol{R}\}$. Na množině $\boldsymbol{C}$ definujme operace sčítání a násobení takto:

$$[a, b] + [c, d] = [a + c, b + d] ,$$

$$[a, b] \cdot [c, d] = [ac - bd, ad + bc].$$

Lze ukázat, že $(\boldsymbol{C}, +, \cdot)$ je těleso. Neutrálním prvkem vzhledem operaci sčítání je $[0, 0]$, neutrálním prvkem vzhledem operaci násobení je $[1, 0]$; opačným prvkem k prvku $[a, b]$ je dvojice $[-a, -b]$, převráceným prvkem k prvku $[a, b]$, kde $a^2 + b^2 \neq 0$, je uspořádaná dvojice $\left[\frac{a}{a^2+b^2}, \frac{-b}{a^2+b^2}\right]$. Platí $[0, 1] \cdot [0, 1] = [-1, 0]$, tj. $[0, 1]^2 + [1, 0] = [0, 0]$.

Nechť nyní $f: \boldsymbol{R} \to \boldsymbol{C}$ je zobrazení definované pro každé reálné číslo $r \in \boldsymbol{R}$ předpisem $f(r) = [r, 0]$. Pak f je vnoření tělesa $(\boldsymbol{R}, +, \cdot)$ do tělesa $(\boldsymbol{C}, +, \cdot)$.

Definice 5.3. Těleso $(\boldsymbol{C}, +, \cdot)$ se nazývá těleso komplexních čísel.

Poznámka 5.4. Z předchozí definice plyne, že rovnice $A + X = B$ má v oboru komplexních čísel vždy jednoznačné řešení $X = B - A$ a také rovnice $A \cdot X = B$ má za podmínky $A \neq [0, 0]$ v oboru komplexních čísel vždy jednoznačné řešení $X = \frac{B}{A}$. V oboru komplexních čísel tedy lze neomezeně odčítat i dělit (kromě „dělení nulou“). Snadno lze odvodit příslušné vztahy:

$$[a, b] - [c, d] = [a - c, b - d] ,$$

$$\frac{[a,b]}{[c,d]} = \left[\frac{ac + bd}{c^2 + d^2}, \frac{bc - ad}{c^2 + d^2}\right], \quad [c, d] \neq 0.$$

Poznámka 5.5. Ve smyslu poznámky 5.2. lze ztotožnit každé reálné číslo r s komplexním číslem $[r, 0]$. Zápis $[0, 1]^2 + [1, 0] = [0, 0]$ tedy skutečně znamená, že rovnice $x^2 + 1 = 0$ má v množině všech komplexních čísel řešení. Tímto řešením je komplexní číslo $[0, 1]$. Toto číslo ale nemůže být reálné; zavádíme pro něj označení i a nazýváme ho komplexní jednotka. Protože z definice obou operací sčítání a násobení lze psát každé komplexní číslo $[a, b]$ ve tvaru $[a, b] = [a, 0] + [0, b] = [a, 0] + [b, 0] \cdot [0, 1]$, lze při uvedeném ztotožnění a označení psát $[a, b] = a + bi$.

Definice 5.6. Zápis $\alpha = a + bi$ se nazývá algebraický tvar komplexního čísla $\alpha = [a, b]$. Číslo a se nazývá reálná část komplexního čísla α , číslo b se nazývá imaginární část komplexního čísla α. . Je-li $a = 0$, říkáme, že číslo α je ryze imaginární. Reálná část komplexního čísla α se někdy také označuje $Re\alpha$, imaginární část komplexního čísla α se někdy také označuje $Im\alpha$.

Poznámka 5.7. Vzhledem k rovnosti $i^2 = -1$ platí pro mocniny čísla i následující vztahy:

$i^n = i$ pro $n \equiv 1 \pmod 4$,

$i^n = -1$ pro $n \equiv 2 \pmod 4$,

$$i^n = -i \text{ pro } n \equiv 3 \pmod 4,$$
$$i^n = 1 \text{ pro } n \equiv 0 \pmod 4.$$

V algebraickém tvaru lze potom zapsat všechny čtyři základní operace takto:

$$(a + bi) + (c + di) = (a + c) + (b + d)i\,,$$

$$(a + bi) - (c + di) = (a - c) + (b - d)i\,,$$

$$(a + bi) \cdot (c + di) = (ac - bd) + (ad + bc)i,$$

$$\frac{a+bi}{c+di} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}\,i\,.$$

Věta 5.8. V množině všech komplexních čísel ***C*** neexistuje relace uspořádání.

Definice 5.9. Nechť $\alpha = a + bi$ je komplexní číslo. Pak komplexní číslo $\overline{\alpha} = a - bi$ se nazývá komplexně sdružené číslo k číslu α. Nezáporné reálné číslo $|\alpha| = \sqrt{a^2 + b^2}$ se nazývá absolutní hodnota komplexního čísla α.

Věta 5.10. Nechť α, β jsou komplexní čísla, pak platí:

(1) $|\alpha| = 0 \Leftrightarrow \alpha = 0$;

(2) $|-\alpha| = |\alpha|$;

(3) $|\alpha + \beta| \le |\alpha| + |\beta|$;

(4) $|\alpha \cdot \beta| = |\alpha| \cdot |\beta|$;

(5) $|\alpha - \beta| \ge \big||\alpha| - |\beta|\big|$;

(6) $\dfrac{|\alpha|}{|\beta|} = \left|\dfrac{\alpha}{\beta}\right|$ pro $\beta \neq 0$;

(7) $|\alpha|^2 = \alpha \cdot \overline{\alpha}$;

(8) $\overline{\alpha + \beta} = \overline{\alpha} + \overline{\beta}$;

(9) $\overline{\alpha \cdot \beta} = \overline{\alpha} \cdot \overline{\beta}$;

(10) $Re\,\alpha = \dfrac{1}{2}(\alpha + \overline{\alpha})$, $Im\,\alpha = -\dfrac{i}{2}(\alpha - \overline{\alpha})$.

Poznámka 5.11. Víme už, že v oboru všech komplexních čísel lze provádět všechny čtyři základní operace sčítání, odčítání, násobení a dělení (kromě dělení nulou). Nyní se budeme zabývat mocninami a odmocninami komplexních čísel. K tomu ale musíme zavést vhodnější vyjádření komplexního čísla než je algebraický tvar. Znázorníme-li každé komplexní číslo $a + bi$ geometricky v tzv. Gaussově rovině, bude jeho obraz ležet v bodě s kartézskými souřadnicemi $[a, b]$. Z matematické analýzy je však známo ještě vyjádření polohy bodu pomocí polárních souřadnic. V těchto souřadnicích se kartézské průměty na osy x, y nahradí vzdáleností daného bodu od počátku soustavy souřadnic a orientovaným úhlem, který svírá průvodič spojující daný bod s počátkem soustavy souřadnic s polopřímkou vyjadřující kladný směr osy x. Např. bod $[1, 1]$ má v polárních souřadnicích vyjádření $\sqrt{2}\,(\cos 45° + \sin 45°)$, bod $[-\sqrt{3}, 1]$ má v polárních souřadnicích vyjádření $2(\cos 150° + \sin 150°)$, atd. Vyjádříme-li tímto způsobem komplexní číslo, řekneme, že jsme ho vyjádřili v goniometrickém tvaru.

Komplexní číslo $\alpha = a + bi$ je tedy v goniometrickém tvaru $\alpha = r(\cos \varphi + i \sin \varphi)$. V tomto vyjádření $r = |\alpha|$ a úhel φ určíme pomocí znalostí *a, b* a znalostí zavedení goniometrických funkcí pomocí jednotkové kružnice.

Věta 5.12. Nechť $\alpha = r(\cos \varphi + i \sin \varphi)$, $\beta = s(\cos \psi + i \sin \psi)$, $\beta \neq 0$ jsou komplexní čísla. Pak platí:

(1) $\alpha \cdot \beta = rs(\cos(\varphi + \psi) + i \sin(\varphi + \psi))$,

(2) $\frac{\alpha}{\beta} = \frac{r}{s}(\cos(\varphi - \psi) + i \sin(\varphi - \psi))$.

Poznámka 5.13. Pro libovolné komplexní číslo existuje jeho *n*-tá mocnina. Je-li dané číslo vyjádřeno v algebraickém tvaru, lze užít binomickou větu, kde mocniny čísla *i* převádíme podle poznámky 5.7. Je-li ve tvaru goniometrickém, užijeme tzv. Moivreovu větu. Tento postup bývá početně snazší.

Věta 5.14. (Moivreova). Nechť $\alpha = r(\cos \varphi + i \sin \varphi)$ je libovolné komplexní číslo, nechť $n \in \boldsymbol{N}$. Pak platí:

$$\alpha^n = r^n(\cos n\varphi + i \sin n\varphi).$$

Poznámka 5.15. Nyní obrátíme pozornost k odmocninám komplexních čísel. Protože v oboru $\boldsymbol{C}$ neexistuje relace uspořádání, nemá smysl uvažovat o kladných či záporných komplexních číslech, a proto pro každé $n \in \boldsymbol{N}$ existuje *n*-tá odmocnina z komplexního čísla α. Označíme-li tuto odmocninu z , platí pro ni vztah $z = \sqrt[n]{\alpha}$, tedy $z^n = \alpha$. Poslední rovnice je však rovnicí binomickou, jejíž řešení je z algebry známé. Víme dokonce, že tato rovnice má *n* řešení, protože těleso komplexních čísel je algebraicky uzavřené. Existuje tedy celkem *n* odmocnin *n*-tého řádu z komplexního čísla α.

Věta 5.16. Nechť je dána binomická rovnice $z^n = \alpha$. Číslo α vyjádříme v goniometrickém tvaru jako $\alpha = r(\cos \varphi + i \sin \varphi)$, pak řešení dané rovnice je:

$$z_k = \sqrt[n]{r}(\cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n}),\ k = 0, 1, \ldots, n-1.$$

Poznámka 5.17. Postupným konstruováním jednotlivých číselných oborů od polookruhu čísel přirozených až k tělesu komplexních čísel jsme dospěli ke struktuře, která je z algebraického hlediska „nejbohatší“. I když v $\boldsymbol{C}$ neexistuje uspořádání, lze provádět všechny čtyři základní operace (kromě dělení nulou) a pro každé komplexní číslo existuje jeho mocnina i odmocnina libovolného řádu. Těleso komplexních čísel je algebraicky uzavřené, tedy každý polynom stupně *n* má v $\boldsymbol{C}$ právě *n* kořenů (počítáme-li každý tolikrát, kolik je jeho násobnost). Proto již z praktického hlediska nemá větší význam zkoumat další možnosti rozšíření tělesa komplexních čísel. I když existuje rozšíření na těleso kvaternionů, není účelné se na tomto místě touto problematikou zabývat.

6. Cyklické grupy

Poznámka 6.1. V dalším textu budeme někdy (nebude-li možno dojít k nedorozumění) algebraické struktury označovat pouze symbolem jejich nosné množiny, tzn. např. místo označení grupy *(G, +)* budeme psát pouze *G*. Text této, 6. části, je volně zpracován podle publikací [9] a [11], v níž lze nalézt i důkazy jednotlivých tvrzení.

Poznámka 6.2. Nechť *G* je grupa. Ze základního kurzu algebry víme, že průnik libovolného počtu podgrup grupy *G* je rovněž podgrupa grupy *G*.

Věta 6.3. Nechť *G* je grupa, nechť *M* je libovolná podmnožina množiny *G*. Symbolem $\langle M \rangle$ označme průnik všech podgrup v *G*, které obsahují množinu *M*. Pak $\langle M \rangle$ je nejmenší podgrupa v *G* (z hlediska její mohutnosti), obsahující množinu *M*.

Definice 6.4. Podgrupa $\langle M \rangle$ se nazývá podgrupa generovaná množinou *M*. Je-li *M = {a},* pak budeme psát $\langle a \rangle$ a hovořit o podgrupě generované prvkem *a* .

Příklad 6.5. *G = {1, 2, 3}, S(G) = {e, a, b, c, d, f}* je grupa všech permutací množiny *G,* kde:

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},\ a = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix},\ b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix},$$

$$c = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},\ d = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},\ f = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}.$$

Sestavíme operační tabulku grupy *(S(G), o),* kde *o* je operace skládání permutací:

o	*e*	*a*	*b*	*c*	*d*
			f		
e	*e*	*a*	*b*	*c*	*d*
a	*f*				
b	*a*	*e*	*d*	*f*	*b*
c	*c*				
d	*b*	*c*	*e*	*a*	*f*
f	*d*				
	c	*b*	*f*	*d*	*e*
	a				
	d	*f*	*a*	*e*	*c*
	b				
	f	*d*	*c*	*b*	*a*
	e				

Grupa *(S(G), ∘)* má tyto podgrupy:

$H_1 = \{e\},\ H_2 = \{e, a\},\ H_3 = \{e, b\},\ H_4 = \{e, f\},\ H_5 = \{e, c, d\},\ H_6 = S(G).$

Pak platí:

$$\langle e \rangle = H_1,\ \langle a \rangle = H_2,\ \langle b \rangle = H_3,\ \langle c \rangle = \langle d \rangle = H_5,\ \langle f \rangle = H_4,\ \langle \{a, b\} \rangle = H_6.$$

Věta 6.6. Nechť *G* je grupa, nechť $a \in G$. Potom $\langle a \rangle = \{a^k;\ k \in \mathbf{Z}\}$.

Definice 6.7. Grupa *G,* která je generovaná jedním prvkem, tj. $G = \langle a \rangle$, se nazývá cyklická grupa. Prvek *a* se nazývá základní prvek cyklické grupy.

Příklad 6.8.

a) Grupa $G = \{1, -1, i, -i\}$ čtvrtých odmocnin z jedné je cyklická, základními prvky jsou buď i nebo $-i$.
b) Grupa $(\mathbf{Z}, +)$ je cyklická, základními prvky jsou buď 1 nebo -1.
c) Grupa $(\mathbf{Z}_m, +)$ je cyklická, základní prvek je C_1.

Definice 6.9. Nechť *G* je konečná grupa. Pak počet prvků této grupy se nazývá řád grupy *G* .

Věta 6.10. (Lagrange) V libovolné konečné grupě *G* je řád této grupy *G* dělitelný řádem každé její podgrupy.

Věta 6.11. Nechť $G = \langle a \rangle$ je konečná cyklická grupa řádu *n* (tj. $G = \{e = a^0, a^1, a^2, ..., a^{n-1}\}$). Pak prvek a^k je základním prvkem grupy $G \Leftrightarrow NSD(k, n) = 1$.

Příklad 6.12. Grupa $(\mathbf{Z}_6, +)$ je cyklická grupa řádu *6*, základními prvky jsou C_1 nebo C_5 .

7. Faktorové struktury

Definice 7.1. Nechť $(G, \cdot)$ je grupoid. Nechť $X, Y \subseteq G$. Pak součinem množin X, Y rozumíme množinu $X \cdot Y = \{z;\ z = x \cdot y;\ x \in X,\ y \in Y\}$. Je-li jedna z množin X, Y jednoprvková, např. $X = \{x\}$, pak místo zápisu $\{x\} \cdot Y$ budeme psát pouze $x \cdot Y$ nebo stručně xY.

Definice 7.2. Nechť $(G, \cdot)$ je grupoid, nechť Ω je rozklad na množině G. Pak Ω nazveme vytvořující rozklad na grupoidu G, jestliže pro každé dvě třídy $X, Y \in \Omega$ existuje třída $Z \in \Omega$ s vlastností $X \cdot Y \subseteq Z$. Položíme-li $X \circ Y = Z$, pak $(\Omega, \circ)$ je grupoid, který nazýváme faktoroid grupoidu G (nebo krátce faktorgrupoid).

Příklad 7.3. a) Nechť $(G, \cdot)$ je libovolný grupoid. Pak nejhrubší rozklad $\Omega_1 = \{G\}$ i nejjemnější rozklad $\Omega = \{\{g\};\ g \in G\}$ jsou vytvořující.
b) Nechť m je pevné přirozené číslo větší než dvě. Nechť $\mathbf{Z}_m = \{C_0, \ldots, C_{m-1}\}$ je rozklad množiny $\mathbf{Z}$ na zbytkové třídy. Pak tento rozklad je vytvořující a $(\mathbf{Z}_m, +)$ je faktorgrupoid grupoidu $(\mathbf{Z}, +)$.

Definice 7.4. Nechť $(G, \cdot)$ je grupoid, nechť $\equiv$ je relace ekvivalence na G. Pak $\equiv$ je relace kongruence na grupoidu $(G, \cdot)$, jestliže platí

$$a \equiv b \Rightarrow a \cdot c \equiv b \cdot c,\ c \cdot a \equiv c \cdot b \text{ pro libovolné } a, b, c \in G.$$

Věta 7.5. Nechť $(G, \cdot)$ je grupoid, nechť $\equiv$ je relace ekvivalence na G. Pak jsou následující výroky ekvivalentní:
(1) Relace $\equiv$ je kongruence na $(G, \cdot)$;
(2) $a \equiv b, c \equiv d \Rightarrow a \cdot c \equiv b \cdot d$ pro libovolné $a, b, c, d \in G$.

Věta 7.6. Nechť $(G, \cdot)$ je grupoid, nechť $\equiv$ je relace ekvivalence na G, nechť Ω je rozklad na G příslušný ekvivalenci $\equiv$. Pak relace $\equiv$ je kongruence na grupoidu $(G, \cdot)$, právě když Ω je vytvořujícím rozkladem.

Věta 7.7. Nechť $(G, \cdot)$ je grupa, nechť $(H, \cdot)$ je podgrupa grupy G. Pak $\{a \cdot H;\ a \in G\}$, resp. $\{H \cdot a;\ a \in G\}$ jsou rozklady na G.

Definice 7.8. Nechť H je podgrupa grupy G. Pak rozklad $\{a \cdot H;\ a \in G\}$, resp. $\{H \cdot a;\ a \in G\}$ se nazývá levý, resp. pravý rozklad grupy G podle podgrupy H. Označení: $G/_l H$, $G/_p H$. Třída $a \cdot H$, resp. $H \cdot a$ tohoto rozkladu se nazývá levá, resp. pravá třída prvku a vzhledem k podgrupě H.

Poznámka 7.9. Z předchozího plynou následující důsledky:
1. $a \in a \cdot H$, $a \in H \cdot a$ (neboť $a = a \cdot e = e \cdot a$, $e \in H$),
2. $H \in G/_l H$, $H \in G/_p H$ (neboť $H = e \cdot H = H \cdot e$),
3. $x \in a \cdot H \Leftrightarrow x \cdot H = a \cdot H$ (tedy každá levá třída je určena libovolným svým prvkem; podobně pro pravé třídy),

4. $H \cdot H = H$.

Věta 7.10. Nechť $(G, \cdot)$ je grupa, nechť $(H, \cdot)$ je podgrupa grupy G, nechť $a, b \in G$. Pak platí:
(1) a, b patří do jedné třídy $G/_l H \Leftrightarrow a^{-1} \cdot b \in H$,
(2) a, b patří do jedné třídy $G/_p H \Leftrightarrow b \cdot a^{-1} \in H$.

Věta 7.11. Nechť $(G, \cdot)$ je grupa, nechť $(H, \cdot)$ je podgrupa grupy G, nechť $a, b \in G$ jsou libovolné prvky. Pak existují následující bijektivní zobrazení $f: a \cdot H \to H \cdot a$, $g: a \cdot H \to b \cdot H$, $h: G/_l H \to G/_p H$.

Poznámka 7.12. Třídy rozkladu jsou stejně početné vzhledem k dané grupě. Všechny třídy rozkladu (pravé i levé) jsou stejně početné vzhledem k libovolnému prvku. Počet tříd v levém i pravém rozkladu vzhledem ke stejné podgrupě je stejný.

Definice 7.13. Podgrupa H grupy G se nazývá invariantní podgrupa (někdy též normální dělitel), jestliže pro každý prvek $a \in G$ platí $a \cdot H = H \cdot a$.

Věta 7.14. Nechť $(G, \cdot)$ je grupa, nechť $(H, \cdot)$ je podgrupa grupy G. pak jsou následující výroky ekvivalentní:
(1) H je normální dělitel,
(2) $h \in H,\ g \in G$ libovolně $\Rightarrow\ g^{-1} \cdot h \cdot g \in H$,
(3) $g \in G$ libovolně $\Rightarrow\ g^{-1} \cdot H \cdot g = H$,
(4) $G/_l H = G/_p H$,
(5) $G/_l H,\ G/_p H$ jsou vytvořující rozklady na grupě G.

Poznámka 7.15. Je-li H je normální dělitel v grupě G, pak $G/_l H = G/_p H$. Proto se v tomto případě užívá pouze označení G/H. Rozklad G/H je vytvořujícím rozkladem na G. Poznamenejme ještě, že v komutativní grupě je každá podgrupa invariantní.

Poznámka 7.16. Z teorie cyklických grup víme, že řádem konečné grupy je počet prvků této grupy. Dále je dokazována Lagrangeova věta, podle které v konečné grupě je její řád dělitelný řádem každé její podgrupy. Odtud mj. plyne, že konečná grupa, jejíž počet prvků je prvočíslo, má pouze dvě podgrupy: triviální a sebe samu. Pro každou (konečnou) podgrupu H konečné grupy G dále platí, že počet prvků ve všech třídách rozkladů $G/_l H,\ G/_p H$ je stejný a je roven počtu prvků podgrupy H, a že počet tříd rozkladů $G/_l H,\ G/_p H$ je rovněž stejný.

Definice 7.17. Nechť H je podgrupa konečné grupy G. Pak systémy $G/_l H,\ G/_p H$ mají stejný počet tříd, který se nazývá index podgrupy H v grupě G.

Věta 7.18. Nechť H je podgrupa konečné grupy G. Pak řád grupy G je součinem řádu podgrupy H a indexu podgrupy H v grupě G. (Důsledkem je Lagrangeova věta.)

Věta 7.19. Nechť $(H, \cdot)$ je invariantní podgrupa grupy $(G, \cdot)$. Pak faktorgrupoid $(G/H, \circ)$ je grupa. Jednotkovým prvkem této grupy je třída H a pro libovolné $x, y \in G$ platí:

$$(x \cdot H) \circ (y \cdot H) = (x \cdot y) \cdot H, \qquad (x \cdot H)^{-1} = x^{-1} \cdot H.$$

Definice 7.20. Nechť $(H, \cdot)$ je invariantní podgrupa grupy $(G, \cdot)$. Pak faktorgrupoid $(G/H, \circ)$ se nazývá faktorgrupa grupy G podle normální podgrupy H.

Věta 7.21. Všechny vytvořující rozklady na grupě jsou právě rozklady grupy vytvořené jejími invariantními podgrupami, tedy jediné faktorgrupoidy grupy jsou její faktorgrupy.

Příklad 7.22. V příkladu 6.5. byla uvedena grupa $(S(G), \circ)$ permutací tříprvkové množiny a všechny její podgrupy. Uvažujme dvě z nich, a to nejprve podgrupu $H = \{e, a\}$ a potom podgrupu $K = \{e, c, d\}$. Platí:

a) $S(G)/_l H = \{\{e, a\}, \{b, c\}, \{d, f\}\}$, $S(G)/_p H = \{\{e, a\}, \{b, d\}, \{c, f\}\}$, tj. $S(G)/_l H \neq S(G)/_p H$. Podgrupa H není invariantní. Řád podgrupy H je 2, její index je 3.

b) $S(G)/_l K = \{\{e, c, d\}, \{a, b, f\}\}$, $S(G)/_p K = \{\{e, c, d\}, \{a, b, f\}\}$, tedy $S(G)/_l K = S(G)/_p K$. Podgrupa K je tedy invariantní a platí $S(G)/K = \{\{e, c, d\}, \{a, b, f\}\}$. Řád podgrupy K je 3, její index je 2. Označme nyní třídy rozkladu $S(G)/K$, např. $E = \{e, c, d\}$, $A = \{a, b, f\}$, pak faktorgrupa $(S(G)/K, \circ)$ grupy $(S(G), \circ)$ je určena operační tabulkou

o	E	A
E	E	A
A	A	E

Definice 7.23. Nechť $(R, +, \cdot)$ je okruh. Neprázdná množina $I \subseteq R$ se nazývá ideál okruhu R, jestliže platí:
(1) $i, j \in I \Rightarrow i - j \in I$,
(2) $i \in I, r \in R \Rightarrow i \cdot r \in I, r \cdot i \in I$.

Poznámka 7.24. Platí, že $(I, +, \cdot)$ je podokruh okruhu $(R, +, \cdot)$ a $(I, +)$ je invariantní podgrupa grupy $(R, +)$. Rozklad $(R, +)/(I, +)$ budeme značit pouze R/I. Poznamenejme dále, že každý okruh obsahuje dva základní ideály, a to nulový ideál $\{0_R\}$ a nevlastní ideál R.

Věta 7.25. Nechť R je okruh, I jeho ideál. Pak rozklad R/I je vytvořující rozklad na grupoidu $(R, \cdot)$.

Věta 7.26. Nechť R je okruh, I jeho ideál. Pak $(R/I, +, \cdot)$ je okruh, jehož operace jsou definovány následujícím způsobem: Nechť a, b jsou libovolné prvky množiny R. Pak platí

$$(a + I) + (b + I) = (a + b) + I, \qquad (a + I) \cdot (b + I) = (a \cdot b) + I .$$

Definice 7.27. Nechť R je okruh, I jeho ideál. Pak okruh $(R/I, +, \cdot)$ se nazývá faktorokruh okruhu R podle ideálu I.

Věta 7.28. Nechť $(R, +, \cdot)$ je okruh a Ω vytvořující rozklad na grupoidech $(R, +)$ i $(R, \cdot)$, tentýž na obou těchto grupoidech. Nechť $I \in \Omega$ je ta třída, která obsahuje 0_R. Pak I je ideál okruhu R a platí $R/I = \Omega$.

Definice 7.29. Nechť R je okruh, I jeho ideál. Řekneme, že prvky $a, b \in R$ jsou kongruentní podle ideálu I, jestliže platí $a - b \in I$. Píšeme $a \equiv b \ (I)$.

Věta 7.30. Nechť R je okruh, I jeho libovolný ideál. Kongruence podle ideálu I je kongruence na grupoidech $(R, +)$ i $(R, \cdot)$, rozklad příslušný této kongruenci je R/I.

Věta 7.31. Nechť $(R, +, \cdot)$ je okruh. Pak všechny kongruence na grupoidech $(R, +)$ i $(R, \cdot)$ jsou kongruencemi podle některého ideálu okruhu R. Každý faktorokruh okruhu R je tedy faktorokruhem podle některého ideálu. okruhu R.

8. Svazy a Booleovy algebry

Definice 8.1. Svazem nazýváme algebraickou strukturu $S = (S, \wedge, \vee)$ se dvěma binárními operacemi průsek ($\wedge$) a spojení ($\vee$), které splňují pro každé tři prvky $a, b, c \in S$ následující podmínky:

(1) $a \wedge (b \wedge c) = (a \wedge b) \wedge c$, $a \vee (b \vee c) = (a \vee b) \vee c$,

(2) $a \wedge b = b \wedge a$, $a \vee b = b \vee a$,

(3) $a \wedge a = a$, $a \vee a = a$,

(4) $a \wedge (a \vee b) = a$, $a \vee (a \wedge b) = a$.

Poznámka 8.2. Svaz lze také definovat jako uspořádanou množinu $(S, \leq)$, v níž pro každé dva prvky a, b existuje jejich infimum (ozn. $\wedge$) a supremum (ozn. $\vee$).

Definice 8.3. Svaz $(S, \wedge, \vee)$ se nazývá:

(1) distributivní, jestliže pro každé $a, b, c \in S$ platí $a \wedge (b \vee c) = (a \wedge b) \vee (a \wedge c)$, $a \vee (b \wedge c) = (a \vee b) \wedge (a \vee c)$;

(2) modulární, jestliže pro každé $a, b, c \in S$ splňující $a \leq c$ platí $a \vee (b \wedge c) = (a \vee b) \wedge c$;

(3) komplementární, jestliže má nejmenší prvek 0 a největší prvek 1 a ke každému prvku $a \in S$ existuje jeho komplement, tj. prvek $b \in S$ s vlastností $a \vee b = 1$, $a \wedge b = 0$;

(4) booleovský, je-li distributivní a komplementární (pak jsou komplementy určeny jednoznačně);

(5) úplný, jestliže pro každou podmnožinu množiny S (i nekonečnou) existuje její supremum a infimum.

Definice 8.4. Svaz, který je úplný, distributivní a komplementární (doplňkový), se nazývá Booleova algebra.

Poznámka 8.5. Booleovu algebru je možno definovat přímo, bez využití svazové interpretace. To je obsahem následující definice.

Definice 8.6. Nechť B je neprázdná množina, na níž jsou definovány dvě binární operace $+, \cdot$ a jedna unární operace $`$ (doplněk), splňující pro každé $x, y, z \in B$ následující axiomy (symbol pro násobení $\cdot$ budeme bez újmy na srozumitelnosti často vynechávat):

(1) $x + y = y + x$, $x y = y x$

(2) $x + (y + z) = (x + y) + z$, $x(y z) = (x y) z$

(3) $x \cdot (y + z) = (x y) + (x z)$, $x + (y z) = (x + y) \cdot (x + z)$

(4) $x + 0 = x$, $x \cdot 1 = x$

(5) $x + x` = 1$ , $x \cdot x` = 0$.

Pak algebraická struktura $(B, +, \cdot)$ se nazývá Booleova algebra.

Poznámka 8.7. V interpretaci Booleovy algebry pomocí svazů je operace sčítání (ozn.+) jiným označením operace spojení (ozn. $\vee$) a operace násobení (ozn. $\cdot$) jiným označením

operace průsek (ozn. $\wedge$). Pro „počítání“ v Booleově algebře platí kromě axiomů z definice řada zajímavých pravidel. Některé z nich jsou obsahem následující věty:

Věta 8.8. Nechť $(B, +, \cdot)$ je Booleova algebra, nechť $x, y \in B$. Pak platí:

(1) $(x`)` = x$,

(2) $1` = 0$ , $0` = 1$,

(3) $x + x = x$, $x \cdot x = x$,

(4) $x + 1 = 1$, $x \cdot 0 = 0$,

(5) $(x + y)` = x` \cdot y`$ , $(x \cdot y)` = x` + y`$,

(6) $x + (x \cdot y) = x$, $x \cdot (x + y) = x$,

(7) $x + (x` \cdot y) = x + y$ , $x \cdot (x` + y) = x \cdot y$,

(8) $x + y = 0 \Leftrightarrow x = 0$ a $y = 0$, $x \cdot y = 1 \Leftrightarrow x = 1$ a $y = 1$,

(9) $x = y \Leftrightarrow x y` + x` y = 0$,

(10) $x = y \Leftrightarrow (x + y`) \cdot (x` + y) = 1$.

Poznámka 8.9. V Booleově algebře platí princip duality: Nechť φ je platná formule Booleovy algebry. Jestliže v této formuli nahradíme operaci sčítání násobením a naopak, operaci násobení sčítáním, a dále zaměníme prvky *0, 1,* dostaneme opět platnou formuli Booleovy algebry. Jako ilustrace může sloužit předchozí definice a věta.

Poznámka 8.10. Existují dva nejvýznamnější modely Booleovy algebry, a to množinová algebra a algebra pravdivostních hodnot výroků.

a) Množinová algebra. Nechť M je neprázdná množina. Nosičem B Booleovy algebry bude systém 2^M všech podmnožin množiny M, roli operace sčítání bude hrát operace sjednocení množin a roli operace násobení bude hrát operace průnik množin. Jako doplněk prvku Booleovy algebry bude vystupovat doplněk množiny v množině M. Prvkem *0* bude prázdná množina, prvkem *1* základní množina M.

b) Algebra pravdivostních hodnot výroků. $B = \{0, 1\}$, jako operace sčítání bude figurovat disjunkce výroků, jako násobení bude figurovat konjunkce výroků. Roli doplňku bude hrát negace výroku, prvkem *0* bude nepravdivý výrok, prvkem *1* pravdivý výrok.

V tomto smyslu lze konstatovat, že množinová algebra i algebra pravdivostních hodnot výroků mají tentýž matematický základ.

Příklad 8.11. Zjednodušte zápis množiny:

$$(A \cap E \cap C) \cup [(D \cap A)` \cup B]` \cup (E \cap C` \cap A) \cup [(B \cup D)` \cap A]` .$$

Řešení: Zadaný zápis množiny přepíšeme do Booleovy algebry. Dostaneme booleovský výraz, který upravíme:

$aec + [(da)` + b]` + ec`a + [(b + d)`a] = ae(c + c`) + dab` + b`d`a = ae + ab`(d + d`) = ae + ab` = a(e + b`)$.

Po zpětném přepisu do symboliky množinové algebry dostaneme hledané zjednodušení:

$$A \cap (E \cup B`) .$$

9. Číselné soustavy

Poznámka 9.1. Problematika zápisů čísel provází lidstvo už od starověku. Je známá řada poznatků o způsobech numerace během historického vývoje, např. numerace ve starém Egyptě a Mezopotámii, numerace antického Řecka a Říma nebo numerace starých Mayů. Jedná se o velmi zajímavé otázky, kterými se však na tomto místě nemůžeme zabývat. Konstatujme pouze, že během vývoje se vykrystalizovaly dva typy číselných soustav, a to poziční a nepoziční. Základní rozdíl je v tom, že nepoziční soustavy nerozlišují řád číslice v zápisu čísla, kdežto poziční soustavy ano. Většina numeračních soustav v dávné historii byla nepoziční (Egypt, Mezopotámie, Řecko, Řím), zatímco v dnešní době se užívají výhradně poziční soustavy. Jediná nepoziční soustava, se kterou se ještě dnes můžeme setkat, jsou římské číslice. Uvědomme si ovšem, že s římskými číslicemi nepočítáme (neprovádíme žádné početní výkony), slouží pouze jako zápisy letopočtů atp. Poziční soustavy, jak už bylo řečeno, rozlišují řád číslice. Proto je potřeba mít určen tzv. základ poziční číselné soustavy. Dnes se užívá pro běžné počítání výhradně soustava se základem deset (desítková soustava). Ve výpočetní technice se můžeme setkat ještě se soustavami, jejichž základem jsou některé mocniny čísla dvě (soustava dvojková, čtyřková, osmičková a šestnáctková). Pozičním číselným soustavám bude věnována tato kapitola. Budeme se zabývat převody zápisů čísel a početními výkony v nedesítkových číselných soustavách. Zřejmě se můžeme omezit pouze na kladná čísla; začneme čísly přirozenými a následně si uvedeme i převody zápisů čísel racionálních.

Příklad 9. 2. Nepoziční soustavy nerozlišují řád číslice, zatímco poziční soustavy ano. Tedy např. v zápise římskými číslicemi je číslo I I I rovno třem, zatímco v desítkové soustavě je číslo 111 rovno sto jedenácti. Nepoziční soustavy nemají symbol pro nulu, který je naopak v pozičních soustavách nutný. Např. čísla stojedna, tisíc jedna jsou zapsána v desítkové soustavě 101, 1001, zatímco pomocí římských číslic C I, M I.

Věta 9. 3. Nechť z je pevně zvolené přirozené číslo větší než jedna, nechť a je libovolné přirozené číslo. Pak platí:
(1) Existuje přirozené číslo n s vlastností $z^n \leq a < z^{n+1}$.
(2) Číslo a lze vyjádřit právě jedním způsobem ve tvaru

$$a = a_n z^n + a_{n-1} z^{n-1} + a_{n-2} z^{n-2} + \ldots + a_2 z^2 + a_1 z + a_0 , \qquad (\star)$$

kde a_i , $i = 0, 1, 2, \ldots, n$ jsou nezáporná celá čísla menší než z.

Definice 9. 4. Nechť platí označení předchozí věty a pro čísla a, n platí vyjádření $(\star)$. Pak říkáme, že jsme číslo a vyjádřili v číselné soustavě o základu z. Zkráceně píšeme $a = (a_n a_{n-1} \ldots a_0)_z$, přičemž závorky lze v zápisu vynechat. Číslo z nazýváme základ číselné soustavy, symboly a_i , $i = 0, \ldots, n$ se nazývají číslice (cifry). O číslici a_i říkáme, že je řádu i, číslo z^i se nazývá jednotka řádu i pro $i = 0, \ldots, n$.

Poznámka 9. 5. Je-li $z > 10$, plyne z předchozí věty, že v soustavě o základu z musí existovat právě z různých cifer $0, 1, \ldots, z - 1$. Protože v běžně užívané desítkové soustavě máme k dispozici pouze deset cifer $0, \ldots, 9$, je nutno doplnit další symboly. Podle mezinárodní

konvence se užívá $A = 10, B = 11, C = 12, D = 13, E = 14, F = 15$. Soustavy o základu větším než 16 se již nepoužívají, proto není potřeba zavádět další symboly.

Poznámka 9. 6. (Porovnávání čísel). V každé poziční číselné soustavě platí stejná pravidla pro porovnávání čísel jako v soustavě desítkové (obecně není problém ověřit). Konkrétně tedy platí: Obsahuje-li zápis přirozeného čísla a v číselné soustavě o základu z právě n číslic (číslice nejvyššího řádu je nenulová), pak $z^{n-1} \leq a < z^n$. Jsou.li zapsána dvě přirozená čísla a, b v číselné soustavě o stejném základu (číslice nejvyššího řádu jsou nenulové), pak platí:
1. To číslo, v jehož zápisu je více číslic, je větší.
2. Mají-li zápisy obou čísel stejný počet číslic, pak je větší to číslo, v jehož zápisu číslice nejvyššího řádu označuje větší přirozené číslo.
3. Nechť dvě různá čísla a, b jsou zapsána v téže soustavě zápisem o stejném počtu číslic, tj. $(a_n a_{n-1} \ldots a_0)_z$, $(b_n b_{n-1} \ldots b_0)_z$. Existuje-li číslo k $(0 \leq k < n)$ s vlastností $a_i = b_i$ pro $i = n, n-1, \ldots, k+1, a_k \neq b_k$, pak větší je to číslo, v jehož zápise číslice řádu k označuje větší přirozené číslo.

Poznámka 9. 7. (Převádění zápisů přirozených čísel) Při převádění zápisu přirozeného čísla a z desítkové soustavy do číselné soustavy o základu z postupujeme tak, že číslo a vydělíme číslem z se zbytkem. V dalším kroku vezmeme neúplný podíl předchozího dělení a opět dělíme základem soustavy. Takto pokračujeme tak dlouho, dokud není neúplný podíl roven nule (po konečném počtu dělení tento případ musí nastat). Hledaný zápis čísla a v soustavě o základu z je určen všemi zbytky po všech provedených děleních, které napíšeme vedle sebe počínaje od posledního k prvnímu. Při praktickém převádění využíváme nejčastěji jednoduché schéma o dvou sloupcích, které si ilustrujeme nejprve pro $a = 986, z = 4$, pak pro $a = 2507, \ z = 16$. Do prvního řádku zapíšeme do záhlaví čísla a, z, do levého sloupce píšeme neúplné podíly a do pravého sloupce zbytky. Výsledný zápis pak získáme zapsáním zbytků „odspodu nahoru“. Obrácený převod z nedesítkové do desítkové soustavy se provádí rozvojem v nedesítkové soustavě.

Příklad 9. 8.

986	4
246	2
61	2
15	1
3	3
0	3

$$986 = 33122_4 .$$

Zkouška: $3122_4 = 3 . 4^4 + 3 . 4^3 + 1 . 4^2 + 2 . 4 + 2 = 3 . 256 + 3 . 64 + 16 + 8 + 2 = 986.$

Příklad 9. 9.

2507	16
156	11
9	12
0	9

$$2057 = 9CB_{16} .$$

Zkouška: $9CB_{16} = 9 . 16^2 + 12 . 16 + 11 = 9 . 256 + 12 . 16 + 11 = 2304 + 192 + 11 = 2507.$

Povšimněme si, že v případě $z > 10$ přepisujeme dvouciferné zbytky pomocí písmen a opačně, při rozvoji čísla místo písmene použijeme příslušné dvouciferné číslo.

Poznámka 9. 10. Na základě poznámky 9.7. lze nyní převést zápis jakéhokoliv přirozeného čísla z desítkové soustavy do nedesítkové a naopak. V případě, že chceme převést zápis přirozeného čísla zapsaného v nedesítkové soustavě do jiné nedesítkové soustavy, je nejvýhodnější přechod přes desítkovou soustavu. Existují ovšem případy (a jsou hojně využívány zejména v informatice), kdy lze takový převod mezi dvěma nedesítkovými soustavami provést přímo. To lze provést tehdy, jestliže pro dva základy soustav z_1 , z_2 platí vztah $z_1 = z_2^n$ pro nějaké přirozené číslo n. S ohledem na praktické využití jsou důležité zejména přímé převody mezi soustavou dvojkovou a čtyřkovou, dvojkovou a osmičkovou, dvojkovou a šestnáctkovou, resp. mezi čtyřkovou a šestnáctkovou. Převody se provádí na základě následující věty:

Věta 9. 11. Nechť pro dva základy soustav z_1 , z_2 platí vztah $z_1 = z_2^n$ pro nějaké přirozené číslo n. Pak číslo zapsané n ciframi v číselné soustavě o základu z_2 lze zapsat jedinou cifrou v číselné soustavě o základu z_1 .

Příklad 9. 12. Převeďte číslo 110110010110_2 do soustavy se základem 8.
Víme, že $8 = 2^3$. Platí : $110101010110_2 = 1 . 2^{11} + 1 . 2^{10} + 0 . 2^9 + 1 . 2^8 + 0 . 2^7 + 1 . 2^6 + 0 . 2^5 + 1 . 2^4 + 0 . 2^3 + 1 . 2^2 + 1 . 2 + 0 = (1 . 2^2 + 1 . 2 + 0) . (2^3)^3 + (1 . 2^2 + 0 . 2 + 1) . (2^3)^2 + (0 . 2^2 + 1 . 2 + 0) . 2^3 + (1 . 2^2 + 1 . 2 + 0) = 6 . 8^3 + 5 . 8^2 + 2 . 8 + 6 = 6526_8$.

Poznámka 9. 13. Postup uvedený v předchozím příkladu je těžkopádný a nepřehledný. V praxi postupujeme tak, že při převodu zápisu přirozeného čísla ze základu z_2 na základ $z_1 = z_2^n$ zapíšeme dané číslo ve zkráceném tvaru v soustavě z_2, rozdělíme zprava na n-ciferné skupiny, přičemž každá taková skupina n cifer dá podle věty 9. 11. jednu cifru v soustavě z_1. Příklad 9.12. lze pak psát takto: $110110010110_2 = 110/110/010/110_2 = 6526_8$. Při opačném převodu postupujeme analogicky. Musíme si však uvědomit, že vždy vytváříme z každé cifry v soustavě z_1 skupinu n cifer v soustavě z_2, tedy např. $301_4 = 110001_2$, $301_8 = 011000001_2$, tzn. např. číslo nula je zapsáno v prvním případě dvěma nulami, zatímco ve druhém případě třemi nulami.

Poznámka 9. 14. Nyní se budeme zabývat převody zápisů reálných čísel. Bez újmy na obecnosti se můžeme omezit na kladná reálná čísla. Připomeneme potřebné označení.

Nechť α je kladné reálné číslo. Pak největší celé číslo, nepřevyšující číslo α , označíme $[\alpha]$ a budeme nazývat celá část čísla α . Číslo $\alpha - [\alpha]$ se označuje $\langle \alpha \rangle$ a nazývá se necelá část reálného čísla α. Platí tedy: $\alpha = [\alpha] + \langle \alpha \rangle$, $[\alpha] \leq \alpha < [\alpha] + 1$, $0 \leq \langle \alpha \rangle < 1$, $[\alpha] \in \boldsymbol{Z}$. V případě $\alpha > 0$ je dokonce $[\alpha] \in \boldsymbol{N}$.
Převod zápisu kladného reálného čísla α provádíme následujícím způsobem. Platí $\alpha = [\alpha] + \langle \alpha \rangle$. Protože $[\alpha] \in \boldsymbol{N}$, lze zápis čísla $[\alpha]$ převést do soustavy o základu z metodami popsanými výše pro převod zápisů přirozených čísel. Zbývá převést do soustavy o základu z i necelou část čísla α , tedy $\langle \alpha \rangle$,. Platí $0 \leq \langle \alpha \rangle < 1$, přičemž případ $\langle \alpha \rangle = 0$ je triviální a budeme ho z úvah vylučovat (číslo α by bylo v tomto případě přirozené). Uvažujeme tedy pouze případ $0 < \langle \alpha \rangle < 1$. Převody zápisů takových čísel se nyní budeme zabývat. Protože nemůže dojít k nedorozumění, můžeme místo $\langle \alpha \rangle$ psát pouze α.

Věta 9. 15. Nechť α je kladné reálné číslo s vlastností $0 < \alpha < 1$, nechť z je přirozené číslo větší než jedna. Položme $a_0 = 0$, $\alpha_0 = \alpha$. Pro $n = 1, 2, \ldots$ nyní položíme

$a_n = [z \,.\, \alpha_{n-1}]$, $\alpha_n = \langle z \,.\, \alpha_{n-1} \rangle$. Pak číslo α lze vyjádřit ve tvaru $\alpha = a_0 \,,\, a_1 a_2 a_3 ....$, přičemž toto vyjádření je jednoznačné.

Poznámka 9. 16. Jak jsme již uvedli v kapitole o tělese racionálních a reálných čísel, rozvoj čísla α je buďto ukončený nebo periodický pro α racionální, zatímco pro α iracionální je rozvoj nekonečný a neperiodický. Typ rozvoje však nemusí být tentýž jako v desítkové soustavě, což ukážeme na příkladech.

Příklad 9. 17.

a) $\alpha = 0{,}5,\ z = 3$. Položíme $a_0 = 0,\ \alpha_0 = 0{,}5$. Vypočteme $3 \,.\, 0{,}5 = 1{,}5$ a dostáváme $a_1 = 1,\ \alpha_1 = 0{,}5$. Opět vypočteme $3 \,.\, 0{,}5 = 1{,}5$ a obdržíme stejné hodnoty $a_2 = 1,\ \alpha_2 = 0{,}5$. Takto lze pokračovat do nekonečna, tedy platí $0{,}5 = 0{,}1111...._3$. Číslo 0,5 je tedy ve trojkové soustavě číslem periodickým. Správnost výpočtu snadno ověříme: $0{,}1111...._3 = 1 \,.\, 3^{-1} + 1 \,.\, 3^{-2} + 1 \,.\, 3^{-3} + ... = \dfrac{\frac{1}{3}}{1 - \frac{1}{3}} = 0{,}5$ (jedná se o konvergentní geometrickou řadu).

b) $a = 7{,}65,\ z = 4$. Podle úmluvy $\alpha = 0{,}65$. Položíme $a_0 = 0,\ \alpha_0 = 0{,}65$. Vypočteme $4 \,.\, 0{,}65 = 2{,}6$ a dostáváme $a_1 = 2,\ \alpha_1 = 0{,}6$. Opět vypočteme $4 \,.\, 0{,}6 = 2{,}4$ a obdržíme hodnoty $a_2 = 2,\ \alpha_2 = 0{,}4$. Dále již bez komentáře: $4 \,.\, 0{,}4 = 1{,}6\,,\ a_3 = 1,\ \alpha_3 = 0{,}6$; $4 \,.\, 0{,}6 = 2{,}4\,,\ a_2 = 2,\ \alpha_2 = 0{,}4$; $4 \,.\, 0{,}4 = 1{,}6\,,\ a_3 = 1,\ \alpha_3 = 0{,}6$ atd. Platí tedy $0{,}65 = 0{,}2\overline{21}_4$. Protože podle zadání jsme měli převést zápis čísla $a = 7{,}65$, stačí doplnit převod celé části tohoto čísla, tzn. čísla 7. Snadno zjistíme, že $7 = 13_4$, dohromady tedy máme $7{,}65 = 13{,}2\overline{21}_4$.

10. Základní pojmy a tvrzení z teorie dělitelnosti

Obecná teorie dělitelnosti v okruhu

Poznámka 10. 1. Všude v dalším budeme předpokládat, že okruh R má jedničku, kterou označíme 1_R (existence nulového prvku 0_R je samozřejmá). Dále poznamenejme, že tato část o obecné teorii dělitelnosti v okruhu, včetně důkazů tvrzení, je převzata z publikace [5].

Definice 10. 2. Nechť R je okruh, nechť $a, b \in R$. Jestliže existuje prvek $r \in R$ takový, že $a = b \,.\, r$, pak říkáme, že b dělí a (prvek a je dělitelný prvkem b) a píšeme $b \mid a$. V opačném případě říkáme, že prvek a není dělitelný prvkem b a píšeme $b \nmid a$. Relace $\mid$ se nazývá relace dělitelnosti na okruhu R .

Poznámka 10. 3. Slovních formulací předchozí definice existuje celá řada. Lze např. říci, že prvek a je násobkem prvku b , prvek b je dělitelem prvku a atd. Prvek 0_R je dělitelný všemi prvky okruhu R (ve vztahu $0_R = b \,.\, r$ stačí položit $r = 0_R$), naproti tomu prvkem 0_R je dělitelný právě jen prvek 0_R (vztah $a = 0_R \,.\, r$ je splněn jedině v případě $a = 0_R$). Velmi často se v teorii dělitelnosti prvek 0_R z úvah vylučuje a omezujeme se pouze na nenulové prvky okruhu.

Věta 10. 4. Nechť R je okruh, pak platí:
1. Relace dělitelnosti na R je reflexivní a tranzitivní.
2. Nechť $a_1, a_2, ..., a_k$, b jsou takové prvky okruhu R , pro které platí $b \mid a_i$ pro $i = 1, 2, ..., k$. Nechť $t_1, t_2, ..., t_k$ jsou libovolné prvky z R. Pak $b \mid \sum_{i=1}^{k} a_i t_i$.

Definice 10. 5. Nechť $e \in R$ je prvek s vlastností $e \mid 1_R$. Pak prvek e se nazývá jednotka okruhu R .

Poznámka 10. 6. Jednotka okruhu R je zřejmě takový prvek, k němuž existuje inverzní prvek vzhledem k operaci násobení. Lze dokázat, že množina $J(R)$ všech jednotek okruhu R tvoří vzhledem k operaci násobení grupu.

Definice 10. 7. Nechť R je okruh. Jestliže pro prvky $a, b \in R$ existuje jednotka $e \in J(R)$ s vlastností $a = b \,.\, e$, pak říkáme, že prvek a je asociován s prvkem b.

Věta 10. 8. Relace asociovanosti z definice 10. 7. je relace ekvivalence na množině R .

Poznámka 10. 9. Vzhledem k předchozí větě platí, že je-li prvek a je asociován s prvkem b, pak je také prvek b asociován s prvkem a. Můžeme tedy říkat, že prvky a, b jsou v R asociovány a píšeme $a \sim b$.

Poznámka 10. 10. Relace asociovanosti je ekvivalence na množině R . Existuje tedy rozklad množiny R , který je touto ekvivalencí určen. Třídy tohoto rozkladu jsou tvořeny navzájem asociovanými prvky. Jednou třídou je vždy množina $\{0_R\}$, další třídou je vždy množina $J(R)$, protože všechny jednotky jsou asociovány s jedničkou 1_R. Dále již obecně nelze říci nic, snad s výjimkou případu, kdy R je těleso. V tělese je každý nenulový prvek jednotkou, a proto rozklad $R/\sim$ má právě dvě třídy $\{0_R\}$ a $J(R) = R - \{0_R\}$. Z hlediska dělitelnosti je proto těleso

nezajímavé (také proto se v matematice nezkoumá dělitelnost v oboru racionálních nebo reálných čísel).

Poznámka 10. 11. Nyní se zaměříme na případ, kdy R bude oborem integrity. Všude v dalším budeme tedy v R kromě existence jedničky předpokládat neexistenci vlastních dělitelů nuly.

Věta 10. 12. Nechť R je obor integrity. pak platí:

$$a \sim b \;\Leftrightarrow\; a \mid b \;\wedge\; b \mid a\,.$$

Věta 10. 13. Nechť R je obor integrity, nechť $a, b, a_0, b_0 \in R$. Pak platí:
1. Pro každou jednotku $e \in J(R)$ a každý prvek $r \in R$ platí $e \mid r$.
2. Jestliže platí $a_0 \sim a$, $b_0 \sim b$, pak $a \mid b \;\Leftrightarrow\; a_0 \mid b_0$.

Důsledek 10. 14. Každý prvek oboru integrity R je dělitelný všemi jednotkami z R a všemi s ním asociovanými prvky v R.

Definice 10. 15. Nechť R je obor integrity, nechť $r \in R$. Pak všechny jednotky z R a všechny prvky asociované s prvkem r se nazývají nevlastní dělitelé prvku r (někdy též triviální dělitelé). Ostatní dělitelé prvku r (pokud existují), se nazývají vlastní dělitelé.

Definice 10. 16. Nechť $r \in R$ je nenulový prvek, který není jednotkou v R. Pak prvek r se nazývá reducibilní (rozložitelný) v R, jestliže má v R vlastní dělitele. v opačném případě se tento prvek nazývá ireducibilní (nerozložitelný).

Poznámka 10. 17. Prvek $r \in R$ se tedy nazývá reducibilní, jestliže jej lze vyjádřit jako součin dvou takových prvků oboru integrity R, z nichž žádný není v R jednotkou ani není s prvkem r asociován. Pokud takové vyjádření neexistuje, je prvek r ireducibilní. Odtud dále plyne, že v tělese, kde každý nenulový prvek je jednotkou a všechny nenulové prvky jsou navzájem asociovány, nemá otázka reducibility a ireducibility opodstatnění (všechny nenulové prvky tělesa jsou ireducibilní).

Věta 10. 18. Nechť R je obor integrity, nechť $r, s \in R$, nechť platí $r \sim s$. Potom platí:

$$r \text{ je ireducibilní v } R \;\Leftrightarrow\; s \text{ je ireducibilní v } R\,.$$

Definice 10. 19. Nechť R je obor integrity, nechť M je neprázdná podmnožina R. Pak prvek $t \in R$ se nazývá společný dělitel množiny M v R, jestliže pro každý prvek $m \in M$ platí $t \mid m$. Píšeme $t \mid M$.

Definice 10. 20. Nechť R je obor integrity, nechť M je neprázdná podmnožina R. Pak prvek $d \in R$ se nazývá největší společný dělitel množiny M v R, jestliže platí:
1. $d \mid M$
2. Pro každé $t \in R$ platí: $t \mid M \;\Rightarrow\; t \mid d$.

Poznámka 10. 21. Je-li M konečná množina, např. $M = \{a_1, \ldots, a_k\}$, pak hovoříme o společném děliteli (největším společném děliteli) prvků $a_1, \ldots, a_k$. Poznamenejme ještě, že obecně v oboru integrity z definice 10. 20. neplyne existence největšího společného dělitele množiny M. O jeho jednoznačnosti však obecné tvrzení vyslovit lze.

Věta 10. 22. Nechť R je obor integrity a nechť existuje největší společný dělitel d množiny M v R. Pak $D = \{ r \in R ; r \sim d \}$ je množina všech největších společných dělitelů množiny M v R.

Dělitelnost v oboru celých čísel

I. Úvod, základní pojmy

Poznámka 10. 23. Z algebry víme, že množina všech celých čísel s operacemi sčítání a násobení tvoří obor integrity. Proto lze dělitelnost v množině všech celých čísel chápat jako speciální případ výše popsané obecné teorie dělitelnosti v oboru integrity. Jednotky oboru integrity $\boldsymbol{Z}$ jsou čísla $1, -1,$ s každým celým číslem z je asociováno pouze opačné celé číslo $-z$. Protože víme, že každé celé číslo je dělitelné všemi jednotkami v $\boldsymbol{Z}$ a všemi celými čísly s ním asociovanými, plyne odtud, že každé celé číslo z má čtyři triviální dělitele: $1, -1, z, -z$. Ireducibilními prvky v oboru integrity $\boldsymbol{Z}$ jsou právě všechna prvočísla, reducibilními prvky jsou čísla složená. Do oboru integrity $\boldsymbol{Z}$ lze přímo přenést i definici největšího společného dělitele. Protože však teorie dělitelnosti v množině celých čísel patří mezi základní učivo při výuce matematiky na všech stupních škol, uvedeme dále tuto teorii přímo, bez odkazu na obecnou teorii dělitelnosti v okruhu. Budeme postupovat velmi stručně, zájemce lze odkázat na publikaci [2] a elektronický učební kurz [17].

Definice 10. 24. Říkáme, že celé číslo b dělí celé číslo a (nebo b je dělitelem a nebo a je dělitelné b nebo a je násobkem b), právě když existuje celé číslo x, pro které platí $a = b \,.\, x$. Zapisujeme $b \mid a$. Jestliže k číslům $a, b \in \boldsymbol{Z}$ neexistuje $x \in \boldsymbol{Z}$ takové, že $a = b \,.\, x$, říkáme, že b nedělí a a zapisujeme $b \nmid a$.

Definice 10. 25. Platí-li $a = b \,.\, x,$ pak čísla b a x jsou dělitelé čísla a a nazývají se sdružení dělitelé čísla a. Dělitelé čísla a patřící do množiny přirozených čísel se nazývají přirození dělitelé čísla a.

Poznámka 10. 26.

1. Každé celé číslo $a \neq 0, 1, -1$ má alespoň 4 celočíselné dělitele, a to čísla $1, a, -1, -a$. Tyto dělitele nazýváme samozřejmými (triviálními) děliteli čísla a. (Ostatní dělitele čísla a, pokud existují, nazýváme nesamozřejmými nebo netriviálními děliteli čísla a.)
2. Čísla 1 a -1 mají právě dva dělitele v množině $\boldsymbol{Z}$, a to $1, -1$.
3. Číslo 0 má nekonečně mnoho dělitelů, a to každé celé číslo.
4. Číslo 0 není dělitelem žádného nenulového čísla a, protože neexistuje žádné celé číslo x tak, aby platilo $0 \,.\, x = a$.
5. Číslo 0 je dělitelem sebe sama ($0|0$), neboť pro libovolné celé číslo x platí $0 \,.\, x = 0$. Poznamenejme ještě, že tento poslední případ se v praxi nezavádí ani nevyužívá. Proto ve školské matematice říkáme, že podíl $\frac{0}{0}$ není definován (pouze v matematické analýze se předchozí zlomek řeší jako tzv. neurčitý výraz při počítání limit).

Věta 10. 27. Pro libovolná celá čísla a, b, c platí:

a) $(b \mid a \wedge b \mid c) \Rightarrow (b \mid (a + c) \wedge b \mid (a - c)$,

b) $b \mid a \Rightarrow (-b) \mid a$,

c) $b \mid a \Rightarrow b \mid (-a)$.

Poznámka 10. 28. Na základě části b) a c) věty 10.27. můžeme dále teorii dělitelnosti budovat jen v množině přirozených čísel. (Určíme-li přirozené dělitele přirozeného čísla a, umíme snadno určit všechny dělitele čísla a i čísla $-a$).

Definice 10. 29. Celé číslo, které je dělitelné dvěma se nazývá sudé číslo. Celé číslo, které není dělitelné dvěma (tj. při dělení dvěma dává zbytek *1*) se nazývá liché číslo.

II. Znaky dělitelnosti

Znaky dělitelnosti jsou věty, které umožňují rozhodnout o dělitelnosti čísla jiným číslem bez provedení dělení, jen ze zápisu daného čísla. Ve všech dalších úvahách máme na mysli přirozená čísla zapsaná v desítkové soustavě.

Věta 10. 30.

1. Přirozené číslo a je dělitelné dvěma (pěti, deseti) právě tehdy, když je dvěma (pěti, deseti) dělitelné číslo, zapsané jeho cifrou nultého řádu.
2. Přirozené číslo a je dělitelné čtyřmi, právě když je čtyřmi dělitelné číslo zapsané jeho posledním dvojčíslím.
3. Přirozené číslo a je dělitelné osmi, právě když je osmi dělitelné číslo zapsané jeho posledním trojčíslím.
4. Přirozené číslo a je dělitelné třemi (devíti), právě když je třemi (devíti) dělitelný jeho ciferný součet. (Ciferný součet je součet všech čísel zapsaných jednotlivými číslicemi v zápisu čísla a)
5. Přirozené číslo a je dělitelné jedenácti, právě když je jedenácti dělitelný součet čísel zapsaných jednotlivými ciframi sudého řádu zmenšený o součet čísel zapsaných jednotlivými ciframi lichého řádu v zápisu čísla a.

Uvedené znaky dělitelnosti plynou z obecnější věty:

Věta 10. 31.

I. Dělíme-li přirozené číslo a dvěma (pěti, deseti) dostaneme stejný zbytek, jako když dělíme dvěma (pěti, deseti) číslo zapsané cifrou nultého řádu v zápisu čísla a.
II. Dělíme-li přirozené číslo a (aspoň trojciferné) čtyřmi, dostaneme stejný zbytek, jako když dělíme čtyřmi číslo zapsané jeho posledním dvojčíslím.
III. Dělíme-li přirozené číslo a (aspoň čtyřciferné) osmi, dostaneme stejný zbytek, jako když dělíme osmi číslo zapsané jeho posledním trojčíslím.
IV. Dělíme-li přirozené číslo a třemi (devíti), dostaneme stejný zbytek, jako když dělíme třemi (devíti) jeho ciferný součet.
V. Dělíme-li přirozené číslo a jedenácti, dostaneme stejný zbytek, jako když dělíme jedenácti součet čísel zapsaných ciframi sudého řádu zmenšený o součet čísel zapsaných ciframi lichých řádů.

Věta 10. 32. Je-li celé číslo a součtem dvou celých čísel, z nichž jedno je násobkem celého čísla b, pak druhý sčítanec dává při dělení číslem b stejný zbytek jako číslo a.

III. Největší společný dělitel

Definice 10. 33. Společný dělitel přirozených čísel *a, b* je každé přirozené číslo *d*, pro které platí $d \mid a$ a $d \mid b$. Největší společný dělitel přirozených čísel *a, b* je ten ze společných dělitelů, který je dělitelný všemi společnými děliteli. Označujeme *NSD(a, b).*

Poznámka 10. 34. V množině přirozených čísel lze též říci, že největší společný dělitel je největší (maximální) číslo z množiny všech společných dělitelů.

Poznámka 10. 35. Největší společný dělitel dvou čísel můžeme určit různými způsoby:

a) využitím definice,
b) pomocí tzv. Euklidova algoritmu (na základě následující věty 10. 36.),
c) pomocí rozkladu daných čísel na součin prvočinitelů.

Věta 10. 36. Jestliže přirozené číslo *a* dává při dělení nenulovým přirozeným číslem *b* nenulový zbytek *z*, tzn. $a = b \,.\, q + z$ a platí nerovnost $z < b$, pak platí, že množina všech společných dělitelů čísel *a, b* je množinou všech společných dělitelů čísel *b, z*. Také největší společný dělitel čísel *a, b* je roven největšímu společnému děliteli čísel *b, z*, tj. *NSD(a, b) = NSD(b, z).* Tím převádíme problém určení *NSD(a, b)* na určení *NSD(b, z).* Čísla *b* a z jsou menší než čísla *a, b*.

Na větě 10. 36. je založen postup výpočtu největšího společného dělitele dvou přirozených čísel nazývaný Euklidův algoritmus. Použití Euklidova algoritmu ukážeme na příkladě:

Příklad 10. 37. Určete *NSD(600, 252)* pomocí Euklidova algoritmu.

Řešení:

600 : 252 = 2 *96*	neboli	*600 = 252 . 2 + 96*
252 : 96 = 2 *60*		*252 = 96 . 2 + 60*
96 : 60 = 1 *36*		*96 = 60. 1 + 36*
60 : 36 = 1 *24*		*60 = 36 . 1 + 24*
36 : 24 = 1 *12*		*36 = 24 . 1 + 12*
24 : 12 = 2 *0*		*24 = 12 . 2*

Největší společný dělitel čísel *600* a *252* je číslo *12*, tj. poslední nenulový zbytek při postupném dělení.

Definice 10.38. Přirozená čísla *a, b* se nazývají nesoudělná, právě když je jejich největší společný dělitel roven *1*, tedy *NSD(a, b) = 1*. Přirozená čísla *a, b* se nazývají soudělná, právě když je jejich největší společný dělitel větší než *1*, tedy *NSD(a, b) > 1*.

Poznámka 10. 39. Definice 10. 33. a 10. 38. lze rozšířit na libovolný konečný počet přirozených čísel. V případě, že počet těchto čísel je větší než dvě, je ale nutno pojem nesoudělnosti upřesnit.

Definice 10. 40. Nechť $a_1, a_2, a_3, ..., a_n, n > 2,$ jsou nesoudělná přirozená čísla (s vlastností $NSD(a_1, a_2, a_3, ..., a_n) = 1$). Jestliže pro libovolnou dvojici indexů $i, j \in \{1, 2, ..., n\}$ platí $NSD(a_i, a_j) = 1,$ pak říkáme, že čísla $a_1, a_2, a_3, ..., a_n$ jsou po dvou nesoudělná. Jestliže naopak existuje dvojice indexů $i, j \in \{1, 2, ..., n\}$ s vlastností $NSD(a_i, a_j) > 1,$ pak říkáme, že čísla $a_1, a_2, a_3, ..., a_n$ nejsou po dvou nesoudělná (jsou pouze nesoudělná podle předpokladu).

Příklad 10. 41. Čísla *7, 19, 31* jsou po dvou nesoudělná, zatímco čísla *6, 10, 15* jsou „pouze“ nesoudělná.

IV. Nejmenší společný násobek

Definice 10. 42. Společný násobek přirozených čísel *a, b* je každé přirozené číslo *m*, které je dělitelné oběma čísly *a, b*, tj. $a \mid m$ a $b \mid m$. Nejmenší kladný společný násobek přirozených čísel *a, b* je ten ze společných násobků, který je dělitelem všech společných násobků čísel *a, b*. Zapisujeme *NSN(a, b)*.

Poznámka 10. 43. V množině přirozených čísel lze též říci, že *NSN(a, b)* je nejmenší číslo z kladných společných násobků čísel *a,b*. Definici 10. 42. lze rozšířit na libovolný konečný počet přirozených čísel $a_1, ..., a_n$.

Poznámka 10. 44. Nejmenší společný násobek čísel *a, b* můžeme určit různými způsoby:

a) využitím definice,
b) pomocí vztahu mezi *NSN(a, b)* a *NSD(a, b)*
c) pomocí rozkladu daných čísel na součin prvočinitelů

Věta 10. 45. Pro každá dvě přirozená čísla *a, b* platí $a \cdot b = NSN(a, b) \cdot NSD(a, b)$.

Poznámka 10. 46. Větu 10. 45. nelze rozšířit na více než dvě přirozená čísla.

V. Obecná kritéria dělitelnosti:

Věta 10.47: Je-li přirozené číslo dělitelné po dvou nesoudělnými čísly, je dělitelné i jejich součinem. Tuto větu lze také obrátit.

Příklad 10. 48. Platí $12 = 3 \cdot 4, 18 = 2 \cdot 9, 165 = 3 \cdot 5 \cdot 11$. Proto lze dělitelnost číslem dvanáct odvodit ze současné dělitelnosti čísly *3* a *4*, dělitelnost číslem *18* pomocí dělitelnosti čísly *2* a *9* a dělitelnost číslem *165* pomocí dělitelnosti čísly *3*, *5* a *11*.

Věta 10. 49. (Obecné kritérium dělitelnosti přirozeného čísla $a = a_0 + 10a_1 + 10^2a_2 + 10^3a_3 + ... + 10^m a_m$ přirozeným číslem *n*):

Pro dané přirozené číslo a vypočteme jeho ciferný součet c s vahami jednotlivých cifer takto: Pro každé $k = 0, ..., m$ označíme β_k zbytek po dělení čísla 10^k číslem n (platí tedy $\beta_k \equiv 10^k (mod\ n)$). Potom $c = a_0\ \beta_0 + a_1\ \beta_1 + a_2\ \beta_2 + ... + a_m\ \beta_m$. Podle pravidel pro počítání s kongruencemi (bude uvedeno dále) dává číslo c při dělení číslem n stejný zbytek, jako číslo a. Odtud plyne tvrzení: Číslo a je dělitelné číslem n, právě když číslo c je dělitelné číslem n .

Poznámka 10. 50. Poznamenejme, že posloupnost čísel β_k je vždy konečná a počet jejích prvků nemůže být větší než číslo $n–1$ (počet možných nenulových zbytků při dělení číslem n). V opačném případě, pokud by některá mocnina deseti byla dělitelná číslem n, nepoužili bychom toto obecné kritérium. Kritérium dělitelnosti číslem n by potom bylo analogické kritériu dělitelnosti číslem *4, 8, 25*,...).

Příklad 10. 51.
a) Dělitelnost čísla *5894* sedmi. Platí: $1 \equiv 1(mod\ 7),\ 10 \equiv 3(mod\ 7n),\ 100 \equiv 2^k(mod\ 7),\ 1000 \equiv 6(mod\ 7),\ 10^4 \equiv 4(mod\ 7),\ 10^4 \equiv 5(mod\ 7),\ 10^6 \equiv 1(mod\ 7),\ 10^7 \equiv 3(mod\ 7),\ 10^8 \equiv 2(mod\ 7)$ atd. Induktivním postupem jsme zjistili, že posloupnost zbytků *1, 3, 2, 6, 4, 5* se neustále opakuje. Proto $\beta_0 = 1,\ \beta_1 = 3,\ \beta_2 = 2,\ \beta_3 = 6,\ \beta_4 = 4,\ \beta_5 = 5,\ \beta_6 = 1,\ \beta_7 = 3,\ \beta_8 = 2$ atd. Nyní vypočteme $c = 4\ .\ 1 + 9\ .\ 3 + 8\ .\ 2 + 5\ .\ 6 = 77,$ což je číslo dělitelné sedmi. Proto i číslo *5894* je dělitelné sedmi. Poznamenejme, že s ohledem na vlastnosti kongruencí lze v posloupnosti čísel β_k nehradit kterékoliv z nich číslem kongruentním s n, tedy posloupnost *1, 3, 2, 6, 4, 5* lze nahradit posloupností *1, 3, 2, –1, –3, –2,* která je lépe zapamatovatelná a při výpočtech vhodnější (vypočtená čísla c jsou menší než pro původní hodnoty). Např. pro číslo *5894* by bylo $c = 4\ .\ 1 + 9\ .\ 3 + 8\ .\ 2 + 5\ .\ (–1) = 42.$

b) Dělitelnost čísla a *=548 893 672 185 729 643* číslem *17.* Vypočteme posloupnost zbytků β_k (podrobnosti si již odpustíme): *1, –7, –2, –3, 4, 6, –8, 5, –1, 7, 2, 3, –4, –6, 8, –5.* Nyní určíme ciferný součet c čísla a s vahami cifer: $c = 3.1 - 4.7 - 6.2 - 9.3 + 2.4 + 7.6 - 5.8 + 8.5 - 1.1 + 2.7 + 7.2 + 6.3 - 3.4 - 9.6 + 8.8 - 8.5 + 4.1 - 5.7 = –42.$ Číslo c dává po dělení číslem *17* zbytek *9,* tj. také zadané číslo a dává při dělení sedmnácti zbytek *9*, není tedy číslem *17* dělitelné.

VI. Prvočísla, čísla složená

Definice 10. 52. Přirozené číslo $p > 1$ nazýváme prvočíslem, právě když má právě dva různé přirozené dělitele (tj. čísla *1* a p). Přirozené číslo $a > 1$, které není prvočíslem (tj. má více než dva přirozené dělitele), nazýváme složeným číslem.

Poznámka 10. 53. Číslo *1* podle definice není prvočíslo ani číslo složené.

Věta 10. 53. Každé složené přirozené číslo $n > 1$ má alespoň jednoho prvočíselného dělitele, menšího než $\sqrt{n}$.

Důsledek 10. 54. Jestliže přirozené číslo n není dělitelné žádným prvočíslem menším nebo rovným $\sqrt{n}$, pak n je prvočíslo.

Věta 10. 55.. Každé složené číslo a lze vyjádřit právě jedním způsobem ve tvaru součinu konečného počtu prvočísel

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$$

kde $p_1, p_2, \ldots, p_k$ jsou prvočísla, $e_1, e_2, \ldots, e_k$ jsou nenulová přirozená čísla.
Tento zápis se nazývá prvočíselný (někdy též kanonický) rozklad přirozeného čísla a a $p_1, p_2, \ldots, p_k$ jsou tzv. prvočinitelé rozkladu.

Poznámka 10. 56. Prvočíselný rozklad přirozeného čísla využíváme především
a) k výpočtu největšího společného dělitele a nejmenšího kladného společného násobku daných čísel *a, b*
b) k určení počtu všech přirozených dělitelů daného přirozeného čísla *a*
c) k určení všech přirozených dělitelů daného přirozeného čísla *a.*

ad a) Největší společný dělitel daných přirozených čísel je součinem všech prvočinitelů, kteří se současně vyskytují v prvočíselných rozkladech všech daných čísel, a to s nejmenším s vyskytujících se exponentů. Nejmenší společný násobek daných čísel je součinem všech různých prvočinitelů, kteří se vyskytují v rozkladech daných čísel, a to v největší mocnině.

Příklad 10. 57. Určete *NSD(108, 90)* a *NSN(108, 90).*

Řešení: $108 = 2^2 . 3^3 \qquad 90 = 2 . 3^2 . 5$
$NSD(108, 90) = 2 . 3^2 = 18$
$NSN(108, 90) = 2^2 . 3^3 . 5 = 540$

ad b) Určení počtu všech přirozených dělitelů daného přirozeného čísla:

Věta 10. 58. Je-li $a = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$ prvočíselný rozklad přirozeného čísla $a > 1$, pak počet všech přirozených dělitelů čísla a (ozn. $\tau(a)$) je určen takto:

$$\tau(a) = (e_1 + 1).(e_2 + 1). \ \ldots \ .(e_k + 1)$$

ad c) Všechny přirozené dělitele čísla *a* určíme jako všechny možné součiny všech prvočinitelů čísla *a*, přičemž každý prvočinitel je umocněn postupně na všechny mocniny od *0* až po tu, ve které se vyskytují v kanonickém rozkladu čísla *a* .

Příklad 10. 59. Zjistěte počet všech přirozených dělitelů čísla *648* a napište všechny přirozené dělitele čísla *648*. Dále určete všechny dvojice sdružených dělitelů čísla *648*.

Řešení: $648 = 2^3 . 3^4$, $\tau(648) = (3+1) . (4+1) = 20$,
tzn. číslo *648* má *20* přirozených dělitelů.

	3^0	3^1	3^2	3^3	3^4
2^0	1	3	9	27	81
2^1	2	6	18	54	162
2^2	4	12	36	108	324
2^3	8	24	72	216	648

Sdružené dvojice dělitelů: *1 . 648, 2 . 324, 3 . 216, 4 . 162, 6 . 108, 8 . 81, 9 . 72, 12 . 54, 18 . 36, 24 . 27.*

VII. Neurčité rovnice (někdy též diofantické nebo diofantovské)

Neurčité rovnice jsou rovnice se dvěma nebo více neznámými, které se řeší v oboru všech celých čísel.

Definice 10. 60.

Lineární neurčitá rovnice o dvou neznámých x, y je rovnice

$$a \,.\, x + b \,.\, y = c,\ a \neq 0, b \neq 0\ ,\ a, b, c \in \boldsymbol{Q}.$$

Poznámka 10. 61. Je-li alespoň jeden z koeficientů *a, b, c* racionální necelé číslo, vynásobíme rovnici vhodným číslem tak, aby všechny tři koeficienty nabyly celočíselných hodnot.

Věta 10. 62. (Řešitelnost lineární neurčité rovnice.)
Neurčitá rovnice $a \,.\, x + b \,.\, y = c$ má řešení v případě, že největší společný dělitel koeficientů *a, b* je také dělitelem čísla *c* . Pak řešením je nekonečně mnoho dvojic celých čísel *x , y.*
V případě, že největší společný dělitel čísel *a, b* není dělitelem koeficientu *c*, pak rovnice nemá řešení.

Postup řešení neurčité rovnice:
I. Nechť $x_0\ ,\ y_0$ je jedno pevné řešení neurčité rovnice. Potom obecné řešení je dáno vztahy

$$x = x_0 + \frac{b \cdot t}{NSD(a,b)}, \quad y = y_0 - \frac{a \cdot t}{NSD(a,b)}, \quad t \in \boldsymbol{Z}\ .$$

Výchozí dvojice $x_0\ ,\ y_0$ se určí buďto úsudkem nebo se vypočte z podílů Eukleidova algoritmu při hledání *NSD(a, b).*

II. Redukční metoda.

VIII. Kongruence, rozklad na zbytkové třídy.

Poznámka 10. 63. Problematika kongruencí a zbytkových tříd je důležitou součástí moderní algebry. Lze ji rozdělit na dvě součásti, které jsou obě založené na relaci kongruence v oboru všech celých čísel. V první části se budeme nejprve věnovat samotné relaci kongruence a jejím důležitým vlastnostem (podobným vlastnostem rovnic). Jejich význam a užití poznáte ve cvičeních. V následující části se pak stručně dotkneme i rozkladu na zbytkové třídy a vlastnostem algebraických struktur definovaných na systémech zbytkových tříd. I když jste se těmto strukturám již věnovali dříve, do kapitoly o dělitelnosti organicky patří také.

Věta 10. 64. Nechť *a, b* jsou celá čísla taková, že $b \neq 0$. Potom existují celá čísla *q, r* splňující vztah:

$$a = bq + r,\ 0 \leq r < |b|,$$ přičemž toto vyjádření je jednoznačné.

Poznámka: Je nutno si uvědomit, že zbytek *r* při dělení je vždy nezáporný, a to i při dělení záporným číslem. Např. $a = -26,\ b = 8,\ q = -4,\ r = 6$, protože $-26 = 8 \,.\, (-4) + 6$.

Definice 10. 65. Eulerova funkce $\varphi(n)$ vyjadřuje počet přirozených čísel menších nebo rovných číslu *n*, nesoudělných s *n*. Nechť $n = p_1^{\alpha_1} \,.\, \ldots\, p_k^{\alpha_k}$, pak platí $\varphi(n) = n \,.\, \prod_{i=1}^{k} (1 - \frac{1}{p_i})$. Je-li *n* prvočíslo, pak $\varphi(n) = n - 1$.

Definice 10. 66. (**Kongruence)** Nechť $a, b \in \boldsymbol{Z}$, $m \in \boldsymbol{N}$, $m \geq 2$. Pak říkáme, že číslo a je kongruentní s číslem b podle modulu m a píšeme $a \equiv b \ (mod\ m)$**,** právě když $m \mid (a - b)$. Dvě čísla kongruentní podle nějakého modulu m dávají při dělení tímto modulem m týž zbytek.

Věta 10. 67. Relace kongruence je ekvivalence na množině všech celých čísel (je reflexivní, symetrická a tranzitivní).

Věta 10. 68. *Vlastnosti kongruencí*:

1) Nechť p je prvočíslo, pak $a \equiv b \pmod{p^n} \Rightarrow a \equiv b \pmod{p}$

Platí-li kongruence podle modulu, který je mocninou prvočísla, platí i podle modulu rovného tomuto prvočíslu.

2) $a \equiv b \pmod{m_i}$, $i = 1,2,...,k \Rightarrow a \equiv b \pmod{NSN(m_1,...,m_k)}$

Platí-li kongruence podle několika modulů, platí i podle modulu rovného nejmenšímu společnému násobku těchto modulů.

3) $a_i \equiv b_i \pmod{m}$, $i = 1,...,k \Rightarrow \sum_{i=1}^{k} a_i \equiv \sum_{i=1}^{k} b_i \pmod{m}$, $\prod_{i=1}^{k} a_i \equiv \prod_{i=1}^{k} b_i \pmod{m}$.

Kongruence podle téhož modulu lze sčítat i násobit.

Nechť v dalším platí $a \equiv b \pmod{m}$:

4) $a + x \equiv b + x \pmod{m}$, $a \,.\, y \equiv b \,.\, y \pmod{m}$

K oběma stranám kongruence lze přičíst stejné celé číslo a obě strany kongruence lze vynásobit týmž celým číslem. Obecně ale nelze obě strany kongruence dělit týmž celým číslem, např. $24 \equiv 40 \ (mod\ 8)$, ale po vydělení čtyřmi $6 \not\equiv 10 \ (mod\ 8)$.

5) $m \mid z \Rightarrow a + z \equiv b \pmod{m}$

Celé číslo, které je násobkem modulu, lze přičíst pouze k jedné straně kongruence.

6) $a^n \equiv b^n \pmod{m}$

Obě strany kongruence lze umocnit na libovolný přirozený exponent.

7) $d \mid a \wedge d \mid b \wedge \text{NSD}(d, m) = 1 \Rightarrow \frac{a}{d} \equiv \frac{b}{d} \pmod{m}$

Obě strany kongruence lze vydělit celým číslem nesoudělným s modulem.

8) $ac \equiv bc \pmod{mc}$

Obě strany kongruence i modul lze vynásobit týmž celým kladným číslem.

9) $e \mid a \wedge e \mid b \wedge e \mid c \Rightarrow \frac{a}{e} \equiv \frac{b}{e} \pmod{\frac{m}{e}}$

Obě strany kongruence i modul lze vydělit týmž celým kladným číslem různým od nuly.

10) $a \equiv b \pmod{m} \wedge d \mid m \Rightarrow a \equiv b \pmod{d}$

Platí-li kongruence podle modulu m, platí i podle modulu rovnému libovolnému kladnému děliteli čísla m, většímu než jedna.

Věta 10. 69. (Eulerova věta**)** Nechť $m \in \boldsymbol{N}$, $m > 1$, $a \in \boldsymbol{Z}$, $NSD(a, m) = 1$, pak platí:

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Je-li specielně p prvočíslo, které není dělitelem čísla a, pak platí $a^{p-1} \equiv 1 \ (mod\ p)$ (tzv. malá Fermatova věta).

Definice 10. 70. Nechť m je pevné přirozené číslo větší než jedna. Označme
$C_i = \{ x \in \boldsymbol{Z}$; x dává po dělení číslem m zbytek $i \}$, pro $i = 0, 1, ..., m - 1$.
Pak množina C_i se nazývá zbytková třída podle modulu m. Symbolem $\boldsymbol{Z}_m$ pak označíme množinu všech zbytkových tříd podle modulu m , tj. $\boldsymbol{Z}_m = \{C_0 , C_1 , ..., C_{m-1}\}$.

Poznámka 10. 71. Protože při dělení číslem m jsou možné zbytky $0, 1, ..., m - 1,$ je počet zbytkových tříd podle modulu m roven číslu m. Každá zbytková třída podle modulu m obsahuje nekonečně mnoho celých čísel, která dávají při dělení modulem m týž zbytek (tzn. liší se o nějaký celočíselný násobek modulu m).

Příklad 10. 72. a) $m = 4$
$C_0 = \{... , -8, -4, 0, 4, 8, ... \}$
$C_1 = \{... , -7, -3, 1, 5, 9, ... \}$
$C_2 = \{... , -6, -2, 2, 6, 10, ...\}$
$C_3 = \{... , -5, -1, 3, 7, 11, ...\}$

b) $m = 5$
$C_0 = \{..., -10, -5, 0, 5, 10, ...\}$
$C_1 = \{... , -9, -4, 1, 6, 11, ... \}$
$C_2 = \{... , -8, -3, 2, 7, 12, ...\}$
$C_3 = \{... , -7, -2, 3, 8, 13, ...\}$
$C_4 = \{... , -6, -1, 4, 9, 14, ...\}$

Věta 10. 73. Nechť m je pevné přirozené číslo větší než jedna. Pak množina $\boldsymbol{Z}_m$ všech zbytkových tříd podle modulu m tvoří rozklad množiny $\boldsymbol{Z}$ všech celých čísel.

Poznámka 10. 74. Nyní se budeme zabývat binárními operacemi sčítání a násobení definovanými na množině $\boldsymbol{Z}_m$ pro různé moduly m. Obě operace na systému všech zbytkových tříd budeme chápat následujícím způsobem: Nechť např. $m = 5$. Zápis součtu $C_3 + C_4 = C_2$ znamená, že sečtením libovolného celého čísla dávajícího při dělení pěti zbytek 3 s libovolným celým číslem dávajícím při dělení pěti zbytek 4 dostaneme vždy celé číslo, které při dělené pěti dává zbytek 2. Analogicky zápis spoje násobení $C_2 . C_4 = C_3$ znamená, že vynásobením libovolného celého čísla dávajícího při dělení pěti zbytek 2 s libovolným celým číslem dávajícím při dělení pěti zbytek 4 dostaneme vždy celé číslo, které při dělené pěti dává zbytek 3. Populárně řečeno, výsledek sčítání či násobení zbytkových tříd podle modulu m získáme tak, že sečteme nebo vynásobíme indexy zbytkových tříd ze zadání úlohy, zjistíme zbytek součtu či součinu při dělení číslem m a tento zbytek je indexem zbytkové třídy hledaného součtu nebo součinu. Jinými slovy, rozklad $\boldsymbol{Z}_m$ množiny $\boldsymbol{Z}$ je vytvořující vzhledem k operaci sčítání i operaci násobení.

Poznámka 10. 75. V následujících tvrzeních se budeme zabývat typy algebraických struktur definovaných na množinách zbytkových tříd. Tvrzení opět nebudeme dokazovat, vždy

uvedeme jen ilustraci dané struktury pomocí tabulky. Kvůli zjednodušení zápisů rovněž budeme místo třídy C_i uvádět pouze index i (zřejmě nebude moci dojít k nedorozumění).

Věta 10. 76: Nechť m je pevné přirozené číslo větší než jedna. Pak algebraická struktura $(\boldsymbol{Z}_m\ ,\ +)$ je komutativní grupa s neutrálním prvkem C_0.

Ilustrace $(\boldsymbol{Z}_4\ ,\ +)$:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Věta 10. 77. Nechť m je pevné přirozené číslo větší než jedna. Pak algebraická struktura $(\boldsymbol{Z}_m\ ,\ .\ )$ je komutativní pologrupa s neutrálním prvkem C_1 a agresivním prvkem C_0.

Ilustrace $(\boldsymbol{Z}_4\ ,\ .)$:

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Ilustrace $(\boldsymbol{Z}_5\ ,\ .)$:

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Poznámka 10. 78. Prohlédneme-li si pozorně obě tabulky v ilustraci předchozí věty, vidíme, že při operaci násobení zřejmě podstatně závisí na modulu. Odstraníme-li z obou těchto tabulek první řádek a první sloupec, odpovídající třídě C_0, dostáváme následující tabulky struktur $(\boldsymbol{Z}_4 - \{C_0\}\ ,\ .)$ a $(\boldsymbol{Z}_5 - \{C_0\}\ ,\ .)$:

Ilustrace $(\boldsymbol{Z}_4 - \{C_0\}\ ,\ .)$:

.	1	2	3
1	1	2	3
2	2	0	2
3	3	2	1

Ilustrace ($\boldsymbol{Z}_5 - \{C_0\}$, .):

.	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

Struktura ($\boldsymbol{Z}_4 - \{C_0\}$, .) nyní již není ani grupoid, neboť obsahuje v tabulce prvek *0* , který nepatří do nosné množiny (není v záhlaví tabulky). Oproti tomu, struktura ($\boldsymbol{Z}_5 - \{C_0\}$, .) se ještě „zlepšila, nyní jde již o komutativní grupu. Který případ nastane, závisí na modulu.

Věta 10. 79. Nechť modul *m* je prvočíslo. Pak algebraická struktura ($\boldsymbol{Z}_m - \{C_0\}$, .) je komutativní grupa. Je-li modul *m* číslo složené, pak ($\boldsymbol{Z}_m - \{C_0\}$, .) není ani grupoidem.

Důsledek 10. 80. Nechť modul *m* je prvočíslo. Pak algebraická struktura se dvěma operacemi ($\boldsymbol{Z}_m - \{C_0\}$,+, .) je komutativní těleso.

Poznámka 10. 81. Podle předchozího tvrzení není ($\boldsymbol{Z}_m - \{C_0\}$, .) pro složený modul ani grupoidem. Protože je však potřeba popsat i struktury zbytkových tříd se dvěma operacemi pro složený modul *m*, musíme nějak „ošetřit“ situaci nul vyskytujících se v tabulkách (např. ($\boldsymbol{Z}_4 - \{C_0\}$, .)).

Definice 10. 82. Nechť modul *m* je složené číslo, nechť pro dvě zbytkové třídy C_u , C_v podle modulu *m* platí $C_u \neq C_0$, $C_v \neq C_0$. Jestliže C_u . $C_v = C_0$, pak obě třídy C_u , C_v se nazývají vlastní dělitelé nulového prvku C_0 .

Poznámka 10. 83. Definice vlastních dělitelů nulového prvku (stručně jen dělitelů nuly) je samozřejmě obecnější. Struktury zbytkových tříd však poskytují užitečnou ilustraci tohoto pojmu. Současně ve shodě s obecnou teorií algebraických struktur se dvěma operacemi umožňuje existence dělitelů nuly popsat i struktury ($\boldsymbol{Z}_m$,+, .) pro složený modul *m*.

Věta 10. 84. Nechť modul *m* je složené číslo. Pak algebraická struktura se dvěma operacemi ($\boldsymbol{Z}_m$,+, .) je komutativní okruh, který nikdy není oborem integrity (obsahuje dělitele nuly).

Příklad 10. 85. V okruhu ($\boldsymbol{Z}_4$,+, .) je dělitelem nuly C_2 ; v okruhu ($\boldsymbol{Z}_6$,+, .) jsou dělitelé nuly C_2, C_3 ; v okruhu ($\boldsymbol{Z}_8$,+, .) jsou dělitelé nuly C_2, C_4, C_6 .

11. Polynomy

Poznámka 11. 1. Tato kapitola 11 o polynomech i kapitola následující, věnovaná řešení algebraických rovnic, je převzata (volně zpracována) z publikace [5].

Poznámka 11. 2. Nebude-li výslovně řečeno jinak, budeme se zabývat pouze polynomy s reálnými koeficienty.

Definice 11. 3. Polynomem f jedné proměnné nad tělesem reálných čísel budeme nazývat algebraický výraz tvaru

$$f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 \ . \qquad (1)$$

Reálná čísla a_i pro $i = 0, \ldots, n$ se nazývají koeficienty polynomu f, x označuje proměnnou. Koeficient a_n se nazývá vedoucí koeficient polynomu f, koeficient a_0 se nazývá absolutní člen polynomu f. Stupeň polynomu je vždy určen nejvyšší mocninou u proměnné x; při označení polynomu (1) je stupeň polynomu f roven n , píšeme $st(f) = n$. Je-li $a_n = 1$, říkáme, že polynom f je normovaný. Množinu všech polynomů jedné proměnné x nad tělesem reálných čísel budeme označovat $\boldsymbol{R}[x]$. Polynom f budeme někdy označovat též $f(x)$.

Poznámka 11. 4. Je-li stupeň polynomu roven nule, neobsahuje výraz (1) proměnnou x. To ovšem znamená, že každé reálné číslo lze chápat také jako polynom nad tělesem reálných čísel.

Definice 11. 5. Nechť $f = r$, $r \in \boldsymbol{R}$, $r \neq 0$. Pak říkáme, že polynom f je konstantní polynom a platí $st(f) = 0$. Je-li $f = 0$, pak říkáme, že f je nulový polynom (označujeme **0**) a definitoricky klademe stupeň takového polynomu roven $-\infty$. Nulový polynom není tedy totéž jako polynom stupně nula. Je-li $f = 1$, pak říkáme, že f je jednotkový polynom (označujeme **1**). Polynomy stupně jedna nazýváme též lineární polynomy, polynomy stupně dva nazýváme kvadratické polynomy a polynomy stupně tři kubické polynomy. Pro polynomy vyšších stupňů se zvláštní označení běžně nezavádí.

Poznámka 11. 6. Přesná formální matematická definice polynomu je složitější. Polynom nad okruhem R je obecně definován jako jistá nekonečná posloupnost prvků z R. Tímto se zde nebudeme zabývat, zájemce může podrobné informace nalézt v publikaci [5], s. 15 – 18.

Poznámka 11. 7. Pro operace sčítání a násobení polynomů platí pravidla, běžně známá už ze základní školy. Jejich znalost nadále předpokládáme.

Věta 11. 8. Algebraická struktura $(\boldsymbol{R}[x], +, .)$ je obor integrity, který není tělesem. Nulovým prvkem je nulový polynom **0** , jedničkou je jednotkový polynom **1**. Tento okruh budeme krátce značit jen $\boldsymbol{R}[x]$.

Důkaz: Operace sčítání polynomů je zřejmě komutativní a asociativní, neutrálním prvkem je **0.** Ke každému polynomu f existuje opačný polynom $-f$, tedy $(\boldsymbol{R}[x], +)$ je komutativní grupa. Operace násobení polynomů je rovněž komutativní a asociativní s neutrálním prvkem **1** . Inverzní prvek (převrácený polynom) však obecně neexistuje (pouze pro polynomy **1** a –1). Distributivnost operace násobení k operaci sčítání je zřejmá, proto $(\boldsymbol{R}[x], +, .)$ je okruh, který není tělesem. Neexistence dělitelů nuly v $(\boldsymbol{R}[x], +, .)$ plyne z obecné věty 1. 3. a jejího důsledku ([5], s. 20 – 21).

Poznámka 11. 9. Z obecné teorie dělitelnosti v oboru integrity plyne, že jednotkami okruhu $\boldsymbol{R}[x]$ jsou právě všechny nenulové konstantní polynomy (nenulová reálná čísla, viz též [5], věta 1. 4. s. 21) a s každým polynomem $f \in \boldsymbol{R}[x]$ jsou asociovány všechny jeho násobky nenulovým reálným číslem. Poznamenejme dále, že z předchozí věty plyne existence neomezeně definované operace odčítání polynomů v $\boldsymbol{R}[x]$ (převádí se na přičítání opačného polynomu), zatímco operace dělení polynomů v $\boldsymbol{R}[x]$ není obecně definována. Tomu se budeme dále věnovat. Pro operace sčítání a násobení polynomů v $\boldsymbol{R}[x]$ platí řada zřejmých vztahů, z nichž některé nyní uvedeme (předpokládáme, že $f, g \in \boldsymbol{R}[x]$):

$$st(f + g) \leq max\ \{st(f), st(g)\},$$

$$st\ (f\ .\ g) = st\ (f) + st(g)\ ,$$

platí zákony o krácení $(f \neq \boldsymbol{0},\ f\ .\ g = f\ .\ h \Rightarrow g = h\ )$.

Poznámka 11. 10. Vlastnosti polynomů nad $\boldsymbol{R}[x]$ nejsou v obecném případě tak samozřejmé, jak se zdá na první pohled. Např. u polynomů nad okruhem $\boldsymbol{Z}_4$ platí pro $f = 2x,\ g = 2x^2$ vztah $st(f\ .\ g) = st\ (0\ x^3) = st(\boldsymbol{0}) = -\infty < 3 = st(f) + st(g)$, v $\boldsymbol{Z}_4[x]$ dále platí $(1 + 2x)\ .\ (1 + 2x) = 1$, tzn. jednotkou v $\boldsymbol{Z}_4[x]$ může být i lineární polynom. Těmito případy se však nebudeme zabývat (podle poznámky 11. 2. se omezujeme pouze na polynomy s reálnými koeficienty).

Definice 11. 11. Nechť $f, g \in \boldsymbol{R}[x]$. Existuje-li polynom $h \in \boldsymbol{R}[x]$ s vlastností $f = g\ .\ h$, pak říkáme, že polynom g dělí polynom f a píšeme $g \mid f$. V opačném případě říkáme, že polynom g nedělí polynom f a píšeme $g \nmid f$.

Poznámka 11. 12. Analogicky jako v obecné teorii je nulový polynom v $\boldsymbol{R}[x]$ dělitelný každým polynomem z $\boldsymbol{R}[x]$, zatímco vztah $\boldsymbol{0} \mid f$ platí jedině v případě, že $f = \boldsymbol{0}$. Protože $\boldsymbol{R}[x]$ je obor integrity (a $\boldsymbol{R}$ je dokonce těleso), lze na dělitelnost v $\boldsymbol{R}[x]$ převést všechny pojmy a tvrzení z obecné teorie dělitelnosti v oboru integrity.

Definice 11. 13. Nechť $f, g \in \boldsymbol{R}[x]$ jsou dva reálné polynomy, $g \neq \boldsymbol{0}$. Jestliže existují polynomy $q, r \in \boldsymbol{R}[x]$ s následujícími vlastnostmi
1. $f = g\ .\ q + r,$
2. $st\ (r) < st\ (g),$
pak říkáme, že lze provést dělení se zbytkem polynomu f polynomem g . Polynom q se nazývá podíl a polynom r zbytek tohoto dělení.

Věta 11. 14. Dělení se zbytkem polynomu f polynomem g lze provést pro libovolnou dvojici reálných polynomů $f, g \in \boldsymbol{R}[x],\ g \neq \boldsymbol{0}$, přičemž podíl i zbytek jsou určeny jednoznačně.

Poznámka 11. 15. V obecném případě polynomů f, g nad libovolným okruhem se může stát, že dělení se zbytkem nelze vůbec provést, případně že podíl a zbytek nejsou určeny jednoznačně. S těmito případy se ale ve školské praxi běžně nesetkáváme, proto se jimi nebudeme zabývat. Podrobnosti lze nalézt v [5] na s.23 – 25.

Poznámka 11. 16. Známe těleso reálných čísel $\boldsymbol{R}$ i těleso komplexních čísel $\boldsymbol{C}$, přičemž víme, že těleso $\boldsymbol{C}$ je nadtělesem tělesa $\boldsymbol{R}$. Proto lze všechny polynomy s reálnými koeficienty chápat současně jako polynomy v $\boldsymbol{C}[x]$, tj. polynomy s komplexními koeficienty. Pro libovolnou dvojici takových komplexních polynomů $f, g \in \boldsymbol{C}[x],\ g \neq \boldsymbol{0}$, které mají všechny

koeficienty reálné, vždy ale dostaneme jako podíl i zbytek opět polynomy se všemi reálnými koeficienty.

Definice 11. 17. Nechť $f \in \boldsymbol{R}[x]$ je polynom tvaru (1), nechť $c \in \boldsymbol{R}$ je pevně zvolené reálné číslo. Pak reálné číslo

$$a_n c^n + a_{n-1} c^{n-1} + \ldots + a_2 c^2 + a_1 c + a_0$$

se nazývá hodnota polynomu f v bodě c a označuje $f(c)$. Je-li $f(c) = 0$, pak číslo c nazýváme kořen polynomu f.

Poznámka 11. 18. Kořenem nulového polynomu je každé reálné číslo, naopak každý polynom stupně nula nemá nikdy žádný kořen. Pro polynomy z $\boldsymbol{R}[x]$ platí následující fakta:
- Lineární polynom má vždy právě jeden kořen.
- Polynomy vyšších stupňů kořeny mít mohou, ale také nemusí.
- Neexistuje obecný algoritmus pro určení kořenů polynomu.

V dalším textu se k problematice určování kořenů ještě vrátíme.

Věta 11. 19. Nechť $f, g \in \boldsymbol{R}[x]$. Pak platí:
1. $f = g \Rightarrow \forall c \in \boldsymbol{R} ; f(c) = g(c)$.
2. $\forall c \in \boldsymbol{R} ; (f + g)(c) = f(c) + g(c)$
   $(f - g)(c) = f(c) - g(c)$
   $(f . g)(c) = f(c) . g(c)$

Věta 11. 20. Reálné číslo c je kořenem polynomu $f \in \boldsymbol{R}[x]$, právě když polynom $(x - c)$ dělí polynom f. Pro polynom $(x - c)$ se v tomto případě užívá název kořenový činitel.

Definice 11. 21. Nechť $\boldsymbol{R}$ je těleso všech reálných čísel, nechť k je přirozené číslo. Prvek $c \in \boldsymbol{R}$ se nazývá k – násobný kořen (kořen násobnosti k) polynomu $f \in \boldsymbol{R}[x]$, jestliže platí:
1. $(x - c)^k \mid f$.
2. $(x - c)^{k+1} \nmid f$.

Pro $k = 1$ budeme užívat názvu jednoduchý kořen.

Poznámka 11. 22. Jestliže platí podle předchozí definice $(x - c)^k \mid f$, pak také samozřejmě platí $(x - c)^m \mid f$ pro všechna přirozená čísla $m = 1, 2, \ldots, k$. Proto je k – násobný kořen podle věty 11. 20. kořenem ve smyslu definice 11. 17.

Věta 11. 23. Nechť $f \in \boldsymbol{R}[x]$ je polynom s reálnými koeficienty, $f \neq \boldsymbol{0}$. Jsou-li reálná čísla $c_1, c_2, \ldots, c_n$ navzájem různé kořeny polynomu f o násobnostech $k_1, k_2, \ldots, k_n$, pak polynom f je dělitelný polynomem $(x - c_1)^{k_1} \cdot (x - c_2)^{k_2} \cdot \ldots \cdot (x - c_n)^{k_n}$.

Důsledek 11. 24. Nechť $f \in \boldsymbol{R}[x]$ je reálný polynom stupně $m \geq 0$. Pak platí: Jsou-li reálná čísla $c_1, c_2, \ldots, c_n$ navzájem různé kořeny polynomu f o násobnostech $k_1, k_2, \ldots, k_n$, pak platí nerovnost $k_1 + k_2 + \ldots + k_n \leq m$. Každý reálný polynom stupně $m \geq 0$ má tedy nejvýše m reálných kořenů .

Poznámka 11. 25. Až doposud jsme chápali reálné polynomy ve smyslu definice 11. 3. jako algebraické výrazy. Z matematické analýzy však víme, že reálný polynom lze současně chápat jako předpis jisté reálné funkce s velmi „sympatickými“ vlastnostmi (je definovaná a

spojitá na celé reálné ose, v každém bodě má derivaci, snadno se integruje atd.). Tuto možnost nyní teoreticky popíšeme.

Definice 11. 26. Nechť $f \in \boldsymbol{R}[x]$ je reálný polynom. Pak zobrazení $\Phi_f : \boldsymbol{R} \to \boldsymbol{R}$, definované vztahem $\Phi_f(r) = f(r)$ pro libovolné reálné číslo r, se nazývá polynomiální funkce polynomu f. Je-li $\Psi: \boldsymbol{R} \to \boldsymbol{R}$ nějaké zobrazení, pak Ψ se nazývá polynomiální funkce, je-li polynomiální funkcí nějakého reálného polynomu z $\boldsymbol{R}[x]$.

Definice 11. 27. Řekneme, že dva reálné polynomy $f, g \in \boldsymbol{R}[x]$ jsou funkčně rovné, platí-li $\Phi_f = \Phi_g$, tzn. pro libovolné reálné číslo r platí $f(r) = g(r)$.

Věta 11. 28. Dva reálné polynomy $f, g \in \boldsymbol{R}[x]$ jsou rovné, právě když jsou funkčně rovné.

Poznámka 11. 29. Předchozí věta 11. 28. platí obecně nejen pro polynomy nad tělesem reálných čísel, ale nad libovolným nekonečným oborem integrity (viz [5], s. 31.). Obecně tedy není možné z funkční rovnosti dvou polynomů nad libovolným okruhem usuzovat na jejich rovnost (opačná implikace plyne z věty 11. 19.). S touto situací se však běžně v praxi nesetkáte (příklad viz [5], s. 31.). Proto je možné (a v matematické analýze běžně využívané) ztotožnit polynom s jeho polynomiální funkcí (někdy se užívá i názvu polynomická funkce).

Poznámka 11. 30. Nyní se budeme zabývat problematikou dělitelnosti v oboru integrity $\boldsymbol{R}[x]$, tj. dělitelností reálných polynomů. Můžeme využít všech pojmů a tvrzení, které jsme uvedli v kapitole o obecné teorii dělitelnosti v oboru integrity.

Věta 11. 31. Nechť $f, g \in \boldsymbol{R}[x]$ jsou dva reálné polynomy takové, že $f \neq \boldsymbol{0}$ a $g \mid f$. Pak platí:

$$st(g) \leq st(f).$$

Věta 11. 32. Nechť $f, g \in \boldsymbol{R}[x]$ jsou dva reálné polynomy. Pak jsou následující výroky ekvivalentní:

1. $f \sim g$
2. $f \mid g \wedge g \mid f$
3. Existuje nenulové reálné číslo c s vlastností $f = c \cdot g$

Poznámka 11. 33. Připomeňme, že jednotkami okruhu $\boldsymbol{R}[x]$ jsou právě všechny nenulové konstantní polynomy (nenulová reálná čísla, viz též [5], věta 1. 4. s. 21). Podle předchozí věty jsou s každým polynomem $f \in \boldsymbol{R}[x]$ asociovány všechny jeho násobky nenulovým reálným číslem.

Věta 11. 33. Nechť pro polynomy z $\boldsymbol{R}[x]$ platí: $g \mid f_1, g \mid f_2, \ldots, g \mid f_k$ (kde k je pevné přirozené číslo), nechť $h_1, h_2, \ldots, h_k$ jsou libovolné reálné polynomy z $\boldsymbol{R}[x]$. Pak $g \mid \sum_{i=1}^{k} f_i h_i$.

Definice 11. 34. Nechť $h, f_1, f_2, \ldots, f_k \in \boldsymbol{R}[x]$. Platí-li $h \mid f_i$ pro $i = 1, 2, \ldots, k$, pak polynom h se nazývá společný dělitel polynomů $f_1, f_2, \ldots, f_k$.

Definice 11. 35. Nechť $f_1, f_2, \ldots, f_k \in \boldsymbol{R}[x]$. Pak největším společným dělitelem polynomů $f_1, f_2, \ldots, f_k$ nazýváme polynom $d \in \boldsymbol{R}[x]$, pro který platí:

1. d je společným dělitelem polynomů $f_1, f_2, \ldots, f_k$,

2. je-li $h \in \boldsymbol{R}[x]$ společným dělitelem polynomů $f_1, f_2, ..., f_k$, pak je $h \mid d$.
Označujeme $d = NSD\ (f_1, f_2, ..., f_k)$.

Věta 11. 36. K libovolným polynomům $f_1, f_2, ..., f_k \in \boldsymbol{R}[x]$ ($k \in \boldsymbol{N}$) existuje největší společný dělitel.

Věta 11. 37. Množinu všech největších společných dělitelů polynomů $f_1, f_2, ..., f_k \in \boldsymbol{R}[x]$ obdržíme jako množinu všech nenulových konstantních násobků jednoho (libovolného) největšího společného dělitele polynomů $f_1, f_2, ..., f_k \in \boldsymbol{R}[x]$.

Poznámka 11. 38. V množině všech největších společných dělitelů polynomů $f_1, f_2, ..., f_k \in \boldsymbol{R}[x]$ existuje vždy jeden, který je normovaný. Ten budeme označovat pouze $(f_1, f_2, ..., f_k)$.

Poznámka 11. 39. Důležitou otázkou je nyní způsob výpočtu největšího společného dělitele reálných polynomů. Nejvýhodnější metodou je Eukleidův algoritmus postupného dělení, jehož princip již byl uveden v kapitole o dělitelnosti v oboru celých čísel. Ukázka praktického výpočtu je uvedena v [5], s. 36 – 39.

Věta 11. 40. Nechť $f, g \in \boldsymbol{R}[x]$ jsou reálné polynomy, z nichž alespoň jeden je nenulový. Potom platí:
1. Existují polynomy $u, v \in \boldsymbol{R}[x]$ s vlastností $f \,.\, u + g \,.\, v = (f, g)$
2. Je-li navíc $st(f), st(g) \geq 1$, pak lze polynomy u, v z části 1. vybrat tak, že platí nerovnosti
   $st(f) > st(v)\ ,\ st(g) > st(u)$.

Definice 11. 41. Polynomy $f, g \in \boldsymbol{R}[x]$ nazýváme nesoudělné, je-li $(f, g) = 1$.

Věta 11. 42. Nechť $f, g \in \boldsymbol{R}[x]$; pak polynomy f, g jsou nesoudělné, právě když existují polynomy $u, v \in \boldsymbol{R}[x]$ s vlastností $f \,.\, u + g \,.\, v = 1$.

Věta 11. 43. Nechť $f, g, h \in \boldsymbol{R}[x]$, pak platí:
1. $(f, g) = 1 \ \wedge\ (f, h) = 1 \ \Rightarrow\ (f, g.h) = 1$
2. $h \mid (f.g) \ \wedge\ (h, f) = 1 \ \Rightarrow\ h \mid g$
3. $g \mid f \ \wedge h \mid f \ \wedge\ (g, h) = 1 \ \Rightarrow\ (g.h) \mid f$

Poznámka 11. 44. Nyní následuje stručné pojednání o rozkladu polynomů nad tělesem reálných čísel. Protože víme, že v tomto případě často hraje důležitou roli i těleso čísel komplexních (např. polynom $x^2 + 1$ nelze rozložit v oboru reálných čísel, ale je možno ho rozložit v oboru čísel komplexních), budeme od nynějška do svých úvah zahrnovat i těleso komplexních čísel. Jak víme, jedná se o nadtěleso tělesa všech reálných čísel. Množinu všech polynomů nad tělesem komplexních čísel budeme označovat $\boldsymbol{C}[x]$.

Definice 11. 45. Nechť $f \in \boldsymbol{R}[x],\ st\ (f) \geq 1$. Řekneme, že polynom f je reducibilní (rozložitelný) v $\boldsymbol{R}[x]$ (nebo též nad tělesem $\boldsymbol{R}$), jestliže existují polynomy $g, h \in \boldsymbol{R}[x],\ 1 \leq st(g), st(h) < st(f)$ takové, že platí

$$f = g \,.\, h$$

V opačném případě říkáme, že polynom f je v $\boldsymbol{R}[x]$ ireducibilní (nerozložitelný).

Věta 11. 46. Nechť $f \in \boldsymbol{R}[x]$. Pak platí:

1. Je-li f reducibilní v $\boldsymbol{R}[x]$, pak je reducibilní v $\boldsymbol{C}[x]$.
2. Je-li f ireducibilní v $\boldsymbol{C}[x]$, pak je ireducibilní v $\boldsymbol{R}[x]$.

Poznámka 11. 47. Každý lineární polynom je vždy ireducibilní (jak v $\boldsymbol{R}[x]$, tak v $\boldsymbol{C}[x]$).

Věta 11. 48. Nechť $f, g \in \boldsymbol{R}[x]$, nechť f je ireducibilní nad $\boldsymbol{R}$. Pak platí: $(f, g) = 1 \vee f \mid g$.

Věta 11. 49. Nechť $f \in \boldsymbol{R}[x]$; pak jsou následující výroky ekvivalentní:
a) f je ireducibilní v $\boldsymbol{R}[x]$
b) je-li $f \mid (g \,.\, h)$, kde $g, h \in \boldsymbol{R}[x]$, pak $f \mid g$ nebo $f \mid h$.

Poznámka 11. 50. Část b) předchozí věty lze matematickou indukcí rozšířit pro libovolný konečný součin polynomů. Vyjádřeno slovy: Jestliže ireducibilní polynom dělí součin konečně mnoha polynomů , potom musí dělit alespoň jednoho z nich.

Věta 11. 51. Nechť $f \in \boldsymbol{R}[x], st\,(f) \geq 1$. Pak platí:
1. Polynom f lze vyjádřit jako součin konečného počtu ireducibilních polynomů nad $\boldsymbol{R}$
2. Toto vyjádření je jednoznačné až na pořadí a asociovanost.

Příklad 11. 52. Část 2. předchozí věty lze ilustrovat takto:
Zřejmě platí $x^2 - 1 = (x + 1)(x - 1)$, ale také např. $x^2 - 1 = (4x + 4)\left(\frac{1}{4}x - \frac{1}{4}\right)$ nebo také $x^2 - 1 = \left(\frac{1}{3}x - \frac{1}{3}\right)(3x + 3)$ atd. Podle části 2. předchozí věty se jedná o tentýž rozklad polynomu $x^2 - 1$.

Definice 11. 53. Nechť $(M, +, .)$ je libovolné těleso. Řekneme, že toto těleso je algebraicky uzavřené, jestliže každý polynom $f \in M[x], st\,(f) \geq 1$, má v M alespoň jeden kořen.

Věta 11. 54. Nechť $(M, +, .)$ je libovolné těleso. Pak následující výroky jsou ekvivalentní:
1. Těleso M je algebraicky uzavřené.
2. Každý polynom $f \in M[x], st\,(f) \geq 1$ lze vyjádřit ve tvaru součinu lineárních polynomů z $M[x]$.
3. Ireducibilní polynomy v $M[x]$ jsou právě všechny lineární polynomy.

Věta 11. 55. Nechť M je algebraicky uzavřené těleso. Pak každý polynom $f \in M[x]$, $st\,(f) = n \geq 1$ má v M právě n kořenů, počítáme-li každý kořen tolikrát, kolik je jeho násobnost.

Poznámka 11. 56. Vlastnost algebraické uzavřenosti jsme definovali obecně pro libovolná tělesa. Vrátíme-li se k našemu předpokládanému omezení na těleso $\boldsymbol{R}$ a jeho nadtěleso $\boldsymbol{C}$, je zřejmý rozdíl mezi nimi. I když se řešením algebraických rovnic budeme ještě v dalším zabývat, již na tomto místě si připomeneme to, co je intuitivně známé z dřívějšího studia: Těleso $\boldsymbol{R}$ není algebraicky uzavřené (jistě si každý sám sestaví rovnici, která nemá reálné kořeny), zatímco těleso $\boldsymbol{C}$ algebraicky uzavřené je. Dokázat přesně formálně tuto skutečnost je ale velmi obtížné. Proto následující větu (nazývanou „**Základní věta algebry**“) uvedeme stejně jako ostatní tvrzení bez důkazu i bez odkazu na něj. Možná se zdá formulace základní

věty algebry zbytečná (sám fakt je intuitivně jasný), ale z historického hlediska má tato věta značný význam.

Věta 11. 57. Těleso $\boldsymbol{C}$ všech komplexních čísel je algebraicky uzavřené.

Poznámka 11. 58. Protože těleso $\boldsymbol{C}$ je algebraicky uzavřené, platí pro něj všechno to, co jsme uvedli obecně pro algebraicky uzavřená tělesa (věty 11. 54. a 11. 55.). Stačí ve tvrzeních těchto vět nahradit označení M písmenem $\boldsymbol{C}$.

Definice 11. 59. Nechť $f \in \boldsymbol{R}[x]$ je reálný polynom, kde

$$f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 . \qquad (2)$$

Pak derivací polynomu f rozumíme polynom $f' \in \boldsymbol{R}[x]$ definovaný vztahem:

$$f' = \begin{cases} 0, & je-li\ st(f) \le 0 \\ n \cdot a_n \cdot x^{n-1} + \ldots + 2a_2 \cdot x + a_1, & je-li\ st(f) \ge 1 \end{cases} .$$

Poznámka 11. 60. I když jsme (na rozdíl od matematické analýzy) definovali derivaci polynomu čistě formálně, lze snadno rozepsáním dokázat, že její vlastnosti jsou analogické jako v matematické analýze. Uveďme některé z nich:

- nechť $st\ (f) = n$, pak $st\ (f') = n - 1$;
- $(f + g)' = f' + g'$;
- $(f . g)' = f'g + fg'$;
- $(f^k)' = k . f^{k-1} . f'$.

Analogicky se zavádí rovněž derivace vyšších řádů pomocí vztahu

$$f^{(k+1)} = (f^{(k)})' , \text{ pro } k \in \boldsymbol{N_0} , f^{(0)} = f .$$

Definice 11. 61. Nechť $f \in \boldsymbol{R}[x]$ je reálný polynom tvaru (2), nechť $c \in \boldsymbol{R}$ je pevně zvolené reálné číslo. Je-li

$$f(x) = a_0 + a_1 (x - c) + a_2 (x - c)^2 + \ldots + a_n (x - c)^n ; \quad a_i \in \boldsymbol{R}$$

pak pravou stranu nazýváme Taylorův rozvoj polynomu f o středu c .

Věta 11. 62. Nechť $f \in \boldsymbol{R}[x]$, $st\ (f) = n \ge 1$, nechť $c \in \boldsymbol{R}$. Pak existuje právě jeden Taylorův rozvoj polynomu f o středu c , který je tvaru

$$f(x) = f(c) + \frac{f'(c)}{1!} (x - c) + \frac{f''(c)}{2!} (x - c)^2 + \ldots + \frac{f^{(n)}(c)}{n!} (x - c)^n .$$

Poznámka 11. 63.

a) Pozorný čtenář si jistě povšimnul, že Taylorův rozvoj polynomu f o středu c je jeho přesné vyjádření, proto v něm nevystupuje žádný zbytek (jako při rozvojích funkcí e^x, $\sin x$, $\cos x$ apod.).

b) Pro výpočet koeficientů Taylorova rozvoje polynomu f o středu c (a obecně pro dělení polynomu lineárním polynomem) existuje algoritmus, zvaný Hornerovo schéma. Jeho princip poznáte dále, zdůvodnění viz [5], s. 51 – 52.

c) Význam derivace polynomu v algebře při hledání kořenů polynomu bude ukázán v kapitole o algebraických rovnicích.

Poznámka 11. 64. Užití Hornerova schématu:

1. Dělení polynomu lineárním normovaným polynomem.
2. Výpočet koeficientů Taylorova rozvoje.
3. Zjištění hodnoty polynomu v daném bodě.
4. Zjištění, zda dané číslo je kořenem polynomu (řešením příslušné algebraické rovnice.

Příklad 11. 65. Ukázka Hornerova schématu.
Základní funkcí Hornerova schématu je dělení polynomu f lineárním normovaným polynomem g. Není-li g normovaný polynom, tj. je tvaru $ax + b$, $a \neq 0$, $a \neq 1$, pak nejprve dělence f i dělitele g vydělíme číslem a. Polynom g tím normujeme a upravíme na tvar $x - c$. . Nechť tedy jsou oba polynomy vyjádřeny takto:

$$f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 \ , \quad g = x - c.$$

Hornerovo schéma je tabulka, obsahující dva řádky a dva sloupce. Levé horní záhlaví nevyplňujeme, do pravého horního záhlaví vypíšeme všechny koeficienty dělence f (včetně nulových). Do levé spodní části napíšeme číslo c z dělitele a jsme připraveni počítat hodnoty v pravé spodní části. Koeficient a_n sepíšeme o řádek níž. Potom číslem c vynásobíme toto číslo a_n a přičteme číslo a_{n-1} z horního řádku. Vypočtené číslo zapíšeme pod koeficient a_{n-1}. Vynásobíme jím číslo c, přičteme a_{n-2} a výsledek napíšeme pod a_{n-1} . Takto postupujeme, dokud nejsou v pravé horní části vyčerpány všechny koeficienty dělence. Poslední číslo napravo v dolním řádku oddělíme. Toto oddělené číslo je zbytkem při dělení, kdežto čísla neoddělená v pravé dolní části označují koeficienty podílu. Postup ilustrujeme na příkladu:

$f = 3x^5 - 2x^3 - 7x^2 + 4x - 8$, $g = x - 2$.

	3	0	–2	–7	4	–8
2	3	6	10	13	30	52

Platí tedy: $3x^5 - 2x^3 - 7x^2 + 4x - 8 : x - 2 = 3x^4 + 6x^3 + 10x^2 + 13x + 30$, zbytek je 52. Současně jsme ověřili, že číslo 2 není kořenem polynomu f, protože $f(2) = 52$.

Poznámka 11. 66. V poslední části kapitoly o polynomech se krátce dotkneme i problematiky interpolačních polynomů a polynomů více proměnných.

Věta 11. 67. Nechť $f, g \in \boldsymbol{R}[x]$ jsou reálné polynomy, $st\,(f), st\,(g) \geq n$, kde n je pevné přirozené číslo. Jestliže oba polynomy f, g nabývají stejných hodnot v alespoň $(n + 1)$ různých bodech, pak platí $f = g$.

Věta 11. 68. Nechť $c_1 , c_2 , \ldots, c_{n+1}$ jsou navzájem různá reálná čísla, nechť $y_1 , y_2 , \ldots, y_{n+1}$ jsou libovolná reálná čísla. Pak existuje právě jeden reálný polynom $f \in \boldsymbol{R}[x]$ takový, že $st\,(f) \leq n$ a platí $f(c_i) = y_i$ pro $i = 1, 2, \ldots, n + 1$.

Poznámka 11. 69. Lagrangeův tvar interpolačního polynomu.
Nechť platí předpoklady a označení věty 11. 68. Pak hledaný polynom $f(x)$ je tvaru

$$f(x) = y_1 \cdot \frac{(x-c_2)(x-c_3)\cdot\ldots\cdot(x-c_{n+1})}{(c_1-c_2)(c_1-c_3)\cdot\ldots\cdot(c_1-c_{n+1})} + y_2 \cdot \frac{(x-c_1)(x-c_3)\cdot\ldots\cdot(x-c_{n+1})}{(c_2-c_1)(c_2-c_3)\cdot\ldots\cdot(c_2-c_{n+1})} +$$
$$\ldots + y_{n+1} \cdot \frac{(x-c_1)(x-c_2)\cdot\ldots\cdot(x-c_n)}{(c_{n+1}-c_1)(c_{n+1}-c_2)\cdot\ldots\cdot(c_{n+1}-c_n)} \ .$$

Polynomy více proměnných

Poznámka 11. 70. Polynomy více proměnných jsou formálně definovány analogicky jako polynomy jedné proměnné pomocí nekonečných posloupností. Tímto se zde nebudeme zabývat (podrobnosti viz [5]). Pro naše účely postačí intuitivní představa, podle níž mají polynomy více proměnných tvar analogický polynomům jedné proměnné s tím rozdílem, že obsahují další proměnné (obecně značené x_1 , x_2 , ..., x_n , v případě nejvýše tří proměnných bývá běžnější označení x, y, z). Polynomy více proměnných jsou tedy např. polynomy

$$f = 6\,x^3 y\,z^2 + 2\,x\,z^3 - 5\,y^4 z + 1,$$

$$g = x^3 + y^3 + z^3, \text{ atd.}$$

I z našeho intuitivního pohledu je ale zřejmé, že na polynomy více proměnných nelze mechanicky přenést některé pojmy z teorie polynomů jedné proměnné, např. stupeň polynomu. Tím se nyní budeme zabývat. Množinu všech polynomů n proměnných nad tělesem reálných čísel budeme označovat $\boldsymbol{R}[x_1 , ..., x_n]$. Polynomům více proměnných nad jinými okruhy se opět nebudeme věnovat. Poznamenejme ještě, že analogicky jako u polynomů jedné proměnné jsou definovány operace sčítání, odčítání a násobení polynomů více proměnných.

Věta 11. 71. $\boldsymbol{R}[x_1 , ..., x_n]$ s operacemi sčítání a násobení je obor integrity.

Definice 11. 72. Nechť $\boldsymbol{R}[x_1 , ..., x_n]$ je obor integrity polynomů n proměnných nad tělesem reálných čísel. Nechť $i_1 , ..., i_n$ jsou nezáporná celá čísla. Pak výraz

$$x_1^{i_1} \cdot x_2^{i_2} \cdot \ldots \cdot x_n^{i_n} \qquad (\bullet)$$

nazýváme členem o n proměnných, nebo stručně členem.

Je-li $f = \sum a \cdot x_1^{i_1} \cdot x_2^{i_2} \cdot \ldots \cdot x_n^{i_n} \in \boldsymbol{R}[x_1 , ..., x_n]$, pak (●) nazýváme členem polynomu f . Reálné číslo a nazýváme koeficientem členu (●). Stupněm členu $x_1^{i_1} \cdot x_2^{i_2} \cdot \ldots \cdot x_n^{i_n}$ nazýváme číslo $i_1 + ... + i_n$.

Definice 11. 73. Stupeň nenulového polynomu $f \in \boldsymbol{R}[x_1 , ..., x_n]$ je roven maximálnímu ze stupňů jeho členů s nenulovými koeficienty. Polynom, jehož všechny členy mají stejný stupeň s, nazýváme homogenní polynom (stupně s).

Věta 11. 74. Každý polynom $f \in \boldsymbol{R}[x_1 , ..., x_n]$ lze napsat ve tvaru součtu homogenních polynomů navzájem různých stupňů, přičemž toto vyjádření je jednoznačné (až na pořadí).

Definice 11. 75. Nechť $f = \sum a \cdot x_1^{i_1} \cdot x_2^{i_2} \cdot \ldots \cdot x_n^{i_n} \in \boldsymbol{R}[x_1 , ..., x_n]$ a nechť $(c_1, ..., c_n)$ je uspořádaná n-tice reálných čísel. Pak reálné číslo $\sum a \cdot c_1^{i_1} \cdot c_2^{i_2} \cdot \ldots \cdot c_n^{i_n}$ se nazývá hodnota polynomu f v bodě $(c_1, ..., c_n)$ a označuje se $f(c_1, ..., c_n)$. Je-li $f(c_1, ..., c_n) = 0$, říkáme, že $(c_1, ..., c_n)$ je kořenem polynomu f.

Poznámka 11. 76. Otázky hledání kořenů, reducibility a ireducibility v $\boldsymbol{R}[x_1 , ..., x_n]$ jsou poměrně komplikované, proto je zde řešit nebudeme. Povšimneme si pouze možnosti ztotožnění polynomu více proměnných s jeho polynomiální funkcí (je definována analogicky jako u polynomů jedné proměnné).

Věta 11. 77. Nechť $f, g \in \boldsymbol{R}[x_1 , ..., x_n]$. Pak platí:

$$f = g \Leftrightarrow \forall (c_1, ..., c_n) \in \boldsymbol{R}^n;\ f(c_1, ..., c_n) = g(c_1, ..., c_n) .$$

Dva polynomy z $\boldsymbol{R}[x_1 , ..., x_n]$ jsou tedy rovné, právě když jsou funkčně rovné.

Poznámka 11. 78. Při studiu polynomů jedné proměnné jsme využívali toho, že jeho členy bylo možno seřadit sestupně nebo vzestupně. Tuto metodu však u polynomů více proměnných nelze použít. Musíme proto definovat jiný postup.

Definice 11. 79. Nechť $A = x_1^{k_1} \cdot x_2^{k_2} \cdot ... \cdot x_n^{k_n}$, $B = x_1^{s_1} \cdot x_2^{s_2} \cdot ... \cdot x_n^{s_n}$ jsou dva členy o n proměnných. Řekneme, že člen A je před členem B, existuje-li index i, $1 \le i \le n$, splňující

$$k_1 = s_1 , ... , k_{i-1} = s_{i-1} , k_i > s_i .$$

Jestliže člen A je před členem B nebo $A = B$, píšeme $A \gg B$.

Věta 11. 80. Relace $\gg$ je relace lineárního uspořádání na množině všech členů o n proměnných.

Definice 11. 81. Relaci $\gg$ nazýváme relací lexikografického uspořádání členů o n proměnných. Jsou-li členy polynomu $f \in \boldsymbol{R}[x_1 , ..., x_n]$ uspořádány pomocí této relace, říkáme, že jsme členy polynomu f uspořádali lexikograficky. Člen, který je před všemi ostatními členy tohoto polynomu f , nazýváme vedoucí člen polynomu f.

Věta 11. 82. Nechť $f, g \in \boldsymbol{R}[x_1 , ..., x_n]$ jsou libovolné dva reálné nenulové polynomy n proměnných. Pak součin vedoucích členů polynomů f a g je vedoucím členem součinu $f .g$.

Definice 11. 83. Polynom $f(x_1, ..., x_n) \in \boldsymbol{R}[x_1 , ..., x_n]$ se nazývá symetrický, jestliže se nezmění žádnou permutací proměnných, tzn. pro libovolnou permutaci $(\alpha_1, ..., \alpha_n)$ indexů $1, 2, ..., n$ platí:

$$f\left(x_{\alpha_1} , ... , x_{\alpha_n}\right) = f(x_1, ..., x_n) .$$

Množinu všech symetrických polynomů n proměnných nad tělesem reálných čísel budeme označovat $\boldsymbol{R}_s[x_1 , ..., x_n]$.

Věta 11. 84. $\boldsymbol{R}_s[x_1 , ..., x_n]$ je podobor integrity oboru integrity $\boldsymbol{R}[x_1 , ..., x_n]$.

Věta 11. 85. Nechť $A = x_1^{k_1} \cdot x_2^{k_2} \cdot ... \cdot x_n^{k_n}$ je vedoucí člen symetrického polynomu $f(x_1, ..., x_n)$. Pak platí $k_1 \ge k_2 \ge ... \ge k_n$.

Věta 11. 86. Nechť $A = x_1^{k_1} \cdot x_2^{k_2} \cdot ... \cdot x_n^{k_n}$ je člen o n proměnných. Pak existuje pouze konečně mnoho vedoucích členů symetrických polynomů o n proměnných, které jsou za členem A.

Definice 11. 87. Polynomy z $\boldsymbol{R}[x_1 , ..., x_n]$ tvaru:

$$\sigma_1 (x_1, ..., x_n) = x_1 + x_2 + ... + x_n$$

$$\sigma_2(x_1, \ldots, x_n) = x_1 x_2 + x_1 x_3 + \ldots + x_1 x_n + x_2 x_3 + \ldots + x_{n-1} x_n$$
$$\vdots$$
$$\sigma_k(x_1, \ldots, x_n) = \sum_{i_1 \prec i_2 \prec \ldots \prec i_k} x_{i_1} \cdot x_{i_2} \cdot \ldots \cdot x_{i_n}$$
$$\vdots$$
$$\sigma_n(x_1, \ldots, x_n) = x_1 \,.\, x_2 \,.\, \ldots \,.\, x_n$$

nazýváme elementární symetrické polynomy n proměnných.

Poznámka 11. 88. Elementární polynom σ_1 je tedy součtem všech proměnných $x_1, \ldots, x_n$, polynom σ_2 je součtem všech součinů jejich dvojic, polynom σ_3 je součtem všech součinů trojic, σ_4 čtveřic atd. Polynom σ_n je nakonec součinem všech proměnných $x_1, \ldots, x_n$. Pro případ $n = 3$ a zavedené označení proměnných x, y, z je tedy:

$$\sigma_1 = x + y + z$$
$$\sigma_2 = xy + xz + yz$$
$$\sigma_3 = xyz$$

Poznámka 11. 89. Předchozí definicí 11. 88., společně s větami 11. 85 a 11. 86 jsme si „připravili půdu“ pro uvedení hlavní věty o symetrických polynomech, která řeší existenci a jednoznačnost vyjádření libovolného symetrického polynomu pomocí elementárních symetrických polynomů. Uvedením této věty končíme naše pojednání o polynomech více proměnných. Praktický převod symetrických polynomů pomocí elementárních symetrických polynomů je poměrně pracný a zdlouhavý a poznáte jej ve cvičení, včetně řady zajímavých aplikací v praxi.

Věta 11. 90. Každý symetrický polynom $f(x_1, \ldots, x_n) \in \boldsymbol{R}_s[x_1, \ldots, x_n]$ lze vyjádřit jako polynom n proměnných $\sigma_1, \sigma_2, \ldots, \sigma_n$ nad $\boldsymbol{R}$, tzn.

$$f(x_1, \ldots, x_n) = \varphi(\sigma_1, \ldots, \sigma_n)$$

přičemž toto vyjádření je jednoznačné.

12. Rozklady polynomů, algebraické rovnice a jejich řešení

Definice 12. 1. Algebraickou rovnicí budeme rozumět rovnici tvaru

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 = 0\,, \qquad (3)$$

kde $a_i \in \boldsymbol{R}$ pro $i = 0, 1, \ldots, n$.

Poznámka 12. 2. Řešení algebraické rovnice je, jak je vidět z jejího tvaru (3), úzce spjato s hledáním kořenů polynomů. Řešit algebraickou rovnici (3) znamená hledat kořeny její levé strany. Kořeny lze nalézt mnoha způsoby. Řadu z nich dále uvedeme. Důležité však je (a v praxi se často využívá) umět rozložit polynom na levé straně rovnice (3). Poznamenejme ještě, že rozklad levé strany (3) má značný význam také v případě, že se jedná o algebraickou nerovnici. Poslední poznámka je terminologická. Pod označením řešení rovnice se rozumí buďto početní postup vedoucí k získání kořenů nebo přímo množina kořenů rovnice (3). Řekneme-li tedy, že řešení je pracné a zdlouhavé, máme na mysli proces, kdežto výrok „Rovnice nemá řešení" znamená, že množina kořenů je prázdná. Z kontextu bude vždy jasné, co máme na mysli.

Poznámka 12. 3. Jak již bylo uvedeno v definici 12. 1**., v**šude v této části se budeme zabývat polynomy a algebraickými rovnicemi, jejichž všechny koeficienty jsou reálná čísla; jejich kořeny však mohou být jak reálné, tak komplexní. Jedná se tedy v těchto rovnicích o polynomy nad tělesem komplexních čísel, tj. o polynomy z $\boldsymbol{C}[x]$. Protože však s polynomy, jejichž alespoň jeden koeficient je komplexní, se v praxi běžně nesetkáte, můžeme si dovolit výše uvedené zjednodušení.

Poznámka 12. 4. Z předchozí části připomínáme, že těleso komplexních čísel je algebraicky uzavřené, což má mj. tyto důsledky:
1. Ireducibilní v $\boldsymbol{C}[x]$ jsou právě všechny lineární polynomy (tzn. každý polynom stupně alespoň dvě lze v oboru $\boldsymbol{C}$ rozložit)
2. Každý polynom stupně m má v $\boldsymbol{C}$ právě m kořenů (počítáme-li každý kořen tolikrát, kolik je jeho násobnost).
3. Každý polynom $f \in \boldsymbol{C}[x]$, $f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0$ $(a_n \neq 0)$ lze vyjádřit jako součin n lineárních normovaných polynomů a nenulové konstanty ve tvaru

$$f = a_n \,.\, (x - c_1) \,.\, (x - c_2) \ldots (x - c_n)\,,\ c_i \in \boldsymbol{C},\ i = 1, 2, \ldots, n$$

(toto vyjádření, které je jednoznačné až na pořadí, se nazývá kanonický rozklad polynomu f).

Poznámka 12. 5. Nyní se vrátíme k pojmu derivace polynomu z $\boldsymbol{R}[x]$ a uvedeme, jak lze derivaci využít při hledání jeho kořenů.

Věta 12. 6. Nechť $f \in \boldsymbol{R}[x]$ a nechť $c \in \boldsymbol{R}$ je k - násobným kořenem polynomu f.
a) Je-li $k = 1$, pak c není kořenem f'
b) Je-li $k > 1$, pak c je $(k-1)$ – násobným kořenem f'.

Věta 12. 7. Nechť $f \in \boldsymbol{R}[x]$, $c \in \boldsymbol{R}$, nechť $k > 1$ je přirozené číslo. Pak platí:
1. c je k – násobný kořen $f \Leftrightarrow c$ je $(k-1)$ – násobným kořenem polynomu (f, f')
2. c je k – násobný kořen $f \Leftrightarrow f(c) = f'(c) = \ldots = f^{(k-1)}(c) = 0,\ f^{(k)}(c) \neq 0.$

Věta 12. 8. Nechť $f \in \boldsymbol{R}[x]$, $st\,(f) \geq 1$. Nechť dále $q \in \boldsymbol{R}[x]$ je polynom splňující

$$f = (f, f') \,.\, q$$

Pak polynom q má stejné kořeny jako polynom f, ale každý pouze jednoduchý.

Poznámka 12. 9. Nyní se budeme věnovat problematice kořenů a rozkladem polynomů z $\boldsymbol{C}[x]$ s reálnými koeficienty.

Věta 12. 10. Nechť $f \in \boldsymbol{C}[x]$ je polynom s reálnými koeficienty. Nechť komplexní číslo c je k – násobným kořenem polynomu f. Pak také komplexně sdružené číslo $\overline{c}$ je k – násobným kořenem polynomu f.

Věta 12. 11. Ireducibilními polynomy v $\boldsymbol{R}[x]$ jsou právě všechny lineární polynomy a všechny kvadratické polynomy se záporným diskriminantem.

Důsledek 12. 13. Pro každý polynom $f \in \boldsymbol{C}[x]$ s reálnými koeficienty platí:
1. Polynom f má vždy sudý počet imaginárních kořenů (jsou „spárované“ po dvou komplexní sdružeností) – nemusí mít ovšem žádný imaginární kořen.
2. Je-li f lichého stupně, musí mít lichý počet reálných kořenů.
3. Každý reálný polynom f, stupně alespoň 3, je nad tělesem $\boldsymbol{R}$ reducibilní.
4. Každý reálný polynom lze vyjádřit jako součin reálného číslo a konečného počtu reálných normovaných lineárních polynomů a reálných normovaných kvadratických polynomů se zápornými diskriminanty. Je-li f nenulový polynom, pak je toto vyjádření jednoznačné až na pořadí.

Poznámka 12. 14. Předchozí důsledek mj. říká, že každý polynom stupně alespoň tři lze v $\boldsymbol{R}$ rozložit, a to až na lineární a kvadratické nerozložitelné činitele. Neříká ale, jakým způsobem. Hledání rozkladů polynomů není obecně algoritmicky řešitelné. Používá se buďto hledání kořenů a postupné dělení kořenovými činiteli, dále se užívá různých vzorců, vytýkání a umělých úprav.

Příklad 12. 15. Rozložte v $\boldsymbol{R}$ polynom $f = x^4 + 1$.

$x^4 + 1 = (x^4 + 2x^2 + 1) - 2x^2 = (x^2 + 1)^2 - 2x^2 = (x^2 + \sqrt{2}\,x + 1)(x^2 - \sqrt{2}\,x + 1).$

Z rozkladu je současně vidět, že algebraická rovnice $x^4 + 1 = 0$ nemá žádný reálný kořen, ale dvě dvojice komplexně sdružených kořenů (jejich výpočet není zajímavý). Další možností, jak tuto rovnici vyřešit, je řešit ji jako rovnici binomickou. O tom se ještě dále zmíníme.

Poznámka 12. 16. Mezi kořeny a koeficienty polynomů v $\boldsymbol{C}[x]$ platí zajímavé tzv. Viètovy vztahy, které nyní uvedeme. Jistě si povšimnete, že pro kvadratické polynomy se tyto vztahy probírají už na střední škole. Poznamenejme, že v této větě uvažujeme všechny kořeny, tj. i komplexní (pouze v oboru $\boldsymbol{C}$ má polynom stupně n právě n kořenů).

Věta 12. 17. Nechť $f \in \boldsymbol{C}[x]$, $st\,(f) = n \geq 1$, kde

$$f = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0\,,$$

a nechť $c_1, c_2, \ldots, c_n$ jsou kořeny polynomu f. Pak platí:

$$-\frac{a_{n-1}}{a_n} = c_1 + c_2 + \ldots + c_n$$

$$\frac{a_{n-2}}{a_n} = c_1 c_2 + c_1 c_3 + \ldots + c_1 c_n + c_2 c_3 + \ldots + c_{n-1} c_n$$

$$\vdots$$

$$(-1)^k \frac{a_{n-k}}{a_n} = \sum_{i_1 \prec \ldots \prec i_k} c_{i_1} \cdot c_{i_2} \cdot \ldots \cdot c_{i_k}$$
$$\vdots$$
$$(-1)^n \frac{a_0}{a_n} = c_1 \,.\, c_2 \,.\, \ldots \,.\, c_n$$

Poznámka 12. 18. Pravé strany ve Viètových vztazích jsou elementární symetrické polynomy vytvořené z kořenů polynomu *f*. Jejich užití na příkladech opět poznáte ve cvičení.

Poznámka 12. 19. Nyní provedeme v rovnici (3) další omezení. Budeme předpokládat, že všechny koeficienty polynomu na levé straně rovnice (3) jsou celá čísla. Je-li alespoň jeden z nich číslo racionální (nikoliv celé), pak rovnici vynásobíme společným jmenovatelem všech takovýchto racionálních koeficientů a tím všechny koeficienty převedeme na celočíselné hodnoty. Uvedeme nyní několik užitečných tvrzení, které mohou napomoci při hledání kořenů takových rovnic s celočíselnými koeficienty. I když často k cíli vést nemusí, ve školské praxi jsou velmi užitečné. Jejich použití opět poznáte ve cvičení.

Věta 12. 20. Nechť
$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 \,,\; a_i \in \boldsymbol{Z},\; a_n \neq 0 \qquad (4)$$
je polynom s celými koeficienty a nechť racionální číslo $\frac{r}{s}$ je kořenem *f* (*r, s* jsou nesoudělná čísla). Pak platí: $r \mid a_0$ a současně $s \mid a_n$.

Důsledek 12. 21.
1. Je-li celé číslo *c* kořenem polynomu s celočíselnými koeficienty, pak $c \mid a_0$.
2. Je-li levá strana rovnice (4) normovaný polynom (tj. $a_n = 1$), pak každý racionální kořen je celé číslo.

Poznámka 12. 22. Všechna tvrzení předchozí věty i jejího důsledku mají tvar implikace, přičemž žádnou z nich nelze obrátit. Tyto implikace se nejčastěji využívají v obměněném tvaru (zformulujte sami). Nelze tedy např. tvrdit, že každý celočíselný dělitel absolutního členu je řešením rovnice (4). Lze ale všechny dělitele čísla a_0 nalézt a pomocí Hornerova schématu vyzkoušet, zda mezi nimi není kořen. Pokud ani jeden z těchto dělitelů není kořenem rovnice (4), pak víme, že daná rovnice celočíselná řešení nemá. Podobně lze vypsat všechny „podezřelé zlomky“ a ověřit, zda některý není kořenem. Těchto zlomků však může být velmi mnoho a jejich zkoušení může být zdlouhavé. Proto uvedeme ještě jedno tvrzení, pomocí kterého je možné většinu „podezřelých“ zlomků ještě před zkoušením Hornerovým schématem vyřadit.

Věta 12. 23. Nechť
$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 \,,\; a_i \in \boldsymbol{Z},\; a_n \neq 0$$
je polynom s celými koeficienty a nechť racionální číslo $\frac{r}{s}$ je kořenem *f* (*r, s* jsou nesoudělná čísla). Pak platí: $\forall m \in \boldsymbol{Z}:\; (r - ms) \mid f(m)$.

Poznámka 12. 24. Předchozí věta se užívá téměř vždy ve dvou specielních případech, a to pro hodnoty *m* rovny *1* a *–1*; platí tedy $(r - s) \mid f(1),\; (r + s) \mid f(-1)$.

Poznámka 12. 25. Při hledání kořenů algebraických rovnic je užitečné i následující tvrzení, platné pro algebraické rovnice s reálnými koeficienty. (Podrobnosti viz [13]).

Věta 12. 26. Nechť

$$a_n x^n + a_{n-1} x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0 = 0$$

je algebraická rovnice. Nechť $c_1, \ldots, c_n$ jsou její kořeny (reálné i komplexní).
Nechť $A = max \{| a_i | ; \ i = 0, \ldots, n-1\}$. Pak platí:

1. Pro každý index i, $i = 1, 2, \ldots, n$ platí nerovnost $| c_i | < 1 + \frac{A}{|a_n|}$.

2. Počet kladných reálných kořenů je roven počtu znaménkových změn v posloupnosti nenulových koeficientů $a_n , a_{n-1} , \ldots, a_1 , a_0$ nebo o sudé číslo menší.

Důsledek 12. 27. Jsou-li všechny koeficienty polynomu kladná reálná čísla, nemůže mít tento polynom kladné kořeny.

Příklad 12. 27. Je dána algebraická rovnice $4x^6 - x^3 + 4x^2 + x - 8 = 0$.
$A = 8, \ | c_i | < 1 + \frac{8}{|4|} = 3$. Absolutní hodnota všech kořenů tedy leží v intervalu $(-3, 3)$.
Posloupnost koeficientů je $4, -1, 4, 1, -8$, obsahuje tedy 3 znaménkové změny. Proto tato rovnice má buďto 3 nebo 1 kladný kořen v intervalu $(0, 3)$.

Poznámka 12. 28. Nyní stručně popíšeme základní metody řešení některých vybraných typů algebraických rovnic (podrobnosti viz [5], s. 102 – 105).

I. Lineární rovnice $ax + b = 0$ zřejmé

II. Kvadratická rovnice $ax^2 + bx + c = 0$ známé ze střední školy

III. Kubická rovnice $a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$ (5)

Nejprve vydělíme rovnici (5) číslem a_3 (předpokládáme samozřejmě $a_3 \neq 0$), přeznačíme koeficienty a proměnnou označíme z:

$$z^3 + a z^2 + b z + c = 0$$

Zavedeme substituci $z = x - \frac{a}{3}$. Po dosazení a úpravě dostaneme rovnici v tzv. redukovaném tvaru

$$x^3 + p x + q = 0 . \qquad (6)$$

Označíme $\varepsilon = cos\frac{2\pi}{3} + i \, sin\frac{2\pi}{3} = \frac{1}{2} + i \frac{\sqrt{3}}{2}$. Dále nechť $K = \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}$ označuje jednu (pevně zvolenou) z obou hodnot napsaného výrazu. Nechť dále u značí libovolnou (pevnou) ze tří třetích odmocnin $\sqrt[3]{-\frac{q}{2} + K}$ a konečně v značí tu z třetích odmocnin $\sqrt[3]{-\frac{q}{2} - K}$, která splňuje vztah $3uv = -p$. Potom kořeny rovnice (6) jsou

$$x_1 = u + v, \quad x_2 = \varepsilon . u + \varepsilon^2 . v, \quad x_3 = \varepsilon^2 . u + \varepsilon . v . \qquad (7)$$

Vzorce (7) se nazývají Cardanovy vzorce.

Zaveďme nyní výraz $D = -4p^3 - 27q^2$, který budeme nazývat diskriminant. O druhu kořenů rovnice (6) lze rozhodnout podle hodnoty diskriminantu polynomu na levé straně rovnice (6). Omezíme se na kubickou rovnici (6) s reálnými nenulovými koeficienty (v případě $p = 0$ nebo $q = 0$ je řešení triviální).

a) $D = 0$ $x_1 = -2\sqrt[3]{\frac{q}{2}}$, $x_2 = x_3 = \sqrt[3]{\frac{q}{2}}$.

b) $D > 0$ jeden kořen reálný a dva imaginární komplexně sdružené kořeny, určené vztahy (7).

c) $D < 0$ tři reálné kořeny, které však ani pomocí Cardanových vzorců (7) nelze vyřešit (tzv.“cassus irreducibilis“). Nutné je použít goniometrické řešení:

Nejprve z rovnice $\cos\varphi = \frac{-\frac{q}{2}}{\sqrt{\left(\frac{|p|}{3}\right)^3}}$ vypočítáme hodnotu úhlu φ (jednu pevně zvolenou).

Kořeny rovnice (6) jsou pak určeny vztahy: $x_1 = 2\left(\sqrt{\frac{|p|}{3}}\right)\cdot\cos\frac{\varphi}{3}$,

$$x_2 = -2\left(\sqrt{\frac{|p|}{3}}\right)\cdot\cos\left(\frac{\varphi}{3}-\frac{\pi}{3}\right), \quad x_3 = -2\left(\sqrt{\frac{|p|}{3}}\right)\cdot\cos\left(\frac{\varphi}{3}+\frac{\pi}{3}\right).$$

Poznamenejme, že Cardanovy vzorce i posledně uvedené vztahy jsou pro praktické počítání velmi pracné a zdlouhavé. Problém je rovněž v tom, že obdržené formální výsledky je nutno často pracně upravovat na použitelný tvar, zejména, užijeme-li počítače. Výjimkou jsou pouze speciálně sestavené kubické rovnice na ilustraci Cardanových vzorců. Uvedeme příklad.

Příklad: Řešte rovnici $x^3 - 3x + 1 = 0$.

Vypočteme potřebné hodnoty. Podle zadání $p = -3$, $q = 1$. Potom $D = -23 < 0$; dále tedy

$\cos\varphi = \frac{-\frac{1}{2}}{\sqrt{\left(\frac{|-3|}{3}\right)^3}} = \frac{-\frac{1}{2}}{1} = -\frac{1}{2}$, odtud $\varphi_1 = \frac{2\pi}{3}$, $\varphi_2 = \frac{4\pi}{3}$. Zvolíme $\varphi = \frac{2\pi}{3}$. Potom po dosazení a úpravě obdržíme řešení

$$x_1 = 2\cos\frac{2\pi}{9},\ x_2 = -2\cos\frac{\pi}{9},\ x_3 = -2\cos\frac{5\pi}{9}.$$

V tomto případě je řešené poměrně snadné (i když kořeny obdržíme pouze pomocí goniometrických funkcí). Nyní si ukážeme, jaké „problémy“ může způsobit využití některého matematického softwaru. Pomocí programu Derive obdržíme následující:

$$x_1 = \frac{1}{2}\sqrt[3]{-4+4i\sqrt{3}} + \frac{2}{\sqrt[3]{-4+4i\sqrt{3}}},$$

$$x_2 = -\frac{1}{4}\sqrt[3]{-4+4i\sqrt{3}} - \frac{1}{\sqrt[3]{-4+4i\sqrt{3}}} + \frac{1}{2}i\sqrt{3}\left(\frac{1}{2}\sqrt[3]{-4+4i\sqrt{3}} - \frac{2}{\sqrt[3]{-4+4i\sqrt{3}}}\right),$$

$$x_3 = -\frac{1}{4}\sqrt[3]{-4+4i\sqrt{3}} - \frac{1}{\sqrt[3]{-4+4i\sqrt{3}}} - \frac{1}{2}i\sqrt{3}\left(\frac{1}{2}\sqrt[3]{-4+4i\sqrt{3}} - \frac{2}{\sqrt[3]{-4+4i\sqrt{3}}}\right).$$

Je jasné, že pro jakékoliv další využití jsou takto vyjádřené kořeny zcela nevhodné. Proto musejí následovat formální úpravy. Převedeme-li komplexní číslo $-4+4i\sqrt{3}$ na goniometrický tvar $8\left(\cos\frac{2\pi}{3}+i\sin\frac{2\pi}{3}\right)$, lze určit tři hodnoty výrazu $\sqrt[3]{-4+4i\sqrt{3}}$: $2\left(\cos\frac{2\pi}{9}+i\sin\frac{2\pi}{9}\right)$, $2\left(\cos\frac{8\pi}{9}+i\sin\frac{8\pi}{9}\right)$, $2\left(\cos\frac{14\pi}{9}+i\sin\frac{14\pi}{9}\right)$. Dosadíme-li první z hodnot odmocniny do výrazu pro kořen x_1, dostaneme po úpravě reálnou hodnotu $x_1 = 2\cos\frac{2\pi}{9}$. Dalším dosazením dostáváme z počítačem určených výsledků kořeny $x_2 = 2\cos\frac{4\pi}{9}$, $x_3 = 2\cos\frac{8\pi}{9}$. Snadno se přesvědčíme, že $-2\cos\frac{\pi}{9} = 2\cos\frac{8\pi}{9}$ a také $-2\cos\frac{5\pi}{9} = 2\cos\frac{4\pi}{9}$, tj. trojice řešení vypočtená přímo podle Cardanovy teorie a pomocí počítače je samozřejmě tatáž. Pro úplnost dodejme přibližné číselné hodnoty kořenů: $x_1 = 2\cos\frac{2\pi}{9} = 1{,}532088886$, $x_2 = 2\cos\frac{4\pi}{9} = 0{,}3472963553$, $x_3 = 2\cos\frac{8\pi}{9} = -1{,}879385241$.

Závěrem poznamenejme, že Cardanovy vzorce se v obecném případě využívají až tehdy, když není možný žádný jiný postup. V kubických rovnicích ve školské matematice se většinou podaří jeden z kořenů určit přímo, např. užitím teorie hledání kořenů polynomů s celočíselnými koeficienty (věta 12.20 až věta 12. 26). Po vydělení kořenovým činitelem pomocí Hornerova schématu již není problém vyřešit zbylé dva kořeny jako řešení kvadratické rovnice. Pokud to tvar kubické rovnice umožňuje, lze rovněž tuto rovnici řešit jako rovnici binomickou.

IV. Rovnice čtvrtého stupně $a_4 x^4 + a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$ (8)

Stručně popíšeme metodu řešení podle R. Descarta (viz [19]). Rovnici (8) vydělíme číslem a_4 (zřejmě $a_4 \neq 0$, jinak by rovnice nebyla čtvrtého stupně). Obdržíme rovnici

$$x^4 + Bx^3 + Cx^2 + Dx + E = 0$$

Nyní použijeme substituci $x = y - \frac{B}{4}$. Po dosazení a úpravě dostaneme rovnici v redukovaném tvaru

$$y^4 + Py^2 + Qy + R = 0 \qquad (9)$$

Polynom čtvrtého stupně na levé straně rovnice (9) se nyní budeme snažit rozložit na dva normované kvadratické trojčleny. Použijeme metodu neurčitých koeficientů. Rozklad předpokládáme ve tvaru

$$(y^2 + Ky + L)(y^2 + My + N),$$

musí tedy platit

$$(y^2 + Ky + L)(y^2 + My + N) = 0. \qquad (10)$$

Po roznásobení a porovnání koeficientů s rovnicí (9) dostaneme soustavu rovnic

$$\begin{aligned} K + M &= 0 \\ KM + L + N &= P \\ KN + LM &= Q \\ LN &= R \end{aligned}$$

Řešení takových soustav je obecně velmi obtížné. V tomto případě ale budeme úspěšní (musíme ale využít umělého kroku). Nejprve za M dosadíme $-K$ a vypočteme

$$\begin{aligned} L + N &= P + K^2 \\ L - N &= -\frac{Q}{K} \\ LN &= R \end{aligned}$$

Nyní následuje avizovaný umělý obrat. Pro součet, součin a rozdíl dvou libovolných čísel u, v platí vztah:

$$(u + v)^2 - (u - v)^2 = 4uv$$

Tento vztah nyní uplatníme na výrazy L, N:

$$(P + K^2)^2 - \left(-\frac{Q}{K}\right)^2 = 4R$$

Hodnoty P, Q, R jsou však koeficienty rovnice (9). Proto lze z poslední rovnice vypočítat hodnotu K . Po úpravě dostaneme

$$K^6 + 2PK^4 + K^2(P^2 - 4R) - Q^2 = 0$$

Tato rovnice obsahuje pouze sudé mocniny neznámé K. Proto zavedeme substituci $S = K^2$. Tím získám kubickou rovnici o neznámé S, jejíž řešení bylo už popsáno dříve. Po vyřešení tří kořenů S po zpětném dosazení získáme hodnoty K a můžeme dopočítat hodnoty L, N.

Nyní již můžeme dosadit do rozkladu (10) a po vyřešení dvou kvadratických rovnic získat řešení v proměnné y . Pak už jen stačí dosadit první substituci $x = y - \frac{B}{4}$ a konečně získáme hledané řešení rovnice čtvrtého stupně (8) proměnné x.

Z uvedené metody (není samozřejmě jediná možná) plyne, že obecné řešení rovnice čtvrtého stupně je nesmírně pracné a zdlouhavé a v praxi se takřka nepoužívá. V rovnicích ve školské praxi je vždy možno využít jiný postup (nalezení kořene a dělení kořenovými činiteli, řešení jako rovnice binomická nebo reciproká), případně je v praxi nutno použít počítač.

V. Rovnice vyšších stupňů

Pro rovnice 5. stupně a stupňů vyšších už žádný obecný algoritmus řešení neexistuje. Podle teorie, vytvořené francouzským matematikem Galoisem, pro každé $n \geq 5$ existuje algebraická rovnice stupně n, která není řešitelná algebraickými metodami. Mnohé rovnice vyšších stupňů řešit můžeme, musí mít ale speciální tvar. Buďto je možné postupné „hádání“ kořenů podle 12. 20. až 12. 26. nebo je rovnice takového tvaru, který umožňuje řešit rovnici jako binomickou nebo reciprokou. Obě tyto metody znáte ze střední školy.

Další metodou, jak získat kořeny algebraické rovnice, je užití numerických metod. Tyto metody se užívají velmi často v souvislosti s rozvojem výpočetní techniky. Obecný postup sestává ze tří kroků: ohraničení kořenů, jejich separace a aproximace. Mezi dnes užívané

metody patří metoda půlení intervalů, metoda prosté iterace, metoda tečen (Newtonova metoda) a Halleyova metoda. Těmito problémy se nebudeme zabývat, jsou obsahem disciplíny Numerické metody.

13. Literatura

[1] BERAN, LADISLAV. *Grupy a svazy*. 1. vyd. Praha : SNTL - Nakladatelství technické literatury, 1974. 358 s.

[2] DRÁBEK, JAROSLAV, a kol. *Základy elementární aritmetiky pro učitelství 1. stupně ZŠ*. 1. vyd. Praha: Státní pedagogické nakladatelství, 1985. 223 s., 14-521-85.

[3] HALAŠ, RADOMÍR. *Teorie čísel.* 1. vyd. Olomouc: Univerzita Palackého, 1997. 140 s. ISBN 80-7067-707-4.

[4] HEJNÝ, MILAN. *Teória vyučovania matematiky.* 2. vyd. Bratislava : Slovenské pedagogické nakladateľstvo, 1990. 554 s. ISBN 80-08-01344-3.

[5] HORÁK, PAVEL. *Polynomy*. 1. vyd. Brno : Rektorát UJEP, 1978. 127 s. r78U.

[6] HORÁK, PAVEL. *Algebra a teoretická aritmetika.* 2. vyd. Brno : Masarykova univerzita, 1993. 145 s. ISBN 80-210-0816-4.

[7] HORÁK, PAVEL. *Algebra a teoretická aritmetika. II [Horák, 1988]*. 1. vyd. Praha : Státní pedagogické nakladatelství, 1988. 205 s.

[8] HORÁK, PAVEL. *Cvičení z algebry a teoretické aritmetiky I.* 2. vyd. Brno : Masarykova univerzita, 1998. 221 s. ISBN 80-210-1853-4.

[9] KATRIŇÁK, TIBOR. *Algebra a teoretická aritmetika 1*. 1. vyd. Bratislava : Alfa, 1985. 349 s., 63-568-85.

[10] KOPKA, JAN. *Svazy a Booleovy algebry*. 1. vyd. Ústí n. Labem : Univerzita Jana Evangelisty Purkyně v Brně, 1991. 243 s.

[11] KOSMÁK, LADISLAV – HORT, DANIEL. *Algebra.* 1. vyd. Brno: Masarykova Univerzita, 2001. 99 s. ISBN 80-210-2738-X.

[12] KUČERA, RADAN - SKULA, LADISLAV. *Číselné obory*. Vyd. 1. Brno : Masarykova univerzita, 1998. 95 s. ISBN 80-210-1965-4.

[13] MAŘÍK, ROBERT. *Matematika (nejen) pro krajináře a nábytkáře.* Elektronický učební text, MZLU, Brno 2011.

[14] ODVÁRKO, OLDŘICH - ŠEDIVÝ, JAROSLAV - CALDA, EMIL – ŽIDEK, STANISLAV. *Metody řešení matematických úloh.* 1. vyd. Praha : Státní pedagogické nakladatelství, 1990. 261 s. ISBN 80-04-20434-1.

[15] SKULA, LADISLAV. *Algebra a teoretická aritmetika. III, Číselné obory*. 1. vyd. Praha : Státní pedagogické nakladatelství, 1984. 117 s.

[16] SUŠKEVIČ, A. K. *Teorie čísel.* Charkov: Vydavatelství Univerzity A. M. Gorkéhov Charkově, 1954. 204 s.

[17] VAŇUROVÁ, MILENA. *Aritmetika 2.* Elektronický učební kurz Pedagogické fakulty MU. Dostupné z elektronické adresy *https://moodlinka.ped.muni.cz/login/index.php*, citováno dne 14. 7. 2011.

[18] *Dělitelnost.* In: Wikipedie – otevřená encyklopedie. Dostupné z elektronické adresy *http://cs.wikipedia.org/wiki/Dělitelnost*, citováno dne 12. 7. 2011.

[19] Kvartická rovnice. In: Wikipedie – otevřená encyklopedie. Dostupné z elektronické adresy *http://cs.wikipedia.org/wiki/Kvartická_rovnice*, citováno dne 13. 8. 2011.