Univerzita Hradec Králové

Přírodovědecká fakulta

Katedra matematiky

Dělitelnost v oboru integrity

Bakalářská práce

Autor: Kristýna Myšková

Studijní program: B1101 Matematika

Studijní obor: Společenské vědy se zaměřením na vzdělávání
Matematika se zaměřením na vzdělávání

Vedoucí práce : RNDr. Jitka Kühnová, Ph.D.

Hradec Králové červen 2019

Prohlášení:

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně a že jsem v seznamu použité literatury uvedla všechny prameny, z kterých jsem vycházela.

V Hradci Králové dne Kristýna Myšková

Poděkování

Ráda bych poděkovala především vedoucí své bakalářské práce RNDr. Jitce Kühnové, Ph.D., a to nejen za odborné vedení, ale i za pomoc, kterou mně během psaní práce poskytla, včetně doporučení a zapůjčení potřebné literatury.

Anotace

MYŠKOVÁ, Kristýna. *Dělitelnost v oboru integrity*. Hradec Králové, 2019. Bakalářská práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí bakalářské práce RNDr. Jitka Kühnová, Ph.D. 72 s.

Bakalářská práce je zaměřena na přehled základních pojmů z teorie okruhů dělitelnosti v oborech integrity. Práce je rozdělena na dvě hlavní kapitoly. První se zabývá okruhy, druhá dělitelností v oboru integrity.

Klíčová slova

Dělitelnost, Eukleidův obor, Gaussův obor, Okruhy, Ideál.

Annotation

MYŠKOVÁ, Kristýna. *Divisibility in the Integral Domains*. Hradec Králové, 2019. Bachelor Thesis at Faculty of Science University of Hradec Králové. Head of Bachelor Thesis RNDr. Jitka Kühnová, Ph.D. 72 s.

The main focus of this thesis was the overview of the basic concepts of the circuit theory and divisibility in the fields of integrity... The fist chapter deals with the circuits and the second one with the divisibility in the field of integrity.

Keywords

Divisibility, Euclidean discipline, Gaussian discipline, Circuits, Ideal.

Obsah

Úvod

Ve své bakalářské práci se zabývám otázkou dělitelností oboru integrity, která spadá do odvětví algebry. Téma je velice široké a obsáhlé, teorie je prakticky uzavřena. Touto problematikou se matematika zaobírá od nepaměti, mezi nejznámější odborníky patří například Euklidés z Alexandrie.

Cílem této práce je zpracování a rozbor hlavních typy oborů integrity, v nichž je pojem zaveden. Důraz je kladen na popsání jednotlivých typů oboru integrity, jejich vlastností a vazeb mezi nimi. Zároveň je na příkladech ukázána jejich konkrétní aplikace.

Práce je rozdělena do dvou hlavních kapitol. První kapitola je zaměřena na pojmy z okruhu algebraické struktury s jednou a dvěmi operacemi. Druhá kapitola je zaměřena na dělitelnost v oboru integrity.

Některá značení

$\mathbb{N}$ ... množina všech přirozených čísel, tzn. čísel {0, 1, 2, 3, ...},

$\mathbb{Z}$ ... množina všech celých čísel, tzn. {..., -2, -1, 0, 1, 2, ...},

$\mathbb{Q}$ ... množina všech racionálních čísel,

$\mathbb{R}$ ... množina všech reálných čísel,

$\mathbb{C}$ ... množina všech komplexních čísel,

G^* ... je množina invertibilních prvků v pologrupě $(G, \cdot)$,

$|H|$ ... mohutnost množiny, resp. počet prvků konečné množiny,

$|G|$ ... řád grupy G,

$\langle M \rangle$ ... podgrupa, resp. ideál, generovaná množinou M,

$[a]$ ... faktorové třídy,

M/A ... faktorový okruh podle ideálu A,

G/H ... faktorová grupa podle podgrupy H,

$a \equiv b \pmod{m}$.

Kapitola 1

Okruhy

Na začátek si připomeneme základní pojmy z teorie grup a okruhů.

1.1 Algebraické struktury s jednou operací

Definice 1.1. Nechť M je libovolná neprázdná množina, $n \in \mathbb{N}$. Zobrazení F kartézské mocniny M^n do množiny M se nazývá n-ární **algebraická operace** na množině M.
Je-li $(a_1, a_2, \ldots, a_n)$ libovolná n-tice z množiny M^n, nazývá se prvek $b \in M$, který je jejím obrazem v zobrazení F, **výsledkem** operace F (provedené na prvky $a_1, a_2, a_3, \ldots a_n$, tzv operandy, v tomto pořadí) a značí se $b = F(a_1, a_2, \ldots, a_n)$.

Poznámka

1) n-ární operací na množině M rozumíme zobrazení $F : M^n \to M$. Speciálně, 0-ární operace je zobrazení z jednoprvkové množiny M° do M, tedy konstanta. Místo 1-ární říkáme unární, místo 2-ární říkáme binární.

2) Binární operace se zpravidla značí symboly $+, \cdot, *, \circ$ apod.

3) Pokud jako symbol pro binární operaci užijeme znak „+“ , mluvíme o **aditivním** zápisu operace.

4) Pokud jako symbol pro binární operaci užijeme znak „$\bullet$“ , mluvíme o **multiplikativním** zápisu operace.

5) Řekneme že podmnožina $A \subseteq M$ je **uzavřena** na binární operaci „$*$“ , pokud pro každé $a, b \in A$ platí $a * b \in A$.

Dohoda

Dále se budeme zabývat především binárními operacemi, takže termínem „operace“ budeme rozumět binární algebraickou operaci.

Definice 1.2. Je-li $M \neq \emptyset$ a Ω libovolná neprázdná množina operací (i různých četností) definovaných na množině M, nazývá se dvojice (M, Ω) **algebraická struktura** (stručně struktura).
Množina M se pak nazývá nosič algebraické struktury (M, Ω).

Poznámka

Pro zjednodušení vyjadřování se někdy místo o struktuře (M, Ω) mluví pouze jako o struktuře M a to v případě, kdy nemůže dojít k nedorozumění.

V dalším se budeme zabývat strukturami s jednou nebo se dvěma binárními operacemi.

Definice 1.3. Struktura $(M, *)$ se nazývá **asociativní** (resp. operace „$*$“ na množině M se nazývá asociativní), právě když platí

$$(\forall x, y, z \in M)\ x * (y * z) = (x * y) * z.$$

Definice 1.4. Struktura $(M, *)$ se nazývá **komutativní**, právě když platí

$$(\forall x, y \in M)\ x * y = y * x.$$

Definice 1.5. Struktura $(M, *)$ se nazývá **struktura s neutrálním prvkem**, právě když platí:

$$(\exists x \in M)\ (\forall y \in M) \quad (x * y = y \wedge y * x = y).$$

Prvek $x \in M$ se nazývá **neutrální prvek** struktury $(M, *)$.

Poznámka

• Každá algebraická struktura $(M, *)$ má nejvýše jeden neutrální prvek, který se obvykle označuje symbolem e, resp. n.

• Při multiplikativním zápisu operace se pak obvykle neutrální prvek označuje symbolem „1“ a nazývá se **jednotkový** prvek.

• Při aditivním zápisu operace se pak obvykle neutrální prvek označuje symbolem „0“ a nazývá se **nulový** prvek.

Definice 1.6. Struktura $(M, *)$ se nazývá **struktura s inverzními prvky**, právě když má neutrální prvek e a když platí:

$$(\forall x \in M)\ (\exists y \in M) \quad (x * y = e \wedge y * x = e).$$

Prvek $y \in M$ se nazývá **inverzní prvek** k prvku x.

Poznámka

- Je-li prvek y inverzní k prvku x píšeme také $y = \bar{x}$.
- V případě multiplikativního zápisu pak píšeme: $y = x^{-1}$.
- V případe aditivního zápisu píšeme: $y = -x$, a říkáme, že prvek y je **opačný** prvek k prvku x.

Definice 1.7. Struktura $(M, *)$ se nazývá **struktura s krácením**, právě když platí:

$$(\forall x, y, z \in M)\ (x * y = y * z \Rightarrow x = y) \wedge (z * x = z * y \Rightarrow x = y).$$

Pak také říkáme, že prvkem $z \in M$ (s touto vlastností) lze **krátit** v struktuře $(M, *)$.

Struktura $(M, *)$ se nazývá **struktura s dělením**, právě když platí:

$$(\forall x, y, z \in M)(\exists z, z' \in M)\ [x * z = y \wedge z' * x = y].$$

Také říkáme, že operace „$*$“ má vlastnost **řešitelnosti základních rovnic**.

Jestliže platí:

$$(\forall x, y, z \in M)(\exists! z, z' \in M)\ [x * z = y \wedge z' * x = y],$$

nazývá se struktura $(M, *)$ **struktura s jednoznačným dělením**.

Definice 1.8. Algebraická struktura (M, $*$) se nazývá **pologrupa**, právě když struktura (M, $*$) je asociativní.

Definice 1.9. Algebraická struktura $(G, *)$ se nazývá **grupa**, právě když je to asociativní struktura s neutrálním prvkem a s inverzními prvky.
Je-li $(G, *)$ navíc komutativní struktura, se nazývá abelovská, resp. Abelova, resp. komutativní grupa.

Definice 1.10. Je-li G konečná množina, **řádem grupy** $(G, *)$ rozumíme počet prvků množiny G. Je-li G nekonečná množina, pak říkáme, grupa $(G, *)$ je grupa nekonečného řádu. Píšeme $|G|$.

Definice 1.11. Nechť a je libovolný prvek grupy $(G, *)$.
Existuje-li nejmenší kladné celé číslo k takové, že $a^k = e_G$, (e_G je neutrální prvek G) pak říkáme, že číslo k je **řád prvku** a, resp. že prvek a je řádu k v grupě $(G, *)$. Píšeme $k = o(a)$, resp. $k = |a|$.
Pokud takové číslo k neexistuje, říkáme, že prvek a je nekonečného řádu.

Poznámka
Uvažujeme-li multiplikativní grupu $(G, \cdot)$, pak k je řád prvku a, právě když $a^k = 1$. (Zápisem a^k rozumíme $a^k = a_1 \cdot a_2 \cdots a_k$).
V aditivní grupě $(G, +)$ je k řád prvku a, právě když $k \times a = 0$. (Zápisem $k \times a$ rozumíme $k \times a = a_1 + a_2 + \cdots + a_k$).

Definice 1.12. Struktura $(H, \circ)$ se nazývá **podgrupa** grupy $(G, \circ)$, právě když platí:

1. $H \subseteqq G$
2. (H, $\circ$) je grupa.

V dalším budeme, pokud nebude řečeno jinak, zapisovat grupy multiplikativně, resp. aditivně

Definice 1.13. Grupa G se nazývá **cyklická**, pokud je generovaná jedním prvkem. Tedy pokud
$G = \langle a \rangle_G$ pro nějaké $a \in G$.

Definice 1.14. Nechť $(G, *)$ je grupa, M je libovolná podmnožina množiny G. Průnik všech těch podgrup grupy G, které obsahují množinu M, je podgrupa v grupě G, která se nazývá **podgrupa generovaná množinou** M a značí se $\langle M \rangle$.
Množina M se nazývá systém generátorů grupy $\langle M \rangle$ a její prvky generátory této grupy.

Věta 1.1. Buď G cyklická grupa. Je-li G nekonečná, pak je izomorfní grupě $(\mathbb{Z}, +)$. Je-li G konečná n-prvková, pak je izomorfní grupě $(\mathbb{Z}_n, +)$.

Příklad 1.1.

• Grupy $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -1 \rangle$ a $(\mathbb{Z}_n, +) = \langle 1 \rangle$ pro libovolné přírozené číslo n jsou cyklické.

• Grupy $(\mathbb{C}_n, \cdot)$ sestávající ze všech komplexních kořenů polynomu $x^n - 1$ (jako podgrupy $(\mathbb{C}^*, \cdot)$) jsou cyklické, $\mathbb{C}_n = \langle e^{2\pi i/n} \rangle$.

• Grupy $(\mathbb{Z}_p^*, \cdot)$ jsou cyklické pro každé prvočíslo p. Např. $\mathbb{Z}_5^* = \langle 2 \rangle, \mathbb{Z}_7^* = \langle 3 \rangle, \mathbb{Z}_{11}^* = \langle 2 \rangle$.

• Některé $(\mathbb{Z}_n^*, \cdot)$, n složené, mohou být cyklické: např. $\mathbb{Z}_6^*$ obsahuje pouze prvky 1 a 5 tedy $\mathbb{Z}_6^* = \langle 5 \rangle$. Naopak např. $\mathbb{Z}_8^*$ cyklická není, všechny prvky mají řád nejvýše 2.

• Každá grupa $(G, \cdot)$ prvočíselného řádu p je cyklická. Všechny prvky kromě jednotkového prvku mají řád p, tj. generují G.

[1]

Příklad 1.2. Podgrupy grupy $(\mathbb{Z}, +)$ jsou právě $a\mathbb{Z} = \langle a \rangle, a \in \mathbb{Z}$. Přitom

$$a\mathbb{Z} = b\mathbb{Z} \Leftrightarrow a = \pm b.$$

[1]

Definice 1.15. Buď $(G, \cdot)$ grupa a H její podgrupa.

(1) Levým rozkladem grupy G podle podgrupy H se rozumí množina $\{aH : a \in G\}$, přičemž množinám $aH = \{ah : h \in H\}$ se říká **levé** rozkladové třídy.

(2) Pravým rozkladem grupy G podle podgrupy H se rozumí množina $\{Ha : a \in G\}$, přičemž množinám $Ha = \{ha : h \in H\}$ se říká pravé rozkladové třídy.

Věta 1.2. Pro každé $a, b \in G$ platí:

(1) buď $aH = bH$, nebo $aH \cap bH = \emptyset$.

(2) buď $Ha = Hb$, nebo $Ha \cap Hb = \emptyset$, tedy jednotlivé rozkladové třídy jsou disjunktivní.

Věta 1.3. Pro každé $a, b \in G$ platí

(1) $aH = bH$ právě tehdy, když $a^{-1}b \in H$.

(2) $Ha = Hb$ právě tehdy, když $ab^{-1} \in H$.

Věta 1.4. (1) Pro každé $a \in G$ platí $|aH| = |Ha| = |H|$.

(2) Levý i pravý rozklad G podle H mají stejný počet prvků

Definice 1.16. Velikost levého i pravého rozkladu jsou stejné. Tato hodnota se nazývá **index podgrupy** H **v grupě** G a značí se

$$[G : H] = |\{aH : a \in G\}| = |\{Ha : a \in G\}|.$$

Věta 1.5. (Lagrangeova)
Nechť $(G, \cdot)$ grupa řádu n, H její podgrupa řádu k a indexu m. Pak platí: $n = k \cdot m$.

Definice 1.17. Podgrupu H grupy G nazýváme **normální**, značíme $H \trianglelefteq G$, pokud pro každé $a \in G$ platí $aH = Ha$.

Poznámka

Každá podgrupa komutativní grupy je normální podgrupa.

Buď $G = (G, \cdot)$ grupa, H její normální podgrupa. Definujeme relaci

$$a \sim b \Leftrightarrow a \cdot b^{-1} \in H.$$

Podle Věty 1.3 je $a \sim b$ právě tehdy, když $Ha = Hb$, a tedy z Věty 1.2 plyne, že relace $\sim$ je ekvivalence. Její bloky jsou rozkladové třídy grupy G podle podgrupy H, a protože je H normální, levé i pravé rozkladové třídy jsou totéž, tj.
$aH = Ha = [a]$.

Na těchto blocích definujeme operace předpisy
$[a] \cdot [b] := [a \cdot b]$ a $[a]^{-1} := [a^{-1}]$.

Věta 1.6. Nechť G je grupa, H její normální podgrupa. Strukturu
$G/H = (\{[a] : a \in G\}, \cdot)$ je grupa tzv. **faktorová grupa** podle podgrupy H.

Příklad 1.3.

Grupu $(\mathbb{Z}, +)$ můžeme rozložit podle normální podgrupy $n\mathbb{Z}$, na třídy
$[a] = \{k \in \mathbb{Z} : k \equiv a \pmod{n}\}, a = 0, ..., n-1$. Faktorgrupa $\mathbb{Z}/n\mathbb{Z}$ tedy má n prvků, přičemž $[a] + [b] = [a + b] = [a + b \bmod n]$ a $-[a] = [-a] = [n - a]$.
Vidíme, že operace na prvcích $\mathbb{Z}/n\mathbb{Z}$ jsou jako operace na číslech $0, ..., n-1$ modulo n. Jinými slovy, $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}n$.

[1]

Příklad 1.4.

Grupu $\mathbf{S}n$ můžeme rozložit podle normální podgrupy $\mathbf{A}n$, na dvě rozkladové třídy, a to množinu S sudých permutací a množinu L lichých permutací. Operace na těchto třídách je $S \circ S = L \circ L = S$ a $S \circ L = L \circ S = L$. Jde o dvouprvkovou grupu.

[1]

1.2 Algebraické struktury se dvěmi operacemi

Definice 1.18. Nechť jsou na množině M definovány dvě (binární algebraické) operace „$*$" a „$\circ$".

(1) Říkáme, že operace „$\circ$" je **distributivní** vzhledem k operaci „$*$" resp. že struktura $(M, *, \text{„}\circ\text{"})$ je $(*, \circ)$ - distributivní, právě když platí:

$$(\forall x, y, z \in M)(x * y) \circ z = (x \circ z) * (y \circ z) \wedge z \circ (x * y) = (z \circ x) * (z \circ y).$$

(2) Říkáme, že operace „$*$" je **distributivní** vzhledem k operaci „$\circ$" resp. že struktura $(M, *, \text{„}\circ\text{"})$ je $(\circ, *)$ - distributivní, právě když platí:

$$(\forall x, y, z \in M)(x \circ y) * z = (x * z) \circ (y * z) \wedge z * (x \circ y) = (z * x) \circ (z * y).$$

Poznámka

V dalším budeme u struktur $(M, *, \circ)$ se dvěma operacema značit první operaci aditivně („+“) a druhou multiplikativně („$\cdot$“).

Definice 1.19. Algebraická struktura (M,+,$\cdot$) se nazývá okruh, právě když platí:

(1) $(M, +)$ je abelovská grupa,

(2) $(M, \cdot)$ je pologrupa,

(3) struktura $(M, +, \cdot)$ je $(+, \cdot)$ distributivní.

Okruh, kde struktura $(M, \cdot)$ je komutativní, se nazývá komutativní okruh.

Poznámka

(a) Abelova grupa $(M, +)$ se nazývá aditivní grupa okruhu M; její neutrální prvek nazýváme nulový prvek okruhu M a píšeme 0;

(b) Pologrupa $(M, \cdot)$ multiplikativní pologrupa okruhu M; její neutrální prvek (pokud existuje) nazýváme jednotkový prvek okruhu M a píšeme 1;
(c) Okruh $(\{0\}, +, \cdot)$, který obsahuje pouze nulový prvek, se nazývá triviální, resp. nulový okruh.

Věta 1.7. V libovolném okruhu $(M, +, \cdot)$ pro libovolné prvky $a, b, c \in M$ platí:
1. $a \cdot 0 = 0 \cdot a = 0$;
2. pokud $a + c = b + c$, pak $a = b$;
3. $-(-a) = a, \ -(a + b) = -a - b$;
4. $-(a \cdot b) = (-a) \cdot b = a \cdot (-b), \ (-a) \cdot (-b) = ab$.

Poznámka

• Jestliže v okruhu $(M, +, \cdot)$ existují prvky x, y tak, že

$$x \neq 0 \wedge y \neq 0 \wedge xy = 0,$$

pak říkáme, že prvky x, y jsou dělitelé nuly v okruhu M.

• Neexistence dělitelů nuly v okruhu M je ekvivalentní se „zákonem nenulového součinu“, tj. platí:
$(\forall x, y \in M)\ xy = 0 \Rightarrow x = 0 \vee y = 0$, resp. $xy = 0 \wedge x \neq 0 \Rightarrow y = 0$.

Definice 1.20. Podmnožina $A \subseteq M$ tvoří podokruh okruhu M, pokud je uzavřena na všechny operace, tj. pokud $0 \in A, -a \in A, a + b \in A$ a $a \cdot b \in A$ pro každé $a, b \in A$. Podokruhy M a $\{0\}$ nazýváme **nevlastní**. Je zřejmé, že podokruhy splňují všechny axiomy okruhů a jsou to tedy také okruhy. Podokruhy komutativních okruhů jsou komutativní, ovšem podokruh nemusí obsahovat jednotkový prvek.

Příklad 1.5. Podokruhy okruhu $(\mathbb{Z}, +, \cdot)$ tvoří právě množiny $a\mathbb{Z}, a \in \mathbb{Z}$. protože to musí být podgrupy grupy $(\mathbb{Z}, +)$, $a\mathbb{Z}$ jsou jedinými kandidáty. Není těžké ověřit, že jde o podokruhy. Přitom jednotkový prvek obsahuje pouze nevlastní podokruh $\mathbb{Z}$.

[1]

Definice 1.21. Struktura $(I, +, \cdot)$ se nazývá obor integrity, právě když je to netriviální komutativní okruh s jednotkovým prvkem, ve kterém neexistují dělitelé nuly.

Příklad 1.6.

• Uvažujme množinu

$$\mathbb{Z}[i] = \{a + bi;\ a \in \mathbb{Z} \wedge b \in \mathbb{Z}\}$$

a za operace $\mathbb{Z}[i]$ uvažujme zúžení operací „+“ „$\cdot$“ v $\mathbb{C}$ na $\mathbb{Z}[i]$. Pak $(\mathbb{Z}[i], +, \cdot)$ je obor integrity - takzvaný **obor integrity celých Gaussových čísel**.

• Nechť $M = \{a + bi\sqrt{5};\ a \in \mathbb{Z} \wedge b \in \mathbb{Z}\}$; a operace v M jsou definované takto:

$(a + bi\sqrt{5}) + (c + di\sqrt{5}) = (a + c) + (b + d)i\sqrt{5}$

$(a+bi\sqrt{5})\cdot(c+di\sqrt{5}) = (ac-5bd)+(ad+bc)i\sqrt{5}, \forall a, b, c, d \in \mathbb{Z}$. Uvažujme obor integrity $(M, +, \cdot)$

Struktura $(M, +, \cdot)$ je zřejmě obor integrity.

[1]

Definice 1.22. Algebraická struktura $(T, +, \cdot)$ se nazývá **těleso**, právě když platí:

1. $(T, +)$ je abelovská grupa,
2. $(T - \{0\}, \cdot)$ je grupa (0 je nulový prvek $(T, +)$),
3. struktura $(T, +, \cdot)$ je $(+, \cdot)$ distributivní.

Těleso, kde struktura $(T - \{0\}, \cdot)$ je komutativní, se nazývá komutativní těleso resp. pole.

Poznámka

1. V tělese $(T, +, \cdot)$ existuje ke každému prvku $x \in T$, $x \neq 0$, prvek inverzní.
2. V tělese neexistují dělitelé nuly. Tedy každé komutativní těleso je obor integrity.
3. Každé těleso je vlastně netriviální okruh, v němž ke každému nenulovému prvku existuje prvek inverzní.

Definice 1.23. Nechť $(M, +, \cdot)$ je netriviální okruh. Existuje-li nejmenší kladné celé číslo n takové, že pro každé $a \in M$ platí $n \times a = 0$, pak říkáme, že n je charakteristika okruhu M a píšeme $n = charM$. Jestliže takové kladné celé číslo neexistuje, říkáme že okruh M má charakteristiku 0, resp ∞.

Poznámka

• Zřejmě char(M) = 1, právě když okruh je triviální.

• Řádem prvu a v okruhu $(M, +, \cdot)$ rozumíme řád tohoto prvku v aditivní grupě $(M, +)$.

• Je zřejmé, že charakteristika okruhu je nejmenší společný násobek řádu všech prvků okruhu.

• V okruhu s jednotkovým prvkem se charakteristika rovná řádu jednotkového prvku.

Věta 1.8. Charakteristika netriviálního okruhu bez dělitelů nuly je 0 nebo prvočíslo.

Věta 1.9. Každý konečný obor integrity resp. těleso, má (nenulovou) prvočíselnou charakteristiku.

Definice 1.24. Nechť $(M, +, \cdot)$ je komutativní okruh. Neprázdná podmnožina A množiny M, pro kterou platí:

$$(\forall a, b \in A) \quad a - b \in A \tag{1.1}$$

$$(\forall a \in A)(\forall x \in M) \quad ax \in A \tag{1.2}$$

se nazývá **ideál** v okruhu $(M, +, \cdot)$

Poznámka

1. Jinak řečeno, ideál je podgrupa aditivní grupy $(M, +)$ okruhu M, která je uzavřená vzhledem k operaci „násobení prvkem x"pro všechny prvky $x \in M$.

2. Je zřejmé, že každý ideál okruhu $(M, +, \cdot)$ je podokruhem okruhu $(M, +, \cdot)$. Ovšem ne každý podokruh je ideál. Např. podokruh $(\mathbb{Z}, +, \cdot)$ okruhu $(\mathbb{Q}, +, \cdot)$ není ideál v $(\mathbb{Q}, +, \cdot)$

3. Pojem ideál lze zavést i v případě, že výchozí okruh není komutativní. Podmínka (1.2) z definice se pak nahrazuje podmínkou

$$(\forall a \in A)(\forall x \in M)ax \in A \wedge xa \in A$$

hovoříme potom o **oboustranném ideálu**.

4. Obdobně lze zavést pojem **levého**, resp. **pravého ideálu** v okruhu M pomocí podmínky

$$(\forall a \in A)(\forall x \in M)\ ax \in A, \qquad \text{resp. } xa \in A.$$

5. Z Definice je zřejmé, že v každém okruhu $(M, +, \cdot)$ existují vždy alespoň dva ideály: **nulový ideál**, obsahující pouze nulový prvek okruhu $(M, +, \cdot)$, a okruh $(M, +, \cdot)$ sám. Tyto ideály se nazývají **triviální ideály** v $(M, +, \cdot)$.

6. Okruh $(M, +, \cdot)$ se nazývá jednoduchý, právě když je netriviální a jsou-li $(\{0\}, +, \cdot)$ a $(M, +\cdot)$ jeho jediné ideály.

7. Nebude-li řečeno jinak, omezíme se v dalších úvahách pouze na komutativní okruhy.

Poznámka

Buď M okruhu a I_1, I_2 jeho ideály. Pak množiny $I_1 \cap I_2$ a $I_1 + I_2 = \{a_1 + a_2 : a_1 \in I_1, a_2 \in I_2\}$ tvoří ideály okruhu M.

Definice 1.25. Nechť M je okruh, nechť R je libovolná podmnožina množiny M. Průnik všech ideálů okruhu M, které obsahují množinu R, se nazývá **ideál generovaný množinou** R a píšeme $\langle R \rangle$. Množina R se nazývá **systém generátorů ideálu** $\langle R \rangle$ a její prvky **generátory** tohoto ideálu.

Poznámka

1. Pokud je množina R konečná, například $R = \{a_1, a_2, ..., a_n\}$, budeme místo $[\{a_1, a_2, ..., a_n\}]$ psát pouze $[a_1, a_2, ..., a_n]$.

2. Prázdná množina generuje zřejmě v libovolném okruhu nulový ideál.

Věta 1.10. Jsou-li $a_1, a_2, ..., a_n$ libovolné prvky z ideálu A v okruhu M, je i každá jejich lineární kombinace s koeficienty z M prvkem ideálu A tj.

$$(\forall x_1, x_2, ..., x_n \in M)\ a_1x_1 + a_2x_2 + \cdots + a_nx_n \in A. \tag{1.3}$$

Příklad 1.7. V okruhu celých čísel $\mathbb{Z}$ máme určit ideál $A = [96, 14]$. Pomocí (1.3) se snažíme v tomto ideálu nalézt nenulové číslo s co nejmenší absolutní hodnotou.

Podle (1.3) musí být $1 \,.\, 96 + (-6) \,.\, 14 = 12 \in A$,

a tedy též $1 \,.14 + (-1) \,.\, 12 = 2 \in A$.

Podle (1.2) obsahuje A všechny celočíselné násobky čísla 2, tj. všechna sudá čísla. Protože podle

Definice 1.23 množina všech sudých čísel tvoří zřejmě ideál v $\mathbb{Z}$, je

$$A = \{..., -6, -4, -2, 0, 2, 4, 6, ...\} = [2].$$

Věta 1.11. Nechť M je okruh s jednotkovým prvkem 1 a nechť $R = \{a_1, a_2, ..., a_n\} \subseteq M$. Pak ideál $\langle R \rangle$ se skládá právě ze všech prvků tvaru (1.3), tj. $\langle R \rangle = A$, kde

$$A = \{a_1x_1 + a_2x_2 + ... + a_nx_n; x_1, x_2, ..., x_n \in M\}.$$

Poznámka

Nechť M je okruh s jednotkovým prvkem 1, nechť A je ideál v okruhu M. Pak platí: $1 \in A \Rightarrow A = M$.

Definice 1.26. Polynomem proměnné x nad oborem integrity I rozumíme formální výraz

$$a_0 + a_1x + a_2x^2 + ... + a_nx^n,$$

nebo zkráceně

$$\sum_{i=0}^{n} a_ix^i,$$

kde $a_0, ..., a_n \in I$ a $a_n \neq 0$. Prvky $a_0, ..., a_n$ nazýváme koeficienty a symbol x proměnná. Číslo n nazýváme stupeň polynomu, značíme deg f. Prvek a_n se nazývá vedoucí koeficient a a_0 absolutní člen. Polynom se nazývá **monický**, pokud je vedoucí člen 1. Je třeba speciálně dodefinovat nulový polynom; pro něj položíme deg 0 = -1.

Poznámka

Na množině všech polynomů definujeme operace předpisy

1. $\sum_{i=0}^{m} a_ix^i + \sum_{i=0}^{n} b_ix^i = \sum_{i=0}^{max(m,n)} (a_i + b_i)x^i, \quad -\sum_{i=0}^{m} a_ix^i \sum_{i=0}^{m} (-a_i)x^i.$
2. $(\sum_{i=0}^{m} a_ix^i) \cdot (\sum_{i=0}^{n} b_ix^i) = \sum_{i=0}^{m+n} (\sum_{j+k=i} a_jb_k)x^i.$
3. Množina všech polynomů jedné proměnné nad oborem integrity I se značí $I[x]$.
4. $I[x]$ je spolu s operacemi definovanými v 2. obor integrity.

Příklad 1.8. V oboru integrity $\mathbb{Z}[x]$ polynomů jedné proměnné s celočíselnými koeficienty máme sestrojit ideál $[x, 2]$.

Podle Věty 1.11 (neboť v $\mathbb{Z}[x]$ existuje jednotkový prvek) se tento ideál skládá ze všech prvků tvaru

$$x.\ f_1(x) + 2.f_2(x),\ \text{ kde }\ f_1(x), f_2(x) \in \mathbb{Z}[x].$$

Tedy $[x, 2]$ je množina všech polynomů $a_0 + a_1x + ... + a_xx^n \in \mathbb{Z}[x]$, jejichž absolutní člen a_0 je sudé číslo. Ideál $[x, 2]$ je tudíž vlastní podmnožina v $\mathbb{Z}[x]$.

[1]

Příklad 1.9. Hledejme ideál $[x, 2]$ v oboru integrity $\mathbb{Z}_5[x]$ polynomů jedné proměnné nad tělesem $(\mathbb{Z}_5, +, \cdot)$.

Ideál $[x, 2]$ se podle Věty 1.11 skládá z polynomů tvaru

$$x.g_1(x) + 2.g_2(x),\ \text{ kde }\ g_1(x), g_2(x) \in \mathbb{Z}_5[x].$$

Protože $\mathbb{Z}_5$ je těleso, existuje prvek $2^{-1} = 3 \in \mathbb{Z}_5$. Volíme-li tedy speciálně $g_1(x) = 0,\ g_2(x) = 3$, máme

$$x \cdot g_1(x) + 2 \cdot g_2(x) = x \cdot 0 + 2 \cdot 3 = 1$$

Tedy ideál $[x, 2]$ obsahuje jednotkový prvek 1 okruhu $\mathbb{Z}_5$[x], takže podle Věty 1.8

$$[x, 2] = [1] = \mathbb{Z}_5[x].$$

[1]

Definice 1.27. Ideál A v okruhu M se nazývá **hlavní ideál** v M, právě když má alespoň jeden systém generátorů, který je jednoprvková množina.

Příklad 1.10.

(1) Hlavním ideálem v oboru integrity I je pro libovolný prvek $a \in I$ podmnožina

$$aI = \{am : m \in I\} = \{u \in I; a/u\}.$$

Opravdu:

• Pro libovolné prvky $u, v \in aI$ platí: $u - v = am_1 - am_2, m_1, m_2 \in I$, tedy $u - v = a(m_1 - m_2) \in aI$.

• Pro libovolný prvek $u \in aI$ a libovolný prvek $x \in I$ platí: $ax = (am)x = a(mx) \in I$.

(2) Např. $0I = \{0\}$ A $1 \cdot I = I$ jsou ideály v každém oboru integrity.

[2]

Příklad 1.11. Ukážeme, že ideál $[x, 2]$ z předchozího příkladu není hlavní ideál v $\mathbb{Z}[x]$. Předpokládejme opak, že $[x, 2]$ je hlavní ideál v $\mathbb{Z}[x]$. Pak musí existovat polynom $p(x) \in \mathbb{Z}[x]$ tak, že $[x, 2] = [p(x)]$. Protože $2 \in [p(x)]$, existuje podle Věty 1.11 polynom $g(x) \in \mathbb{Z}[x]$ takový, že

$$2 = p(x) \cdot g(x).$$

Oba polynomy $p(x)$ a $g(x)$ musí mít stupeň 0, takže jsou vlastně celočíselné konstanty, jejichž součin je roven 2. Tedy

$$p(x) = \pm 2 \vee p(x) = \pm 1.$$

Kdyby platilo $p(x) = \pm 2$, byl by každý prvek z $[p(x)]$ násobkem čísla 2, avšak $x \in [p(x)]$ a nemá zřejmě tento tvar. Nemůže však platit ani $p(x) = \pm 1$, neboť pak by byl ideál $[x, 2]$ roven celému okruhu $\mathbb{Z}[x]$, což nenastane.
Tedy náš předpoklad, že $[x, 2]$ je hlavní ideál v $\mathbb{Z}[x]$, vedl ve všech případech ke sporu, takže $[x, 2]$ hlavní ideál v $\mathbb{Z}[x]$ není.
Právě ukončený příklad dokazuje existenci ideálů, které nejsou hlavní. Přesto však existují okruhy, které nemají jiné ideály než hlavní.

[1]

Definice 1.28. Okruh M se nazývá **okruh hlavních ideálů**, právě když je každý ideál okruhu M hlavní.

Příklad 1.12. Triviálním příkladem okruhu hlavních ideálů je libovolné těleso T. Opravdu: Nechť A je ideál v T; jestliže A neobsahuje žádný nenulový prvek, je A nulový ideál, takže $A = [0]$. Obsahuje-li A alespoň jeden nenulový prvek a, musí podle (1.2)

$$a \cdot a^{-1} = 1 \in A,$$

takže $A = [1] = T$. Tedy všechny ideály v T jsou hlavní.

[2]

Věta 1.12. Nechť M je okruh s jednotkovým prvkem. Pak okruh M je pole, právě když má pouze nevlastní (triviální) ideály, tj. právě když M je jednoduchý okruh.

Poznámka

Konstrukce faktorového okruhu:

Nechť M okruh, A jeho ideál. Definujme relaci

$$a \sim b \Leftrightarrow a - b \in A.$$

Protože $(M, +)$ je abelovská grupa a $(A, +)$ její normální podgrupa, relace „$\sim$“ je ekvivalence a její bloky rozkladové třídy M/A tj. $[a] = a + A$ pro každé $a \in M$.

Na těchto blocích definujme operace předpisy

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

Věta 1.13. Nechť M je okruh, A je ideál v M. Pak struktura $M/A = (\{[a]; a \in M\}+, \cdot)$ je okruh. Je to tzv. **faktorový okruh** podle ideálu A.

Věta 1.14. Nechť A je ideál v okruhu M, pak struktu $(M/A, +, \cdot)$ je okruh (s nulovým prvkem A); je-li M okruh s jednotkovým prvkem 1, má i $(M/A, +, \cdot)$ jednotkový prvek (jimž je třída $[1] = 1 + A$).

Příklad 1.13. Vezměme okruh $\mathbb{Q}[x]$ polynomů jedné proměnné nad tělesem racionálních čísel $\mathbb{Q}$ a za ideál A v $\mathbb{Q}[x]$ zvolme hlavní ideál generovaný polynomem $x^3 + 1$, tj.
$A = \langle x^3 + 1 \rangle$. Pak faktorový okruh $\mathbb{Q}[x]/A = \mathbb{Q}[x]/\langle x^3 + 1 \rangle$ se skládá ze všech tříd tvaru

$$(a_2x^2 + a_1x + a_0) + A, \qquad \text{kde } \ a_2, a_1, a_0 \in \mathbb{Q}.$$

Operace sčítání a násobení v $\mathbb{Q}$[x]/A objasníme opět pouze na příkladech.

$$(x^2 + 2x - 3 + A) + (2x^2 - 3x + A) = 3x^2 - x - 3 + A,$$
$$(x^2 + 2x - 3 + A).(2x^2 - 3x + A) = 2x^4 + x^3 - 12x^2 + 9x + A.$$

Protože výsledná třída není zapsána v základním tvaru, upravíme její zápis takto:

$$(2x^4 + 2x) + (x^3 + 1) - 12x^2 + 7x - 1 + A = 2x(x^3 + 1) + (x^3 + 1) - 12x^2 + 7x - 1 + A =$$
$$= (2x + 1)(x^3 + 1) - 12x^2 + 7x - 1 + A.$$

[1]

Definice 1.29. Ideál A okruhu M se nazývá **prvoideál**, jestliže pro každé dva prvky $a, b \in M$ takové, že $a \notin A, b \notin A$, je $ab \notin A$. Ideál A se nazývá **maximální**, jestliže je $A \neq M$ a z $A \subseteq J \subseteq M, J$ ideál v M, plyne buď $J = A$, nebo $J = M$.

Věta 1.15. Buď A ideál okruhu M. Pak A je prvoideál, právě když faktorový okruh M/A je obor integrity.

Věta 1.16. Buď A ideál okruhu M. Pak A je maximální ideál, právě když faktorový okruh M/A je komutativní těleso.

Poznámka

Víme, že komutativní okruh je tělesem, právě když nemá žádné vlastní ideály, viz Věta 1.12. Uvědomíme-li si ještě, že ve faktorovém okruhu M/A třída A hraje roli nulového prvku, můžeme očekávat, že ideál A je prvoideál, právě když faktorový okruh M/A je obor integrity, a že A je maximální ideál, právě když faktorový okruh M/A je těleso.

Věta 1.17. Každý maximální ideál komutativního okruhu M je prvoideál.

Definice 1.30. Nechť $(M, +, \cdot)$ je okruh, R relace v množině M; pak R se nazývá **kongurence v okruhu** M, právě když je ekvivalencí v M a platí pro ní

$$(\forall x_1, x_2, y_1, y_2 \in M)(x_1 R x_2 \wedge y_1 R y_2) \Rightarrow [(x_1 + y_1) R (x_2 + y_2) \wedge x_1 y_1 R y_1 y_2].$$

Je-li R kongruence v okruhu M, označme M/R (disjunktní) rozklad množiny M indukovaný ekvivalencí R a dále pro libovolné $x \in M$ označme T_x, příslušnou třídu rozkladu M podle R tj. $T_x = \{y \in M; yRx\}$. Definujeme-li ještě

$$(\forall\ T_x, T_y \in M/R)\ T_x + T_y = T_{x+y}$$

a

$$(\forall\ T_x, T_y \in M/R)\ T_x.T_y = T_{xy},$$

lze ukázat, že tyto podmínky definují skutečně operace v M/R a že struktura $(M/R, +, \cdot)$ je okruh, který nazveme **faktorový okruh okruhu M podle kongruence R**.

Příklad 1.14. V oboru integrity $\mathbb{Z}[x]$ zaveďme relaci R tímto způsobem:

$$(\forall f(x), g(x) \in \mathbb{Z}[x])\ f(x)Rg(x) \Leftrightarrow f(0) = g(0),$$

takže polynom $f(x)$ je v relaci R s polynomem $g(x)$, právě když $f(x)$ a $g(x)$ mají týž absolutní člen. Je zřejmé, že relace R je ekvivalence na $\mathbb{Z}[x]$.
Dále, nechť $f_1(x), f_2(x), g_1(x)$ a $g_2(x)$ jsou libovolné polynomy ze $\mathbb{Z}[x]$ takové, že $f_1(x)\ Rf_2(x)$ a $g_1(x)\ Rg_2(x)$. Pak
$[f_1(0) = f_2(0) \wedge g_1(0) = g_2(0)] \Rightarrow f_1(0)+g_1(0) = f_2(0)+g_2(0) \wedge f_1(0).g_1(0) = f_2(0).g_2(0) \Rightarrow$
$\Rightarrow f_1(x) + g_1(x) R f_2(x) + g_2(x) \wedge f_1(x).g_1(x) R f_2(x).g_2(x)$
Prvky faktorového okruhu $\mathbb{Z}[x]/R$ jsou tedy rozkladové třídy tvaru (pro libovolné $f(x) \in \mathbb{Z}[x]$)

$$T_{f(x)} = \{g(x) \in \mathbb{Z}[x];\ f(x)Rg(x)\} = \{g(x) \in \mathbb{Z}[x]; f(0) = g(0)\}$$

například

$$T_{3x+5} = \{g(x) \in \mathbb{Z}[x];\ g(0) = 5\} = \{a_n x^n + ... + a_1 x + 5; a_n, ..., a_1 \in \mathbb{Z}\}.$$

[1]

Věta 1.18. V libovolném okruhu M lze vzájemně jednoznačně přiřadit ideály v M a kongruence na M tak, že faktorové okruhy podle ideálu a podle kongruence, které si v tomto přiřazení odpovídají, jsou si rovny.

Kapitola 2

Dělitelnost v oboru integrity

Definice 2.1. Nechť $(I, +, \cdot)$ je obor integrity a, b jsou prvky z I. Řekneme, že prvek a **dělí** prvek b (v oboru integrity I), právě když existuje prvek x z I tak, že $b = ax$. Píšeme $a|b$.

Věta 2.1. Nechť I je libovolný obor integrity. Pak platí:

1. $(\forall a \in I)\ a|a$
2. $(\forall a \in I)\ 1/a$
3. $(\forall a, b, c \in I)\ a|b \wedge b|c \Rightarrow a|c$
4. $(\forall a \in I)\ a|0 \wedge (0|a \Leftrightarrow a = 0)$
5. $(\exists a, b \in)\ a|b \wedge b \nmid a$
6. $(\forall a, b, c \in I)\ a|b \Rightarrow a|bc$
7. $(\forall a, b, c \in I)\ ab|c \Rightarrow (a|c \wedge b|c)$
8. $(\forall a, b, c \in I)\ a|b \wedge a|c \Rightarrow a|(bx + cy), x, y \in I$
9. $(\forall a, b_1, b_2, ..., b_n \in I)\ a \mid b_1 \wedge\ a \mid b_2\ \cdots \wedge a \mid b_n \Rightarrow a \mid \sum_{i=1}^{n} b_i x_i, x_1, ..., x_n \in I$
10. $(\forall a, b, c \in I)\ c \neq 0 \Rightarrow (a|b \Leftrightarrow ac|bc)$.

Poznámka:

1. Na množině I tedy máme definovanou binární relaci „dělí“. Z výše uvedené věty je

zřejmé, že tato relace je reflexivní a tranzitivní, která není symetrická.

2. Pokud je daný obor integrity I tělesem, plyne z vlastností tělesa a z tvrzení (4) předchozí věty, že formule $a|b$ platí pro všechna a a nenulová b z tělesa I. Proto se budeme spíše zabývat obory integrity, které nejsou tělesa.

2.1 Jednotky v oboru integrity

Definice 2.2. Nechť I je obor integrity. Prvek $j \in I$ se nazýva **jednotka** (ve smyslu dělitelnosti) v oboru inegrity I, právě když v oboru integrity I existuje k prvku j prvek inverzní j^{-1}.

Poznámka

- Jinak řečeno, j je jednotkou v I, právě když existuje $x \in I$ tak, že $jx = 1$, tj. $j/1$.
- Je-li j jednotka v I, pak zřejmě $1|j$.
- V každém oboru integrity existují vždy alespoň dvě jednotky. Jednotkový prvek 1 a prvek k němu opačný -1.

Věta 2.2. Nechť I je obor integrity. Pak platí:

(1) Jestliže j je jednotka v oboru integrity I, pak $j|a$ pro každé $a \in I$.

(2) Nechť $J(I)$ je množina všech jednotek v oboru integrity I. Pak $(J(I), \cdot)$ je podgrupa v multiplikativní pologrupě $(I, \cdot)$ oboru integrity I.

(3) Nechť $a_1, a_2, ..., a_n \in I$, $j = a_1 a_2 \cdots a_n$. Potom prvek j je jednotka v oboru integrity I, právě když pro každé $i = 1, 2, ..., n$ je a_i jednotka v I.

Důkaz.

(1) Nechť j jednotka v oboru integrity I. Pak existuje prvek $j^{-1} \in I$ tak, že $jj^{-1} = 1$. Pro libovolný prvek a tedy platí $a = 1 \cdot a = j(j^{-1}a)$ a $j|a$.

(2) $J(I) \subseteq I, J(I) \neq \emptyset$ $(1 \in J(I))$.

Nechť $j_1, j_2 \in J(I)$ jsou libovolné prvky. Pak existují $x, y \in I$ tak, že $j_1 x = 1$ a $j_2 y = 1$, tedy $(j_1 x)(j_2 y) = 1$. Protože $(I, \cdot)$ je komutativní, máme $(j_1 \cdot j_2)(xy) = 1$ a $j_1 j_2 \in J(I)$.

Operace „$\cdot$“ je zřejmě asociativní.

$1 \in J(I)$ je neutrální prvek struktury $(J(I), \cdot)$.

Nechť $j \in J(I)$ je libovolný prvek. Pak existuje $j^{-1} \in I$ tak, že $j \cdot j^{-1} = 1$, a tedy také $j^{-1} \in J(I)$.

(3) Nechť $j = a_1 \cdots a_n, a_1, ..., a_n \in I$.

„$\Rightarrow$“ Nechť $j = a_1 \cdots a_n \in J(I)$. Pak $j|1$, tedy $a_1 \cdots a_n|1$ a podle Věty 2.1 tvrzení 7 také $a_1|1 \wedge \cdots \wedge a_n|1$ a $a_1, ..., a_n \in J(I)$.

„$\Leftarrow$“ Jsou-li $a_1, ..., a_n \in J(I)$, pak podle tvrzení (2) je také $a_1 \cdots a_n \in J(I)$.

□

Příklad 2.1. Ve struktuře $(\mathbb{Z}, +, \cdot)$ existují právě dvě jednotky; jsou jimi čísla 1 a -1: Protože $1 \cdot 1 = 1$ a $(-1) \cdot (-1) = 1$, jsou obě čísla $1, -1$ jednotky. Ukážeme, že jiné jednotky $(\mathbb{Z}, +, \cdot)$ neexistují.

Nechť nějaké $a \in \mathbb{Z}$ je jednotka, pak musí existovat $b \in \mathbb{Z}$ tak, že $ab = 1$. Potom však také $|ab| = |a| \cdot |b| = 1$, takže $|a| = 1$ (a také $|b|$=1), což znamená, že $a = 1$ nebo $a = -1$. Tedy $J(\mathbb{Z}) = \{1, -1\}$

[1]

Příklad 2.2. Uvažujme obor integrity $(\mathbb{Z}[i], +, \cdot)$. Jednotkami v $\mathbb{Z}[i]$ jsou prvky $1, -1, i - i$: Zřejmě všechny čtyři uvedené prvky jsou jednotky v $\mathbb{Z}[i]$. Skutečnost, že $\mathbb{Z}[i]$ neobsahuje jiné jednotky, ověříme obdobně jako v Příkladu 2.1. Nechť $g = a + bi$ je jednotka v $\mathbb{Z}[i]$, pak existuje $h = c + di \in \mathbb{Z}[i]$ tak, že $gh = 1$. Pak ale je též

$$|gh| = |g| \cdot |h| = \sqrt{a^2 + b^2} \cdot \sqrt{c^2 + d^2} = 1, \text{ neboli } (a^2 + b^2)(c^2 + d^2) = 1$$

což vzhledem k tomu, že $a, b, c, d \in \mathbb{Z}$, a tedy $a^2, b^2, c^2, d^2 \in \mathbb{N}$ dává pro a, b (a obdobně pro c, d) tyto možnosti:

$$(a = 1 \wedge b = 0) \Rightarrow g = 1$$

$$(a = -1 \wedge b = 0) \Rightarrow g = -1$$

$$(a = 0 \wedge b = 1) \Rightarrow g = i$$

$$(a = 0 \wedge b = -1) \Rightarrow g = -i$$

[1]

Příklad 2.3.

1. V oboru integrity polynomů jedné neurčité $\mathbb{Q}[x]$ nad tělesem racionálních čísel jsou jednotkami právě všechny polynomy nultého stupně, tj. všechna čísla $c \in \mathbb{Q}, c \neq 0$.
Každý polynom nultého stupně je zřejmě jednotkou. Zbývá ověřit že v $\mathbb{Q}[x]$ jiné jednotky nejsou. Buď tedy $f(x) \in \mathbb{Q}[x]$ a nechť existuje $g(x) \in \mathbb{Q}[x]$ tak, že $f(x)g(x) = 1$. Potom ale f i g jsou nenulové polynomy; nechť f má stupeň n, g stupeň m. Součin fg má stupeň $m+n$. Díky podmínce $f(x)g(x) = 1$ je $n+m = 0$. Poněvadž je však $n, m \geqq 0$, je $n = m = 0$. Tedy polynom $f(x)$ je stupeň nula. Poznamenejme ještě, že $\mathbb{Q}[x]$ je zřejmě příkladem oboru integrity, v němž existuje nekonečně mnoho jednotek. Tedy $J(\mathbb{Q}[x]) = \mathbb{Q}^*$.

2. V oboru integrity $\mathbb{Z}_3[x]$ polynomů jedné neurčité nad tělesem $\mathbb{Z}_3$ jsou jednotkami právě nenulové konstanty $\bar{1}, \bar{2} \in \mathbb{Z}_3$, a tedy $J(\mathbb{Z}_3[x]) = \{\bar{1}, \bar{2}\}$.

[1]

Příklad 2.4. V obor integrity $(M, +, \cdot)$, kde $M = \{a + bi\sqrt{5}; a \in \mathbb{Z} \wedge b \in \mathbb{Z}\}$ jsou jednotkami v M pouze prvky 1 a -1.
Skutečnost, že 1 a -1 jsou jednotky v M, je zřejmá. Nechť tedy prvek $a + bi\sqrt{5} \in M$ je jednotka. Pak existuje $c + di\sqrt{5} \in M$ tak, že $(a + bi\sqrt{5}) \cdot (c + di\sqrt{5}) = 1$, tedy
$|a + bi\sqrt{5}| \cdot |c + di\sqrt{5}| = 1$.
Přejdeme-li k absolutním hodnotám a umocníme-li celou rovnost, obdržíme

$$(a^2 + 5b^2)(c^2 + 5d^2) = 1. \tag{2.1}$$

Pokud je $b \neq 0$, je součin na levé straně větší než 1, takže musí být $b = d = 0$. Tedy rovnost (2.1) přejde v

$$a^2c^2 = 1, \quad a, c \in \mathbb{Z}, \tag{2.2}$$

odkud již ihned plyne $a = 1$ nebo $a = -1$. Tedy $J(M) = \{1, -1\}$.

[1]

Definice 2.3. Nechť I je obor integrity. Řekneme, že prvky $a, b \in I$ jsou v I **asociované**, právě když $a \mid b$ a současně $b \mid a$. Píšeme $a \mid\mid b$ (resp. $a \sim b$).

Poznámka

• Protože pro každou jednotku j v I platí: $1|j$ a $1|j$ tak $j \parallel 1$.

• Dělitel prvku $a \in I$ se nazývá **vlastní**, jestliže není asociovaný ani s 1 ani s a. V opačném případě se nazývá **nevlastní dělitel**.

• Je zřejmé, že relace "||" je ekvivalence na množině I, a tedy existuje roklad I na třídy navzájem asociovaných prvků.

Věta 2.3. Nechť I je obor integrity. Pak pro libovolné prvky $a, b \in I$ platí, že a, b jsou asociované v oboru I, právě když existuje jednotka $j \in I$ tak, že $b = aj$.

Důkaz.

„⇐“ Předpokládejme, že $b = a \cdot j, j$ je jednotka v I. Pak platí $a|b$. Protože také $bj^{-1} = a$, platí i $b|a$, a tedy $a \parallel b$.

„⇒“ Nechť nyní $a \parallel b$. Pak $a|b$ a $b|a$ a můžeme psát $a = bu, b = av$, pro nějaká prvky $u, v \in I$. Tedy $a = bu = a \cdot v \cdot u$.

• je-li $a \neq 0, b \neq 0$, tak krácením dostáváme $uv = 1$, čili u, v jsou jednotky v I.

• Případ $a = 0, b = 0$ je triviální.

□

Poznámka

Množina všech jednotek $J(I)$ oboru inegrity I je podgrupa v grupě $(I, \cdot)$, a tedy lze zavést rozklad množiny I podle grupy $J(I)$, tj. rozklad

$$I/J(I) = \{aJ(I)\}_{a \in I}.$$

V množině I je tímto rozkladem indukovaná ekvivalence, která je podle Věty 2.3 zřejmě relací „$\parallel$“.

Tedy pro libovolné prvky $a, b \in I$ platí $a \parallel b \Leftrightarrow a \in bJ(I)$,

neboli $bJ(I) = \{a \in I; a = bj, j \in J(I)\}$.

Příklad 2.5.

• V oboru $\mathbb{Z}$ jsou jednotky pouze prvky ± 1. Tedy $a \parallel b$ právě tehdy, když $a = \pm b$.

• V oboru $\mathbb{Z}[i]$ jsou jednotky pouze prvky $\pm 1, \pm i$. Tedy $a \parallel b$ právě tehdy, když $a = \pm b$

nebo $a = \pm ib$.

• V oboru $\mathbb{R}[x]$ jsou jednotky právě polynomy stupně 0, jejichž člen je jednotkou v $\mathbb{R}$. Tedy $f(x) \parallel g(x)$ v $\mathbb{R}[x]$, právě tehdy, když existuje $c \in \mathbb{R}, c \neq 0$, tak, že $f(x) = cg(x)$.

[2]

Příklad 2.6. Je-li T komutativní těleso, pak ke každému nenulovému prvku $a \in T$ existuje prvek inverzní a^{-1}, takže podle Definice 2.2 jsou všechny nenulové prvky tělesa T jednotky. Protože pro každé dva nenulové prvky $a, b \in T$ platí $a = bb^{-1}a$, kde $b^{-1}a \neq 0$, je jednotka v T, jsou podle Věty 2.3 každé dva nenulové prvky z T asociované.

[1]

Příklad 2.7. Pozor na následující záludnost.

• $3x + 6 \parallel x + 2$ v oboru $\mathbb{Q}[x]$, protože $3x + 6 = 3 \cdot (x + 2)$ a $x + 2 = \frac{1}{3}(3x + 6)$;

• $3x + 6 \nparallel x + 2$ v oboru $\mathbb{Z}[x]$, protože $\frac{1}{3} \notin \mathbb{Z}$.

[2]

Příklad 2.8.

• V $(\mathbb{Z}, +, \cdot)$ existují, právě dvě jednotky, 1 a -1, takže $J(\mathbb{Z}) = \{1, -1\}$. Tedy rozklad $\mathbb{Z}$ na třídy asociovaných prvků obsahuje vedle třídy $\{0\}$ vesměs dvouprvkové množiny tvaru $\{a, -a\}, a \in \mathbb{Z}$.

• V $\mathbb{Z}[i]$ existují právě čtyři jednotky $1, -1, i, -i$, takže $J(\mathbb{Z}[i]) = \{1, -1, i, -i\}$. Tedy rozklad $\mathbb{Z}[i]$ na třídy asociovaných prvků obsahuje vedle třídy $\{0\}$ vesměs čtyřprvkové množiny tvaru $\{a + bi, -a - bi, ai - b, -ai + b\}$.

[1]

Věta 2.4. Nechť I je obor integrity. Pak pro libovolné prvky a_1, a_2, b_1, $b_2 \in$ I platí:
$(a_1 \parallel a_2 \wedge b_1 \parallel b_2) \Rightarrow (a_1 \mid b_1 \Leftrightarrow a_2 \mid b_2)$.

Důkaz.

• Nechť $a_1, a_2, b_1, b_2 \in I$ a nechť $a_1 \parallel a_2$ a $b_1 \parallel b_2$. Nechť $a_1 \mid b_1$. Pak podle Definice 2.3 je $a_2 \mid a_1$ a $b_1 \mid b_2$. Podle Věty 2.1 tvrzení 3 dostáváme z $(a_2 \mid a_1 \wedge a_1 \mid b_1 \wedge b_1 \mid b_2)$ hledaný výsledek $a_2 \mid b_2$.

• Nechť nyní $a_2 \mid b_2$. Z předpokladu dále plyne, že $a_1 \mid a_2$ a $b_2 \mid b_1$, tedy máme $a_1 \mid a_2, a_2 \mid b_2$ a $b_2 \mid b_1$ a opět podle Věty 2.1 tvrzení 3 dostáváme, že $a_1 \mid b_1$. □

Poznámka

Právě dokázaná věta vlastně říká, že pravdivost či nepravdivost výroku $a_1 \mid b_1$ se nezmění, nahradíme-li prvek a_1 nebo b_1 libovolným prvkem s ním asociovaným. Proto — jak uvidíme dále i každá vlastnost prvků z I, kterou lze popsat pouze pomocí relace „|“ , se přenáší i na prvky s nimi asociované.

Příklad 2.9. Ukažte, že relace „dělí“ definovaná na množině $I/J(I)$ tříd asociovaných prvků v I tímto způsobem:

$$(\forall aJ(I), bJ(I)) \in I/J(I))\ aJ(I) \mid bJ(I) \Leftrightarrow a \mid b$$

je neostré uspořádání v množině $I|J(I)$.

(1) •$(\forall aJ \in I/J(I))\ aJ \mid aJ \Leftrightarrow a \mid a$, což platí pro $\forall a \in I$, podle Věty 2.1 tvrzení 1, a tedy relace je reflexivní.

•$(\forall aJ, bJ \in I/J(I))\ aJ \mid bJ \wedge bJ \mid aJ \Rightarrow a \mid b \wedge b \mid a \Rightarrow a \parallel b \Rightarrow aJ = bJ$, relace je antisymetrická.

•$(\forall aJ, bJ, cJ \in I/J(I))\ aJ \mid bJ \wedge bJ \mid cJ \Rightarrow a \mid b \wedge b \mid c \Rightarrow a \mid c \Rightarrow aJ \mid cJ$, podle Věty 2.1 tvrzení 3, relace je tedy tranzitivní.

Daná relace je opravdu neostré uspořádání.

(2) • Dále $(\forall a \in I)1/a$, tak $1J/aJ$ podle Věty 2.1 tvrzení 2 pro $\forall aJ \in I/J(I)$, tedy $1J = J$ je první prvek uspořádané množiny $(I/J(I), |)$

• Protože $(\forall a \in I)a|0$, tak $aJ/0J$ pro $\forall aJ \in I/J(I)$, tedy $0J(I) = \{0\}$ je podle Věty 2.1 tvrzení 4 poslední prvek uspořádané množiny $(I/J(I), |)$.

2.2 Největší společný dělitel

Definice 2.4. Nechť a_1, a_2, ... , a_k jsou libovolné prvky z oboru integrity I. Prvek $d \in I$ se nazývá **největší společný dělitel** prvků a_1, a_2, ... , a_k v I, právě když současně platí:

$$d \mid a_1 \wedge d \mid a_2 \wedge \cdots \wedge d \mid a_k \tag{2.3}$$

$$(\forall d_1 \in I)\ [(d_1 \mid a_1 \wedge d_1 \mid a_2 \wedge \cdots \wedge d_1 \mid a_k) \Rightarrow d_1 \mid d]. \tag{2.4}$$

Píšeme $d = D\ (a_1, a_2, \dots\ , a_k)$.

Příklad 2.10. Nechť $I = \mathbb{Z}$; hledejme $D(8, 52)$.
Společnými děliteli čísel 8 a 52 jsou prvky 1, -1, 2, -2, 4, -4; největšími společnými děliteli jsou pak prvky 4 a -4 (nikoliv jen prvek 4).

Z tohoto příkladu plyne, že největší společný dělitel ve smyslu definice nemusí být vždy největším prvkem mezi všemi společnými děliteli vzhledem k uspořádání v uvažované struktuře. Adjektivum „největší“ přežívá z doby, kdy se dělitelnost studovala pouze na množině kladných celých čísel. Dále z příkladu plyne, že největším společným dělitelem daných prvků z I nemusí být pouze jediný prvek z I.

Věta 2.5. Nechť pro prvky $a_1,\ a_2, ...,\ a_k$ z oboru integrity I existuje $D(a_1,\ a_2, ...,\ a_k) = d$. Pak platí $(\forall\ d' \in I)\ d' = D(a_1, a_2, ..., a_k) \Leftrightarrow d \parallel d'$.

Důkaz.

„$\Rightarrow$“ Nechť tedy $d = D(a_1, ..., a_k)$. Předpokládejme nejprve, že též $d' = D(a_1, ..., a_k)$. Potom (podle (2.3) aplikované na d') $d' \mid a_i$ pro všechna $i = 1, 2, ..., k$ a (podle (2.4) vztažené k d) $d' \mid d$. Obdobně ověříme $d \mid d'$, takže $d \parallel d'$.
„$\Leftarrow$“ Nechť $d' \in I$ je takový prvek, že $d' \parallel d$, tj. $d'|d$ a $d|d'$.
• Protože $d'|d$ a $d = D(a_1, ..., a_k)$, tak $d'|d$ a $d|a_i, i = 1, ..., k$, tedy podle Věty 2.1 tvrzení 3 $d'|a_i, i = 1, ..., k$, tj. d' je společný dělitel prvků $a_1, ..., a_k$.
Nechť $d_1 \in I$ je libovolný prvek takový, že $d_1|a_i, i = 1, ..., k$. Pak $d_1 \mid d$ $(d = D(a_1, ..., a_k))$, ale zároveň podle předpokladu $d \mid d'$, tedy opět podle Věty 2.1 tvrzení 3 pak $d_1 \mid d'$.
Podle Definice 2.4 je tedy $d' = D(a_1, ..., a_k)$. □

Poznámka

Z Věty 2.5 tedy plyne, že největší společný dělitel není danými prvky $a_1, ..., a_k \in I$ (pokud vůbec existuje) určen jednoznačně, nýbrž jednoznačně je určena pouze třída asociovaných prvků, v nichž všichni společní dělitelé uvedených prvků leží.

Dohoda:

Pro zjednodušení vyjadřování se dohodneme na tom, že v dalsím nebudeme (pokud nebude řečeno jinak) mezi navzájem asociovanými největšími děliteli rozlišovat a budeme psát $d = d_1$ místo přesnějšího $d \parallel d_1$.

Věta 2.6. Nechť a, b, c jsou libovolné prvky z oboru integrity I, pak platí:
a) existuje-li $D(a, b)$, existuje též $D(b, a)$ a je $D(a, b) = D(b, a)$;
b) existuje-li $D(a, b) = d$ a $D(d, c)$ (anebo $D(b, c) = y$ a $D(a, y)$), existuje též $D(a, b, c)$, přičemž

$$D(D(a, b), c) = D(a, D(b, c)) = D(a, b, c)$$

Důkaz.

a) Tvrzení plyne ihned z Definice 2.4.
b) Předpokládejme, že existují $d = D(a, b)$ a $d' = D(d, c)$. Pak $d/a \wedge d/b \wedge d'/d \wedge d'/c$. Podle Věty 2.1 tvrzení 3 pak $d'/a \wedge d'/b \wedge d'/c$, tedy d' je společný dělitel prvků a, b, c. Nechť $d_1 \in I$ je libovolný prvek takový, že $d_1/a \wedge d_1/b \wedge d_1/c$. Pak ovšem $d_1/d \wedge d_1/c$, což ovšem podle (2.4) znamená, že d_1/d'. Tedy $d' = D(a, b, c)$. □

Věta 2.7. Nechť existuje největší společný dělitel k libovolným dvěma prvkům oboru integrity I; pak existuje největší společný dělitel ke každé n-tici $a_1, a_2, ..., a_n$ prvků z I.

Důkaz. Budeme postupovat úplnou indukcí podle n.
Pro $n = 2$ existuje $D = (a_1, a_2)$ podle předpokladu.
Nechť $n > 2$ a předpokládejme, že existuje největší společný dělitel pro každou skupinu $n - 1$ prvků z I. Jsou-li $(a_1, a_2, ..., a_{n-1}, a_n)$ libovolné prvky z I, pak podle indukčního předpokladu existuje prvek $d' = D(a_1, ..., a_{n-1})$ a podle předpokladu Věty existuje prvek $d \in I$ tak, že $d = D(d', a_n)$.
Ukažme, že $d = D(a_1, ..., a_n)$.

Protože $d = D(d', a_n)$, je $d/d' \wedge d/a_n$. Zároveň ovšem $d'/a_1 \wedge \cdots \wedge d'/a_{n-1}$ (podle indukčního předpokladu), což znamená, že podle Věty 2.1 tvrzení 3 je $d/a_1 \wedge d/a_2 \wedge \cdots \wedge d/a_{n-1} \wedge d/a_n$, tj. d je společný dělitel prvků $a_1, a_2, ..., a_{n-1}, a_n$. Nechť d_1 je libovolný prvek z I takový, že $d_1/a_1 \wedge \cdots \wedge d_1/a_{n-1} \wedge d_1/a_n$. Pak podle (2.4) $d_1/d' \wedge d_1/a_n$, tedy d_1/d. Opravdu tedy $d = D(a_1, ..., a_n)$. □

Důsledek

Jestliže ke každým dvěma prvkům oboru integrity I existuje největší společný dělitel, pak $D(a_1, a_2, ..., a_n) = D((a_1, a_2, ..., a_{n-1}), a_n)$ pro každou n-tici prvků $a_1, a_2, ..., a_n \in I$.

Poznámka

Použijeme-li navíc „komutativnost“ a „asociativnost“ operace tvoření největšího společného dělitele, vidíme, že výsledek nezáleží ani na pořadí, v němž tuto operaci provádíme, ani na pořadí prvků $a_1, a_2, ..., a_n$, takže například
$D(a_1, a_2, a_3, a_4) = D(a_1, D(D(a_2, a_3), a_4)) = D(a_3 D(a_1, D(a_4, a_2)))$.

Definice 2.5. Nechť I je obor integrity prvky $a, b \in I$ se nazývají **prvky nesoudělné**, právě když $D(a, b) = 1$.

Prvky $a_1,\ a_2, ...,\ a_n \in I$ nazveme **nesoudělné**, právě když $D(a_1,\ a_2, ...,\ a_n) = 1$,
a nazveme je **po dvou nesoudělné**, právě když pro každé dva různé indexy $i, j \in \{1, 2, ..., n\}$ je $D(a_i, a_j) = 1$.

Poznámka

• Skutečně: Pro libovolný prvek $a \in I$ je $D(a, 0) = a$. Speciálně tedy je $D(0, 0) = 0$. Skutečně $a \mid a$ a $a \mid 0$ podle Věty 2.1 tvrzení 10, a kdykoliv $t \mid a$ a $t \mid 0$, pak $t \mid a$, což jsme potřebovali ověřit.

• Analogicky ukázat, že pro libovolné $a, b \in I$ platí: $a \mid b \Leftrightarrow D(a, b) = a$.

Věta 2.8. Nechť v oboru integrity I existuje největší společný dělitel k libovolným dvěma prvkům. Nechť $a_1,\ a_2, ...,\ a_k, c \in I$. Pak platí

$$D\ (ca_1,\ ca_2, ...,\ ca_k) = D\ c(a_1, a_2, ..., a_k)$$

Důkaz. Pro $c = 0$ zřejmě tvrzení platí.

Nechť dále je $c \neq 0$. Označme $x = D(a_1, ..., a_n), y = D(ca_1, ..., ca_n)$. Dokážeme, že $y \parallel cx$.

Poněvadž $x|a_i$ pro všechna $i = 1, 2, ..., n$, platí zřejmě $cx|ca_i$ (Věta 2.1 tvrzení 10), a tedy také $cx|y$. Zbývá dokázat, že $y|cx$. Jistě $c|ca_i$ pro všechna $a_i (i = 1, ..., n)$; potom z definice y plyne $c|y$. To ale znamená, že existuje prvek $b \in I$ tak, že $cb = y$. Dosazením do $y|ca_i$ dostáváme $cb|ca_i$, odkud plyne $b|a_i$ pro všechna a_i takže $b|x$. Potom však $cb|cx$, neboli $y|cx$, což jsme měli dokázat. □

Věta 2.9. Nechť v oboru integrity I existuje $D(a_1, a_2, ..., a_k) = d,\ d \neq 0$. Pak

$$D(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_k}{d}) = 1.$$

Důkaz. Nechť $d = D(a_1, a_2, ..., a_k)$. Pak $d|a_1, d|a_2, ..., d|a_k$, tj. existují prvky $b_1, b_2, ..., b_k \in I$ tak, že $a_1 = db_1, a_2 = db_2, ..., a_k = db_k$.
Tedy $d = D(a_1, a_2, ..., a_k) = D(db_1, db_2, ..., db_k) = dD(b_1, b_2, ..., b_k), d \neq 0$ (viz Věta 2.8), a proto je $1 = D(b_1, b_2, ..., b_k) = D(\frac{a_1}{d}, \frac{a_2}{d}, \cdots, \frac{a_k}{d})$. □

Věta 2.10. Nechť $a, b, c \in I$ a nechť v oboru integrity I existuje největší společný dělitel $D(a, b) = d$. Pak platí:

1. $(a \mid c \wedge b \mid c) \Rightarrow ab \mid cd$.

2. Je-li $d = 1$, pak platí: $a \mid c \wedge b \mid c \Rightarrow ab \mid c$.

Důkaz. Nechť $a, b, c \in I$ jsou takové prvky, že $D(a, b) = d$ a $a|c$ a $b|c$. Pak zřejmě

$$D(a, c) = a, D(b, c) = b.$$

Místo $ab|cd$ budeme dokazovat (ekvivalentní tvrzení), že $D(ab, cd) = ab$. Užitím Věty 2.8 a Věty 2.6 a vztahu popsaném výše postupně obdržíme
$D(ab, cd) = D(ab, cD(a, b)) = D(ab, D(ac, bc)) = D(D(ab, ac), bc) = D(aD(b, c), bc) =$
$= D(ab, bc) = b \cdot D(a, c) = ab.$ □

Věta 2.11. Nechť $a, b, c \in I$ a nechť v I existuje největší společný dělitel k libovolným dvěma prvkům. Jestliže $D(a, b) = D(a, c) = 1$, pak $D(a, bc) = 1$.

Důkaz. Je $a = D(a, ac)$ a podle Věty 2.9 je $D(ac, bc) = c$. Pak ale podle Věty 2.6 máme $D(a, bc) = D(D(a, ac)bc) = D(a, D(ac, bc)) = D(a, c \cdot D(a, b)) = D(a, c) = 1.$ □

Věta 2.12. Nechť a, b, c jsou prvky oboru integrity I existuje k libovolným dvěma prvkům největšího společného dělitele. Jestliže $a \mid bc$ a $D(a, b) = 1$, pak $a \mid c$.

Důkaz. Je $a = D(a, bc)$ a $a = D(a, ac)$. Kromě toho podle Věty 2.8 je
$c = c \cdot D(a, b) = D(ac, bc)$, takže podle důsledku Věty 2.6 konečně máme
$a = D(a, bc) = D(D(a, ac), bc) = D(a, D(ac, bc)) = D(a, c \cdot D(a, b)) = D(a, c)$,
a tedy $a \mid c$. □

2.3 Nejmenší společný násobek

Definice 2.6. Nechť $a_1,\ a_2, ...,\ a_k$ jsou libovolné prvky z oboru integrity I. Prvek $n \in I$ se nazývá **nejmenší společný násobek** prvků $a_1, a_2, ..., a_k$ v I, právě když současně platí:
• $a_1 \mid n \wedge a_2 \mid n \wedge \cdots \wedge a_k \mid n$
• pro libovolný prvek $n_1 \in I$ platí: jestliže $a_1 \mid n_1 \wedge a_2 \mid n_1 \wedge \cdots \wedge a_k \mid n_k$, pak $n \mid n_1$.
Píšeme $n = [a_1, a_2, ..., a_k]$.

Poznámka

• Prvek n je tedy nejmenším společným násobkem prvků $a_1, ..., a_k$, právě když n je společným násobkem všech a_i a když každý společný násobek n_1 těchto prvků je násobkem prvku n.
• Porovnáme-li právě vyslovenou definici nejmenšího společného násobku s definicí největšího společného dělitele, vidíme, že se od ní liší pouze záměnou pořadí prvků v relaci „dělí“, takže vlastně jednu definici obdržíme z druhé, nahradíme-li v ní relaci „dělí“ relací k ní inverzní. Protože relace „|“ není symetrická, jsou oba takto definované pojmy odlišné. Lze však nahlédnout, že z každého tvrzení pro největší společný dělitel dostaneme - přechodem k zmíněné inverzní relaci „duální“ - tvrzení pro nejmenší společný násobek.

Věta 2.13. Nechť pro prvky $a_1, a_2, ..., a_k$ z oboru integrity I existuje $[a_1, a_2, ..., a_k] = n$. Nechť $n_1 \in I$ je libovolný prvek. Pak platí:

$$n_1 = [a_1, a_2, ..., a_k] \Leftrightarrow n \parallel n_1.$$

Důkaz. Důkaz je analogický jako u Věty 2.5. □

Věta 2.14. Nechť v oboru integrity I existuje nejmenší společný násobek k libovolným dvěma prvkům. Pak existuje v oboru integrity I nejmenší společný násobek k libovolné konečné množině prvků z oboru integrity I.

Důkaz. Důkaz je analogický jako u Věty 2.7. □

Věta 2.15. Nechť v oboru integrity I existuje největší společný dělitel k libovolným dvěma prvkům. Pak v oboru integrity I existuje nejmenší společný násobek k libovolné konečné množině prvků z oboru integrity I.

Důkaz. Díky Větě 2.14 stačí ukázat, že pro libovolné dva prvky $a, b \in I$ existuje v I jejich nejmenší společný násobek $[a, b]$.

Nechť $a, b \in I$ jsou libovolné prvky.

(a) Je-li $a = 0$ nebo $b = 0$, pak je $[a, b] = 0$.

(b) Nechť je tedy $a \neq 0$ a $b \neq 0$. Podle předpokladu existuje $D(a, b) = d$ a protože $a \neq 0, b \neq 0$, je i $d \neq 0$.

Protože $d \mid a, d \mid b$, existují prvky $a_1, b_1 \in I$ tak, že

$$da_1 = a,\ db_1 = b.$$

Podle Věty 2.9 je $(a_1, b_1) = 1$.

Označme $n = da_1b_1$. Dokažeme, že $[a, b] = n$.

Protože $n = (da_1)b_1 = ab_1 = a_1(db_1) = a_1b$, je $a \mid n$ a $b \mid n$, tj. n je společný násobek prvků a, b.

Předpokládejme, že $n_1 \in I$ je libovolný prvek takový, že $a \mid n_1$ a $b \mid n_1$.

Pak také $d \mid n_1$ a existuje $n_2 \in I$ tak, že $n_1 = dn_2$.

Tedy máme $da_1 \mid dn_2$ a $db_1 \mid dn_2$ a $d \neq 0$ tj. $a_1 \mid n_2$ a $b_1 \mid n_2$.

Protože $(a_1, b_1) = 1$, dostáváme podle Věty 2.10 tvrzení 2., že $a_1b_1 \mid n_2$.

Potom však $da_1b_1 \mid dn_2$ neboli $n \mid n_1$.

To ovšem znamená, že $[a, b] = n$.

□

Věta 2.16. Nechť v oboru integrity I existuje největší společný dělitel k libovolným dvěma prvkům. Pak pro libovolné prvky $a, b \in I$ platí: $D(a, b) \cdot [a, b] = a \cdot b$. Speciálně je-li $D(a, b) = 1$, pak $[a, b] = a \cdot b$.

Důkaz. Důkaz plyne ihned z důkazu Věty 2.15.

Víme, že $n = da_1b_1 = [a, b]$ a $a = a_1d, b = b_1d$. Tedy $[a, b] = \frac{a_1db_1d}{d} = \frac{ab}{d}$, kde $d = D(a, b)$. Tedy $D(a, b) \cdot [a, b] = ab$

□

2.4 Eukleidovy obory integrity

V předchozí kapitole jsme zavedli definici největšího společného dělitele v oboru integrity I. Ovšem ne vždy k libovolným dvěma prvkům $a, b \in I$ existuje jejich největší společný dělitel .

Příklad 2.11. Uvažujme obor integrity $(M, +, \cdot) = (\{a + ib\sqrt{5}; a \in \mathbb{Z} \wedge b \in \mathbb{Z}\}, +, \cdot)$. Zvolme si nyní prvky $9, 3(2 + i\sqrt{5}) \in M$.

Děliteli prvku 9 jsou právě čísla $\pm1, \pm3, \pm(2 + i\sqrt{5}), \pm(2 - i\sqrt{5}), \pm9$; děliteli prvku $3(2 + i\sqrt{5})$ pak čísla $\pm1, \pm3, \pm(2 + i\sqrt{5}), \pm3(2 + i\sqrt{5})$. Společnými děliteli jsou prvky $\pm1, \pm3, \pm(2 + i\sqrt{5})$; žádný z nich však nevyhovuje druhé podmínce definice největšího společného dělitele v M proto největší společný dělitel prvků 9 a $3(2+i\sqrt{5})$ v M neexistuje.

[1]

Definice 2.7. Obor integrity I se nazývá **Eukleidův obor integrity**, právě když existuje zobrazení $\upsilon : I - \{0\} \Rightarrow \mathbb{N}$ - říkáme mu **Eukleidova norma** - takové, že pro libovolná $a, b \in I, b \neq 0$, platí současně

$$a \mid b \Rightarrow \upsilon(a) \leqq \upsilon(b,) \tag{2.5}$$

$$(\exists q, r \in I)[a = bq + r \wedge (r = 0 \vee \upsilon(r) < \upsilon(b))]. \tag{2.6}$$

Poznámka

Z uvedené Definice ihned plyne, že v Euklidově oboru integrity platí:

$(\forall a, b \in I, b \neq 0)a \mid b \wedge b \mid a \Rightarrow \upsilon(a) = \upsilon(b)$

Věta 2.17. Nechť I je Eukleidův obor integrity. Potom pro libovolné $a, b \in I, b \neq 0$, platí

$$a \mid b \Rightarrow (\upsilon(a) = \upsilon(b) \Rightarrow b \mid a).$$

Důkaz. Nechť tedy $a \mid b$ a současně $v(a) = v(b)$. Podle (2.6) existují $q, r \in I$ tak, že $a = bq + r$, kde buď $r = 0$ nebo $v(r) < v(b)$. V prvém případě $a = bq$, a tedy $b \mid a$, což jsme měli dokázat. Když $r \neq 0$, je $v(r) < v(b)$ a také $v(r) < v(a)$. Z předpokladu $a \mid b$ vyplývá existence takového prvku $a' \in I$, že $aa' = b$. Potom ale $a = bq + r = aa'q + r$; odtud $r = a(1 - a'q)$, a tedy $a \mid r$. To však podle (2.5) implikuje $v(a) \leqq v(r)$. Dostáváme se tak ke sporu s $v(r) < v(a)$. Tedy možnost $r \neq 0$ nemůže nastat, čímž je věta dokázána. □

Poznámka

Nyní se dá předchozí Věta a Poznámka za Definicí formulovat takto: v libovolném Eukleidově oboru integrity I platí:

$$(\forall a, b \in I)[(b \neq 0 \wedge a \mid b) \Rightarrow (v(a) = v(b) \Leftrightarrow a \mid\mid b)]. \tag{2.7}$$

Věta 2.18. Je-li I Euklidův obor integrity $u \in I, u \neq 0$ a $v(u) = 0$, pak u je jednotka.

Důkaz. Přímo z Definice 2.7, máme $1 = uq + i, q, i \in I, i = 0$ nebo $v(i) < v(u)$. Protože ale případ $v(i) < 0$ nemůže nastat, je $i = 0$, a tedy $1 = uq$. □

Věta 2.19. Buď I Eukleidův obor integrity. Pak k libovolným dvěma prvkům z I existuje největší společný dělitel.

Důkaz. Nechť $a, b \in I$. Jestliže $b = 0$, je $D(a, b) = a$. Předpokladejme dále, že $b \neq 0$. Z podmínky (2.6) definice Eukleidova oboru integrity plyne existence prvků $q_1, r_1 \in I$ takových, že $a = bq_1 + r_1$, kde $r_1 = 0$ nebo $v(r_1) < v(b)$. Jestliže $r_1 = 0$, je $b \mid a$, a tedy $D(a, b) = b$. Nechť tedy $r_1 \neq 0$; potom opět podle (2.6) aplikované nyní na prvky b a r_1 existují $q_2, r_2 \in I$ tak, že $b = r_1q_2 + r_2$, kde $r_2 = 0$ nebo $v(r_2) < v(r_1)$.
V případě, že $r_2 \neq 0$, dostáváme $r_1 = r_2q_3 + r_3$ a $r_3 = 0$ nebo $v(r_3) < v(r_2)$. V tomto postupu (pro $r_i \neq 0$) pokračujeme dále. Po jistém konečném počtu kroků nechť jich je $n + 1$ musíme dospět k výsledku

$$r_{n-1} = r_nq_{n+1} + r_{n+1}, \text{ kde } r_{n+1} = 0.$$

Vyplývá to ze skutečnosti, že

$$v(b) > v(r_1) > v(r_2) > \cdots \geqq 0.$$

Přepišme si ještě jednou celý postup za předpokladu, že $r_i \neq 0$, pro $i = 1, 2, ..., n$ a $r_{n+1} = 0$:

$$\begin{aligned}
a &= bq_1, + r_1 && \upsilon(r_1) < \upsilon(b) \\
b &= r_1 q_2 + r_2 && \upsilon(r_1) < \upsilon(r_2) \\
r_1 &= r_2 q_3 + r_3 && \upsilon(r_2) < \upsilon(r_3) \\
&\cdot && \cdot \\
&\cdot && \cdot \\
&\cdot && \cdot \\
r_{n-2} &= r_{n-1} \cdot q_n + r_n && \upsilon(r_n) < \upsilon(r_{n-1}) \\
r_{n-1} &= r_n q_{n+1} + r_{n+1} && r_{n+1} = 0
\end{aligned} \tag{2.8}$$

Nyní dokážeme, že $r_n = D(a, b)$. Z poslední rovnosti v 2.8 plyne, že $r_n \mid r_{n-1}$, z předposlední pak po dosazení za r_{n-1} je $r_{n-2} = r_n(q_{n+1}q_n+1)$, a tedy $r_n \mid r_{n-2}$. Analogicky postupujeme „směrem nahoru“ až k výsledkům $r_n \mid b$ a $r_n \mid a$. Tedy r_n je společným dělitelem prvků a, b. Zbývá ověřit, že je ze všech společných dělitelů největší. Nechť pro libovolné $x \in I$ platí $x \mid a$ a zároveň $x \mid b$. Ukažeme, že $x \mid r_n$. Nyní budeme postupovat „směrem dolů“. Z první rovnice je $r_1 = a - q_1 b$, a tedy podle Věty 2.1 tvrzení 8 $x \mid r_1$, z druhé získáme $x \mid r_2$ atd. až dojdeme ke vztahu $x \mid r_n$, což jsme měli dokázat. □

Poznámka

Postup popsaný formulemi (2.8) nazýváme Eukleidův algoritmus.

Věta 2.20. (Bezoutova rovnost)
Nechť I je Eukleidův obor integrity, $a, b \in I$. Pak existují prvky $c_1, c_2 \in I$ tak, že $D(a, b) = c_1 a + c_2 b$.

Důkaz. Nechť jsou splněny předpoklady Věty. Jestliže je $b = 0$, je $D(a, b) = a$ a stačí volit $c_1 = 1$, c_2 libovolně. Nechť dále $b \neq 0$. Potom díky Eukleidovu algoritmu je $r_1 = a+(-q_1)b$ (v případě, že $r_1 = 0$, je důkaz triviální). Dosazením za r_1 do druhé rovnice v (2.8) dostáváme $r_2 = (-q_2)a + (1 + q_1 q_2)b$. Dále vyjádříme prvek r_3 a po dosazení r_1, r_2 vidíme,

že i r_3 je lineární kombinací prvků a, b. Takto postupujeme „směrem dolů“ až k poslední rovnici k vyjádření $r_n = D(a, b)$ ve formě lineární kombinace prvků a, b.

□

Triviálním důsledkem předchozí věty je.

Věta 2.21. Nechť I je Eukleidův obor integrity, $a, b \in I$. Jestliže a, b jsou nesoudělné prvky, existují $c_1, c_2 \in I$ tak, že $ac_1 + bc_2 = 1$.

Zaměříme se na konkrétní Eukleidovy obory integrity.

Věta 2.22. $(\mathbb{Z}, +, \cdot)$ je Eukleidův obor integrity.

Důkaz. Definujme normu v takto: pro každé $a \in \mathbb{Z}$, $a \neq 0$, nechť $\upsilon(a) = |a|$. Nejprve ověříme, že pro každé $b \neq 0$, když $a \mid b$, je $\upsilon(a) \leqq \upsilon(b)$. Nechť tedy $a \mid b$; potom existuje $x \in \mathbb{Z}$ tak, že $ax = b$.
Je $|b| = |ax| = |a| \cdot |x|$. Jestliže $|x| = 1$, je $|a| = |b|$, takže $\upsilon(a) = \upsilon(b)$. V případě, že $x \neq 1$, je $|x| > 1$, což znamená, že $|a| < |b|$, a tedy $\upsilon(a) < \upsilon(b)$.
Dále ověříme podmínku (1.1) z Definice 2.7. Ta plyne z následující Věty.
$(\forall a, b \in \mathbb{Z})(\exists! q, n \in \mathbb{Z}); b \neq 0, a = bq + n \wedge 0 \leq n < |b|$. □

Věta 2.23. (Věta o dělení se zbytkem)
Nechť a, b jsou libovolná celá čísla, $b \neq 0$. Pak existují jednoznačně určená celá čísla q a r taková, že jsou splněny následující dvě podmínky:

1. Platí rovnost $a = q \cdot b + r$.
2. Číslo r splňuje nerovnost $0 \leq r < |b|$.

Důkaz.

1. Nejprve dokážeme existenci čísel q a r. Protože platí $(-q) \cdot (-b) = q \cdot b$, můžeme bez újmy na obecnosti předpokládat, že $b > 0$. Budeme rozlišovat dva případy:

(a) Číslo a je větší nebo rovno 0. Budeme postupovat indukcí podle a.

• Je-li $a = 0$, je tvrzení triviální, protože můžeme zvolit $q = r = 0$.

• Předpokládejme, že pro $a \geq 0$ existují celá čísla q, r taková, že $a = bq + r$ a $0 \leq r < |b| = b$.

Potom $a+1 = bq + (r+1)$, kde $r+1 \leq b$. Je-li $r+1 < b$, jsme hotovi. Je-li $r+1 = b$, pak $a+1 = bq + b = (q+1) \cdot b + 0$.

(b) Číslo a je menší než 0. Podle předchozího existují celá čísla q', r' taková, že $-a = q' \cdot b + r'$ a $0 \leq r' < b$. Opět odlišíme dva případy.

• Jestliže $r' = 0$, položme $q = -q'$ a $r = 0$. (Platí totiž $a = (-q') \cdot b + 0$.)

• Jestliže $r' > 0$, položme $q = -q' - 1$ a $r = b - r'$. Platí totiž $a = (-q' - 1) \cdot b + (b - r')$ a $0 < (b - r') < b$.

2. Zbývá ukázat, že číslo q a r jsou určena čísly a a b jednoznačně. Předpokládejme, že jsme vyjádřili číslo a dvěma způsoby, tj. předpokládejme, že existují celá čísla q_1, q_2, r_1 a r_2 taková, že platí

$a = q_1 \cdot b + r_1 \qquad 0 \leq r_1 < b$

$a = q_2 \cdot b + r_2 \qquad 0 \leq r_2 < b.$

Potom platí $q_1 \cdot b + r_1 = q_2 \cdot b + r_2$ a tudíž $(q_1 - q_2) \cdot b = r_1 - r_2$. Protože platí $0 \leq r_1 < b$ a $0 \leq r_2 < b$, je $|r_2 - r_1| < b$. Tudíž je $|(q_1 - q_2) \cdot b| < b$, tedy $q_1 = q_2$. Z toho plyne, že $r_1 = r_2$.

□

Příklad 2.12.

Nalezněte největší společný dělitel, koeficienty c1; c2 v Bezoutově rovnosti a nejmenší společný násobek čísel $a = 210, b = 330$.

(1)Použijeme Eukleidův algoritmus:

$$330 = 210 \cdot 1 + 120,$$
$$210 = 120 \cdot 1 + 90,$$
$$120 = 90 \cdot 1 + 30,$$
$$90 = 30 \cdot 3.$$

Tedy $D(210, 330) = 30$.

(2) Označme dále $a = 330, b = 210, x = D(210, 330)$. Budeme hledat celá čísla c_1, c_2

tak, aby $x = c_1 a + c_2 b$. Použijeme postupné úpravy „směrem dolů“ a dostáváme:

$$\begin{aligned} a &= b \cdot 1 + 120 && \Rightarrow 120 = a - b \\ b &= (a-b) \cdot 1 + 90 && \Rightarrow 90 = -a + 2b \\ a - b &= (-a + 2b) \cdot 1 + 30 && \Rightarrow 30 = 2a - 3b \\ x = 30 &= 2a - 3b \end{aligned}$$

Stačí tedy položit $c_1 = 2, c_2 = -3$.

(3) $[330, 210] = \frac{330 \cdot 210}{30} = 2\,310$.

Tedy $[330, 210] = 2\,310$.

Věta 2.24. Obor integrity $(\mathbb{Z}[i], +, \cdot)$ Gaussových celých čísel je Eukleidův obor integrity.

Důkaz. Definujme normu υ takto: pro každé $a + bi \in \mathbb{Z}[i] - \{0\}$ nechť $\upsilon(a + bi) = a^2 + b^2$. Zřejmě υ je zobrazení $\mathbb{Z}[i] - \{0\}$ do $\mathbb{N}$.

• Nechť $a + bi, c + di \in \mathbb{Z}[i], c + di \neq 0$, takové, že $(a + bi)|(c + di)$. Pak existuje prvek $e + fi \in \mathbb{Z}[i]$ tak, že $(a + bi)(e + fi) = (c + di)$. Tedy $\upsilon((a + bi)(e + fi)) = \upsilon(c + id)$. Ale, jak snadno zjistíme, $\upsilon((a + bi)(e + fi)) = (a^2 + b^2)(e^2 + f^2)$ a $\upsilon(c + di) = c^2 + d^2$. Protože $\upsilon(a+bi) = a^2+b^2$, plyne z předchozích rovností vztah $\upsilon(a+bi) \leqq \upsilon(c+di)$, takže platí (2.5) z Definice 2.7.

• Zbývá dokázat, že existují $q_1 + q_2 i, r_1 + r_2 i \in \mathbb{Z}[i]$ tak, že $(a + bi) =$
$= (c + di) \cdot (q_1 + q_2 i) + (r_1 + r_2 i)$, kde $r_1 + r_2 i = 0$ nebo $\upsilon(r_1 + r_2 i) < \upsilon(c + di)$. Budeme postupovat tak, že podáme návod na nalezení $(q_1 + q_2 i)$ a $(r_1 + r_2 i)$ splňujících výše uvedenou podmínku. Prvky $a + bi, c + di \in \mathbb{Z}[i]$ jsou zároveň prvky tělesa komplexních čísel. Lze proto vytvořit podíl $\frac{a+bi}{c+di}$ a nalézt prvky $x, y \in \mathbb{R}$ (dokonce to budou prvky z $\mathbb{Q}$) tak, že

$$\frac{a + bi}{c + di} = x + yi. \tag{2.9}$$

Pokud x i y jsou celá čísla, stačí volit $q_1 + q_2 i = x + yi, r_1 + r_2 i = 0$.
V opačném případě zvolíme q_1, q_2 tak, aby $q_1, q_2 \in \mathbb{Z}$ a aby

$$|x - q_1| \leqq 0,5 \quad a \quad |y - q_2| \leqq 0,5; \tag{2.10}$$

taková q_1, q_2 jistě existují. Prvek $r_1 + r_2 i$ pak získáme ze vztahu

$$(r_1 + r_2 i) = (a + bi) - (c + di)(q_1 + q_2 i), \tag{2.11}$$

takže zřejmě $r_1, r_2 \in \mathbb{Z}$. Dosazením z (2.9) do (2.11) dostáváme

$$r_1 + r_2 i = (c + di)(x + yi) - (c + di)(q_1 + q_2 i) = (c + di)[(x - q_1) + (y - q_2)i].$$

Označme, pro snažší vyjadřování, $x - q_1 = p_1$ a $y - q_2 = p_2$. Pak

$$(r_1 + r_2 i) = (c + di)(p_1 + p_2 i). \tag{2.12}$$

Zbývá dokázat že $\upsilon(r_1 + r_2 i) < \upsilon(c + di)$.
Z (2.12) plyne $\upsilon(r_1 + r_2 i) = \upsilon((c + di)(p_1 + p_2 i)) = (c^2 + d^2)(p_1^2 + p_2^2 i)$.
Uvědomíme-li si, že $\upsilon(c + di) = c^2 + d^2$ a že díky (2.10) je
$(p_1^2 + p_2^2) = (x - q_1)^2 + (y - q_2)^2 \leqq 0,5$, dostaneme ihned dokazovanou nerovnost $\upsilon(r_1 + r_2 i) < \upsilon(c + di)$. Tím je důkaz Věty dokončen. □

Poznámka

Důkaz předchozí věty obsahuje návod na výpočet největšího společného dělitele v $\mathbb{Z}[i]$.

Příklad 2.13.

Nalezněte největší společný dělitel, koeficienty c_1, c_2 v Bezoutově rovnosti a nejmenší společný násobek čísel $a = 22 + 14i, b = 9 - i$.

(1) $\dfrac{22 + 14i}{9 - i} \cdot \dfrac{9 + i}{9 + i} = \dfrac{184 + 148i}{82} = \dfrac{184}{82} + \dfrac{148}{82} i = \dfrac{92}{41} + \dfrac{74}{41} i.$

Tedy, užíváme-li stejné značení jako ve zmíněném důkazu, je $x = \dfrac{92}{41}, y = \dfrac{74}{41}$.

Prvky q_1, q_2 určíme tak, aby $|x - q_1| \leqq 0,5, |y - q_2| \leqq 0,5$; položíme tedy $q_1 = 2, q_2 = 2$ tj. $Q_1 = q_1 + q_2 i = 2 + 2i$. Vypočteme dále

$$R_1 = r_1 + r_2 i = (22 + 14i) - (9 - i)(2 + 2i) = 22 + 14i - (20 + 16i) = 2 - 2i.$$

Dále postupujeme metodou Eukleidova algoritmu. Je

$$\frac{9 - i}{2 - 2i} \cdot \frac{2 + 2i}{2 + 2i} = \frac{20 + 16i}{8} = \frac{5}{2} + 2i$$

$x = \frac{5}{2}, y = 2$ Určíme prvky q_1' a q_2' tak, aby $|x - q_1'| \leq 0,5$ a $|y - q_2'| \leq 0,5$, položíme $q_1' = 2, q_2' = 2$ a máme $Q_2 = q_1' + q_2' i = 2 + 2i$.
Pak $R_2 = r_1' + r_2' i = (9 - i) - (2 - 2i)(2 + 2i) = (9 - i) - 8 = 1 - i$.
V dalším kroku Eukleidova algoritmu je

$$\frac{2 - 2i}{1 - i} \cdot \frac{1 + i}{1 + i} = \frac{4}{2} = 2.$$

Poněvadž nyní již $x, y \in \mathbb{Z}$, je $(2-2i) = (1-i)\cdot 2+0$ a tedy $D(22+14i, 9-i) = R_2 = 1-i$ a všechny prvky s ním asociované.

(2) Označme dále $a = 22 + 14i, b = 9 - i, x = D(22 + 14i, 9 - i)$. Budeme hledat celá čísla c_1, c_2 tak, aby $x = c_1 a + c_2 b$. Použijeme postupné úpravy „směrem dolů“ a dostáváme: $a = bQ_1 + R_1 \Rightarrow R_1 = a - b(2 + 2i)$

$b = R_1 Q_2 + R_2 \Rightarrow R_2 = b - [a - b(2 + 2i)](2 + 2i) = b - [a(2 + 2i) - b(2 + 2i)^2] =$
$= a(-2 - 2i) + b(1 + 8i)$ a $R_2 = D(a, b)$. Tedy $c_1 = -2 - 2i, c_2 = 1 + 8i$.

(3) $[22 + 14i, 9 - i] = \frac{(22+14i)\cdot(9-i)}{1-i} = \frac{212+104i}{1-i} \cdot \frac{1+i}{1+i} = \frac{108+316i}{2} = 54 + 158i$.
Tedy $[22 + 14i, 9 - 1] = 54 + 158i$.

Věta 2.25. Nechť T je komutativní těleso, potom obor integrity $T[x]$ polynomů jedné neurčité nad T je Eukleidův obor integrity.

Důkaz. Pro libovolné $f(x) \in T[x], f(x) \neq 0$, definujeme $\upsilon(f(x)) = stf(x)$ - krátce jen $\upsilon(f)$ - jako stupeň polynomu f. Zřejmě υ je zobrazení $T[x] - \{0\}$ do $\mathbb{N}$. Buďte dále $f(x), g(x) \in T[x], g(x) \neq 0$.

• Dokažme nejprve, že platí $f(x)|g(x) \Rightarrow \upsilon(f) \leqq \upsilon(g)$.

Nechť $f(x)|g(x)$, pak existuje $h(x) \in T[x]$ tak, že $f(x)h(x) = g(x)$.Protože $g(x) \neq 0$, je také $f(x) \neq 0$ a $h(x) \neq 0$, a tedy $st\ g(x), st\ h(x), st\ f(x) \in \mathbb{N}$. Víme, že stupeň součinu polynomů je roven součtu jejich stupňů, tedy $st\ g(x) = st\ f(x) + st\ h(x)$. Pak $st\ f(x) \leq st\ g(x)$, a tedy $\upsilon(f) \leq \upsilon(g)$.

• Předpokládejme dále, že

$$f(x) = a_0 + a_1 x + \cdots + a_n x \quad (a_n \neq 0),$$
$$g(x) = b_0 + b_1 x + \cdots + b_m x \quad (b_m \neq 0).$$

Je tedy $\upsilon(f) = n, \upsilon(g) = m$. Chceme dokázat, že

$$(\exists\ q(x), r(x) \in T[x])[f(x) = g(x)q(x) + r(x) \wedge (r(x) = 0 \vee v(r) < v(g))]. \tag{2.13}$$

Když $n < m$, stačí položit $q(x) = 0$ a $r(x) = f(x)$ a podmínka (2.13) platí. Přepokládejme proto dále, že $n \geqq m$. Důkaz tvrzení (2.13) provedeme matematickou indukcí podle stupně n polynomu $f(x)$.

a) Nechť nejprve $n = 0$, pak i $m = 0$ a je $f(x) = a_0,\ g(x) = b_0$, kde $a_0, b_0 \neq 0$. Poněvadž $a_0,\ b_0 \in T$, existuje $c_0 \in T$ tak, že $a_0 = b_0 c_0$. Označíme-li $q(x) = c_0$ a $r(x) = 0$, tvrzení (2.13) je ověřeno.

b) Předpokládejme, že (2.13) platí pro všechny polynomy stupně menšího než n; dokážeme, že platí i pro polynom $f(x)$ stupně n. Poněvadž $n \geqq m$, je $n - m \geqq 0$. Pokusíme se setrojit nový polynom $f_1(x)$ tak, aby byl lineární kombinací polynomů $f(x)$ a $g(x)$, a aby jeho stupeň byl menší než n. K tomu stačí si uvědomit že platí

$$a_n x^n - a_n b_m^{-1} x^{n-m} b_m x^m = 0. \tag{2.14}$$

Označme

$$f_1(x) = f(x) - a_n b_m^{-1} x^{n-m} g(x). \tag{2.15}$$

Potom díky (2.14) je opravdu stupeň $f_1(x)$ nižší než n podle indukčního předpokladu k němu tedy existují polynomy $q_1(x),\ r_1(x) \in T[x]$ tak, že

$$f_1(x) = g(x)q_1(x) + r_1(x) \wedge [r_1(x) = 0 \vee v(r_1) < v(g)]. \tag{2.16}$$

Dosadíme-li do (2.16) za $f_1(x)$ podle (2.15), dostaneme

$$f(x) - a_n b_m^{-1} x^{n-m} g(x) = q(x)q_1(x) + r_1(x)$$

a po úpravě

$$f(x) = g(x)(q_1(x) + a_n b_m^{-1} x^{n-m}) + r_1(x).$$

Označíme-li

$$q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}, r(x) = r_1(x),$$

je $f(x) = g(x)q(x) + r(x)$, kde podle (2.16) $r(x) = 0$ nebo $\upsilon(r) < \upsilon(g)$. Je-li $f(x) = 0$, stačí zřejmě volit $q(x) = r(x) = 0$. Tím je věta dokázána. □

Příklad 2.14.

Nalezněte největší společný dělitel, koeficienty c_1, c_2 v Bezoutově rovnosti a nejmenší společný násobek polynomů $f(x)$ a $g(x)$ jestliže:
$f(x) = x^6 + 2x^4 - 4x^3 - 3x^2 + 8x - 5$
$g(x) = x^5 + x^2 - x + 1.$

(1) Užijeme opět Eukleidův algoritmus. Vzhledem k tomu, že $D(f(x), g(x))$ se nezmění, pracujeme-li, místo s $f(x), g(x)$ s polynomy s nimi asociovanými, vynásobíme nejprve $f(x)$ číslem 2 a teprve pak provedeme dělení. Dostaneme

$$(x^6 + 2x^4 - 4x^3 - 3x^2 + 8x - 5) = (x^5 + x^2 - x + 1)x + (2x^4 - 5x^3 - 2x^2 + 7x - 5).$$

Tedy $q_1(x) = x, r_1(x) = 2x^4 - 5x^3 - 2x^2 + 7x - 5.$

V dalším kroku dělíme polynomy $g(x)$ a $r_1(x)$; z hlediska početního je však výhodnější nahradit $g(x)$ polynomem $2x^5 + 2x^2 - 2x + 2$ s ním asociovaným. Je

$$(2x^5 + 2x^2 - 2x + 2) = (2x^4 - 5x^3 - 2x^2 + 7x - 5)(x + \frac{5}{2}) + (\frac{29}{2}x^3 - \frac{29}{2}x + \frac{29}{2}),$$

takže $q_2(x) = x + \frac{5}{2}$ a $r_2(x) = \frac{29}{2}x^3 - \frac{29}{2}x + \frac{29}{2}$.

Polynom $r_2(x)$ opět nahradíme vhodným polynomem s ním asociovaným, tj. polynomem $x^3 - x + 1$, a provedeme další dělení. Dostáváme

$$(2x^4 - 5x^3 - 2x^2 + 7x - 5) = (x^3 - x + 1)(2x - 5) + 0,$$

tj. $q_3(x) = x - 2, r_3(x) = 0.$
Tedy $D(f(x), g(x)) = x^3 - x + 1.$

(2) Hledejme polynomy $c_1(x), c_2(x) \in T[x]$ tak, že $D(f(x), g(x)) = f(x)c_1(x) + g(x)c_2(x)$:

$$\begin{aligned} f(x) = g(x)q_1(x) + r_1(x) \Rightarrow r_1(x) &= f(x) - g(x)q_1(x) \\ q(x) = r_1(x)q_2(x) + r_2(x) \Rightarrow r_2(x) &= 2g(x) - r_1(x)q_2(x) \\ &= 2g(x) - q_2(x)[f(x) - g(x)q_1(x)] \\ &= f(x)(-q_2(x)) + g(x)(2 + q_1(x)q_2(x)) \end{aligned}$$

Tedy $c_1(x) = -q_2(x) = x + \frac{5}{2}$,

$c_2(x) = 2 + q_1(x)q_2(x) = 2 + x(x + \frac{5}{2}) = 2 + x^2 + \frac{5}{2}x$.

(3) $[f(x), g(x)] = \frac{f(x)\cdot g(x)}{D(f(x),g(x))} = \frac{(x^6+2x^4-4x^3-3x^2+8x-5)\cdot(x^5+x^2-x+1)}{x^3-x+1}$

Věta 2.26. Každý Eukleidův obor integrity je okruh hlavních ideálů.

Důkaz. Nechť I je Eukleidův obor integrity s normnou υ, nechť A je libovolný ideál v I. Pro $A = \{0\}$ je $A = \langle 0\rangle$ hlavní ideál, takže můžeme předpokládat, že je $A \neq \{0\}$. Ukážeme, že prvek $0 \neq a \in A$ takový, že $\upsilon(a) \leq \upsilon(b)$ pro každé $b \in A$, je generátor ideálu A. Existence takového prvku plyne z toho, že $\upsilon(1) \leq \upsilon(x)$ pro každé $x \in I \setminus \{0\}$, takže existuje $a \in A$ tak, že $\upsilon(a) = \min\{\upsilon(x) \mid 0 \neq x \in A\}$. Jelikož $a \in A$, je $\langle a\rangle \subseteq A$. Na druhé straně, je-li $0 \neq b \in A$ libovolný prvek, existují prvky $q, r \in I$ takové, že $b = aq + r$, kde $\upsilon(r) < \upsilon(a)$. Pro $r \neq 0$ je $r = b - qa \in A$, takže nerovnost $\upsilon(r) < \upsilon(a)$ dává spor s volbou prvku a. Tedy je nutně $r = 0, b = aq \in \langle a\rangle$, čímž je rovnost $A = \langle a\rangle$ dokázána. □

2.5 Gaussovy obory integrity

Nejprve zavedeme pojem, který zobecňuje pojem prvočísla. Jak víme, lze prvočísla v množině všech přirozených čísel $\mathbb{N}$ charakterizovat mnoha způsoby, z nichž si některá připomeneme.

Přirozené číslo $a > 1$ je prvočíslo, právě když

(a) je dělitelné pouze číslem 1 a sebou samým,

(b) dělí-li součin dvou přirozených čísel, dělí alespoň jedno z nich,

(c) každé z čísel $1, 2, \ldots, a-1$ je nesoudělné s a.

Definice 2.8. Prvek a oboru integrity I takový, že $a \neq 0$, $a \nparallel 1$ (tj. a není jednotka v I), se nazývá **ireducibilní prvek** v I, právě když má pouze nevlastní dělitele, tj. právě když platí

$$(\forall b \in I)\ b \mid a \Rightarrow (b \parallel a \vee b \parallel 1). \tag{2.17}$$

Nenulový prvek z I, který není jednotkou a není ireducibilní, se nazývá **reducibilní** nebo též **složený prvek** z I.

Příklad 2.15.

a) Příklady ireducibilních prvků v oboru integrity $\mathbb{Z}$ jsou např. všechna prvočísla v $\mathbb{N}$.

b) V oboru integrity $M = (\{a + bi\sqrt{5};\ a \in \mathbb{Z} \wedge b \in \mathbb{Z}\}, +, \cdot)$ lze ukázat, že například čísla ± 3, $2 + i\sqrt{5}, 2 - i\sqrt{5}$ jsou ireducibilní prvky a číslo $6 = (1 + i\sqrt{5})(1 - i\sqrt{5}) = 2 \cdot 3$ je reducibilní.

c) V oboru integrity polynomů jedné neurčité $T[x]$ nad tělesem T je každý polynom stupně prvního ireducibilním prvkem: každý jeho dělitel $g(x)$, musí mít stupeň menší nebo roven jedné. Má-li $g(x)$ stupeň nula, je jednotkou $T[x]$, a má-li stupeň jedna, je asociován s daným polynomem.

[1]

Definice 2.9. Nechť I je obor integrity. Prvek $p \in I, p \neq 0, p \nmid 1$ se nazývá **prvočinitelem** v I, právě když

$$(\forall a, b \in I)\ p \mid ab \Rightarrow (p \mid a \vee p \mid b). \tag{2.18}$$

Je ihned zřejmé, že tuto podmínku též zapsat ve tvaru

$$(\forall a, b \in I)(p \mid ab \wedge p \nmid a) \Rightarrow p \mid b, \tag{2.19}$$

Poznámka

1. Dříve než přejdeme k vyšetřování vlastností nově zavedených pojmů, zdůrazněme, že když mluvíme o ireducibilním prvku či prvočiniteli, je vždy nutné uvést, jakou strukturu přitom máme na mysli. Například číslo 2 je totiž prvočinitelem i ireducibilním prvkem z $\mathbb{Z}$, avšak v oboru integrity Gaussových celých čísel $\mathbb{Z}[i]$ není: 2 není ani prvočinitelem, ani ireducibilním prvkem:

- $2 = (1 + i)(1 - i)$, tedy 2 je v $\mathbb{Z}[i]$ reducinilní.
- $2/(1 + i)(1 - i)$, ale $2 \nmid (1 + i)$ ani $2 \nmid (1 - i)$, tedy 2 není prvočinitel v $\mathbb{Z}[i]$.

2. Protože podmínky (2.17) a (2.18) v definicích ireducibilního prvku a prvočinitele jsou formulovány pouze pomocí relace „dělí“, lze podle Věty 2.4 vlastnost „být ireducibilním prvkem“, respektivě „být prvočinitelem“ přenést vždy na celou třídu asociovaných prvků. Tuto skutečnost zachycuje následující Věta.

Věta 2.27. Nechť a, b jsou libovolné asociované prvky v oboru integrity I. Pak oba současně buď jsou, nebo nejsou ireducibilní prvky, respektivě prvočinitelé v I.

Věta 2.28. Nechť $p \in I$ je prvočinitelem v I. Pak pro každé $n \in \mathbb{N}$ platí

$$(\forall a_1, ..., a_n \in I)\ p \mid a_1 a_2 ... a_n \Rightarrow (\exists i)\ (1 \leqq i \leqq n \wedge p \mid a_i).$$

Důkaz. Nechť $n \geq 2$. Předpokládejme, že tvrzení platí pro $n-1$ prvků. Z $p|a_1 a_2 \cdots a_n$ plyne, že buď $p|a_1 a_2 \cdots a_{n-1}$, nebo $p|a_n$. V prvním případě existuje podle indukčního předpokladu index $i = \{1, 2, ..., n-1\}$ tak, že $p \mid a_i$ a Věta je dokázána. □

Věta 2.29. Nechť p je prvočinitelem v I, pak p je též ireducibilní prvek I.

Důkaz. Předpokládejme, že p je prvočinitel v I. Aby p byl ireducibilním prvkem v I, musíme dokázat, že pro každého dělitele $a \in I$ prvku p platí $a \parallel p$ nebo $a \parallel 1$. Jestliže tedy a je libovolný prvek z I takový, že $a \mid p$, existuje $q \in I$ tak, že $p = aq$. Pak ale $p \mid aq$, a poněvadž p je prvočinitelem v I, je buď $p \mid a$ nebo $p \mid q$. V prvém případě dostáváme $a \mid p$ a zároveň $p \mid a$, a tedy $p \parallel a$. Když $p \mid q$, je $p \parallel q$ (neboť z rovnosti $p = aq$ plyne $q \mid p$). Existuje tedy jednotka $j \in I$ taková, že $p = jq$. Protože zároveň $p = aq$ (a $p \neq 0$, a tedy i $q \neq 0$), je $a = j$ neboli $a \parallel j$. □

Poznámka

Poznamenejme, že tvrzení obrácené věty neplatí a že tedy Definice 2.8 a 2.9 — ač jsou zobecněním dvou vlastností téhož pojmu prvočísla v $\mathbb{N}$, určují v obecném případě různé pojmy. Ukázku ireducibilního prvku, který není prvočinitelem, uvedeme v následujícím příkladě.

Příklad 2.16. Nechť $M = \{a + bi\sqrt{5}; a \in \mathbb{Z} \wedge b \in \mathbb{Z}\}$ a $(M, +, \cdot)$ je obor integrity. Čísla $3, 2 + i\sqrt{5}, 2 - i\sqrt{5}$ jsou ireducibilní prvky v oboru integrity
$M = (\{a + bi\sqrt{5}, a \in \mathbb{Z} \wedge b \in \mathbb{Z}\}, +, \cdot)$ (viz Příklad 2.15 (b)). Platí však

$$3 \mid (2 + i\sqrt{5})(2 - i\sqrt{5}) = 9$$

a přitom (díky ireducibilnosti prvků $2 + i\sqrt{5}, 2 - i\sqrt{5}$ v M) $3 \nmid (2 + i\sqrt{5})$ a $3 \nmid (2 - i\sqrt{5})$. Tedy číslo 3 není prvočinitelem v M.

[1]

Poznámka

Říkáme, že obor integrity I splňuje podmínku prvočinitelovou, jestliže každý ireducibilní prvek je prvočinitelem.

Věta 2.30. Nechť v oboru integrity I existuje k libovolným dvěma prvkům největší společný dělitel. Pak každý ireducibilní prvek v I je současně prvočinitel v I.

Důkaz. Buď $p \in I$ ireducibilní prvek. Jestliže $p \mid ab$ pro nějaké prvky $a, b \in I$ a $p \nmid a$, pak nutně $(p, a) = 1$ vzhledem k tomu, že p má pouze nevlastní dělitele (podle předpokladu je p ireducibilní). Podle Věty 2.12 tedy $p \mid b$ a p je prvočinitel v I. □

Důsledek

V Eukleidově oboru integrity je libovolný prvek ireducibilní, právě když je prvočinitel.

Definice 2.10. Řeknem, že obor integrity I splňuje **podmínku konečnosti řetězce dělitelů** (pro zjednodušení je **podmínku (D)**), právě když pro každou posloupnost prvků v I tvaru

$$a_1, a_2, a_3, \cdots \in I, a_{i+1} \mid a_i \quad i = 1, 2, 3, \ldots, \tag{2.20}$$

platí

$$(\exists\, n \in \mathbb{N})(\forall\, r, s \in \mathbb{N})(n \leqq r \wedge n \leqq s) \Rightarrow a_r \parallel a_s, \tag{2.21}$$

neboli existuje $n \in \mathbb{N}$ tak, že

$$a_n \parallel a_{n+1}, a_{n+1} \parallel a_{n+2}, a_{n+2} \parallel a_{n+3}, \ldots \ .$$

Příklad 2.17. Z následujících čtyř posloupností v oboru integrity celých čísel zřejmě první tři mají tvar (2.20) a poslední tento tvar nemá.

24, -24, 12, -12, 6, -6, 3, -3, 1, -1, -1, 1, ...

0, 0, 0, 729, 81, 27, 27, -27, 27, 27, -27, 27, $\cdots$

7, 7, 7, 7, 1, 1, 1, 1, 1, 1, ...

6, 2, 6, 3, 6, 3, 6, 2, ...

Obdobně další dvě ukázky posloupnosti prvků z $\mathbb{Q}[x]$ mají tvar (2.20):

$$x_2 + 2x + 1, x + 1, 537x + 537, 1/2x + 1/2, 12/7, 3/4, 1, 1 \ldots$$
$$\text{x - 1, 2x - 2, 3x - 3, 4x -4, 5x -5, } \ldots$$

Všechny z uvedených posloupností, které mají tvar (2.20), splňují podmínku (2.21). To tedy naznačuje, že obory integrity $\mathbb{Z}$ a $\mathbb{Q}[x]$ by mohly splňovat podmínku (D). Odpověď nám dá následující věta.

[1]

Věta 2.31. V každém eukleidovském oboru integrity platí podmínka (D).

Důkaz. Nechť I je Eukleidův obor integrity a nechť $a_1, a_2, a_3, \cdots \in I$ je libovolná posloupnost tvaru (2.20). Máme ukázat, že pro ní platí (2.21).

Platí-li pro všechny její členy, že $a_i = 0$, jsou všechny spolu asociovány a stačí v (2.21) zvolit $n = 1$. Existuje-li člen $a_k \neq 0$, musí být díky (2.20) $a_{k+1} \neq 0, a_{k+2} \neq 0, \ldots$, takže daná posloupnost může mít nulové členy nejvýše na prvních $(k-1)$ místech. Protože posloupnost $a_1, a_2, a_3, \ldots$ a z ní vybraná posloupnost $a_k, a_{k+1}, a_{k+2}, \ldots$ mají tu vlastnost, že obě současně buď splňují, anebo nesplňují (2.21), můžeme předpokládat, že výchozí posloupnost má všechny členy nenulové. Poněvadž jde o prvky Eukleidova oboru integrity, můžeme přejít k posloupnosti jejich norem, pro něž podle (2.5) z definice Eukleidova oboru integrity platí nerovnosti $v(a_1) \geqq v(a_2) \geqq v(a_3) \geqq \cdots \geqq 0$.

V této nerostoucí posloupnosti přirozených čísel může nastat ostrá nerovnost pouze na konečně mnoha (nejvýše na $v(a_1)$) místech, takže existuje n tak, že pro libovolné indexy r, s kde $r \geqq n$ a $s \geqq n$, je

$$v(a_r) = v(a_s). \tag{2.22}$$

Z tranzitivnosti relace „dělí“ pak vyplývá, že buď $a_r \mid a_s$ nebo $a_s \mid a_r$, takže podle Věty 2.18 plyne z (2.22) vztah $a_r \parallel a_s$.

Tedy pro libovolnou posloupnost v I tvaru (2.20) platí (2.21), čímž je tvrzení věty dokázáno. □

Věta 2.32. Nechť obor integrity I spňuje podmínku (D) a nechť $a \in I, a \neq 0$ a $a \nmid 1$. Pak prvek a lze vyjádřit ve tvaru součinu konečně mnoha prvků ireducibilních v I neboli, jak se též říká, provést rozklad a v součin ireducibilních prvků.

Důkaz. Nejprve ukážeme, že každý prvek $a \neq 0$ z I, který není jednotkou, je dělitelný alespoň jedním ireducibilním prvkem. Jestliže a není ireducibilní, pak $a = a_1 b_1$, kde a_1, b_1 jsou vlastní dělitelé čísla a. Dále budeme pokračovat úplnou indukcí. Předpokládejme, že pro nějaké $n \geq 1$ jsme sestrojili prvky $a_1, a_2, ..., a_n, b_1, b_2, ..., b_n$ takové, že $a = a_1 a_2 ... a_n b_n$ a b_{i+1} je vlastním dělitelem b_i pro každé $i = 1, 2, ..., n-1$. Je-li prvek b_n ireducibilní jsme hotovy. V opačném případě je $b_n = a_{n+1} b_{n+1}$ kde a_{n+1} a b_{n+1} jsou vlastní dělitelé prvku b_n a $a = a_1 a_2 ... a_n a_{n+1} b_{n+1}$. Protože I splňuje podmínku konečnosti řetězců vlastních dělitelů, existuje nutně index m takový, že prvek b_m je ireducibilní dělitel prvku a. Nyní se již důkaz snadno dokončí. Jestliže a není ireducibilní, existuje ireducibilní prvek p_1 tak, že $a = p_1 a_1$. Předpokládejme, že pro nějaké $n \geq 1$ jsme sestrojili ireducibilní prvky $p_1, p_2, ..., p_n$ a prvky $a_1, a_2, ..., a_n$ z I takové, že $a = p_1 p_2 ... p_n a_n$ a a_{i+1} je vlastním dělitelem prvku a_i pro každé $i = 1, ..., n-1$. Je-li a_n ireducibilní, jsme hotovy. V opačném případě je podle první části důkazu $a_n = p_{n+1} a_{n+1}$, kde $p_{n+1} \in I$ je ireducibilní, a a_{n+1} je tudíž vlastním dělitelem prvku a_n. Z podmínky konečnosti řetězců vlastních dělitelů tedy plyne existence takového indexu m, že prvek a_m je ireducibilní a $a = p_1 p_2 ... p_m a_m$ je rozklad prvku a na součin ireducibilních prvků. □

Poznámka

Z důkazu předchozí Věty je zřejmé, že platí: Nechť obor integrity I splňuje podmínku (D) a nechť $x \in I, x \neq 0, x \nmid 1$. Pak x je dělitelný alespoň jedním prvkem ireducibilním v I.

Věta 2.33. Nechť I je eukleidovský obor integrity. Potom je možné každý nenulový prvek z I, který není jednotkou, rozložit v součin (konečně mnoha) ireducibilních prvků.

Důkaz. Ihned plyne z Věty 2.31 a Věty 2.32. □

Definice 2.11. Nechť I je obor integrity,

$$a = p_1 p_2 ... p_n, \ a = q_1 q_2 ... q_m$$

nechť jsou rozklady prvku $a \in I$ v součin ireducibilních prvků. Řekneme, že tyto **rozklady jsou spolu asociovány**, právě, když $m = n$ a při vhodném očíslování činitelů platí $p_i \parallel q_i$ pro $i = 1, 2, ..., n$.

Definice 2.12. Obor integrity I se nazývá **Gaussův obor integrity**, respektivě **obor integrity**
s jednoznačným rozkladem, právě když pro každé $a \in I,\ a \neq 0, a \nmid 1$ existuje rozklad v součin ireducibilních prvků a když libovolné dva rozklady prvku a jsou spolu asociovány.

Věta 2.34. Nechť obor integrity splňuje podmínku (D) a nechť v I k libovolným dvěma prvkům existuje největší společný dělitel. Pak I je Gaussův obor integrity.

Důkaz. Nechť obor integrity I splňuje předpoklady věty a nechť $a \neq 0, a \nmid 1$ je jinak libovolný prvek z I. Podle Věty 2.32 existují rozklady prvku a v součin konečně mnoha ireducibilních prvků. Je třeba dokázat, že všechny takové rozklady prvku a jsou spolu asociovány. Nechť tedy

$$a = p_1 p_2 ... p_n = q_1 q_2 ... q_m \tag{2.23}$$

jsou libovolné rozklady prvku a v součin ireducibilních prvků, přičemž můžeme předpokládat, že $n \leqq m$. Asociovanost těchto rozkladů dokážeme indukcí podle n,

Jestliže $n = 1$, je $a = p_1$. Poněvadž zároveň $a = q_1 ... q_m$ a ireducibilní prvek $a = p_1$ je podle Věty 2.30 prvočinitel, musí podle Věty 2.28 existovat index $j (1 \leqq j \leqq m)$ tak, že $a \mid q_j$. Protože prvek q_j je ireducibilní a $a \nmid 1$, musí platit $a \parallel q_j$ neboli $p_1 \parallel q_j$. Zbývá tedy dokázat, že $m = 1$. Předpokládejme $m \neq 1$. Je

$$p_1 = q_j (q_1 q_2 ... q_{j-1} q_{j+1} ... q_m),$$

a protože $p_1 \parallel q_j$, musí být součin $q_1 ... q_{j-1} q_{j+1} ... q_m$ jednotka v I, a tedy každý jeho činitel je jednotka v I. To však je ve sporu s předpokladem, že všechna $q_i (i = 1, ..., m)$ jsou ireducibilní prvky.

Předpokládejme dále, že Věta platí pro všechny prvky z I, jejichž „kratší“ rozklad má nejvýše $n - 1$ prvků. Ověříme platnost Věty pro prvek a, který má rozklady (2.23). Z (2.23) plyne

$$p_n (p_1 p_2 ... p_{n-1}) = q_1 q_2 ... q_m, \tag{2.24}$$

takže $p_n|q_1q_2...q_m$. Z předpokladu o oboru integrity I plyne, že p_n je nejen ireducibilní prvek, ale i prvočinitel; existuje podle Věty 2.29 index $k(1 \leqq k \leqq m)$ takový, že $p_n|q_k$. Díky komutativnosti struktury $(I, \cdot)$ můžeme činitele q_i přečíslovat tak, že $k = m$, a tedy $p_n|q_m$. Protože q_m je ireducibilní prvek a $p_n \nparallel 1$, musí platit $p_n \parallel q_m$. To znamená, že existuje jednotka $j \in J(I)$ tak, že $jp_n = q_m$. Po dosazení do (2.24) a po zkrácení prvkem $p_n \neq 0$ dostáváme

$$p_1p_2...p_{n-1} = q_1q_2...q_{m-1}j = q_1q_2...q_{m-2}q'_{m-1}, \tag{2.25}$$

kde $q'_{m-1} = jq_{m-1}$. První z rozkladů v (2.25) má $n-1$ činitelů, a tedy podle indukčního předpokladu musí být rozklady spolu asociovány. Proto je $n-1 = m-1$, a tedy též $n = m$, a při vhodném přečíslování je $p_1 \parallel q_1, ..., p_{n-1} \parallel q_{m-1}$. Protože již víme, že platí též $p_n \parallel q_m$, jsou rozklady (2.23) spolu asociovány, čímž je věta dokázána.

□

Bezprostředním důsledkem právě dokázané Věty 2.34 , Věty 2.29 a Věty 2.31 je toto tvrzení:

Věta 2.35. Každý Euklidův obor integrity je rovněž Gaussovým oborem integrity.

Tato věta se nedá obrátit. Existují Gaussovy obory integrity, které nejsou Eukleidovy, např. obor integrity $\mathbb{Z}[x]$ (viz Příklad 1.7.)

Poznámka

• V Gaussově oboru integrity můžeme libovolný rozklad prvku a

$$a = p_1p_2...p_m \tag{2.26}$$

v součin ireducibilních prvků upravit tak, že sdružíme vždy všechny ty činitele z (2.26), které jsou spolu asociovány. Rozklad (2.26) pak můžeme psát ve tvaru

$$a = jq_1^{r_1}q_2^{r_2}...q_n^{r_n}, \tag{2.27}$$

kde $j \in J(I), q_1, q_2, ...q_n$ jsou ireducibilní prvky z rozkladu (2.26), z nichž žádné dva s různými indexy nejsou spolu asociovány, a $r_1, r_2, ..., r_n$ jsou nenulová přirozená čísla. Takovému rozkladu (2.27) říkáme **kanonický rozklad** (prvku a v součin ireducibilních

prvků).

• Někdy je užitečné připustit v rozkladu (2.27) též exponenty rovné 0. Pak hovoříme o takzvaném **zobecněném kanonickém rozkladu**.

Příklad 2.18. Číslo $(-54) \in \mathbb{Z}$ má např. tento rozklad (v součin prvočísel):

$$(-54) = 2 \cdot 3 \cdot (-3) \cdot 3$$

Jeho kanonický rozklad pak sestrojíme takto:

$$(-54) = 2 \cdot ((-1) \cdot 3) \cdot 3 \cdot 3 = (-1) \cdot 2^1 \cdot 3^3$$

rovněž

$$(-54) = (-1) \cdot (-2)^1 \cdot (-3)^3$$

je jeho kanonický rozklad. Všimněme si, že jednotce (-1) se při zápisu kanonického rozkladu čísla (-54) nemůžeme vyhnout.

Příklad 2.19. Pro čísla $3\,675$, $11\,880 \in \mathbb{Z}$ která mají rozklady

$$3\,675 = 3 \cdot 5 \cdot (-5) \cdot (-7) \cdot 7 = 3 \cdot 5^2 \cdot 7^2,$$

$$11\,880 = 2 \cdot (-2) \cdot (-2) \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 11 = 2^3 \cdot 3^3 \cdot 5 \cdot 11,$$

mají zobecněné kanonické rozklady s touž množinou ireducibilních prvků tvar

$$3\,675 = 2^0 \cdot 3 \cdot 5^2 \cdot 7^2 \cdot 11^0,$$

$$11\,880 = 2^3 \cdot 3^3 \cdot 5 \cdot 7^0 \cdot 11.$$

Věta 2.36. Nechť I je gaussův obor integrity. Pak platí:

(1) Nechť prvek $a \in I, a \neq 0, a \neq 1$ má (zobecněný) kanonický rozklad $a = jp_1^{k_1} p_2^{k_2} \cdots p_n^{k_n}$. Pak nenulový prvek $b \in I$ je dělitelem prvku a, právě když (zobecněný) kanonický rozklad $b = j' p_1^{s_1} p_2^{s_2} \cdots p_n^{s_n}$, kde j' je jednotka a $s_i \in \mathbb{N}, s_i \leq k_i$ pro každé $i = 1, 2, ..., n$. Přitom b je vlastním dělitelem prvku a, právě když existuje $i \in \{1, 2, ..., n\}$ tak, že $s_i < k_i$ a $j \in \{1, 2, ..., n\}$ tak, že $s_j > 0$ (případ $i = j$ není vyloučen);

(2) Jsou-li $a = j_1 p_1^{k_1}, \cdots, p_n^{k_n}$ a $b = j_2 p_1^{s_1} \cdots p_n^{s_n}$ dva prvky z I takové, že
$k_1, k_2, ..., k_n, s_1, s_2, ..., s_n \in \mathbb{N}$, pak označíme-li $r_i = \min(k_i, s_i)$,
a $u_i = \max(k_i, s_i), i = 1, 2, \cdots, n$, je $(a, b) = p_1^{r_1} p_2^{r_2} \cdots p_n^{r_n}$ a $[a, b] = p_1^{u_1} p_2^{u_2} \cdots p_n^{u_n}$.

Důkaz. Je-li $a = bc$, kde $c = j''p_1^{m_1}p_2^{m_2}\cdots p_n^{m_n}, j'' \parallel 1$, pak zřejmě $j = j'j''$ a $k_i = s_i + m_i$ pro každé $i = 1, 2, ..., n$, odkud snadno plyne tvrzení (1).

Dále, prvek $d = p_1^{r_1}p_2^{r_2}\cdots p_2^{r_n}$ je podle (1) společným dělitelem prvků a, b.

Je-li t libovolný společný dělitel těchto prvků, pak $t = \bar{j}p_1^{l_1}p_2^{l_2}\cdots p_n^{l_n}$, kde $\bar{j}$ je jednotka v I a $l_i \leq k_i, l_i \leq s_i$ pro každé $i = 1, 2, ..., n$ podle (1). Pak ale $l_i \leq r_i, i = 1, 2, ..., n$, a $d = (a, b)$. Tvrzení o nejmenším společném násobku se dokáže analogicky. □

Poznámka

Z tvrzení (2) předchozí Věty ihned plyne, že v libovolném Gaussově oboru integrity I (existuje i pro libovolnou n-tici prvků z T) největší společný dělitel a nejmenší společný násobek.

Příklad 2.20. Počítejme v oboru integrity $\mathbb{Z}$ největší společný dělitel $D(750, 910, -1320) = x$ a nejmenší společný násobek $[750, 910, -1320] = y$.

Nejprve vytvoříme vhodné zobecněné rozklady daných čísel:

$$750 = 2^1 \cdot 3^1 \cdot 5^3 \cdot 7^0 \cdot 11^0 \cdot 13^0$$

$$910 = 2^1 \cdot 3^0 \cdot 5^1 \cdot 7^1 \cdot 11^0 \cdot 13^1$$

$$(-1320) = (-1) \cdot 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^1 \cdot 13^0$$

Potom $x = 2^{t_1} \cdot 3^{t_2} \cdot 5^{t_3} \cdot 7^{t_4} \cdot 11^{t_5} \cdot 13^{t_6}$ kde $t_1 = \min$ (1, 1, 3), $t_2 = \min$ (1, 0, 1) atd.;

tedy $x = 2^1 \cdot 3^0 \cdot 5^1 \cdot 7^0 \cdot 11^0 \cdot 13^0 = 2 \cdot 5 = 10$.

Obdobně $y = 2^{u_1} \cdot 3^{u_2} \cdot 5^{u_3} \cdot 7^{u_4} \cdot 11^{u_5} \cdot 13^{u_6}$,kde $u_1 = \max$ (1, 1, 3), $u_2 = \max$ (1, 0, 1), atd.; takže $y = 2^3 \cdot 3^1 \cdot 5^3 \cdot 7^1 \cdot 11^1 \cdot 13^1 = 3\ 003\ 000$.

Věta 2.37. Obor integrity I je Gaussovým oborem integrity, právě když v I k libovolným dvěma prvkům existuje největší společný dělitel a když I splňuje podmínku (D).

Důkaz. Splňuje-li daný obor integrity I podmínku (D) a existuje-li v něm největší společný dělitel pro libovolné dva prvky, je I podle Věty 2.34 Gaussův obor integrity.

Je-li I Gaussův obor integrity, existuje v I podle Věty 2.36 tvrzení (2) největší společný dělitel. Zbývá tedy ověřit, že I splňuje též podmínku (D). Nechť

$$a_1, a_2, ..., \text{kde } a_{i+1} \mid a_i \ (i = 1, 2, ...) \tag{2.28}$$

je libovolná posloupnost v I. Můžeme předpokládat, že $a_1 \neq 0$.A tedy i všechny členy této

posloupnosti jsou nenulové. Pak existuje zobecněný kanonický rozklad a_1; nechť je tvaru

$$a_1 = jp_1^{k_1}p_2^{k_2}\cdots p_n^{k_n}.$$

Podle Věty 2.36 tvrzení (1) mají všechny členy posloupnosti (2.28) zobecněné kanonické rozklady téhož tvaru, pouze s eventuálně menšími exponenty. Pokud $a_{i+1} \nmid a_i$, musí v rozkladu prvku a_{i+1} alespoň jeden exponent být menší než odpovídající mocnitel v rozkladu prvku a_i. Proto v posloupnosti (2.28) může být nejvýše $k_1 + k_2 + \cdots k_n$ členů, které nejsou spolu asociovány. To znamená, že existuje index m takový, že pro $s, r \geqq m$ je $a_s \parallel a_r$. Obor integrity I tedy splňuje podmínku (D), čímž je věta dokázána.

□

Poznámka

Tato Věta je nutná a postačující podmínka pro to, aby obor integrity byl Gaussův.

2.6 Příklady

Příklad 2.21. Nalezněte největší společný dělitel, koeficienty c_1, c_2 v Bezoutově rovnosti a nejmenší společný násobek čísel $a = 1\,331, b = -550$.

(1) Použijeme Eukleidova algoritmus:

$$\begin{aligned}
1\,331 &= -550 \cdot (-2) + 231\\
-550 &= 231 \cdot (-3) + 143\\
231 &= 143 \cdot 1 + 88\\
143 &= 88 \cdot 1 + 55\\
88 &= 55 \cdot 1 + 33\\
55 &= 33 \cdot 1 + 22\\
33 &= 22 \cdot 1 + 11\\
22 &= 11 \cdot 2 + 0
\end{aligned}$$

Tedy $D(1\,331, -550) = 11$.

(2) Označme dále $a = 1\,331, b = -550, x = D(1\,331, -550)$. Budeme hledat celá čísla c_1, c_2 tak, aby $x = c_1 a + c_2 b$. Použijeme postupné úpravy „směrem dolů“ a dostáváme:

$$\begin{aligned}
a &= b \cdot (-2) + 231 && \Rightarrow 231 = a + 2b \\
b &= (a + 2b)(-3) + 143 && \Rightarrow 143 = 3a + 7b \\
a + 2b &= (3a + 7b) \cdot 1 + 88 && \Rightarrow 88 = -2a - 5b \\
3a + 7b &= (-2a - 5b) \cdot 1 + 55 && \Rightarrow 55 = 5a + 12b \\
-2a - 5b &= (5a + 12b) \cdot 1 + 33 && \Rightarrow 33 = -7a - 17b \\
5a + 12b &= (-7a - 17b) \cdot 1 + 22 && \Rightarrow 22 = 12a + 29b \\
-7a - 17b &= (12a + 29b) \cdot 1 + 11 && \Rightarrow 11 = -19a - 46b \\
x = 11 &= -19a - 46b
\end{aligned}$$

Stačí tedy položit $c_1 = -19, c_2 = -46$.

(3) $[a, b] = \frac{a \cdot b}{D(a,b)} = [1\,331, -550] = \frac{1\,331 \cdot (-550)}{11} = -66\,550$.
Tedy $[1\,331, -550] = -66550$.

Příklad 2.22. Nalezněte největší společný dělitel a nejmenší společný násobek čísel $a = 126 + 64i, b = 48 - 72i$.

(1) $\frac{126+64i}{48-72i} \cdot \frac{48+72i}{48+72i} = \frac{1\,440}{7\,488} + \frac{3\,036}{1\,862}i = \frac{15}{78} + \frac{1\,518}{931}i$

$|\frac{15}{78} - q_1| \leq \frac{1}{2} \qquad |\frac{1\,518}{931} - q_2| \leq \frac{1}{2} \Rightarrow q_1 = 0, q_2 = 2 \Rightarrow Q_1 = 2i$

$\bullet R_1 = r_1 + r_2 i = (126 + 64i) - (48 - 72i)(2i) = -18 - 32i$

$\frac{48-72i}{-18-32i} \cdot \frac{-18+32i}{-18+32i} = \frac{1\,440}{1\,348} + \frac{2\,831}{1\,348}i = \frac{360}{337} + \frac{2\,831}{1\,348}i$

$|\frac{360}{337} - q_1'| \leq \frac{1}{2} \qquad |\frac{2\,831}{1\,348} - q_2'| \leq \frac{1}{2} \Rightarrow q_1' = 1, q_2' = 2 \Rightarrow Q_2 = 1 + 2i$

$\bullet R_2 = r_1' + r_2' i = (48 - 72i) - (-18 - 32i)(1 + 2i) = 2 - 4i$

$\frac{-18-32i}{2-4i} \cdot \frac{2+4i}{2+4i} = \frac{92}{20} - \frac{136}{20}i = \frac{23}{5} - \frac{34}{5}i$

$|\frac{23}{5} - q_1'| \leq \frac{1}{2} \qquad |-\frac{34}{5} - q_2'| \leq \frac{1}{2} \Rightarrow q_1'' = 5, q_2'' = -7 \Rightarrow Q_3 = 5 - 7i$

$\bullet R_3 = r_1'' + r_2'' i = (-18 - 32i) - (2 - 4i)(5 - 7i) = 2i$

$\frac{2-4i}{2i} \cdot \frac{-2i}{-2i} = \frac{-8-4i}{4} = -2 - i$

$|-2 - q_1''| \leq \frac{1}{2} \qquad |-1 - q_2''| \leq \frac{1}{2} \Rightarrow q_1''' = -2, q_2''' = -1 \Rightarrow Q_4 = -2 - i$

$\bullet R_4 = r_1''' + r_2''' i = (2 - 4i) - (2i)(-2 - i) = 0$

Tedy $D(a,b) = 2i$.

(2) $[a,b] = \frac{a \cdot b}{D(a,b)} = \frac{(126+64i)\cdot(48-72i)}{2i} \cdot \frac{-2i}{-2i} = \frac{-12\,000-21\,312i}{4} = -3\,000 - 5\,328i$

[4]

Příklad 2.23. Nalezněte největší společný dělitel polynomů $f(x), g(x), h(x)$ jestliže:

$f(x) = 2x^4 + 3x^3 - 3x^2 - 5x + 2$

$g(x) = 2x^3 + x^2 - x - 1$

$h(x) = 2x^5 - 2x^3 - x^2 + 4x + 1.$

Podle Věty 2.6 tvrzení b) je $D(f(x), g(x), h(x)) = D(D(f(x), g(x)), h(x))$.

(1) Určíme $D(f(x), g(x))$.

$(2x^4 + 3x^3 - 3x^2 - 5x + 2) : (2x^3 + x^2 - x - 1) = x + 1$

$\underline{-2x^4 - x^3 + x^2 + x}$

$2x^3 - 2x^2 - 4x + 2$

$\underline{-2x^3 - x^2 + x + 1}$

$-3x^2 - 3x + 3$

Vzhledem k tomu, že se největší společný dělitelpolynomů nezmění, nahradíme-li polynom $-3x^2 - 3x + 3$ polynomem $x^2 + x + 1$ s ním asociovaným. Je

$(2x^3 + x^2 - x - 1) : (x^2 + x - 1) = 2x - 1$

$\underline{-2x^3 - 2x^2 + 2x}$

$-x^2 + x - 1$

$\underline{x^2 - x + 1}$

0

Tedy $D(f(x), g(x)) = x^2 + x - 1$.

(2) Určíme $D(D(f(x), g(x), h(x)))$.

$(2x^5 - 2x^3 - x^2 + 4x + 1) : (x^2 + x - 1) = 2x^3 - 2x^2 + 2x - 5$

$\underline{-2x^5 - 2x^4 + 2x^3}$

$-2x^4 - x^2 - 4x + 1$

$\underline{2x^4 + 2x^3 - 2x^2}$

$2x^3 - 3x^2 + 4x + 1$

$$\underline{-2x^3 - 2x^2 - 2x}$$
$$-5x^2 + 6x + 1$$
$$\underline{5x^2 - 5x - 5}$$
$$11x - 4$$

Polynom $x^2 + x - 1$ nahradíme polynomem $11x^2 + 11x - 11$ s ním asociovaným. Dostáváme

$(11x^2 + 11x - 11) : (11x - 4) = x + \frac{15}{11}$

$\underline{-11x^2 + 4x}$

$15x - 11$

$\underline{-15x + \frac{60}{11}}$

$-\frac{60}{11}$

Tedy $D(D(f(x), g(x), h(x))) = -\frac{60}{11}$.

Příklad 2.24.

Mezi nejdůležitější rozšíření oboru celých čísel patří tzv. kvadratická rozšíření, tj obory typu $\mathbb{Z}[\sqrt{s}]$. Pro některá s se dělitelnost chová pěkně (jsou to dokonce Eukleidovy obory), pro některá naopak velmi špatně (nejsou to ani Gaussovy obory).

Nechť v dalším je s celé číslo, jež není dělitelné druhou mocninou žádného prvočísla, a nechť υ je zobrazení

$$\upsilon : \mathbb{Z}[\sqrt{s}] = \{a + b\sqrt{s}; a \in \mathbb{Z} \wedge b \in \mathbb{Z}\} \longrightarrow \mathbb{N} \text{ takové, že } \upsilon(a + b\sqrt{s}) = |a^2 - sb^2|. \qquad (2.29)$$

Je dobré mít na paměti, že pro $s < 0$ je $\upsilon(u) = |u|^2$, (obyčejná absolutní hodnota komplexního čísla), díky čemuž se dá často aplikovat geometrický náhled na situaci. Některé obory $\mathbb{Z}[\sqrt{s}]$ jsou Eukleidovy, např. $s = -1, \pm 2, 3$, některé ne, např. pro $s = -3, 5$.

Dá se dokázat, že pro každé $u, v \in \mathbb{Z}[\sqrt{s}]$ platí:

(1) $\upsilon(u \cdot v) = \upsilon(u) \cdot \upsilon(v)$,

(2) $\upsilon(u) = 1$, právě když u je invertibilní.

Důkaz.

(1) Označme $u = a + b\sqrt{s}$ a $v = c + d\sqrt{s}$. Pak

$$\begin{aligned} \upsilon(u \cdot v) &= \upsilon((ac + sbd) + (ad + bc)\sqrt{s}) = \\ &= |a^2c^2 + 2sabcd + s^2b^2d^2 - s(a^2d^2 + 2abcd + b^2c^2)| = \\ &= |a^2c^2 + s^2b^2d^2 - sa^2d^2 - sb^2c^2| = \\ &= |a^2 - sb^2| \cdot |c^2 - sd^2| = \upsilon(u) \cdot \upsilon(v). \end{aligned}$$

(2) Pokud $\upsilon(a + b\sqrt{s}) = |a^2 - sb^2| = 1$, pak $a^2 - sb^2 = (a - b\sqrt{s})(a + b\sqrt{s}) = \pm 1$, a tedy $(a + b\sqrt{s}) \parallel 1$.
Opačná implikace plyne z (1): je-li $u \parallel 1$, tj. existuje v takové, že $uv = 1$, pak $1 = \upsilon(1) = \upsilon(uv) = \upsilon(u)\upsilon(v)$, a tedy $\upsilon(u) = \upsilon(v) = 1$.

□

Podmínku (2) lze s úspěchem využít pro hledání invertibilních prvků.

- V oboru $\mathbb{Z}[i]$ máme $\vartheta(a + bi) = a^2 + b^2$, tedy $\vartheta(u) = 1 \Leftrightarrow u = \pm 1, u = \pm i$.
- V oboru $\mathbb{Z}[i\sqrt{2}]$ máme $\upsilon(a + bi) = a^2 + 2b^2$, tedy $\upsilon(u) = 1 \Leftrightarrow u = \pm 1$.

Podmínka (1) říká, že pokud $u \mid v$, pak $\upsilon(u) \mid \upsilon(v)$. Navíc, pokud je u vlastní dělitel, pak $1 \neq \upsilon(u) \neq \upsilon(v)$. Tyto vlastnosti lze s úspěchem využít pro hledání ireducibilních rozkladů. Jednak, je-li $\upsilon(u)$ prvočíslo, pak je u zaručeně ireducibilní. Opačná implikace neplatí, např. v $\mathbb{Z}[i]$ je prvek 3 ireducibilní, ačkoliv má normu 9. Uvedená vlastnost však pomáhá k nalezení dělitele či k důkazu ireducibility: např. pro zmíněný prvek 3 v $\mathbb{Z}[i]$, pokud by existoval netriviální rozklad, pak jedině na dva prvky normy 3; prvky normy 3, ale v $\mathbb{Z}[i]$ nejsou.

Pro některé obory $\mathbb{Z}[\sqrt{s}]$ je uvedené zobrazení υ Eukleidovou normou. Ukážeme tento fakt pro Gaussova celá čísla, tj. ukážeme, že zobrazení υ definované v (2.29) je Eukleidova norma v $\mathbb{Z}[i]$.

Důkaz. Je třeba ověřit podmínky (2.5) a (2.6) z Definice 2.7.

- Podmínka (2.5) plyne ihned z předchozího tvzení (1).

• Pro důkaz (2.6) uvažujme $a, b \in \mathbb{Z}[i], b \neq 0$, a položme

$$z = \frac{a}{b} \in \mathbb{C}$$

(přesný podíl v $\mathbb{C}$). Buď q nejbližší prvek $\mathbb{Z}[i]$ k prvku z (tj. takový, pro který je $|z - q|$ minimální); je-li takových více, zvolme libovolný z nich. Položme

$$r = a - bq.$$

Pak zřejmě $bq + r = a$ a zbývá dokázat, že $\upsilon(r) < \upsilon(b)$. Jaká je vzdálenost q a z? V nejhorším případě je z uprostřed čtverce s celočíselnými vrcholy, tedy určitě $|z - q| \leq \frac{\sqrt{2}}{2} < 1$. Proto

$$\upsilon(r) = |r|^2 = |a - bq|^2 = |b|^2 \cdot |\frac{a}{b} - q|^2 = |b|^2 \cdot |z - q|^2 < |b|^2 = \upsilon(b).$$

□

Pro obory $\mathbb{Z}[i\sqrt{2}]$ či $\mathbb{Z}^{2\pi i/3}$ lze důkaz provést zcela analogicky, protože i zde platí $\upsilon(u) = |u|^2$ a jediný rozdíl tak je v odhadu $|z - q|$. Pro $\mathbb{Z}[i\sqrt{3}]$ už důkaz neprojde, protože střed obdélníka má vzdálenost od vrcholu rovnou 1. Ve skutečnosti tento obor není ani Gaussův.

Pro obory $\mathbb{Z}[s]$ pro s kladné schází geometrická představa. Pro $s = 2, 3$ však funguje podobný algoritmus dělení: stačí zaokrouhlit koeficienty přesného podílu. Důkaz odhadu normy zbytku je však o něco komplikovanější.

Studium různých rozšíření oboru celých čísel není nijak samoúčelné, matematici se k těmto oborům dostali při řešení řady jiných úloh. K rozvoji teorie nezanedbatelně přispěly např. pokusy dokázat tímto způsobem Velkou Fermatovu větu (tj. dokázat, že neexistují nenulová celá čísla x, y, z splňující $x^n + y^n = z^n$ pro nějaké $n \geq 3$). Už Leonhard Euler použil v roce 1753 počítání v oboru $\mathbb{Z}[i\sqrt{3}]$ k řešení Velké Fermatovy věty pro exponent 3 a asi největšího úspěchu touto metodou dosáhl Kummer v polovině 19. století, když se mu povedlo vyřešit všechny exponenty menší než 100 kromě 37, 59, 67, 74.

Pro ilustraci ukážeme řešení jedné speciální diofantické rovnice. Metoda využívá řadu teoretických vlastností oboru $\mathbb{Z}[i]$, např. existence největšího společného dělitele a jednoznačnost rozkladů na ireducibilní prvky.

[2]

Příklad 2.25. Řeště v oboru integrity celých čísel rovnici

$$x^2 + 1 = y^3.$$

Nejprve rozložíme $x^2+1 = (x+i)(x-i)$ a dokážeme, že jsou čísla $x-i, x+i$ nesoudělná. Platí $D(x+i, x-i) = D(x+i, 2i) = D(x-i, 2i)$, a protože $2i = (1+i)^2$, musí být výsledek jedno z čísel $1, 1+i, (1+i)^2$. Pokud je x liché, pak je $v(x+i) = v(x-i) \equiv 2 \ (mod\ 4)$ (dosaďme $x = 2k+1$), a tedy $(1+i)^2$ nedělí $x+i$ ani $x-i$ (tj. v ireducibilním rozkladu těchto čísel je $1+i$ nejvýše jednou). Protože je součin $(x+i)(x-i)$ třetí mocninou, počet čísel $1+i$ v jeho ireducibilním rozkladu musí být dělitelný třemi; čili jediná možnost je, že tam není žádné. Tedy $D(x+i, x-i) = 1$.

Dokázali jsme, že $x+i$ a $x-i$ jsou nesoudělné v $\mathbb{Z}[i]$. Protože jejich součin je třetí mocninou čísla y, každé z nich musí být třetí mocninou nějakého prvku $\mathbb{Z}[i]$.Uvažujme takové $a+bi$: z rovnosti
$(a+bi)^3 = (a^3 - ab^2) + (a^2b - b^3)i = x+i$ plyne $b(a^2-b^2) = 1$, což má jediné celočíselné řešení: $b = -1, a = 0$. To dává jediné celočíselné řešení původní rovnice $x = 0, y = 1$.

[2]

Příklad 2.26.

$\mathbb{Z}[\sqrt{2}]$ spolu s normou $v(u) = v(a+bi) = |a^2 - 2b^2|$ je Euklidův obor integrity (respektivě norma v je Euklidova norma).

Řešení.

1. Dokážeme, že pro libovolné prvky $u, v \in \mathbb{Z}[\sqrt{2}], v \neq 0$, platí:

$$u \mid v \Rightarrow v(u) \leq v(v) :$$

Nechť $u = a + b\sqrt{2},\ v = c + d\sqrt{2}\ \in \mathbb{Z}[\sqrt{2}]$, $c + d\sqrt{2} \neq 0$ jsou takové prvky, že
$(a + b\sqrt{2}) \mid (c + d\sqrt{2})$. Pak existuje prvek $e + f\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, tak, že
$c + d\sqrt{2} = (a + b\sqrt{2})(e + f\sqrt{2})$.
Tedy $v((a + b\sqrt{2}) \cdot (e + f\sqrt{2})) = v(c + d\sqrt{2})$.
Ale protože víme z Příkladu 0.4, že $v(a + b\sqrt{2})(e + f\sqrt{2}) = v(a + b\sqrt{2})v(e + f\sqrt{2})$, tak

$|a^2 - 2b^2| \cdot |e^2 - 2f^2| = |c^2 - 2d^2|$, a tedy

$|a^2 - 2b^2| \leq |c^2 - 2d^2|$, neboli $\upsilon(a + b\sqrt{2}) \leq \upsilon(c + d\sqrt{2})$, tj. $\upsilon(u) \leq \upsilon(v)$.

2. Dále dokážeme, že pro libovolné prvky $u, v \in \mathbb{Z}[\sqrt{2}], v \neq 0$, existují prvky $q, r \in \mathbb{Z}[\sqrt{2}])$ tak, že $u = vq + r, \upsilon(r) = 0$ nebo $\upsilon(r) < \upsilon(v)$.

Nechť $u = a + b\sqrt{2}, v = c + d\sqrt{2}$.

Vytvoříme podíl $\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{a+b\sqrt{2}}{c+d\sqrt{2}} \cdot \frac{c-d\sqrt{2}}{c-d\sqrt{2}} = \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2}$, kde $\frac{ac-2bd}{c^2-2d^2}, \frac{bc-ad}{c^2-2d^2} \in \mathbb{Q}$.

Lze tedy nalázt racionální čísla x, y tak, že

$$\frac{a+b\sqrt{2}}{c+d\sqrt{2}} = \frac{ac-2bd}{c^2-2d^2} + \frac{bc-ad}{c^2-2d^2}\sqrt{2} = x + y\sqrt{2}. \tag{2.30}$$

(a) Pokud jsou $x, y \in \mathbb{Z}$, stačí volit $q_1 + q_2\sqrt{2} = x + y\sqrt{2}, r_1 + r_2\sqrt{2} = 0$.

(b) V opačném případě zvolíme celá čísla q_1, q_2 tak, že

$$|x - q_1| = |\tfrac{ac-2bd}{c^2-2d^2} - q_1| \leq \tfrac{1}{2} \text{ a } |y - q_2| = |\tfrac{bc-ad}{c^2-2d^2} - q_2| \leq \tfrac{1}{2}. \tag{2.31}$$

Taková čísla q_1, q_2 jistě existují.

Prvek $r = r_1 + r_2\sqrt{2}$ získáme z rovnice

$$r = r_1 + r_2\sqrt{2} = (a + b\sqrt{2}) - (c + d\sqrt{2})(q_1 + q_2\sqrt{2}), \text{ takže } r_1, r_2 \in \mathbb{Z}. \tag{2.32}$$

Dosazením z (2.30) do (2.32) máme

$$r_1 + r_2\sqrt{2} = (x + y\sqrt{2})(c + d\sqrt{2}) - (c + d\sqrt{2})(q_1 + q_2\sqrt{2}) = (c + d\sqrt{2})[(x - q_1) + (y - q_2)\sqrt{2}].$$

Označme $x - q_1 = p_1$ a $y - q_2 = p_2$. Pak

$$r_1 + r_2\sqrt{2} = (c + d\sqrt{2})(p_1 + p_2\sqrt{2}). \tag{2.33}$$

Z (2.33) plyne, že

$$\upsilon(r_1 + r_2\sqrt{2}) = \upsilon(c + d\sqrt{2})\upsilon(p_1 + p_2\sqrt{2}) = |c^2 - 2d^2| \cdot |p_1^2 - 2p_2^2|.$$

Díky (3.21) je $|p_1^2 - 2p_2^2| = |(x - q_1)^2 - 2(y - q_2)^2| \leq \frac{1}{2}$. Tedy $\upsilon(r_1 + r_2\sqrt{2}) < \upsilon(c + d\sqrt{2})$.

Poznámka

Analogicky lze postupovat i v případě oborů integrity $\mathbb{Z}[\sqrt{3}]$ a $\mathbb{Z}[i\sqrt{2}]$.

[4]

Příklad 2.27.

Nalezněte největší společný dělitel a nejmenší společný násobek čísel
$a = -50 + 3\sqrt{2}, b = 22 + 15\sqrt{2}$.

(1) $\frac{-50+3\sqrt{2}}{22+15\sqrt{2}} \cdot \frac{22-15\sqrt{2}}{22-15\sqrt{2}} = \frac{-1190}{34} + \frac{816}{34}\sqrt{2} = -35 + 24\sqrt{2} = q_1 + q_2\sqrt{2}$.

• $R_1 = r_1 + r_2\sqrt{2} = (-50 + 3\sqrt{2}) - (22 + 15\sqrt{2})(-35 + 24\sqrt{2}) = 0$.

Tedy $D(a, b) = 22 + 15\sqrt{2}$.

(2) $[a, b] = \frac{a \cdot b}{D(a,b)} = a = -50 + 3\sqrt{2}$

[4]

Příklad 2.28. Nalezněte největší společný dělitel a nejmenší společný násobek čísel
$a = 10 + 2\sqrt{3}, b = 54 + 44\sqrt{3}$.

(1) $\frac{54+44\sqrt{3}}{10+2\sqrt{3}} \cdot \frac{10-2\sqrt{3}}{10-2\sqrt{3}} = \frac{276+332\sqrt{3}}{88} = \frac{276}{88} + \frac{332}{88}\sqrt{3} = \frac{69}{22} + \frac{83}{22}\sqrt{3}$

$|\frac{69}{22} - q_1| \leq \frac{1}{2} \qquad |\frac{83}{22} - q_2| \leq \frac{1}{2} \Rightarrow q_1 = 3, q_2 = 4 \Rightarrow Q_1 = 3 + 4\sqrt{3}$

• $R_1 = r_1 + r_2\sqrt{3} = (54 + 44\sqrt{3}) - (10 + 2\sqrt{3})(3 + 4\sqrt{3}) = -2\sqrt{3}$

$\frac{10+2\sqrt{3}}{-2\sqrt{3}} \cdot \frac{2\sqrt{3}}{2\sqrt{3}} = \frac{12+20\sqrt{3}}{-12} = -1 - \frac{5}{3}\sqrt{3}$.

$q_1' = -1, |\frac{5}{3} - q_2'| \leq \frac{1}{2} \Rightarrow q_2' = -2 \Rightarrow Q_2 = -1 - 2\sqrt{3}$

• $R_2 = r_1' + r_2'\sqrt{3} = (10 + 2\sqrt{3}) + 2\sqrt{3}(-1 - 2\sqrt{3}) = -2$

$\frac{-2\sqrt{3}}{-2} = \sqrt{3} \qquad \Rightarrow Q_3 = \sqrt{3}, r'' = 0.$

Tedy $D(a, b) = -2$.

(2) $[a, b] = \frac{a \cdot b}{D(a,b)} = \frac{(10+2\sqrt{3}) \cdot (54+44\sqrt{3})}{-2} = (54 + 44\sqrt{3})(5 + \sqrt{3}) = 666 + 274\sqrt{3}$

[4]

Příklad 2.29. Nalezněte největší společný dělitel a nejmenší společný násobek čísel
$a = 4 + 32i\sqrt{2}, b = 24 - 17i\sqrt{2}$.

(1) $\frac{4+32i\sqrt{2}}{24-17i\sqrt{2}} \cdot \frac{24+17i\sqrt{2}}{24+17i\sqrt{2}} = \frac{96+68i\sqrt{2}+768i\sqrt{2}+544i^2\sqrt{2}^2}{576+408i\sqrt{2}-408i\sqrt{2}-289i^2\sqrt{2}^2} = -\frac{992}{1\,154} + \frac{836i\sqrt{2}}{1\,154} = -\frac{496}{577} + \frac{418i\sqrt{2}}{577}$

$|-\frac{496}{577} - q_1| \leq \frac{1}{2} \qquad |\frac{418}{577} - q_2| \leq \frac{1}{2} \Rightarrow q_1 = 3, q_2 = 4 \Rightarrow Q_1 = -1 + i\sqrt{2}$

• $R_1 = r_1 + r_2 i\sqrt{2} = (4 + 32i\sqrt{2}) - (24 - 147i\sqrt{2}) \cdot (-1 + i\sqrt{2}) = 28 - 9i\sqrt{2} - 34 =$
$= -6 - 9i\sqrt{2}$

$\frac{24-147i\sqrt{2}}{-6-9i\sqrt{2}} \cdot \frac{-6+9i\sqrt{2}}{-6+9i\sqrt{2}} = \frac{162+318i\sqrt{2}}{198} = \frac{9}{11} + \frac{53i\sqrt{2}}{33}$

$|\frac{9}{11} - q_1'| \leq \frac{1}{2} \qquad |\frac{53}{33} - q_2'| \leq \frac{1}{2} \Rightarrow q_1' = 1, q_2' = 2 \Rightarrow Q_2 = 1 + 2i\sqrt{2}$

• $R_2 = r_1' + r_2' i\sqrt{2} = (24 - 17i\sqrt{2}) - (-6 - 9i\sqrt{2}) \cdot (1 + 2i\sqrt{2}) = -6 + 4i\sqrt{2}$

$\frac{-6-9i\sqrt{2}}{-6+4i\sqrt{2}} \cdot \frac{-6-4i\sqrt{2}}{-6-4i\sqrt{2}} = -\frac{9}{17} + \frac{20i\sqrt{2}}{17}$

$|\frac{9}{17} - q_1''| \leq \frac{1}{2} \qquad |\frac{20}{17} - q_2''| \leq \frac{1}{2} \Rightarrow q_1'' = -1, q_2'' = 1 \Rightarrow Q_3 = -1 + i\sqrt{2}$

• $R_3 = r_1'' + r_2'' i\sqrt{2} = (-6 - 9i\sqrt{2}) - (-6 + 4i\sqrt{2}) \cdot (-1 + i\sqrt{2}) = -4 + i\sqrt{2}$

$\frac{-6+4i\sqrt{2}}{-4+i\sqrt{2}} \cdot \frac{-4-i\sqrt{2}}{-4-i\sqrt{2}} = \frac{16}{9} - \frac{5i\sqrt{2}}{9}$

$|\frac{16}{9} - q_1'''| \leq \frac{1}{2} \qquad |\frac{5}{9} - q_2'''| \leq \frac{1}{2} \Rightarrow q_1''' = 2, q_2''' = -1 \Rightarrow Q_4 = 2 - i\sqrt{2}$

• $R_4 = r_1''' + r_2''' i\sqrt{2} = (-6 + 4i\sqrt{2}) - (-4 + i\sqrt{2}) \cdot (2 - i\sqrt{2}) = -2i\sqrt{2}$

$\frac{-4+i\sqrt{2}}{-2i\sqrt{2}} \cdot \frac{2i\sqrt{2}}{2i\sqrt{2}} = -\frac{1}{2} - i\sqrt{2}$

$|\frac{1}{2} - q_1^{IV}| \leq \frac{1}{2} \qquad |1 - q_2^{IV}| \leq \frac{1}{2} \Rightarrow q_1^{IV} = -1, q_2^{IV} = -1 \Rightarrow Q_5 = -1 - i\sqrt{2}$

•$R_5 = r_1^{\mathrm{IV}} + r_2^{\mathrm{IV}} i\sqrt{2} = (-4 + i\sqrt{2}) - (-2i\sqrt{2}) \cdot (-1 - i\sqrt{2}) = -i\sqrt{2}$

$\frac{-2i\sqrt{2}}{-i\sqrt{2}} = 2 \qquad \Rightarrow Q_6 = 2, R_6 = 0.$

Tedy $D(a, b) = -i\sqrt{2}$.

(2) $[a, b] = \frac{a \cdot b}{D(a,b)} = \frac{(4+32i\sqrt{2})(24-17i\sqrt{2})}{-i\sqrt{2}} \cdot \frac{i\sqrt{2}}{i\sqrt{2}} = \frac{11\,84i\sqrt{2} - 1\,400}{2} = 592i\sqrt{2} - 700$

[4]

Příklad 2.30. Obor $\mathbb{Z}[\sqrt{5}]$ není Gaussův obor integrity. Dokažte.

Důkaz.

$$4 = 2 \cdot 2 = (\sqrt{5} - 1)(\sqrt{5} + 1)$$

• Prvky 2 a $\pm 1 + \sqrt{5}$ jsou navzájem neasociované, protože všechny prvky dělitelné 2 mají oba koeficienty sudé.11x^2 + 11x - 11

• Dokážeme, že prvky 2 a $\pm 1 + \sqrt{5}$ jsou ireducibilní.

$v(u) = v(a + b\sqrt{5}) = |a^2 - 5b^2| = a^2 + 5b^2$, pro libovolný prvek $u \in \mathbb{Z}[\sqrt{5}]$.

Protože $v(2) = 4, v(\pm 1 + \sqrt{5}) = |1 - 5 \cdot 1| = 4$ tj. normy prvků 2 a $\pm 1 + \sqrt{5}$ jsou 4, bude netriviální rozklad rozkladem na součin dvou prvků normy 2.

V $\mathbb{Z}[\sqrt{5}]$ však neexistují prvky s normou 2: je-li $u = a + b\sqrt{5}$ a a, b mají opačnou paritu, pak je $\upsilon(u)$ liché, a mají-li stejnou paritu, pak je $\upsilon(u)$ dělitelné 4.

□

[2]

Příklad 2.31. Nalezněte všechny jednotky v oboru integrity I jestliže:

(1) $I = \mathbb{Z}[i\sqrt{2}]$:

$(\forall u \in \mathbb{Z}[i\sqrt{2}]) \quad \upsilon(u) = \upsilon(a + bi\sqrt{2}) = |a^2 + 2b^2| = a^2 + 2b^2$.

Prvek $u \in \mathbb{Z}[i\sqrt{2}]$ je jednotka, právě když $\upsilon(u) = 1$ (viz Příklad 2.24).

Tedy $\upsilon(u) = a^2 + 2b^2 = 1$, což nastane právě tehdy, když $b = 0$ a $a = \pm 1$.

Pak $u = 1$ a $u = -1$ jsou všechny jednotky v $\mathbb{Z}[i\sqrt{2}]$.

(2) $I = \mathbb{Z}[\sqrt{2}]$:

$(\forall u \in \mathbb{Z}[\sqrt{2}]) \quad \upsilon(u) = \upsilon(a + b\sqrt{2}) = |a^2 - 2b^2|$ a $|a^2 - 2b^2| = 1 \Leftrightarrow a^2 - 2b^2 = \pm 1$

(a) $a^2 - 2b^2 = -1$. Dosazujeme-li postupně do rovnice čísla $b = 0, 1$, dostáváme hodnoty $a^2 = -1, a^2 = 1$. Tedy nejmenší kladné řešení této rovnice je $[a_0, b_0] = [1, 1]$ a $u = 1 + \sqrt{2}$ je jednotka v $\mathbb{Z}[\sqrt{2}]$.

Protože vlastně hledáme všechna řešení Pellových rovnic $a^2 - 2b^2 = -1$ a $a^2 - 2b^2 = 1$, tak

- pro n liché, $u \in \mathbb{Z}^+$, budou $(1 + \sqrt{2})^n$ všechna kladná řešení rovnice $a^2 - 2b^2 = -1$,
- pro n sudé, $u \in \mathbb{Z}^+$, budou $(1 + \sqrt{2})^n$ všechna kladná řešení rovnice $a^2 - 2b^2 = 1$.

(b) $a^2 - 2b^2 = +1$, pro $b = 0$ je $a^2 = 1$ a $u = \pm 1$ jsou jednotky v $\mathbb{Z}[\sqrt{2}]$.

Tedy všemi jednotkami v oboru integrity $\mathbb{Z}[\sqrt{2}]$ jsou $u = \pm 1$ a dále $u = \pm(1 + \sqrt{2})^n$, $n \in \mathbb{Z} - \{0\}$ (viz Věta 2.2 tvrzení (2)).

Příklad 2.32. Dokažte, že v oboru integrity $\mathbb{Z}[\sqrt{5}]$.

(1) Je prvek $(2 + \sqrt{5})^n$ jednotka pro $u \in \mathbb{Z}$.

(2) Jsou prvky $1 - \sqrt{5}$ a $-199 - 89\sqrt{5}$ asociované.

(1) Prvek $u \in \mathbb{Z}[\sqrt{5}], u = a + b\sqrt{5}$, je jednotka, právě když $\upsilon(u) = 1$, tj. právě když $|a^2 - 5b^2| = 1$. Uvažujme nejprve prvek $u = 2 + \sqrt{5}$. Pak $\upsilon(u) = |4 - 5 \cdot 1| = 1$, a tedy u je

jednotka v $\mathbb{Z}[\sqrt{5}]$.

Podle Věty 2.2 tvrzení (2) ovšem také $(2+\sqrt{5})^n, n \in \mathbb{Z}$, je jednotka v $\mathbb{Z}[\sqrt{5}]$.

(2) Nechť $x = 1-\sqrt{5}, y = -199-89\sqrt{5}$. Prvky x, y jsou asociované v $\mathbb{Z}[\sqrt{5}]$, právě když $x \mid y \wedge y \mid x$.

$\frac{x}{y} = \frac{1-\sqrt{5}}{-199-89\sqrt{5}} = \frac{1-\sqrt{5}}{-199-89\sqrt{5}} \cdot \frac{-199+89\sqrt{5}}{-199+89\sqrt{5}} = \frac{-644+288\sqrt{5}}{-4} = 161-72\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$, tj. $y \mid x$.

$\frac{y}{x} = \frac{-199-89\sqrt{5}}{1-\sqrt{5}} = \frac{-199-89\sqrt{5}}{1-\sqrt{5}} \cdot \frac{1+\sqrt{5}}{1+\sqrt{5}} = \frac{-644-288\sqrt{5}}{-4} = 161+72\sqrt{5} \in \mathbb{Z}[\sqrt{5}]$, tj. $x \mid y$.

Příklad 2.33. Dokažte, že v oboru integrity $\mathbb{Z}[\sqrt{3}]$.

(1) Je prvek $(2+\sqrt{3})^n, n \in \mathbb{Z}$, jednotka.

(2) Jsou prvky $3-2\sqrt{3}$ a $45+26\sqrt{3}$ asociované.

(1) Prvek $u = 2+\sqrt{3}$ je jednotka v $\mathbb{Z}[\sqrt{3}]$, právě když je invertibilní, tj. existuje prvek $u^{-1} \in \mathbb{Z}[\sqrt{3}]$ tak, že $u \cdot u^{-1} = 1$.

Je-li $u = 2+\sqrt{3}$, pak $u^{-1} = \frac{1}{2+\sqrt{3}} = \frac{1}{2+\sqrt{3}} \cdot \frac{2-\sqrt{3}}{2-\sqrt{3}} = 2-\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$. Tedy $u = 2+\sqrt{3}$ je jednotka v $\mathbb{Z}[\sqrt{3}]$.

Podle Věty 2.2 tvrzení (2) je i $(2+\sqrt{3})^n, n \in \mathbb{Z}$, jednotka v $\mathbb{Z}[\sqrt{3}]$.

(2) Nechť $x = 3-2\sqrt{3}, y = 45+26\sqrt{3} \in \mathbb{Z}[\sqrt{3}]$. Prvky x a y jsou asociované v $\mathbb{Z}[\sqrt{3}]$, právě když existuje jednotka $j \in \mathbb{Z}[\sqrt{3}]$ tak, že $y = x \cdot j$.

$\frac{45+26\sqrt{3}}{3-2\sqrt{3}} = \frac{45+26\sqrt{3}}{3-2\sqrt{3}} \cdot \frac{3+2\sqrt{3}}{3+2\sqrt{3}} = \frac{291+168\sqrt{3}}{-3} = -97-56\sqrt{3}$.

Zároveň $-97-56\sqrt{3} = -(2+\sqrt{3})^4$ a $-(2+\sqrt{3})^4$ je jednotka v $\mathbb{Z}[\sqrt{3}]$, tedy $x \parallel y$.

Příklad 2.34. Nalezněte největší společný dělitel, koeficienty c_1, c_2 v Bezoutově rovnosti a nejmenší společný násobek čísel $a, b \in \mathbb{Z}[\sqrt{2}]$, jestliže:

$a = 22+14\sqrt{2}, \quad b = 9-\sqrt{2}$.

(1) $\frac{22+14\sqrt{2}}{9-\sqrt{2}} \cdot \frac{9+\sqrt{2}}{9+\sqrt{2}} = \frac{226}{77} + \frac{148}{77}\sqrt{2}$

$|\frac{226}{77} - q_1| \leq \frac{1}{2} \qquad |\frac{148}{77} - q_2| \leq \frac{1}{2} \Rightarrow q_1 = 3, q_2 = 2 \Rightarrow Q_1 = 3+2\sqrt{2}$

$\bullet R_1 = r_1 + r_2\sqrt{2} = (22+14\sqrt{2}) - (9-\sqrt{2}) \cdot (3+2\sqrt{2}) = -1-\sqrt{2}$

$\frac{9-\sqrt{2}}{-1-\sqrt{2}} \cdot \frac{-1+\sqrt{2}}{-1+\sqrt{2}} = 11-10\sqrt{2} = q' = q'_1 + q'_2\sqrt{2}$, tedy $r' = r'_1 + r'_2\sqrt{2} = 0$

Pak $D(a,b) = -1-\sqrt{2}$.

(2) $a = b \cdot q + r \Rightarrow r = a - b \cdot q = a - b(3+2\sqrt{2}) = D(a,b), c_1 = 1, c_2 = -3-2\sqrt{2}$.

(3) $[a,b] = \frac{(22+14\sqrt{2})(9-\sqrt{2})}{-1-\sqrt{2}} \cdot \frac{-1+\sqrt{2}}{-1+\sqrt{2}} = -38+66\sqrt{2}$

Příklad 2.35. Nalezněte největší společný dělitel, koeficienty c_1, c_2 v Bezoutově rovnosti a nejmenší společný násobek čísel $a, b \in \mathbb{Z}[\sqrt{2}]$, jestliže:
$a = 21+4\sqrt{2}, \quad b = 36+7\sqrt{2}.$

(1) $\frac{36+7\sqrt{2}}{21+4\sqrt{2}} \cdot \frac{21-4\sqrt{2}}{21-4\sqrt{2}} = \frac{700}{409} + \frac{3}{409}\sqrt{2}$

$|\frac{700}{409} - q_1| \leq \frac{1}{2} \qquad |\frac{3}{409} - q_2| \leq \frac{1}{2} \Rightarrow q_1 = 2, q_2 = 0 \Rightarrow Q_1 = 2$

$\bullet R_1 = r_1 + r_2\sqrt{2} = (36+7\sqrt{2}) - (21+4\sqrt{2}) \cdot (2) = -6-\sqrt{2}$

$\frac{21+4\sqrt{2}}{-6-\sqrt{2}} \cdot \frac{-6+\sqrt{2}}{-6+\sqrt{2}} = -\frac{118}{34} - \frac{3}{34}\sqrt{2}$

$|\frac{-118}{34} - q_1'| \leq \frac{1}{2} \qquad |\frac{-3}{34} - q_2'| \leq \frac{1}{2} \Rightarrow q_1' = -3, q_2' = 0 \Rightarrow Q_2 = -3$

$\bullet R_2 = r_1' + r_2'\sqrt{2} = (21+4\sqrt{2}) - (-6-\sqrt{2}) \cdot (-3) = 3+\sqrt{2}$

$\frac{-6-\sqrt{2}}{3+\sqrt{2}} \cdot \frac{3-\sqrt{2}}{3-\sqrt{2}} = -\frac{16}{7} + \frac{3}{7}\sqrt{2}$

$|-\frac{16}{7} - q_1''| \leq \frac{1}{2} \qquad |\frac{3}{7} - q_2''| \leq \frac{1}{2} \Rightarrow q_1'' = -2, q_2'' = 0 \Rightarrow Q_3 = -2$

$\bullet R_3 = r_1'' + r_2''\sqrt{2} = (-6-\sqrt{2}) - (3+\sqrt{2}) \cdot (-2) = \sqrt{2}$

$\frac{3+\sqrt{2}}{\sqrt{2}} \cdot \frac{\sqrt{2}}{\sqrt{2}} = 1 + \frac{3}{2}\sqrt{2}$

$|1 - q_1'''| \leq \frac{1}{2} \qquad |\frac{3}{2} - q_2'''| \leq \frac{1}{2} \Rightarrow q_1''' = 1, q_2''' = 1 \Rightarrow Q_4 = 1+\sqrt{2}$

$\bullet R_4 = r_1''' + r_2'''\sqrt{2} = (3+\sqrt{2}) - \sqrt{2} \cdot (1+\sqrt{2}) = 1$

Tedy $D(a,b) = 1$

(2)

$$b = a \cdot q + r \Rightarrow r = b - aq = b - 2a$$

$$a = r \cdot q' + r' \Rightarrow r' = a - rq' = a - (b-2d)(-3) = -5a + 3b$$

$$r = r'q'' + r'' \Rightarrow r''c = r - r'q'' = b - 2a - (-5a+3b)(-2) = -12a + 7b$$

$$r' = r''q''' + r''' \Rightarrow r''' = r' - r''q'' = -5a + 3b - (-12a+7b) \cdot (1+\sqrt{2}) =$$

$$= -5a + 3b + 12a(1+\sqrt{2}) - 7b(1+\sqrt{2}) = a(7+12\sqrt{2}) + b(-4-7\sqrt{2}).$$

Tedy $c_1 = 7+12\sqrt{2} \quad c_2 = -4-7\sqrt{2}$.

(3) $[a,b] = \frac{(21+4\sqrt{2})(36+7\sqrt{2})}{1} = 812+291\sqrt{2}$

Závěr

Ve své bakalářské práci jsem vytvořila přehled základních pojmů z okruhů teorie dělitelnosti v oboru integrity a objastnila jsem uvedené pojmy na příkladech.

Cílem bylo spojit matematické věty s algebraickými důkazy a příslušnými příklady. V první kapitele jsem se zaměřila na pojmy z teorie okruhů. Ve druhé kapitole na dokazování vět.

Prohloubila jsem si znalosti z oboru integrity struktur s jednou a se dvěmi operacemi. Na konkrétních příkladech jsem si procvičila dokazování vět. Práce mi přinesla pochopení pro nalezení největšího společného dělitele a nejmenšího společného násobku v $\mathbb{Z}[i]$. Získané poznatky budu moci uplatnit v dalším studiu, případně v praxi.

Seznam použité literatury

[1] BLAŽEK, Jaroslav a Milan KOMAN, VOJTÁŠKOVÁ, Blanka, *Algebra a teoretická aritmetika*. Praha: Státní pedagogické nakladatelství, 1985. Učebnice pro vysoké školy (Státní pedagogické nakladatelství).

[2] STANOVSKÝ, David. *Základy algebry*. Praha: Matfyzpress, 2010. ISBN 978-80-7378-105-7.

[3] BICAN, Ladislav. *Algebra (pro učitelské studium)*. Praha: Academia, 2001. ISBN 80-200-0860-8.

[4] HEFLER, Stanislav. *Příklady na dělitelnost v oborech integrity*. Plzeň, 2013, 65s. Bakalářská práce. Západočeská univerzita v Plzni. Pedagogická fakulta. Vedoucí práce Doc. RNDr. Jaroslav Hora, CSc.