VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA STROJNÍHO INŽENÝRSTVÍ
ÚSTAV MATEMATIKY

FACULTY OF MECHANICAL ENGINEERING
INSTITUTE OF MATHEMATICS

ZÁKLADY KVADRATICKÝCH TĚLES

FUNDAMENTALS OF QUADRATIC FIELDS

BAKALÁŘSKÁ PRÁCE
BACHELOR'S THESIS

AUTOR PRÁCE — VOJTĚCH IVIČIČ
AUTHOR

VEDOUCÍ PRÁCE — prof. RNDr. LADISLAV SKULA, DrSc.
SUPERVISOR

BRNO 2011

Vysoké učení technické v Brně, Fakulta strojního inženýrství

Ústav matematiky
Akademický rok: 2010/2011

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

student(ka): Vojtěch Ivičič

který/která studuje v **bakalářském studijním programu**

obor: **Matematické inženýrství (3901R021)**

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách a se Studijním a zkušebním řádem VUT v Brně určuje následující téma bakalářské práce:

Základy kvadratických těles

v anglickém jazyce:

Fundamentals of quadratic fields

Stručná charakteristika problematiky úkolu:

Úkolem této bakalářské práce je prezentovat základy kvadratických těles. Předpokládá se, že v úvodní části budou vysvětleny pojmy z oblasti kongruence modulo celé číslo větší než 1, polynomy nad tělesem a oborem integrity a uvedeny vlastnosti dělitelnosti těchto polynomů.
Hlavní část práce bude zaměřena na výklad kvadratického rozšíření tělesa racionálních čísel, celá čísla tohoto tělesa a na jejich vlastnosti týkající se dělitelnosti. Tato část se bude také týkat specielních kvadratických těles, zejména Gaussova tělesa a Gaussových celých čísel a bude pojednávat o kvadratických tělesech, ve kterých platí jednoznačnost rozkladu celého čísla na algebraická prvočísla.
Závěr práce bude věnován pojmu ideálu kvadratického tělesa.

Cíle bakalářské práce:

Autor práce by měl dokázat, že zvládl oblast obecné algebry týkající se polynomů nad tělesem, kvadratického rozšíření tělesa a aritmetiky okruhu celých čísel kvadratického tělesa.

Seznam odborné literatury:

1)Š.Schwarz, Algebraické čísla, JČMF, Praha, 1950.
2)J.Karásek, L.Skula, Obecná algebra, VUT Brno, 2008.
3) O.Borůvka, Základy teorie grupoidů a grup, ČSAV, Praha, 1962.
4)K.Ireland, M.Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, New York, 1982.

Vedoucí bakalářské práce: prof. RNDr. Ladislav Skula, DrSc.

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2010/2011.

V Brně, dne 18.11.2010

L.S.

prof. RNDr. Josef Šlapal, CSc. Ředitel ústavu	prof. RNDr. Miroslav Doupovec, CSc. Děkan fakulty

Abstrakt

Cílem práce je popsat základy kvadratických těles. Úvodní kapitoly jsou zaměřeny na aritmetiku celých čísel a polynomů. V hlavní části se zabýváme pojmem kvadratického tělesa, celým algebraickým číslům tohoto tělesa, Gaussovu tělesu a Gaussovým celým číslům. Závěr je věnován kvadratickým tělesům, kde neplatí jednoznačnost rozkladu, a řešení tohoto problému pomocí ideálů.

Summary

The aim of the thesis is to describe the fundamentals of quadratic fields. In the first part integer and polynomial arithmetic is mentioned. The main part discusses the topic of quadratic field, quadratic integer, Gaussian field and Gaussian integer. The final part deals with quadratic fields without unique factorization and a solution of the problem through ideals.

Klíčová slova

Aritmetika celých čísel, aritmetika polynomů, kvadratické těleso, celé algebraické číslo kvadratického tělesa, Gaussovo celé číslo, diofantická rovnice

Keywords

Integer arithmetic, polynomial arithmetic, quadratic field, quadratic integer, Gaussian integer, Diophantine equation

IVIČIČ, V. *Základy kvadratických těles*. Brno: Vysoké učení technické v Brně, Fakulta strojního inženýrství, 2011. 35 s. Vedoucí prof. RNDr. Ladislav Skula, DrSc.

Prohlašuji, že jsem bakalářskou práci *Základy kvadratických těles* vypracoval samostatně pod vedením prof. RNDr. Ladislava Skuly, DrSc. s použitím materiálů uvedených v seznamu literatury.

Vojtěch Ivičič

Děkuji svému školiteli prof. RNDr. Ladislavu Skulovi, DrSc. za vedení mé bakalářské práce

Vojtěch Ivičič

Obsah

1. Úvod

Kvadratická tělesa se používají při řešení diofantických rovnic. Cílem této práce je popsat jejich základní vlastnosti, vlastnosti dělitelnosti a na závěr problém nejednoznačnosti rozkladu v součin prvočinitelů.

Tato práce je zpracována podle metod [3] a [2]. Základní studijní literaturou bylo [6], jako doplnění informací [1]. Dále na základy aritmetiky celých čísel jsem použil [4] a pro podrobnější poznatky o kvadratických tělesech [5].

Text práce je rozdělen na úvod, 4 hlavní kapitoly a závěr. Na konci každé kapitoly jsou řešené příklady. Ty osvětlují, jak se v praxi používá vysvětlená teorie.

Ve druhé kapitole se zabýváme aritmetikou celých čísel. Položíme základy dělitelnosti, definujeme si zde největšího společného dělitele a Euklidův algoritmus, kterým můžeme největšího společného dělitele nalézt. První část kapitoly zakončíme větou o jednoznačnosti rozkladu celého čísla na prvočísla, další část věnujeme vlastnostem kongruence modulo celé číslo větší než 1.

Třetí kapitola je zaměřena na vlastnosti dělitelnosti polynomů nad tělesem. Podobně jako u celých čísel zavedeme největšího společného dělitele, tentokrát dvou polynomů a Euklidův algoritmus pro polynomy. Kapitolu uzavřeme větou o jednoznačnosti rozkladu polynomu na ireducibilní polynomy.

Následující, stěžejní kapitola této práce se týká kvadratického tělesa. Nejdříve si definujeme kvadratické těleso, jeho celá algebraická čísla a dále zkoumáme tvar těchto čísel. Obsahem třetí části této kapitoly je dělitelnost v okruhu celých čísel kvadratického tělesa a nalezení všech jednotek těchto těles.

Pátá kapitola je věnována speciálnímu kvadratickému tělesu, a to Gaussova tělesu. Zavádíme zde Gaussova čísla a popisujeme zákony dělitelnosti. Opět můžeme definovat největšího společného dělitele dvou Gaussových čísel a nakonec dokážeme větu o jednoznačnosti rozkladu Gaussova čísla na Gaussova prvočísla.

Tato věta ovšem neplatí obecně ve všech kvadratických tělesech. Tímto problémem se zabýváme v závěru. Uvedeme zde, co jsou jednoduchá tělesa a kolik jich existuje. Dále se snažíme nejednoznačnost rozkladu nějak vyřešit. K tomuto účelu zavádíme ideály z oboru integrity celých algebraických čísel kvadratického tělesa. Nakonec uvedeme větu o jednoznačnosti rozkladu ideálu na prvoideály.

2. Některé příklady aritmetiky celých čísel

2.1. Rozklad celého čísla na prvočísla

Definice 1. Nechť a, b jsou celá čísla a $b \neq 0$. Řekneme, že číslo a je *dělitelné* číslem b, jestliže existuje celé číslo q takové, že $a = bq$. Stručně označujeme $b \mid a$.

Poznámka. Věty $1 - 14$ jsou všeobecně známé, proto jsou zde prezentovány bez důkazů.

Věta 1. *Nechť $a, b, c \in \mathbb{Z}$, $b \mid a$ a $c \mid b$, pak $c \mid a$.*

Věta 2. *Nechť $a, b, c \in \mathbb{Z}$, $bc \mid ac$ a $c \neq 0$, pak platí $b \mid a$.*

Věta 3. *Nechť $a, b, c \in \mathbb{Z}$, $c \mid a$ a $c \mid b$, potom pro libovolná čísla x, $y \in \mathbb{Z}$ platí*

$$c \mid ax + by.$$

Definice 2. Nechť ε je celé číslo a $\varepsilon \mid 1$, pak ε nazýváme *jednotkou*.

Věta 4. *V celých číslech tedy máme dvě jednotky,* 1 *a* -1.

Definice 3. Řekneme, že celá čísla a a b jsou *asociovaná*, jestliže platí $a = b\varepsilon$, kde ε je jednotka.

Věta 5. *Celá čísla a a b jsou asociovaná, právě když $a \mid b$ a zároveň $b \mid a$.*

Věta 6. *Nechť $a_1, a_2, b_1, b_2 \in \mathbb{Z}$, a_1 je asociované k a_2, b_1 je asociované k b_2 a $a_1 \mid b_1$. Potom platí $a_2 \mid b_2$.*

Věta 7. *Nechť $a, b \in \mathbb{Z}$, $b \mid a$ a $a \neq 0$, pak $|a| \geq |b|$. Rovnost $|a| = |b|$ platí, právě když a a b jsou asociované.*

Definice 4. Nechť p je celé číslo, $|p| > 1$. Pokud je p dělitelné jen čísly k němu asociovanými a jedničkou, nazveme toto číslo *prvočíslem*.

Věta 8. *Nechť $a, b \in \mathbb{Z}$, $b \neq 0$. Pak existují celá čísla q a r tak, že platí*

$$a = bq + r,\ 0 \leq r < |b|.$$

Dvojice čísel q a r je určena jednoznačně.

Definice 5. Nechť $a, b, c \in \mathbb{Z}$. Číslo c nazýváme *společným dělitelem* čísel a a b, když platí $c \mid a$ a $c \mid b$.

Definice 6. Nechť $a, b, d \in \mathbb{Z}$. Číslo d nazýváme *největším společným dělitelem* čísel a a b, když platí

(a) d je společným dělitelem čísel a a b,

(b) pro každého dalšího společného dělitele d' čísel a a b platí $d' \mid d$.

Věta 9. *Pro každé dvě celá čísla $a \neq 0$, $b \neq 0$ existuje celé číslo d, které je jejich největším společným dělitelem. Číslo d je až na asociovanost jednoznačné.*

Poznámka. Nezápornou hodnotu největšího společného dělitele d celých čísel a a b budeme označovat symbolem $d = (a, b)$. Můžeme ji určit pomocí Euklidova algoritmu.

Euklidův algoritmus. Nechť $a, b \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$, $a \geq b$. Podle věty 8 můžeme sestavit systém rovnic

$$\begin{aligned} a &= bq_0 + r_0, 0 < r_0 < |b|, \\ b &= r_0q_1 + r_1, 0 < r_1 < r_0, \\ r_0 &= r_1q_2 + r_2, 0 < r_2 < r_1, \\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_nq_{n+1}, \end{aligned}$$

kde $n \in \mathbb{N}$, $q_0, q_1, \ldots, q_{n+1}, r_0, r_1, \ldots, r_{n+1} \in \mathbb{Z}$. Protože $|b| > r_0 > r_1 > \cdots > r_n > r_{n+1}$ je klesající posloupnost nezáporných celých čísel, musí existovat n, pro které $r_{n+1} = 0$. Číslo r_n je pak největší společný dělitel čísel a a b.

Věta 10. *Nechť $a, b \in \mathbb{Z}$ a $d = (a, b)$ je jejich největším společným dělitelem. Pak existují celá čísla x a y, pro která platí*

$$ax + by = d.$$

Definice 7. Řekneme, že celá čísla a a b jsou *nesoudělná*, jestliže $(a, b) = 1$.

Věta 11. *Nechť $a, b, c \in \mathbb{Z}$, $(a, b) = 1$ a $a \mid bc$, pak $a \mid c$.*

Věta 12. *Nechť $a, b \in \mathbb{Z}$, p je prvočíslo a $p \mid ab$. Pak platí aspoň jeden ze vztahů $p \mid a$ a $p \mid b$.*

Věta 13. *Nechť $a_1, a_2, \ldots, a_k \in \mathbb{Z}$, p je prvočíslo a $p \mid a_1a_2 \ldots a_k$. Číslo p pak dělí alespoň jedno z čísel a_i.*

Věta 14. *Nechť $a \in \mathbb{Z}$ a $|a| > 1$, pak se číslo a dá rozložit v součin konečného počtu prvočísel. Tento rozklad je až na pořadí a asociativitu dělitelů jednoznačný.*

2.2. Kongruence modulo m v $\mathbb{Z}$

Definice 8. Nechť a, b, m jsou celá čísla a $m > 0$. Řekneme, že a je *kongruentní s b modulo m*, jestliže $m \mid a - b$. Krátce značíme $a \equiv b \pmod{m}$.

Věta 15. *Nechť $a, b, c, m \in \mathbb{Z}$, potom platí:*

(a) $a \equiv a \pmod{m}$.

(b) $a \equiv b \pmod{m} \implies b \equiv a \pmod{m}$.

(c) $a \equiv b \pmod{m}$ a $b \equiv c \pmod{m} \implies a \equiv c \pmod{m}$.

Důkaz. (a) Podle definice $m \mid a - a$, tj. $m \mid 0$.

(b) Když $m \mid a - b$, pak i $m \mid b - a$.

(c) Když $m \mid a - b$ a $m \mid b - c$, pak $m \mid (a - b) + (b - c)$ a tedy $m \mid a - c$. □

Důsledek věty 15: Kongruence je relace reflexivní, symetrická a transitivní, je to tedy relace ekvivalence.

Definice 9. Nechť $a \in \mathbb{Z}$ a $\bar{a}$ označme množinu všech celých čísel kongruentních k a podle modulu m. Pak $\bar{a}$ se nazývá *třída kongruence modulo* m. Tyto třídy kongruence modulo m jsou právě třídy rozkladu příslušného relaci ekvivalence $\equiv \pmod{m}$.

Věta 16. *Tříd kongruence modulo m je přesně m.*

Důkaz. Nechť $\bar{0}, \bar{1}, \ldots, \overline{m-1}$ jsou třídy kongruence modulo m. Předpokládejme, že $0 \leq k, l < m$ a $\bar{k} = \bar{l}$. Tedy $k \equiv l \pmod{m} \implies m \mid l - k$. To ale platí jen pokud $l - k = 0$ (protože $0 \leq |l - k| < m$). Proto $k = l$ a všech m tříd kongruence je různých.

Nyní nechť $a \in \mathbb{Z}$. Existují celá čísla q a r, pro která platí $a = mq + r$, kde $0 \leq r < m$, tj. $a \equiv r \pmod{m}$. Každé celé číslo patří do jedné z m tříd kongruence. □

Věta 17. *Nechť $a, b, c, d, m \in \mathbb{Z}$. Když platí $a \equiv c \pmod{m}$ a $b \equiv d \pmod{m}$, pak platí*

(a) $a + b \equiv c + d \pmod{m}$,

(b) $ab \equiv cd \pmod{m}$.

Důkaz. (a) Když $m \mid a - c$ a $m \mid b - d$, pak podle věty 3 máme $m \mid (a - c) + (b - d)$, tedy $m \mid (a + b) - (c + d)$ a $a + b \equiv c + d \pmod{m}$.

(b) Opět podle věty 3 dostáváme $m \mid b(a - c) + c(b - d)$, tj. $m \mid ab - cd$, z čehož plyne $ab \equiv cd \pmod{m}$. □

Věta 18. *Nechť $a, b, m \in \mathbb{Z}$, $ab \equiv 0 \pmod{m}$ a $(m, b) = 1$, pak platí $a \equiv 0 \pmod{m}$.*

Důkaz. $m \mid ab$, $(m, b) = 1$, podle věty 11 dostáváme $m \mid a$. □

Věta 19. *Nechť $a, b \in \mathbb{Z}$, $ab \equiv 0 \pmod{p}$ a $p > 1$ je prvočíslo, pak platí alespoň jeden ze vztahů $a \equiv 0 \pmod{p}$ a $b \equiv 0 \pmod{p}$.*

Důkaz. $p \mid ab$, podle věty 12 číslo p dělí aspoň jedno z čísel a a b. □

Věta 20. *Nechť $a, b, c, m \in \mathbb{Z}$, $ac \equiv bc \pmod{m}$ a $(c, m) = 1$, pak $a \equiv b \pmod{m}$.*

Důkaz. $m \mid ac - bc$, tj. $m \mid c(a - b)$, podle věty 11 máme $m \mid a - b$. □

Věta 21. *Nechť $a, b, c, d, m \in \mathbb{Z}$, $ac \equiv bc \pmod{m}$ a $(c, m) = d$, pak $a \equiv b \pmod{\frac{m}{d}}$.*

Důkaz. $m \mid c(a - b)$, čísla c i m jsou dělitelné číslem d, takže můžeme psát $\frac{m}{d} \mid \frac{c}{d}(a - b)$. $(\frac{m}{d}, \frac{c}{d}) = 1$, podle věty 11 máme $\frac{m}{d} \mid (a - b)$. □

Definice 10. *Úplným systémem zbytků podle modulu m* nazýváme množinu m celých čísel $r_1, r_2, \ldots, r_m$, jestliže každé z těchto čísel patří do jiné třídy kongruence podle modulu m.

Věta 22. *Mějme prvočíslo p a úplný systém zbytků modulo p*

$$r_1, r_2, \ldots, r_p.$$

Pak pro každé $a \in \mathbb{Z}$ nesoudělné s p je i

$$ar_1, ar_2, \ldots, ar_p$$

úplný systém zbytků modulo p.

Důkaz. Provedeme sporem. Předpokládejme, že $ar_i \equiv ar_j \pmod{p}$, pro nějaké i, j, $1 \leq i, j \leq p$, $i \neq j$. Rovnici upravíme na $a(r_i - r_j) \equiv 0 \pmod{p}$. p je prvočíslo, můžeme použít větu 19 a dostáváme $r_i - r_j \equiv 0 \pmod{p}$, tj. $r_i \equiv r_j \pmod{p}$. Z toho plyne, že $r_1, r_2, \ldots, r_p$ netvoří úplný systém zbytků a to je spor s předpokladem. □

Věta 23. *Nechť $a, b, x \in \mathbb{Z}$, p je prvočíslo. Potom má kongruence*

$$ax \equiv b \pmod{p}, \quad (a, p) = 1 \tag{2.1}$$

právě jedno řešení.

Poznámka. Za různé nebudeme považovat řešení ležící ve stejné třídě kongruence.

Důkaz. 1. Existence. Nechť

$$0, 1, 2, \ldots p - 1.$$

je úplný systém zbytků modulo p. Podle věty 22 je úplný systém zbytků modulo p i

$$0, a, 2a, \ldots, (p-1)a.$$

Můžeme tedy najít celé číslo x, pro které xa patří do stejné třídy kongruence jako b, tj. platí $ax \equiv b \pmod{p}$. Číslo x je proto řešením kongruence 2.1.

2. Jednoznačnost. Mějme celá čísla x_1 a x_2, splňující kongruenci 2.1, tj. $ax_1 \equiv b \pmod{p}$ a $ax_2 \equiv b \pmod{p}$. Odečtením dostáváme $a(x_1 - x_2) \equiv 0 \pmod{p}$ a podle věty 19 máme $x_1 - x_2 \equiv 0 \pmod{p}$. To znamená, že čísla x_1 a x_2 patří do stejné třídy kongruence a nepovažujeme je za různá.

□

Malá Fermatova věta. *Nechť $a \in \mathbb{Z}$, p je prvočíslo a a a p jsou nesoudělná, tj. $(a, p) = 1$. Pak platí*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Důkaz. Nechť je množina

$$0, 1, 2, \ldots p - 1. \tag{2.2}$$

úplný systém zbytků modulo p. Podle věty 22 je úplný systém zbytků modulo p i

$$0, a, 2a, \ldots, (p-1)a,$$

která je permutací množiny 2.2, to znamená, že můžeme psát

$$\begin{aligned} a &\equiv r_1 \pmod p, \\ 2a &\equiv r_2 \pmod p, \\ &\vdots \\ (p-1)a &\equiv r_{p-1} \pmod p, \end{aligned}$$

kde $r_1, r_2, \ldots, r_{p-1}$ jsou až na pořadí čísla $0, 1, 2, \ldots p-1$. Nyní rovnice vynásobíme a dostáváme

$$(p-1)!a^{p-1} \equiv (p-1)! \pmod p$$

Číslem $(p-1)!$ můžeme kongruenci vykrátit, protože $(p, (p-1)!) = 1$, a máme tedy

$$a^{p-1} \equiv 1 \pmod p.$$

□

2.3. Příklady

Poznámka. Nevyřešené příklady v celé této práci jsou přebrány z [3] a [6].

Příklad 2.1. Dokažte, že součet čtverců dvou lichých čísel nemůže být čtvercem žádného celého čísla.

Řešení. Nechť $a = 2k_1 + 1, b = 2k_2 + 1$ jsou lichá čísla, $c, k_1, k_2 \in \mathbb{Z}$. Máme dokázat, že $a^2 + b^2 \neq c^2$ pro žádné a, b, c.

$$a^2 + b^2 = (2k_1 + 1)^2 + (2k_2 + 1)^2 = 4(k_1^2 + k_1 + k_2^2 + k_2) + 2$$

Součet $a^2 + b^2$ je sudý, předpokládejme tedy číslo c ve tvaru $c = 2k_3$, $k_3 \in \mathbb{Z}$.

$$c^2 = 4k_3^2$$

Rovnice

$$4(k_1^2 + k_1 + k_2^2 + k_2) + 2 = 4k_3^2$$

ale nemá řešení pro $k_1, k_2, k_3 \in \mathbb{Z}$. □

Příklad 2.2. Najděte největšího společného dělitele čísel $444, 252$. Vyjádřete potom $(444, 252)$ ve tvaru $444x + 252y$.

Řešení. K nalezení největšího společného dělitele použijeme Euklidův algoritmus. Sestavíme systém rovnic

$$\begin{aligned} 444 &= 1 \times 252 + 192 \\ 252 &= 1 \times 192 + 60 \\ 192 &= 3 \times 60 + 12 \\ 60 &= 5 \times 12. \end{aligned}$$

Poslední nenulový zbytek je 12, tedy $(444, 252) = 12$. Úpravou rovnic Euklidova algoritmu dostáváme

$$\begin{aligned} 192 &= 444 - 252 \\ 60 &= 252 - 192 = 252 \times 2 - 444 \\ 12 &= 192 - 60 \times 3 = 444 - 252 - 252 \times 6 + 444 \times 3 = 444 \times 4 - 252 \times 7. \end{aligned}$$

□

Příklad 2.3. Nechť $a, b, m, m_1 \in \mathbb{Z}$. Dokažte, že když $a \equiv b \pmod{m}$ a $m_1 \mid m$, pak $a \equiv b \pmod{m_1}$.

Řešení. Podle definice kongruence a dělení máme $m \mid a - b$,

$$\begin{aligned} &m \times q_1 = a - b, && m_1 \times q_2 = m, \qquad q_1, q_2 \in \mathbb{Z}, \\ &m_1 \times q_2 \times q_1 = a - b. \end{aligned}$$

Z toho plyne, že $m_1 \mid a - b$ a tedy $a \equiv b \pmod{m}$. □

Příklad 2.4. Dokažte, že když je m celé číslo, potom platí $m^2 \equiv 0 \pmod 4$ nebo $m^2 \equiv 1 \pmod 4$.

Řešení. Kongruence modulo 4 nám rozloží celá čísla na 4 třídy a pomocí věty 17 umocníme na druhou:

$$\begin{aligned} m &\equiv 0 \pmod 4 & m^2 &\equiv 0 \pmod 4 \\ m &\equiv 1 \pmod 4 & m^2 &\equiv 1 \pmod 4 \\ m &\equiv 2 \pmod 4 & m^2 &\equiv 0 \pmod 4 \\ m &\equiv 3 \pmod 4 & m^2 &\equiv 1 \pmod 4. \end{aligned}$$

□

Příklad 2.5. Dokažte, že když je m celé číslo nedělitelné číslem 5, potom platí $m^2 \equiv 1 \pmod 5$ nebo $m^2 \equiv 4 \pmod 5$.

Řešení. Kongruence modulo 5 nám rozloží celá čísla na 5 tříd, z nichž jednu vynecháme (obsahující čísla dělitelná 5) a pomocí věty 17 umocníme na druhou:

$$\begin{aligned} m &\equiv 1 \pmod 5 & m^2 &\equiv 1 \pmod 5 \\ m &\equiv 2 \pmod 5 & m^2 &\equiv 4 \pmod 5 \\ m &\equiv 3 \pmod 5 & m^2 &\equiv 4 \pmod 5 \\ m &\equiv 4 \pmod 5 & m^2 &\equiv 1 \pmod 5. \end{aligned}$$

□

Příklad 2.6. Řešte kongruence:

(a) $3x + 2 \equiv 0 \pmod 5$,

(b) $4x + 3 \equiv 4 \pmod 7$.

Řešení. (a) Použijeme větu 17:

$$\begin{aligned} 3x + 2 &\equiv 0 \pmod 5 \quad / \times 2 \\ x + 4 &\equiv 0 \pmod 5 \\ x &\equiv 1 \pmod 5, \end{aligned}$$

(b)

$$\begin{aligned} 4x + 3 &\equiv 4 \pmod 7 \quad / \times 2 \\ x + 6 &\equiv 1 \pmod 7 \\ x &\equiv 2 \pmod 7. \end{aligned}$$

□

Příklad 2.7. Dokažte, že kongruence $2x \equiv 5 \pmod 4$ nemá řešení.

Řešení. Z definice kongruence máme $4 \mid 2x-5$. Tento výraz ale nemá řešení pro $x \in \mathbb{Z}$. □

Příklad 2.8. Řešte kongruenci $3x \equiv 9 \pmod{15}$.

Řešení. Použijeme větu 21, $d = (3, 15) = 3$, kongruenci můžeme vydělit číslem 3:

$$\begin{aligned} 3x &\equiv 9 \pmod{15} \quad /3 \\ x &\equiv 3 \pmod 5. \end{aligned}$$

□

3. Některé příklady aritmetiky polynomů nad tělesem

3.1. Základní věty o dělitelnosti polynomů

Definice 11. Nechť T je těleso, $p(x)$ je polynom ve tvaru

$$p(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n,$$

kde $a_0 \neq 0$, $a_i \in T$, pro $i = 0, 1, \ldots n$. Polynom p pak nazveme *polynomem n-tého stupně nad tělesem T*.

Poznámka. Budete předpokládat, že známe pojmy těleso, polynom a stupeň polynomu a umíme polynomy násobit a sčítat.

Definice 12. Nechť T je těleso, $a(x), b(x)$ jsou polynomy nad tělesem T. Řekneme, že *polynom $a(x)$ je dělitelný polynomem $b(x)$*, jestliže existuje polynom $q(x)$ nad tělesem T takový, že platí

$$a(x) = b(x)q(x).$$

Stručně značíme $b(x) \mid a(x)$.

Poznámka. Dělitelnost polynomů má analogické vlastnosti jako dělitelnost celých čísel. Proto některé věty vynecháme a zaměříme se jen na věty pro nás důležitější. Stejně tak vynecháme definici asociovanosti, jednotkových (konstantních) polynomů, nesoudělnosti a největšího společného dělitele.

Věta 24. *Nechť T je těleso, $a(x), b(x)$ jsou polynomy nad tělesem T a $b(x) \neq 0$. Pak existují polynomy $q(x), r(x)$ nad tělesem T takové, že*

$$a(x) = b(x)q(x) + r(x),$$

kde $r(x)$ je polynom, jehož stupeň je nižší než stupeň polynomu $b(x)$. Dvojice polynomů $q(x)$ a $r(x)$ je určena jednoznačně.

Důkaz. 1. Existence. Nechť

$$a(x) = a_0x^m + a_1x^{m-1} + \cdots + a_{m-1}x + a_m,$$
$$b(x) = b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n.$$

Předpokládejme nejprve, že $n > m$. Potom položíme $q(x) = 0, r(x) = a(x)$.

V opačném případě, tj. když $n \leq m$, odečteme od sebe polynom $a(x)$ a $b(x)$ vynásobený mocninou x^{m-n} a koeficientem $c_0 = \frac{a_0}{b_0}$:

$$a(x) - c_0x^{m-n}b(x) = a_1(x)$$

Tím jsme dostali polynom $a_1(x)$, který má stupeň $m_1 < m$. Takto sestrojujeme pomocí vhodných koeficientů c_i a mocnin x^{j_i} $(j_i \geq 0)$ i další polynomy $a_i(x)$ postupně s nižšími stupni m_i, až m_i bude menší než n. První takový polynom nazveme $r(x)$. Dostáváme

$$a(x) - c_0x^{m-n}b(x) - c_1x^{j_1}b(x) - \cdots = r(x),$$
$$a(x) = b(x)(c_0x^{m-n} + c_1x^{j_1} + \ldots) + r(x).$$

2. Jednoznačnost. Předpokládejme, že máme dva různé rozklady polynomu $a(x)$, tj. $a(x) = b(x)q_1(x) + r_1(x)$ a $a(x) = b(x)q_2(x) + r_2(x)$. Můžeme je od sebe odečíst a upravit, dostáváme $r_1(x) - r_2(x) = b(x)(q_2(x) - q_1(x))$, tedy platí, že $b(x) \mid r_1(x) - r_2(x)$. Polynom $r_1(x) - r_2(x)$ má ale nižší stupeň než polynom $b(x)$, proto musí být $r_1(x) - r_2(x) = 0$. To znamená, že $r_1(x) = r_2(x)$ a $q_1(x) = q_2(x)$. □

Euklidův algoritmus pro polynomy. Nechť T je těleso, $a(x), b(x)$ jsou nenulové polynomy nad tělesem T a stupeň polynomu $a(x)$ je větší než stupeň polynomu $b(x)$. Podle věty 24 můžeme sestavit systém rovnic

$$\begin{aligned}
a(x) &= b(x)q_0(x) + r_0(x),\\
b(x) &= r_0(x)q_1(x) + r_1(x),\\
r_0(x) &= r_1(x)q_2(x) + r_2(x),\\
&\vdots\\
r_{n-2}(x) &= r_{n-1}(x)q_n(x) + r_n(x),\\
r_{n-1}(x) &= r_n(x)q_{n+1}(x),
\end{aligned}$$

kde $n \in \mathbb{N}$, $q_0, q_1, \ldots, q_{n+1}, r_0, r_1, \ldots, r_{n+1}$ jsou polynomy nad tělesem T a stupně polynomů $b(x), r_0(x), r_1(x), \ldots, r_n(x)$ tvoří klesající posloupnost. Proto musí existovat n, pro které $r_{n+1}(x) = 0$. Polynom $r_n(x)$ je pak největší společný dělitel polynomů $a(x)$ a $b(x)$.

Věta 25. *Nechť T je těleso, $a(x), b(x)$ jsou polynomy nad tělesem T a $d(x) = (a(x), b(x))$ je jejich největším společným dělitelem. Pak existují polynomy $f(x)$ a $g(x)$ nad tělesem T, pro které platí*

$$a(x)f(x) + b(x)g(x) = d(x).$$

Důkaz. Úpravíme rovnice Euklidova algoritmu a postupně za $r_1, r_2, \ldots, r_{n-1}$ dosaďme:

$$\begin{aligned}
r_0(x) &= a(x) - b(x)q_0(x),\\
r_1(x) &= b(x) - r_0(x)q_1(x) = b - (a - bq_0)q_1 = a(-q_1) + b(1 + q_0q_1),\\
r_2(x) &= r_0(x) - r_1(x)q_2(x) = a - bq_0 - [a(-q_1) + b(1 + q_0q_1)]q_2 =\\
&\quad = a(1 + q_1q_2) + b(-q_0 - q_2 - q_0q_1q_2),\\
&\vdots\\
r_n(x) &= r_{n-2}(x) - r_{n-1}(x)q_n(x) = \ldots
\end{aligned}$$

Z forem těchto rovnic lze odvodit, že i $r_n(x)$ (což je největší společný dělitel polynomů $a(x)$ a $b(x)$) můžeme psát ve tvaru $r_n(x) = a(x)f(x) + b(x)g(x)$. □

Definice 13. Nechť T je těleso, $p(x)$ polynom stupně většího než 1 nad tělesem T. Pokud je $p(x)$ dělitelný jen polynomy k němu asociovanými a jednotkovými polynomy (tj. polynomy stupně 1), nazveme $p(x)$ *nerozložitelným (ireducibilním) polynomem.*

Věta 26. *Nechť T je těleso a $c(x)$ polynom stupně $n > 0$ nad tělesem T, pak se polynom $c(x)$ dá rozložit v součin konečného počtu ireducibilních polynomů. Tento rozklad je až na pořadí a asociativitu dělitelů jednoznačný.*

Důkaz. 1. Existence. Provedeme indukcí.

(a) Pro stupeň polynomu $n = 1$ je každý polynom ireducibilní.

(b) Předpokládejme tedy $n > 1$ a platnost věty pro všechny polynomy stupně $m < n$. Když je polynom $c(x)$ je ireducibilní, není co dokazovat. V opačném případě je možné polynom $c(x)$ rozložit na $c(x) = c_1(x)c_2(x)$, kde $c_1(x), c_2(x)$ jsou polynomy nad tělesem T, které mají nižší stupeň než $c(x)$, a podle indukčního předpokladu je lze rozložit v součin konečného počtu ireducibilních polynomů.

2. Jednoznačnost. Předpokládejme, že $n, m \in \mathbb{N}$ a polynom c má dva rozklady

$$c(x) = p_1(x)p_2(x)\dots p_n(x) = q_1(x)q_2(x)\dots q_m(x),$$

kde $p_1(x), p_2(x), \dots, p_n(x), q_1(x), q_2(x), \dots, q_m(x)$ jsou nerozložitelné polynomy nad tělesem T.

Bez újmy na obecnosti mějme $m \geq n$. Polynom $p_1(x) \mid c(x)$, to znamená, že $p_1(x) \mid q_1(x)q_2(x)\dots q_m(x)$. $p_1(x)$ tedy musí dělit jedem z polynomů $q_i(x)$, $1 \leq i \leq m$. Protože $p_1(x)$ i $q_i(x)$ jsou ireducibilní polynomy, platí $p_1(x) = \varepsilon(x)q_i(x)$, kde $\varepsilon(x)$ je jednotkový polynom. Oba rozklady můžeme vykrátit polynomem $p_1(x)$ a dále přeznačíme polynomy $q_1(x)q_2(x)\dots q_m(x)$ na $q_1'(x)q_2'(x)\dots q_m'(x)$ tak, aby $q_i = q_1'$. Zůstává

$$p_2(x)p_3(x)\dots p_n(x) = \varepsilon q_2'(x)q_3'(x)\dots q_m'(x).$$

V krácení a přeznačování pokračujeme, až nakonec na pravé straně zbude jen 1:

$$1 = \varepsilon^* q_{n+1}^*(x)\dots q_m^*(x).$$

Tato rovnice ale nemá řešení pro polynomy $q_i(x)$, $n+1 \leq i \leq m$, které nejsou jednotkové. Proto musí být $n = m$ a oba rozklady jsou shodné, až na pořadí a asociovanost dělitelů. □

3.2. Příklady

Příklad 3.1. Rozložte polynom $f(x) = x^4 - 8x^2 + 15$ v součin ireducibilních činitelů (a) v tělese $\mathbb{Q}$, (b) v $\mathbb{Q}(\sqrt{3})$, (c) v $\mathbb{R}$.

Řešení. (a) Nejdříve předpokládejme, že polynom $f(x)$ lze rozložit v součin dvou kvadratických polynomů. Použijeme vzorec pro řešení kvadratické rovnice pro x^2 a za kořeny dostáváme čísla 3 a 5. Potom

$$f(x) = x^4 - 8x^2 + 15 = (x^2 - 3)(x^2 - 5).$$

Jelikož $\sqrt{3}$ a $\sqrt{5}$ nejsou racionální čísla, nemá polynom $f(x)$ v $\mathbb{Q}$ za dělitele žádné lineární polynomy.

(b) V tělese $\mathbb{Q}(\sqrt{3})$ můžeme navíc rozložit i výraz $(x^2 - 3) = (x - \sqrt{3})(x + \sqrt{3})$. Tedy

$$f(x) = x^4 - 8x^2 + 15 = (x - \sqrt{3})(x + \sqrt{3})(x^2 - 5).$$

(c) V tělese reálných čísel lze rozložit oba kvadratické polynomy a

$$f(x) = x^4 - 8x^2 + 15 = (x - \sqrt{3})(x + \sqrt{3})(x - \sqrt{5})(x + \sqrt{5}).$$

□

Příklad 3.2. Najděte největšího společného dělitele polynomů (nad tělesem $\mathbb{Q}$)

$$a(x) = x^3 - x^2 + x - 1, \quad b(x) = x^5 + x^3 + 2x^2 + 2.$$

Vyjádřete ho ve tvaru $d(x) = a(x)f(x) + b(x)g(x)$.

Řešení. Největšího společného dělitele vypočítáme Euklidovým algoritmem:

$$\begin{aligned} x^5 + x^3 + 2x^2 + 2 &= (x^3 - x^2 + x - 1)(x^2 + x + 1) + 3(x^2 + 1), \\ x^3 - x^2 + x - 1 &= (x^2 + 1)(x - 1). \end{aligned}$$

Tedy $d(x) = (x^2 + 1)$.

$$\begin{aligned} (x^2 + 1) &= \frac{1}{3}(x^5 + x^3 + 2x^2 + 2) - \frac{1}{3}(x^3 - x^2 + x - 1)(x^2 + x + 1) = \\ &= -\frac{1}{3}(x^2 + x + 1)a(x) + \frac{1}{3}b(x). \end{aligned}$$ □

Příklad 3.3. Nalezněte největšího společného dělitele $d(x)$ polynomů $a(x) = x^3 + 1$ a $b(x) = x^4 + x^2 + 1$ z tělesa $\mathbb{Z}_7$ a najděte polynomy nad $\mathbb{Z}_7$ tak, aby platilo

$$d(x) = a(x)f(x) + b(x)g(x).$$

Řešení. Opět použijeme Euklidův algoritmus.

$$\begin{aligned} x^4 + x^2 + 1 &= x(x^3 + 1) + (x^2 - x + 1), \\ x^3 + 1 &= (x + 1)(x^2 - x + 1). \end{aligned}$$

Největší společný dělitel polynomů $a(x)$ a $b(x)$ je $(x^2 - x + 1)$

$$\begin{aligned} (x^2 - x + 1) &= (x^4 + x^2 + 1) - x(x^3 + 1), \\ &= a(x) + (-x)b(x). \end{aligned}$$ □

4. Okruh celých čísel kvadratického tělesa

4.1. Pojem kvadratického tělesa

Definice 14. Nechť $d \in \mathbb{Z}$, $d \neq 0$, $d \neq 1$ a není dělitelné čtvercem žádného čísla. Potom množinu $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$ nazýváme *kvadratickým tělesem.*

Poznámka. Zřejmě tedy platí $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{d}) \subseteq \mathbb{C}$.

Věta 27. *Nechť $d_1, d_2 \in \mathbb{Z}$, $d_1 \neq d_2$, $d_1 \neq 1$, $d_2 \neq 1$, $a^2 \nmid d_1$, $a^2 \nmid d_2$, kde $a \in \mathbb{Z}$, $a > 1$ (tj. d_1 ani d_2 nejsou dělitelné čtvercem celého čísla většího než 1), pak $\mathbb{Q}(\sqrt{d_1}) \neq \mathbb{Q}(\sqrt{d_2})$.*

Důkaz. Stačí, když dokážeme $\sqrt{d_1} \notin \mathbb{Q}(\sqrt{d_2})$. Důkaz provedeme sporem.

Předpokládejme tedy, že můžeme $\sqrt{d_1}$ vyjádřit ve tvaru $\sqrt{d_1} = a + b\sqrt{d_2}$, kde $a, b \in \mathbb{Q}$. Po umocnění máme

$$d_1 = a^2 + 2ab\sqrt{d_2} + b^2 d_2.$$

Kdyby $a \neq 0$ a $b \neq 0$, dostali bychom

$$\sqrt{d_2} = \frac{d_1 - a^2 - b^2 d_2}{2ab}.$$

To ale znamená, že d_2 je čtvercem a to je spor s předpokladem.

Kdyby dále bylo $a \neq 0$ a $b = 0$, máme $d_1 = a^2$ a tedy zase dostáváme spor.

Předpokládejme tedy $a = 0$ a $b \neq 0$. Potom $d_1 = b^2 d_2$. Nechť b je celé číslo. Když bude $b^2 = 1$, máme $d_1 = d_2$, jinak $b^2 \mid d_2$. Ani jeden případ však není možný, opět máme spor s předpoklady.

Pokud $b \in \mathbb{Q}$, $b = \frac{p}{q}$, kde $p, q \in \mathbb{Z}$ a jsou nesoudělné. Pak $q^2 d_1 = p^2 d_2$, tedy $p^2 \mid d_1$ a dostáváme spor. $\sqrt{d_1}$ do $\mathbb{Q}(\sqrt{d_2})$ nepatří a věta je tím dokázána. □

Definice 15. Nechť a, b jsou racionální čísla, $\mathbb{Q}(\sqrt{d})$ kvadratické těleso a $\alpha = a + b\sqrt{d}$ číslo z toho tělesa. Číslo

$$N(\alpha) = \alpha\alpha',$$

kde α' je číslo konjugované k α, pak nazveme *normou čísla* α.

Poznámka. Číslem konjugovaným k číslu $\alpha = a + b\sqrt{d}$, myslíme číslo $\alpha' = a - b\sqrt{d}$.

Definice 16. Nechť α je číslo z kvadratického tělesa T. Pak normovaný polynom $p(\alpha)$ nejnižšího možného stupně s racionálními koeficienty, který splňuje $p(\alpha) = 0$, nazveme *minimálním polynomem čísla* α a rovnici $p(\alpha) = 0$ *minimální rovnicí čísla* α.

Věta 28. *Minimální polynom čísla α z kvadratického tělesa T dělí každý nenulový polynom s racionálními koeficienty, který má za kořen číslo α.*

Důkaz. Nechť $p(x)$ je polynom s kořenem α a $\varphi(x)$ je minimální polynom čísla α. Protože je α číslo z kvadratického tělesa, stupeň $\varphi(x) = 2$. Platí $p(x) = \varphi(x)q(x) + r(x)$, kde q, r jsou polynomy s racionálními koeficienty a stupeň polynomu $r(x)$ je menší než stupeň polynomu $\varphi(x)$.

(1) Předpokládejme, že stupeň $r(x) = 1$, tedy $r(x) = x-\gamma$, $\gamma \in \mathbb{Q}$. Pro $x = \alpha$ dostáváme rovnici

$$p(\alpha) = \varphi(\alpha)q(\alpha) + \alpha - \gamma.$$

$p(\alpha) = 0$ i $\varphi(\alpha) = 0$, dostáváme tedy $\alpha = \gamma$, což není možné.

(2) Nyní nechť stupeň $r(x) = 0$, $r(x) = \gamma$, $\gamma \in \mathbb{Q}$. Pro $x = \alpha$ máme

$$p(\alpha) = \varphi(\alpha)q(\alpha) + \gamma.$$

Z toho plyne $\gamma = 0$.

Tedy polynom $r(x) = 0$ a platí $p(x) = \varphi(x)q(x)$, tedy $\varphi(x) \mid p(x)$. □

Věta 29. *Nechť a, b jsou racionální čísla, $a \neq 0$, $b \neq 0$, $\mathbb{Q}(\sqrt{d})$ kvadratické těleso a $\alpha = a + b\sqrt{d}$ číslo z toho tělesa. Minimální rovnice čísla α je potom*

$$x^2 - 2ax + N(\alpha) = 0, \text{ kde } N(\alpha) = a^2 - db^2. \tag{4.1}$$

Důkaz. Položme

$$p(x) = x^2 - 2ax + N(\alpha).$$

Rozepsáním normy dostáváme

$$N(\alpha) = \alpha\alpha' = (a + b\sqrt{d})(a - b\sqrt{d}) = a^2 - db^2.$$

Tedy $p(x) = x^2 - 2ax + a^2 - db^2$, dosazením se můžeme přesvědčit, že platí $p(\alpha) = 0$.

Nechť $\varphi(x)$ je minimální polynom čísla α. Pak stupeň polynomu $\varphi(x) = 2$, protože podle předpokladu α není racionální.

Podle věty 28 platí $\varphi(x) \mid p(x)$. Existuje tedy polynom nad tělesem racionálních čísel $q(x)$ takový, že $p(x) = \varphi(x)q(x)$. Stupeň $p(x)$ je roven součtu stupňů $\varphi(x)$ a $q(x)$. Stupeň $p(x)$ = stupeň $\varphi(x) = 2$, z toho plyne, že stupeň polynomu $q(x) = 0$, tedy $q \in \mathbb{Q}$, $q \neq 0$ a platí rovnice

$$p(x) = q\varphi(x).$$

Oba polynomy $p(x)$ a $\varphi(x)$ jsou normované, pro q může platit jen $q = 1$.

Tedy $p(x) = \varphi(x)$ a rovnice

$$x^2 - 2ax + N(\alpha) = 0$$

je minimální rovnicí čísla α. □

Poznámka. Zřejmě uvedená rovnice je také minimální rovnicí čísla α'.

Věta 30. *Mějme dvě čísla α a β z libovolného kvadratického tělesa. Pak*

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

Důkaz. Z definice normy dostáváme

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

□

4.2. Celá čísla kvadratického tělesa

Definice 17. Nechť $\mathbb{Q}(\sqrt{d})$ je kvadratické těleso. Řekneme, že číslo $\alpha = a + b\sqrt{d}$ z tohoto tělesa je *celým algebraickým číslem tělesa* $\mathbb{Q}(\sqrt{d})$, když α vyhovuje rovnici

$$x^2 + c_1 x + c_2 = 0, \tag{4.2}$$

kde koeficienty c_1, c_2 jsou celá čísla.

Věta 31. *Jestliže α je celé algebraické číslo kvadratické tělesa $\mathbb{Q}(\sqrt{d})$, pak i α' je zřejmě celé algebraické číslo tohoto tělesa.*

Věta 32. *Nechť $\mathbb{Q}(\sqrt{d})$ je kvadratické těleso. Všechny celá algebraická čísla tohoto tělesa jsou tvaru*

a) $a + b\sqrt{d}$ v případě, že $d \not\equiv 1 \pmod 4$,

b) $a + b\frac{1+\sqrt{d}}{2}$ v případě, že $d \equiv 1 \pmod 4$,

kde a, b jsou celá čísla.

Důkaz. Označme si $\mathcal{M}$ množinu všech celých čísel kvadratického tělesa $\mathbb{Q}(\sqrt{d})$ a $\mathcal{N}$ množinu všech čísel α kvadratického tělesa $\mathbb{Q}(\sqrt{d})$ tvaru $\alpha = a_0 + b_0\theta$, kde $a_0, b_0 \in \mathbb{Z}$ a

$$\theta = \begin{cases} \sqrt{d} & \text{pro } d \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{pro } d \equiv 1 \pmod 4. \end{cases}$$

Máme dokázat, že $\mathcal{M} = \mathcal{N}$.

(1) Nechť $\alpha \in \mathcal{N}$, α je tedy tvaru $a_0 + b_0\theta$ a máme dokázat, že α je celé algebraické číslo tělesa $\mathbb{Q}(\sqrt{d})$.

a) Předpokládejme $d \not\equiv 1 \pmod 4$, $\theta = \sqrt{d}$, $\alpha = a_0 + b_0\sqrt{d}$, $a_0, b_0 \in \mathbb{Z}$. Číslo α zřejmě vyhovuje rovnici 4.2, kde koeficienty $c_1 = -2a_0$ a $c_2 = a_0^2 - db_0^2$ jsou celá čísla, tedy α je podle definice 17 algebraické celé číslo tělesa $\mathbb{Q}(\sqrt{d})$.

b) Nyní nechť $d \equiv 1 \pmod 4$, $\theta = \frac{1+\sqrt{d}}{2}$, $\alpha = a_0 + b_0\frac{1+\sqrt{d}}{2}$, $a_0, b_0 \in \mathbb{Z}$. Po úpravě dostáváme $\alpha = (a_0 + \frac{b_0}{2}) + \frac{b_0}{2}\sqrt{d}$. Když si označíme $a = (a_0 + \frac{b_0}{2}), b = \frac{b_0}{2}$, můžeme se dosazením přesvědčit, že α opět vyhovuje rovnici 4.2, kde koeficienty c_1, c_2 jsou:

$$\begin{aligned} c_1 &= -2a = -2\left(a_0 + \frac{b_0}{2}\right) = -2a_0 - b_0, \\ c_2 &= a^2 - db^2 = \left(a_0 + \frac{b_0}{2}\right)^2 - d\left(\frac{b_0}{2}\right)^2 = a_0^2 + a_0 b_0 + \frac{b_0^2}{4} - d\frac{b_0^2}{4} = \\ &= a_0^2 + a_0 b_0 + b_0^2\frac{1-d}{4}. \end{aligned}$$

Čísla c_1, c_2 jsou celá (protože $d \equiv 1 \pmod 4$, takže $\frac{1-d}{4} \in \mathbb{Z}$) a číslo α je celé algebraické číslo tělesa $\mathbb{Q}(\sqrt{d})$.

Dokázali jsme, že $\mathcal{N} \subseteq \mathcal{M}$.

(2) Nechť $\alpha \in \mathcal{M}$, α je tedy celé algebraické číslo tělesa $\mathbb{Q}(\sqrt{d})$, $\alpha = a + b\sqrt{d}$, $a, b \in \mathbb{Q}$, α je kořenem rovnice

$$x^2 - 2ax + a^2 - db^2 = 0,$$

kde koeficienty $-2a$ a $a^2 - db^2$ jsou celá čísla. Označme si je jako $c_1 = -2a$ a $c_2 = a^2 - db^2$. Pomocí c_1 si vyjádříme $a = -\frac{c_1}{2}$ a dosadíme do druhé rovnice:

$$c_2 = \frac{c_1^2}{4} - db^2.$$

Číslo b je racionální, můžeme ho psát ve tvaru zlomku $b = \frac{u}{v}$, kde $u, v \in \mathbb{Z}$, $v \geq 1$, $(u, v) = 1$. Máme tedy $c_2 = \frac{c_1^2}{4} - d\frac{u^2}{v^2}$, vynásobením $4v^2$ dostáváme

$$\begin{aligned} 4c_2v^2 &= c_1^2v^2 - 4du^2, \\ v^2(4c_2 - c_1^2) &= -4du^2. \end{aligned}$$

Z tohoto vztahu plyne $v^2 \mid 4du^2$, v a u jsou nesoudělná čísla, tedy $v^2 \mid 4d$. Nyní může platit jen $v = 1$ nebo $v = 2$, protože jinak by bylo d dělitelné čtvercem celého čísla.

a) Pro $v = 1$ máme $b = u \in \mathbb{Z}$, $c_2 = \frac{c_1^2}{4} - du^2$. Číslo $\frac{c_1^2}{4}$ je celé, tedy $4 \mid c_1^2$ a $2 \mid c_1$.

   I) Pro $d \not\equiv 1 \pmod 4$ je $\alpha = -\frac{c_1}{2} + u\sqrt{d}$, $a_0 = -\frac{c_1}{2}$ i $b_0 = u$ jsou celé.

   II) Pro $d \equiv 1 \pmod 4$ je

$$\alpha = -\frac{c_1}{2} + u\sqrt{d} = \left(-\frac{c_1}{2} - u\right) + 2u\frac{1 + \sqrt{d}}{2},$$

   $a_0 = -\frac{c_1}{2} - u$ i $b_0 = 2u$ jsou opět celé.

b) Pro $v = 2$ máme $b = \frac{u}{2}$, u je liché,

$$c_2 = \frac{c_1^2}{4} - \frac{du^2}{4} = \frac{1}{4}(c_1^2 - du^2).$$

   Platí, že $4 \mid (c_1^2 - du^2)$, tedy $c_1^2 \equiv du^2 \pmod 4$. Číslo u je liché, $u^2 \equiv 1 \pmod 4$, po dosazení dostáváme $c_1^2 \equiv d \pmod 4$. Čtverec celého čísla může být kongruentní s 0 nebo 1 modulo 4.

   I) Pro $d \not\equiv 1 \pmod 4$ není přípustná ani jedna možnost, kdyby platilo $c_1^2 \equiv 0 \equiv d \pmod 4$, bylo by d dělitelné čtvercem, ale to je spor s předpokladem.

   II) Pro $d \equiv 1 \pmod 4$ máme $c_1^2 \equiv 1 \equiv d \pmod 4$, takže c_1 je liché.

$$\alpha = a + b\sqrt{d} = (a - b) + 2b\frac{1 + \sqrt{d}}{2} = a_0 + b_0\frac{1 + \sqrt{d}}{2},$$

   $a_0 = a - b$ a $b_0 = 2b$ musí být celá čísla. To je splněno, neboť $b_0 = u$ a

$$a - b = -\frac{c_1}{2} - \frac{u}{2} = -\frac{1}{2}(c_1 + u),$$

   c_1 i u jsou lichá, jejich součet je sudý, takže a_0 i b_0 jsou celá čísla.

Dokázali jsme, že každé celé algebraické číslo α, lze vyjádřit ve tvaru $\alpha = a_0 + b_0\theta$, kde $a_0, b_0 \in \mathbb{Z}$, $\mathcal{M} \subseteq \mathcal{N}$ a tedy $\mathcal{M} = \mathcal{N}$. □

Definice 18. Nechť $\mathbb{Q}(\sqrt{d})$ je kvadratické těleso. Zaveďme označení

$$\theta = \begin{cases} \sqrt{d} & \text{pro } d \not\equiv 1 \pmod 4 \\ \frac{1+\sqrt{d}}{2} & \text{pro } d \equiv 1 \pmod 4. \end{cases}$$

Poznámka. Množinu všech celých algebraických čísel kvadratického tělesa $\mathbb{Q}(\sqrt{d})$ budeme značit $\mathbb{Z}[\theta]$. Zřejmě je $\mathbb{Z}[\theta]$ obor integrity a $\mathbb{Z}[\theta] = \{a + b\theta \mid a, b \in \mathbb{Z}\}$.

Definice 19. Nechť T je kvadratické těleso a θ_1, θ_2 jsou celá algebraická čísla tohoto tělesa. Pokud můžeme každé další číslo z oboru integrity $\mathbb{Z}[\theta]$ vyjádřit jednoznačně ve tvaru

$$a_1\theta_1 + a_2\theta_2,$$

kde a_1, a_2 jsou celá čísla, potom řekneme, že θ_1, θ_2 tvoří *bázi oboru integrity* $\mathbb{Z}[\theta]$.

Věta 33. *Celá čísla 1 a θ tvoří bázi oboru integrity $\mathbb{Z}[\theta]$.*

Důkaz. Zřejmě každé celé algebraické číslo v tělesa $\mathbb{Q}(\sqrt{d})$ se dá vyjádřit pomocí čísel 1 a θ, stačí tedy, když sporem dokážeme jednoznačnost.

Předpokládejme, že $\alpha = a_1 + b_1\theta$ a $\alpha = a_2 + b_2\theta$ jsou dva rozklady celého algebraického čísla α tělesa $\mathbb{Q}(\sqrt{d})$, $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Platí $a_1 - a_2 + (b_1 - b_2)\theta = 0$ a tedy

$$\theta = \frac{a_1 - a_2}{b_2 - b_1}.$$

Tady ale dostáváme spor, protože θ není racionální číslo. □

4.3. Dělitelnost v okruhu celých čísel kvadratického tělesa

Definice 20. Nechť $T = \mathbb{Q}(\sqrt{d})$ je kvadratické těleso a α, β jsou celá algebraická čísla tohoto tělesa. Řekneme, že číslo α je *dělitelné* číslem β, jestliže existuje celé algebraické číslo μ z tělesa T takové, že $\alpha = \beta\mu$. Stručně značíme $\beta \mid \alpha$.

Věta 34. *Nechť α je celé algebraické číslo kvadratického tělesa T, pak $\alpha \mid \alpha$.*

Důkaz. Existuje celé číslo $\mu = 1$ tak, že platí $\alpha = \alpha\mu$. □

Věta 35. *Nechť α, β, γ jsou celá algebraická čísla kvadratického tělesa T, $\beta \mid \alpha$ a $\gamma \mid \beta$, potom $\gamma \mid \alpha$.*

Důkaz. Z předpokladu plyne, že existují celá algebraická čísla z kvadratického tělesa T, pro které platí $\alpha = \beta\mu$ a $\beta = \gamma\nu$. Platí $\alpha = \gamma\nu\mu$, $\nu\mu$ je opět celé algebraické číslo tělesa T, tedy $\gamma \mid \alpha$. □

Poznámka. Dělitelnost je tedy relace reflexivní a transitivní.

Věta 36. *Nechť α, β, γ jsou celá algebraická čísla kvadratického tělesa T, $\beta\gamma \mid \alpha\gamma$, $\gamma \neq 0$, potom $\beta \mid \alpha$.*

Důkaz. Existuje celé algebraické číslo μ z kvadratického tělesa T tak, že $\alpha\gamma = \beta\gamma\mu$. Když není $\gamma = 0$, můžeme s ní rovnici vydělit, dostáváme $\alpha = \beta\mu$ a tedy $\beta \mid \alpha$. □

Věta 37. *Nechť α, β, γ jsou celá algebraická čísla kvadratického tělesa T, $\gamma \mid \alpha$, $\gamma \mid \beta$, pak pro každá dvě celá algebraická čísla ξ, η kvadratického tělesa T platí $\gamma \mid \alpha\xi + \beta\eta$.*

Důkaz. Existují celá algebraická čísla μ a ν z kvadratického tělesa T tak, že $\alpha = \gamma\mu$ a $\beta = \gamma\nu$, takže $\alpha\xi = \gamma\mu\xi$ a $\beta\eta = \gamma\nu\eta$, po sečtení $\alpha\xi+\beta\eta = \gamma(\mu\xi+\nu\eta)$, tedy $\gamma \mid \alpha\xi+\beta\eta$. □

Definice 21. *Jednotkou kvadratického tělesa T* nazýváme celé algebraické číslo ε takové, že platí $\varepsilon \mid 1$.

Věta 38. *Nechť je ε jednotkou kvadratického tělesa T, pak je jednotkou tohoto tělesa i $\frac{1}{\varepsilon}$.*

Důkaz. Podle předpokladu $\varepsilon \mid 1$, tedy existuje celé algebraické číslo μ, které splňuje rovnost $\varepsilon\mu = 1$. Z toho vyplývá, že i $\mu = \frac{1}{\varepsilon}$ dělí 1 a je tedy jednotkou. □

Věta 39. *Nechť $T = \mathbb{Q}(\sqrt{d})$ je kvadratické těleso a α je celé algebraické číslo tohoto tělesa, potom $N(\alpha) \in \mathbb{Z}$.*

Důkaz. Když $d \equiv 1 \pmod 4$, je celé algebraické číslo α tvaru $\alpha = a_1 + a_2\frac{1+\sqrt{d}}{2}$, kde $a_1, a_2 \in \mathbb{Z}$. Norma čísla α je potom

$$N(\alpha) = \alpha\alpha' = (a_1 + a_2\frac{1+\sqrt{d}}{2})(a_1 + a_2\frac{1-\sqrt{d}}{2}) = a_1^2 + a_1a_2 + a_2^2\frac{1-d}{4}.$$

Každý ze členů v tomto výrazu je celé číslo, proto je i $N(\alpha) \in \mathbb{Z}$.

Když bude naopak $d \not\equiv 1 \pmod 4$, celé algebraické číslo α je tvaru $\alpha = a_1 + a_2\sqrt{d}$, kde $a_1, a_2 \in \mathbb{Z}$ a

$$N(\alpha) = (a_1 + a_2\sqrt{d})(a_1 - a_2\sqrt{d}) = a_1^2 - da_2^2,$$

tedy opět $N(\alpha) \in \mathbb{Z}$. □

Věta 40. *Nechť α a β jsou celá algebraická čísla kvadratického tělesa T a $\beta \mid \alpha$. Potom $N(\beta) \mid N(\alpha)$.*

Důkaz. Z předpokladu plyne, že existuje celé algebraické číslo μ kvadratického tělesa T takové, že $\alpha = \beta\mu$. Použitím věty 30 dostáváme $N(\alpha) = N(\beta)N(\mu)$. Podle věty 39 je $N(\mu) \in \mathbb{Z}$. Proto $N(\beta) \mid N(\alpha)$. □

Věta 41. *Nechť α je celým číslem kvadratického tělesa T. Pak je α jednotkou, pravě když $N(\alpha) = \pm 1$.*

Důkaz. a) Nechť je α jednotkou, tj. $\alpha \mid 1$. Podle věty 40 máme $N(\alpha) \mid 1$. Norma $N(\alpha)$ má být celá, tedy $N(\alpha) = \pm 1$.

b) Nechť $N(\alpha) = \pm 1 = \alpha\alpha'$. Protože i α' je celé algebraické číslo, máme $\alpha \mid 1$, to znamená, že α je jednotkou. □

Definice 22. Mějme celá algebraická čísla α, β kvadratického tělesa T. Řekneme, že α je *asociované* s β, jestliže splňují rovnici $\alpha = \beta\varepsilon$, kde ε je jednotkou kvadratického tělesa T.

Poznámka. Zřejmě je asociovanost relace reflexivní, symetrická a transitivní. Je to tedy relace ekvivalence.

Věta 42. *Nechť jsou α, β celá algebraická čísla kvadratického tělesa T. Pak jsou tyto čísla asociovaná, právě když platí $\alpha \mid \beta$ a zároveň $\beta \mid \alpha$.*

Důkaz. a) Nechť α a β jsou asociované, pak je podle definice $\alpha = \beta\varepsilon$. Tedy zřejmě $\alpha \mid \beta$ a $\beta \mid \alpha$.

b) Nechť naopak $\alpha \mid \beta$ a $\beta \mid \alpha$. Existují celá algebraická čísla μ_1 a μ_2 z tělesa T takové, že platí $\alpha = \beta\mu_1$ a $\beta = \alpha\mu_2$. Proto máme $\alpha = \alpha\mu_2\mu_1$, po úpravě $1 = \mu_2\mu_1$. Tedy čísla μ_1 a μ_2 jsou jednotkami tělesa T a čísla α a β jsou asociované. □

Věta 43. *Nechť $\alpha_1, \alpha_2, \beta_1, \beta_2$ jsou celá algebraická čísla kvadratického tělesa T, α_1 je asociované k α_2, β_1 je asociované k β_2 a $\alpha_1 \mid \beta_1$. Potom platí $\alpha_2 \mid \beta_2$.*

Důkaz. Podle předpokladu existuje celá algebraické číslo μ, pro které platí $\beta_1 = \alpha_1\mu$ a dále $\alpha_1 = \alpha_2\varepsilon_1$ a $\beta_1 = \beta_2\varepsilon_2$, kde ε_1 a ε_2 jsou jednotky tělesa T. Po dosazení máme $\beta_2 = \alpha_2\varepsilon_1\frac{1}{\varepsilon_2}\mu$. Teda $\alpha_2 \mid \beta_2$. □

Věta 44. *Nechť α a β jsou celá algebraická čísla kvadratického tělesa T, $\alpha \neq 0$, $\beta \mid \alpha$, pak $|N(\alpha)| \geq |N(\beta)|$. Rovnost $|N(\alpha)| = |N(\beta)|$ platí, právě když jsou čísla α a β asociované.*

Důkaz. Podle předpokladu existuje celé algebraické číslo μ tak, že platí $\alpha = \beta\mu$, a tedy $N(\alpha) = N(\beta)N(\mu)$ a $|N(\alpha)| = |N(\beta)||N(\mu)|$. Číslo $\alpha \neq 0$, proto máme $|N(\mu)| \geq 1$. Tedy $|N(\alpha)| \geq |N(\beta)|$. Pokud by bylo $|N(\mu)| = 1$, tj. μ by bylo jednotkou a čísla α a β asociované, máme $|N(\alpha)| = |N(\beta)|$. □

Definice 23. Nechť π je celé algebraické číslo kvadratického tělesa T, $|N(\pi)| > 1$. Pokud je číslo π dělitelné jen čísly k němu asociovanými a jednotkami tělesa T, nazveme toto číslo *algebraickým prvočíslem tělesa T*.

Věta 45. *Nechť je π algebraickým prvočíslem kvadratického tělesa T, potom je i číslo π' k němu konjugované algebraickým prvočíslem tohoto tělesa.*

Důkaz. Provedeme sporem. Předpokládejme, že π' není algebraickým prvočíslem tělesa T a můžeme ho psát ve tvaru $\pi' = \eta\xi$, kde η a ξ jsou celá algebraická čísla tělesa T, $|N(\eta)| > 1$ a $|N(\xi)| > 1$. Potom

$$\pi = (\pi')' = (\eta\xi)' = \eta'\xi',$$

kde $N(\eta) = N(\eta')$ a $N(\xi) = N(\xi')$. To ale znamená, že π je složené číslo, což je spor. □

Věta 46. *Nechť je α celé algebraické číslo kvadratického tělesa T, $N(\alpha) = p$, kde p je prvočíslo. Potom je α algebraickým prvočíslem.*

Důkaz. Provedeme sporem. Předpokládejme, že α není algebraickým prvočíslem tělesa T a můžeme ho psát ve tvaru $\alpha = \eta\xi$, kde η a ξ jsou celá algebraická čísla tělesa T, $|N(\eta)| > 1$ a $|N(\xi)| > 1$. Tedy $p = N(\alpha) = N(\eta)N(\xi)$, prvočíslo p však nemůžeme rozložit v součin dvou celých čísel, jejichž absolutní hodnota je větší než 1. Dostáváme tedy spor. □

Věta 47. *Nechť je α celé algebraické číslo kvadratického tělesa T, $|N(\alpha)| > 1$. Pak lze toto číslo rozložit v součin konečného počtu algebraických prvočísel tělesa T.*

Důkaz. Provedeme indukcí.

(a) Každé celé algebraické číslo α takové, že $|N(\alpha)| = 2$, je podle věty 46 algebraickým prvočíslem tělesa T.

(b) Předpokládejme tedy celé algebraické číslo α, $|N(\alpha)| > 2$ a platnost věty pro každé celé číslo β, pro které platí $|N(\beta)| < |N(\alpha)|$. Když je α algebraické prvočíslo, je věta dokázaná. V opačném případě je možné číslo α rozložit na $\alpha = \beta\gamma$, kde β, γ jsou celá algebraická čísla tělesa T a podle věty 44 platí $1 < |N(\beta)| < |N(\alpha)|$ a $1 < |N(\gamma)| < |N(\alpha)|$. Podle indukčního předpokladu však lze čísla β a γ rozložit v součin konečného počtu algebraických prvočísel. □

Věta 48. *V oboru integrity $\mathbb{Z}[\theta]$ každého kvadratického tělesa $\mathbb{Q}(\sqrt{d})$, kde $d < 0$, je konečně mnoho jednotek. Konkrétně:*

(a) v případě $d = -1$ máme 4 jednotky a to $1, -1, i, -i$,

(b) v případě $d = -3$ máme 6 jednotek a to $1, -1, \varrho, -\varrho, \varrho^2, -\varrho^2$, kde $\varrho = \frac{-1+i\sqrt{d}}{2}$,

(c) jinak 2 jednotky a to 1 a -1.

Důkaz. Všechny celá algebraická čísla kvadratického čísla jsou tvaru $\alpha = x + y\theta$, kde $a, b \in \mathbb{Z}$. Jejich norma je

$$N(\alpha) = \alpha\alpha' = \begin{cases} x^2 - dy^2 & \text{pro } d \not\equiv 1 \pmod 4 \\ x^2 + xy + \frac{1-d}{4}y^2 & \text{pro } d \equiv 1 \pmod 4. \end{cases}$$

Aby bylo α jednotkou, musí platit $N(\alpha) = \pm 1$. Řešíme tedy rovnice

$$x^2 - dy^2 = \pm 1,$$
$$x^2 + xy + \frac{1-d}{4}y^2 = \pm 1,$$

kde $x, y \in \mathbb{Z}$ a $d < 0$. Proto jsou výrazy $x^2 - dy^2$ a $x^2 + xy + \frac{1-d}{4}y^2$ vždy kladné, hledáme tedy jen řešení rovnic

$$x^2 - dy^2 = 1, \tag{4.3}$$
$$x^2 + xy + \frac{1-d}{4}y^2 = 1. \tag{4.4}$$

(a) Řešme rovnici 4.3, $d < 0$ a $d \not\equiv 1 \pmod 4$. Nechť $d = -1$, pak dostáváme řešení $(x, y) = (1, 0), (-1, 0), (0, 1), (0, -1)$. V kvadratickém tělese $\mathbb{Q}(\sqrt{-1})$ tedy existují 4 jednotky $1, -1, i, -i$.

Pro $d < -1$ má rovnice 4.3 jen dvě řešení $(x, y) = (1, 0), (-1, 0)$, tedy jednotky jsou 1 a -1.

(b) V rovnici 4.4 musí platit $d < 0$, $d \equiv 1 \pmod 4$. Pro $d = -3$ máme 6 řešení $(x, y) = (1, 0), (-1, 0), (0, 1), (0, -1), (1, 1), (1, -1)$, tedy čísla

$$1, -1, \frac{1+\sqrt{-3}}{2}, \frac{-1-\sqrt{-3}}{2}, \frac{-1+\sqrt{-3}}{2}, \frac{1-\sqrt{-3}}{2}.$$

Jsou to čísla $1, -1, \varrho, -\varrho, \varrho^2, -\varrho^2$, kde $\varrho = \frac{-1+i\sqrt{d}}{2}$.

Pro $d < -3$ dostáváme zase jen dvě řešení $(x, y) = (1, 0), (-1, 0)$, tj. čísla 1 a -1. □

Nyní si uvedeme dvě věty bez důkazů.

Věta 49. *V oboru integrity $\mathbb{Z}[\theta]$ každého kvadratického tělesa $\mathbb{Q}(\sqrt{d})$, kde $d > 0$, je nekonečně mnoho jednotek.*

Věta 50. *V oboru integrity $\mathbb{Z}[\theta]$ kvadratického tělesa $\mathbb{Q}(\sqrt{d})$, kde $d > 0$, existuje ε^* (fundamentální jednotka) a pro každou další jednotku ε platí $\varepsilon = +(\varepsilon^*)^n$ nebo $\varepsilon = -(\varepsilon^*)^n$, kde $n \in \mathbb{N}$.*

4.4. Příklady

Příklad 4.1. Dokažte, že pro α, β z kvadratického tělesa platí

$$N\left(\frac{\alpha}{\beta}\right) = \frac{N(\alpha)}{N(\beta)}.$$

Řešení.

$$N\left(\frac{\alpha}{\beta}\right) = \left(\frac{\alpha}{\beta}\right)\left(\frac{\alpha}{\beta}\right)' = \left(\frac{\alpha}{\beta}\right)\left(\frac{\alpha'}{\beta'}\right) = \frac{\alpha\alpha'}{\beta\beta'} = \frac{N(\alpha)}{N(\beta)}.$$

□

Příklad 4.2. Dokažte, že čísla $\theta_1 = 1 + i$ a $\theta_2 = 3 + 2i$ tvoří bázi celých čísel tělesa $\mathbb{Q}(i)$.

Řešení. Aby tvořila čísla θ_1, θ_2 bázi celých čísel tělesa $\mathbb{Q}(i)$, musí jít každé celé algebraické číslo $\alpha = a_1 + a_2 i$ $(a_1, a_2 \in \mathbb{Z})$ tohoto tělesa jednoznačně vyjádřit ve tvaru

$$\alpha = a_1 + a_2 i = c_1(1 + i) + c_2(3 + 2i),$$

kde $c_1, c_2 \in \mathbb{Z}$.

Porovnáním reálných a imaginárních částí dostáváme $c_1 = -2a_1 + 3a_2$ a $c_2 = a_1 - a_2$. Tedy každé celé algebraické číslo tělesa $\mathbb{Q}(i)$ lze vyjádřit pomocí θ_1, θ_2 a ty tvoří bázi celých čísel tohoto tělesa. □

Příklad 4.3. Nechť θ_1, θ_2 tvoří bázi celých čísel tělesa $T = \mathbb{Q}(\sqrt{d})$. Dokažte, že každá jiná báze je tvaru

$$\begin{aligned} \theta_1^* &= c_{11}\theta_1 + c_{12}\theta_2, \\ \theta_2^* &= c_{21}\theta_1 + c_{22}\theta_2, \end{aligned}$$

kde

$$\begin{vmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{vmatrix} = \pm 1, \quad c_{11}, c_{12}, c_{21}, c_{22} \in \mathbb{Z}.$$

Řešení. Označme

$$\mathcal{B} = \{[\theta_1^*, \theta_2^*] : \theta_1^*, \theta_2^* \text{ tvoří bázi algebraických celých čísel tělesa } T\}$$

$$\mathcal{C} = \{[\theta_1^*, \theta_2^*] : \exists c_{ij} \in \mathbb{Z}, 1 \le i, j \le 2, det(c_{ij}) = \pm 1, \begin{array}{l} \theta_1^* = c_{11}\theta_1 + c_{12}\theta_2, \\ \theta_2^* = c_{21}\theta_1 + c_{22}\theta_2 \end{array} \}.$$

Máme dokázat, že $\mathcal{B} = \mathcal{C}$.

(1) Nechť $[\theta_1^*, \theta_2^*] \in \mathcal{B}$, tedy je θ_1^*, θ_2^* báze celých čísel tělesa T. Existují $d_{ij} \in \mathbb{Z}, 1 \leq i, j \leq 2$ tak, že platí

$$\theta_1 = d_{11}\theta_1^* + d_{12}\theta_2^*,$$
$$\theta_2 = d_{21}\theta_1^* + d_{22}\theta_2^*.$$

Označme si

$$\Theta = \begin{bmatrix}\theta_1 \\ \theta_2\end{bmatrix}, \quad \Theta^* = \begin{bmatrix}\theta_1^* \\ \theta_2^*\end{bmatrix}, \quad C = \begin{bmatrix}c_{11} & c_{12} \\ c_{21} & c_{22}\end{bmatrix}, \quad D = \begin{bmatrix}d_{11} & d_{12} \\ d_{21} & d_{22}\end{bmatrix}.$$

Potom můžeme psát

$$C\Theta = \Theta^*, \quad D\Theta^* = \Theta.$$

Tedy $DC\Theta = \Theta$, z toho plyne, že $DC = I_2$. Podle Cauchyovy věty o součinu determinantů dostáváme $det(C)det(D) = det(I_2) = 1$. Determinant matice C i matice D je celé číslo, tedy $det(C) = \pm 1$. Tím jsme dokázali, že $[\theta_1^*, \theta_2^*] \in \mathcal{C}$.

(2) Nechť $[\theta_1^*, \theta_2^*] \in \mathcal{C}$, tedy $\Theta^* = C\Theta$, $det(C) = \pm 1$. Nechť $\beta = a\theta_1 + b\theta_2$ je celé algebraické číslo z T, $a, b \in \mathbb{Z}$ a $\alpha = (a, b)$. Pak $\beta = \alpha\Theta$. Determinant $det(C) = \pm 1$, existujete proto inverzní matice C^{-1}, pro kterou platí $\Theta = C^{-1}\Theta^*$ a

$$C^{-1} = \frac{1}{det(C)} adj(C) = \pm adj(C) = \pm \begin{bmatrix}c_{22} & -c_{21} \\ -c_{12} & c_{11}\end{bmatrix}.$$

Prvky matice $adj(C)$ a tedy i C^{-1} jsou celá čísla. Číslo β tedy můžeme psát ve tvaru $\beta = \alpha C^{-1}\Theta^*$. Z toho plyne, že čísla $[\theta_1^*, \theta_2^*]$ tvoří bázi algebraických čísel tělesa T, neboť lze pomocí nich vyjádřit každé celé algebraické číslo z tělesa T. Platí $\mathcal{B} = \mathcal{C}$ a věta je tím dokázána. □

Příklad 4.4. Dokažte, že číslo

$$\begin{vmatrix}\theta_1 & \theta_1' \\ \theta_2 & \theta_2'\end{vmatrix}^2$$

je nezávislé na volbě báze a je závislé jen na tělese (je to diskriminant tělesa).

Řešení. Nechť $[\theta_1, \theta_2], [\theta_1^*, \theta_2^*]$ jsou báze tělesa T a

$$\theta_1^* = x\theta_1 + y\theta_2,$$
$$\theta_2^* = u\theta_1 + v\theta_2.$$

Označme si

$$\Theta = \begin{bmatrix}\theta_1 \\ \theta_2\end{bmatrix}, \quad \Theta^* = \begin{bmatrix}\theta_1^* \\ \theta_2^*\end{bmatrix}, \quad \Theta' = \begin{bmatrix}\theta_1' \\ \theta_2'\end{bmatrix}, \quad (\Theta^*)' = \begin{bmatrix}(\theta_1^*)' \\ (\theta_2^*)'\end{bmatrix}, \quad M = \begin{bmatrix}x & y \\ u & v\end{bmatrix}.$$

Potom platí

$$\Theta^* = M\Theta, \quad (\Theta^*)' = M\Theta',$$

a

$$(\Theta^*, (\Theta^*)') = (M\Theta, M\Theta') = M(\Theta, \Theta').$$

Opět podle Cauchyovy věty o součinu determinantů máme

$$det(\Theta^*, (\Theta^*)') = det(M)det(\Theta, \Theta').$$

Podle příkladu 4.3 je $det(M) = \pm 1$, tedy

$$det(\Theta^*, (\Theta^*)')^2 = det(M)^2 det(\Theta, \Theta')^2 = det(\Theta, \Theta')^2.$$

Diskriminant tělesa je tedy na volbě báze nezávislý. □

Příklad 4.5. Dokažte, že těleso $\mathbb{Q}(\sqrt{d})$ má diskriminant rovný číslu d, resp. $4d$ podle toho, jestli $d \equiv 1 \pmod 4$ nebo ne.

Řešení. Nechť $d \not\equiv 1 \pmod 4$, $\theta_1 = a_1 + a_2\sqrt{d}$ a $\theta_2 = b_1 + b_2\sqrt{d}$. Pak

$$\begin{vmatrix} \theta_1 & \theta_1' \\ \theta_2 & \theta_2' \end{vmatrix}^2 = ((a_1b_1 - a_1b_2\sqrt{d} + a_2b_1\sqrt{d} - a_2b_2d) - (a_1b_1 + a_1b_2\sqrt{d} - a_2b_1\sqrt{d} - a_2b_2d))^2 =$$
$$= (2\sqrt{d})^2(a_2b_1 - a_1b_2)^2 = 4d(a_2b_1 - a_1b_2)^2.$$

Podle příkladu 4.3 je $(a_2b_1 - a_1b_2) = \pm 1$, tedy

$$\begin{vmatrix} \theta_1 & \theta_1' \\ \theta_2 & \theta_2' \end{vmatrix}^2 = 4d.$$

Nyní nechť $d \equiv 1 \pmod 4$, $\theta_1 = a_1 + a_2\frac{1-\sqrt{d}}{2}$ a $\theta_2 = b_1 + b_2\frac{1-\sqrt{d}}{2}$. Pak

$$\begin{vmatrix} \theta_1 & \theta_1' \\ \theta_2 & \theta_2' \end{vmatrix}^2 = \left(\frac{1-\sqrt{d}}{2} - \frac{1+\sqrt{d}}{2}\right)^2 (a_2b_1 - a_1b_2)^2 = d(a_2b_1 - a_1b_2)^2 = d. \qquad \square$$

Příklad 4.6. Dokažte, že v tělese $\mathbb{Q}(\sqrt{5})$ platí

(a) čísla $2 + \sqrt{5}, 2 - \sqrt{5}$ jsou jednotkami,

(b) čísla $3 + \sqrt{5}, 1 - \sqrt{5}$ jsou asociované, nejsou však jednotkami,

(c) čísla $4 + \sqrt{5}, 4 - \sqrt{5}$ jsou algebraickými prvočísly.

Řešení. (a) Algebraické celé číslo je jednotkou, pokud dělí číslo 1. Musí platit $2+\sqrt{5} \mid 1$ a $2 - \sqrt{5} \mid 1$, tedy čísla $\frac{1}{2+\sqrt{5}}$ a $\frac{1}{2-\sqrt{5}}$ musí být celá algebraická čísla.

$$\frac{1}{2+\sqrt{5}} = \frac{1}{2+\sqrt{5}}\frac{2-\sqrt{5}}{2-\sqrt{5}} = \frac{2-\sqrt{5}}{4-5} = -2 + \sqrt{5} = -3 + 2\frac{1+\sqrt{5}}{2},$$
$$\frac{1}{2-\sqrt{5}} = \frac{1}{2-\sqrt{5}}\frac{2+\sqrt{5}}{2+\sqrt{5}} = \frac{2+\sqrt{5}}{4-5} = -2 - \sqrt{5} = -1 - 2\frac{1+\sqrt{5}}{2}.$$

Čísla $\frac{1}{2+\sqrt{5}}$ a $\frac{1}{2-\sqrt{5}}$ jsou celá algebraická čísla tělesa $\mathbb{Q}(\sqrt{5})$ a tedy $2 + \sqrt{5}$ a $2 - \sqrt{5}$ jsou jednotkami.

(b) Aby byly čísla $3+\sqrt{5}, 1-\sqrt{5}$ jsou asociovaná, musí platit $3+\sqrt{5} \mid 1-\sqrt{5}$ a zároveň $1 - \sqrt{5} \mid 3 + \sqrt{5}$.

$$\frac{1-\sqrt{5}}{3+\sqrt{5}} = -4 + 2\sqrt{5} = -6 + 4\frac{1+\sqrt{5}}{2}.$$
$$\frac{3+\sqrt{5}}{1-\sqrt{5}} = -2 - \sqrt{5} = -1 - 2\frac{1+\sqrt{5}}{2}.$$

Tedy čísla $3+\sqrt{5}, 1-\sqrt{5}$ jsou asociovaná, nejsou však jednotkami, protože

$$\frac{1}{3+\sqrt{5}} = \frac{3-\sqrt{5}}{4},$$
$$\frac{1}{1-\sqrt{5}} = \frac{1+\sqrt{5}}{-4},$$

nejsou celá algebraická čísla tělesa $\mathbb{Q}(\sqrt{5})$.

(c) Pokud bude norma čísel $4+\sqrt{5}, 4-\sqrt{5}$ prvočíslem, budou podle věty 46 čísla $4+\sqrt{5}$ a $4-\sqrt{5}$ algebraická prvočísla.

$$N(4+\sqrt{5}) = (4+\sqrt{5})(4-\sqrt{5}) = 16-5 = 11,$$
$$N(4-\sqrt{5}) = (4-\sqrt{5})(4+\sqrt{5}) = 16-5 = 11.$$

Číslo 11 je opravdu prvočíslo, tedy $4+\sqrt{5}$ a $4-\sqrt{5}$ jsou algebraická prvočísla. □

5. Gaussova celá čísla

5.1. Aritmetika Gaussových čísel

Definice 24. Celá algebraická čísla tělesa $\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(i)$ nazveme *Gaussovými celými čísly*. Jsou to tedy čísla tvaru $a + bi$, kde $a, b \in \mathbb{Z}$.

Věta 51. *Mějme dvě Gaussova celá čísla α, β, $\beta \neq 0$, pak existují Gaussova celá čísla ν a μ takové, že platí*

$$\alpha = \beta\mu + \nu, \text{ kde } N(\nu) < N(\beta).$$

Důkaz. Nechť $\frac{\alpha}{\beta} = A + Bi$, kde $A, B \in \mathbb{Q}$, a x, y jsou celá čísla taková, že platí

$$|A - x| \leq \frac{1}{2},$$
$$|B - y| \leq \frac{1}{2}.$$

Mějme nyní Gaussova celá čísla $\mu = x+iy$ a $\nu = \alpha-\mu\beta$. Tyto čísla splňují požadované vlastnosti:

$$\nu = \alpha - \mu\beta = \beta\left(\frac{\alpha}{\beta} - \mu\right) = \beta(A + Bi - x - iy) = \beta[(A - x) + i(B - y)],$$

tedy podle věty 30 přejdeme k normám a dostáváme

$$N(\nu) = N(\beta)[(A - x)^2 + (B - y)^2] \leq N(\beta)\left(\frac{1}{4} + \frac{1}{4}\right) = \frac{1}{2}N(\beta) \leq N(\beta). \qquad \square$$

Definice 25. Gaussovo celé číslo δ nazveme *největším společným dělitelem* dvou Gaussových celých čísel α a β, pokud

(a) δ dělí α i β,

(b) každé další Gaussovo celé číslo, dělící α a β, dělí i δ.

Euklidův algoritmus pro Gaussova celá čísla. Pro každá dvě Gaussova celá čísla α, β, z nichž alespoň jedno z nich je různé od nuly, existuje největší společný dělitel δ. Ten je až na asociovanost určen jednoznačně a lze vyjádřit ve tvaru

$$\delta = \alpha\xi + \beta\eta,$$

kde ξ a η jsou Gaussova celá čísla.

Důkaz. Předpokládejme $\beta \neq 0$. Podle věty 51 můžeme sestavit systém rovnic

$$\begin{aligned}
\alpha &= \mu_0\beta + \nu_0, N(\nu_0) < N(\beta),\\
\beta &= \mu_1\nu_0 + \nu_1, N(\nu_1) < N(\nu_0),\\
\nu_0 &= \mu_2\nu_1 + \nu_2, N(\nu_2) < N(\nu_1),\\
&\vdots\\
\nu_{k-2} &= \mu_k\nu_{k-1} + \nu_k, N(\nu_k) < N(\nu_{k-1}),\\
\nu_{k-1} &= \mu_{k+1}\nu_k,
\end{aligned}$$

kde $k \in \mathbb{N}$, $\mu_0, \mu_1, \dots \mu_{k+1}, \nu_0, \nu_1, \dots \nu_{k+1}$ jsou Gaussova celá čísla. Dostáváme klesající posloupnost

$$N(\beta) > N(\nu_0) > N(\nu_1) > \cdots > N(\nu_k) > N(\nu_{k+1}) = 0,$$

tedy pro určité k musí platit $N(\nu_{k+1}) = 0$. Gaussovo celé číslo $\nu_k = \delta$ potom je největší společný dělitel čísel α a β.

Stejně jako u polynomů, upravíme rovnice Euklidova algoritmu pro Gaussova celá čísla a postupným dosazováním dostaneme rovnici

$$\delta = \nu_k = \alpha\xi + \beta\eta,$$

kde ξ a η jsou Gaussova celá čísla. □

Definice 26. Pokud je největší společný dělitel dvou Gaussových celých čísel jednotka, nazveme je *nesoudělnými*.

Věta 52. *Nechť α, β, γ jsou Gaussova celá čísla, α a β jsou nesoudělná a $\alpha \mid \beta\gamma$. Pak $\alpha \mid \gamma$.*

Důkaz. Čísla α a β jsou nesoudělná, existují tedy Gaussova celá čísla ξ, η tak, že platí $\alpha\xi + \beta\eta = 1$. Celou rovnici vynásobíme číslem γ, dostáváme $\alpha\gamma\xi + \beta\gamma\eta = \gamma$. Zřejmě $\alpha \mid \alpha\gamma$ a podle předpokladu $\alpha \mid \beta\gamma$, tedy $\alpha \mid \alpha\gamma\xi + \beta\gamma\eta$, tj. $\alpha \mid \gamma$. □

Definice 27. Algebraická prvočísla tělesa $\mathbb{Q}(i)$ budeme nazývat *Gaussovými prvočísly*.

Věta 53. *Mějme Gaussovo prvočíslo π a Gaussova celá čísla α, β. Když $\pi \mid \alpha\beta$ a $\pi \nmid \beta$, platí $\pi \mid \alpha$.*

Důkaz. Protože $\pi \nmid \beta$, jsou π a β nesoudělná, podle věty 52 $\pi \mid \alpha$. □

Věta 54. *Nechť je π Gaussovo prvočíslo, $\alpha_1, \alpha_2, \dots, \alpha_k$ jsou Gaussova celá čísla, $k \in \mathbb{N}$. Pokud $\pi \mid \alpha_1\alpha_2 \dots \alpha_k$, pak pro alespoň jedno $i \in \mathbb{N}, 0 < i \leq k$, platí $\pi \mid \alpha_i$.*

Důkaz. Jestliže platí $\pi \mid \alpha_1$, je věta dokázána. Jinak $\pi \nmid \alpha_1$ a podle věty 53 dostáváme $\pi \mid \alpha_2\alpha_3 \dots \alpha_k$. Pokud opět $\pi \nmid \alpha_2$, máme $\pi \mid \alpha_3\alpha_4 \dots \alpha_k$. Podobně můžeme pokračovat, dokud nezůstane jen $\pi \mid \alpha_k$, π teda dělí aspoň jedno z čísel $\alpha_1, \alpha_2, \dots, \alpha_k$. □

Věta 55. *Nechť je α Gaussovo celé číslo, $|N(\alpha)| > 1$. Pak lze toto číslo rozložit v součin konečného počtu Gaussových prvočísel. Až na pořadí a asociativitu dělitelů je tento rozklad jednoznačný.*

Důkaz. Existenci rozkladu jsme dokázali ve větě 47, nyní dokážeme ještě jednoznačnost.

Nechť $\alpha = \pi_1\pi_2 \dots \pi_n$ a $\alpha = \pi_1^*\pi_2^* \dots \pi_m^*$ jsou dva rozklady čísla α, $n, m \in \mathbb{N}$. Platí $\pi_1 \mid \alpha$, tedy $\pi_1 \mid \pi_1^*\pi_2^* \dots \pi_m^*$ a podle věty 54 $\pi_1 \mid \pi_i^*$ pro nějaké $i \in \mathbb{N}, 0 < i \leq k$. Čísla π_1 i π_i^* jsou Gaussova prvočísla a platí $\pi_i^* = \varepsilon_1\pi_1$, kde ε_1 je jednotka. Můžeme tedy vydělit oba rozklady číslem π_i^* a zároveň si přeznačíme druhý rozklad tak, aby $\pi_i^* = \pi_1^{**}$. Dostáváme tedy

$$\pi_2\pi_3 \dots \pi_n = \varepsilon_1\pi_2^{**}\pi_3^{**} \dots \pi_m^{**}.$$

Tento postup opakujeme, dokud na jedné straně nezbude žádné Gaussovo prvočíslo.

Pokud by bylo $n < m$, dostali bychom po n krocích

$$1 = \varepsilon^*\tilde{\pi}_{n+1} \dots \tilde{\pi}_m,$$

to ovšem není možné. Stejně by dopadl i případ $n > m$. Musí tedy platit, že $n = m$ a oba rozklady jsou až na pořadí a asociativitu dělitelů shodné. □

Věta 56. *Nechť π je Gaussovo prvočíslo. Potom existuje právě jedno prvočíslo $p > 0, p \in \mathbb{Z}$ takové, že platí $\pi \mid p$.*

Důkaz. Provedeme sporem. Předpokládejme, že máme dvě různé prvočísla p_1, p_2, $\pi \mid p_1$ a $\pi \mid p_2$. Tedy $\pi \mid \xi p_1 + \eta p_2$, kde ξ, η jsou celá Gaussova čísla. Prvočísla p_1 a p_2 jsou nesoudělná, existují proto dvě celá čísla x, y a platí $1 = xp_1 + yp_2$. π by tedy muselo dělit číslo 1, ale to není možné. □

Věta 57. *Nechť jsou α, β, μ Gaussova celá čísla, α, β jsou nesoudělná a $\alpha\beta = \mu^n$, kde $n \in \mathbb{N}$. Pak je každé z čísel α, β asociované s n-tou mocninou Gaussova celého čísla.*

Důkaz. Podle věty 55 lze jednoznačně rozložit číslo μ na součin Gaussových prvočísel. Nechť tedy $\mu = \pi_1\pi_2 \dots \pi_k$ je rozklad čísla μ, $k \in \mathbb{N}$. Dostáváme

$$\alpha\beta = \pi_1^n\pi_2^n \dots \pi_k^n.$$

Čísla α, β jsou nesoudělná, jestliže jedno z čísel α, β bude dělitelné určitým Gaussovým prvočíslem π_s, bude dělitelné i jeho n-tou mocninou π_s^n. Žádné Gaussovo prvočíslo nemůže dělit α i β. Čísla α, β jsou tedy asociovaná s n-tou mocninou Gaussova čísla. □

5.2. Aplikace

Problém 1. *Najděte všechna řešení diofantické rovnice*

$$x^2 + y^2 = z^2, \tag{5.1}$$

kde x, y, z jsou kladná celá čísla a $(x, y) = 1$.

Řešení. Čísla x, y nemohou být sudá, protože by neplatil předpoklad $(x, y) = 1$. Nemohou být ani obě lichá, jelikož $x^2+y^2 \equiv 1+1 \pmod 4$, potom by muselo platit $z^2 \equiv 2 \pmod 4$, ale to není možné. Tedy jedno z čísel x, y je sudé, druhé liché, číslo z je také liché.

Nyní můžeme rovnici 5.2 přepsat pomocí Gaussových celých čísel:

$$(x + yi)(x - yi) = z^2.$$

Tyto Gaussova celá čísla $x + yi$ a $x - yi$ jsou nesoudělná. To můžeme dokázat nepřímo.

Předpokládejme, že existuje Gaussovo celé číslo δ, které není jednotkou a je největší společný dělitel čísel $x + yi$ a $x - yi$. Potom δ dělí taky rozdíl a součet těchto čísel, tedy $\delta \mid 2x$ a $\delta \mid 2y$. Čísla x, y jsou ovšem nesoudělná i v oboru integrity Gaussových celých čísel, δ může dělit nejvýše číslo 2, je tedy asociované buď s číslem $1 + i$, nebo 2.

Kdyby bylo δ asociované s $1 + i$, číslo $\frac{x+yi}{1+i} = \frac{x+y}{2} + i\frac{x-y}{2}$ by muselo být Gaussovo celé číslo. Ale to by platilo, jen pokud by x, y byla obě buď sudá, nebo lichá.

Podobně nemůže být δ asociované ani s 2, aby bylo $\frac{x+yi}{2}$ Gaussovo celé musela by x, y být sudá.

Nyní, protože víme, že $x + yi$ a $x - yi$ jsou nesoudělná, můžeme použít větu 57, každé z čísel $x + yi$ a $x - yi$ je asociované s druhou mocninou nějakého Gaussova celého čísla:

$$x + yi = \varepsilon\alpha^2,$$

kde $\alpha = a + bi$, $a, b \in \mathbb{Z}$ a ε je jednotkou. Jednotky v Gaussových číslech jsou $1, -1, i, -i$, jednotně je můžeme zapsat jako i^r, kde $r = 0, 1, 2, 3$. Naši rovnici upravíme:

$$x + yi = i^r(a + bi)^2 = i^r(a^2 + 2abi - b^2) = i^r(a^2 - b^2) + i^{r+1}2ab.$$

Když porovnáme reálné a imaginární části této rovnice, dostáváme

$$x = \pm(a^2 - b^2), \quad y = \pm 2ab, \quad \text{pro } i = 0 \text{ nebo } i = 2,$$

nebo

$$x = \mp 2ab, \quad y = \pm(a^2 - b^2), \quad \text{pro } i = 1 \text{ nebo } i = 3.$$

Pro komplexně sdružená čísla platí:

$$x - yi = i^{-r}(a - bi)^2,$$

tedy

$$z = \pm\sqrt{(x + yi)(x - yi)} = \pm(a^2 + b^2).$$

Nyní vyřešíme, jaká mají být čísla a, b, aby byly splněny podmínky $x > 0, y > 0, z > 0$, $(x, y) = 1$. Jedno z čísel x, y má být sudé, druhé liché, požadujme tedy navíc, aby x bylo sudé, y liché. Tomuto případu vyhovují rovnice

$$x = \mp 2ab, \quad y = \pm(a^2 - b^2) \quad z = \mp(a^2 + b^2).$$

Dosazením každé z trojic x, y, z do rovnice 5.2 se přesvědčíme, že tato rovnice opravdu platí.

Protože má být z kladné, můžeme brát v úvahu jen spodní znaménka. Aby byla i čísla x, y kladná, musí platit $0 < a < b$, na splnění nesoudělnosti x a y musí být a, b nesoudělná a různé parity.

(V případě, že by platilo $(a, b) > 1$, nebyla by čísla x, y nesoudělná.

Když naopak zvolíme a, b nesoudělná a různé parity, můžeme nepřímo dokázat, že $(x, y) = 1$. Předpokládejme, že $(x, y) = d > 1$. Potom d dělí i součet x a y, tedy $d \mid (a^2+b^2)$, $d \mid (a^2 - b^2)$ a také $d \mid 2a^2$, $d \mid 2b^2$. Čísla a, b jsou nesoudělná, muselo by platit $d \mid 2$, to je $d = 2$. To ale není možné, protože y je liché číslo a nemůže být dělitelné číslem 2.) □

Dokázali jsme:

Věta 58. *Řešení diofantické rovnice*

$$x^2 + y^2 = z^2,$$

x, y, z jsou celá kladná čísla, x je sudé, y, z jsou liché a $(x, y) = 1$, je určeno rovnicemi

$$x = 2ab, \quad y = b^2 - a^2 \quad z = a^2 + b^2,$$

kde $a, b \in \mathbb{Z}$, $0 < a < b$, a, b jsou nesoudělná a různé parity.

Problém 2. *Najděte všechna řešení diofantické rovnice*

$$x^2 + 4 = y^3, \tag{5.2}$$

kde x, y jsou celá čísla.

Řešení. Opět si rozložíme levou stranu rovnice pomocí Gaussových celých čísel:

$$(x+2i)(x-2i) = y^3.$$

Podle parity x budeme rozlišovat dva případy:

(1) Předpokládejme, že x je liché. Potom jsou čísla $(x+2i), (x-2i)$ nesoudělná.

Kdyby totiž existovalo Gaussovo celé číslo δ, které není jednotkou, a dělilo by čísla $(x+2i)$ a $(x-2i)$, pak by dělilo i jejich součet a rozdíl, tj. $\delta \mid 2x$ a $\delta \mid 4i$. Označme si $\pi = (i+1)$, π je Gaussovo prvočíslo. Nyní můžeme psát $2 = -i\pi^2$, $4 = \pi^4$. Protože δ není jednotkou musí platit $\pi \mid \delta$, tedy $\pi \mid (x+2i)$. Dále máme $\pi \mid 2i$, z toho plyne, že také $\pi \mid x$. Po přechodu k normám máme $N(\pi) \mid N(x)$, tedy $2 \mid x^2$, což je ale spor, protože x je liché.

Stejně jako u minulé rovnice použijeme větu 57 a dostáváme

$$x + 2i = i^r(a_1 + ib_1)^3,$$
$$x - 2i = i^{-r}(a_1 - ib_1)^3.$$

Platí $1^3 = 1, i^3 = -i, (-1)^3 = -1, (-i)^3 = i$, každá jednotka je tedy třetí mocninou (liší se jen znaménkem pro r liché). Jednotky i^r tedy můžeme vsunout do závorek:

$$x + 2i = (a + ib)^3,$$
$$x - 2i = (a - ib)^3,$$

kde $a, b \in \mathbb{Z}$. Odečtením rovnic máme

$$x = a^3 - 3ab^2, \tag{5.3}$$
$$2 = b(3a^2 - b^2). \tag{5.4}$$

Z druhé rovnice vidíme, že může být $b = \pm 1$ nebo $b = \pm 2$.

(a) V případě $b = \pm 1$ je $3a^2 - b^2 = \pm 2$, tedy $a = \pm 1$, ale to není možné, protože by x bylo sudé.

(b) V případě $b = \pm 2$ je $3a^2 - b^2 = \pm 1$, tedy $a = \pm 1$. Kdyby bylo $b = 2$, neměla by rovnice 5.4 řešení.

Pro $b = -2$ a $a = \pm 1$ tedy dostáváme výsledky $x = \pm 11$ a $y = 5$.

(2) Nechť je x sudé, můžeme ho psát ve tvaru $x = 2u$. Potom je sudé i y, píšeme $y = 2v$, $u, v \in \mathbb{Z}$. Dostáváme tedy rovnici

$$u^2 + 1 = 2v^3.$$

Pravá strana rovnice je sudá, aby byla sudá i levá strana, musí být u liché. Rovnici můžeme upravit na tvar

$$\left(\frac{u+1}{2}\right)^2 + \left(\frac{u-1}{2}\right)^2 = v^3.$$

Čísla $\frac{u+1}{2}$ a $\frac{u+1}{2}$ jsou nesoudělná. Kdyby totiž měly největšího společného dělitele δ, který by nebyl jednotkou, platilo by, že δ dělí i jejich součet a rozdíl. Dělil by tedy číslo 1, ale tady dostáváme spor.

Použijeme Gaussova celá čísla a větu 57, jednotky i^r, kde $r = 0, 1, 2$ nebo 3, opět vsuneme do závorek:

$$\left(\frac{u+1}{2} + \frac{u-1}{2}i\right)\left(\frac{u+1}{2} - \frac{u-1}{2}i\right) = v^3,$$

$$\left(\frac{u+1}{2} + \frac{u-1}{2}i\right) = (a+bi)^3,$$
$$\left(\frac{u+1}{2} - \frac{u-1}{2}i\right) = (a-bi)^3,$$

kde $a, b \in \mathbb{Z}$. Porovnáním reálné a imaginární části dostáváme

$$\frac{u+1}{2} = a^3 - 3ab^2,$$
$$\frac{u-1}{2} = 3a^2b - b^3,$$

čísla a, b musí být nesoudělná a různé parity. Rovnice odečteme:

$$a^3 - 3a^2b - 3ab^2 + b^3 = 1,$$
$$(a+b)(a^2 - 4ab + b^2) = 1,$$

tedy $a + b = \pm 1$, $a^2 - 4ab + b^2 = \mp 1$.

Rovnice se spodním znaménkem nemají žádné celočíselné řešení. Pro horní znaménko jsou řešením dvě dvojice čísel $a = 1, b = 0$ a $a = 0, b = 1$, tedy $u = \pm 1, x = \pm 2$ a $y = 2$. □

Věta 59. *Diofantické rovnice*

$$x^2 + 4 = y^3,$$

má pro $x, y \in \mathbb{Z}$ právě 4 dvojice řešení: $(-11, 5), (11, 5), (-2, 2)$ *a* $(2, 2)$.

6. Závěr

Věta 60. *V okruhu celých čísel kvadratického tělesa* $\mathbb{Q}(\sqrt{-5})$ *neplatí věta o jednoznačnosti rozkladu na algebraická prvočísla.*

Důkaz. Celé číslo 6 kvadratického tělesa $\mathbb{Q}(\sqrt{-5})$ můžeme rozložit na

$$21 = (1 + 2\sqrt{-5})(1 - 2\sqrt{-5}) = 3 \cdot 7.$$

Dokážeme, že čísla $\pi_1 = (1 + 2\sqrt{-5}), \pi_2 = (1 - 2\sqrt{-5}), \pi_3 = 3, \pi_4 = 7$ jsou algebraická prvočísla a π_1 není asociované s π_3 ani s π_4.

a) Důkaz provedeme sporem. Předpokládejme, že 3 není algebraické prvočíslo. Pak musí existovat dvě celá algebraická čísla $\alpha_1 = x_1 + y_1\sqrt{-5}, \alpha_2 = x_2 + y_2\sqrt{-5}$, $x_1, x_2, y_1, y_2 \in \mathbb{Q}$, a platí

$$3 = \alpha_1\alpha_2 = (x_1 + y_1\sqrt{-5})(x_2 + y_2\sqrt{-5}).$$

Přejdeme k normám a dostáváme

$$9 = (x_1^2 + 5y_1^2)(x_2^2 + 5y_2^2).$$

Nyní může být $x_1^2 + 5y_1^2 = 1, 3$ nebo 9.

Pokud by platilo $x_1^2 + 5y_1^2 = 1$, dostáváme pro x_1, y_1 celočíselná řešení $(\pm 1, 0)$, ale to jsou jednotky a každé prvočíslo je dělitelné jednotkami.

V případě $x_1^2 + 5y_1^2 = 3$ není rovnice vůbec řešitelná pro $x_1, y_1 \in \mathbb{Z}$.

A konečně řešením rovnice $x_1^2+5y_1^2 = 9$ jsou dvojice čísel $(\pm 3, 0)$ a $(\pm 2, \pm 1)$. Dvojice $(\pm 3, 0)$ nám nedává nového dělitele a čísla $\pm 2 \pm \sqrt{-5}$ nejsou vůbec dělitelé čísla 3.

Podobně se ověří, že ani další z čísel $(1+2\sqrt{-5}), (1-2\sqrt{-5})$ a 7 není algebraickým prvočíslem.

b) Číslo π_1 je asociované s π_3 nebo π_4, když platí $\pi_1\varepsilon = \pi_3$ nebo $\pi_1\varepsilon = \pi_4$, kde ε je jednotkou. Podle věty 48 existují v tělese $\mathbb{Q}(\sqrt{-5})$ jen dvě jednotky: 1 a -1. Vynásobením čísla π_1 těmito jednotkami však nemůžeme dostat čísla π_3 a π_4. □

Definice 28. Nechť $\mathbb{Q}(\sqrt{d})$ je kvadratické těleso. Když $d < 0$ mluvíme o *imaginárním kvadratickém tělese*, v případě $d > 0$ o *reálném kvadratickém tělese.*

Definice 29. Kvadratické těleso $\mathbb{Q}(\sqrt{d})$, ve kterém platí věta o jednoznačnosti rozkladu, nazýváme *jednoduché těleso.* Z imaginárních kvadratických těles je jen 9 jednoduchých a to pro

$$d = -1, -2, -3, -7, -11, -19, -43, -67, -163.$$

Poznámka. V roce 1934 Heilbronn a Linfoot dokázali, že by mohlo existovat i desáté imaginární jednoduché těleso. Lehmer však ukázal, že hodnota $|d|$ by musela být vetší než $5 \cdot 10^9$. Heegner se v roce 1952 snažil dokázat, že žádné desáté imaginární těleso neexistuje, ovšem jeho důkaz obsahoval chyby. Nakonec se to povedlo až v roce 1966 Bakerovi a o rok později jinou metodou i Starkovi.

Gauss se na druhou stranu domníval, že reálných jednoduchých těles je nekonečně mnoho, i když důkaz ještě nebyl nalezen.

V určitých kvadratických tělesech tedy vzniká defekt v podobě nejednoznačnosti rozkladu na algebraická prvočísla. Důsledkem toho je, že v těchto tělesech nemůžeme používat zákony aritmetiky, na něž jsme zvyklí například z celých čísel nebo polynomů. Dvě čísla α, β z nejednoduchého tělesa nemusí mít vůbec největšího společného dělitele s vlastnostmi, které jsme požadovali dříve, a pokud ho mají, nemusí jít rozložit na tvar $\delta = \alpha\xi + \beta\eta$, kde ξ, η jsou ze stejného tělesa jako α, β. Proto by bylo vhodné tuto nejednoznačnost nějakým způsobem odstranit.

Jako první si tohoto problému všimnul v polovině 19. století Kummer. Ten navrhoval přidat do kvadratického tělesa určité prvky, kterým říkal „ideální čísla“, se kterými by v tomto tělese začala platit jednoznačnost rozkladu.

V důkazu věty 60 by to byla čísla ve tvaru $\sqrt{x + y\sqrt{-5}}$, $x, y \in \mathbb{Z}$. Pokud si označíme

$$j_1 = \sqrt{2 + \sqrt{-5}}, \qquad j_3 = \sqrt{-2 + 3\sqrt{-5}},$$
$$j_2 = \sqrt{2 - \sqrt{-5}}, \qquad j_4 = \sqrt{-2 - 3\sqrt{-5}},$$

dostáváme potom

$$3 = j_1 j_2,\ 7 = j_3 j_4,\ 1 + 2\sqrt{-5} = j_1 j_3,\ 1 - 2\sqrt{-5} = j_2 j_4, \text{ a tedy } 21 = j_1 j_2 j_3 j_4.$$

Tato „ideální čísla“ ovšem nepatří do tělesa $\mathbb{Q}(\sqrt{d})$, ale lze je vyjádřit pomocí $\mathbb{Z}[\theta]$. Např. číslo j_1 můžeme charakterizovat množinou celých algebraických čísel $\mathbb{Z}[\theta]$, které jsou dělitelné číslem j_1. Takovou množinu pojmenoval Dedekind ideálem.

Definice 30. Mějme čísla $\alpha_1, \alpha_2, \ldots, \alpha_n$ z oboru integrity celých algebraických čísel $\mathbb{Z}[\theta]$ kvadratického tělesa a aspoň jedno z $\alpha_1, \alpha_2, \ldots, \alpha_n$ je nenulové. Pak *ideálem z oboru integrity* $\mathbb{Z}[\theta]$ nazveme množinu čísel ve tvaru

$$\alpha_1\xi_1 + \alpha_2\xi_2 + \cdots + \alpha_n\xi_n,$$

kde $\xi_1, \xi_2, \ldots, \xi_n \in \mathbb{Z}[\theta]$. Tento ideál značíme $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Definice 31. Nechť $\mathbb{Z}[\theta]$ je obor integrity celých algebraických čísel a $\mathfrak{a} = (\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\mathfrak{b} = (\beta_1, \beta_2, \ldots, \beta_m)$ jsou ideály z tohoto oboru integrity, $n, m \in \mathbb{N}$. Pak *součinem ideálů* $\mathfrak{a}$ a $\mathfrak{b}$ rozumíme ideál

$$\mathfrak{ab} = (\alpha_1\beta_1, \alpha_1\beta_2, \ldots, \alpha_1\beta_m, \alpha_2\beta_1, \ldots, \alpha_n\beta_m).$$

Definice 32. Řekneme, že ideál z oboru integrity $\mathbb{Z}[\theta]$ je *hlavním ideálem*, pokud lze psát ve tvaru $\mathfrak{a} = (a)$

Poznámka. Podobně jako u celých čísel můžeme mezi ideály definovat dělitelnost, jednotkový ideál, ireducibilní prvky (prvoideály), největšího společného dělitele atp. Pro bližší informace nebo důkaz následujících vět viz např. [6].

Věta 61. *Nechť $\alpha, \beta \in \mathbb{Z}[\theta]$, pak $(\alpha) = (\beta)$, právě když jsou α a β asociované.*

Věta 62. *Nechť $\mathfrak{a}$ je nejednotkový ideál z oboru integrity $\mathbb{Z}[\theta]$. Pak ho můžeme rozložit na součin konečného počtu prvoideálů. Tento rozklad je až na pořadí faktorů jednoznačný.*

Literatura

[1] IRELAND, K., ROSEN, M.: *A Classical Introduction to Modern Number Theory*. New York: Springer-Verlag, 1982

[2] KARÁSEK, J., SKULA, L.: *Lineární algebra*. Brno: Akademické nakladatelství CERM, 2005

[3] KARÁSEK, J., SKULA, L.: *Obecná algebra*. Brno: Akademické nakladatelství CERM, 2008

[4] KONEČNÝ, Z.: *Užití počítačů v teorii čísel*. Brno, 2009

[5] RIBENBOIM, P.: *Classical Theory of Algebraic Numbers*. New York: Springer-Verlag, 2001

[6] SCHWARZ, Š.: *Algebraické čísla*. Praha: Přírodovědecké nakladatelství, 1950