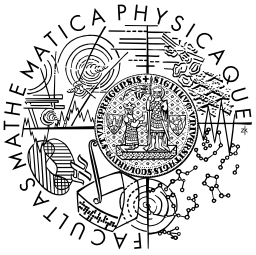

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁRSKA PRÁCA

Simona Hlavinková

Štruktúra zovšeobecnených pytagorejských trojíc

Katedra algebry

Vedúci bakalárskej práce: doc. Mgr. Vítězslav Kala, Ph.D.

Študijný program: Obecná matematika

Praha 2023

Prehlasujem, že som túto bakalársku prácu vypracovala samostatne a výhradne s použitím citovaných prameňov, literatúry a ďalších odborných zdrojov. Táto práca nebola využitá na získanie iného alebo rovnakého titulu.

Beriem na vedomie, že sa na moju prácu vzťahujú práva a povinnosti vyplývajúce zo zákona č. 121/2000 Sb., autorského zákona v platnom znení, najmä skutočnosť, že Univerzita Karlova má právo na uzatvorenie licenčnej zmlúvy o použití tejto práce ako školského diela podľa §60 odst. 1 autorského zákona.

V ..... dňa ....

Podpis autorky

Moje poďakovanie patrí vedúcemu práce doc. Mgr. Vítězslavovi Kalovi, Ph.D za jeho trpezlivosť a čas. Ďakujem Bohu za to, že ma počas celého štúdia sprevádzal pri tých najťažších chvíľach. Chcela by som poďakovať Bc. Tatiane Piliarovej za gramatické pripomienky. V neposlednom rade patrí veľká vďaka mojej rodine, priateľovi a spolubývajúcim za podporu v každej chvíli.

Názov práce: Štruktúra zovšeobecnených pytagorejských trojíc

Autorka: Simona Hlavinková

Katedra: Katedra algebry

Vedúci bakalárskej práce: doc. Mgr. Vítězslav Kala, Ph.D., Katedra algebry

Abstrakt: Hlavnou motiváciou pre našu prácu je popísanie zovšeobecnených pytagorejských trojíc. Tento problém prevedieme na problém hľadania riešenia rovnice $|x^2+Dy^2| = z^2$. Cieľom tejto práce je podrobne dokázať štruktúru a počet riešení rovnice $|x^2 + Dy^2| = z^2$ pre $-D \equiv 2{,}3 \pmod 4$ bezštvorcové. Dôkazy čiastkových lem budeme robiť v ideálovej triednej grupe číselného telesa $\mathbb{Q}[\sqrt{-D}]$. Najprv dokážeme lemu, ktorá nám dá nevyhnutné podmienky pre existenciu riešenia. Popíšeme súvislosť jednoznačnosti, respektíve nejednoznačnosti riešenia a voľby D. Kľúčovým krokom dôkazu je vyjadrenie riešenia v špeciálnom tvare. Zároveň uvedieme príklady štruktúr ideálových triednych grup pre rôzne číselné telesá.

Kľúčové slová: zovšeobecnené pytagorejské trojice, diofantické rovnice, číselné teleso, okruh celistvých prvkov číselného telesa, ideálová triedna grupa

Title: Structure of generalized Pythagorean triples

Author: Simona Hlavinková

Department: Department of algebra

Supervisor: doc. Mgr. Vítězslav Kala, Ph.D., Department of Algebra

Abstract: The motivation for our thesis is to describe generalized of Phytagorean triples. We convert this problem into the problem of finding a solution of the equation $|x^2+Dy^2| = z^2$. The goal of this thesis is to prove in detail the structure and the number of solutions of the equation $|x^2 + Dy^2| = z^2$ for $-D \equiv 2{,}3 \pmod 4$ and square-free. The proofs of lemmas are proved by using properties of ideal class group of number field $\mathbb{Q}[\sqrt{-D}]$. We first prove a lemma that gives us the necessary conditions for the existence of a solution. We describe the connection between uniqueness, respectively ambiguity of the solution and the choice of D. The most important step of the proof is to express the solution in a special form. We also give examples of structure of ideal class group of various number fields.

Keywords: generalized Phytagorean triples, diophantine equation, number field, set of algebraic integers of number field, ideal class group

Obsah

Úvod

Riešenie diofantických rovníc, čiže hľadanie riešenia pre $f(x_1 \dots x_n) = 0$ pre nejaký polynóm f, má bohatú históriu. Rovnica $x^2 + y^2 = z^2$ sa používa pre hľadanie takzvaných pytagorejských trojíc. Pomocou Pellovej rovnice $x^2 - Dy^2 = \pm 1$, kde $D \in \mathbb{N}$ bezštvorcové, dokážeme nájsť jednotky kvadratických rozšírení $\mathbb{Z}[\sqrt{-D}]$. Jej riešenie dokážeme popísať pomocou reťazových zlomkov [1, Kapitola 2]. Zaujímavým prípadom tejto rovnice je aj rovnica $x^2 + Dy^2 = z^2$, pomocou ktorej dokážeme popísať takzvané zovšeobecnené pytagorejské trojice.

V tejto práci sa budeme venovať riešeniu rovnice

$$|x^2 + Dy^2| = z^2 \tag{1}$$

pre ľubovoľné bezštvorcové D také, že $-D \equiv 2{,}3 \pmod 4$. Všimnime si, že pre voľbu $D = 1$ dostávame pytagorejské trojice a pre $D < 0$ spolu s $z = \pm 1$ máme Pellovu rovnicu.

Existuje viac spôsobov, ako môžeme na rovnicu (1) nahliadať. V hlavnom zdroji práce, v článku Connections of class numbers to the group structure of generalized Pythagorean triples od autorov Jaklitscha, Martineza, Millera, a Mukherjeea [2], na rovnicu (1) nahliadajú ako na kvadratickú formu reprezentujúcu číslo z^2 pre $D > 0$ také, že $-D \equiv 2{,}3 \pmod 4$. Zároveň na ňu môžeme nahliadať ako na diofantickú rovnicu. V tejto práci budeme pracovať v kvadratickom rozšírení $\mathbb{Q}[\sqrt{-D}]$ pre $-D \equiv 2{,}3 \pmod 4$ a jeho ideálovej triednej grupe.

V kapitole 1 tejto práce sa budeme venovať zavádzaniu základných pojmov a definic, vyslovíme aj základné vety, ktoré k ďalšiemu dokazovaniu budeme potrebovať.

Sekcia 1.1 je zameraná na základné algebraické definície. V sekcii 1.2 uvedieme základné vlastnosti okruhu celistvých prvkov a vyslovíme aj vetu 1.24 o rozklade ideálov na prvoideály.

Keďže autori článku [2] volia prístup cez kvadratické formy a my budeme pracovať v ideáloch okruhu celistvých prvkov kvadratického rozšírenia $\mathbb{Q}[\sqrt{-D}]$ pre $-D \equiv 2{,}3 \pmod 4$, tak v sekcii 1.3 uvedieme medzi týmito dvomi štruktúrami základný vzťah.

Sekcia 1.4 je venovaná náznaku zovšeobecnenia pre nie bezštvorcové D. Zavedieme pojem rádu a uvedieme jeho základné vlastnosti spolu s pravidlami pre prácu s nimi.

Kapitola 2 je zameraná na explicitné dokazovanie vety opisujúcej štruktúru a počet riešení rovnice (1). V kapitole 2.1 dokážeme vetu 2.11 o tvare c pre riešenie (a,b,c) a základnú vetu 2.4 definujúcu nevyhnutné podmienky pre existenciu riešenia.

Sekcia 2.2 je venovaná faktorizácii v množine prvkov $a + b\sqrt{-D} \in \mathbb{Q}[\sqrt{-D}]$, ktoré majú normu v absolútnej hodnote jednotkovú. Zároveň vyslovíme a dokážeme vetu 2.6 o jednoznačnosti, respektíve nejednoznačnosti, riešenia. Vo vete 2.8 opíšeme štruktúru riešenia pomocou špeciálne zavedeného pohľadu.

V sekcii 2.3 vyslovíme a dokážeme vetu 2.13, ktorá je hlavnou vetou tejto práce, opisujúcu štruktúru a počet riešení rovnice (1) pre bezštvorcové D a $-D \equiv$

2,3 (mod 4). Zároveň dokážeme aj vetu a lemu, ktoré čiastočne dokazujú hlavnú vetu.

Sekcia 2.4 je venovaná základným príkladom, v ktorých rozoberieme základné možnosti, ktoré môžu nastať pre ideálove triedne grupy kvadratického rozšírenia $\mathbb{Q}[\sqrt{-D}]$.

Teraz popíšeme vlastný prínos autorky práce. Všeobecne povedané, hlavným prínosom je prepracovanie dôkazov z článku [2] z jazyka kvadratických foriem do jazyka ideálových triedných grup. Zároveň článok [2] dokazuje štruktúru a počet riešení pre rovnicu $x^2 + Dy^2 = z^2$ pre $D > 0$, $-D \equiv 2{,}3 \pmod 4$ a D bezštvorcové, my vďaka práci s rovnicou (1) môžeme tvrdenia dokazovať pre ľubovoľné bezštvorcové D také, že $-D \equiv 2{,}3 \pmod 4$.

Toto prepracovanie bolo náročné najmä v dôkaze lemy 2.4 udávajúcej nevyhnutné podmienky pre existenciu riešenia. Kým táto lema je v článku [2] dokázaná cez kvadratické formy pomocou Henslovej lemy vyslovenej v sekcii 1.3, my ju budeme dokazovať v ideálovej triednej grupe kvadratického rozšírenia $\mathbb{Q}[\sqrt{-D}]$. Podobne sme prepracovali aj lemu 2.5 a vetu 2.8.

Lemu 2.3 sme spracovali pre rovnicu $|x^2 + Dy^2| = z^2$ podľa postupu v článku [2]. V leme 2.6 sme znenie aj dôkaz rozšírili o možnosť $D < 0$.

Keďže uvažujeme aj $D < 0$, tak v znení vety 2.8 sme museli použiť ε ako všeobecnú jednotku v rozšírení $\mathbb{Z}[\sqrt{-D}]$, kým v článku [2] používajú $\varepsilon = \pm 1$. Podľa toho sme aj prepracovali dôkaz.

V dôkazoch všetkých ostatných lem a viet nespomenutých v predošlých odsekoch v dôkazoch postupujeme podľa dôkazov v článku [2] a upravujeme alebo rozširujeme ich aj pre možnosť $D < 0$ pomocou rovnice (1).

V sekcii 2.4 uvádzame základné príklady ideálových triednych grup a porovnávame ich štruktúry pre číselné telesá $K_1 = \mathbb{Q}[\sqrt{d}]$ a $K_2 = \mathbb{Q}[\sqrt{-d}]$, kde $d \in \mathbb{N}$.

1. Algebraická teória čísel

1.1 Základné algebraické definície

V tejto podkapitole vyslovíme základné algebraické definície a tvrdenia zo skrípt Davida Stanovského k predmetu Algebra [3] a zo skrípt Vítězslava Kalu k predmetu Teória čísel [1] a k predmetu Úvod do komutatívnej algebry [4].

Definícia 1.1. Buď $R \leq S$ telesá a $a_1, a_2, \ldots, a_n \in S$, potom $R(a_1, a_2, \ldots, a_n)$ najmenšie podteleso S obsahujúce R aj prvky $a_1, a_2, \ldots, a_n$ nazývame *telesovým rozšírením R o prvky $a_1, a_2, \ldots, a_n$*. Teleso K je *číselným telesom*, ak je to rozšírenie $\mathbb{Q}$ konečného stupňa. Okruh všetkých prvkov telesa K celistvých nad $\mathbb{Z}$ značíme $\mathcal{O}_K$.

Veta 1.2. [4, Veta 4.3] *Ak $K = \mathbb{Q}\left(\sqrt{N}\right)$, tak*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{N}] & \text{ak } N \equiv 2,3 \text{ (mod 4)}, \\ \mathbb{Z}[\frac{1+\sqrt{N}}{2}] & \text{ak } N \equiv 1 \text{ (mod 4)}. \end{cases}$$

Definícia 1.3. Buď $K = \mathbb{Q}[\sqrt{-D}]$, kde $D \neq 0,1$. *Normu prvku* definujeme ako zobrazenie

$$N : K \longrightarrow \mathbb{Q}$$

také, že pre $\alpha = a + b\sqrt{D}$ platí:

$$N(\alpha) = \alpha\alpha' = a^2 - b^2 D,$$

kde $\alpha' = a - b\sqrt{D}$.

V tejto práci budeme pracovať v kvadratickom rozšírení $K = \mathbb{Q}[\sqrt{-D}]$, kde $D \in \mathbb{Z}$ je bezštvorcové.

Definícia 1.4. Buď p prvočíslo a $a \in \mathbb{Z}$. Potom a je *kvadratický zbytok modulo p*, ak existuje b také, že $b^2 \equiv a \pmod{p}$. Inak je to *kvadratický nezbytok*. Definujeme *Legenderov symbol*:

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{ak } p \nmid a \text{ a } a \text{ je kvadratický zbytok mod } p; \\ -1 & \text{ak } p \nmid a \text{ a } a \text{ nie je kvadratický zbytok mod } p; \\ 0 & \text{ak } p \mid a. \end{cases}$$

Tvrdenie 1.5. [1, Dôsledok 4.2] *Pre Legenderov symbol platí vlastnosť $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, kde a,b $\in \mathbb{Z}$ a p prvočíslo.*

Definícia 1.6. Nech $m \in \mathbb{N}$ také, že $m \neq d^2$ pre každé $d \in \mathbb{N}$, potom definujeme *Pellovu rovnicu* ako $x^2 - my^2 = 1$. Povieme, že dvojica (a,b) je riešením Pellovej rovnice pre nejaké $m \in \mathbb{N}$, ak $a^2 - mb^2 = 1$.

Pre ľubovoľné $m \in \mathbb{N}$ požadovaného tvaru existuje triviálne riešenie $(\pm 1,0)$. Existencia netriviálneho riešenia plynie z následujúcej vety, ktorá je dokázaná ako tvrdenia 2.1 v [1].

Veta 1.7. *Nech $m \in \mathbb{N}$ také, že $m \neq d^2$ pre každé $d \in \mathbb{N}$, potom má Pellova rovnica $x^2 - my^2 = 1$ netriviálne riešenie v $\mathbb{Z}$.*

Nasledujúca veta nám dáva tvar riešení Pellovej rovnice. Jej dôkaz nájdeme v [1] vo vete 2.3.

Veta 1.8. *Nech $m \in \mathbb{N}$ také, že $m \neq d^2$ pre každé $d \in \mathbb{N}$. Potom existuje riešenie (a_0,b_0) také, že*

$$\left\{(a,b) \ : \ a + b\sqrt{m} = \pm(a_0 + b_0\sqrt{m})^n; n \in \mathbb{Z}\right\}$$

sú práve všetky riešenia.

Podrobnejšie je popísaný spôsob riešenia Pellovej rovnice v druhej kapitole skript [1].

Definícia 1.9. Nech A je abelovská grupa a $(A_i \mid i \in I)$ systém podgrup A taký, že každý prvok $a \in A$ je možné zapísať práve jedným spôsobom ako súčet $a = \sum_{i \in F} a_i$, kde F je konečná podmnožina I a $a_i \in A_i$ pre každé $i \in F$. Potom povieme, že A je *vnútorným direktným súčtom grup $(A_i \mid i \in I)$*, značíme

$$A = \coprod_{i \in I} A_i.$$

Abelovská grupa F sa nazýva *voľná*, ak je vnútorným súčtom nekonečných cyklických grup.

1.2 Základné vlastnosti okruhu celistvých prvkov

V tejto sekcii zhrnieme tvrdenia a definície o číselnom telese a okruhu celistvých prvkov zo skript Siu Hang Mana [5], kapitola 7, a základné definície z algebraickej teórie čísel zo skript [4], kapitola 4.

Lema 1.10. [4, Tvrdenie 4.8] *Nech $I = (\alpha_1, \ldots, \alpha_n)$ a $J = (\beta_1, \ldots, \beta_l)$ sú ideály v $\mathcal{O}_K$, potom*

1. *$I + J = (\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_l)$,*
2. *$I \cdot J = (\alpha_1\beta_1, \ldots, \alpha_j\beta_j, \ldots, \alpha_n\beta_l)$,*
3. *$I \subset J$ práve vtedy, keď každé α_i je $\mathcal{O}_K$-lineárnou kombináciou β_j,*

Definícia 1.11. Nech I, J sú ideály v $\mathcal{O}_K$. Povieme, že I *delí* J, značíme $I \mid J$, ak existuje ideál H v $\mathcal{O}_K$ taký, že $J = I \cdot H$.

Pozorovanie 1.12. *Pre α, $\beta \in \mathcal{O}_K$ platí, že $\alpha \mid \beta$ práve vtedy, keď $(\alpha) \mid (\beta)$.*

Lema 1.13. [4, Tvrdenie 4.9] *Nech $\alpha \in \mathcal{O}_K$ a $I = (\beta_1,\beta_2,\ldots,\beta_n)$ pre nejaké $n \in \mathbb{N}$. Potom nasledujúce tvrdenia sú ekvivalentné:*

1. *$(\alpha) \mid I$,*
2. *$\alpha \mid \beta_j$ pre všetky $j \in \{1,2,\ldots,n\}$,*

3. $I \subset (\alpha)$.

Veta 1.14. [4, Veta 4.10] *Buď K číselné teleso a I,J nenulové ideály v $\mathcal{O}_K$. Potom $I \mid J$ práve vtedy, keď $J \subset I$.*

Tvrdenie 1.15. [4, Tvrdenie 4.13] *Buď K číselné teleso a I,J, H ideály v $\mathcal{O}_K$ také, že $H \neq 0$ a $HI = HJ$. Potom $I = J$.*

Dôsledok. *Buď K číselné teleso, P prvoideál v $\mathcal{O}_K$ a I,J ideály v $\mathcal{O}_K$. Ak $P \mid IJ$, tak $P \mid I$ alebo $P \mid J$.*

Tvrdenie 1.16. [4, Tvrdenie 4.16] *Buď K číselné teleso P prvoideál v $\mathcal{O}_K$. Potom nasledujúce tvrdenia sú ekvivalentné:*

1. *P je nenulový prvoideál,*
2. *P je maximálny ideál,*
3. *P je vlastný ideál a ak $P = IJ$ pre nejaké ideály I,J v $\mathcal{O}_K$, tak $I = \mathcal{O}_K$ alebo $I = \mathcal{O}_K$.*

Veta 1.17. [4, Veta 4.17] *Nech $K = \mathbb{Q}[\sqrt{D}]$ pre $D \neq 0{,}1$ bezštvorcové. Každý nenulový ideál I v $\mathcal{O}_K$ môžeme rozložiť na súčin prvoideálov*

$$I = P_1^{k_1} P_2^{k_2} \dots P_r^{k_r},$$

kde k_1,k_2,…,$k_r \in \mathbb{N}$ a $P_1^{k_1}$,$P_2^{k_2}$,…,$P_r^{k_r}$ sú po dvoch rôzne prvoideály v $\mathcal{O}_K$. Tento rozklad je jednoznačný až na poradie.

Definícia 1.18. *Lomeným ideálom číselného telesa K* rozumieme $\mathcal{O}_K$-modul tvaru γa, kde $\gamma \in K$ a a je ideál v $\mathcal{O}_K$. Množinu všetkých vlastných lomených ideálov v $\mathcal{O}_K$ budeme značiť I_K. *Hlavným lomeným ideálom* je každý lomený ideál, ktorý je generovaný jedným prvkom. Množinu všetkých hlavných lomených ideálov v $\mathcal{O}_K$ budeme značiť P_K. Definujeme *ideálovú triednu grupu* ako faktorgrupu $Cl_K := I_K / P_K$.

Definícia 1.19. Nech K je číselné teleso, $\mathcal{O}_K$ jeho okruh celistvých prvkov a α_1,α_2,…,α_n $\mathbb{Z}$-báza $\mathcal{O}_K$. *Diskriminant číselného telesa K* definujeme ako

$$\Delta K := det\left(\sigma_i(\alpha_j)_{i,j=1}^n\right)^2,$$

kde $\sigma_i : K \hookrightarrow \mathbb{C}$ je vnorenie K do $\mathbb{C}$.

Poznámka. *Ak $K = \mathbb{Q}\left(\sqrt{N}\right)$, tak*

$$\Delta K = \begin{cases} 4N & ak\ N \equiv 2{,}3\ (mod\ 4), \\ N & ak\ N \equiv 1\ (mod\ 4). \end{cases}$$

Definícia 1.20. Nech L je konečné rozšírenie číselného telesa, $\mathfrak{p}$ prvoideál v $\mathcal{O}_K$ a $\mathfrak{q}$ ideál v $\mathcal{O}_L$. Povieme, že $\mathfrak{q}$ *leží nad* $\mathfrak{p}$, ak $\mathfrak{q} \cap \mathcal{O}_K = \mathfrak{p}$, značíme $\mathfrak{q} \mid \mathfrak{p}$.

Definícia 1.21. Majme $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1} \mathfrak{q}_2^{e_2} \dots \mathfrak{q}_g^{e_g}$ faktorizáciu ideálu $\mathfrak{p}\mathcal{O}_L$ v $\mathcal{O}_L$. Index e_i nazývame *index vetvenia* $\mathfrak{p}$ *v* $\mathfrak{q}_i$ pre všetky $1 \leq i \leq g$. Faktorokruh $\mathcal{O}_L/\mathfrak{q}_i$ je rozšírenie telesa $\mathcal{O}_K/\mathfrak{p}$, ktorého stupeň nazývame *stupeň inercie* $\mathfrak{p}$ *v* $\mathfrak{q}_i$ a značíme $f_i = f_{\mathfrak{q}_i|\mathfrak{p}}$.

Definícia 1.22. Nech $\mathfrak{p}$ je prvoideál v $\mathcal{O}_K$ a máme rozklad $\mathfrak{p}\mathcal{O}_L = \mathfrak{q}_1^{e_1}\mathfrak{q}_2^{e_2}\dots\mathfrak{q}_g^{e_g}$ v $\mathcal{O}_L$, kde L je konečné rozšírenie číselného telesa K. Potom povieme, že $\mathfrak{p}$ sa *vetví v* L, ak aspoň pre jedno $1 \leq i \leq g$ platí $e_i > 1$. Povieme, že $\mathfrak{p}$ je *nerozvetvené v* L, tak pre všetky $1 \leq i \leq g$ platí $e_i = 1$. Povieme, že sa *štiepi úplne*, ak pre všetky $1 \leq i \leq g$ platí $e_i = f_i = 1$. Povieme, že $\mathfrak{p}$ je *inertný v* L, ak $e_i = 1$ a $f_i = [L : K]$, teda $\mathfrak{p}\mathcal{O}_L$ je prvoideál v L.

Lema 1.23. [5, Tvrdenie 7.23] *Nech K je kvadratické teleso s diskriminantom D a $p \in \mathbb{Z}$ je prvočíslo, potom platí:*

- *ak $\left(\frac{D}{p}\right) = 0$, potom $p\mathcal{O}_K = \mathfrak{p}^2$, teda p sa vetví v K,*
- *ak $\left(\frac{D}{p}\right) = 1$, potom $p\mathcal{O}_K = \mathfrak{p}\mathfrak{p}'$, kde $\mathfrak{p} \neq \mathfrak{p}'$, teda p sa štiepi v K,*
- *ak $\left(\frac{D}{p}\right) = -1$, potom $p\mathcal{O}_K$ je prvoideál v $\mathcal{O}_K$, teda p je inertný v K.*

Vlastnosti z následujúcej lemy nájdeme dokázané v kapitole 4.3 a kapitole 4.6 v [1].

Lema 1.24. *Nech $\mathcal{O}_K$ je okruh všetkých prvkov kvadratického telesa K celistvých nad $\mathbb{Z}$. Potom platí:*

1. *$N(\alpha\mathcal{O}_K) = N(\alpha)$ pre $\alpha \in \mathcal{O}_K$, $\alpha \neq 0$.*
2. *$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b})$ pre všetky vlastné ideály v $\mathcal{O}_K$.*
3. *$\mathfrak{a}\overline{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}_K$ pre vlastný ideál $\mathfrak{a}$ v $\mathcal{O}_K$.*

1.3 Vzťah kvadratických foriem a ideálov

Na rovnicu $x^2 + Dy^2 = z^2$ môžeme nazerať ako na kvadratickú formu s diskriminantom $-4D$ reprezentujúcu číslo z^2. Tento pohľad využívajú aj autori článku [2]. Preto si v tejto sekcii uvedieme vzťah medzi triednou grupou týchto kvadratických foriem a ideálovou triednou grupou, ktorý je dokázaný v tvrdení 7.46 v skriptách k predmetu Kvadratické formy a triedne telesá od autora Siu Hang Mana [5].

Uvedieme si aj základné definície z oblasti kvadratických foriem, ktoré budeme potrebovať na vyslovenie tohto vzťahu.

Definícia 1.25. *Kvadratická forma Q hodnosti $n \in \mathbb{N}$* je polynóm stupňa 2 s n premennými

$$Q(x_1, \dots, x_n) = \sum_{n=1}^{\infty} a_{ij}x_ix_j,$$

pre $a_{ij} \in R$, pre R komutatívne teleso.

Definícia 1.26. Pre kvadratickú formu Q definujeme *maticu kvadratickej formy* ako

$$M(Q) = \begin{pmatrix} a_{11} & \frac{a_{12}}{2} & \cdots & \frac{a_{1n}}{2} \\ \frac{a_{21}}{2} & a_{22} & \cdots & \frac{a_{2n}}{2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{a_{1n}}{2} & \frac{a_{2n}}{2} & \cdots & a_{nn} \end{pmatrix} = \left(\frac{1}{2}\frac{\partial^2}{\partial x_i \partial x_j}Q(x_1, \dots, x_n)\right)_{i,j=1}^{n}.$$

Definícia 1.27. *Determinant kvadratickej formy* Q je $det(Q) := det(M(Q))$. *Diskriminant kvadratickej formy* Q je $D = -4det(Q)$.

Definícia 1.28. Dve kvadratické formy Q_1,Q_2 sú *ekvivalentné*, ak $Q_1(x,y) = Q_2(px + qy, rx + sy)$ a zároveň $ps - qr = 1$ pre p,q,r,$s \in \mathbb{Z}$.

Poznámka. *Pri ekvivalencii kvadratických foriem by mohlo nastať, že* $ps - qr = -1$. *Tento prípad v našej práci nebudeme uvažovať.*

Definícia 1.29. Kvadratická forma Q nad $\mathbb{Z}$ *reprezentuje* m, ak existujú x,$y \in \mathbb{Z}$ také, že $Q(x,y) = m$ a $\mathrm{NSD}(x,y) = 1$.

Poznámka. *V prípade reprezentácie čísla* m *kvadratickou formou* Q *by mohlo nastať, že NSD*$(x,y) \neq 1$. *Tento prípad nebudeme v našej práci uvažovať.*

Definícia 1.30. Nech Q je kvadratická forma nad $\mathbb{R}$, povieme, že Q je *pozitívne definitná*, ak pre každý nenulový prvok (x,y) platí $Q(x,y) > 0$.

Definícia 1.31. Nech $f(x,y) = ax^2 + bxy + cy^2$ a $g(x,y) = a'x^2 + b'xy + c'y^2$ sú primitívne pozitívne definitné kvadratické formy s diskriminantom $D < 0$ splňujúce $\mathrm{NSD}(a,a',\frac{b+b'}{2}) = 1$. Potom *Dirichletovým skladaním* f *a* g nazveme kvadratickú formu

$$F(x,y) = aa'x^2 + Bxy + \tfrac{B^2-D}{4aa'}y^2,$$

kde $B \pmod{2aa'}$ je jednoznačné a spĺňa

$$B \equiv b \pmod{2a},\ B \equiv b' \pmod{2a'},\ B^2 \equiv D \pmod{4aa'}.$$

Následujúca lema dokázaná v leme 3.2 v [6] dokazuje, že Dirichletovo skládanie je dobre definované.

Lema 1.32. *Nech* $f(x,y) = ax^2+bxy+cy^2$ *a* $g(x,y) = a'x^2+b'xy+c'y^2$ *sú formy s diskriminantom* $D < 0$ *splňujúce NSD*$(a,a',\frac{b+b'}{2}) = 1$. *Potom existuje práve jedno* $B \pmod{2aa'}$ *také, že*

$$B \equiv b \pmod{2a},\ B \equiv b' \pmod{2a'},\ B^2 \equiv D \pmod{4aa'}.$$

Veta 1.33. *Nech* K *je komplexné kvadratické číselné teleso s diskriminantom* $D < 0$ *a* $f(x,y) = ax^2 + bxy + cy^2$ *je primitívna, pozitívne definitná kvadratická forma s diskriminantom* D. *Zobrazenie*

$$\Phi\colon f(x,y) \longmapsto [a, \tfrac{-b+\sqrt{D}}{2}]$$

je izomorfizmus medzi triedovou grupou kvadratických foriem $C(D)$ *a ideálovou triednou grupou* Cl_K, *kde* $\mathbb{Z}$*-modul generovaný a a* $\frac{-b+\sqrt{D}}{2}$, *značíme* $[a, \frac{-b+\sqrt{D}}{2}]$, *je vlastný ideál v* $\mathcal{O}_K$.

Poznámka. *Vďaka tomuto vzťahu máme, že násobenie ideálov v* $\mathcal{O}_K$ *pre číselné teleso* K *zodpovedá operácii Dirichletovho skládania v triednej grupe kvadratických foriem* $C(D)$

Lema 1.34 (Henslova lema)**.** *Nech* $f(x)$ *je polynom s celočíselnými koeficientami,* k *kladné celé číslo a* r *celé číslo také, že* $f(r) \equiv 0 \pmod{p^k}$. *Majme* $m \leq k$ *kladné celé číslo, potom ak* $f'(r) \neq 0 \pmod{p}$, *tak existuje celé číslo* s *také, že* $f(s) \equiv 0 \pmod{p^{k+m}}$ *a* $s \equiv r \pmod{p^k}$.

1.4 Rády

Ak by sme v našej práci uvažovali aj D, ktoré nie ej bezštvorcové, tak by sme museli pracovať v ideáloch v ráde $\mathcal{O}$ číselného telesa K. V tejto kapitole si uvedieme základné definície a pravidlá s prácou v takejto štruktúre.

Definícia 1.35. *Rád* $\mathcal{O}$ v kvadratickom telese K je podmnožina $\mathcal{O} \subset K$ taká, že

- $\mathcal{O}$ je podokruh K obsahujúci jednotku;
- $\mathcal{O}$ je konečne generovaný $\mathbb{Z}$-modul;
- $\mathcal{O}$ obsahuje $\mathbb{Q}$-bázu K.

Poznámka. *Podľa poznámky za definíciu číselného telesa platí, že* $\mathcal{O}_K$ *je vždy rádom. Prvý a druhý bod definície rádu implikujú, že pre každý rád* $\mathcal{O}$ *telesa* K *platí, že* $\mathcal{O} \subset \mathcal{O}_K$*. Z toho dostávame, že* $\mathcal{O}_K$ *je maximálny rád telesa* K*.*

Definícia 1.36. Nech K je číselné teleso a $\mathcal{O}$ rád v ňom. *Ideálovú triednu grupu rádu* $\mathcal{O}$ ako faktorgrupu $C(\mathcal{O}) := I(\mathcal{O})/P(\mathcal{O})$.

Podľa článku [7] dostávame vlastnosti ideálov v rádoch $\mathcal{O}$ v číselnom telese K.

Definícia 1.37. Lomený $\mathcal{O}$-ideál $\mathfrak{a}$ je *invertibilný*, ak existuje lomený $\mathcal{O}$-ideál $\mathfrak{b}$ taký, že $\mathfrak{ab} = \mathcal{O}$.

Definícia 1.38. Buď K číselné teleso a $\mathcal{O}$ jeho rád. *Sprievodcu rádu* $\mathcal{O}$ definujeme ako

$$\mathfrak{c} = \mathfrak{c}_{\mathcal{O}} = \{x \in K \ : \ x\mathcal{O}_K \subset \mathcal{O}\}\,.$$

Poznámka. *Z toho, že* $1 \in \mathcal{O}_K$ *dostávame, že* $\mathfrak{c}$ *je podmnožina rádu* $\mathcal{O}$*, takže*

$$\mathfrak{c} = \{x \in \mathcal{O}_K \ : \ x\mathcal{O}_K \subset \mathcal{O}\} = \{x \in \mathcal{O} \ : \ x\mathcal{O}_K \subset \mathcal{O}\}\,.$$

Z posledného vyjadrenia dostávame, že $\mathfrak{c}$ *je anhilátor faktorgrupy* $\mathcal{O}_K/\mathcal{O}$ *ako* $\mathcal{O}$*-modulu, značíme* $\mathfrak{c} = Ann_{\mathcal{O}}(\mathcal{O}_K/\mathcal{O})$*.*

Veta 1.39. *Buď* K *číselné teleso a* $\mathcal{O}$ *jeho rád nesúdelný so sprievodcom je súčinom invertibilných prvoideálov. Navyše, každý ideál nesúdelný so sprievodcom je invertibilný.*

Z knihy [6] dostávame vzťahy medzi ideálmi v rádoch $\mathcal{O}$ číselného telesa K a kvadratickými formami.

Veta 1.40. *Nech* K *je komplexné kvadratické číselné teleso,* $\mathcal{O}$ *rád s diskriminantom* D*. Zobrazenie posielajúce primitívnu pozitívne definitnú kvadratickú formu* $f(x,y) = ax^2 + bxy + cy^2$ *s diskriminantom* D *na ideál* $[a, \frac{-b+\sqrt{D}}{2}]$ *je izomorfizmom medzi triednou grupou kvadratických foriem* $C(D)$ *a ideálovou triednou grupou* $C(\mathcal{O})$*.*

Veta 1.41. *Majme* $\mathcal{O}$ *rád s diskriminantom* D *v kvadratickom telese* K *a primitívnu pozitívne definitnú kvadratickú formu* $f(x,y) = ax^2 + bxy + cy^2$ *s diskriminantom* D*. Kladné celé číslo* m *je reprezentované kvadratickou formou* $f(x,y)$ *práve vtedy, keď* m *je norma* $N(\mathfrak{a})$ *nejakého ideálu* $\mathfrak{a}$ *v zodpovedajúcej ideálovej triede v* $C(\mathcal{O})$*.*

2. Štruktúra riešenia diofantickej rovnice

V tejto kapitole sa budeme zaoberať explicitným dokazovaním lem a tvrdení, ktoré nám pomôžu dokázať vetu, ktorá popisuje štukrúru a počet riešení rovnice $|x^2 + Dy^2| = z^2$, kde $D \equiv 2{,}3 \pmod 4$ a D je bezštvorcové.

V tomto prípade bude pre okruh celistvých prvkov nad $\mathbb{Z}$ podľa vety 1.2 platiť $\mathcal{O}_K = \mathbb{Z}[\sqrt{-D}]$ a môžeme využiť všetky vyššie uvedené tvrdenia.

2.1 Existencia riešenia

Táto sekcia bude venovaná dokazovaniu podmienky pre existenciu riešenia a základným definíciam, ktoré na to budeme potrebovať.

Definícia 2.1. Riešenie (a,b,c) pre $a,b,c \in \mathbb{Z}$ rovnice $|x^2 + Dy^2| = z^2$ sa nazýva *normalizované*, ak $\mathrm{NSD}(a,b,c) = 1$.

Definícia 2.2. Pre $D \in \mathbb{Z}$ definujeme množinu

$$G_D(\mathbb{Q}) := \left\{a + b\sqrt{-D} \in \mathbb{Q}[\sqrt{-D}] : |a^2 + Db^2| = 1\right\}.$$

Lema 2.3. *Majme $D \in \mathbb{Z}$ také, že $-D \equiv 2{,}3 \pmod 4$. Ak (a,b,c) je normalizované riešenie rovnice $|x^2 + Dy^2| = z^2$, tak c musí byť nepárne celé číslo.*

Dôkaz. Z predpokladu máme $|a^2 + Db^2| = c^2$. Ak by $2 \mid c$, tak $4 \mid c^2$, čo implikuje $4 \mid |a^2 + Db^2|$. Modulo 4 je kvadratickým zbytkom len 0 a 1, takže môžu nastať štyri možnosti.

Ak by $b^2 \equiv a^2 \equiv 0 \pmod 4$, tak $4 \mid a^2, b^2$ a $2 \mid a,b,c$, čo je spor s predpokladom nesúdelnosti.

Možnosť $b^2 \equiv 1 \pmod 4$ a $a^2 \equiv 0 \pmod 4$, by dala, že $4 \mid |D|$, čo je spor s podmienkou $-D \equiv 2{,}3 \pmod 4$.

Ak by $b^2 \equiv 0 \pmod 4$ a $a^2 \equiv 1 \pmod 4$, tak dostávame $|a^2 + Db^2| = 1 \pmod 4$, čo je spor s predpokladom $4 \mid |a^2 + Db^2|$.

Z možnosti $b^2 \equiv a^2 \equiv 1 \pmod 4$ dostávame $|a^2 + Db^2| = |D + 1| \pmod 4$. Keďže máme predpoklad $-D \equiv 2{,}3 \pmod 4$, tak dostávame $|a^2 + Db^2| = 2{,}3 \pmod 4$, čo je spor s predpokladom $4 \mid |a^2 + Db^2|$.

Rozborom možností sme dostali, že $2 \nmid c$, takže c musí byť nepárne prirodzené číslo. □

Vďaka predošlej leme môžeme v prvočíselnom rozklade c uvažovať len nepárne prvočísla. V následujúcej leme dokážeme nutnú podmienku pre existenciu riešenia rovnice $|x^2 + Dy^2| = z^2$.

Lema 2.4. *Buď $-D \equiv 2{,}3 \pmod 4$ a $K = \mathbb{Q}[\sqrt{-D}]$. Predpokladajme, že $Cl_K \cong (\mathbb{Z}_2)^n$ pre nejaké $n \geq 0$. Nech $p_1^{n_1}, \ldots, p_k^{n_k}$ sú nepárne prvočísla a $c = p_1^{n_1} \ldots p_k^{n_k}$ pre $n_1, \ldots, n_k \in \mathbb{N}_0$. Potom existuje normalizované riešenie (a,b,c) pre $|x^2 + Dy^2| = z^2$ práve vtedy, keď $(\frac{-D}{p_i}) = 1$ pre každé $1 \leq i \leq k$.*

Dôkaz. „$\Longrightarrow$“ Nech c je tvaru ako v znení lemy a existuje normalizované riešenie (a,b,c) rovnice $|x^2+Dy^2| = z^2$. Potom trojica (a,b,c) spĺňa rovnosť $|a^2+Db^2| = c^2$. Ak si obe strany vyjadríme modulo p_i pre ľubovoľné fixné $1 \leq i \leq k$, dostávame

$$|a^2 + Db^2| \equiv 0 \pmod{p_i}.$$

Keďže je to kongruentné nule, tak vďaka vlastnostiam kongruencie môžeme uvažovať rovnosť $a^2 + Db^2 \equiv 0 \pmod{p_i}$ a dostávame:

$$a^2 \equiv -Db^2 \pmod{p_i}$$

Ak by p_i delilo b, tak by muselo deliť aj a a zo znenia vieme, že p_i delí c. Z toho by sme dostali NSD$(a,b,c) \neq 1$, čo je spor s predpokladom nesúdelnosti, takže p_i nemôže deliť b. Preto platí $-D \equiv (\frac{a}{b})^2 \pmod{p_i}$ a $-D$ je kvadratický zbytok modulo p_i. Z definície Legenderovho symbolu dostávame $\left(\frac{-D}{p_i}\right) = 1$.

„$\Longleftarrow$“ Pre dôkaz opačnej implikácie najprv dokážeme tvrdenie pre $c = p$ je nepárne prvočíslo také, že $\left(\frac{-D}{p}\right) = 1$.

Z lemy 1.23 a poznámky za definíciu diskriminantu číselného telesa dostávame, že (p), ideál generovaný prvkom p, sa v $\mathcal{O}_K$ štiepi a platí $(p) = \mathcal{P}\overline{\mathcal{P}}$, pre nejaké prvoideály $\mathcal{P}$ a $\overline{\mathcal{P}}$ také, že $\mathcal{P} \neq \overline{\mathcal{P}}$.

Z vlastnosti ideálov dostávame

$$(p^2) = \mathcal{P}^2\overline{\mathcal{P}}^2 = (\alpha\overline{\alpha}) = (N(\alpha)).$$

pre $\alpha = a + b\sqrt{-D}$. Druhá rovnosť plynie z toho, že $Cl_K \cong (\mathbb{Z}_2)^n$ pre nejaké $n \geq 0$, takže $\mathcal{P}^2$ a $\overline{\mathcal{P}}^2$ sú hlavné ideály. Z definície platí, že ak $\mathcal{P}^2$ je generovaný α, tak $\overline{\mathcal{P}}^2$ je generovaný $\overline{\alpha}$.

Z tejto rovnosti plynie, že $p^2 = \varepsilon(a^2+Db^2)$, kde ε je jednotka v $\mathcal{O}_K^*$, a zároveň $\varepsilon = \frac{p^2}{a^2+Db^2}$, čo implikuje, že $\varepsilon \in \mathbb{Q}$.

Všetky jednotky v $\mathcal{O}_K^*$ tvaru $a + b\sqrt{-D}$ dostneme riešením Pellovej rovnice $a^2+Db^2 = 1$. Jediné jednotky ležiace v $\mathbb{Q}$ dostaneme z triviálneho riešenia. Takže $\varepsilon = \pm 1$ a $p^2 = |a^2 + Db^2|$ je hľadané riešenie.

V druhom kroku dôkazu to dokážeme pre všeobecné c. Nech c má tvar ako v znení lemy, potom z jednoznačného rozkladu na prvoideály v $\mathcal{O}_K$ a vlastnosti ideálov platí rovnosť

$$(c^2) = (p_1^{2n_1}p_2^{2n_2}\dots p_k^{2n_k}) = (p_1)^{2n_1}(p_2)^{2n_2}\dots(p_k)^{2n_k} = \mathcal{P}_1^{2n_1}\overline{\mathcal{P}_1}^{2n_1}\dots\mathcal{P}_k^{2n_k}\overline{\mathcal{P}_k}^{2n_k},$$

kde druhá rovnosť plynie z vlastnosti ideálov a tretia z vlastnosti dokázanej vyššie pre $c = p$.

Z vlastnosti $Cl_K \cong (\mathbb{Z}_2)^n$ pre nejaké $n > 0$ platí $\mathcal{P}_i^2 = (\alpha_i)$ pre každé $0 \leq i \leq k$ pre nejaké $\alpha_i \in \mathbb{Z}[\sqrt{-D}]$, takže analogicky s príkladom pre $c = p$ dostávame

$$\mathcal{P}_1^{2n_1}\overline{\mathcal{P}_1}^{2n_1}\dots\mathcal{P}_k^{2n_k}\overline{\mathcal{P}_k}^{2n_k} = (\alpha_1^{n_1}\overline{\alpha_1}^{n_1}\dots\alpha_k^{n_k}\overline{\alpha_k}^{n_k})$$

Definujme $\gamma := \alpha_1^{n_1}\dots\alpha_k^{n_k}$. Potom z komutativity platí

$$(\alpha_1^{n_1}\overline{\alpha_1}^{n_1}\dots\alpha_k^{n_k}\overline{\alpha_k}^{n_k}) = (N(\gamma))$$

Z rovnosti $(c^2) = (p_1^{2n_1}p_2^{2n_2}\dots p_k^{2n_k}) = (N(\gamma))$ a vlastnosti dokázanej pre $c = p$ dostávame $\gamma = p_1^{2n_1}\dots p_k^{2n_k}$.

Nech p je prvočíslo také, že

$$p \mid \gamma \mid N(\gamma),$$

Rovnosť $\gamma = p_1^{2n_1} \dots p_k^{2n_k}$ implikuje, že p musí deliť niektoré z prvočísel p_i pre $1 \leq i \leq k$.

Nech bez straty na všeobecnosti platí, že $p \mid p_1$, potom dostávame vzťah

$$(p) = \mathcal{P}_1\overline{\mathcal{P}_1} \mid (\gamma) \mid \mathcal{P}_1^{2n_1}\overline{\mathcal{P}_1}^{2n_1} \dots \mathcal{P}_k^{2n_k}\overline{\mathcal{P}_k}^{2n_k}.$$

Tento vzťah implikuje

$$\overline{\mathcal{P}_1} \mid \mathcal{P}_1^{2n_1}\overline{\mathcal{P}_1}^{2n_1} \dots \mathcal{P}_k^{2n_k}\overline{\mathcal{P}_k}^{2n_k}$$

Keďže $\overline{\mathcal{P}_1}$ je prvoideál, dostávame, že $\overline{\mathcal{P}_1} \mid \mathcal{P}_i$ pre nejaký index i. Z tvrdenia 1.16 vyplýva, že prvoideály sú maximálne ideály, takže $\overline{\mathcal{P}_1} = \mathcal{P}_i$. Môžu nastať dve možnosti:

- ak $i = 1$, tak $\overline{\mathcal{P}_1} = \mathcal{P}_1$, to implikuje, že (p) sa vetví, čo je spor z predpokladom, že (p) sa štepí,
- ak $i \neq 1$, tak $p_1 = N(\overline{\mathcal{P}_1}) = N(\mathcal{P}_i) = p_i$, čo je spor z vlastnosťou, že $p_i \neq p_j$ pre každý index $i \neq j$.

Takže γ nie je delená žiadným prvočíslom a teda NSD(a,b) = 1 a zároveň $|a^2 + Db^2| = c$. To dokazuje, že za podmienky $(\frac{-D}{p_i}) = 1$ pre $1 \leq i \leq k$, kde $c = p_1^{n_1} \dots p_k^{n_k}$, existuje normalizované riešenie rovnice $|x^2 + Dy^2| = z^2$. □

2.2 Faktorizácia $G_D(\mathbb{Q})$

Táto sekcia bude zameraná na popis faktorizácie v $G_D(\mathbb{Q})$.

Lema 2.5. *Pre nepárne prvočíslo p také, že $\left(\frac{-D}{p}\right) = 1$, majme $x_0^2 + Dy_0^2 = p^{2\alpha}$ s vlastnosťou NSD(x_0,y_0) = 1. Predpokladajme, že $p^{2\alpha} \mid c^2 + Dd^2$ pre nejaké c,d, také, že NSD(c,d) = 1. Potom v $\mathbb{Z}[\sqrt{-D}]$ nastane práve jedna z nasledujúcich možností:*

$$x_0 + y_0\sqrt{-D} \mid c + d\sqrt{-D},$$

alebo

$$x_0 - y_0\sqrt{-D} \mid c + d\sqrt{-D}.$$

Dôkaz. Z vlastnosti normy platí $N(x_0 + y_0\sqrt{-D}) = x_0^2 + Dy_0^2 = p^{2\alpha}$ a zároveň $p^{2\alpha} \mid c^2 + Dd^2 = N(c + d\sqrt{-D})$. Z predpokladu vieme, že $\left(\frac{-D}{p}\right) = 1$, čo spolu s lemou 1.23 dáva štiepiteľnosť (p). Takže $(p^2) = \mathcal{P}^2\overline{\mathcal{P}}^2$ pre nejaké prvoideály $\mathcal{P} \neq \overline{\mathcal{P}}$.

Z vlastnosti ideálov dostávame $\mathcal{P}^{2\alpha}\overline{\mathcal{P}^{2\alpha}} \mid (c + d\sqrt{-D})(c - d\sqrt{-D})$.

Ak by aj $\mathcal{P}$ aj $\overline{\mathcal{P}}$ delilo niektorý z členov, bez ujmy na všeobecnosti predpokladajme $(c + d\sqrt{-D})$, tak by sme dostali

$$(p) = \mathcal{P}\overline{\mathcal{P}} \mid (c + d\sqrt{-D}),$$

takže $p \mid c$,d, čo je spor s podmienkou NSD(c,d) = 1.

V predchádzajúcom odstavci sme dokázali, že nemôže nastať, aby aj $\mathcal{P}$ aj $\overline{\mathcal{P}}$ delilo niektorý z členov. Bez ujmy na všeobecnosti predpokladajme, že

$$\mathcal{P}^{2\alpha} \mid (c + d\sqrt{-D}) \text{ a } \overline{\mathcal{P}}^{2\alpha} \mid (c - d\sqrt{-D}).$$

Zároveň platí $\mathcal{P}^{2\alpha}\overline{\mathcal{P}}^{2\alpha} \mid (x_0 + y_0\sqrt{-D})(x_0 - y_0\sqrt{-D})$. Analogicky so situáciou pre $(c+d\sqrt{-D})(c-d\sqrt{-D})$ platí, že $\mathcal{P}^{2\alpha}$ delí práve jeden z členov $(x_0+y_0\sqrt{-D})$ a $(x_0 - y_0\sqrt{-D})$, rovnako aj pre $\overline{\mathcal{P}}^{2\alpha}$.

Nech teda $\mathcal{P}^{2\alpha} \mid (x_0 \pm y_0\sqrt{-D})$. Z vlastnosti $(p^{2\alpha}) = \mathcal{P}^{2\alpha}\overline{\mathcal{P}}^{2\alpha} = (x_0 + y_0\sqrt{-D})(x_0 - y_0\sqrt{-D})$ dostávame $\mathcal{P}^{2\alpha} = (x_0 \pm y_0\sqrt{-D})$. Analogicky $\overline{\mathcal{P}^{2\alpha}} = (x_0 \mp y_0\sqrt{-D})$.

Všetky tieto vlastnosti dohromady implikujú, že práve jeden z $(x_0+y_0\sqrt{-D})$ a $(x_0 - y_0\sqrt{-D})$ delí $(c + d\sqrt{-D})$, čo dokazuje vlastnosť, že práve jedno z $x_0 + y_0\sqrt{-D}$ a $x_0 - y_0\sqrt{-D}$ delí $c + d\sqrt{-D}$. □

Lema 2.6. *Nech p je nepárne prvočíslo, potom platí*

1. *ak $D > 0$, tak $x^2 + Dy^2 = z^2$ má jednoznačné normalizované riešenie tvaru (a,b,p);*

2. *ak $D < 0$ a máme fixované riešenie (a_0,b_0,p), tak pre všetky normalizované riešenia tvaru (a,b,p) platí $a+b\sqrt{-D} = \varepsilon(a_0+b_0\sqrt{-D})$ pre nejakú jednotku $\varepsilon \in \mathbb{Z}[\sqrt{-D}]$.*

Dôkaz. Pre dôkaz prvého bodu najprv ukážeme, že ak $a + b\sqrt{-D} \mid c + d\sqrt{-D}$ a zároveň $c + d\sqrt{-D} \mid a + b\sqrt{-D}$, tak $a = \pm c$ a $b = \pm d$.

Ak $a+b\sqrt{-D} \mid c+d\sqrt{-D}$ a $c+d\sqrt{-D} \mid a+b\sqrt{-D}$ tak z vlastnosti deliteľnosti dostávame $a+b\sqrt{-D} = \varepsilon(c+d\sqrt{-D})$, kde ε je jednotka v kvadratickom rozšírení $\mathbb{Z}[\sqrt{-D}]$. Z riešenia Pellovej rovnice $a^2 + Db^2 = 1$ dostávame, že jediné jednotky v $\mathbb{Z}[\sqrt{-D}]$ pre $D > 0$ sú ± 1, čo implikuje rovnosti $a = \pm c$ a $b = \pm d$.

Pre dôkaz jednoznačnosti predpokladajme, že existujú dve riešenia

$$p^2 = x_1^2 + Dy_1^2 = x_2^2 + Dy_2^2$$

také, že $\mathrm{NSD}(x_1,y_1) = 1$ a $\mathrm{NSD}(x_2,y_2) = 1$.

Podľa lemy 2.4 dostávame $\left(\frac{-D}{p}\right) = 1$, takže sú splnené predpoklady lemy 2.5 a dostávame štyri možnosti:

1. ak $x_1+y_1\sqrt{-D} \mid x_2+y_2\sqrt{-D}$ a $x_2+y_2\sqrt{-D} \mid x_1+y_1\sqrt{-D}$, tak z vlastnosti dokázanej v prvej časti dôkazu dostávame, že $x_1 = \pm x_2$ a $y_1 \pm y_2$, takže $x_1^2 = x_2^2$ a $y_1^2 = y_2^2$a riešenia sú rovnaké;

2. ak $x_1+y_1\sqrt{-D} \mid x_2+y_2\sqrt{-D}$ a $x_2-y_2\sqrt{-D} \mid x_1+y_1\sqrt{-D}$, tak dostávame $x_1-y_1\sqrt{-D} \mid x_2-y_2\sqrt{-D} \mid x_1+y_1\sqrt{-D}$, čo dáva $x_1+y_1\sqrt{-D} \mid x_1-y_1\sqrt{-D}$ a $x_1 - y_1\sqrt{-D} \mid x_1 + y_1\sqrt{-D}$. Z vlastnosti dokázanej v prvej časti dôkazu máme $x_1 = -x_1$ alebo $y_1 = -y_1$. Keďže x_1 je nenulové, tak $x_1 = \pm p$ a $y_1 = 0$;

3. ak $x_1 - y_1\sqrt{-D} \mid x_2+y_2\sqrt{-D}$ a $x_2+y_2\sqrt{-D} \mid x_1+y_1\sqrt{-D}$, tak dostávame $x_1 - y_1\sqrt{-D} \mid x_2 - y_2\sqrt{-D} \mid x_1 + y_1\sqrt{-D}$ a analogicky s druhým bodom dostávame rovnosť riešení;

4. ak $x_1 - y_1\sqrt{-D} \mid x_2 + y_2\sqrt{-D}$ a $x_2 - y_2\sqrt{-D} \mid x_1 + y_1\sqrt{-D}$, tak máme $x_1 - y_1\sqrt{-D} \mid x_2 + y_2\sqrt{-D}$ a $x_2 + y_2\sqrt{-D} \mid x_1 - y_1\sqrt{-D}$ a analogicky s prvým bodom dostávame pomocou vlastnosti z prvej časti rovnosť riešení.

Takže ak by existovali dve normalizované riešenia tvaru (a,b,p), tak by sa museli rovnať.

V dôkaze druhého bodu budeme postupovať analogicky. Ak pre $D < 0$ platí že $a + b\sqrt{-D} \mid c + d\sqrt{-D}$ a $c + d\sqrt{-D} \mid a + b\sqrt{-D}$, tak z vlastností deliteľnosti dostávame $a + b\sqrt{-D} = \varepsilon(c + d\sqrt{-D})$, čo ukazuje druhý bod. □

Poznámka. *Predošlá lema nám dáva, že pre $D > 0$ existuje jednoznačné riešenie. Pre $D < 0$ existuje riešenie jednoznačné až na prenádsobenie jednotkou ε z $\mathbb{Z}[\sqrt{-D}]$.*

V následujúcej časti tejto sekcie popíšeme riešenia rovnice $|x^2 + Dy^2| = z^2$ z iného pohľadu.

Definícia 2.7. Pre každé prvočíslo q, pre ktoré platí $\left(\frac{-D}{q}\right) = 1$, definujeme *elementárne riešenie* ako

$$\zeta_q := \tfrac{x_0 + y_0\sqrt{-D}}{q},$$

kde $q^2 = |x_0^2 + Dy_0^2|$ a $x_0,y_0 > 0$.

Poznámka. *Existencia x_0,y_0 plynie z lemy 2.4 a predpokladu $Cl_K \cong (\mathbb{Z}_2)^n$ pre $n > 0$. Jednoznačnosť dostávame z lemy 2.6.*

Veta 2.8. *Nech $Cl_K \cong (\mathbb{Z}_2)^n$ pre $n > 0$ a $K = \mathbb{Q}[\sqrt{-D}]$, $\delta = \frac{a+b\sqrt{-D}}{c} \in G_D(\mathbb{Q})$, kde $NSD(a,b) = 1$ a $c = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, pre p_i nepárne prvočíslo a $\alpha_i \in \mathbb{N}_0$ pre každé $1 \le i \le k$, potom*

$$\delta = \varepsilon \cdot \zeta_{p_1}^{\pm\alpha_1} \dots \zeta_{p_k}^{\pm\alpha_k},$$

pre nejakú voľbu znamienok $\pm$ v exponentoch a ε jednotku v $\mathbb{Z}[\sqrt{-D}]$.

Dôkaz. Z definície elementárneho riešenia platí, že

$$|a^2 + Db^2| = c^2 = p_1^{2\alpha_1} p_2^{2\alpha_2} \dots p_k^{2\alpha_k}.$$

Podľa lemy 2.4 platí $\left(\frac{-D}{p_i}\right) = 1$ pre každé $1 \le i \le k$. Lema 1.23 implikuje, že (p_i) sa bude pre každé $1 \le i \le k$ v $\mathcal{O}_K$ štiepiť, takže dostávame

$$\mathcal{P}_i^{2\alpha_i} \overline{\mathcal{P}}_i^{2\alpha_i} \mid (a + b\sqrt{-D})(a - b\sqrt{-D}).$$

Analogicky s dôkazom lemy 2.5 dostávame, že každé z $\mathcal{P}_i^{2\alpha_i}$ a $\overline{\mathcal{P}}_i^{2\alpha_i}$ delí práve jedno z $(a + b\sqrt{-D})$ a $(a - b\sqrt{-D})$.

Pre každé $1 \le i \le k$ označme $\mathcal{P}_{i,+}^{2\alpha_i}$ ideál, ktorý delí $(a + b\sqrt{-D})$ a analogicky $\mathcal{P}_{i,-}^{2\alpha_i}$ ideál, ktorý delí $(a - b\sqrt{-D})$.

Z dokázaného plynie, že

$$\prod_{1 \le i \le k} \mathcal{P}_{i,+}^{2\alpha_i} = (a + b\sqrt{-D})$$

a zároveň

$$\prod_{1 \le i \le k} \mathcal{P}_{i,-}^{2\alpha_i} = (a - b\sqrt{-D}).$$

Pre každé $1 \le i \le k$ máme jednoznačné riešenie $p_i^2 = |x_i^2 + Dy^2|$, kde $x_i, y_i > 0$. Z toho dostávame

$$\mathcal{P}_{i,+}^{2\alpha_i} = \varepsilon_i(x_i + u_i y_i\sqrt{-D}) \text{ a } \mathcal{P}_{i,+}^{2\alpha_i} = \varepsilon_i^{-1}(x_i - u_i y_i\sqrt{-D})$$

pre $u_i = \pm 1$ a jednoznačnú jednotku ε_i.

Keďže $\mathcal{P}_{i,-}^2$ aj $\mathcal{P}_{i,+}^2$ sú hlavné ideály z vlastnosti $Cl_K \cong (\mathbb{Z}_2)^n$ pre nejaké $n \geq 0$, kde $K = \mathbb{Q}[\sqrt{-D}]$, tak dostávame

$$\prod_{1\leq i\leq k} \mathcal{P}_{i,-}^{\alpha_i} = \prod_{1\leq i\leq k} [\varepsilon_i(x_i - u_i y_i\sqrt{-D})]^{\alpha_i} = \left(\prod_{1\leq i\leq k} \varepsilon_i(x_i - u_i y_i\sqrt{-D})^{\alpha_i}\right),$$

rovnako

$$\prod_{1\leq i\leq k} \mathcal{P}_{i,+}^{\alpha_i} = \prod_{1\leq i\leq k} [(x_i + u_i y_i\sqrt{-D})]^{\alpha_i} = \left(\prod_{1\leq i\leq k} (x_i + u_i y_i\sqrt{-D})^{\alpha_i}\right),$$

kde NSD(γ_i,β_i) = 1 pre každé $1 \leq i \leq k$.

Spojením všetkých rovností a z vlastnosti ideálov dostávame

$$a + b\sqrt{-D} = \varepsilon \cdot \prod_{1\leq i\leq k} (x_i + u_i y_i\sqrt{-D})^{\alpha_i}$$

pre $\varepsilon = \varepsilon_1^{\alpha_1} \dots \varepsilon_k^{\alpha_k}$.

Dostávame

$$\frac{a + b\sqrt{-D}}{c} = \varepsilon \cdot \left(\frac{x_1 + u_1 y_1\sqrt{-D}}{p_1}\right)^{\alpha_1} \dots \left(\frac{x_k + u_k y_k\sqrt{-D}}{p_k}\right)^{\alpha_k} = \varepsilon \cdot \zeta_{p_1}^{u_1\alpha_1} \dots \zeta_{p_k}^{u_k\alpha_k},$$

kde ε je jednotka v $\mathbb{Z}[\sqrt{-D}]$. □

2.3 Popis riešenia pomocou faktorizácie

V tejto sekcii vyslovíme a dokážeme hlavnú vetu tejto práce, ktorá popisuje štruktúru riešení rovnice $|x^2 + Dy^2| = z^2$. Najprv ale potrebujeme dokázať ešte dve čiastkové vety a jednu pomocnú lemu.

Lema 2.9. *Nech* $\delta_1 = \frac{a_1 + b_1\sqrt{-D}}{c_1} \in G_D(\mathbb{Q})$ *a* $\delta_2 = \frac{a_2 + b_2\sqrt{-D}}{c_2} \in G_D(\mathbb{Q})$ *také, že* NSD(a_1,b_1) =NSD(a_2,b_2) =NSD(c_1,c_2) = 1. *Potom*

$$(a_1a_2 - Db_1b_2, a_1b_2 + a_2b_1, c_1c_2)$$

je normalizované riešenie rovnice $|x^2 + Dy^2| = z^2$ *a* NSD($a_1a_2 - Db_1b_2, a_1b_2 + a_2b_1$) = 1.

Dôkaz. Zo znenia vety vieme, že $|a_1^2 + Db_1^2| = c_1^2$ a zároveň $|a_2^2 + Db_2^2| = c_2^2$. Dosadením do rovnice $x = a_1a_2 - Db_1b_2$ a $y = a_1b_2 + a_2b_1$ dostávame

$$|(a_1a_2 - Db_1b_2)^2 + D(a_1b_2 + a_2b_1)^2| = |(a_1^2 + Db_1^2)(a_2^2 + Db_2^2)| = |c_1^2c_2^2| = c_1^2c_2^2.$$

Pre normalizovanosť riešenia stačí ukázať, že $a_1a_2 - Db_1b_2$ a $a_1b_2 + a_2b_1$ nemajú spoločného deliteľa.

Pre spor predpokladajme, že existuje také prvočíslo q, ktoré ich delí. Potom dostávame

$$q \mid (-b_2)(a_1a_2 - Db_1b_2) + (a_2)(a_1b_2 + a_2b_1),$$

takže platí $q \mid b_1(a_2^2 + Db_2^2)$.

Ak by $q \mid b_1$, tak potom $q \mid a_1a_2$ a $q \mid a_1b_2$. Zo znenia máme vlastnosť NSD(a_1,b_1) = 1, ktorá implikuje $q \nmid a_1$, takže musí platiť $q \mid a_2$ a $q \mid b_2$, čo je spor s predpokladom NSD(a_2,b_2) = 1, takže $q \mid a_2^2 + Db_2^2 = c_2$.

Z toho, že $q \mid a_1a_2 - Db_1b_2$ a zároveň $q \mid a_1b_2 + a_2b_1$ dostávame

$$q \mid (a_1)(a_1a_2 - Db_1b_2) + (Db_1)(a_1b_2 + a_2b_1) = a_2(a_1^2 + Db_1^2),$$

to implikuje, že $q \mid a_2$ alebo $q \mid (a_1^2 + Db_1^2)$.

Predpokladajme najprv, že $q \mid a_2$, potom $q \mid Db_1b_2$ a $q \mid a_1b_2$, čo implikuje $q \mid a_1$ a $q \nmid b_2$.

Pre spor predpokladajme $q \mid D$, potom $q \mid a_2^2 + Db_2^2 = c_2^2$. Z toho, že q je prvočíslo, dostávame $q^2 \mid c_2^2$, čo implikuje $q^2 \mid Db_2^2$. Keďže $q \nmid b_2$, tak $q^2 \mid D$ a dostávame spor s tým, že D je bezštvorcové.

Kombináciou vlastností $q \mid a_2$, $q \nmid D$ a NSD(a_2,b_2) = 1 dostávame $q \mid b_1$ a $q \mid a_1$, čo je spor s vlastnosťou NSD(a_1,b_1) = 1. Takže dostávame, že $q \nmid a_2$, preto $q \mid (a_1^2 + Db_1^2) = c_1$.

Z oboch dokázaných bodov dostávame, že $q \mid c_1$ a zároveň $q \mid c_2$, čo je spor s vlastnosťou NSD(c_1,c_2) = 1. Takže sme dokázali, že spoločný deliteľ q nemôže existovať. □

Definícia 2.10. Majme $K = \mathbb{Q}[\sqrt{-D}]$ pre $-D \equiv 2{,}3 \pmod 4$. Povieme, že $\delta \in G_D(\mathbb{Q})$ *zodpovedá* normalizovanému riešeniu (a,b,c) rovnice $|x^2 + Dy^2| = z^2$, ak $\delta = \frac{a+b\sqrt{-D}}{c}$.

Veta 2.11. *Majme $K = \mathbb{Q}[\sqrt{-D}]$ pre $-D \equiv 2{,}3$ (mod 4) také, že $Cl_K \cong (\mathbb{Z}_2)^n$ pre $n > 0$. Nech pre $\delta \in G_D(\mathbb{Q})$ platí $\delta = \varepsilon \cdot \zeta_{p_1}^{\pm\alpha_1} \dots \zeta_{p_k}^{\pm\alpha_k}$ pre nejakú voľbu znammienok $\pm$ v exponentoch, kde $\left(\frac{-D}{p_i}\right) = 1$ pre každé $0 \le i \le k$ a ε je jednotkou v $\mathbb{Z}[\sqrt{-D}]$. Potom ak δ zodpovedá nejakému normalizovanému riešeniu (a,b,c), tak $c = p_1^{\alpha_1} \dots p_k^{\alpha_k}$.*

Dôkaz. Z lemy 2.4 pre každé $c = p_i^{\alpha_i}$ dostávame, že existuje normalizované riešenie tvaru (a,b,$p_i^{\alpha_i}$) rovnice $|x^2 + Dy^2| = z^2$. Preto môžeme definovať

$$\zeta_{p_i}^{\pm\alpha_i} = \frac{a_i + b_i\sqrt{-D}}{p_i^{\alpha_i}}.$$

Induktívnym aplikovaním lemy 2.9 dostávame, že $(\alpha,\beta,p_1^{\alpha_1} \dots p_k^{\alpha_k})$ je rovnako normalizovaným riešením rovnice $|x^2 + Dy^2| = z^2$. Prvok $\delta = \varepsilon \cdot \zeta_{p_1}^{\pm\alpha_1} \dots \zeta_{p_k}^{\pm\alpha_k}$ bude zodpovedať tomuto riešeniu.

Zo znenia vety platí, že δ zodpovedá aj normalizovanému riešeniu (a,b,c). Zároveň vieme, že každý prvok z množiny $G_D(\mathbb{Q})$ zodpovedá jedinému normalizovanému riešeniu. To implikuje $c = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, čo dokazuje znenie vety. □

Veta 2.12. *Nech $K = \mathbb{Q}[\sqrt{-D}]$ pre $-D \equiv 2{,}3$ (mod 4) také, že $Cl_K \cong (\mathbb{Z}_2)^n$ pre $n > 0$ a $c = p_1^{n_1} \dots p_k^{n_k}$. Potom existuje normalizované riešenie $|x^2 + Dy^2| = z^2$ tvaru (a,b,c) práve vtedy, keď pre každé p_i platí, že $\left(\frac{-D}{p_i}\right)$. Navyše,*

1. *ak $D > 0$, tak existuje práve 2^{k-1} normalizovaných riešení tvaru (a,b,c);*
2. *ak $D < 0$, tak existuje nekonečne veľa riešení.*

Dôkaz. Z lemy 2.4 vieme, že normalizované riešenie existuje práve vtedy, keď $\left(\frac{-D}{p_i}\right) = 1$ pre každé $0 \leq i \leq k$.

Druhý bod z druhej časti tvrdenia plynie z lemy 2.6 a toho, že v $\mathbb{Z}[\sqrt{-D}]$ je pre $D < 0$ nekonečne veľa jednotiek podľa riešenia Pellovej rovnice $x^2 + Dy^2 = 1$ a z vety 1.8.

Pre dôkaz prvého bodu druhej časti tvrdenia fixujme $c = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ také, že $\left(\frac{-D}{p_i}\right) = 1$ pre každé $0 \leq i \leq k$.

Definujeme množiny

$$T_1 := \left\{ \frac{a + b\sqrt{-D}}{c} : |a^2 + Db^2| = c^2, \mathrm{NSD}(a,b) = 1, \right\}$$

a

$$T_2 := \left\{ \pm\zeta_{p_1}^{\varepsilon_1 n_1} \dots \zeta_{p_k}^{\varepsilon_1 n_k} : \varepsilon_i \text{ je jednotka v } \mathbb{Z}[\sqrt{-D}] \right\}.$$

Z lemy 2.8 dostávame, že každý prvok množiny T_1 môže byť vyjadrený v tvare prvku z množiny T_2, takže platí $T_1 \subset T_2$ a z lemy 2.11 dostávame, že $T_2 \subset T_1$.

Pre každé riešenie (a,b) rovnice $x^2 + Dy^2 = c^2$ môžeme nájsť ďalšie riešenie prenásobením $z = \frac{a+b\sqrt{-D}}{c}$ prvkom ± 1 alebo konjugáciou c.

Ak Γ je grupa rádu štyri generovaná násobením -1 a konjugáciou, ktorá pôsobí na množinu $G_D(\mathbb{Q})$, potom platí, že všetky riešenia zodpovedajúce a, b sú v orbite $\frac{a+b\sqrt{-D}}{c}$. Z toho dostávame, že normalizované riešenia rovnice $|x^2+Dy^2| = z^2$ sú dané T_1/Γ.

Komplexná konjugácia prvku $z \in T_2$ zodpovedá zobrazeniu $\varepsilon_i \to -\varepsilon_i$, takže dostávame

$$T_2/\Gamma = \left\{ \zeta_{p_1}^{n_1} \zeta_{p_2}^{\varepsilon_2 n_2} \dots \zeta_{p_k}^{\varepsilon_k n_k} : \varepsilon = \{\pm 1\} \right\}.$$

Z vlastnosti $T_1/\Gamma = T_2/\Gamma$ dostávame, že množina všetkých normalizovaných riešení je daná T_2/Γ.

Máme $k-1$ prvkov ε_i a pre každý z nich máme dve možnosti, takže $|T_1/\Gamma| = |T_2/\Gamma| = 2^{k-1}$. Z toho dostávame, že ak $\left(\frac{-D}{p_i}\right)$, tak bude existovať 2^{k-1} normalizovaných riešení rovnice $|x^2 + Dy^2| = z^2$ tvaru (a,b,c). □

Teraz dokážeme pomocou všetkých predošlých lem a viet hlavnú vetu tejto práce.

Veta 2.13. *Majme $-D \equiv 2,3$ (mod 4). Predpokladajme $Cl_K \cong (\mathbb{Z}_2)^n$ pre $n > 0$ a $K = \mathbb{Q}[\sqrt{-D}]$. Potom $G_D(Q) \cong U \times F$, kde U je grupa jednotiek v $\mathbb{Z}[\sqrt{-D}]$ a F je voľná abelovská grupa generovaná ζ_p pre všetky p také, že $\left(\frac{-D}{p}\right) = 1$. Ak $c = p_1^{n_1} \dots p_k^{n_k}$ také, že $\left(\frac{-D}{p_i}\right) = 1$ pre všetky $1 \leq i \leq k$, tak*

1. *ak $D > 0$, tak počet normalizovaných riešení tvaru (a,b,c) je 2^{k-1};*
2. *ak $D < 0$, tak existuje nekonečne veľa riešení.*

Inak neexistuje normalizované riešenie tvaru (a,b,c).

Dôkaz. Voľme F ako voľnú abelovskú grupu generovanú prvkami ζ_p. Potom platí $G_D(Q) = U \times F$.

Ak $c = p_1^{n_1} \dots p_k^{n_k}$ také, že $\left(\frac{-D}{p_i}\right) = 1$ pre všetky $1 \leq i \leq k$, tak z lemy 2.4 dostávame, že bude existovať normalizované riešenie.

Z predpokladu, že $\left(\frac{-D}{p_i}\right) = 1$ pre každé $1 \leq i \leq k$ lema 2.12 dáva, že pre $D > 0$ existuje práve 2^{k-1} a pre $D < 0$ existuje nekonečne veľa riešení.

Keďže 2.4 je ekvivalenciou, tak v prípade, že nie je splnený predpoklad $\left(\frac{-D}{p_i}\right) = 1$ pre všetky $1 \leq i \leq k$, tak riešenie nebude existovať. □

2.4 Príklady

Z predpokladu vety 2.13 vieme, že bude platiť práve vtedy, keď $Cl_K \cong (\mathbb{Z}_2)^n$ pre číselné teleso $K = \mathbb{Q}[\sqrt{-D}]$ s $-D \equiv 2{,}3 \pmod 4$ a $n \in \mathbb{N}$. V tejto kapitole si uvedieme príklady ideálových triednych grup pre rôzne D.

Existujú dva spôsoby, ktorými rovnicu $x^2 + Dy^2 = z^2$ môžeme riešiť. Buď budeme pracovať v rozšírení $\mathbb{Q}[\sqrt{-D}]$, alebo na ňu môžeme nahliadať ako na rovnicu $x^2 = z^2 - Dy^2$ a riešiť ju v rozšírení $\mathbb{Q}[\sqrt{D}]$.

Označme pre $d > 0$ číselné telesá $K_1 = \mathbb{Q}[\sqrt{d}]$ a $K_2 = \mathbb{Q}[\sqrt{-d}]$. V nasledujúcich príkladoch budeme uvažovať $d \equiv 2 \pmod 4$, pretože potom aj $-d \equiv 2 \pmod 4$. Pre $d \equiv 3 \pmod 4$ by sme v zápornom prípade dostali $-d \equiv 1 \pmod 4$, to ale nespĺňa predpoklady vety 2.4.

Môžu nastať štyri možnosti pre m,$n \in \mathbb{N}$:

- $Cl_{K_1} \cong (\mathbb{Z}_2)^m$ a $Cl_{K_2} \cong (\mathbb{Z}_2)^n$;
- $Cl_{K_1} \cong (\mathbb{Z}_2)^m$ a $Cl_{K_2} \ncong (\mathbb{Z}_2)^n$;
- $Cl_{K_1} \ncong (\mathbb{Z}_2)^m$ a $Cl_{K_2} \cong (\mathbb{Z}_2)^n$;
- $Cl_{K_1} \ncong (\mathbb{Z}_2)^m$ a $Cl_{K_2} \ncong (\mathbb{Z}_2)^n$.

Na hľadanie štruktúry ideálovej triednej grupy pre rôzne D sme využili webovú stránku The L-functions and modular forms database (LMFDB) [8], v ktorej si môžeme vyhľadať štruktúru pomocou veľkosti diskriminantu aj rôznych iných kritérií.

Možnosť $Cl_{K_1} \ncong (\mathbb{Z}_2)^m$ a $Cl_{K_2} \cong (\mathbb{Z}_2)^n$ pre nejaké m,$n \in \mathbb{N}$ a $0 \leq d \leq 200$ nenastane.

Následujúce dva príklady sú konkrétne príklady možnosti, keď $Cl_{K_1} \ncong (\mathbb{Z}_2)^m$ a $Cl_{K_2} \cong (\mathbb{Z}_2)^n$.

Príklad. Majme $d = 136$ a rozšírenia $K_1 = \mathbb{Q}[\sqrt{136}]$ a $K_2 = \mathbb{Q}[\sqrt{-136}]$, kde $-136 \equiv 2 \pmod 4$ a $136 \equiv 2 \pmod 4$. Z definície diskriminantu číselného telesa dostávame, že $disc(K_1) = -544$ a $disc(K_2) = 544$. Platí, že $Cl_{K_1} \cong \mathbb{Z}_4$ a $Cl_{K_2} \cong \mathbb{Z}_2$. Z toho plynie, že K_2 spĺňa predpoklady vety a K_1 nie.

Príklad. Nech $d = 26$, $K_1 = \mathbb{Q}[\sqrt{26}]$ a $K_2 = \mathbb{Q}[\sqrt{-26}]$, kde $-26 \equiv 2 \pmod 4$ a $26 \equiv 2 \pmod 4$. Z definície diskriminantu dostávame $disc(K_1) = -104$ a $disc(K_2) = 104$. Platí, že $Cl_{K_1} \cong \mathbb{Z}_6$ a $Cl_{K_2} \cong \mathbb{Z}_2$. Z toho plynie, že K_2 spĺňa predpoklady vety a K_1 nie.

Nasledujúce dva príklady sú zamerané na možnosť kedy $Cl_{K_1} \cong (\mathbb{Z}_2)^m$ a $Cl_{K_2} \cong (\mathbb{Z}_2)^n$.

Príklad. Nech $d = 6$, $K_1 = \mathbb{Q}[\sqrt{6}]$ a $K_2 = \mathbb{Q}[\sqrt{-6}]$, kde $-6 \equiv 2 \pmod 4$ a $6 \equiv 2 \pmod 4$. Z definície diskriminantu číselného telesa dostávame, že $disc(K_1) = -24$ a $disc(K_2) = 24$. Platí, že $Cl_{K_1} \cong \mathbb{Z}_2$ a $Cl_{K_2} \cong \mathbb{Z}_2^0$. Takže obe ideálové triedne grupy spĺňajú predpoklady našej vety.

Príklad. Majme $d = 10$ a rozšírenia $K_1 = \mathbb{Q}[\sqrt{10}]$ a $K_2 = \mathbb{Q}[\sqrt{-10}]$, kde $-10 \equiv 2 \pmod 4$ a $10 \equiv 2 \pmod 4$. Podľa definície diskriminantu číselného telesa dostávame, že $disc(K_1) = -40$ a $disc(K_2) = 40$. Platí, že $Cl_{K_1} \cong \mathbb{Z}_2$ a $Cl_{K_2} \cong \mathbb{Z}_2$. Takže obe ideálové triedne grupy spĺňajú predpoklady našej vety.

V posledných dvoch príkladoch sa zameriame na možnosť $Cl_{K_1} \ncong (\mathbb{Z}_2)^m$ a $Cl_{K_2} \ncong (\mathbb{Z}_2)^n$.

Príklad. Nech $d = 82$ a majme rozšírenia $K_1 = \mathbb{Q}[\sqrt{82}]$ a $K_2 = \mathbb{Q}[\sqrt{-82}]$, kde $-82 \equiv 2 \pmod 4$ a $82 \equiv 2 \pmod 4$. Analogicky s predošlými príkladmi dostávame $disc(K_1) = -328$ a $disc(K_2) = 328$. Platí, že $Cl_{K_1} \cong \mathbb{Z}_4$ a $Cl_{K_2} \cong \mathbb{Z}_4$, takže ani jedna z ideálových triednych grup nespĺňa podmienky našej vety.

Príklad. Majme $d = 142$ a rozšírenia $K_1 = \mathbb{Q}[\sqrt{142}]$ a $K_2 = \mathbb{Q}[\sqrt{-142}]$, kde $-142 \equiv 2 \pmod 4$ a $142 \equiv 2 \pmod 4$. Podľa definície diskriminantu číselného telesa dostávame, že $disc(K_1) = -184$ a $disc(K_2) = 184$. Platí, že $Cl_{K_1} \cong \mathbb{Z}_4$ a $Cl_{K_2} \cong \mathbb{Z}_3$. Takže žiadna z týchto ideálových triedných grup nespĺňa predpoklady našej vety.

Na záver si v príkladoch uvedieme faktorizáciu rovnakého riešenia pomocou vety 2.8.

Príklad. Majme rovnicu $x^2+2y^2 = z^2$. Platí, že ideálova triedna grupa $Cl_{\mathbb{Q}[\sqrt{2}]} \cong \mathbb{Z}_2^0$ a ideálova triedna grupa $Cl_{\mathbb{Q}[\sqrt{-2}]} \cong \mathbb{Z}_2^0$, takže obe spĺňajú predpoklady viet z našej práce.

Rovnica $x^2 + 2y^2 = z^2$ má normalizované riešenie (7,4,9). Podľa vety 2.8 platí, že toto riešenie dokážeme vyjadriť ako

$$\delta_1 = \varepsilon_1 \left(\frac{a + b\sqrt{-2}}{3} \right)^2,$$

kde a,b nájdeme podľa definície ako riešenie rovnice $a^2 + 2b^2 = 3^2$. Dostávame, riešenie $a = 1$ a $b = -2$ Jednotku ε_1 v kvadratickom rozšírení $\mathbb{Z}[\sqrt{-2}]$ dopočítame podľa toho, že vieme, že z definície

$$\delta_1 = \left(\frac{7 + 4\sqrt{-2}}{9} \right).$$

Konečne, môžeme δ_1 vyjadriť v tvare podľa vety 2.8

$$\delta_1 = -\left(\frac{1 - 2\sqrt{-2}}{3} \right)^2.$$

Teraz nazerajme na túto rovnicu ako na $x^2 = z^2 - 2y^2$. Potom dostávame normalizované riešenie (9,4,7). Podľa vety 2.8 analogicky s prvou časťou príkladu dostávame

$$\delta_2 = \varepsilon_2 \left(\frac{9 + 4\sqrt{2}}{7} \right),$$

kde ε_2 je jednotka v kvadratickom rozšírení $\mathbb{Z}[\sqrt{2}]$. Jednotku dopočítame podobne ako pri rovnici $x^2 + 2y^2 = z^2$ a dostávame, že $\varepsilon_2 = 1$.

Konečne, dostávame

$$\delta_2 = \left(\frac{9 + 4\sqrt{2}}{7}\right).$$

Takže sme to isté riešenie vyjadrili dvoma úplne odlišnými spôsobmi.

Príklad. Majme rovnicu $x^2 + 6y^2 = z^2$. Podľa príkladov uvedených vyššie vieme, že ideálova triedna grupa $\mathbb{Q}[\sqrt{6}]$ aj ideálova triedna grupa $\mathbb{Q}[\sqrt{-6}]$ spĺňajú predpoklady viet z našej práce.

Rovnica $x^2 + 6y^2 = z^2$ má riešenie $(23, -4, 25)$. Podľa vety 2.8 vieme, že toto riešenie môžeme vyjadriť v tvare

$$\delta_1 = \varepsilon_1 \left(\frac{a + b\sqrt{-6}}{5}\right)^2,$$

kde a aj b získame vyriešením rovnice $a^2 + 6b^2 = 5^2$. V tomto prípade dostávame riešenie $a = 1$ a $b = 2$. Jednotku ε_1 v kvadratickom rozšírení $\mathbb{Z}[\sqrt{-6}]$, dopočítame podľa toho, že z definície vieme, že δ_1 bude mať tvar

$$\delta_1 = \left(\frac{23 - 4\sqrt{-2}}{25}\right).$$

Dostávame, že $\varepsilon_1 = -1$. Môžeme vyjadriť

$$\delta_1 = -\left(\frac{1 + 2\sqrt{-6}}{5}\right)^2.$$

Rovnako ako v predošlom príklade budeme teraz na túto rovnicu nahliadať ako na $x^2 = z^2 - 6y^2$ a dostávame normalizované riešenie $(25, -4, 23)$. Analogicky s prvou časťou príkladu dostávame

$$\delta_2 = \varepsilon_2 \left(\frac{25 - 4\sqrt{6}}{23}\right),$$

kde ε_2 dopočítame podľa toho, že

$$\delta_2 = \left(\frac{25 - 4\sqrt{6}}{23}\right)$$

a dostávame $\varepsilon_2 = 1$.

Finálne,

$$\delta_2 = \left(\frac{25 - 4\sqrt{6}}{23}\right).$$

Znovu nám každý pohľad na danú rovnicu dal úplne inú faktorizáciu toho istého riešenia.

Záver

V tejto práci sme pomocou lem a tvrdení dokázali vetu 2.13 o štruktúre a počte riešení rovnice $|x^2 + Dy^2| = z^2$ pre $D \in \mathbb{Z}$, bezštvorcové a $-D \equiv 2{,}3 \pmod 4$. V dôkazoch jednotlivých viet tvrdení sme pracovali v ideálovej triednej grupe telesa $\mathbb{Q}[\sqrt{-D}]$.

Ak by sme to chceli rozšíriť aj pre $-D \equiv 1 \pmod 4$, tak podľa poznámky za definíciou číselného telesa by sme dostali $\mathcal{O}_K = \mathbb{Z}[\frac{1+\sqrt{-D}}{2}]$, preto by sme aj špeciálne museli zadefinovať normu prvku.

Ak by sme chceli riešiť rovnicu aj pre nie bezštvorcové D, tak by sme museli využiť podkapitolu štyri v kapitole dva o rádoch. Označme $D = EF^2$, kde E je bezštvorcové a $EF^2 \equiv 2{,}3 \pmod 4$. Z toho, že kvadratickými zbytkami modulo 4 sú len 1 a 0, dostávame kongruenciu $E \equiv 2{,}3 \pmod 4$.

Podľa toho platí, že by sme museli pracovať v ideáloch rádu $\mathcal{O} = \mathbb{Q}[F\sqrt{E}]$, čo by si vyžadovalo podrobnejšie spracovanie teórie o tejto štruktúre pomocou [2].

Zoznam použitej literatúry

[1] Vítězslav Kala. Teorie čísel. https://www.karlin.mff.cuni.cz/~kala/files/TC22.pdf, 2022.

[2] T. Jaklitsch, T.C. Martinez, S.J. Miller, and S. Mukherjee. Connections of class numbers to the group structure of generalized pythagorean triples. https://arxiv.org/abs/2112.03663v1, 2020.

[3] David Stanovský. Učební text algebra. https://www2.karlin.mff.cuni.cz/~stanovsk/vyuka/2122/algebra22.pdf, 2021.

[4] Vítězslav Kala. Úvod do komutativní algebry. http://karlin.mff.cuni.cz/~kala/files/UKA22.pdf, 2022.

[5] Siu Hang Man. Quadratic forms and class fields i. https://drive.google.com/file/d/1EvKdhC8Pv-Qe519sA_L2szlQwRT2ylWw/edit, 2022.

[6] David A. Cox. *Primes of the form* x^2+ny^2. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989. Fermat, class field theory and complex multiplication.

[7] Keith Conrad. The conductor of an order. https://kconrad.math.uconn.edu/blurbs/gradnumthy/conductor.pdf, 2020.

[8] The LMFDB Collaboration. The L-functions and modular forms database. https://www.lmfdb.org, 2023. [Online; accessed 21 April 2023].