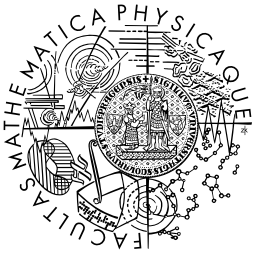

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

DIPLOMOVÁ PRÁCE

Bc. Martin Kuděj

Polomřížky a nerozložitelné prvky

Katedra algebry

Vedoucí diplomové práce: doc. Mgr. Vítězslav Kala, Ph.D.
Studijní program: Matematické struktury
Studijní obor: Matematické struktury

Praha 2024

Prohlašuji, že jsem tuto diplomovou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Tato práce nebyla využita k získání jiného nebo stejného titulu.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Rád bych poděkoval vedoucímu práce doc. Mgr. Vítězslavu Kalovi, Ph.D. za představení tématu této práce a mimořádnou ochotu při konzultacích, bez kterých by tato práce nemohla vzniknout. Dále bych chtěl poděkovat všem, co mě během studia podporovali.

Název práce: Polomřížky a nerozložitelné prvky

Autor: Bc. Martin Kuděj

Katedra: Katedra algebry

Vedoucí diplomové práce: doc. Mgr. Vítězslav Kala, Ph.D., Katedra algebry

Abstrakt: Tato práce se zabývá teorií polomřížek, což jsou netriviální diskrétní podmonoidy v $\mathbb{R}^n$ se sčítáním, které jsou obsaženy v nějakém kuželi. Speciální pozornost je věnována jejich nerozložitelným prvkům. Nejdůležitější případ polomřížek je odvozen z reálných kvadratických číselných těles, kterému je věnována značná část práce a charakterizace nerozložitelných prvků těchto polomřížek je v práci dokázána dvěma způsoby, k čemuž je využito různých partií z teorie čísel, především se jedná o řetězové zlomky, k nim příslušné polokonvergenty a jejich aproximační vlastnosti, Fareyho dvojice, ale také je použita algebraická teorie čísel. Závěrečná část práce je dále věnována hornímu odhadu normy nerozložitelných prvků v polomřížce, odpovídající Minkowského vnoření příslušného číselného tělesa.

Klíčová slova: Polomřížky, nerozložitelné prvky, řetězové zlomky, algebraická teorie čísel, Minkowského prostor

Title: Semilattices and indecomposable elements

Author: Bc. Martin Kuděj

Department: Department of algebra

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

Abstract: This thesis concerns the theory of semilattices, which are non-trivial discrete additive submonoids of $\mathbb{R}^n$, which are contained in a cone. Special emphasis is on their indecomposable elements. The most important example of semilattices is derived from real quadratic number fields, which involves the most parts of the thesis and all indecomposable elements of such semilattices are characterised in two ways. That includes using various tools from number theory, mainly continued fractions, their corresponding semiconvergents and their approximation properties, Farey pairs, but also some tools from algebraic number theory. The final part of the thesis concerns the upper bound of the norm of indecomposable elements in a semilattice, derived from the Minkowski embedding of the corresponding number field.

Keywords: Semilattices, indecomposable elements, continued fractions, algebraic number theory, Minkowski space

Obsah

Úvod

Polomřížky jsou algebraické objekty, které mají strukturu monoidu (tedy na nich uvažujeme asociativní binární operaci, kterou v našem případě vždy bude standardní sčítání na $\mathbb{R}^n$, čímž speciálně říkáme, že se vždy bude jednat o podmonoidy $\mathbb{R}^n$, které navíc obsahují neutrální prvek k této binární operaci, kterým je vždy 0), obsahují alespoň jeden nenulový prvek, jedná se o diskrétní množinu (tedy o množinu bez hromadných bodů vzhledem ke standardní topologii na $\mathbb{R}^n$) a zároveň všechny prvky polomřížky jsou obsaženy v nějakém kuželi, což je taková neprázdná konvexní množina v $\mathbb{R}^n$, že nenulové prvky jeho topologického uzávěru jsou obsaženy v nějakém otevřeném poloprostoru, což je množina všech bodů $(x_1, x_2, \ldots, x_n)$, vyhovující podmínce $a_1x_1 + a_2x_2 + \ldots + a_nx_n > 0$ pro fixní hodnoty $a_1, a_2, \ldots, a_n \in \mathbb{R}$, a navíc prvky kužele C jsou uzavřeny na násobení kladnými reálnými čísly, tedy pro $x \in C$ a $t \in \mathbb{R}^+$ platí $tx \in C$ (geometricky řečeno, pro každý bod x z kužele C, obsahuje tento kužel i celou polopřímku, procházející bodem x, která je ukotvená v 0). Všechny tyto pojmy jsou v práci postupně zadefinovány, konkrétně je například kužel zadefinován v definici 1.6 a polomřížka v definici 1.8.

Důležitou roli v polomřížkách mají její nerozložitelné prvky, což jsou takové prvky, které nelze netriviálně (tedy bez použití 0) napsat jako součet dvou prvků ze stejné polomřížky. Množina všech nerozložitelných prvků je totiž generující množinou dané polomřížky (uvažujeme generování jako monoidu), což je konkrétně dokázáno ve větě 1.15. Zároveň se jedná o minimální množinu generátorů, tedy každá další množina generátorů této polomřížky všechny nerozložitelné prvky nutně musí obsahovat.

Nejdůležitější příklad polomřížek, který v této práci budeme zkoumat, je odvozen ze základních objektů algebraické teorie čísel: Pro reálné kvadratické číselné těleso $K = \mathbb{Q}(\sqrt{D})$, kde $D \neq 1$ je bezčtvercové přirozené číslo, uvažujme v rámci jeho celistvých prvků (tedy kořenů nějakých monických polynomů z celočíselnými koeficienty), které značíme $\mathcal{O}_K$, takové prvky, které jsou totálně nezáporné (tedy samotný prvek i jeho konjugát jsou větší nebo rovny 0) a navíc budeme uvažovat pouze takové prvky, které jsou větší nebo rovny svému konjugátu. Tuto výslednou množinu značíme S_K a ta již tvoří polomřížku, jak si ve 3. kapitole práce ukážeme. Velká pozornost bude věnována nerozložitelným prvkům těchto polomřížek, neboť tyto nerozložitelné prvky lze přesně charakterizovat pomocí tzv. polokonvergentů, což jsou jisté řetězové zlomky aproximující číslo $\sqrt{D}$, pokud $D \equiv 2, 3 \bmod 4$ $\left(\text{nebo číslo } \dfrac{\sqrt{D}-1}{2}, \text{ pokud } D \equiv 1 \bmod 4\right)$, ve smyslu definice 2.16. Teorií řetězových zlomků autor navazuje na svoji bakalářskou práci, která byla zároveň lehce rozšířena a publikována jakožto článek [9].

V první kapitole této práce jsou zadefinovány základní topologické a algebraické pojmy, které jsou potřebné k tomu, abychom vůbec mohli zadefinovat pojem polomřížky. Důležitou vlastností polomřížek je, že její nosná množina musí být diskrétní, tedy nesmí obsahovat hromadné body vzhledem ke standardní topologii na $\mathbb{R}^n$. Pokud budeme chtít ověřit, že nějaká množina je diskrétní, tak se stačí podívat na tvrzení 1.5, které nám popisuje postačující podmínku k tomu, aby nějaká množina byla diskrétní: stačí ověřit, že daná množina má konečný

průnik s každou z množin z nějakého systému kompaktních množin, jenž pokrývá celé $\mathbb{R}^n$. Zároveň platí, že každá diskrétní množina má konečný průnik s úplně každou kompaktní množinou, což je zároveň nutná podmínka k ověření diskrétnosti podle tvrzení 1.3. Tato dvě tvrzení jsou vyslovena a dokázána v sekci 1.1, tyto důkazy jsou vlastním přínosem autora. V sekci 1.2 se poté podrobněji zaměříme na polomřížky v jedné dimenzi, hlavním výsledkem této sekce je charakterizace polomřížek v jedné dimenzi pomocí existence bijekce s $\mathbb{N}$, která zachovává uspořádání, což je znění tvrzení 1.11, jehož důkaz je opět vlastním dílem autora. V sekci 1.3 se podíváme na obecné polomřížky v libovolné dimenzi a zadefinujeme důležitý pojem nerozložitelného prvku. Ve větě 1.15 se ukáže, že množina nerozložitelných prvků nějaké polomřížky tuto polomřížku generuje (jako monoid), za zmínku rovněž stojí zajímavé tvrzení 1.17, které popisuje jednoznačnost vyjádření pomocí nějaké generující množiny v souvislosti na lineární nezávislosti této generující množiny, což nám ukazuje, že tato vlastnost, která přirozeně platí v celém $\mathbb{R}^n$ (což je známé z lineární algebry), se dá zobecnit i do polomřížek. Všechny důkazy tvrzení z této sekce jsou vlastním dílem autora s částečnou inspirací z článku [14], neboť zde zobecňujeme do libovolného počtu dimenzí právě některá tvrzení z tohoto článku.

Ve druhé kapitole této práce se věnujeme připomenutí a případnému doplnění potřebného aparátu z teorie čísel, abychom se v následující kapitole mohli zaměřit na důležitý příklad polomřížek. Základním nástrojem z teorie čísel, který budeme potřebovat, jsou tzv. řetězové zlomky, které obecně slouží k aproximaci iracionálních čísel racionálními, čímž autor navazuje na svoji bakalářskou práci, která byla v lehce rozšířené podobě publikována jako článek [9]. V sekci 2.1 jsou tyto řetězové zlomky zadefinovány a zároveň jsou připomenuty jejich nejdůležitější vlastnosti, které jsou dokázány v článku [9] případným odkazem na další literaturu. Sekce 2.2 je věnována důležitému případu řetězových zlomků, kterými jsou tzv. polokonvergenty, které jsou zadefinovány v definici 2.10, přičemž počet polokonvergentů přiřazených ke svému racionálnímu číslu je konečný a přesně popsán v lemmatu 2.11, jehož důkaz je vlastním dílem autora. Poté v části 2.2.2 je krátce rozvinuta teorie Fareyho dvojic, která byla čerpána z diplomové práce [10], některé důkazy však byly v této práci oproti zdroji zjednodušeny, což je případ lemmatu 2.14. V tvrzení 2.15 je poté popsána souvislost Fareyho dvojic a polokonvergentů. V části 2.2.3 se poté ve větě 2.17 ukáže, že právě polokonvergenty tvoří tzv. dobré horní aproximace ve smyslu definice 2.16. Důkaz této věty je vlastním dílem autora. V sekci 2.3 podrobněji zkoumáme řetězové zlomky algebraických čísel stupně 2, obzvlášť důležitá je věta 2.22, kde je přesně popsán tvar řetězového zlomku těch nejdůležitějších algebraických čísel stupně 2. Z části 2.3.1 jsou důkazy všech tvrzení k nalezení v článku [9], s výjimkou lemmatu 2.23, jehož důkaz je zde podrobně zpracován a je vlastním dílem autora, stejně jako důkazy všech tvrzení z části 3.2.3, kromě posledního lemmatu 2.27, které je čerpáno z článku [3]. Sekce 2.4 je věnována připomenutí toho nejdůležitějšího aparátu z algebraické teorie čísel, jsou zde připomenuty definice těch nejdůležitějších pojmů a vyslovena potřebná tvrzení, k nimž lze nalézt důkazy v knize [11], kromě části 2.4.2, kde jsou dvě lemmata 2.34 a 2.35, která jsou čerpána z článku [3].

Ve třetí kapitole této práce budeme aplikovat připomenutý aparát z teorie čísel z minulé kapitoly ke zjištění důležitých informací o polomřížkách S_K, popsaných ve třetím odstavci tohoto úvodu. Sekce 3.1 je věnována úhlovým oblastem, což

je pomocný příklad polomřížek. Úhlové oblasti jsou zadefinovány v definici 3.1 a ve větě 3.5 jsou charakterizovány jejich nerozložitelné prvky pomocí vhodných polokonvergentů vhodných algebraických čísel stupně 2. Důsledky 3.3 a 3.6 jsou vlastním dílem autora (dochází zde ke zobecnění výsledků z článku [3] v porovnání nejen úhlových oblastí $F_{\alpha,\beta}$ a E_α, ale i $F_{\alpha,\beta}$ a E_β). Ostatní důkazy z této sekce jsou převzaty z článku [3]. Sekce 3.2 je poté věnována popisu nerozložitelných prvků v polomřížce S_K. Nejprve je zde vysvětleno, proč S_K tvoří polomřížku, a proč ji netvoří $\mathcal{O}_K^{+,0}$, či dokonce $\mathcal{O}_K$, a poté použitím věty 3.5 dostaneme větu 3.8, která nám obecně popisuje všechny nerozložitelné prvky v S_K. Následující části 3.2.2 a 3.2.3 jsou poté věnovány jednoduššímu popisu nerozložitelných prvků, respektive jde o jejich konečný výčet, až na násobení čtvercem libovolné, předem určené jednotky $\varepsilon > 1$. Část 3.2.2 je zpracována podle článku [3], některé části byly zpřehledněny, přeuspořádány, lemma 3.9 je v tomto článku pouze vysloveno, jeho důkaz zde je vlastním dílem autora, a byl vysvětlen jejich algebraický kontext, aby bylo jasné, která množina tvoří polomřížku a která nikoliv. Samotný konečný výčet nerozložitelných prvků, až na násobení čtvercem jednotky $\varepsilon > 1$, je popsán v důsledku 3.14. Část 3.2.3 je naopak celá vlastním dílem autora, zde je s použitím tvrzení 2.25 a 2.26 ukázáno, že konečný výčet prvků až na násobení čtvercem jednotkou z důsledku 3.14 skutečně odpovídá obecnému popisu z věty 3.8. Navíc se v části 3.2.3 pozastavíme i nad jednoznačností vyjádření nerozložitelných prvků tvaru dle důsledku 3.14.

Ve čtvrté kapitole této práce se podíváme na odhad norem nerozložitelných prvků v Minkowského prostoru, přičemž tuto normu budeme nazývat normou v polomřížce L a tuto normu budeme definovat pomocí součinu všech souřadnic, což v případě polomřížek $\sigma(\mathcal{O}_K^{+,0})$ přesně odpovídá pojmu normy z algebraické teorie čísel. V sekci 4.1 se budeme věnovat právě polomřížkám tvaru $\sigma(\mathcal{O}_K^{+,0})$, kde K je libovolné totálně reálné (tedy nejen reálné kvadratické) číselné těleso a σ je Minkowského vnoření. Zde budeme místo normy v dané polomřížce dle definice 4.1 používat klasickou normu, kterou známe z předchozích dvou kapitol, abychom jednodušeji aplikovali nástroje ze třetí kapitoly (tyto normy jsou navíc stejné). Ve větě 4.2 je popsán a dle článku [3] dokázán odhad na normu nerozložitelných prvků v případě reálných kvadratických číselných těles, přičemž tento odhad je optimální, pokud v daném číselném tělese existuje jednotka s normou -1. Ve větě 4.3 je poté dokázán méně přesný odhad pro obecná totálně reálná číselná tělesa, tento důkaz je reprodukován z článku [8] a používá, mimo jiné, Minkowského větu o mřížových bodech, která je uvedena v části 2.4.3 jakožto věta 2.36. Celkově tedy dojdeme k závěru, že v tomto případě polomřížek nemohou mít nerozložitelné prvky libovolně velkou normu ve své polomřížce. V sekci 4.2 však ukážeme, že pro obecné polomřížky toto neplatí: v této sekci zkonstruujeme příklad polomřížky v libovolné dimenzi, kde nerozložitelné prvky mohou mít libovolně velkou normu ve své polomřížce. Tento příklad je vlastním dílem autora a tento výsledek je shrnut ve větě 4.5.

Významu nerozložitelných prvků v polomřížkách $\sigma(\mathcal{O}_K^{+,0})$ bylo využito v řadě nedávných článků, aby bylo možné dokázat například to, že univerzální kvadratické formy musí mít hodně proměnných, o čemž pojednávají články [2] a [7]. Jinému popisu monoidu $\mathcal{O}_K^{+,0}$ pro případ reálných kvadratických číselných těles se rovněž věnuje článek [5].

1. Základní vlastnosti polomřížek

1.1 Připomenutí známých pojmů

1.1.1 Základní topologické pojmy

V úvodní části této sekce si stručně připomeneme známé pojmy z topologie, které budeme v práci potřebovat, a zároveň ukážeme nějaké souvislosti mezi těmito pojmy.

Topologickým prostorem budeme rozumět dvojici (X, τ), kde X je neprázdná množina a τ je systém podmnožin X, který obsahuje prázdnou množinu, množinu X a je uzavřený na konečné průniky a libovolná sjednocení. Systém množin τ nazýváme *topologií* a množiny patřící do systému τ nazveme *otevřené množiny*. V této práci nás bude pouze zajímat situace $X = \mathbb{R}^n$ a τ bude *standardní topologie*, kterou si nyní představíme:

Standardní topologie na $\mathbb{R}^n$ je indukována *eukleidovskou normou*, kde eukleidovská norma bodu $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ je definována jako

$$||x||_2 = \sqrt{x_1^2 + x_2^2 + \ldots + x_n^2}.$$

Nyní můžeme zadefinovat pojmy *koule*, *sféry* a jejich *poloměrů* $\varepsilon > 0$: *Otevřenou koulí* kolem bodu $x \in \mathbb{R}^n$ o poloměru ε budeme rozumět množinu všech bodů $y \in \mathbb{R}^n$, že $||x - y||_2 < \varepsilon$, *uzavřenou koulí* kolem bodu $x \in \mathbb{R}^n$ o poloměru ε budeme rozumět množinu všech bodů $y \in \mathbb{R}^n$, že $||x - y||_2 \leq \varepsilon$ a *sférou* kolem bodu $x \in \mathbb{R}^n$ o poloměru ε budeme rozumět množinu všech bodů $y \in \mathbb{R}^n$, že $||x - y||_2 = \varepsilon$. Otevřené koule budeme značit symbolem $U_x(\varepsilon)$ nebo U_x, pokud konkrétní volba ε nebude důležitá, obdobně budeme uzavřené koule značit $\overline{U_x(\varepsilon)}$ či $\overline{U_x}$ a sféry budeme značit $S_x(\varepsilon)$ či S_x. Nyní si můžeme již konkrétně říci, co je to standardní topologie na $\mathbb{R}^n$. Jako otevřené množiny budeme uvažovat právě takové množiny $G \subseteq \mathbb{R}^n$, že pro všechna $x \in G$ existuje otevřená koule U_x tak, že $U_x \subseteq G$. Opravdu se jedná o topologii a navíc dostáváme, že všechny otevřené koule jsou otevřené množiny.

Dále budeme používat trojúhelníkovou nerovnost, která říká, že pro všechna x,$y \in \mathbb{R}^n$ platí $||x + y||_2 \leq ||x||_2 + ||y||_2$.

Důležitý pro nás bude pojem *hromadného bodu* množiny $M \subseteq \mathbb{R}^n$:

Definice 1.1. *Nechť $M \subseteq \mathbb{R}^n$ a uvažujme bod $x \in \mathbb{R}^n$. Řekneme, že bod x je* hromadný bod *množiny M, pokud pro všechny otevřené koule U_x kolem bodu x platí, že $M \cap (U_x \setminus \{x\}) \neq \emptyset$. Množinu M nazveme* diskrétní*, pokud žádný bod $x \in \mathbb{R}^n$ není hromadným bodem množiny M.*

Nyní si připomeneme pojmy *uzavřené množiny* a *topologického uzávěru*. Množinu $M \subseteq \mathbb{R}^n$ nazveme uzavřenou, pokud pro každý hromadný bod x množiny M platí, že $x \in M$. Dá se ukázat, že uzavřené množiny jsou právě doplňky otevřených množin (vzhledem k $\mathbb{R}^n$). *Topologickým uzávěrem* množiny $M \subseteq \mathbb{R}^n$ rozumíme nejmenší uzavřenou množinu (co do inkluze), která obsahuje množinu M. Topologický uzávěr množiny M budeme značit symbolem $\overline{M}$, což se shoduje s již zmíněným značením u otevřených a uzavřených koulí, neboť topologickým uzávěrem každé otevřené koule je uzavřená koule o tom samém poloměru, speciálně dostáváme, že uzavřené koule jsou uzavřené množiny.

Dále budeme potřebovat pojem *kompaktní množiny*, k jehož zadefinování využijeme pojmu *pokrytí* množiny $M \subseteq \mathbb{R}^n$, což je takový systém otevřených množin $(G_i)_{i\in I}$ v $\mathbb{R}^n$, že $M \subseteq \bigcup_{i\in I} G_i$. Množinu $M \subseteq \mathbb{R}^n$ nazveme *kompaktní*, pokud „z každého pokrytí lze vybrat konečné podpokrytí“, neboli pro každé pokrytí $(G_i)_{i\in I}$ množiny M existuje konečná množina $J \subseteq I$ tak, že $(G_j)_{j\in J}$ tvoří pokrytí množiny M.

Tato definice kompaktní množiny je validní pro obecné topologické prostory, avšak v případě topologického prostoru $\mathbb{R}^n$ se standardní topologií můžeme využít dvě jednoduché charakterizace kompaktních množin: Množina $M \subseteq \mathbb{R}^n$ je kompaktní, právě když každá její nekonečná podmnožina má hromadný bod v M, a dále je množina M kompaktní, právě když M je *uzavřená* (pro každý hromadný bod x množiny M platí, že $x \in M$, ekvivalentně $X \setminus M$ je otevřená množina) a *omezená* (existuje $c \in \mathbb{R}$ tak, že $||x||_2 < c$ pro všechna $x \in M$). Příkladem kompaktních množin jsou uzavřené koule, sféry, ale také krychle, které si nyní představíme:

Definice 1.2. *Nechť $c \in \mathbb{R}$ je kladné číslo.* Krychlí *v $\mathbb{R}^n$ s parametrem c rozumíme množinu $K(c) = \{y \in \mathbb{R}^n \mid \forall i \in \{1, 2, \ldots, n\}, -c \leq y_i \leq c\}$.*

Nyní již přejdeme k tvrzením, která si dokážeme, která propojují výše představené pojmy a zároveň se nám budou hodit i v dalších sekcích této kapitoly.

Tvrzení 1.3. *Buďte $X, M \subseteq \mathbb{R}^n$, nechť X je kompaktní množina a M je diskrétní množina. Potom $X \cap M$ je konečná množina.*

Důkaz. Pro každé $x \in X$ platí, že x není hromadným bodem množiny M, proto existuje otevřená koule U_x tak, že $M \cap U_x \subseteq \{x\}$. Systém otevřených koulí $(U_x)_{x\in X}$ tvoří pokrytí množiny X, která je kompaktní, proto existuje konečná množina $Y \subseteq X$ tak, že $(U_y)_{y\in Y}$ rovněž tvoří pokrytí množiny X. Poté platí:

$$|X \cap M| \leq \left| \bigcup_{y\in Y} U_y \cap M \right| \leq |Y|,$$

nicméně Y je konečná množina, čímž je tvrzení dokázané. □

Toto tvrzení má následující důsledek:

Důsledek 1.4. *Každá diskrétní množina $M \subseteq \mathbb{R}^n$ je nejvýše spočetná.*

Důkaz. Stačí pokrýt celé $\mathbb{R}^n$ spočetně mnoho kompaktními množinami, k čemuž můžeme využít systém krychlí $K(m)_{m\in\mathbb{N}}$. Potom $|M| \leq |\bigcup_{m\in\mathbb{N}} K(m) \cap M|$. Každá z množin $K(m) \cap M$ je konečná díky tvrzení 1.3. Nyní si stačí uvědomit, že sjednocení spočetně mnoha konečných množin je nejvýše spočetná množina, čímž byl důkaz dokončen. □

O vztahu kompaktních a diskrétních množin v $\mathbb{R}^n$ si ukážeme platnost ještě jednoho tvrzení, které úzce souvisí s tvrzením 1.3. Zároveň budeme toto tvrzení často využívat k tomu, abychom dokázali, že nějaká množina je diskrétní.

Tvrzení 1.5. *Nechť $M \subseteq \mathbb{R}^n$. Předpokládejme, že pro každou krychli ze systému $(K(m), m \in \mathbb{N})$ v $\mathbb{R}^n$ platí, že $K(m) \cap M$ je konečná množina. Potom M je diskrétní množina.*

Důkaz. Důkaz provedeme sporem. Nechť $x \in \mathbb{R}^n$ je hromadný bod množiny M. Induktivním opakováním definice hromadného bodu dostaneme, že otevřená koule $U_x(1)$ (otevřená koule kolem bodu x s poloměrem 1) obsahuje nekonečně mnoho prvků množiny M. Není těžké odvodit existenci krychle $K(m)$, která bude obsahovat otevřenou kouli $U_x(1)$, speciálně bude obsahovat nekonečně mnoho bodů z množiny M, čímž však dostáváme spor s předpokladem, že $K(m) \cap M$ je konečná množina. □

Tvrzení 1.5 by rovněž platilo, pokud bychom předpokládali konečný průnik množiny M s každou z množin z libovolného systému kompaktních množin v $\mathbb{R}^n$, který pokrývá celé $\mathbb{R}^n$. My se však budeme zabývat především případem, kdy daný systém kompaktních množin tvoří krychle.

Na závěr této části si zavedeme pojem *kužele*. Množina $M \in \mathbb{R}^n$ je *konvexní*, pokud pro všechna x,$y \in M$ a pro všechna $t \in [0,1]$ platí, že $tx + (1-t)y \in M$. Každá konvexní množina M je uzavřená na *konvexní kombinace*, tedy pro všechna $x_1, x_2, \ldots x_k \in M$ a všechna $t_1, t_2, \ldots, t_k \in \mathbb{R}_0^+$ taková, že $\sum_{i=1}^k t_i = 1$ platí, že $\sum_{i=1}^k t_i x_i \in M$. *Konvexním obalem* množiny M rozumíme nejmenší (co do inkluze) konvexní množinu, která množinu M obsahuje. *Otevřeným poloprostorem* v $\mathbb{R}^n$ budeme rozumět množinu všech bodů $x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n$ takovou, že pro nějaká fixní čísla $a_1, a_2, \ldots, a_n \in \mathbb{R}$ platí $a_1x_1 + a_2x_2 + \ldots + a_nx_n > 0$, přičemž po označení $a := (a_1, a_2, \ldots, a_n)$ budeme pro součet $a_1x_1 + a_2x_2 + \ldots + a_nx_n$ používat značení $\langle a, x \rangle$, odpovídající standardnímu skalárnímu součinu vektorů a, x. Dále budeme využívat toho, že skalární součin $\langle a, x \rangle$ jakožto funkce n-dimenzionální proměnné x je spojitá funkce, a tedy na každé kompaktní množině nabývá tato funkce svého maxima a minima, speciálně je tato funkce na této množině omezená. Nyní již zadefinujeme pojem kužele:

Definice 1.6. *Neprázdnou konvexní množinu C v $\mathbb{R}^n$ nazveme* kuželem*, pokud platí, že existuje otevřený poloprostor takový, že všechny prvky $\overline{C} \setminus \{0\}$ v tomto otevřeném poloprostoru leží, a navíc pro všechna $x \in C$ platí, že C obsahuje bod tx pro všechna $t \in \mathbb{R}_0^+$.*

Jednoduchým příkladem kužele je množina $(\mathbb{R}_0^+)^n$, tedy množina všech bodů z $\mathbb{R}^n$, které mají všechny souřadnice nezáporné (nenulové prvky tohoto kužele leží v otevřeném poloprostoru daném nerovnicí $x_1 + x_2 + \ldots + x_n > 0$). V případě $n = 2$ bude pro nás význačný kužel, který je zkonstruován jako konvexní obal dvou polopřímek, které na sebe nejsou opačné, a zároveň mají společný počáteční bod v bodě (0,0). Kužele v jedné dimenzi budou charakterizovány v odstavci před tvrzením 1.11.

V této práci využijeme následující vlastnost kuželů:

Tvrzení 1.7. *Nechť $C \subseteq \mathbb{R}^n$ je kužel takový, že nenulové prvky $\overline{C}$ leží v otevřeném poloprostoru určeném nerovnicí $\langle a, x \rangle > 0$ a pro všechna reálná čísla $t \in \mathbb{R}^+$ označme $U_t := \{x \in \mathbb{R}^n \mid 0 < \langle a, x \rangle \leq t\}$. Potom pro všechna $t \in \mathbb{R}^+$ je množina $C \cap U_t$ omezená, tedy $\overline{C \cap U_t}$ je kompaktní množina.*

Důkaz. Důkaz provedeme sporem, nechť $t \in \mathbb{R}^+$ je takové, že $C \cap U_t$ není omezená množina. Zvolme posloupnost prvků $(\beta_i)_{i \in \mathbb{N}}$ následujícím způsobem: Nechť $||\beta_1||_2 > 1$ a pro všechna $i \in \mathbb{N}$, nechť $||\beta_{i+1}||_2 > 2\,||\beta_i||_2$. Taková posloupnost prvků z $C \cap U_t$ existuje díky neomezenosti této množiny a dále snadno nahlédneme, že $||\beta_i||_2 \overset{i \to \infty}{\to} \infty$. Dále pro všechna i položme $r_i := \frac{1}{||\beta_i||_2}$. Poté pro všechna i

platí, že $||r_i\beta_i||_2 = 1$, $0 < r_i < 1$ a navíc $r_i \overset{i\to\infty}{\to} 0$. Nyní si uvědomíme, že skalární součiny $\langle a, r_i\beta_i\rangle$ konvergují k 0:

$$0 \overset{r_i\beta_i\in C}{\leq} \langle a, r_i\beta_i\rangle = r_i\langle a, \beta_i\rangle \overset{\beta_i\in U_t}{\leq} tr_i \overset{i\to\infty}{\to} 0. \tag{1.1}$$

Teď využijeme toho, že všechny prvky $r_i\beta_i$ leží na jednotkové sféře, což je kompaktní množina, tedy posloupnost $(r_i\beta_i)_{i\in\mathbb{N}}$ má hromadný bod $\beta \in \overline{C} \cap S_0(1)$ (tedy platí, že $||\beta||_2 = 1$), nechť $r_{i_j}\beta_{i_j} \overset{j\to\infty}{\to} \beta$. Nyní ukážeme, že $\langle a, \beta\rangle = 0$:

$$\langle a, \beta\rangle = \sum_{k=1}^{n} a_k\beta_k = \sum_{k=1}^{n} a_k(\lim_{j\to\infty} r_{i_j}\beta_{i_j})_k = \lim_{j\to\infty}\sum_{k=1}^{n} a_k(r_{i_j}\beta_{i_j})_k =$$

$$= \lim_{j\to\infty}\langle a, r_{i_j}\beta_{i_j}\rangle \overset{(1.1)}{=} 0,$$

kde sčítací index k vždy značil k-tou souřadnici daného prvku. Podle definice kužele C mají všechny nenulové prvky $\overline{C}$ vyhovovat podmínce $\langle a, x\rangle > 0$, nicméně prvek β je nenulový (neboť $||\beta||_2 = 1$), leží v $\overline{C}$, ale $\langle a, \beta\rangle = 0$ a to je spor. Proto je množina $C \cap U_t$ omezená a tvrzení je dokázané. □

1.1.2 Základní algebraické pojmy

Začneme připomenutím algebraických pojmů pologrupy, monoidu, jejich podstruktur a generátorů. *Pologrupou* rozumíme dvojici $(S, +)$, kde $+$ je asociativní binární operace na neprázdné množině S. Pokud navíc množina S obsahuje neutrální prvek 0 k operaci $+$, potom trojice $(S, +, 0)$ je *monoid*. Od teď budeme volně zaměňovat pojem algebraické struktury monoidu $(S, +, 0)$ a jeho nosné množiny S. Libovolná podmnožina monoidu S, která je uzavřená na operaci $+$ a obsahuje 0, tvoří *podmonoid* monoidu S. Pro každou podmnožinu M množiny S můžeme dále uvažovat monoid *generovaný* množinou M, což je monoid na množině

$$\left\{\sum_{i=1}^{t} k_i m_i \mid k_1, k_2, \ldots, k_t \in \mathbb{N}_0, m_1, m_2, \ldots, m_t \in M \text{ a } t \in \mathbb{N}\right\},$$

a budeme pro tento monoid používat značení $\langle M\rangle$.

Máme-li 2 monoidy $(M, +_M, 0_M)$ a $(N, +_N, 0_N)$, tak *homomorfismem* monoidů M a N rozumíme zobrazení $\varphi : M \to N$ takové, že pro všechna $m_1, m_2 \in M$ platí, že

$$\varphi(m_1 +_M m_2) = \varphi(m_1) +_N \varphi(m_2), \varphi(0_M) = 0_N.$$

Monoidy M a N jsou *izomorfní*, pokud mezi nimi existuje *izomorfismus*, neboli bijektivní homomorfismus. Izomorfní monoidy M a N budeme značit $M \simeq N$.

Podrobnější zavedení těchto pojmů lze nalézt v knize [1], která pojednává o univerzální algebře.

V tuto chvíli si již můžeme zadefinovat klíčový pojem celé této práce, pojem polomřížky:

Definice 1.8. *Nechť L je podmonoid monoidu $\mathbb{R}^n$ (s operací standardního sčítání po složkách). Řekneme, že L je* polomřížka*, je-li L diskrétní množina, která obsahuje alespoň jeden nenulový prvek, a zároveň existuje kužel $C \subseteq \mathbb{R}^n$ takový, že $L \subseteq C$.*

Je-li L polomřížka, pak L je jistě nekonečná a neomezená množina, neboť obsahuje všechny násobky nějakého svého nenulového prvku. Zároveň je L spočetná množina, což plyne z důsledku 1.4.

Ve třetí kapitole této práce potkáme případ dvou monoidů, které budou izomorfní, ale pouze jeden z těchto monoidů bude tvořit polomřížku. To nastane kvůli tomu, že izomorfismus nemusí zachovávat, zda-li nosná množina příslušného monoidu je diskrétní. Ve třetí kapitole také nalezneme příklad 2 polomřížek, které budou sice izomorfní, ale jednotlivě budou tvořit polomřížku v jiné dimenzi.

1.2 Polomřížky v jedné dimenzi

V této sekci budeme uvažovat standardní uspořádání $\leq$ na $\mathbb{R}$ a ukážeme si ekvivalentní charakterizaci polomřížek v jedné dimenzi pomocí existence bijekce s $\mathbb{N}_0$ zachovávající standardní uspořádání.

Polomřížkám v jedné dimenzi je rovněž věnován článek [14], kde je pro tyto polomřížky používáno pojmenovaní „liken“, vycházející z anglického „like$\mathbb{N}$“, neboť tyto objekty svou aditivní a multiplikativní strukturou připomínají přirozená čísla. V tomto článku jsou rovněž dokázány různé, především analytické a topologické vlastnosti těchto polomřížek, přičemž některým z těchto vlastností se budeme věnovat později v této kapitole, kde tyto vlastnosti zobecníme pro polomřížky v libovolné dimenzi.

Definice 1.9. *Nechť $M \subseteq \mathbb{R}$ je neprázdná množina. Řekneme, že M je* dobře uspořádaná*, pokud každá neprázdná podmnožina M obsahuje nejmenší prvek.*

Jelikož je standardní uspořádání $\leq$ na $\mathbb{R}$ úplné uspořádání, tak pojem nejmenšího prvku nějaké podmnožiny $\mathbb{R}$ splývá s pojmem minimálního prvku, čehož využijeme při důkazu následujícího lemmatu, které poté využijeme k charakterizaci polomřížek v jedné dimenzi. Dále si snadno uvědomíme, že jediné dva otevřené poloprostory v $\mathbb{R}$ jsou množiny kladných a záporných čísel a jediné kužele v $\mathbb{R}$ jsou právě tyto otevřené poloprostory a jejich topologické uzávěry, což jsou množiny nezáporných a nekladných reálných čísel. Ze symetrie se nám stačí omezit na otevřený poloprostor $\mathbb{R}^+$ a kužel $\mathbb{R}_0^+$, a právě pro tuto situaci zformulujeme následující pomocné lemma a poté i slíbené tvrzení, které charakterizuje polomřížky v jedné dimenzi.

Lemma 1.10. *Nechť $L \subseteq \mathbb{R}_0^+$ je diskrétní množina. Pak L je dobře uspořádaná.*

Důkaz. Tvrzení ukážeme sporem. Nechť L není dobře uspořádaná množina, tedy existuje neprázdná množina $M \subseteq L$ taková, že M neobsahuje nejmenší prvek. Zvolme $y_1 \in M$ libovolně. Potom y_1 není nejmenší (ani minimální) prvek množiny M, a proto existuje $y_2 \in M$ tak, že $y_2 < y_1$. Obdobně, y_2 není nejmenší (ani minimální) prvek množiny M, a proto existuje $y_3 \in M$ tak, že $y_3 < y_2$. Opakováním tohoto postupu dostaneme nekonečnou klesající posloupnost $(y_i)_{i=1}^{\infty}$ prvků z M. Tato posloupnost má limitu, kterou bude nějaké reálné číslo (neboť všechny prvky množiny L jsou nezáporné). Tato limita však poté bude hromadným bodem množiny M, tedy i množiny L, což je spor. Tím je lemma dokázané. □

Tvrzení 1.11. *Nechť $L \subseteq \mathbb{R}_0^+$ je monoid. Následující podmínky jsou ekvivalentní:*

a) Existuje bijekce $\varphi : \mathbb{N}_0 \to L$, pro kterou platí, že $\varphi(0) = 0$ a posloupnost $(\varphi(i))_{i=0}^{\infty}$ je rostoucí.

b) L je polomřížka (k čemuž tedy stačí ověřit, že L je diskrétní množina).

Důkaz. *a)* $\Rightarrow$ *b)*: Nechť existuje bijekce φ s příslušnými vlastnostmi a zvolme libovolné $x \in \mathbb{R}$. Díky struktuře kuželů v jedné dimenzi, kterou jsme zmínili v odstavci před lemmatem 1.10, nám stačí ukázat, že množina L je diskrétní, tedy že x není hromadným bodem množiny L, čili chceme ukázat existenci otevřené koule U_x kolem bodu x tak, aby $U_x \cap L \subseteq \{x\}$. To se nám podaří díky vlastnostem zobrazení φ: Snadno nahlédneme, že existuje právě jeden index $i \in \mathbb{N}$ tak, že můžeme zvolit

$$U_x \subseteq \begin{cases} (\varphi(i-1), \varphi(i+1)), & \text{pokud } x \in L \setminus \{0\}, \\ (\varphi(i), \varphi(i+1)), & \text{pokud } x \notin L, \\ (-\infty, \varphi(1)), & \text{pokud } x = 0, \\ (-\infty, 0), & \text{pokud } x < 0. \end{cases}$$

Poté platí, že $U_x \cap L \subseteq \{x\}$, tedy x není hromadným bodem množiny L a první implikace je dokázána.

b) $\Rightarrow$ *a)*: Buď L diskrétní množina. Podle lemmatu 1.10 je L dobře uspořádaná množina. Definujme zobrazení $\varphi : \mathbb{N}_0 \to L$ následujícím způsobem: Nejprve položme $\varphi(0) = 0$ a poté induktivně definujme $\varphi(i)$ jako nejmenší prvek množiny $L \setminus \bigcup_{j=0}^{i-1} \{\varphi(j)\}$. Takto definované zobrazení φ je zřejmě dobře definované, prosté a posloupnost $(\varphi(i))_{i=0}^{\infty}$ je rostoucí. Zároveň je φ surjektivní zobrazení, což lze odvodit z toho, že neexistuje hromadný bod množiny L. Tím je tvrzení dokázané. □

V článku [14] jsou polomřížky zadefinovány jako rostoucí posloupnosti nezáporných reálných čísel (což odpovídá vlastnosti *a*) z minulého tvrzení), které jsou uzavřené na sčítání (což odpovídá předpokladu na algebraickou strukturu monoidu L). Poté se jednoduše v [[14], Proposition 2] ukáže, že množina L opravdu tvoří pologrupu (dokonce tvoří monoid), a že daná posloupnost roste nad všechny meze, má tedy limitu ∞.

Množina nezáporných racionálních čísel $\mathbb{Q}_0^+$ netvoří polomřížku, protože tato množina obsahuje hromadné body.

Opačná implikace k lemmatu 1.10 neplatí: Obecně platí, že každý podmonoid monoidu $\mathbb{R}_0^+$, který je generován nějakou dobře uspořádanou množinou generátorů, je dobře uspořádaný, bez ohledu na to, zda-li množina generátorů obsahovala hromadné body či nikoliv. Uvažme například monoid generovaný prvky $\left\{1 - \frac{1}{n} \mid n \in \mathbb{N}\right\}$. Takovýto monoid je tedy dobře uspořádaný, ale nejedná se o polomřížku, podrobnosti lze nalézt na odkaze [4].

1.3 Polomřížky ve více dimenzích

Nejprve si zadefinujeme uspořádání ve více dimenzích, které záhy využijeme, přičemž zároveň zobecníme některé vlastnosti jednodimenzionálních polomřížek z článku [14]:

Definice 1.12. *Nechť $M \subseteq \mathbb{R}^n$ je množina a buďte α,$\beta \in M$. Řekneme, že α je* totálně větší *než β (nebo β je* totálně menší *než α), pokud existuje $\gamma \in M$ tak, že $\alpha = \beta + \gamma$. Tuto skutečnost značíme $\alpha \succeq_M \beta$.*

Je jednoduché ověřit, že relace $\succeq_M$ je částečné uspořádání na M. Nejedná se však obecně o dobré, ani o úplné uspořádání.

Stěžejním pojmem této práce je pojem nerozložitelného prvku, což jsou přesně minimální prvky vzhledem k uspořádání $\succeq_M$ na množině $M \setminus \{0\}$. Nejčastěji nás bude zajímat případ, kdy množina M tvoří polomřížku, ovšem v následující definici toto požadovat nebudeme.

Definice 1.13. *Buď $M \subseteq \mathbb{R}^n$ množina a $\alpha \in M$. Řekneme, že α je* nerozložitelný prvek *v M, pokud je nenulový a pro všechna $\beta, \gamma \in M$ taková, že $\alpha = \beta + \gamma$ platí, že buď β nebo γ je rovno nule. Množinu nerozložitelných prvků množiny M budeme značit P_M.*

Snadno nahlédneme, že pokud máme 2 monoidy M_1 a M_2, které jsou izomorfní jako monoidy pomocí izomorfismu φ: $M_1 \to M_2$, tak poté platí, že nerozložitelné prvky se izomorfismem zobrazí na nerozložitelné prvky, neboli $\varphi(P_{M_1}) = P_{M_2}$.

Dále se ukazuje, že množina nerozložitelných prvků nějaké polomřížky je vždy neprázdná, a navíc ji i generuje, což si ukážeme ve větě 1.15. K jejímu důkazu budeme potřebovat následující lemma:

Lemma 1.14. *Nechť L je polomřížka, obsažená v kuželi C takovém, že nenulové prvky $\overline{C}$ leží v otevřeném poloprostoru určeném nerovnicí $\langle a, x\rangle > 0$. Potom pro každé $\alpha \in L$ existuje jen konečně mnoho $\beta \in L$ takových, že $\beta \preceq_L \alpha$.*

Důkaz. Důkaz provedeme sporem. Nechť $B := \{\beta \in L \mid \beta \preceq_L \alpha\}$ je nekonečná množina. S pomocí tvrzení 1.3 se dá snadno odvodit, že množina B je nutně neomezená. Nyní budeme postupovat obdobně jako v důkazu tvrzení 1.7, tedy zkonstruujme posloupnost $(\beta_i)_{i\in\mathbb{N}}$ prvků z B následujícím způsobem: Nechť $||\beta_1||_2 > 1$ a dále pro všechna $i \in \mathbb{N}$ zvolme β_{i+1} tak, že $||\beta_{i+1}||_2 > 2\,||\beta_i||_2$. Taková posloupnost β_i jistě existuje, neboť B je neomezená množina, a navíc $||\beta_i||_2 \overset{i\to\infty}{\to} \infty$. Pro všechna $i \in \mathbb{N}$ definujme $t_i := \frac{1}{||\beta_i||_2}$, tedy bude platit, že $t_i \overset{i\to\infty}{\to} 0$ a navíc $t_i < 1$ pro všechna i. Dále bude platit, že pro všechna i platí $t_i\beta_i \in C$, což plyne z definice kužele C. Použitím multiplikativity normy $||\cdot||_2$ navíc dostaneme, že pro všechna i platí $||t_i\beta_i||_2 = 1$, tedy $t_i\beta_i \in S_0(1)$, což je kompaktní množina, tedy z posloupnosti $(t_i\beta_i)_{i\in\mathbb{N}}$ lze vybrat konvergentní podposloupnost, která má limitu v $\overline{C}$, nechť je touto konvergentní podposloupností $(t_{i_j}\beta_{i_j})_{j\in\mathbb{N}}$ a označme limitu této posloupnosti u. Zároveň si povšimneme, že $||u||_2 = 1$.

Teď využijeme toho, že všechny prvky β_{i_j} jsou totálně menší než α, což z definice znamená, že $\alpha - \beta_{i_j} \in L$. Z definice kužele C plyne, že $t_{i_j}\left(\alpha - \beta_{i_j}\right) \in C$. Nyní se podíváme na normu těchto prvků:

$$\left|\left|t_{i_j}\left(\alpha - \beta_{i_j}\right)\right|\right|_2 \leq \left|\left|t_{i_j}\alpha\right|\right|_2 + \left|\left|t_{i_j}\beta_{i_j}\right|\right|_2 \leq ||\alpha||_2 + 1,$$

kde v první nerovnosti jsme použili trojúhelníkovou nerovnost. Tím jsme však ukázali, že všechny prvky $t_{i_j}\left(\alpha - \beta_{i_j}\right)$ leží v $\overline{U_0(||\alpha||_2 + 1)}$, což je kompaktní množina, tedy posloupnost $\left(t_{i_j}\left(\alpha - \beta_{i_j}\right)\right)_{j\in\mathbb{N}}$ má nějaký hromadný bod, tedy

existuje nějaká konvergentní podposloupnost $\left(t_{i_{j_k}}\left(\alpha - \beta_{i_{j_k}}\right)\right)_{k\in\mathbb{N}}$ s limitou $v \in \overline{C}$. Snadno nahlédneme, že $t_{i_{j_k}}\alpha \overset{k\to\infty}{\to} 0$, protože α je konstantní a $t_{i_{j_k}}$ konvergují k 0. Poté však platí:

$$v = \lim_{k\to\infty} t_{i_{j_k}}\left(\alpha - \beta_{i_{j_k}}\right) = \lim_{k\to\infty} -t_{i_{j_k}}\beta_{i_{j_k}} = -u,$$

čili $u, -u \in \overline{C}$. Všechny nenulové prvky $\overline{C}$ však z definice kužele C musí ležet v tom samém otevřeném poloprostoru, tedy musí platit

$$\langle a, u\rangle > 0, \langle a, -u\rangle > 0, \tag{1.2}$$

neboť $||u||_2 = 1$ a tedy $u \neq 0$, nicméně linearita skalárního součinu nám dává $\langle a, u\rangle = -\langle a, -u\rangle$, což je spor s nerovnostmi (1.2) a lemma je dokázané. □

Nyní již můžeme ukázat, že každá polomřížka je generována svými nerozložitelnými prvky. Tato vlastnost je pro jednodimenzionální polomřížky dokázána v článku [14] jako Proposition 7, přičemž v Proposition 6 v tomtéž článku je ukázáno, že množina nerozložitelných prvků jednodimenzionálních polomřížek je neprázdná, což však v našem obecném případě potřeba dokazovat není, neboť to triviálně plyne z toho, že nerozložitelné prvky generují danou polomřížku, což si nyní ukážeme:

Věta 1.15. *Každá polomřížka L je generována množinou svých nerozložitelných prvků, čili $L = \langle P_L\rangle$.*

Důkaz. Zvolme $\alpha \in L$ a ukažme, že α lze napsat jako součet konečně mnoha nerozložitelných prvků. Označme $M(\alpha)$ množinu takových prvků $\beta \in L$, které jsou totálně menší než α, tedy $\beta \preceq_L \alpha$. Podle lemmatu 1.14 je $M(\alpha)$ konečná množina, a navíc zřejmě $0, \alpha \in M(\alpha)$. Samotný důkaz kýženého tvrzení provedeme matematickou indukcí podle $|M(\alpha)|$.

Nejprve si povšimněme, že kdykoliv napíšeme $\alpha = \beta + \gamma$ pro $\beta, \gamma \in L$, tak nutně $\beta, \gamma \in M(\alpha)$, $M(\beta) \subseteq M(\alpha) \supseteq M(\gamma)$ a pokud $\gamma \neq \alpha \neq \beta$, tak dostaneme $|M(\beta)| < |M(\alpha)| > |M(\gamma)|$.

Je-li $|M(\alpha)| = 1$, pak nutně $\alpha = 0$ a to je prázdná lineární kombinace nerozložitelných prvků.

Pro $|M(\alpha)| = 2$ dostaneme, že kdykoliv $\alpha = \beta + \gamma$ pro $\beta, \gamma \in M(\alpha)$, tak nutně $\beta, \gamma \in \{0, \alpha\}$. To implikuje, že α je nerozložitelný prvek, tedy je i součtem nerozložitelných prvků.

Nyní uvažme přirozené číslo $n \geq 3$. Předpokládejme, že tvrzení platí pro $|M(\alpha)| = 1, 2, \ldots, n-1$ a mějme takové $\alpha \in L$, že $|M(\alpha)| = n$. Rozložme $\alpha = \beta + \gamma$ pro $\beta, \gamma \in M(\alpha)$. Zároveň předpokládejme, že α není nerozložitelný prvek (jinak je situace obdobná případu $|M(\alpha)| = 2$), tedy rozklad $\alpha = \beta + \gamma$ lze zvolit tak, že $\beta \neq \alpha \neq \gamma$. Snadno nahlédneme, že $M(\beta) \subsetneq M(\alpha) \supsetneq M(\gamma)$, čili $|M(\beta)| < |M(\alpha)| > |M(\gamma)|$ a dvojitým použitím indukčního předpokladu dostaneme, že β i γ jsou součtem nerozložitelných prvků, ale poté je i α součtem nerozložitelných prvků a věta je dokázána. □

Nyní zaměříme naši pozornost na polomřížky generované nějakou množinou X (jak lze tuto množinu volit, si za chvíli ukážeme v tvrzení 1.16). Ve větě 1.15

jsme si všimli, že pro polomřížku L lze jako množinu X volit množinu jejích nerozložitelných prvků, tedy P_L. Snadno si uvědomíme, že pro každou polomřížku L, generovanou množinou X platí, že její nerozložitelné prvky P_L musí patřit do množiny X, neboli $P_L \subseteq X$. Tato úvaha projde pro každou generující množinu X, proto nerozložitelné prvky tvoří minimální množinu generátorů polomřížky L (čili nejmenší generující množinu co do inkluze), z čehož mimo jiné plyne, že konečně generované polomřížky jsou právě takové polomřížky s konečným počtem nerozložitelných prvků. Ukazuje se, že aby $\langle X \rangle$ (což je nyní monoid generovaný množinou $X \subseteq \mathbb{R}^n$) tvořil polomřížku, stačí o množině X předpokládat, aby byla diskrétní a byla obsažena v takovém kuželi, že nenulové prvky jeho topologického uzávěru leží v nějakém otevřeném poloprostoru. Ten samý kužel i otevřený poloprostor nám zároveň dosvědčí, že opravdu $\langle X \rangle$ je polomřížka, což si ukážeme v následujícím tvrzení:

Tvrzení 1.16. *Nechť $X \subseteq \mathbb{R}^n$ je diskrétní množina, obsažená v nějakém kuželi C takovém, že nenulové prvky $\overline{C}$ leží v otevřeném poloprostoru určeném nerovnicí $\langle a, x \rangle > 0$. Potom $\langle X \rangle$ je polomřížka, jejíž prvky leží v kuželi C.*

Důkaz. Nejprve ukážeme, že monoid $\langle X \rangle$ leží v kuželi C, tedy v tom samém kuželi, ve kterém ležela množina X: Zvolme $\beta \in \langle X \rangle$ libovolně. Poté existuje $k \in \mathbb{N}$, nezáporná celá čísla $t_1, t_2, \ldots, t_k$ a prvky $\alpha_1, \alpha_2, \ldots, \alpha_k \in X$ tak, že $\beta = \sum_{i=1}^{k} t_i \alpha_i$. Jednoduchou úpravou poslední rovnosti dostáváme:

$$\frac{1}{\sum_{i=1}^{k} t_i} \beta = \sum_{i=1}^{k} \frac{t_i}{\sum_{j=1}^{k} t_j} \alpha_i. \tag{1.3}$$

Povšimněme si, že na pravé straně rovnosti (1.3) máme konvexní kombinaci prvků $\alpha_1, \alpha_2, \ldots, \alpha_k$, z čehož plyne, že celý tento výraz leží v C, protože je to konvexní množina. Podle rovnosti (1.3) platí $\dfrac{1}{\sum_{i=1}^{k} t_i} \beta \in C$, poté však z definice kužele dostáváme, že $\beta \in C$, čímž jsme ukázali, že $\langle X \rangle \subseteq C$.

Nyní zbývá ukázat, že $\langle X \rangle$ je monoid na diskrétní množině. K tomu využijeme tvrzení 1.5, dle kterého stačí ověřit, že $\langle X \rangle$ má konečný průnik s každou z krychlí $K(m)$ pro $m \in \mathbb{N}$. Zvolme $m \in \mathbb{N}$. Nechť $\alpha = \sum_i t_i \alpha_i \in \langle X \rangle \cap K(m)$, kde $t_i \in \mathbb{N}$ a $\alpha_i \in X$ a ukážeme, že takových α existuje pouze konečně mnoho tím, že bude pouze konečně mnoho možností na α_i, které generují α, a zároveň omezíme každý z koeficientů t_i. Jelikož $K(m)$ je kompaktní množina, spojitá funkce skalárního součinu $\langle a, \cdot \rangle$ zde nabývá svého maxima, označme toto maximum t, tedy pro všechna $\beta \in K(m)$ platí $\langle a, \beta \rangle \leq t$. Nyní označme

$$U_t := \{x \in \mathbb{R}^n \mid 0 < \langle a, x \rangle \leq t\},$$

podobně jako v tvrzení 1.7. Potom $K(m) \subseteq U_t$ a jelikož $\langle X \rangle \subseteq C$ (což jsme dokázali výše), dostáváme $\langle X \rangle \cap K(m) \subseteq U_t \cap C$, speciálně $\alpha \in U(t) \cap C$. Množina $U(t) \cap C$ je podle tvrzení 1.7 omezená, její uzávěr je tedy kompaktní množina a použitím tvrzení 1.3 dostáváme, že $X \cap U_t \cap C = X \cap U_t$ je konečná množina (zde jsme využili toho, že X je diskrétní), tedy pouze konečně mnoho prvků $\beta \in X$ vyhovuje podmínce $\langle a, \beta \rangle \leq t$. Dále platí:

$$t \overset{\alpha \in U_t}{\geq} \langle a, \alpha \rangle = \langle a, \sum_i t_i \alpha_i \rangle = \sum_i t_i \langle a, \alpha_i \rangle \geq \langle a, \alpha_j \rangle,$$

kde poslední nerovnost platí pro všechna j. To však znamená, že všechna α_i jsou nutně z $X \cap U_t$, což je konečná množina a tedy možných α_i je jen konečně mnoho. Zbývá omezit koeficienty t_i. Pro všechna j platí:

$$\langle a, \alpha \rangle = \sum_i t_i \langle a, \alpha_i \rangle \geq t_j \langle a, \alpha_j \rangle,$$

přičemž po úpravě dostaneme $t_j \leq \dfrac{\langle a, \alpha \rangle}{\langle a, \alpha_j \rangle}$, čímž jsme omezili koeficienty t_i a z toho již plyne, že možných $\alpha \in \langle X \rangle \cap K(m)$ je jen konečně mnoho, jinými slovy je množina $\langle X \rangle \cap K(m)$ konečná a použitím tvrzení 1.5 dostáváme, že $\langle X \rangle$ je diskrétní množina.

Tím jsme ověřili vše potřebné k tomu, aby $\langle X \rangle$ byla polomřížka, tvrzení je tedy dokázané.

□

Jednodimenzionální případ předchozí věty lze nalézt i v článku [14], konkrétně se jedná o Proposition 12 pro konečně generované polomřížky a Proposition 14 pro nekonečně generované polomřížky.

Na závěr této kapitoly si uvedeme tvrzení, které dává do souvislosti lineární nezávislost nějaké generující množiny X polomřížky L ve vektorovém prostoru $\mathbb{R}^n$ nad tělesem $\mathbb{Q}$ a jednoznačnost vyjádření všech prvků polomřížky L pomocí generátorů z množiny X. Tento fakt je rovněž zmíněn v článku [14] jako Proposition 11 pro jednodimenzionální polomřížky, pokud je generující množina X konečná (a navíc se jedná pouze o implikaci $\Rightarrow$) následujícího tvrzení:

Tvrzení 1.17. *Nechť $L \subseteq \mathbb{R}^n$ je polomřížka, která je generována (potenciálně nekonečnou) množinou X. Potom prvky množiny X jsou lineárně nezávislé ve vektorovém prostoru $\mathbb{R}^n$ nad tělesem $\mathbb{Q}$, právě když každý prvek $\beta \in L$ má jednoznačné vyjádření jako lineární kombinaci prvků z X s celočíselnými nezápornými koeficienty.*

Důkaz. Mějme $X = \{\alpha_i \mid i \in I\}$. Pro všechny prvky $\beta \in L$ platí, že

$$\beta = \sum_{i \in I} m_i \alpha_i = \sum_{i \in I} n_i \alpha_i,$$

pro nějaká $m_i, n_i \in \mathbb{N}_0$, právě když $0 = \sum_{i \in I} (m_i - n_i)\alpha_i$. Tyto úpravy si můžeme dovolit díky tomu, že pouze konečně mnoho m_i je nenulových, stejně jako konečně mnoho n_i je nenulových. Nyní již k důkazu samotné ekvivalence, obě implikace dokážeme nepřímo.

$\Rightarrow$: Nechť existuje $\beta \in L$ takové, že nemá jednoznačné vyjádření jako lineární kombinaci prvků z X, tedy $\beta = \sum_{i \in I} m_i \alpha_i = \sum_{i \in I} n_i \alpha_i$ pro nějaká $m_i, n_i \in \mathbb{N}_0$, a zároveň nějaké $m_i - n_i \neq 0$. Pak ovšem $0 = \sum_{i \in I} (m_i - n_i)\alpha_i$ a jelikož alespoň jeden z koeficientů $m_i - n_i$ je nenulový, ukázali jsme tím, že prvky množiny X jsou lineárně závislé a tato implikace je dokázána.

$\Leftarrow$: Nechť jsou prvky množiny X lineárně závislé nad $\mathbb{Q}$, tedy $0 = \sum_{i \in I} t_i \alpha_i$ pro nějaká $t_i \in \mathbb{Q}$ taková, že jen konečně mnoho z nich je nenulových, ale zároveň alespoň jeden z nich je nenulový. Bez újmy na obecnosti můžeme předpokládat, že všechna $t_i \in \mathbb{Z}$, k tomu stačí celou rovnost vyjadřující 0 jako netriviální lineární

kombinaci přenásobit nějakým společným násobkem jmenovatelů racionálních koeficientů (poté bude nadále platit, že alespoň jeden koeficient t_i bude nenulový, a zároveň těchto nenulových koeficientů je konečně mnoho). Pro všechna $i \in I$ definujme $m_i := \max(0, t_i)$ a $n_i := max(0, -t_i)$. Poté bude platit, že $m_i - n_i = t_i$ pro všechna $i \in I$, zároveň všechna $m_i, n_i \in \mathbb{N}_0$ a také bude pouze konečně mnoho m_i nenulových, obdobně bude pouze konečně mnoho n_i nenulových. Označme $\beta := \sum_{i \in I} m_i \alpha_i = \sum_{i \in I} n_i \alpha_i$. Poté prvek $\beta \in L$ má nejednoznačné vyjádření jako lineární kombinaci prvků z X s celočíselnými nezápornými koeficienty, neboť nějaké t_i bylo nenulové, a proto bude pro příslušné i platit, že $m_i \neq n_i$. Tím je důkaz dokončen. □

2. Teorie čísel

2.1 Zavedení řetězových zlomků

V této části si připomeneme základní vlastnosti řetězových zlomků, které byly zpracovány v článku [9]. Následující definice a tvrzení, která nebudou dokazována, jsou převzata právě z tohoto článku.

Definice 2.1. *Buď $k \in \mathbb{N}_0$.* Konečným řetězovým zlomkem délky k *rozumíme číslo tvaru*

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots + \cfrac{1}{a_k}}}},$$

kde $\{a_i\}_{i=0}^{k}$ je posloupnost reálných čísel, přičemž pokud $i > 0$, tak $a_i > 0$. Pro konečný řetězový zlomek budeme nadále používat značení $[a_0, a_1, \ldots, a_k]$.

Tvrzení 2.2 ([9], tvrzení 2)**.** *Nechť $a_0 \in \mathbb{Z}$ a $\{a_i\}_{i=1}^{\infty}$ je posloupnost přirozených čísel. Pak pro každé $n \geq 0$ celé číslo platí, že $[a_0, a_1, \ldots, a_n] = \dfrac{h_{n+1}(a_0, a_1, \ldots, a_n)}{h_n(a_1, a_2, \ldots, a_n)}$, kde $\{h_i\}_{i=-1}^{\infty}$ je posloupnost polynomů definovaných následujícím rekurentním způsobem:*

$$\begin{aligned} h_{-1} &= 0, \\ h_0 &= 1, \\ \text{pro } i \geq 1, h_i(x_1, \ldots, x_i) &= x_i h_{i-1}(x_1, \ldots, x_{i-1}) + h_{i-2}(x_1, \ldots, x_{i-2}). \end{aligned}$$

Definice 2.3. *Polynom h_i z předchozího tvrzení nazveme i-tým* řetězovým polynomem.

Definice 2.4. *Ať $a_0 \in \mathbb{Z}$ a $\{a_i\}_{i=1}^{\infty}$ je posloupnost přirozených čísel. Položme $p_n := k_{n+1}(a_0, a_1, \ldots, a_n)$, $q_n := k_n(a_1, a_2, \ldots, a_n)$, tedy platí:*

$$\begin{aligned} p_{-1} &= 1, & q_{-1} &= 0, \\ p_0 &= a_0, & q_0 &= 1, \\ p_n &= a_n p_{n-1} + p_{n-2}, & q_n &= a_n q_{n-1} + q_{n-2}. \end{aligned}$$

Pro $n, j \in \mathbb{Z}$ taková, že $n \geq -1$ a $0 \leq j \leq a_{n+2}$, definujme dále

$$p_{n,j} = p_n + j p_{n+1} = k_{n+3}(a_0, a_1, \ldots, a_{n+1}, j),$$

a obdobně

$$q_{n,j} = q_n + j q_{n+1} = k_{n+2}(a_1, \ldots, a_{n+1}, j).$$

Pokud je $a_0 \in \mathbb{N}$, tak jsou posloupnosti $\{p_i\}_{i=-1}^{\infty}$ a $\{q_i\}_{i=-1}^{\infty}$ rostoucí, navíc platí

$$p_n = p_{n,0} < p_{n,1} < \cdots < p_{n,a_{n+2}} = p_{n+2}, \tag{2.1}$$

$$q_n = q_{n,0} < q_{n,1} < \cdots < q_{n,a_{n+2}} = q_{n+2}, \tag{2.2}$$

a dále platí následující rovnosti (pro libovolné $a_0 \in \mathbb{Z}$, $n \in \mathbb{N}_0$, $0 < j < a_{n+2}$):

$$[a_0, a_1, \ldots, a_n] = \frac{k_{n+1}(a_0, a_1, \ldots, a_n)}{k_n(a_1, a_2, \ldots, a_n)} = \frac{p_n}{q_n}, \tag{2.3}$$

$$[a_0, a_1, \ldots, a_{n+1}, j] = \frac{p_{n,j}}{q_{n,j}}, \tag{2.4}$$

přičemž rovnost (2.4) platí i pro $n = -1$. Nepovolujeme případ $j = 0$, aby příslušný řetězový zlomek dával smysl, případně bychom mohli dodefinovat

$$[a_0, a_1, \ldots, a_{n+1}, 0] = \frac{p_n}{q_n},$$

poté by rovnost (2.4) platila i pro $j = 0$.

Nyní zformulujeme další tvrzení o řetězových zlomcích z článku [9], které budeme v této práci potřebovat.

Tvrzení 2.5 ([9], tvrzení 6, [10], Theorem 24)**.** *Pro $k \in \mathbb{N}_0$ platí*

$$p_{k-1}q_k - p_k q_{k-1} = (-1)^k.$$

Důsledek 2.6 ([9], důsledek 7)**.** *Pokud $k \in \mathbb{N}_0$, pak (p_k, q_k), (p_k, p_{k-1}), (q_k, q_{k-1}) jsou dvojice nesoudělných čísel.*

Věta 2.7 ([9], věta 8)**.** *Buď α reálné číslo. Definujme*
$\alpha_0 := \alpha$, $a_0 := \lfloor \alpha_0 \rfloor$. Pokud $i \in \mathbb{N}$ a $a_{i-1} \neq \alpha_{i-1}$, pak rekurentně definujeme

$$\alpha_i := \frac{1}{\alpha_{i-1} - a_{i-1}}, a_i := \lfloor \alpha_i \rfloor. \tag{2.5}$$

Pak nastává jedna ze dvou možností:

- *Existuje $k \in \mathbb{N}_0$ takové, že $\alpha_k = a_k$. Pak α je racionální a platí*

$$\alpha = [a_0, a_1, \ldots, a_k].$$

- *Pro každé $k \in \mathbb{N}_0$, $a_k \neq \alpha_k$. Pak α je iracionální, existuje limita posloupnosti $\lim_{n\to\infty}[a_0, a_1, \ldots, a_n]$ a tato limita je rovna právě číslu α. Budeme též psát $\alpha = [a_0, a_1, a_2, \ldots]$. V tomto případě navíc pro každé $m \in \mathbb{N}_0$ platí*

$$[a_0, a_1, \ldots, a_{2m}] < \alpha < [a_0, a_1, \ldots, a_{2m+1}].$$

Všimněme si, že v předchozí větě platí $a_1, a_2, \ldots \in \mathbb{N}$.

Definice 2.8. *Řetězový zlomek $[a_0, a_1, \ldots]$ z předchozí věty 2.7 se nazývá* řetězovým zlomkem čísla α*, nebo* rozvojem čísla α do řetězového zlomku.

Rozvoj každého iracionálního čísla α do řetězového zlomku je určen jednoznačně. Konečné řetězové zlomky naopak jednoznačně určené nejsou, platí totiž:

$$[a_0, a_1, \ldots, a_n] = [a_0, a_1, \ldots, a_n - 1, 1], \text{pokud } a_n \neq 1. \tag{2.6}$$

Tato nejednoznačnost konečných řetězových zlomků pro nás z technických důvodů může být problematická, konkrétně nám ovlivní to, zda-li racionální čísla budou horním či dolním polokonvergentem sebe sama, přičemž tyto pojmy budou zadefinovány v definici 2.10. Tento předpoklad bude v potřebných místech vysloveně připomenut.

Tvrzení 2.9 ([9], tvrzení 11)**.** *Nechť* $\alpha = [a_0, a_1, \ldots, a_k, \beta]$*, kde* $\alpha > 0, \beta > 1$*. Pak*

$$\alpha = \frac{\beta p_k + p_{k-1}}{\beta q_k + q_{k-1}}. \tag{2.7}$$

2.2 Polokonvergenty

2.2.1 Definice polokonvergentů a jejich počet

V této části této sekce si zadefinujeme konvergenty a polokonvergenty reálných čísel pomocí jejich řetězových zlomků, a poté v lemmatu 2.11 určíme jejich počet, zkoumáme-li polokonvergenty racionálních čísel.

Definice 2.10. *Nechť* α *je reálné číslo a* $[a_0, a_1, a_2, \ldots]$ *je jeho řetězový zlomek. Poté zlomek* $\frac{p_n}{q_n}$ *z definice 2.4 nazveme* n-tým konvergentem *(též* n-tým sblíženým zlomkem*) čísla* $[a_0, a_1, \ldots]$.

Zlomek $\frac{p_{n,j}}{q_{n,j}}$*, kde* $n, j \in \mathbb{Z}$*,* $n \geq -1$*, nazveme* polokonvergentem *čísla* α*, pokud nastane jeden z následujících případů:*

- $n \neq -1$*,* $n \leq k-2$ *pro případ* $\alpha = [a_0, a_1, \ldots, a_k] \in \mathbb{Q}$ *a* $0 \leq j < a_{n+2}$*,*
- $n = -1$*,* $n \leq k-2$ *pro případ* $\alpha = [a_0, a_1, \ldots, a_k] \in \mathbb{Q}$ *a* $0 < j < a_{n+2}$*,*
- $n \neq -1$*,* $\alpha = [a_0, a_1, \ldots, a_k] \in \mathbb{Q}$*,* $k-1 \leq n \leq k$*,* $j = 0$*.*

Polokonvergent $\frac{p_{n,j}}{q_{n,j}}$ *nazveme* horním*, pokud je* n *liché, podobně nazveme polokonvergent* $\frac{p_{n,j}}{q_{n,j}}$ dolním*, pokud je* n *sudé. Pokud* $\alpha \in \mathbb{Q}$*, tak posuzujeme samotné číslo* α *jako* horní i dolní *polokonvergent sebe sama.*

Okamžitě vidíme, že právě iracionální čísla mají nekonečně mnoho polokonvergentů (dokonce i nekonečně mnoho konvergentů). Racionální čísla mají tedy konečně mnoho polokonvergentů a jejich počet přesně určíme v lemmatu 2.11.

Díky rovnostem $p_{n,0} = p_n$ a $q_{n,0} = q_n$ ze vztahů (2.1) a (2.2) dostáváme, že každý konvergent je zároveň polokonvergent (toho samého čísla), konkrétně těmto konvergentům přesně odpovídá případ $j = 0$ z předchozí definice.

V definici 2.10 nepovolujeme za podmínky $n = -1$ případ $j = 0$, protože $\frac{p_{n,0}}{q_{n,0}}$ pro $n = -1$ není dobře definovaný výraz (neboť $q_{n,0} = 0$), proto se nejedná o polokonvergent čísla α. V definici 2.10 nepovolujeme případ $j = a_{n+2}$, neboť tento případ nám nevytvoří žádné nové polokonvergenty, protože podle rovností (2.1) a (2.2) platí $\frac{p_{n,a_{n+2}}}{q_{n,a_{n+2}}} = \frac{p_{n+2}}{q_{n+2}}$ a tyto zlomky tedy dostaneme jako polokonvergenty čísla α pro $j = 0$, dokonce se jedná o konvergenty čísla α.

Kvůli rovnosti (2.6) není na první pohled jasná jednoznačnost polokonvergentů racionálních čísel, neboť jejich řetězové zlomky nejsou kvůli zmíněné rovnosti jednoznačně určeny. Ve skutečnosti tato nejednoznačnost řetězového zlomku nám změní pouze to, zda-li je samotné zkoumané racionální číslo horním či dolním

polokonvergentem sebe sama, tento problém jsme však vyřešili tím, že jsme explicitně v definici 2.10 uvedli, že racionální čísla jsou horním i dolním polokonvergentem sebe sama. Později v práci budeme dokazovat různé charakterizace horních i dolních polokonvergentů čísla α (konkrétně půjde o věty 2.17, 3.5 a jejich důsledky), přičemž důkazy příslušných vlastností polokonvergentu α čísla α budou platit bez ohledu na paritu k, což dává smysl tomu, proč jsou racionální čísla dolním i horním polokonvergentem sebe sama. Přesto musíme být kvůli této nejednoznačnosti konečných řetězových zlomků opatrní, obzvláště při důkazu následujícího lemmatu 2.11, kde budeme určovat počty horních a dolních polokonvergentů racionálního čísla α.

Lemma 2.11. *Nechť* $\alpha = [a_0, a_1, \ldots, a_k] = \dfrac{p_k}{q_k} \in \mathbb{Q}$. *Je-li* k *liché, poté existuje právě* $a_1 + a_3 + \ldots + a_k$ *horních polokonvergentů a* $1 + a_2 + \ldots + a_{k-1}$ *dolních polokonvergentů čísla* α. *Naopak, je-li* k *sudé, poté existuje právě* $a_1 + a_3 + \ldots + a_{k-1}$ *horních polokonvergentů a* $1 + a_2 + \ldots + a_k$ *dolních polokonvergentů čísla* α.

Důkaz. Ověříme počet horních a dolních polokonvergentů čísla α nejprve pro k liché, pro k sudé bude postup zcela analogický a nebudeme jej provádět. Nechť je tedy k liché. Přímo z definice horních polokonvergentů dostáváme, že horní polokonvergenty čísla α jsou právě zlomky tvaru $\dfrac{p_{n,j}}{q_{n,j}}$ dle definice 2.10 pro n liché, $-1 \leq n \leq k$ a $0 \leq j < a_{n+2}$, pro $n = -1$ navíc $j \neq 0$, naopak pro případ $n = k$ povolujeme pouze případ $j = 0$. Snadno nahlédneme, že všechny přípustné hodnoty parametru n jsou $-1, 1, \ldots, k$, přičemž pro $n = -1$ nepovolujeme případ $j \neq 0$ a pro $n = k$ naopak nutně platí $j = 0$. To znamená, že případ $n = -1$ nám dává $a_1 - 1$ horních polokonvergentů, případ $n = 1$ dává a_3 horních polokonvergentů … až nakonec případ $n = k - 2$ nám dá a_k horních polokonvergentů a případ $n = k$ jen jeden horní polokonvergent čísla α, a to číslo α sebe sama. Proto máme celkově $(a_1 - 1) + a_3 + a_5 + \ldots + a_k + 1$ horních polokonvergentů čísla α, což jsme chtěli ukázat.

Pro určení počtu dolních polokonvergentů čísla α, je-li k liché, bude postup velmi podobný: Dolní polokonvergenty čísla α jsou právě zlomky tvaru $\dfrac{p_{n,j}}{q_{n,j}}$ dle definice 2.10 pro n sudé, $-1 < n < k$ a $0 \leq j < a_{n+2}$, přičemž povolené hodnoty parametru n jsou tedy $n = 0, 2, \ldots, k - 1$, kde pro $n = k - 1$ nutně požadujeme $j = 0$. Vidíme, že případ $n = 0$ nám dává a_2 dolních polokonvergentů, případ $n = 2$ dává a_4 dolních polokonvergentů … až nakonec případ $n = k - 3$ nám dá a_{k-1} dolních polokonvergentů a případ $n = k - 1$ jen jeden polokonvergent čísla α, a to číslo α sebe sama. Proto máme celkově $a_2 + a_4 + \ldots + a_{k-1} + 1$ dolních polokonvergentů čísla α, což jsme chtěli ukázat, tím byl důkaz lemmatu dokončen. □

2.2.2 Fareyho zlomky a jejich vlastnosti

V této části této sekce si ukážeme další vlastnosti polokonvergentů nějakého čísla α, které budeme potřebovat dále v práci. Většina z těchto vlastností je převzata z diplomové práce [10], kde jsou tyto vlastnosti zpracovány. Nyní si zadefinujeme Fareyho dvojici, která nám popisuje, co to znamená, že dva zlomky

jsou „blízko u sebe“, přičemž tuto vlastnost budou mít každé dva sousední konvergenty nějakého čísla α i každé dva sousední horní či dolní polokonvergenty nějakého čísla α, jak si později ukážeme:

Definice 2.12. *Libovolné dva zlomky* $\frac{a}{b}$, $\frac{c}{d}$ *pro* $a, c \in \mathbb{Z}$, $b, d \in \mathbb{N}$ *a dvojice čísel* $(a, b), (c, d)$ *jsou nesoudělné, tvoří* Fareyho dvojici, *pokud* $ad - bc = \pm 1$.

V tvrzení 2.5 jsme si všimli, že každé dva sousední konvergenty nějakého čísla α tvoří Fareyho dvojici. Později, konkrétně v tvrzení 2.15 si ukážeme, že i sousední horní i dolní polokonvergenty nějakého čísla α budou tvořit Fareyho dvojici.

Nyní si vyslovíme a dokážeme dvě pomocná lemmata a jednoduché pozorování, která platí pro zcela obecné zlomky:

Pozorování. Pro libovolná celá čísla a, b, c, d, kde b, d jsou kladná, platí, že $\frac{a}{b} \leq \frac{c}{d}$, právě když $bc \geq ad$, což plyne z toho, že

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

Lemma 2.13 ([10], Lemma 25)**.** *Nechť* $\frac{a}{b} < \frac{c}{d}$ *jsou zlomky, které tvoří Fareyho dvojici. Poté pro zlomek* $\frac{e}{f}$, *kde* $e \in \mathbb{Z}$ *a* $f \in \mathbb{N}$ *jsou nesoudělná čísla, pro který platí, že* $\frac{a}{b} < \frac{e}{f} < \frac{c}{d}$, *musí nutně platit vztahy*

$$e = ka + lc, \tag{2.8}$$

$$f = kb + ld, \tag{2.9}$$

kde k, l *jsou vhodně zvolená přirozená čísla. Speciálně dostáváme, že* $e \geq a + c$ *a obdobně* $f \geq b + d$.

Důkaz. Položme $k := cf - de$ a $l := be - af$. Poté k i l jsou opravdu přirozená čísla, což plyne z nerovností $\frac{a}{b} < \frac{e}{f} < \frac{c}{d}$ a pozorování těsně před tímto lemmatem. Nyní ověříme rovnost (2.8):

$$ka + lc = (cf - de)a + (be - af)c = cfa - dea + bec - afc = e(bc - da) = e,$$

kde poslední rovnost plyne z toho, že zlomky $\frac{a}{b} < \frac{c}{d}$ tvoří Fareyho dvojici. Tím je rovnost (2.8) ověřena, rovnost (2.9) se ověří zcela analogicky. Nakonec si uvědomíme, že nerovnosti $e \geq a + c$, $f \geq b + d$ plynou z rovností (2.8) a (2.9) a z toho, že $k, l \in \mathbb{N}$. Tím je důkaz dokončen. □

Lemma 2.14 ([10], Lemma 26)**.** *Buďte* $a, b, c, d, k \in \mathbb{Z}$ *taková čísla, že výrazy* $ad - bc, b + kd, b + (k + 1)d$ *jsou všechny kladné. Poté platí:*

$$\frac{a + (k + 1)c}{b + (k + 1)d} < \frac{a + kc}{b + kd}. \tag{2.10}$$

Důkaz. Dle pozorování před předchozím lemmatem 2.13 stačí ověřit, že

$$(a + kc)(b + (k + 1)d) > (b + kd)(a + (k + 1)c), \tag{2.11}$$

přičemž po roznásobení dostáváme

$$ab + akd + ad + kcb + k(k + 1)cd > ab + bkc + bc + akd + k(k + 1)cd,$$

což je jistě ekvivalentní s

$$ad > bc.$$

Poslední nerovnost však platí z předpokladu tohoto lemmatu. Proto musí platit nerovnost (2.11), a tedy i nerovnost (2.10) a důkaz lemmatu je dokončen. □

Předchozí lemma 2.14 využijeme při důkazu následujícího tvrzení, které dává do souvislosti Fareyho zlomky, konvergenty a polokonvergenty nějakého čísla α. Tvrzení bude zformulováno pouze pro horní polokonvergenty $\frac{p_{n,j}}{q_{n,j}}$ nějakého čísla α, přičemž bude vynechán specifický případ $n = -1$. Důvod, proč horní polokonvergenty jsou pro nás důležitější, než ty dolní, bude popsán v následující kapitole, konkrétně před větou 3.5. Pro dolní polokonvergenty nějakého čísla α bude podobné tvrzení platit rovněž. Případ $n = -1$ a situace pro dolní polokonvergenty budou podrobněji popsány po důkazu tohoto tvrzení, ve kterém budeme zkoumat vlastnosti horních polokonvergentů nějakého čísla α:

Tvrzení 2.15 ([10], Theorem 27)**.** *Nechť α je algebraické číslo stupně 2 a nechť $[a_0, a_1, \ldots]$ je jeho řetězový zlomek. Uvažujme posloupnosti $\{p_i\}_{i=-1}^{\infty}$ a $\{q_i\}_{i=-1}^{\infty}$ zadefinované pomocí posloupnosti $\{a_i\}_{i=0}^{\infty}$ podle vztahu v definici 2.4 a dle stejné definice uvažujme rovněž výrazy $p_{n,j} = p_n + jp_{n+1}$. Dále, buď $n > 0$ liché a pro přehlednost označme $k := a_{n+2}$. Poté platí následující vztahy:*

$$\frac{p_{n+2}}{q_{n+2}} = \frac{p_{n,k}}{q_{n,k}} < \frac{p_{n,k-1}}{q_{n,k-1}} < \cdots < \frac{p_{n,1}}{q_{n,1}} < \frac{p_{n,0}}{q_{n,0}} = \frac{p_n}{q_n}, \tag{2.12}$$

a navíc pro každé dva sousední zlomky ze vztahů (2.12) *platí, že buď si jsou rovny, nebo tvoří Fareyho dvojici.*

Důkaz. Platnosti rovností $\frac{p_{n+2}}{q_{n+2}} = \frac{p_{n,k}}{q_{n,k}}$ a $\frac{p_{n,0}}{q_{n,0}} = \frac{p_n}{q_n}$ jsme si všimli hned za definicí 2.4. Nyní se zaměříme na ostré nerovnosti ze vztahů (2.12), tedy chceme ukázat, že pro všechna $j = 1, 2, \ldots, k$ platí, že

$$\frac{p_{n,j}}{q_{n,j}} < \frac{p_{n,j-1}}{q_{n,j-1}}. \tag{2.13}$$

Tato nerovnost se dá rozepsat jako

$$\frac{p_n + jp_{n+1}}{q_n + jq_{n+1}} < \frac{p_n + (j-1)p_{n+1}}{q_n + (j-1)q_{n+1}},$$

nicméně tato nerovnost plyne přesně z lemmatu 2.14. Abychom toto lemma mohli použít, tak je potřeba ověřit, že výrazy $q_n + jq_{n+1}$, $q_n + (j-1)q_{n+1}$ a $p_nq_{n+1} - q_np_{n+1}$ jsou kladné. První dva výrazy jsou kladné díky tomu, že j je nezáporné a q_n i q_{n-1} jsou kladné (což vidíme přímo z definice 2.4). Třetí zkoumaný výraz je podle

tvrzení 2.5 roven $(-1)^{n+1}$, což je kladné číslo díky tomu, že n je liché, proto jsou opravdu splněny předpoklady lemmatu 2.14. Tím jsme úspěšně ověřili nerovnost (2.13) pro všechna j od 1 do k, čímž jsme dokončili ověření všech vztahů (2.12). Zbývá ověřit, že sousední horní polokonvergenty čísla α, které si nejsou rovny, tvoří Fareyho dvojici. Z důsledku 2.6 plyne, že všechny zlomky, vystupující ve vztazích (2.12), jsou v základním tvaru a všechny výrazy ve jmenovatelích jsou zřejmě kladné, proto stačí ověřit, že pro všechna j od 1 do k platí

$$p_{n,j-1}q_{n,j} - p_{n,j}q_{n,j-1} = \pm 1. \tag{2.14}$$

Skutečně,

$$p_{n,j-1}q_{n,j} - p_{n,j}q_{n,j-1} = (p_n + (j-1)p_{n+1})(q_n + jq_{n+1}) - (p_n + jp_{n+1})(q_n + (j-1)q_{n+1})$$
$$= p_nq_n + jp_nq_{n+1} + (j-1)p_{n+1}q_n + j(j-1)p_{n+1}q_{n+1} - p_nq_n - (j-1)p_nq_{n+1} -$$
$$- jp_{n+1}q_n - j(j-1)p_{n+1}q_{n+1} = p_nq_{n+1} - p_{n+1}q_n = (-1)^{n+1},$$

kde v poslední rovnosti jsme použili tvrzení 2.5. Tím jsme ověřili, že sousední horní polokonvergenty čísla α, které si nejsou rovny, tvoří Fareyho dvojici, čímž je tvrzení dokázané. □

Co se týká případu předchozího tvrzení 2.15 pro $n = -1$, tak zde je jediným problémem, že výraz $\frac{p_{-1,0}}{q_{-1,0}}$ není dobře definovaný. Všechny vztahy ze (2.12), které tento nedefinovaný výraz neobsahují, platí i v tomto případě a jejich ověření je zcela analogické, jinými slovy, platí nerovnost (2.13) pro všechna j od 2 do k.

Pro dolní polokonvergenty nějakého čísla α platí podobné tvrzení (čili nyní uvažujeme případ, kdy $n \geq 0$ je sudé), jako je tvrzení 2.15, akorát nerovnosti ve vztazích (2.12) platí opačně, neboli

$$\frac{p_{n+2}}{q_{n+2}} = \frac{p_{n,k}}{q_{n,k}} > \frac{p_{n,k-1}}{q_{n,k-1}} > \cdots > \frac{p_{n,1}}{q_{n,1}} > \frac{p_{n,0}}{q_{n,0}} = \frac{p_n}{q_n}. \tag{2.15}$$

Důkaz nerovností v (2.15) by se opět dělal pomocí lemmatu 2.14, akorát je potřeba nejprve obě strany daných nerovností vynásobit -1 a z lemmatu 2.14 odůvodnit platnost nerovnosti

$$\frac{(-p_n) + j(-p_{n+1})}{q_n + jq_{n+1}} < \frac{(-p_n) + (j-1)(-p_{n+1})}{q_n + (j-1)q_{n+1}},$$

kde $j = 1, 2, \ldots, k$. Poslední nerovnost opravdu plyne z lemmatu 2.14, obzvlášť zajímavé je povšimnout si platnosti předpokladu na to, aby výraz $-p_nq_{n+1} - q_n(-p_{n+1}) \overset{2.5}{=} (-1)^n$ byl kladný, což plyne z parity n.

I pro dolní polokonvergenty čísla α platí, že sousední polokonvergenty, které si nejsou rovny, tvoří Fareyho dvojici, tam je důkaz zcela analogický tomu pro horní polokonvergenty, pro které jsme si to ukázali v tvrzení 2.15.

Tvrzení 2.15 nám zároveň vysvětluje, proč jsme polokonvergenty nějakého čísla α pro liché n pojmenovali horní. Připomeňme, že pro všechny konvergenty čísla α pro liché n platí $\frac{p_n}{q_n} \geq \alpha$, jehož řetězový zlomek uvažujeme, což jsme si připomněli ve větě 2.7. Horní polokonvergenty čísla α musí ležet mezi $\frac{p_n}{q_n}$ a $\frac{p_{n+2}}{q_{n+2}}$, proto horní polokonvergenty čísla α jsou opět větší nebo rovny číslu α. Zcela obdobně, dolní polokonvergenty čísla α jsou menší nebo rovny číslu α.

2.2.3 Aproximační vlastnosti polokonvergentů

V této části této sekce již využijeme výsledků získaných v této sekci k tomu, abychom si jednoduchým způsobem charakterizovali horní polokonvergenty nějakého čísla α. Obdobně by se daly charakterizovat i dolní polokonvergenty, což si poté také vysvětlíme. Pro účely následující věty 2.17 si zadefinujeme pojmy dobré horní a dolní aproximace čísla α:

Definice 2.16. *Nechť $\alpha \in \mathbb{R}$ a mějme zlomek $\frac{x}{y}$ pro $x \in \mathbb{Z}$, $y \in \mathbb{N}$ a nesoudělná čísla x, y. Řekneme, že zlomek $\frac{x}{y}$ je* dobrá horní aproximace *čísla α, pokud $\frac{x}{y} \geq \alpha$, a zároveň pro všechny zlomky $\frac{x_1}{y_1}$, kde $x_1, y_1 \in \mathbb{Z}$, $y_1 > 0$, které vyhovují podmínce*

$$\frac{x}{y} \geq \frac{x_1}{y_1} \geq \alpha, \tag{2.16}$$

platí buď $y_1 > y$, nebo platí rovnosti $x = x_1$, $y = y_1$.

Obdobně, zlomek $\frac{x}{y}$ je dobrá dolní aproximace *čísla α, pokud $\frac{x}{y} \leq \alpha$, a zároveň pro všechny zlomky $\frac{x_1}{y_1}$, kde $x_1, y_1 \in \mathbb{Z}$, $y_1 > 0$, které vyhovují podmínce*

$$\frac{x}{y} \leq \frac{x_1}{y_1} \leq \alpha \tag{2.17}$$

platí buď $y_1 > y$, nebo platí rovnosti $x = x_1$, $y = y_1$.

Nyní si ukážeme, že horní polokonvergenty čísla α přesně odpovídají dobrým horním aproximacím čísla α:

Věta 2.17. *Nechť $\frac{x}{y}$ pro x,$y \in \mathbb{Z}$ nesoudělná a $y > 0$ je zlomek a $\alpha \in \mathbb{R}$. Zlomek $\frac{x}{y}$ je horní polokonvergent čísla α, právě když je zlomek $\frac{x}{y}$ dobrou horní aproximací čísla α.*

Důkaz. Nejprve se budeme zabývat případem, kdy $\frac{x}{y} = \alpha \in \mathbb{Q}$, což není příliš těžké. Číslo α je horním polokonvergentem sebe sama, což víme přímo z definice 2.10. Proto pro důkaz zkoumané ekvivalence stačí ověřit platnost výroku na pravé straně ekvivalence, tedy že pro všechny zlomky $\frac{x_1}{y_1}$, kde $x_1, y_1 \in \mathbb{Z}$, $y_1 > 0$, které vyhovují podmínce (2.16) platí, že buď $y_1 > y$, nebo platí rovnosti $x = x_1$, $y = y_1$. V tomto případě nutně platí rovnosti mezi všemi třemi příslušnými výrazy, což znamená, že existuje $t \in \mathbb{N}$ tak, že $x_1 = tx$ a $y_1 = ty$, kde jsme využili toho, že čísla x, y jsou nesoudělná. V případě $t = 1$ platí $x = x_1$ a $y = y_1$ a pro $t > 1$ dostáváme $y_1 > y$, neboli číslo α opravdu je dobrou horní aproximací sebe sama, což jsme přesně chtěli ukázat, čímž je speciální případ $\frac{x}{y} = \alpha \in \mathbb{Q}$ vyřešen. Po zbytek důkazu tedy již budeme předpokládat, že $\frac{x}{y} \neq \alpha$:

$\Rightarrow$: Předpokládejme tedy, že $\frac{x}{y} \neq \alpha$ je horní polokonvergent čísla α. Nerovnost $\frac{x}{y} > \alpha$ byla vysvětlena krátce před touto větou (nerovnost plyne z tvrzení 2.15 a z toho, že horní konvergenty čísla α jsou větší nebo rovny číslu α). Nyní uvažujme zlomek $\frac{x_1}{y_1}$, kde $x_1 \in \mathbb{Z}$, $y_1 \in \mathbb{N}$, vyhovující podmínce (2.16) a odlišme dva případy:

1. případ: $\frac{x_1}{y_1}$ je horní polokonvergent čísla α. Potom ze vztahu $\frac{x}{y} \geq \frac{x_1}{y_1}$, vztahů (2.2) a vztahů (2.12) v rámci tvrzení 2.15 plyne, že $y_1 \geq y$ a pro případ rovnosti nastává i rovnost $\frac{x}{y} = \frac{x_1}{y_1}$, čili platí i $x_1 = x$, díky čemuž je v tomto případě zlomek $\frac{x}{y}$ dobrou horní aproximací čísla α a tato implikace je v tomto případě dokázána.

2. případ: $\frac{x_1}{y_1}$ není horní polokonvergent čísla α. Poté díky podmínce (2.16) a tvrzení 2.15 existují dva horní polokonvergenty $\frac{p_{n,i}}{q_{n,i}}$ a $\frac{p_{m,j}}{q_{m,j}}$ čísla α, které vyhovují podmínce

$$\frac{x}{y} \geq \frac{p_{n,i}}{q_{n,i}} > \frac{x_1}{y_1} > \frac{p_{m,j}}{q_{m,j}} \geq \alpha,$$

a zároveň tvoří Fareyho dvojici podle tvrzení 2.15. Podobně jako v prvním případě, ze vztahů (2.2) a vztahů (2.12) v rámci tvrzení 2.15 plyne, že nutně $q_{n,i} \geq y$. Zároveň můžeme použít lemma 2.13 na zlomek $\frac{x_1}{y_1}$, který je vložen mezi dva horní polokonvergenty čísla α, které tvoří Fareyho dvojici, což jsme si dokázali v tvrzení 2.15. Z lemmatu 2.13 plyne, že nutně $y_1 > q_{n,i}$. Celkově dostáváme, že $y_1 > y$, čili opravdu je v tomto případě zlomek $\frac{x}{y}$ dobrou horní aproximací čísla α a tato implikace je dokázána.

$\Leftarrow$: Nyní předpokládejme, že $\frac{x}{y}$ je dobrou horní aproximací čísla α, neboli $\frac{x}{y} \geq \alpha$, a zároveň pro všechny zlomky $\frac{x_1}{y_1}$, kde $x_1, y_1 \in \mathbb{Z}$, vyhovující podmínce (2.16) platí, že buď $y_1 > y$, nebo platí rovnosti $x = x_1, y = y_1$. Předpokládejme pro spor, že $\frac{x}{y}$ není horní polokonvergent čísla α. Nejprve si uvědomíme, že $\frac{x}{y} < \lceil \alpha \rceil$: V opačném případě by totiž volba $x_1 = \lceil \alpha \rceil$, $y_1 = 1$ vyhovovala podmínce (2.16), ale zároveň jistě neplatí $y_1 > y$ a platnost rovností $x = x_1 = \lceil \alpha \rceil$, $y = y_1 = 1$ by znamenala, že $\frac{x}{y}$ je horní polokonvergent čísla α $\left(\frac{x}{y} = [a_0, 1] \text{ nebo } \frac{x}{y} = \alpha\right)$, my však předpokládáme, že tento zlomek není horní polokonvergent čísla α. Proto nutně platí $\frac{x}{y} < \lceil \alpha \rceil$. Dále postupujme obdobně jako v předchozí implikaci ve 2. případě: Jelikož $\frac{x}{y}$ není horní polokonvergent čísla α, musí existovat dva sousední horní polokonvergenty čísla α $\frac{p_{n,i}}{q_{n,i}}$ a $\frac{p_{m,j}}{q_{m,j}}$, které tvoří Fareyho dvojici podle tvrzení

2.15, mezi kterými zlomek $\frac{x}{y}$ leží, konkrétně

$$\frac{p_{n,i}}{q_{n,i}} > \frac{x}{y} > \frac{p_{m,j}}{q_{m,j}} \geq \alpha.$$

Existence takových polokonvergentů je zajištěna mimo jiné tím, že $\frac{x}{y} \neq \lceil \alpha \rceil$, neboť oba hledané polokonvergenty jsou jistě menší nebo rovny hodnotě $\lceil \alpha \rceil$. Nyní použijeme lemma 2.13, dle kterého platí $q_{m,j} < y$. Zároveň však volba $x_1 = p_{m,j}$, $y_1 = q_{m,j}$ vyhovuje podmínce (2.16), ve které je první nerovnost mezi zlomky ostrá, proto z podmínky (2.16) plyne, že $q_{m,j} > y$, což je však spor, protože jsme před chvílí z lemmatu 2.13 odvodili opačnou nerovnost.

Tím jsme ukázali, že $\frac{x}{y}$ je horní polokonvergent čísla α, čímž je důkaz této implikace, a tím pádem i celé věty, dokončen. □

Věta 2.17 má následující důsledek:

Důsledek 2.18. *Je-li $\frac{x}{y}$ horní polokonvergent čísla α, poté $x = \lceil \alpha y \rceil$.*

Důkaz. Pro případ $\frac{x}{y} = \alpha \in \mathbb{Q}$ platí $x = \alpha y = \lceil \alpha y \rceil$. Nyní se tedy stačí zabývat případem $x \neq \alpha y$ a důkaz bude proveden nepřímo, nechť tedy $x \neq \lceil \alpha y \rceil$. Odlišíme 2 případy:

Nejprve předpokládejme, že $x < \lceil \alpha y \rceil$. Potom $x \leq \lfloor \alpha y \rfloor \leq \alpha y$ a alespoň jedna z těchto nerovností bude vždy ostrá (druhá nerovnost bude ostrá, právě když αy není celé číslo, v případě $\alpha y \in \mathbb{Z}$ bude naopak první nerovnost ostrá). Celkově dostáváme, že $x < \alpha y$, proto $\frac{x}{y} < \alpha$ a dle věty 2.17 není zlomek $\frac{x}{y}$ horní polokonvergent čísla α.

Nyní předpokládejme, že $x > \lceil \alpha y \rceil$. Poté platí

$$\frac{x}{y} > \frac{\lceil \alpha y \rceil}{y} \geq \alpha,$$

což nám přesně říká, že pro zlomek $\frac{\lceil \alpha y \rceil}{y}$ platí podmínka (2.16) z věty 2.17, zároveň však první nerovnost v této podmínce je ostrá, a jmenovatele obou zlomků si jsou rovny, proto opět z věty 2.17 plyne, že $\frac{x}{y}$ není horní polokonvergent čísla α, čímž je důsledek dokázán. □

Analogie věty 2.17 a důsledku 2.18 platí i pro dolní polokonvergenty nějakého čísla α, zlomek $\frac{x}{y}$ je dolní polokonvergent čísla α (nebo $\frac{x}{y} = \alpha \in \mathbb{Q}$), právě když jde o dobrou dolní aproximaci, neboli je zkoumaný zlomek menší nebo roven číslu α, a zároveň pro všechny zlomky $\frac{x_1}{y_1}$, vyhovující podmínce (2.17) platí, že buď $y_1 > y$, nebo platí rovnosti $x = x_1, y = y_1$. Dále pro dobré dolní aproximace $\frac{x}{y}$ čísla α platí, že $x = \lfloor \alpha y \rfloor$. Důkazy těchto tvrzení pro dobré dolní aproximace

čísla α jsou zcela analogické důkazům věty 2.17 a důsledku 2.18, včetně případu $\frac{x}{y} = \alpha \in \mathbb{Q}$.

Důkaz implikace $\Leftarrow$ věty 2.17 v trochu obecnější podobě lze rovněž nalézt v práci [10] jako Theorem 28.

2.3 Řetězové zlomky algebraických čísel stupně 2

V této sekci se budeme věnovat tzv. *algebraickým číslům stupně 2*, což jsou taková iracionální čísla, která jsou kořenem nějakého kvadratického polynomu s celočíselnými koeficienty (nebo můžeme též říci, že algebraická čísla stupně 2 jsou právě kořeny ireducibilních polynomů s celočíselnými koeficienty).

2.3.1 Vlastnosti algebraických čísel stupně 2 a jejich řetězových zlomků

V této části této sekce se podíváme na přesný tvar algebraických čísel stupně 2, jejich důležité vlastnosti a také se ve větách 2.21 a 2.22 podíváme na jejich řetězové zlomky.

Algebraická čísla stupně 2 jsou nutně tvaru

$$\frac{\sqrt{D} + r}{s}, \tag{2.18}$$

kde r,$s \in \mathbb{Q}$, $s \neq 0$ a D je přirozené číslo, které není čtvercem (není druhou mocninou žádného přirozeného čísla). Důležitý pro nás bude následující pojem *konjugátu*, který bude později zobecněn.

Definice 2.19. *Je-li α algebraické číslo stupně 2, které je tvaru jako v* (2.18)*, tak* konjugátem *čísla α rozumíme číslo* $\dfrac{-\sqrt{D} + r}{s}$ *a značíme jej α'.*

Snadno si uvědomíme, že pro všechna α, β algebraická čísla stupně 2 platí následující vztahy: $(\alpha + \beta)' = \alpha' + \beta'$, $(\alpha - \beta)' = \alpha' - \beta'$, $(\alpha\beta)' = \alpha'\beta'$ a pokud $\beta \neq 0$, tak $\left(\dfrac{\alpha}{\beta}\right)' = \dfrac{\alpha'}{\beta'}$. Obdobně snadno se dá ověřit i vlastnost $\alpha'' = \alpha$.

Je-li α algebraické číslo stupně 2, tak α' je rovněž algebraické číslo stupně 2 (a dokonce je kořenem toho samého kvadratického polynomu jako α). Speciální postavení mezi algebraickými čísly stupně 2 mají tzv. *redukované kvadratické iracionality*:

Definice 2.20. *Nechť α je algebraické číslo stupně 2. Číslo α nazveme* redukovanou kvadratickou iracionalitou*, pokud $\alpha > 1$, a zároveň $-1 < \alpha' < 0$.*

Podrobnější zavedení těchto pojmů lze nalézt v sekci 3 v článku [9].

Nyní se zaměříme na řetězové zlomky těchto algebraických čísel stupně 2. Právě algebraická čísla stupně 2 mají periodický řetězový zlomek podle věty 26 v článku [9], přičemž redukované kvadratické iracionality mají výstřední postavení

mezi algebraickými čísly stupně 2 díky tomu, že mají ryze periodický řetězový zlomek. Pojem periodického a ryze periodického řetězového zlomku je zaveden v definici 13 v článku [9].

Věta 2.21. *Algebraické číslo stupně 2 je redukovanou kvadratickou iracionalitou, právě když má ryze periodický řetězový zlomek.*

Důkazu této věty je věnována celá sekce 4 v článku [9], konkrétně je jedna z implikací dokázána ve větě 22 a ta druhá ve větě 25.

S použitím věty 2.21 můžeme relativně snadno odvodit přesný tvar řetězového zlomku významných algebraických čísel stupně 2, konkrétně jde o $\sqrt{D}$ a $\dfrac{\sqrt{D}-1}{2}$, kde $D \neq 1$ je bezčtvercové přirozené číslo (D není dělitelné žádným čtvercem přirozeného čísla, různým od 1), a zároveň $D > 1$. Tento předpoklad, aby D bylo bezčtvercové, budeme uvažovat až do konce této práce, přičemž tento předpoklad bude u znění důležitých tvrzení připomenut.

Jak konkrétně tyto řetězové zlomky vypadají, si připomeneme v následující větě, přičemž část o tvaru řetězového zlomku čísla $\sqrt{D}$ je dokázána ve větě 27 v článku [9], část o tvaru řetězového zlomku čísla $\dfrac{\sqrt{D}-1}{2}$ se ukáže podobně:

Věta 2.22. *Pro všechna bezčtvercová přirozená čísla D, $D \neq 1$ platí, že*

$$\sqrt{D} = [a_0, \overline{a_1, \ldots, a_{k-1}, 2a_0}], \quad \frac{\sqrt{D}-1}{2} = [a_0, \overline{a_1, \ldots, a_{k-1}, 2a_0+1}].$$

Pro oba tyto řetězové zlomky platí, že posloupnosti $(a_1, \ldots, a_{k-1})$ jsou symetrické, tedy $a_i = a_{k-i}$ pro všechna i od 1 do $k-1$.

Zkoumání řetězových zlomků zmíněných v předchozí větě 2.22 je pro tuto práci klíčové, neboť horní polokonvergenty těchto řetězových zlomků budou odpovídat nerozložitelným prvkům v důležitých polomřížkách, kterým se budeme podrobněji věnovat v celé následující kapitole práce. Proto si některé vlastnosti prvků posloupností $\{p_i\}_{i=-1}^{\infty}$, $\{q_i\}_{i=-1}^{\infty}$, $\{a_i\}_{i=0}^{\infty}$ a $\{\alpha_i\}_{i=0}^{\infty}$ odpovídající těmto řetězovým zlomkům odvodíme již nyní a zároveň si představíme značení, které budeme později v práci pro kvantity odvozené z těchto řetězových zlomků používat. Toto značení je shrnuto v následující tabulce 2.1, přičemž momentálně jsou pro nás důležité pouze hodnoty D, δ, α a jeho řetězový zlomek. Později budeme zkoumat pojmy normy $N(\delta)$, stopy $Tr(\delta)$ a diskriminantu Δ_K, které budou zadefinovány v sekci 2.4.

Tabulka 2.1: Důležité značení

D	$D \equiv 1 \bmod 4$	$D \equiv 2, 3 \bmod 4$
α	$\frac{\sqrt{D}-1}{2}$	$\sqrt{D}$
řetězový zlomek α	$[a_0, \overline{a_1, \ldots, a_{k-1}, 2a_0+1}]$	$[a_0, \overline{a_1, \ldots, a_{k-1}, 2a_0}]$
δ	$\frac{\sqrt{D}+1}{2}$	$\sqrt{D}$
$N(\delta)$	$\frac{1-D}{4}$	$-D$
$Tr(\delta)$	1	0
Δ_K	D	$4D$

Připomeňme, že v právě uvedené tabulce 2.1 předpokládáme, že číslo D je bezčtvercové, a proto takové číslo D nemůže být kongruentní 0 modulo 4, neboť poté by toto číslo bylo dělitelné čtvercem různým od 1 (konkrétně 4), proto se stačí zabývat případy $D \equiv 1, 2, 3 \bmod 4$.

Nyní se již podíváme na konkrétní potřebné vlastnosti zkoumaných řetězových zlomků. Začneme následujícím lemmatem, které nám aplikací tvrzení 2.9 na tyto řetězové zlomky, spolu se vztahem pro a_k z tvrzení 2.22 dá důležité identity, které záhy využijeme:

Lemma 2.23. *Pro hodnoty D a $\alpha = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo platí následující rovnost:*

$$p_{k-1} = a_0 q_{k-1} + q_{k-2}. \tag{2.19}$$

Pokud navíc $D \equiv 2, 3 \bmod 4$, tak platí i následující rovnost:

$$D q_{k-1} = a_0 p_{k-1} + p_{k-2}. \tag{2.20}$$

Pokud naopak $D \equiv 1 \bmod 4$, tak navíc platí následující vztah:

$$q_{k-1}\frac{D-1}{4} = p_{k-1}(a_0+1) + p_{k-2}. \tag{2.21}$$

Důkaz. Naším cílem je tedy pro případ $D \equiv 2, 3 \bmod 4$ dokázat vztahy (2.19) a (2.20), pro případ $D \equiv 1 \bmod 4$ chceme dokázat vztahy (2.19) a (2.21). Začneme případem $D \equiv 2, 3 \bmod 4$, kdy využijeme strukturu řetězového zlomku čísla $\sqrt{D}$, kterou známe z věty 2.22. Platí

$$\sqrt{D} = [a_0, \overline{a_1, \ldots, a_{k-1}, 2a_0}] = [a_0, a_1, \ldots, a_{k-1}, a_0 + \sqrt{D}]. \tag{2.22}$$

Nyní použijeme tvrzení 2.9 na řetězový zlomek z rovnosti (2.22) a dostáváme následující rovnost:

$$\sqrt{D} = \frac{(\sqrt{D}+a_0)p_{k-1} + p_{k-2}}{(\sqrt{D}+a_0)q_{k-1} + q_{k-2}}.$$

Celou poslední rovnost vynásobíme výrazem ve jmenovateli na pravé straně rovnosti a upravujme:

$$q_{k-1}\sqrt{D}(\sqrt{D}+a_0)+q_{k-2}\sqrt{D}=(\sqrt{D}+a_0)p_{k-1}+p_{k-2},$$

$$q_{k-1}D+q_{k-1}a_0\sqrt{D}+q_{k-2}\sqrt{D}=p_{k-1}\sqrt{D}+p_{k-1}a_0+p_{k-2}.$$

Nyní porovnáme celočíselné koeficienty a koeficienty u $\sqrt{D}$, čímž dostáváme následující 2 rovnosti:

$$q_{k-1}D=p_{k-1}a_0+p_{k-2}, a_0q_{k-1}+q_{k-2}=p_{k-1}.$$

První získaná rovnost je přesně rovnost (2.20) a druhá získaná rovnost je přesně rovnost (2.19), díky čemuž jsme v případě $D\equiv 2,3 \bmod 4$ hotovi.

Nyní se tedy budeme zabývat případem $D\equiv 1 \bmod 4$, kde budeme postupovat zcela analogicky. Podíváme se na řetězový zlomek čísla $\alpha := \dfrac{\sqrt{D}-1}{2}$, který známe opět z věty 2.22:

$$\alpha=[a_0,\overline{a_1,\ldots,a_{k-1},2a_0+1}]=[a_0,a_1,\ldots,a_{k-1},a_0+1+\alpha]. \tag{2.23}$$

Nyní použijeme tvrzení 2.9 na řetězový zlomek z rovnosti (2.23) a dostáváme následující rovnost:

$$\alpha=\frac{(\alpha+1+a_0)p_{k-1}+p_{k-2}}{(\alpha+1+a_0)q_{k-1}+q_{k-2}}.$$

Celou poslední rovnost vynásobíme výrazem ve jmenovateli na pravé straně rovnosti a upravujme:

$$q_{k-1}\alpha(\alpha+1+a_0)+q_{k-2}\alpha=(\alpha+1+a_0)p_{k-1}+p_{k-2},$$

$$q_{k-1}\alpha^2+q_{k-1}a_0\alpha+q_{k-1}\alpha+q_{k-2}\alpha=p_{k-1}\alpha+p_{k-1}a_0+p_{k-1}+p_{k-2}. \tag{2.24}$$

Do rovnosti (2.24) nyní dosadíme následující vztah pro α^2:

$$\alpha^2=\left(\frac{\sqrt{D}-1}{2}\right)^2=\frac{D-2\sqrt{D}+1}{4}=\frac{D-1-2\sqrt{D}+2}{4}=\frac{D-1}{4}-\alpha,$$

čímž dostáváme následující rovnost:

$$q_{k-1}\left(\frac{D-1}{4}-\alpha\right)+q_{k-1}a_0\alpha+q_{k-1}\alpha+q_{k-2}\alpha=p_{k-1}\alpha+p_{k-1}a_0+p_{k-1}+p_{k-2},$$

po úpravě

$$q_{k-1}\frac{D-1}{4}+q_{k-1}a_0\alpha+q_{k-2}\alpha=p_{k-1}\alpha+p_{k-1}a_0+p_{k-1}+p_{k-2}.$$

Nyní porovnáme celočíselné koeficienty a koeficienty u α, čímž dostáváme následující 2 rovnosti:

$$q_{k-1}\frac{D-1}{4}=p_{k-1}(a_0+1)+p_{k-2}, a_0q_{k-1}+q_{k-2}=p_{k-1}.$$

První získaná rovnost je přesně rovnost (2.21) a druhá získaná rovnost je přesně rovnost (2.19), díky čemuž jsme i v případě $D\equiv 1 \bmod 4$ hotovi a lemma je dokázané. □

2.3.2 Vlastnosti parametrů γ_t a $\gamma_{t,j}$

Nyní si zadefinujeme značení pro jisté kvantity, které závisí pouze na řetězovém zlomku čísla α. Toto značení si nyní nejprve formálně zadefinujeme a poté vyslovíme a dokážeme 2 tvrzení, kde budeme zkoumat právě čerstvě zadefinované hodnoty:

Definice 2.24. *Nechť α a δ jsou čísla z tabulky 2.1 a $[a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ je řetězový zlomek čísla α. Pro všechna t, j celá čísla, kde $t \geq -1$ a $0 \leq j < a_{t+2}$, definujme následující 2 hodnoty:*

$$\gamma_t := p_t + q_t\delta, \tag{2.25}$$

$$\gamma_{t,j} = \gamma_t + j\gamma_{t+1}. \tag{2.26}$$

Tvrzení 2.25. *Pro hodnoty D, δ a $\alpha = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo, a pro každé celé číslo $i \geq -1$ uvažujme parametr γ_i podle rovnosti* (2.25)*. Poté platí*

$$\gamma_i\gamma_{k-1} = \gamma_{i+k}. \tag{2.27}$$

Důkaz. Tvrzení bude dokázáno matematickou indukcí podle i, přičemž nejprve vyřešíme samostatně případy $i = -1$ a $i = 0$, poté bude vyřešen obecný indukční krok pro $i \in \mathbb{N}$ s využitím indukčního předpokladu o platnosti tvrzení pro $i - 1$ a $i - 2$.

Případ $i = -1$ je velmi jednoduchý, neboť dosazením za i do požadované rovnosti (2.27) dostáváme $\gamma_{-1}\gamma_{k-1} = \gamma_{k-1}$, čili nám stačí ukázat vztah $\gamma_{-1} = 1$, který však okamžitě plyne z definice γ_i a toho, že $p_{-1} = 1$ a $q_{-1} = 0$.

Pro případ $i = 0$ nejprve upravíme výraz na levé straně rovnosti (2.27):

$$\gamma_0\gamma_{k-1} = (p_0 + q_0\delta)(p_{k-1} + q_{k-1}\delta) = p_0p_{k-1} + q_0q_{k+1}\delta^2 + (p_0q_{k-1} + q_0p_{k-1})\delta =$$

$$= a_0p_{k-1} + q_{k-1}\delta^2 + (a_0q_{k-1} + p_{k-1})\delta. \tag{2.28}$$

Chceme ukázat, že právě upravený výraz se rovná $\gamma_k = p_k + q_k\delta$. K tomu odlišíme 2 případy podle toho, čemu je kongruentní D modulo 4.

Nejprve předpokládejme, že $D \equiv 2, 3 \bmod 4$. Poté platí podle tabulky 2.1, že $\delta = \alpha = \sqrt{D}$ a proto je v tomto případě naším cílem ukázat platnost následující rovnosti:

$$a_0p_{k-1} + q_{k-1}D + (a_0q_{k-1} + p_{k-1})\sqrt{D} = p_k + q_k\sqrt{D}, \tag{2.29}$$

neboli po porovnání celočíselných koeficientů a koeficientů u $\sqrt{D}$ chceme ukázat následující vztahy:

$$a_0p_{k-1} + q_{k-1}D = p_k, \tag{2.30}$$

$$a_0q_{k-1} + p_{k-1} = q_k. \tag{2.31}$$

Oba tyto vztahy budou platit díky rovnostem (2.19) a (2.20) z lemmatu 2.23. Nejprve ověříme vztah (2.31):

$$q_k = a_kq_{k-1} + q_{k-2} \overset{a_k=2a_0}{=} a_0q_{k-1} + a_0q_{k-1} + q_{k-2} \overset{(2.19)}{=} a_0q_{k-1} + p_{k-1},$$

kde vztah $a_k = 2a_0$ můžeme použít díky větě 2.22. Nyní zbývá ověřit vztah (2.30):

$$p_k = a_kp_{k-1} + p_{k-2} \overset{a_k=2a_0}{=} a_0p_{k-1} + a_0p_{k-1} + p_{k-2} \overset{(2.20)}{=} a_0p_{k-1} + Dq_{k-1},$$

což jsme přesně chtěli ukázat, čímž je případ $i = 0$ rovnosti (2.27) za předpokladu $D \equiv 2, 3 \bmod 4$ vyřešen.

Nyní se tedy zabývejme případem $D \equiv 1 \bmod 4$. Pro levou stranu rovnosti (2.27) platí podle vztahu (2.28) následující rovnost:

$$\gamma_0\gamma_{k-1} = a_0p_{k-1} + q_{k-1}\delta^2 + (a_0q_{k-1} + p_{k-1})\delta.$$

Do tohoto vztahu dosadíme následující identitu, platnou pro δ^2 (zde postupujeme podobně, jako při dosazování za α^2 v důkazu lemmatu 2.23):

$$\delta^2 = \left(\frac{\sqrt{D}+1}{2}\right)^2 = \frac{D+2\sqrt{D}+1}{4} = \frac{D-1+2\sqrt{D}+2}{4} = \frac{D-1}{4} + \delta,$$

čímž dostáváme:

$$\gamma_0\gamma_{k-1} = a_0p_{k-1} + q_{k-1}\left(\frac{D-1}{4} + \delta\right) + (a_0q_{k-1} + p_{k-1})\delta =$$

$$= a_0p_{k-1} + q_{k-1}\frac{D-1}{4} + ((a_0+1)q_{k-1} + p_{k-1})\delta.$$

Tento výraz se má rovnat $p_k + q_k\delta$, což opět ověříme porovnáním celočíselných koeficientů a koeficientů u δ, čili chceme ukázat následující 2 vztahy:

$$a_0p_{k-1} + q_{k-1}\frac{D-1}{4} = p_k, \tag{2.32}$$

$$(a_0+1)q_{k-1} + p_{k-1} = q_k. \tag{2.33}$$

Tyto dva vztahy ověříme pomocí vztahů (2.19), (2.21) a toho, že platí $a_k = 2a_0+1$, což víme z věty 2.22. Začneme vztahem (2.32):

$$p_k = a_kp_{k-1} + p_{k-2} \overset{a_k=2a_0+1}{=} a_0p_{k-1} + (a_0+1)p_{k-1} + p_{k-2} \overset{(2.21)}{=} a_0p_{k-1} + q_{k-1}\frac{D-1}{4},$$

čímž je požadovaný vztah úspěšně ověřen. Nyní ověříme vztah (2.33):

$$q_k = a_kq_{k-1} + q_{k-2} \overset{a_k=2a_0+1}{=} (a_0+1)q_{k-1} + a_0q_{k-1} + q_{k-2} \overset{(2.19)}{=} (a_0+1)q_{k-1} + p_{k-1},$$

což jsme přesně chtěli ukázat, tím je tedy úspěšně ověřen případ $i = 0$ rovnosti (2.27) i pokud $D \equiv 1 \bmod 4$, čímž je celkově vyřešen případ $i = 0$ a můžeme se přesunout k indukčnímu kroku:

Zvolme tedy libovolné $i \in \mathbb{N}$ a předpokládejme, že rovnost (2.27) platí pro $i-1$ a $i-2$. Naším úkolem je ověřit tutéž rovnost i pro i. Snadno si uvědomíme z rekurentní definice p_i a q_i, že platí $\gamma_i = a_i\gamma_{i-1} + \gamma_{i-2}$. Nyní již ověřme rovnost (2.27):

$$\gamma_i\gamma_{k-1} = a_i\gamma_{i-1}\gamma_{k-1} + \gamma_{i-2}\gamma_{k-1} \overset{\text{indukční předpoklad}}{=} a_i\gamma_{i+k-1} + \gamma_{i+k-2} \overset{a_i=a_{i+k}}{=}$$

$$\overset{a_i=a_{i+k}}{=} a_{i+k}\gamma_{i+k-1} + \gamma_{i+k-2} = \gamma_{i+k},$$

kde rovnost $a_i = a_{i+k}$ jsme mohli použít díky periodicitě řetězového zlomku čísla α, které jsme si vědomi díky větě 2.22. Tím jsme úspěšně ověřili rovnost (2.27) pro obecné i, čímž je tvrzení dokázané. □

Obdobný, leč mírně složitější bude i důkaz části následujícího tvrzení, kde místo γ_i v rovnosti (2.27) budeme uvažovat jeho konjugát γ_i', přičemž pro $i \geq k-1$ bude výsledek zkoumané rovnosti o dost jiný a pro nás méně zajímavý, přesto si následující důsledek zformulujeme i dokážeme pro všechna $i \geq -1$:

Tvrzení 2.26. *Pro hodnoty D, δ a $\alpha = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo, a pro každé celé číslo $i \geq -1$ uvažujme parametr γ_i podle rovnosti* (2.25)*. Pokud $i \leq k-1$, tak platí následující vztah:*

$$\gamma_i' \gamma_{k-1} = \gamma_{k-i-2}(-1)^{i+1}. \tag{2.34}$$

Pokud máme $i \geq k-1$, tak platí následující vztah:

$$\gamma_i' \gamma_{k-1} = \gamma_{i-k}'(-1)^k. \tag{2.35}$$

Důkaz. Začneme důkazem rovnosti (2.34), důkaz bude velmi podobný důkazu rovnosti (2.27) z tvrzení 2.25, tento důkaz pro $-1 \leq i \leq k-1$ bude tedy proveden matematickou indukcí podle i, přičemž nejprve ověříme tuto rovnost v případech $i = -1$ a $i = 0$.

Případ $i = -1$ je velice jednoduchý, neboť zde stačí dosadit za i do požadované rovnosti (2.34), neboť jistě platí $\gamma_{-1} = \gamma_{-1}' = 1$. Dostáváme:

$$\gamma_{-1}' \gamma_{k-1} = \gamma_{k-1} = \gamma_{k-(-1)-2}(-1)^{(-1)+1},$$

čímž byla skutečně ověřena rovnost (2.34), proto jsme v případě $i = -1$ hotovi.

Nyní budeme zkoumat případ $i = 0$. Začneme úpravou výrazu na levé straně požadované rovnosti (2.34):

$$\gamma_0' \gamma_{k-1} = (p_0 + q_0\delta')(p_{k-1} + q_{k-1}\delta) = p_0 p_{k-1} + q_0 q_{k+1}\delta\delta' + p_0 q_{k-1}\delta + q_0 p_{k-1}\delta' =$$

$$= a_0 p_{k-1} + q_{k-1}\delta\delta' + a_0 q_{k-1}\delta + p_{k-1}\delta'. \tag{2.36}$$

Tento výraz se má rovnost $-\gamma_{k-2} = -p_{k-2} - q_{k-2}\delta$, což ověříme rozlišením na 2 případy podle toho, čemu je číslo D kongruentní modulo 4, dosazením odpovídající hodnoty za δ a porovnáním racionálních a iracionálních koeficientů na obou stranách požadované rovnosti. Za výraz $\delta\delta'$ budeme dosazovat hodnotu $N(\delta)$ podle tabulky 2.1, neboť tato hodnota přímo z definice 2.28 přesně odpovídá výrazu $\delta\delta'$, i když tato definice bude uvedena až v příští sekci.

Nyní předpokládejme, že $D \equiv 2, 3 \bmod 4$. Potom $\delta = \sqrt{D}$ a $\delta\delta' = -D$. Dosazením do výrazu v (2.36) a po vytknutí $\sqrt{D}$ dostáváme:

$$a_0 p_{k-1} - D q_{k-1} + \sqrt{D}(a_0 q_{k-1} - p_{k-1}).$$

Tento výraz se má rovnat $-p_{k-2} - q_{k-2}\sqrt{D}$, což ověříme porovnáním celočíselných koeficientů a koeficientů u $\sqrt{D}$: Mají tedy platit následující vztahy:

$$a_0 p_{k-1} - D q_{k-1} = -p_{k+2}, \tag{2.37}$$

$$a_0 q_{k-1} - p_{k-1} = -q_{k-2}. \tag{2.38}$$

Oba tyto vztahy jsou ekvivalentní rovnostem (2.19) a (2.20) z lemmatu 2.23, díky čemuž je případ $i = 0$ za podmínky $D \equiv 2, 3 \bmod 4$ dokončen.

Nyní se tedy stačí zabývat případem $D \equiv 1 \bmod 4$, kde platí $\delta = \dfrac{1+\sqrt{D}}{2}$ a $\delta\delta' = \dfrac{1-D}{4}$. Opět začneme dosazením těchto vztahů do (2.36):

$$a_0 p_{k-1} + q_{k-1}\frac{1-D}{4} + a_0 q_{k-1}\frac{1+\sqrt{D}}{2} + p_{k-1}\frac{1-\sqrt{D}}{2} =$$
$$= a_0 p_{k-1} + q_{k-1}\frac{1-D}{4} + \frac{a_0 q_{k-1} + p_{k-1}}{2} + \frac{a_0 q_{k-1} - p_{k-1}}{2}\sqrt{D}.$$

Tento výraz se má rovnat $-p_{k-2} - q_{k-2}\delta = -p_{k-2} - \dfrac{q_{k-2}}{2} - \dfrac{q_{k-2}}{2}\sqrt{D}$. To ověříme porovnáním celočíselných koeficientů a koeficientů u $\dfrac{\sqrt{D}}{2}$ obou zkoumaných vztahů. Pro koeficienty u $\dfrac{\sqrt{D}}{2}$ dostáváme vztah

$$a_0 q_{k-1} - p_{k-1} = -q_{k-2}, \tag{2.39}$$

který snadno plyne z rovnosti (2.19) z lemmatu 2.23. Nyní tedy stačí ověřit rovnost

$$a_0 p_{k-1} + q_{k-1}\frac{1-D}{4} + \frac{a_0 q_{k-1} + p_{k-1}}{2} = -p_{k-2} - \frac{q_{k-2}}{2}. \tag{2.40}$$

Do levé strany této rovnosti dosadíme vztah

$$q_{k-1}\frac{1-D}{4} = -p_{k-1}(a_0+1) - p_{k-2},$$

který plyne z rovnosti (2.21) z lemmatu 2.23. Tím dostáváme:

$$a_0 p_{k-1} - p_{k-1}(a_0+1) - p_{k-2} + \frac{a_0 q_{k-1} + p_{k-1}}{2} = -p_{k-2} + \frac{a_0 q_{k-1} - p_{k-1}}{2} \overset{(2.39)}{=}$$
$$\overset{(2.39)}{=} -p_{k-2} - \frac{q_{k-2}}{2},$$

čímž jsme úspěšně ověřili rovnost (2.40), čímž byla úspěšně ověřena rovnost (2.34) pro případ $i = 0$ i za podmínky $D \equiv 1 \bmod 4$, proto nyní budeme zkoumat indukční krok, podobně jako při důkazu minulého tvrzení 2.25. Při tomto indukčním kroku využijeme jednu vlastnost řetězových zlomků zkoumaného čísla α, kterou jsme doposud nepoužili. Touto vlastností je symetrie periody $(a_1, a_2, \ldots, a_{k-1})$, čili rovnosti $a_j = a_{k-j}$ pro každé j od 1 do $k-1$, přičemž platnost těchto rovností známe z věty 2.22. Nyní již proveďme slíbený indukční krok: Vezměme si pevné $i \in \mathbb{N}$ a předpokládejme, že rovnost (2.34) platí pro $i-1$ a $i-2$. Chceme ověřit platnost této rovnosti i pro i:

$$\gamma_i' \gamma_{k-1} = a_i \gamma_{i-1}' \gamma_{k-1} + \gamma_{i-2}' \gamma_{k-1} \overset{\text{indukční předpoklad}}{=}$$
$$= a_i(-1)^i \gamma_{k-i-1} + (-1)^{i+1}\gamma_{k-i} = (-1)^{i+1}(-a_i\gamma_{k-i-1} + \gamma_{k-i}) =$$
$$= (-1)^{i+1}(-a_i\gamma_{k-i-1} + a_{k-i}\gamma_{k-i-1} + \gamma_{k-i-2}) = (-1)^{i+1}\gamma_{k-i-2},$$

kde v poslední rovnosti jsme využili již zmíněnou symetrii periody řetězového zlomku čísla α. Tím je rovnost (2.34) dokázána pro všechna i od -1 do $k-1$.

Konečně se podíváme i na rovnost (2.35), kterou chceme ověřit pro všechna $i \geq k-1$, přičemž pro $i = k-1$ nic ověřovat nemusíme, neboť tento případ splývá s případem $i = k-1$ právě ověřené rovnosti (2.34). Obecný důkaz rovnosti (2.35) je následující:

$$\gamma'_i\gamma_{k-1} \overset{2.25}{=} (\gamma_{i-k}\gamma_{k-1})'\gamma_{k-1} = \gamma'_{i-k}\gamma'_{k-1}\gamma_{k-1} \overset{(2.34)}{=} \gamma'_{i-k}(-1)^k\gamma_{-1} = \gamma'_{i-k}(-1)^k,$$

čímž jsme úspěšně ověřili rovnost (2.35) a tvrzení je dokázané. □

Zajímavou vlastnost má i jeden z horních polokonvergentů čísla α. Půjde o zlomek $\frac{p_{t,j}}{q_{t,j}}$ pro $t = k-2$ a $j = a_0$, kde parametr k reprezentuje délku periody řetězového zlomku čísla α podle tabulky 2.1. Požadovanou vlastnost dokážeme v následujícím lemmatu:

Lemma 2.27 ([3], Lemma 5)**.** *Pro hodnoty D, δ a $\alpha = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo, a pro všechna celá čísla $i, j \geq -1$, $0 \leq j < a_{i+2}$ uvažujme parametry γ_i a $\gamma_{i,j}$ podle rovností* (2.25) *a* (2.26)*. Poté platí následující rovnost:*

$$\gamma_{k-2,a_0} = -\gamma_{k-1}\delta'. \tag{2.41}$$

Důkaz. V první řadě si uvědomíme, čemu je roven koeficient a_k z řetězového zlomku čísla α, což jsme si připomenuli ve větě 2.22 a také v tabulce 2.1:

$$a_k = \begin{cases} 2a_0, & \text{pokud } D \equiv 2, 3 \bmod 4, \\ 2a_0 + 1, & \text{pokud } D \equiv 1 \bmod 4. \end{cases}$$

Vidíme tedy, že $a_k > a_0$, a proto je zlomek $p_{k-2,a_0}/q_{k-2,a_0}$ skutečně horní polokonvergent čísla α. Pro samotný důkaz požadované rovnosti (2.41) nejprve použijeme rovnost (2.7) z tvrzení 2.9, dle které platí:

$$\alpha = \frac{\alpha_k p_{k-1} + p_{k-2}}{\alpha_k q_{k-1} + q_{k-2}},$$

což upravíme do tvaru

$$-\alpha_k(p_{k-1} - q_{k-1}\alpha) = p_{k-2} - q_{k-2}\alpha. \tag{2.42}$$

Nyní upravíme levou stranu rovnosti (2.42), kde využijeme periodicitu řetězového zlomku čísla α, díky které platí vztah $\alpha_1 = \alpha_{k+1}$, a také využijeme vztah $\alpha = -\delta'$, který se dá velmi snadno ověřit.

$$\alpha_k = \alpha_k - a_k + a_k = \frac{1}{\alpha_{k+1}} + a_k = \frac{1}{\alpha_1} + a_k = \alpha - a_0 + a_k,$$
$$p_{k-1} - q_{k-1}\alpha = p_{k-1} + q_{k-1}\delta' = \gamma'_{k-1}.$$

Získané vztahy dosadíme do levé strany rovnice (2.42) a dostáváme:

$$-(\alpha - a_0 + a_k)\gamma'_{k-1} = p_{k-2} - q_{k-2}\alpha.$$

K oběma stranám poslední rovnosti přičteme výraz $a_0\gamma'_{k-1}$ a dostaneme:

$$-(\alpha + a_k - 2a_0)\gamma'_{k-1} = p_{k-2} - q_{k-2}\alpha + a_0\gamma'_{k-1} = p_{k-2} - q_{k-2}\alpha + a_0p_{k-1} - a_0q_{k-1}\alpha =$$

$$= p_{k-2,a_0} - q_{k-2,a_0}\alpha,$$

kde v poslední rovnosti jsme použili definici koeficientů $p_{n,j}$ z definice 2.4. Snadno se ověří vztah $\alpha + a_k - 2a_0 = \delta$, a proto celkově dostáváme

$$-\delta\gamma'_{k-1} = p_{k-2,a_0} - q_{k-2,a_0}\alpha,$$

a po konjugaci výrazů na obou stranách rovnice dostaneme přesně požadovaný vztah (2.41), přičemž na pravé straně rovnosti využíváme toho, že

$$p_{k-2,a_0} + q_{k-2,a_0}\delta = \gamma_{k-2,a_0},$$

což se dá snadno odvodit z rekurentní definice koeficientů p_{k-2,a_0} a q_{k-2,a_0}. Tím je toto lemma dokázané. □

Toto lemma je dokázané i v článku [3] jako Lemma 5. Tento článek zkoumá nerozložitelné prvky ve zajímavém případě polomřížek v $\mathbb{R}$ a v $\mathbb{R}^2$, čemuž se my budeme podrobně věnovat téměř celou příští kapitolu této práce.

2.4 Algebraická teorie čísel

V této sekci práce si připomeneme všechny pojmy z algebraické teorie čísel, které budeme v práci potřebovat. Důkazy většiny tvrzení z této sekce lze nalézt v knize J. Milneho [11], některé jednodušší záležitosti lze nalézt i ve skriptech V. Kaly [6].

2.4.1 Základní pojmy

Základním pojmem algebraické teorie čísel je pojem *číselného tělesa*. Každé těleso K tvoří, až na izomorfismus, vektorový prostor nad tělesem racionálních čísel $\mathbb{Q}$. Těleso K je *číselné těleso*, má-li tento vektorový prostor konečnou dimenzi, kterou označíme n. Tuto dimenzi též nazýváme *stupněm rozšíření* tělesa K, přičemž rovněž říkáme, že K je číselné těleso stupně n.

V každém číselném tělese K mají důležité postavení tzv. *celistvé prvky* (nad $\mathbb{Z}$), čímž jsou myšleny právě takové prvky tělesa K, které jsou kořeny nějakého monického polynomu s koeficienty v $\mathbb{Z}$. Množinu celistvých prvků tělesa K značíme $\mathcal{O}_K$. Tyto celistvé prvky tvoří okruh, což je ukázáno dvěma způsoby v knize [11] jako Theorem 2.1, rovněž lze důkaz nalézt v obecnější podobě pro okruhová rozšíření ve skriptech [6] jako důsledek 2.2.

V této práci bude pro nás nejdůležitější případ totálně reálných kvadratických číselných těles (pojem totálně reálného číselného tělesa bude formálně zaveden v definici 2.29), tedy číselných těles K stupně 2 takových, že $K = \mathbb{Q}(\sqrt{D})$ pro nějaké bezčtvercové přirozené číslo $D \neq 1$. Tato číselná tělesa budeme nadále pojmenovávat reálná kvadratická. Celistvé prvky v těchto číselných tělesech vypadají následovně:

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}], & \text{pokud } D \equiv 2,3 \bmod 4, \\ \mathbb{Z}\left[\dfrac{1+\sqrt{D}}{2}\right], & \text{pokud } D \equiv 1 \bmod 4. \end{cases}$$

Tvar celistvých prvků v reálných kvadratických číselných tělesech je dokázán jako věta 4.3. ve skriptech [6].

Je-li K číselné těleso stupně n, poté platí $K = \mathbb{Q}(\alpha)$, kde α je algebraické číslo stupně n a má minimální polynom f stupně n s celočíselnými koeficienty. Z toho se dá odvodit, že existuje právě n vnoření (prostých homomorfismů) $\sigma_1, \sigma_2, \ldots, \sigma_n$ z tělesa K do tělesa komplexních čísel $\mathbb{C}$, kde kořeny polynomu f jsou právě $\sigma_1(\alpha), \sigma_2(\alpha), \ldots, \sigma_n(\alpha)$. Dále, pro K číselné těleso stupně n, $\beta \in K$ a i od 1 do n označme $\sigma_i(\beta)$ *konjugátem* prvku β. Tato definice konjugátu zobecňuje definici 2.19 v tom smyslu, že v případě $n = 2$ a $K = \mathbb{Q}(\sqrt{D})$ platí, že σ_1 je identické zobrazení a $\sigma_2(a + b\sqrt{D}) = a - b\sqrt{D}$ pro libovolná a,$b \in \mathbb{Q}$. To znamená, že obrazem prvku $a + b\sqrt{D}$ při zobrazení σ_2 je právě konjugát tohoto prvku dle definice 2.19. Nyní definujme další význačné vlastnosti prvků číselných těles, které budou pro nás v práci důležité.

Definice 2.28. *Nechť K je číselné těleso stupně n, $\alpha \in K$ a nechť $\sigma_1, \sigma_2, \ldots, \sigma_n$ jsou všechna vnoření z K do $\mathbb{C}$.* Normou *prvku α rozumíme $N(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha)$ a* stopou *prvku α rozumíme $Tr(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha)$.*

Dá se ukázat, že pro všechny prvky $\alpha, \beta \in K$ platí, že $N(\alpha\beta) = N(\alpha)N(\beta)$ a $Tr(\alpha + \beta) = Tr(\alpha) + Tr(\beta)$. Dále se dá ukázat, že norma i stopa libovolného prvku $\alpha \in K$ je nutně racionální číslo a je-li navíc $\alpha \in \mathcal{O}_K$, poté je $N(\alpha)$ i $Tr(\alpha)$ celé číslo. Pomocí norem můžeme též snadno charakterizovat jednotky, neboli invertibilní prvky okruhu $\mathcal{O}_K$: Prvek α je invertibilní, právě když jeho norma je ± 1, což je vysloveno a dokázáno jako Lemma 5.2 v knize [11].

Nyní si zadefinujeme pojmy totálně reálných těles a totálně kladných prvků:

Definice 2.29. *Nechť K je číselné těleso stupně n a nechť $\sigma_1, \sigma_2, \ldots, \sigma_n$ jsou všechna vnoření z K do $\mathbb{C}$. Těleso K je* totálně reálné*, pokud pro všechna i od 1 do n platí, že $\sigma_i(K) \subseteq \mathbb{R}$. Pro totálně reálné číselné těleso K definujme* totálně kladné prvky *tělesa K jako $\mathcal{O}_K^+ := \{\alpha \in K | \sigma_i(\alpha) > 0 \quad \forall i \in \{1, 2, \ldots, n\}\}$ a podobně definujme* totálně nezáporné prvky *tělesa K jako*

$$\mathcal{O}_K^{+,0} := \{\alpha \in K \mid \sigma_i(\alpha) \geq 0 \quad \forall i \in \{1, 2, \ldots, n\}\}.$$

Dá se ukázat, že pro číselné těleso K tvoří jeho totálně kladné prvky $\mathcal{O}_K^+$ podpologrupu celistvých prvků $\mathcal{O}_K$ vzhledem ke sčítání, tedy pokud $\alpha, \beta \in \mathcal{O}_K^+$, poté $\alpha + \beta \in \mathcal{O}_K^+$. Ze stejného důvodu platí, že $\mathcal{O}_K^{+,0}$ je podmonoid okruhu celistvých prvků $\mathcal{O}_K$.

Dalším pojmem, který budeme v práci potřebovat, je pojem diskriminantu.

Definice 2.30. *Nechť K je číselné těleso stupně n, buďte $\sigma_1, \sigma_2, \ldots, \sigma_n$ všechna vnoření z K do $\mathbb{C}$ a mějme prvky $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$.* Diskriminantem prvků *$\alpha_1, \alpha_2, \ldots, \alpha_n$ rozumíme druhou mocninu determinantu matice o n řádcích a n sloupcích, která obsahuje na místě (i, j) prvek $\sigma_i(\alpha_j)$. Tento diskriminant značíme $\Delta(\alpha_1, \alpha_2, \ldots, \alpha_n)$.*

Definice 2.31. *Nechť K je číselné těleso stupně n. Bázi $\alpha_1, \alpha_2, \ldots, \alpha_n$ vektorového prostoru K nad $\mathbb{Q}$ nazveme* celistvou bází*, pokud prvky $\alpha_1, \alpha_2, \ldots, \alpha_n$ generují $\mathcal{O}_K$ jako $\mathbb{Z}-$modul, neboli $\mathcal{O}_K = \bigoplus_{i=1}^{n} \mathbb{Z}\alpha_i$.*

Dá se ukázat, že celistvá báze existuje pro každé číselné těleso K, viz Proposition 2.29 v knize [11], a navíc každá celistvá báze tělesa K má stejný diskriminant, viz Lemma 2.23 opět v knize [11]. Proto je následující definice diskriminantu tělesa K korektní:

Definice 2.32. *Nechť K je číselné těleso stupně n a $\alpha_1, \alpha_2, \ldots, \alpha_n$ je jeho celistvá báze.* Diskriminantem tělesa K *rozumíme diskriminant prvků $\alpha_1, \alpha_2, \ldots, \alpha_n$ a diskriminant tělesa K značíme Δ_K.*

Nyní se vraťme ke případu reálných kvadratických číselných těles a podívejme se na to, jak zde konkrétně vypadají právě zadefinované vlastnosti číselných těles a jejich prvků. Nechť $K = \mathbb{Q}(\sqrt{D})$ pro $D \neq 1$ bezčtvercové přirozené číslo a $\alpha = a + b\sqrt{D} \in K$. Poté platí, že

$$N(\alpha) = \alpha\alpha' = a^2 - Db^2, Tr(\alpha) = \alpha + \alpha' = 2a.$$

Co se týká celistvých bází a diskriminantu tělesa K, tak je situace následující: Pokud $D \equiv 2, 3 \bmod 4$, tedy $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$, pak celistvou bází tělesa K je $1, \sqrt{D}$ a diskriminant tělesa K je $4D$. Pokud $D \equiv 1 \bmod 4$, tedy $\mathcal{O}_K = \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right]$, pak celistvou bází tělesa K je $1, \frac{1+\sqrt{D}}{2}$ a diskriminant tělesa K je D.

Na závěr této části zmiňme jednoduchou charakterizaci jednotek, tedy invertibilních prvků v kvadratických číselných tělesech (neboli prvků s normu ± 1), k čemuž se vrátíme ke značení z tabulky 2.1.

Tvrzení 2.33. *Pro hodnoty D, δ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo a $K = \mathbb{Q}(\sqrt{D})$ platí, že pro všechna $l, m \in \mathbb{N}$ je prvek $\varepsilon = l + m\delta \in \mathcal{O}_K$ jednotkou, právě když*

$$l = p_{k-1}, m = q_{k-1},$$

kde posloupnosti $\{p_i\}_{i=-1}^{\infty}$ a $\{q_i\}_{i=-1}^{\infty}$ byly zadefinované rekurentně v definici 2.4.

Důkaz tohoto tvrzení lze nalézt v poznámkách [13], kde je mu věnována celá sekce 8.4. Předpoklad $l, m \in \mathbb{N}$ není nijak omezující, do tohoto tvaru lze dostat každou netriviální (různou od ± 1) jednotku okruhu $\mathcal{O}_K$ pomocí přenásobení -1 a případné konjugace, přičemž tyto úpravy nemají vliv na to, zda-li zkoumaný prvek je invertibilní.

2.4.2 Další vlastnosti algebraických čísel stupně 2

V další části této sekce budeme zkoumat další vlastnosti algebraických čísel stupně 2. Nejprve se podíváme na normy a stopy jistých význačných prvků, které budeme vysloveně potřebovat v další kapitole při popisu nerozložitelných prvků v reálných kvadratických číselných tělesech. Tyto vlastnosti byly zpracovány v 1. kapitole článku [3], zde dojde ke sjednocení značení a zpřehlednění.

Nechť $\beta \in \mathbb{Q}(\sqrt{D})$ je iracionální číslo pro $D \neq 1$ bezčtvercové přirozené číslo, řekněme

$$\beta = \frac{\sqrt{D} + r_0}{s_0}, \tag{2.43}$$

kde $r_0, s_0 \in \mathbb{Q}$, s_0 je nenulové a pokud $r_0 = 0$, tak $s_0 \neq 1$ (jinak $\beta \in \mathbb{Q}$). Uvažujme rozvoj čísla β do řetězového zlomku, konkrétně uvažujme posloupnosti $\{a_i\}_{i=0}^{\infty}$ a $\{\alpha_i\}_{i=0}^{\infty}$ dle vztahů (2.5). Potom pro všechna i, bude číslo α_i iracionální a bude prvkem $\mathbb{Q}(\sqrt{D})$, nechť platí následující vztah:

$$\alpha_i = \frac{\sqrt{D} + r_i}{s_i}. \tag{2.44}$$

Budeme tedy uvažovat posloupnosti $\{r_i\}_{i=0}^{\infty}$ a $\{s_i\}_{i=0}^{\infty}$ podle rovností (2.43) a (2.44). Pro prvky těchto posloupností platí zajímavé rekurentní vztahy, které si nyní odvodíme. Pro všechna j od 0 do ∞ platí, že:

$$\frac{\sqrt{D} + r_{j+1}}{s_{j+1}} \overset{(2.44)}{=} \alpha_{j+1} \overset{(2.5)}{=} \frac{1}{\alpha_j - a_j} \overset{(2.44)}{=} \frac{1}{\frac{\sqrt{D}+r_j}{s_j} - a_j} = \frac{s_j}{\sqrt{D} + r_j - a_j s_j} =$$

$$= \frac{s_j(-\sqrt{D} + r_j - a_j s_j)}{(\sqrt{D} + r_j - a_j s_j)(-\sqrt{D} + r_j - a_j s_j)} = \frac{s_j(-\sqrt{D} + r_j - a_j s_j)}{(r_j - a_j s_j)^2 - D} =$$

$$= \frac{\sqrt{D} + a_j s_j - r_j}{\frac{D-(r_j - a_j s_j)^2}{s_j}}.$$

Jelikož racionální koeficienty r,s algebraického čísla stupně 2 ve tvaru (2.18) jsou jednoznačné, tak z rovností výše plynou následující rekurentní vztahy, platné pro každé j od 0 do ∞:

$$r_{j+1} = a_j s_j - r_j,\ s_{j+1} = \frac{D - r_{j+1}^2}{s_j}. \tag{2.45}$$

Nyní již můžeme vyslovit lemma o výpočtu norem a stop jistých prvků:

Lemma 2.34 ([3], Lemma 1)**.** *Nechť β je algebraické číslo stupně 2 tvaru* (2.43)*, uvažujme řetězový zlomek čísla $\beta = [a_0, a_1, \ldots]$ a posloupnosti $\{p_i\}_{i=-1}^{\infty}$ a $\{q_i\}_{i=-1}^{\infty}$, odvozené z posloupnosti $\{a_i\}_{i=0}^{\infty}$ pomocí vztahů popsaných v definici 2.4, stejně jako posloupnosti $\{\alpha_i\}_{i=0}^{\infty}$, $\{r_i\}_{i=0}^{\infty}$ a $\{s_i\}_{i=0}^{\infty}$ jako výše ve vztahu* (2.44)*. Poté pro všechna $j \in \mathbb{N}_0$ platí:*

a) $N(p_{j-1} - q_{j-1}\beta) = (-1)^j \frac{s_j}{s_0}$,

b) $Tr((p_{j-1} - q_{j-1}\beta')(p_j - q_j\beta)) = (-1)^j \frac{2r_{j+1}}{s_0}$.

Důkaz. Před důkazem těchto dvou vztahů si uvědomíme, že platí rovnost

$$p_j - q_j\beta = \frac{-1}{\alpha_{j+1}}(p_{j-1} - q_{j-1}\beta), \tag{2.46}$$

která se dá snadno odvodit úpravou rovnosti $\beta = \frac{p_{j-1} + p_j\alpha_{j+1}}{q_{j-1} + q_j\alpha_{j+1}}$, která plyne přímo z tvrzení 2.9. Nyní již přejdeme k důkazu samotných požadovaných rovností:

Rovnost a) bude dokázána matematickou indukcí podle j: Pro $j = 0$ máme:

$$N(p_{j-1} - q_{j-1}\beta) = N(1) = 1 = (-1)^0 \frac{s_0}{s_0},$$

tedy požadovaný vztah triviálně platí. Nyní provedeme indukční krok:

$$N(p_j - q_j\beta) \overset{(2.46)}{=} N\left(-\frac{1}{\alpha_{j+1}}\right) N(p_{j-1} - q_{j-1}\beta) \overset{(*)}{=} N\left(-\frac{1}{\alpha_{j+1}}\right)(-1)^j \frac{s_j}{s_0} =$$

$$= \frac{1}{\alpha_{j+1}} \frac{1}{\alpha'_{j+1}}(-1)^j \frac{s_j}{s_0} \overset{(2.44)}{=} \frac{s_{j+1}}{r_{j+1} + \sqrt{D}} \frac{s_{j+1}}{r_{j+1} - \sqrt{D}}(-1)^j \frac{s_j}{s_0} =$$

$$\frac{s_{j+1}^2}{r_{j+1}^2 - D}(-1)^j \frac{s_j}{s_0} \overset{(2.45)}{=} \frac{s_{j+1}^2}{-s_{j+1}s_j}(-1)^j \frac{s_j}{s_0} = (-1)^{j+1} \frac{s_{j+1}}{s_0},$$

kde v rovnosti $(*)$ byl použit indukční předpoklad. Tím jsme dokázali rovnost a), nyní ukážeme platnost rovnosti b), důkaz bude proveden přímo:

$$Tr((p_{j-1} - q_{j-1}\beta')(p_j - q_j\beta)) = Tr\left(\frac{(p_{j-1} - q_{j-1}\beta')(p_j - q_j\beta)(p_j - q_j\beta')}{p_j - q_j\beta'}\right) \overset{(2.46)}{=}$$

$$= Tr(-\alpha'_{j+1}(p_j - q_j\beta')(p_j - q_j\beta)) = Tr(-\alpha'_{j+1}N(p_j - q_j\beta)) \overset{a)}{=}$$

$$= Tr\left(\alpha'_{j+1}(-1)^j \frac{s_{j+1}}{s_0}\right) = (-1)^j \frac{s_{j+1}}{s_0}(\alpha_{j+1} + \alpha'_{j+1}) \overset{(2.44)}{=}$$

$$= (-1)^j \frac{s_{j+1}}{s_0}\left(\frac{r_{j+1} + \sqrt{D}}{s_{j+1}} + \frac{r_{j+1} - \sqrt{D}}{s_{j+1}}\right) = (-1)^j \frac{2r_{j+1}}{s_0},$$

čímž je důkaz rovnosti b) dokončen a lemma je dokázané. □

Nyní uvedeme ještě jedno pomocné lemma, které nám popisuje, které vlastnosti parametrů r_0 a s_0 a za jakých podmínek se přenesou i na všechny parametry r_j, respektive s_j:

Lemma 2.35 ([3], Lemma 2)**.** *Nechť β je algebraické číslo stupně 2 a uvažujme posloupnosti $\{a_i\}_{i=0}^{\infty}$, $\{\alpha_i\}_{i=0}^{\infty}$, $\{r_i\}_{i=0}^{\infty}$ a $\{s_i\}_{i=0}^{\infty}$ stejně jako v předchozím lemmatu 2.34. Poté platí následující vlastnosti:*

a) Pokud $r_0, s_0 \in \mathbb{Z}$ a zároveň $D \equiv r_0^2 \bmod s_0$, poté pro všechna $j \in \mathbb{N}_0$ platí, že $r_j, s_j \in \mathbb{Z}$ a $D \equiv r_j^2 \bmod s_j$.

b) Pokud $s_0 > 0$ a zároveň $r_0^2 < D$, poté pro všechna $j \in \mathbb{N}_0$ platí, že $s_j > 0$ a $r_j^2 < D$.

c) Pokud $r_0, s_0 \in \mathbb{Z}$, s_0 je sudé a zároveň $D \equiv r_0^2 \bmod 2s_0$, poté pro všechna $j \in \mathbb{N}_0$ platí, že $r_j, s_j \in \mathbb{Z}$, s_j je sudé a $D \equiv r_j^2 \bmod 2s_j$.

Důkaz. Všechny tyto vlastnosti dokážeme matematickou indukcí podle j: Jelikož u všech vlastností předpokládáme pravdivost tvrzení pro $j = 0$, stačí u každé z vlastností ověřit indukční krok.

a) Nechť $r_j, s_j \in \mathbb{Z}$ a $D \equiv r_j^2 \bmod s_j$. Podle rovností (2.45) dostáváme, že $r_{j+1} = a_j s_j - r_j$, což je podle indukčního předpokladu celé číslo. Zároveň vidíme, že $r_j^2 \equiv r_{j+1}^2 \bmod s_j$ a tím pádem $D \equiv r_{j+1}^2 \bmod s_j$, tedy $\frac{D - r_{j+1}^2}{s_j} \overset{(2.45)}{=} s_{j+1}$ je opět celé číslo. Z toho však plyne, že s_{j+1} dělí $D - r_{j+1}^2$, proto $D \equiv r_{j+1}^2 \bmod s_{j+1}$, čímž jsme ověřili indukční krok a vlastnost *a*) je dokázána.

b) Nechť $s_j > 0$ a $r_j^2 < D$. Poté platí:

$$1 < \alpha_{j+1} \overset{(2.44)}{=} \frac{\sqrt{D} + r_{j+1}}{s_{j+1}} \overset{(2.45)}{=} \frac{\sqrt{D} - r_j + a_j s_j}{s_{j+1}}.$$

Podle indukčního předpokladu je čitatel posledně uvedeného zlomku kladný, tedy musí být kladný i jmenovatel tohoto zlomku, čili $s_{j+1} > 0$, a zároveň $-r_{j+1} < \sqrt{D}$, nyní tedy stačí ukázat nerovnost $r_{j+1} < \sqrt{D}$. Ta plyne ze vztahu

$$a_j < \alpha_j \overset{(2.44)}{=} \frac{\sqrt{D} + r_j}{s_j},$$

po úpravě $0 < \sqrt{D} + r_j - a_j s_j \overset{(2.45)}{=} \sqrt{D} - r_{j+1}$, čímž jsme tedy ukázali, že $r_{j+1}^2 < D$, indukční krok je ověřen a vlastnost *b*) je rovněž dokázána.

c) Nechť $r_j, s_j \in \mathbb{Z}$, s_j je sudé a $D \equiv r_j^2 \bmod 2s_j$. Nejprve ověříme předpoklad vlastnosti *a*), kterou nyní chceme použít, abychom ukázali, že r_{j+1} a s_{j+1} jsou celá čísla. Ověření tohoto předpokladu je však jednoduché, neboť $D \equiv r_0^2 \bmod 2s_0$ snadno implikuje $D \equiv r_0^2 \bmod s_0$. Proto podle vlastnosti *a*) jsou r_{j+1} a s_{j+1} celá čísla, nyní ukažme, že s_{j+1} je sudé. Platí následující rovnosti:

$$s_j s_{j+1} \overset{(2.45)}{=} D - r_{j+1}^2 \overset{(2.45)}{=} D - (a_j s_j - r_j)^2 = (D - r_j^2) + (2a_j s_j r_j) + (-a_j^2 s_j^2).$$

Každý ze tří sčítanců z poslední rovnosti je dělitelný $2s_j$, přičemž u prvního a třetího sčítance používáme indukční předpoklad a u druhého je to zřejmé. Tedy $2s_j$ dělí i součin $s_j s_{j+1}$, čili existuje $x \in \mathbb{Z}$ takové, že $s_j s_{j+1} = 2s_j x$, tím pádem $s_{j+1} = 2x$ a s_{j+1} je sudé číslo, zbývá ukázat kongruenci $D \equiv r_{j+1}^2 \bmod 2s_{j+1}$. Díky sudosti s_{j+1} platí, že $2s_{j+1}$ dělí $s_j s_{j+1} \overset{(2.45)}{=} D - r_{j+1}^2$, což dává přesně požadovanou kongruenci $D \equiv r_{j+1}^2 \bmod 2s_{j+1}$, čímž byl i u vlastnosti *c*) indukční krok ověřen, čímž je celé lemma dokázané. □

2.4.3 Minkowského věta a Minkowského vnoření

V závěrečné části této sekce si připomeneme Minkowského větu o mřížových bodech, kterou budeme později v práci potřebovat při horním odhadu norem nerozložitelných prvků v totálně reálných číselných tělesech. Nejprve si však připomeňme definice pojmů, abychom tuto větu vůbec mohli vyslovit.

Mřížkou ve vektorovém prostoru V dimenze n nad tělesem $\mathbb{R}$ budeme rozumět libovolnou diskrétní podgrupu (vzhledem ke sčítání) vektorového prostoru V, na kterou se díváme jako podmnožinu $\mathbb{R}^n$. Mřížky budeme značit písmenem Λ.

Ekvivalentně se lze na mřížky dívat jako na podgrupy V, které jsou generovány lineárně nezávislými vektory $v_1, v_2, \ldots, v_r$ (s výjimkou případu $\Lambda = \{0\}$, to je pro nás rovněž mřížka), což budeme značit $\Lambda = \bigoplus_{i=1}^{r} v_i$. Pokud $r = n$, tak říkáme, že mřížka Λ je *úplná*. Podrobnější zadefinování mřížky a důkaz ekvivalence obou jejích definic výše uvedených lze nalézt v knize [11] ve 4. kapitole v sekci Lattices, ekvivalence obou definic je dokázána jako Proposition 4.15.

V první kapitole v definici 1.8 jsme definovali pojem polomřížky, což byly takové diskrétní podmonoidy $\mathbb{R}^n$, které jsou obsaženy v nějakém kuželi a obsahují alespoň jeden nenulový prvek. To však znamená, že nemáme žádný vztah mezi mřížkami a polomřížkami, neboť polomřížky nejsou uzavřené na unární operaci $-$, opačně mřížky nejsou obsaženy v nějakém kuželi.

Nyní si zadefinujeme pojem základního rovnoběžnostěnu a jeho objemu. Nechť V je vektorový prostor dimenze n nad tělesem $\mathbb{R}$ a $\Lambda = \bigoplus_{i=1}^{n} v_i$ je úplná mřížka ve V a zvolme $\lambda_0 \in \Lambda$ libovolně. *Základním rovnoběžnostěnem* mřížky Λ rozumíme množinu $P = \{\lambda_0 + \sum_{i=1}^{n} x_i v_i \mid 0 \leq x_i < 1\}$. *Objemem* základního rovnoběžnostěnu P, který budeme značit $\mu(P)$, budeme rozumět $|det(v_1, v_2, \ldots, v_n)|$. Objem základního rovnoběžnostěnu nezávisí na volbě báze $v_1, v_2, \ldots, v_n$, podrobnosti lze opět nalézt v knize [11], tentokrát jde o Remark 4.16.

Nyní již můžeme vyslovit Minkowského větu:

Věta 2.36 ([11], Theorem 4.19)**.** *Nechť V je vektorový prostor dimenze n nad tělesem $\mathbb{R}$, nechť Λ je úplná mřížka ve V a P její základní rovnoběžnostěn. Nechť $T \subseteq V$ je množina, která je jakožto podmnožina $\mathbb{R}^n$ kompaktní, konvexní a symetrická podle počátku (tedy pokud $x \in T$, poté i $-x \in T$). Má-li množina T Lebesgueovou míru alespoň $2^n\mu(P)$, potom $T \cap \Lambda$ obsahuje nenulový bod.*

Ještě si potřebujeme uvést důležitý příklad mřížky, pro který budeme později tuto Minkowského větu aplikovat. Tento příklad mřížky bude odvozen od celistvých prvků číselného tělesa K pomocí tzv. *Minkowského vnoření*, které si nyní představíme.

Nechť K je číselné těleso stupně n a zkoumejme všechna vnoření z K do $\mathbb{C}$. Nechť r různých vnoření $\sigma_1, \ldots, \sigma_r$. splňuje vlastnost $\sigma_i(K) \subseteq \mathbb{R}$ pro všechna i od 1 do r. Ostatních $n - r$ vnoření tedy zobrazí nějaký prvek K na nějaké komplexní číslo a těchto vnoření bude nutně sudý počet (řekněme $2s$), jelikož tato komplexní vnoření jsou spárovány pomocí komplexního sdružení, označme tyto komplexní vnoření $\sigma_{r+1}, \overline{\sigma_{r+1}}, \ldots, \sigma_{r+s}, \overline{\sigma_{r+s}}$. Platí tedy $r + 2s = n$. V definici 2.29 jsme zadefinovali pojem totálně reálných číselných těles, zde vidíme, že jde o právě taková tělesa, pro která platí, že $r = n$.

Nyní již můžeme zadefinovat samotné *Minkowského vnoření*. Jedná se o prostý homomorfismus vektorových prostorů K a $\mathbb{R}^r \times \mathbb{C}^s$. Toto zobrazení budeme značit σ a pro prvek $\beta \in K$ platí, že

$$\sigma(\beta) = (\sigma_1(\beta), \sigma_2(\beta), \ldots, \sigma_r(\beta), \sigma_{r+1}(\beta), \ldots, \sigma_{r+s}(\beta)).$$

Prostor $\mathbb{R}^r \times \mathbb{C}^s$ se též nazývá *Minkowského prostor*.

Nyní si již můžeme konkrétně představit příklad úplné mřížky, kterou budeme v práci potřebovat. Tímto příkladem je $\sigma(\mathcal{O}_K)$ pro libovolné číselné těleso K. Množina $\sigma(\mathcal{O}_K)$ je opravdu úplná mřížka a její základní rovnoběžnostěn má objem $2^{-s}\sqrt{\Delta_K}$, toto tvrzení je dokázáno v obecnější formě v knize [11] jako Proposition 4.26, kde se dokonce ukáže, že pro každý ideál I okruhu $\mathcal{O}_K$ platí, že $\sigma(I)$ je

úplná mřížka (objem jejího základního rovnoběžnostěnu poté závisí i na tzv. normě ideálu I, tu však v této práci potřebovat nebudeme). Dále platí, že jeli K totálně reálné číselné těleso, poté je $\sigma(\mathcal{O}_K^{+,0})$ polomřížka. Diskrétnost této množiny plyne z diskrétnosti $\sigma(\mathcal{O}_K)$, o podmonoid $\mathbb{R}^n$ se jedná díky tomu, že $\mathcal{O}_K^{+,0}$ tvoří podmonoid $\mathcal{O}_K$ a σ je homomorfismus, a konečně $\sigma(\mathcal{O}_K^{+,0}) \subseteq (\mathbb{R}_0^+)^n$, což je kužel.

3. Nerozložitelné prvky v kvadratických číselných tělesech

V této kapitole se budeme podrobněji věnovat nerozložitelným prvkům jistých polomřížek ve dvou dimenzích. Nejprve se zaměříme na tzv. *úhlové oblasti* E_α a $F_{\alpha,\beta}$, přičemž později se v této kapitole ukáže, že speciálním případem úhlových oblastí, až na drobné technické komplikace, je i okruh $\sigma(\mathcal{O}_K^{+,0})$, čímž se tedy propojí geometrická teorie polomřížek s algebraickou teorií čísel.

3.1 Úhlové oblasti

V této sekci se budeme věnovat úhlovým oblastem E_α a $F_{\alpha,\beta}$. Tyto úhlové oblasti si za chvíli zadefinujeme a poté si charakterizujeme nerozložitelné prvky těchto polomřížek pomocí horních polokonvergentů čísel α a β, respektive jejich dobrých horních aproximací dle věty 2.17 (nadále se budeme odvolávat na pojem horních polokonvergentů), čili zde dojde k propojení polomřížek a teorie řetězových zlomků ze sekce 2.1.

Rovněž pro celou tuto sekci budeme předpokládat, že číslo α je libovolné kladné reálné, nebude se tedy jednat o nějaké zcela konkrétní algebraické číslo stupně 2 z tabulky 2.1.

3.1.1 Definice úhlových oblastí

V úvodní části této sekce si zadefinujeme pojem úhlové oblasti a vysvětlíme jejich geometrický význam.

Definice 3.1. *Nechť α, β jsou kladná reálná čísla. Definujme* úhlové oblasti E_α *a $F_{\alpha,\beta}$ následujícím způsobem:*

$$E_\alpha = \{(x, y) \in \mathbb{Z}^2 \mid y \geq 0, x \geq \alpha y\}, \tag{3.1}$$

$$F_{\alpha,\beta} = \{(x, y) \in \mathbb{Z}^2 \mid x \geq -\beta y, x \geq \alpha y\}. \tag{3.2}$$

Vysvětleme si nejprve geometricky, proč jsme tyto množiny pojmenovali úhlové oblasti a proč se jedná o polomřížky v $\mathbb{R}^2$. Co se týká množiny E_α, tak tu tvoří právě takové prvky $\mathbb{R}^2$ s celočíselnými souřadnicemi, které mají první souřadnici kladnou (s výjimkou prvku $(0, 0)$) a leží „mezi“ přímkami $y = 0$ a $x = \alpha y$. To však znamená, že prvky E_α jsou právě takové prvky $\mathbb{R}^2$, které leží v konvexním obalu polopřímek $\{(x, 0) \in \mathbb{R}^2 \mid x \in \mathbb{R}_0^+\}$ a $\{(x, y) \in \mathbb{R}^2 \mid y \in \mathbb{R}_0^+, x = \alpha y\}$. Tyto dvě polopřímky mají společný koncový bod v bodě $(0, 0)$ a zároveň svírají konvexní úhel $\operatorname{arccotg}(\alpha)$, jehož hodnota nepřesáhne $\pi/2$. Obecně platí (ve dvou dimenzích), že konvexní obal libovolných dvou polopřímek, které mají společný koncový bod v počátku soustavy souřadnic a svírají konvexní úhel menší než π, tvoří kužel (který jsme zadefinovali v definici 1.6). Proto prvky E_α leží v nějakém kuželi, navíc volba celočíselných souřadnic zajistí, že E_α je diskrétní množina, Rutinně se dá ověřit, že E_α je podmonoid $\mathbb{R}^2$, a jelikož $(1, 0) \in E_\alpha$, tak skutečně

dostáváme, že E_α je polomřížka v $\mathbb{R}^2$ podle definice 1.8 a můžeme zkoumat její nerozložitelné prvky podle definice 1.13. Analogicky se dá ověřit, že i $F_{\alpha,\beta}$ je polomřížka v $\mathbb{R}^2$, která je obsažena v kuželi, který je konvexním obalem polopřímek $\{(x,y) \in \mathbb{R}^2 \mid y \in \mathbb{R}_0^+, x = \alpha y\}$ a $\{(x,y) \in \mathbb{R}^2 \mid y \in \mathbb{R}_0^+, x = -\beta y\}$, které svírají konvexní úhel $\operatorname{arccotg}(\alpha) + \operatorname{arccotg}(\beta)$, což je úhel menší než π.

3.1.2 Nerozložitelné prvky v úhlových oblastech

V této části této sekce již budeme zkoumat nerozložitelné prvky v těchto úhlových oblastech E_α a $F_{\alpha,\beta}$. Snadno z definic nahlédneme, že $E_\alpha \subseteq F_{\alpha,\beta}$, z čehož plyne, že nerozložitelné prvky v $F_{\alpha,\beta}$ budou nerozložitelné i v E_α. Platí i opačná implikace, kterou si nyní ukážeme v následujícím lemmatu:

Lemma 3.2 ([3], Lemma 3)**.** *Nechť $\alpha, \beta \in \mathbb{R}^+$ a mějme (x,y) nerozložitelný prvek v polomřížce E_α. Poté prvek (x,y) zůstane nerozložitelným i v polomřížce $F_{\alpha,\beta}$.*

Důkaz. Důkaz bude proveden sporem. Nechť $(x,y) = (x_1,y_1) + (x_2,y_2)$ je rozklad prvku (x,y) pro $(x_1,y_1), (x_2,y_2) \in F_{\alpha,\beta} \setminus \{(0,0)\}$. Z nerozložitelnosti prvku (x,y) v E_α plyne, že alespoň jeden z prvků $(x_1,y_1), (x_2,y_2)$ neleží v E_α, bez újmy na obecnosti nechť jde o prvek (x_2,y_2). To nutně znamená, že $y_2 < 0$, z čehož dále dostáváme, že nutně $y_1 > 0$, jinak by $y = y_1 + y_2 \leq 0$ a prvek (x,y) by neležel v E_α. Tedy $y < y_1$ a zároveň připomeňme, že $x_1, x_2 > 0$, čili $x = x_1 + x_2 \geq 2$.

Ukážeme, že $(x-1,y) \in E_\alpha$. To by totiž implikovalo rozložitelnost prvku (x,y) v E_α, neboť $(x,y) = (x-1,y) + (1,0)$, $(1,0) \in E_\alpha$ a měli bychom spor. Nerovnost $y > 0$ jsme již odůvodnili, zbývá ukázat nerovnost $x - 1 \geq \alpha y$. Vskutku,

$$x - 1 = x_1 + (x_2 - 1) \geq x_1 \overset{(x_1,y_1) \in F_{\alpha,\beta}}{\geq} \alpha y_1 > \alpha(y_1 + y_2) = \alpha y,$$

což jsme přesně chtěli ukázat, tím byl důkaz lemmatu dokončen. □

Analogicky se dá ukázat i souvislost nerozložitelných prvků v úhlových oblastech E_β a $F_{\alpha,\beta}$. Platí, že je-li (x,y) nerozložitelný prvek v E_β, poté je $(x,-y)$ nerozložitelný prvek v $F_{\alpha,\beta}$ (a opět triviálně platí i opačná implikace). To nám umožní charakterizovat všechny nerozložitelné prvky v polomřížce $F_{\alpha,\beta}$ pomocí nerozložitelných prvků v polomřížkách E_α a E_β, což zformulujeme jako následující důsledek, ve kterém si zároveň připomeneme značení P_L pro množinu nerozložitelných prvků polomřížky L:

Důsledek 3.3. *Pro parametry $\alpha, \beta \in \mathbb{R}^+$ platí, že*

$$P_{F_{\alpha,\beta}} = P_{E_\alpha} \cup \{(x,y) \mid (x,-y) \in P_{E_\beta}\}, \tag{3.3}$$

neboli nerozložitelné prvky (x,y) polomřížky $F_{\alpha,\beta}$ jsou přesně nerozložitelné prvky polomřížky E_α pro případ $y \geq 0$ a nerozložitelné prvky polomřížky E_β pro případ $y \leq 0$.

Rozklad množiny $P_{F_{\alpha,\beta}}$ z předchozího důsledku 3.3 je téměř disjunktní, průnikem dvou množin z pravé strany rovnice (3.3) je jednoprvková množina, jejíž jediným prvkem je $(1,0)$.

Z předchozího důsledku plyne, že pokud chceme charakterizovat nerozložitelné prvky v $F_{\alpha,\beta}$, stačí se zabývat nerozložitelnými prvky v E_α, respektive v E_β. Abychom tak mohli učinit, zavedeme pomocný pojem $\alpha-$nerozložitelnosti.

Definice 3.4. *Nechť $\alpha \in \mathbb{R}$ a $y \in \mathbb{N}$. Řekneme, že y je $\alpha-$*rozložitelný *prvek, pokud existují $y_1, y_2 \in \mathbb{N}$ tak, že $y = y_1 + y_2$, a zároveň $\lceil \alpha y \rceil = \lceil \alpha y_1 \rceil + \lceil \alpha y_2 \rceil$. V opačném případě řekneme, že y je $\alpha-$*nerozložitelný prvek.

Snadno si uvědomíme obecnou vlastnost horních celých částí, dle které pokud $y = y_1 + y_2$, potom $\lceil \alpha y \rceil \leq \lceil \alpha y_1 \rceil + \lceil \alpha y_2 \rceil$, proto stačí pro ověření $\alpha-$nerozložitelnosti čísla y dokázat opačnou nerovnost. Nyní již můžeme charakterizovat nerozložitelné prvky v E_α pomocí horních polokonvergentů čísla α, přičemž je logické, že budeme uvažovat právě horní polokonvergenty čísla α a nikoliv ty dolní, neboť horní polokonvergenty vyhovují podmínce $\dfrac{x}{y} \geq \alpha$, což nám po úpravě dává nerovnost $x \geq \alpha y$, která nutně musí platit pro všechny prvky (x, y) polomřížky E_α, přesně podle její definice ve vztazích (3.1). Pro dolní polokonvergenty platí opačná nerovnost, což jasně naznačuje, proč v následující větě budeme uvažovat právě horní polokonvergenty čísla α:

Věta 3.5 ([3], Theorem 1)**.** *Nechť $\alpha \in \mathbb{R}^+$ a mějme nesoudělná čísla $x, y \in \mathbb{N}$. Následující podmínky jsou ekvivalentní:*

a) (x, y) patří do E_α a jedná se o nerozložitelný prvek v E_α,

b) y je $\alpha-$nerozložitelný prvek a $x = \lceil \alpha y \rceil$,

c) $\dfrac{x}{y}$ je horní polokonvergent čísla α.

Důkaz. Nejprve ukážeme, že $a) \Leftrightarrow b)$ a poté ukážeme, že $b) \Leftrightarrow c)$.

1) $a) \Rightarrow b)$: Nechť $(x, y) \in E_\alpha$ je nerozložitelný prvek v E_α. Jistě platí, že $(1, 0) \in E_\alpha$, tak nutně nastane případ, že $(x-1, y) \notin E_\alpha$. To nám spolu s předpokladem $(x, y) \in E_\alpha$ dává platnost nerovností $x - 1 < \alpha y \leq x$, což je zřejmě ekvivalentní s konstatováním $\lceil \alpha y \rceil = x$. Proto nám nyní stačí ukázat $\alpha-$nerozložitelnost čísla y, což ukážeme sporem:

Předpokládejme pro spor, že y je $\alpha-$rozložitelný prvek, tedy $y = y_1 + y_2$ a zároveň $\lceil \alpha y \rceil = \lceil \alpha y_1 \rceil + \lceil \alpha y_2 \rceil$ pro nějaká přirozená čísla y_1, y_2. Poté platí:

$$(x, y) = (\lceil \alpha y \rceil, y) = (\lceil \alpha y_1 \rceil, y_1) + (\lceil \alpha y_2 \rceil, y_2).$$

Nicméně prvky $(\lceil \alpha y_i \rceil, y_i)$ pro $i = 1, 2$ patří do E_α, čili jsme právě ukázali, že (x, y) je rozložitelný prvek v polomřížce E_α, což je spor. Tím je implikace $a) \Rightarrow b)$ dokázána.

2) $b) \Rightarrow a)$: Nechť je y $\alpha-$nerozložitelný prvek a $x = \lceil \alpha y \rceil$, chceme ukázat, že prvek (x, y) je nerozložitelný v E_α. Z rovnosti $x = \lceil \alpha y \rceil$ plyne, že $(x, y) \in E_\alpha$, zbývá ukázat samotnou nerozložitelnost v E_α:

Nechť $(x, y) = (x_1, y_1) + (x_2, y_2)$ pro $(x_1, y_1), (x_2, y_2) \in E_\alpha$, platí tedy nerovnosti

$$x_1 \geq \lceil \alpha y_1 \rceil,\ x_2 \geq \lceil \alpha y_2 \rceil. \tag{3.4}$$

Ukážeme, že $(x_1, y_1) = (0, 0)$. Poté platí následující vztahy:

$$\lceil \alpha y \rceil = x = x_1 + x_2 \overset{(3.4)}{\geq} \lceil \alpha y_1 \rceil + \lceil \alpha y_2 \rceil \geq \lceil \alpha y \rceil. \tag{3.5}$$

Jelikož máme na obou koncích vztahů (3.5) stejné výrazy, budou všechny vztahy ve (3.5) a také ve (3.4) nutně rovnosti. Speciálně poukažme na rovnosti

$$x_1 = \lceil \alpha y_1 \rceil,\ \lceil \alpha y \rceil = \lceil \alpha y_1 \rceil + \lceil \alpha y_2 \rceil. \tag{3.6}$$

Nyní využijeme toho, že $y = y_1 + y_2$ (což předpokládáme) a toho, že y je $\alpha-$nerozložitelný, z čehož nutně plyne, že y_1 nebo y_2 není přirozené číslo, bez újmy na obecnosti nechť jde o y_1. Jelikož $(x_1, y_1) \in E_\alpha$, tak z nerovností (3.1) plyne, že $y_1 = 0$. Jelikož nerovnosti (3.4) jsou ve skutečnosti rovnosti, dostáváme rovnost $x_1 = 0$, celkově $(x_1, y_1) = (0, 0)$, jak jsme přesně chtěli ukázat. Proto je prvek (x, y) nerozložitelný v polomřížce E_α a implikace $b) \Rightarrow a)$ je dokázána.

3) $b) \Rightarrow c)$: Nechť je y $\alpha-$nerozložitelný prvek a $x = \lceil \alpha y \rceil$, chceme ukázat, že $\dfrac{x}{y}$ je horní polokonvergent čísla α. Podle věty 2.17 stačí ukázat, že zlomek $\dfrac{x}{y}$ je dobrou horní aproximací čísla α, neboli $\dfrac{x}{y} \geq \alpha$, a zároveň pro všechny zlomky $\dfrac{x_1}{y_1}$, kde $x_1, y_1 \in \mathbb{Z}$ které vyhovují podmínce (2.16), neboli

$$\frac{x}{y} \geq \frac{x_1}{y_1} \geq \alpha, \tag{3.7}$$

platí buď $y_1 > y$, nebo platí rovnosti $x = x_1$, $y = y_1$. Nerovnost $\dfrac{x}{y} \geq \alpha$ plyne ze vztahů v (3.1), neboť $(x, y) \in E_\alpha$, což jsme již ukázali v předchozí implikaci, tedy ve druhé části tohoto důkazu. Proto uvažujme zlomek $\dfrac{x_1}{y_1}$, kde $x_1, y_1 \in \mathbb{Z}$, jenž vyhovuje podmínce (3.7) a ukažme, že buď $y_1 > y$, nebo platí rovnosti $x = x_1$ a $y = y_1$.

Nejprve předpokládejme, že $y_1 = y$. Poté platí:

$$\lceil \alpha y \rceil = x \overset{(3.7)}{\geq} x_1 \overset{(3.7)}{\geq} \alpha y_1 = \alpha y > \lceil \alpha y \rceil - 1.$$

Platí tedy $x_1 = \lceil \alpha y \rceil = x$, což jsme v tomto případě chtěli ukázat. Zbytek důkazu této implikace bude proveden nepřímo: Nechť $y_1 < y$ a ukážeme, že prvek y je $\alpha-$rozložitelný. Nechť $y_2 := y - y_1 \in \mathbb{N}$, platí tedy jistě rovnost $y = y_1 + y_2$. V tuto chvíli stačí ukázat rovnost $\lceil \alpha y \rceil = \lceil \alpha y_1 \rceil + \lceil \alpha y_2 \rceil$, čímž skutečně ukážeme, že prvek y je $\alpha-$rozložitelný a důkaz této implikace by byl hotov. Aby vůbec mohli platit nerovnosti (3.7), musí nutně nastat případ $x > x_1$, nechť $x_2 := x - x_1 \in \mathbb{N}$. Nyní ukážeme, že $\dfrac{x_2}{y_2} \geq \dfrac{x}{y}$, což nám po aplikování nerovností (3.7) dá nerovnost $\dfrac{x_2}{y_2} \geq \alpha$, kterou za chvíli využijeme. Platí:

$$\frac{x_2}{y_2} - \frac{x}{y} = \frac{x - x_1}{y - y_1} - \frac{x}{y} = \frac{y(x - x_1) - x(y - y_1)}{y(y - y_1)} = \frac{xy_1 - yx_1}{y(y - y_1)}. \tag{3.8}$$

Čitatel posledního zlomku je nezáporný díky nerovnostem (3.7) (zde zcela konkrétně využíváme pozorování před lemmatem 2.13) a jmenovatel totožného zlomku je kladný díky vztahům $y > y_1 > 0$, které předpokládáme. Proto opravdu platí $\dfrac{x_2}{y_2} \geq \dfrac{x}{y}$, a tedy

$$\frac{x_2}{y_2} \geq \frac{x_1}{y_1} \geq \alpha.$$

Z těchto nerovností plyne, že $x_1 \geq \lceil \alpha y_1 \rceil$ a $x_2 \geq \lceil \alpha y_2 \rceil$. Proto platí:

$$\lceil \alpha y \rceil = x = x_1 + x_2 \geq \lceil \alpha y_1 \rceil + \lceil \alpha y_2 \rceil,$$

což nám dle textu za definicí $\alpha-$rozložitelnosti 3.4 stačí ukázat k tomu, abychom skutečně ověřili, že y je $\alpha-$rozložitelný, čímž je důkaz této implikace dokončen.

4) $c) \Rightarrow b)$: Nechť $\frac{x}{y}$ je horní polokonvergent čísla α a chceme ukázat, že y je $\alpha-$nerozložitelný prvek a rovnost $x = \lceil \alpha y \rceil$. Rovnost $x = \lceil \alpha y \rceil$ jsme dokázali v důsledku 2.18, $\alpha-$nerozložitelnost prvku y dokážeme sporem: Nechť $y = y_1 + y_2$ pro $y_1, y_2 \in \mathbb{N}$ taková, že $x = \lceil \alpha y \rceil = \lceil \alpha y_1 \rceil + \lceil \alpha y_2 \rceil$ a označme $x_i := \lceil \alpha y_i \rceil$ pro $i = 1, 2$, platí tedy $x = x_1 + x_2$. Podobně jako v důkazu implikace $b) \Rightarrow c)$, konkrétně díky rovnosti (3.8) dostáváme, že jeden ze zlomků $\frac{x_1}{y_1}, \frac{x_2}{y_2}$ je větší nebo roven $\frac{x}{y}$ a ten druhý bude menší nebo roven $\frac{x}{y}$. Bez újmy na obecnosti předpokládejme, že

$$\frac{x_1}{y_1} \geq \frac{x}{y} \geq \frac{x_2}{y_2} \geq \alpha, \tag{3.9}$$

kde poslední nerovnost platí díky vztahům

$$\alpha = \frac{\alpha y_2}{y_2} \leq \frac{\lceil \alpha y_2 \rceil}{y_2} = \frac{x_2}{y_2}.$$

Nyní využijeme toho, že $\frac{x}{y}$ je horní polokonvergent čísla α a použijeme větu 2.17, dle které jde i o dobrou horní aproximaci, a tak dle nerovností (3.9) vyhovuje zlomek $\frac{x_2}{y_2}$ podmínce (2.16), a tak podle věty 2.17 musí platit, že $y_2 > y$ nebo $y = y_2, x = x_2$. Ani jeden z těchto případů však nastat nemůže, neboť díky rovnosti $y = y_1 + y_2$ a $y_1 \in \mathbb{N}$ máme nerovnost $y_2 < y$ a dostali jsme tedy spor, čímž je důkaz této implikace a celé věty 3.5 dokončen. □

Snadno nahlédneme, že důkaz poslední implikace předchozí věty 3.5 bude platný i v případě $\frac{x}{y} = \alpha$. Za těchto podmínek budou všechny nerovnosti ve vztazích (3.9) ve skutečnosti rovnosti, ale nadále bude platit nerovnost $y_2 < y$, čímž bychom dostali spor.

Spojením věty 3.5 a důsledku 3.3 dostáváme charakterizaci nerozložitelných prvků v $F_{\alpha,\beta}$ pomocí horních polokonvergentů čísel α a β, přičemž zde využíváme toho, že věta 3.5 platí, kdybychom místo parametru α uvažovali parametr β. Ještě předtím si však všimneme předpokladu věty 3.5, dle kterého uvažujeme pouze prvky $x, y \in \mathbb{N}$. To však znamená, že jsme zatím neprozkoumali všechny prvky polomřížky E_α, neboť snadno nahlédneme, že pro všechna $x \in \mathbb{N}_0$ platí, že $(x, 0) \in E_\alpha$ (a jedná se o jediné prvky polomřížky E_α s alespoň jednou nekladnou souřadnicí, což se dá nahlédnout z nerovností (3.1)). Pro tyto prvky je však velmi snadno vidět, že jediným nerozložitelným prvkem v E_α (a tedy i v $F_{\alpha,\beta}$ dle lemmatu 3.3) je $(1, 0)$. Nyní již zformulujeme důsledek, který tedy charakterizuje nerozložitelné prvky v $F_{\alpha,\beta}$ pomocí horních polokonvergentů čísel α a β, jehož důkaz plyne okamžitě z věty 3.5 a důsledku 3.3.

Důsledek 3.6. *Pro $\alpha, \beta \in \mathbb{R}^+$ a nesoudělná čísla $x, y \in \mathbb{N}$ je $(x, y) \in F_{\alpha,\beta}$ nerozložitelný prvek v polomřížce $F_{\alpha,\beta}$, právě když nastane jeden z následujících případů:*

a) $(x, y) = (1, 0)$,

b) $\dfrac{x}{y}$ *je horní polokonvergent čísla* α,

c) $-\dfrac{x}{y}$ *je horní polokonvergent čísla* β.

Snadno si uvědomíme, že který z případů v předchozím důsledku nastane, záleží pouze na znaménku y: Případ a) nastane, právě když je $y = 0$, případ b) nastane právě když $y > 0$ a případ c) nastane, právě když $y < 0$. Také vidíme, že jednotlivé případy jsou po dvou disjunktní, tedy pro $(x, y) \in P_{F_{\alpha,\beta}}$ nastane právě jeden z případů $a), b), c)$ z důsledku 3.6.

Věta 3.5 má také následující jednoduchý důsledek:

Důsledek 3.7. *Nechť $\alpha \in \mathbb{R}^+$. Poté platí:*

a) Následující podmínky jsou ekvivalentní:

- *Číslo α je iracionální.*
- *Existuje nekonečně mnoho $\alpha-$nerozložitelných přirozených čísel.*
- *Úhlová oblast E_α obsahuje nekonečně mnoho nerozložitelných prvků.*

b) Je-li číslo α racionální, řekněme $\alpha = [a_0, a_1, \ldots, a_k] = \dfrac{p_k}{q_k}$ pro k liché, což můžeme předpokládat díky rovnosti (2.6)*, poté existuje právě $a_1 + a_3 + \ldots + a_k$ $\alpha-$nerozložitelných přirozených čísel (pro k sudé je těchto $\alpha-$nerozložitelných přirozených čísel $a_1 + a_3 + \ldots + a_{k-1}$) a největším z nich je q_k.*

Důkaz. a): Ekvivalence těchto tří podmínek plyne jednoduše z věty 3.5 a toho, že právě iracionální čísla mají nekonečně mnoho horních polokonvergentů.

b): Je-li číslo α racionální, poté je našim úkolem přesně určit počet jeho horních polokonvergentů, poté stačí použít větu 3.5 a budeme hotovi. Tento počet jsme však přesně určili v lemmatu 2.11. Pro určení největšího $\alpha-$nerozložitelného prvku se stačí podívat na nerovnosti (2.2). □

3.2 Nerozložitelné prvky v $\mathcal{O}_K^{+,0}$

V této sekci si ukážeme, že na případ úhlových oblastí, kterým jsme se věnovali v minulé sekci, se dá převést zkoumání totálně nezáporných prvků v reálných kvadratických číselných tělesech, speciálně si ukážeme, že totálně nezáporné prvky, které jsou větší nebo rovny svému konjugátu (tento technický předpoklad bude brzy vysvětlen), tvoří polomřížku v $\mathbb{R}$.

3.2.1 Obecný popis

Nechť $D \neq 1$ je bezčtvercové přirozené číslo, uvažujme reálné kvadratické číselné těleso $K = \mathbb{Q}(\sqrt{D})$ a uvažujme parametry D, α, δ podle tabulky 2.1.

Povšimneme si, že ve větě 2.22 jsme přesně popsali strukturu řetězových zlomků čísla α, čehož v této sekci budeme využívat.

Nyní se již podívejme na totálně nezáporné prvky v $\mathcal{O}_K$: Jedná se o takové prvky $x + y\delta \in \mathbb{Z}[\delta]$, že $x + \delta y \geq 0$ a $x + \delta' y \geq 0$, přičemž tyto dvě podmínky se dají ekvivalentně popsat jako $x \geq -y\delta$ a $x \geq -\delta' y = \alpha y$, neboli

$$\mathcal{O}_K^{+,0} = \{x + y\delta \in \mathbb{Z}[\delta] \mid x \geq -\delta y, x \geq \alpha y\}, \tag{3.10}$$

což neznamená nic jiného, než

$$\mathcal{O}_K^{+,0} = \{x + y\delta \mid (x, y) \in F_{\alpha,\delta}\}. \tag{3.11}$$

Z popisu $\mathcal{O}_K^{+,0}$ ve vztazích (3.10) a (3.11) je však vidět, že samotný okruh $\mathcal{O}_K^{+,0}$ netvoří polomřížku v $\mathbb{R}$, nejedná se totiž o diskrétní množinu (diskrétnost množiny, tedy existenci hromadných bodů zkoumáme vzhledem ke standardní topologii na $\mathbb{R}$), neboť pro všechna $x \in \mathbb{N}$ existuje $y \in \mathbb{Z}$ tak, že $(x, y) \in F_{\alpha,\delta}$ a zároveň $0 \leq x + y\delta \leq \lceil \delta \rceil$ (pro $x \leq \lceil \delta \rceil$ můžeme volit $y = 0$, pro $x > \lceil \delta \rceil$ zvolíme $y < 0$ tak, aby $0 \leq x + y\delta \leq \lceil \delta \rceil$), z čehož plyne, že $\mathcal{O}_K^{+,0}$ má nekonečný průnik s krychlí $K(\lceil \delta \rceil)$, což je kompaktní množina, a proto z tvrzení 1.3 nepřímo plyne, že množina $\mathcal{O}_K^{+,0}$ není diskrétní.

Abychom zkonstruovali z $\mathcal{O}_K^{+,0}$ polomřížku v $\mathbb{R}$, musíme se omezit na takové totálně nezáporné prvky, pro které platí, že jsou větší nebo rovny svému konjugátu. Pro takový prvek $x + y\delta$ to konkrétně znamená, že

$$0 \leq (x + y\delta) - (x + y\delta)' = y(\delta - \delta'). \tag{3.12}$$

Jistě platí, že $(\delta - \delta') \geq 0$, neboť $\delta > 0$ a $\delta' = -\delta < 0$. Z toho a vztahů (3.12) plyne, že vztah $0 \leq (x + y\delta) - (x + y\delta)'$ je ekvivalentní vztahu $y > 0$. Označme

$$S_K := \{x + y\delta \in \mathcal{O}_K^{+,0} \mid x + y\delta \geq x + y\delta'\} = \{x + y\delta \in \mathcal{O}_K^{+,0} \mid y \geq 0\}.$$

Spolu s použitím rovnosti (3.11) dostáváme následující popis:

$$S_K = \{x + y\delta \mid (x, y) \in F_{\alpha,\delta}, y \geq 0\} = \{x + y\delta \mid (x, y) \in E_\alpha\}. \tag{3.13}$$

Snadno nahlédneme, že právě zadefinovaná množina S_K tvoří monoid. Zároveň se opravdu jedná o polomřížku v $\mathbb{R}$, diskrétnost se dá rutinně ověřit pomocí tvrzení 1.5. Připomeňme, že celý tento monoid leží v kuželi $\mathbb{R}_0^+$.

Polomřížka S_K je izomorfní polomřížce E_α, příslušným izomorfismem je zobrazení $\varphi\colon E_\alpha \to S_K$, $\varphi(x, y) = x + y\delta$. Tento izomorfismus je rovněž izomorfismem monoidů $\mathcal{O}_K^{+,0}$ a $F_{\alpha,\beta}$, nicméně pouze $F_{\alpha,\beta}$ tvoří polomřížku. Polomřížky S_K a E_α jsou si tedy izomorfní, i když každá z těchto množin tvoří polomřížku v jiné dimenzi.

Hned za definicí 1.13 nerozložitelného prvku jsme si všimli, že izomorfismus monoidů zachovává nerozložitelné prvky, díky čemuž můžeme popsat nerozložitelné prvky polomřížky S_K a okruhu $\mathcal{O}_K^{+,0}$ pomocí nerozložitelných prvků polomřížek E_α a $F_{\alpha,\beta}$. Zároveň víme, jak vypadají nerozložitelné prvky v E_α a $F_{\alpha,\beta}$, to známe z minulé sekce.

Použitím věty 3.5 popíšeme díky izomorfismu φ všechny nerozložitelné prvky v polomřížce S_K pomocí horních polokonvergentů čísla α. Zároveň si uvědomíme, že pomocí nerozložitelných prvků polomřížky S_K velmi snadno určíme i nerozložitelné prvky okruhu $\mathcal{O}_K^{+,0}$ díky definici množiny S_K a pozorování, že libovolný prvek je nerozložitelný v $\mathcal{O}_K^{+,0}$, právě když je jeho konjugát nerozložitelný prvek v $\mathcal{O}_K^{+,0}$. Popišme tedy tímto způsobem všechny nerozložitelné prvky v okruhu $\mathcal{O}_K^{+,0}$ v následující větě:

Věta 3.8 ([3], Theorem 2)**.** *Pro hodnoty D, δ a $\alpha = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo a $K = \mathbb{Q}(\sqrt{D})$ je prvek $\beta \in \mathcal{O}_K^{+,0}$ nerozložitelný v $\mathcal{O}_K^{+,0}$, právě když nastane jeden z následujících případů:*

a) $\beta = 1$,

b) $\beta = x + y\delta$ nebo $\beta = x + y\delta'$ pro $x = \lceil \alpha y \rceil$ a $y \in \mathbb{N}$, kde y je α-nerozložitelný prvek.

Pomocí řetězového zlomku čísla $\alpha = [a_0, a_1, \ldots]$ se všechny nerozložitelné prvky monoidu $\mathcal{O}_K^{+,0}$ dají popsat jako $p_{k,j} + q_{k,j}\delta$ a $p_{k,j} + q_{k,j}\delta'$, kde $k \geq -1$ je liché číslo a $0 \leq j < a_{k+2}$.

Případy *a*) a *b*) v předchozí větě jsou zřejmě disjunktní. Předchozí větu bychom rovněž mohli dokázat i bez pozorování, že konjugace zachovává nerozložitelnost, a to přímo z důsledku 3.6, kde bychom zkoumali i horní polokonvergenty čísla δ. ty se však dají snadno odvodit z horních polokonvergentů čísla α, nicméně by bylo potřeba udělat jistý výpočet a zvlášť vyřešit lehce obtížnější případ $D \equiv 1 \bmod 4$, kde $\alpha \neq \delta$.

3.2.2 Popis až na násobení čtvercem jednotky - první důkaz

V této části této sekce představíme jednodušší popis nerozložitelných prvků v $\mathcal{O}_K^{+,0}$, těchto nerozložitelných prvků totiž bude konečně mnoho, až na přenásobení mocninami čtverce nějaké jednotky. Budeme postupovat podle 4. kapitoly článku [3].

Pro celou tuto část této sekce budeme uvažovat parametry D, α a δ podle tabulky 2.1, a dále budeme uvažovat $K = \mathbb{Q}(\sqrt{D})$ a jednotku $\varepsilon = l + m\delta$ v $\mathcal{O}_K$, popis těchto jednotek přesně pomocí parametrů $l, m \in \mathbb{N}$ jsme zmínili v tvrzení 2.33 (neplatí tedy, že příslušná jednotka je nutně fundamentální, jinými slovy pro $\varepsilon = p_{k-1} + q_{k-1}\delta$ nemusíme volit k minimální možné). Snadno si uvědomíme, že pro $z \in \mathbb{Z}$ je $\beta \in \mathcal{O}_K^{+,0}$ nerozložitelný prvek v $\mathcal{O}_K^{+,0}$, právě když je prvek $\varepsilon^{2z}\beta$ nerozložitelný v $\mathcal{O}_K^{+,0}$. Smysl přenásobení čtvercem nějaké jednotky bude vysvětlen následujícím lemmatem:

Lemma 3.9. *Pro libovolný nenulový prvek $\beta \in \mathcal{O}_K^{+,0}$ a jednotku $\varepsilon \in \mathcal{O}_K$, jenž splňuje vztah $\varepsilon > 1$ (ε je tedy tvaru $l + m\delta$ pro $l, m \in \mathbb{N}$) platí, že existuje právě jedno $z \in \mathbb{Z}$ tak, že prvek $\beta_z := \varepsilon^{2z}\beta$ vyhovuje podmínce*

$$\varepsilon^{-2} < \frac{\beta_z}{\beta_z'} \leq \varepsilon^2. \tag{3.14}$$

Důkaz. Začneme úpravou výrazu $\frac{\beta_z}{\beta'_z}$, přičemž využijeme fakt, že jednotky mají normu ± 1, a proto $\varepsilon = \frac{N(\varepsilon)}{\varepsilon'}$:

$$\frac{\beta_z}{\beta'_z} = \frac{\varepsilon^{2z}\beta}{(\varepsilon^{2z}\beta)'} = \frac{\beta}{\beta'}\left(\frac{\varepsilon}{\varepsilon'}\right)^{2z} = \frac{\beta}{\beta'}(N(\varepsilon)\varepsilon^2)^{2z} = \frac{\beta}{\beta'}\varepsilon^{4z}.$$

Dosaďme právě získaný vztah do nerovnic (3.14), o kterých chceme dokázat, že platí pro právě jedno $z \in \mathbb{Z}$. Po vynásobení výrazem ε^{-4z} dostáváme:

$$\varepsilon^{-4z-2} < \frac{\beta}{\beta'} \leq \varepsilon^{-4z+2}. \tag{3.15}$$

Nyní stačí nahlédnout, že nerovnice (3.15) (a tedy i (3.14)) platí pro právě jedno z. Vidíme, že výraz $\frac{\beta}{\beta'}$ nezávisí na z, je to tedy nějaké fixní kladné číslo. Zároveň vidíme, že posloupnost polouzavřených intervalů $((\varepsilon^{-4z-2}, \varepsilon^{-4z+2}])_{z\in\mathbb{Z}}$ je po dvou disjunktní a pokrývá celé $\mathbb{R}^+$, z čehož dostáváme, že $\frac{\beta}{\beta'}$ leží v právě jednom takovém polouzavřeném intervalu, a tedy i nerovnice (3.15) a (3.14) platí pro právě jedno $z \in \mathbb{Z}$, což jsme chtěli ukázat. □

V předchozím lemmatu jsme zakázali případ $\beta = 0$, neboť v tomto případě není podmínka (3.14) dobře definována. Nicméně požadujeme, aby 0 byla součástí námi zkoumaných množin, a to z důvodu zachování algebraické struktury monoidu, aby zkoumané množiny opravdu tvořily polomřížku.

Díky předchozímu lemmatu se stačí zabývat nerozložitelnými prvky na množině $\left\{\beta \in \mathcal{O}_K^{+,0}, \varepsilon^{-2} < \frac{\beta}{\beta'} \leq \varepsilon^2\right\} \cup \{0\}$ a obdobně jako v minulé části této sekce stačí uvažovat takové totálně nezáporné prvky, které jsou větší nebo rovny svému konjugátu, což nám dává podmínku $\frac{\beta}{\beta'} \geq 1$. Kvůli zachování algebraické struktury monoidu přidáme do zkoumané množiny 0 a budeme se tedy zabývat množinou

$$G_\varepsilon := \left\{\beta \in \mathcal{O}_K^{+,0}, 1 \leq \frac{\beta}{\beta'} \leq \varepsilon^2\right\} \cup \{0\}, \tag{3.16}$$

kde $\varepsilon > 1$ je jednotka okruhu $\mathcal{O}_K$. Nyní ukážeme, že právě zadefinovaná množina tvoří polomřížku v $\mathbb{R}$.

Lemma 3.10. *Pro hodnoty D a δ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo a $K = \mathbb{Q}(\sqrt{D})$, nechť $\varepsilon > 1$ je jednotka okruhu $\mathcal{O}_K$. Množina G_ε, zadefinovaná vztahem v* (3.16)*, tvoří polomřížku v $\mathbb{R}$.*

Důkaz. Jistě platí, že

$$G_\varepsilon \subseteq S_K = \{x + y\delta \in \mathcal{O}_K^{+,0} \mid x + y\delta \geq x + y\delta'\} = \left\{\beta \in \mathcal{O}_K^{+,0}, 1 \leq \frac{\beta}{\beta'}\right\} \cup \{0\},$$

přičemž z minulé části této sekce víme, že množina S_K tvoří polomřížku v $\mathbb{R}$, z čehož plyne, že G_ε je diskrétní množina, která leží v nějakém kuželi. Zároveň přímo z definice v (3.16) vidíme, že G_ε obsahuje nulu i nějaký nenulový prvek,

proto nám stačí ukázat, že G_ε tvoří pologrupu (dokonce se bude jednat o podmonoid S_K), neboli chceme ukázat uzavřenost množiny G_ε na sčítání, mějme tedy libovolné prvky $\beta, \gamma \in G_\varepsilon$ a chceme ukázat, že $\beta + \gamma \in G_\varepsilon$, čili chceme ověřit nerovnosti

$$1 \leq \frac{\beta + \gamma}{(\beta + \gamma)'} \leq \varepsilon^2. \tag{3.17}$$

Platnost nerovnosti $1 \leq \frac{\beta + \gamma}{(\beta + \gamma)'}$ plyne z toho, že S_K je pologrupa (čili $\beta' \leq \beta$ a $\gamma' \leq \gamma$), stačí se tedy zabývat druhou požadovanou nerovností $\frac{\beta + \gamma}{(\beta + \gamma)'} \leq \varepsilon^2$.

Nechť $\beta = x_1 + y_1\delta \in G_\varepsilon$ pro $x_1, y_1 \in \mathbb{Z}$ a upravme nerovnost $\frac{\beta}{\beta'} \leq \varepsilon^2$, která platí:

$$\frac{x_1 + y_1\delta}{(x_1 + y_1\delta)'} \leq \varepsilon^2 \Leftrightarrow x_1 + y_1\delta \leq \varepsilon^2(x_1 + y_1\delta') \Leftrightarrow y_1(\delta - \delta'\varepsilon^2) \leq x_1(\varepsilon^2 - 1) \Leftrightarrow$$

$$\Leftrightarrow \frac{\delta - \delta'\varepsilon^2}{\varepsilon^2 - 1} y_1 \leq x_1.$$

Označme

$$b_\varepsilon := \frac{\delta - \delta'\varepsilon^2}{\varepsilon^2 - 1}. \tag{3.18}$$

Tento parametr b_ε, závisející pouze na ε a δ bude důležitý pro celý zbytek této části této sekce a později se mu budeme podrobněji věnovat. Platí tedy nerovnost

$$b_\varepsilon y_1 \leq x_1, \tag{3.19}$$

a stejné úpravy můžeme udělat i s prvkem $\gamma = x_2 + y_2\delta$ pro $x_2, y_2 \in \mathbb{Z}$, proto

$$b_\varepsilon y_2 \leq x_2, \tag{3.20}$$

a našim cílem je ukázat platnost nerovnosti

$$b_\varepsilon(y_1 + y_2) \leq x_1 + x_2,$$

ta však snadno plyne z nerovností (3.19) a (3.20). Tím jsme tedy ověřili i vztah (3.17), díky čemuž je G_ε opravdu pologrupa a tedy i polomřížka v $\mathbb{R}$, čímž je lemma dokázané. □

Ekvivalentní úpravy, které jsme využili v důkazu předchozího lemmatu, budou využity i při důkazu dalšího lemmatu, které ještě více poukáže na důležitost parametru b_ε a zároveň se podíváme na vlastnosti tohoto parametru, konkrétně půjde o jeho vyjádření v závislosti pouze na jednotce ε a o jeho řetězový zlomek. Zároveň v tomto důkazu budeme dělat výpočty zvlášť pro případy $D \equiv 1 \bmod 4$ a $D \equiv 2, 3 \bmod 4$.

Lemma 3.11 ([3], Lemma 4)**.** *Pro hodnoty D, δ a α z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo a $K = \mathbb{Q}(\sqrt{D})$, nechť $\varepsilon = l + m\delta$ je jednotka okruhu $\mathcal{O}_K$, kde $l, m \in \mathbb{N}$. Poté platí*

$$G_\varepsilon = \{x + y\delta \mid (x, y) \in E_{b_\varepsilon}\}, \tag{3.21}$$

kde polomřížka G_ε byla zadefinována vztahem v (3.16)*, čili polomřížka G_ε je izomorfní polomřížce E_{b_ε}, kde parametr $b_\varepsilon = \dfrac{\delta - \delta'\varepsilon^2}{\varepsilon^2 - 1}$, který jsme zadefinovali vztahem v* (3.18)*, je roven*

$$b_\varepsilon = \begin{cases} \dfrac{l}{m}, & \text{pokud } N(\varepsilon) = 1, \\ \dfrac{Dm}{l}, & \text{pokud } N(\varepsilon) = -1 \text{ a } D \equiv 2, 3 \bmod 4, \\ \dfrac{\frac{m(D-1)}{2} - l}{2l + m}, & \text{pokud } N(\varepsilon) = -1 \text{ a } D \equiv 1 \bmod 4, \end{cases}$$

speciálně vidíme, že $b_\varepsilon \in \mathbb{Q}$.

Důkaz. Začneme důkazem rovnosti (3.21). K tomu si stačí uvědomit dvě ekvivalence nerovností:

Zaprvé, pro libovolný nenulový prvek $\beta = x + y\delta \in \mathcal{O}_K$, kde $x, y \in \mathbb{Z}$ platí, že nerovnost $1 \leq \dfrac{\beta}{\beta'}$ je ekvivalentní s nerovností $y \geq 0$, což již známe.

Zadruhé, za stejných předpokladů, nerovnost $\varepsilon^2 \geq \dfrac{\beta}{\beta'}$ je ekvivalentní s nerovností $x \geq yb_\varepsilon$, což jsme si ukázali pro prvky G_ε v rámci minulého lemmatu 3.10 pro prvky G_ε, nicméně tyto ekvivalence platí obecně pro všechny totálně nezáporné prvky $x + y\delta$.

Díky těmto dvěma ekvivalencím nerovností dostáváme opravdu rovnost (3.21), neboť zkoumané nerovnosti definují polomřížky G_ε a E_{b_ε}. Izomorfismem mezi těmito dvěma polomřížkami je souřadnicový izomorfismus vzhledem k celistvé bázi $(1, \delta)$, tedy zobrazení $(x, y) \to x + y\delta$, stejný izomorfismus jako byl izomorfismus polomřížek S_K a E_α v minulé části této sekce. Nyní se již podíváme na vyjádření parametru b_ε dosazením $\varepsilon = l + m\delta$ a odlišíme 2 případy podle toho, jakou normu má jednotka ε.

Nejprve předpokládejme, že $N(\varepsilon) = 1$. Poté platí:

$$b_\varepsilon = \frac{\delta - \delta'\varepsilon^2}{\varepsilon^2 - 1}\frac{\varepsilon'}{\varepsilon'} \overset{\varepsilon\varepsilon'=1}{=} \frac{\delta\varepsilon' - \delta'\varepsilon}{\varepsilon - \varepsilon'} = \frac{\delta(l + m\delta') - \delta'(l + m\delta)}{l + m\delta - l - m\delta'} = \frac{\delta l - \delta' l}{\delta m - \delta' m} = \frac{l}{m},$$

čímž je tento případ vyřešen, proto nyní zkoumejme případ $N(\varepsilon) = -1$ a postupujme podobně:

$$b_\varepsilon = \frac{(\delta - \delta'\varepsilon^2)(-\varepsilon')}{(\varepsilon^2 - 1)(-\varepsilon')} \overset{\varepsilon\varepsilon'=-1}{=} \frac{-\delta\varepsilon' - \delta'\varepsilon}{\varepsilon + \varepsilon'} = -\frac{\delta(l + m\delta') + \delta'(l + m\delta)}{l + m\delta + l + m\delta'} =$$

$$= -\frac{l(\delta + \delta') + 2m\delta\delta'}{2l + m(\delta + \delta')} = -\frac{Tr(\delta)l + N(\delta)2m}{2l + Tr(\delta)m}.$$

Dosazením hodnot $Tr(\delta) = 0$ a $N(\delta) = -D$ pro případ $D \equiv 2, 3 \bmod 4$, stejně jako $Tr(\delta) = 1$ a $N(\delta) = \dfrac{1 - D}{4}$ pro případ $D \equiv 1 \bmod 4$ dostaneme přesně požadované výsledky, čímž je toto lemma dokázané. □

Podotkněme, že v článku [3] je v rámci tohoto lemmatu zároveň vysloveně dokázána identita $b_\varepsilon = b'_\varepsilon$, která pochopitelně platí, ale zároveň plyne z výpočtu b_ε přes parametry l, m, D, neboť všechny tyto parametry jsou přirozená čísla. Zároveň je v článku [3] vysloveně dokázán odhad $b_\varepsilon > \alpha$, který opět platí, nicméně plyne z toho, že $G_\varepsilon \subseteq S_K$, a tedy $E_{b_\varepsilon} \simeq G_\varepsilon \subseteq S_K \simeq E_\alpha$ a nyní stačí použít definici úhlových oblastí. Důkaz lemmatu 3.11 byl tedy lehce zjednodušen oproti důkazu Lemmatu 4 z článku [3].

V následujícím lemmatu, kde prozkoumáme rozvoj parametru b_ε do řetězového zlomku, využijeme přesnějšího popisu jednotek okruhu $\mathcal{O}_K^{+,0}$, který známe z tvrzení 2.33. Toto lemma je dokázané i v článku [3] v rámci Theorem 4, my však tuto část o řetězovém zlomku čísla b_ε nyní uvedeme zvlášť v následujícím lemmatu, přičemž hlavní výsledek Theorem 4 z článku [3] bude zde uveden jako věta 3.13.

Lemma 3.12. *Pro parametry D, δ a $\alpha = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo, dále nechť $K = \mathbb{Q}(\sqrt{D})$, uvažujme jednotku $\varepsilon = p_{k-1} + q_{k-1}\delta \in \mathcal{O}_K$ (tato jednotka nemusí být fundamentální, tedy parametr k nevolíme minimální možný). Pro parametr $b_\varepsilon := \dfrac{\delta - \delta'\varepsilon^2}{\varepsilon^2 - 1}$ platí, že*

$$b_\varepsilon = \begin{cases} [a_0, a_1, \ldots, a_{k-1}], & \text{pokud } N(\varepsilon) = 1, \\ [a_0, a_1, \ldots, a_{k-1}, a_0], & \text{pokud } N(\varepsilon) = -1 \text{ a } D \equiv 2, 3 \bmod 4, \\ [a_0, a_1, \ldots, a_{k-1}, a_0, 1, 1], & \text{pokud } N(\varepsilon) = -1 \text{ a } D \equiv 1 \bmod 4. \end{cases}$$

Důkaz. Nejprve se budeme zabývat jednoduchým případem $N(\varepsilon) = 1$. Z lemmatu 3.11 spolu s tvarem jednotky ε dostáváme vztah $b_\varepsilon = \dfrac{p_{k-1}}{q_{k-1}} = [a_0, a_1, \ldots, a_{k-1}]$.

Nyní zkoumejme případ $N(\varepsilon) = -1$ a nechť $D \equiv 2, 3 \bmod 4$. V tomto případě platí $\delta = \sqrt{D}$ a lemma 3.11 spolu s přesným tvarem jednotky ε nám dává vztah

$$b_\varepsilon = \frac{Dq_{k-1}}{p_{k-1}}. \tag{3.22}$$

Nyní použijeme lemma 2.27, ze kterého dostáváme rovnost

$$p_{k-2,a_0} + q_{k-2,a_0}\delta = \varepsilon(-\delta') = (p_{k-1} + q_{k-1}\sqrt{D})\sqrt{D} = q_{k-1}D + p_{k-1}\delta.$$

Porovnáním celočíselných koeficientů a koeficientů u δ dostaneme rovnosti $q_{k-1}D = p_{k-2,a_0}$ a $p_{k-1} = q_{k-2,a_0}$. Tyto dvě rovnosti dosadíme do vyjádření b_ε ze vztahu (3.22) a dostáváme

$$b_\varepsilon = \frac{p_{k-2,a_0}}{q_{k-2,a_0}} = [a_0, a_1, \ldots, a_{k-1}, a_0],$$

čímž je tento případ vyřešen.

Nyní se stačí zabývat případem, kdy $N(\varepsilon) = -1$ a $D \equiv 1 \bmod 4$. V tomto případě platí $\delta = \dfrac{\sqrt{D}+1}{2}$. V této situaci budeme postupovat lehce jinak, začneme použitím lemmatu 2.27, dle kterého, spolu s využitím snadno ověřitelného vztahu $-\delta' = \delta - 1$, dostáváme:

$$p_{k-2,a_0} + q_{k-2,a_0}\delta = \varepsilon(-\delta') = (p_{k-1} + q_{k-1}\delta)(-\delta') =$$
$$= (p_{k-1}+q_{k-1}\delta)(\delta-1) = q_{k-1}(\delta^2-\delta)-p_{k-1}+p_{k-1}\delta = q_{k-1}(-N(\delta))-p_{k-1}+p_{k-1}\delta =$$
$$= q_{k-1}\frac{D-1}{4} - p_{k-1} + p_{k-1}\delta.$$

Opět porovnáme celočíselné koeficienty a koeficienty u δ a dostaneme rovnost

$$\frac{p_{k-2,a_0}}{q_{k-2,a_0}} = \frac{q_{k-1}\dfrac{D-1}{4} - p_{k-1}}{p_{k-1}} = [a_0, a_1, \ldots, a_{k-1}, a_0]. \tag{3.23}$$

Tento výraz se však nerovná b_ε, pro které dle lemmatu 3.11 opět spolu s použitím tvaru jednotky platí vztah

$$b_\varepsilon = \frac{\dfrac{q_{k-1}(D-1)}{2} - p_{k-1}}{2p_{k-1} + q_{k-1}}. \tag{3.24}$$

Ukážeme, že platí vztah $b_\varepsilon = [a_0, a_1, \ldots, a_{k-1}, a_0, 1, 1]$, což ověříme tím, že spočítáme čitatele a jmenovatele řetězového zlomku na pravé straně požadované rovnosti a výsledky porovnáme s rovností (3.24). Pro snadnější převod mezi příslušnými konvergenty a horními polokonvergenty budeme pracovat s řetězovými polynomy $(h_i)_{i=-1}^{\infty}$, které jsme si zavedli v definici 2.3. Začneme aplikováním rovnosti (2.3) na řetězový zlomek $[a_0, a_1, \ldots, a_{k-1}, a_0, 1, 1]$ a dostaneme

$$[a_0, a_1, \ldots, a_{k-1}, a_0, 1, 1] = \frac{h_{k+3}(a_0, a_1, \ldots, a_{k-1}, a_0, 1, 1)}{h_{k+2}(a_1, \ldots, a_{k-1}, a_0, 1, 1)}.$$

Nyní již budeme aplikovat rekurentní definici řetězových polynomů a posléze vztahy z definice 2.4, nejprve na čitatele zkoumaného řetězového zlomku:

$$h_{k+3}(a_0, a_1, \ldots, a_{k-1}, a_0, 1, 1) =$$
$$h_{k+2}(a_0, a_1, \ldots, a_{k-1}, a_0, 1) + h_{k+1}(a_0, a_1, \ldots, a_{k-1}, a_0) =$$
$$2h_{k+1}(a_0, a_1, \ldots, a_{k-1}, a_0) + h_k(a_0, a_1, \ldots, a_{k-1}) = 2p_{k-2,a_0} + p_{k-1} \overset{(3.23)}{=}$$
$$= 2\left(q_{k-1}\frac{D-1}{4} - p_{k-1}\right) + p_{k-1} = q_{k-1}\frac{D-1}{2} - p_{k-1}.$$

Obdobné úpravy nyní uděláme i s jmenovatelem zkoumaného řetězového zlomku:

$$h_{k+2}(a_1, \ldots, a_{k-1}, a_0, 1, 1) =$$
$$h_{k+1}(a_1, \ldots, a_{k-1}, a_0, 1) + h_k(a_1, \ldots, a_{k-1}, a_0) =$$
$$2h_k(a_1, \ldots, a_{k-1}, a_0) + h_{k-1}(a_1, \ldots, a_{k-1}) = 2q_{k-2,a_0} + q_{k-1} \overset{(3.23)}{=}$$
$$= 2p_{k-1} + q_{k-1}.$$

Právě jsme tedy spočítali, že

$$[a_0, a_1, \ldots, a_{k-1}, a_0, 1, 1] = \frac{h_{k+3}(a_0, a_1, \ldots, a_{k-1}, a_0, 1, 1)}{h_{k+2}(a_1, \ldots, a_{k-1}, a_0, 1, 1)} = \frac{q_{k-1}\dfrac{D-1}{2} - p_{k-1}}{2p_{k-1} + q_{k-1}},$$

což dle rovnosti (3.24) je právě b_ε. Tím byl důkaz tohoto lemmatu dokončen. □

Nyní tedy máme popsanou strukturu polomřížky G_ε, která je tedy izomorfní úhlové oblasti E_{b_ε} a zároveň máme dostatečně prozkoumané i vlastnosti tohoto parametru b_ε. Podívejme se na nerozložitelné prvky této polomřížky. Pomocí věty 3.5 můžeme tyto nerozložitelné prvky popsat pomocí horních polokonvergentů čísla $b_\varepsilon = \dfrac{\delta - \delta'\varepsilon^2}{\varepsilon^2 - 1}$, toto číslo je však racionální, a tak díky důsledku 3.7 je těchto nerozložitelných prvků pouze konečně mnoho. Položme si otázku, zda-li bychom pomocí nerozložitelných prvků polomřížky G_ε nemohli popsat i nerozložitelné prvky polomřížky S_K, respektive monoidu $\mathcal{O}_K^{+,0}$.

Jelikož $G_\varepsilon \subseteq S_K$, tak všechny nerozložitelné prvky polomřížky S_K jsou nerozložitelné i v G_ε. Zároveň, každý prvek S_K patří po přenásobení jednotkou ε^{2z} pro vhodné $z \in \mathbb{Z}$ do G_ε, díky čemuž si stačí uvědomit, které nerozložitelné prvky v G_ε zůstanou nerozložitelné i v S_K, pomocí těchto prvků totiž popíšeme všechny nerozložitelné prvky v S_K, po konjugaci a po přenásobení ε^{2z} tím popíšeme i všechny nerozložitelné prvky okruhu $\mathcal{O}_K^{+,0}$.

Ukážeme, že tuto vlastnost mají všechny nerozložitelné prvky polomřížky G_ε, kromě případu $D \equiv 1 \bmod 4$ a zároveň $N(\varepsilon) = -1$, kde bude jedna výjimka. Podrobněji si toto tvrzení vyslovíme a dokážeme v následující větě:

Věta 3.13 ([3], Theorem 4)**.** *Pro parametry D, δ a $\alpha = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo a $K = \mathbb{Q}(\sqrt{D})$, uvažujme jednotku $\varepsilon = p_{k-1} + q_{k-1}\delta \in \mathcal{O}_K$ (tato jednotka nemusí být fundamentální, tedy parametr k nevolíme minimální možný). Nechť $\beta \in G_\varepsilon$ je nerozložitelný prvek v G_ε. Poté je β nerozložitelný prvek v S_K, právě když nenastane případ $N(\varepsilon) = -1$, $D \equiv 1 \bmod 4$ a zároveň $\beta = q_{k-1}\dfrac{D-1}{2} - p_{k-1} + (2p_{k-1} + q_{k-1})\delta$.*

Důkaz. Důkaz je založen na porovnání horních polokonvergentů čísla b_ε s horními polokonvergenty čísla α, neboť horní polokonvergenty odpovídají nerozložitelným prvkům ve smyslu věty 3.5.

Nejprve se budeme zabývat případem $N(\varepsilon) = 1$. Z lemmatu 2.34 plyne, že k je nutně sudé (po použití vztahu $\alpha = -\delta'$) a z lemmatu 3.12 dostáváme vztah $b_\varepsilon = [a_0, a_1, \ldots, a_{k-1}]$. Vzhledem k paritě k však toto znamená, že b_ε je horní polokonvergent čísla α, a tedy každý horní polokonvergent čísla b_ε je zároveň horním polokonvergentem čísla α. Dvojitým použitím věty 3.5 tedy dostaneme, že každý nerozložitelný prvek polomřížky G_ε je zároveň nerozložitelným prvkem polomřížky S_K, což jsme v tomto případě chtěli ukázat.

Nyní se zbývá zabývat případem, kdy $N(\varepsilon) = -1$ a dle lemmatu 2.34 je k liché. Opět se podíváme na řetězový zlomek čísla b_ε a odlišíme ještě další 2 případy podle toho, čemu je kongruentní D modulo 4.

Nejprve předpokládejme, že $D \equiv 2, 3 \bmod 4$. Opět použijeme lemma 3.12, dle kterého v tomto případě platí $b_\varepsilon = [a_0, a_1, \ldots, a_{k-1}, a_0]$. Vzhledem k tomu, že k je liché, opět dostáváme, že b_ε je horní polokonvergent čísla α (připomeňme, že $a_0 < a_k = 2a_0$) a jsme v situaci známé z případu $N(\varepsilon) = 1$, čili i v tomto případě platí, že každý nerozložitelný prvek polomřížky G_ε je zároveň nerozložitelný i v polomřížce S_K, což uzavírá případ $D \equiv 2, 3 \bmod 4$.

Zbývá vyřešit poslední situaci, a to když $N(\varepsilon) = -1$ (a tedy k je stále liché dle lemmatu 2.34), a zároveň $D \equiv 1 \bmod 4$. Nyní podle lemmatu 3.12 platí $b_\varepsilon = [a_0, a_1, \ldots, a_{k-1}, a_0, 1, 1]$. Jelikož k je liché, tak v tuto chvíli vidíme, že každý

horní polokonvergent čísla b_ε, která je různá od b_ε, je zároveň horním polokonvergentem čísla α. Samotné číslo b_ε není v tomto případě horní polokonvergent čísla α, a tak opakovaně aplikujeme větu 3.5 a dostaneme, že každý nerozložitelný prvek v polomřížce G_ε je zároveň nerozložitelný i v polomřížce S_K s jedinou výjimkou, kterou je prvek odpovídající b_ε, kterým dle izomorfismu mezi G_ε a E_{b_ε} je prvek $q_{k-1}\dfrac{D-1}{2} - p_{k-1} + (2p_{k-1} + q_{k-1})\delta$, což přesně odpovídá tomu, co jsme chtěli ukázat, tím je důkaz této věty dokončen. □

Na závěr této části využijeme dosažených výsledků k přesnému popisu všech nerozložitelných prvků, kterých je tedy konečně mnoho až na přenásobení jednotkami ε^{2z}, přičemž využijeme přesný tvar horních polokonvergentů čísla α. Také se vrátíme ke značení γ_t a $\gamma_{t,j}$ z definice 2.24.

Důsledek 3.14. *Pro parametry D, δ a $\alpha = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo a $K = \mathbb{Q}(\sqrt{D})$, uvažujme jednotku $\varepsilon = p_{k-1} + q_{k-1}\delta \in \mathcal{O}_K$ (tato jednotka nemusí být fundamentální, tedy parametr k nevolíme minimální možný). Označme γ_t a $\gamma_{t,j}$ podle rovností* (2.25) *a* (2.26)*. Všechny nerozložitelné prvky okruhu $\mathcal{O}_K^{+,0}$ jsou právě prvky tvaru*

$$\varepsilon^{2z}\gamma_{t,j},$$

nebo

$$\varepsilon^{2z}\gamma'_{t,j},$$

kde $z, t, j \in \mathbb{Z}$, t je liché číslo a dále $-1 \leq t \leq k-1$ a $0 \leq j < a_{t+2}$, přičemž všechny povolené indexy t, j jsou uvedeny v následující tabulce:

Tabulka 3.1: Povolené indexy t, j

t	j
$-1 \leq t \leq k-3$	$0 \leq j < a_{t+2}$
$t = k-2$	$0 \leq j \leq a_0$
$t = k-1$	$j = 0$

Jinými slovy, pro k liché a $t = k-2$ zároveň musí platit $j \leq a_0$, naopak je-li k sudé, tak pro případ $t = k-1$ nutně požadujeme $j = 0$.

Důkaz. Stačí ukázat, že všechny nerozložitelné prvky v $\mathcal{O}_K^{+,0}$, které zároveň patří do G_ε, jsou právě prvky $\gamma_{t,j}$ a jejich konjugáty, kde t je liché číslo vyhovující podmínce $-1 \leq t \leq k-1$ a $0 \leq j < a_{t+2}$, přičemž pro případ $t = k-2$ zároveň musí platit $j \leq a_0$ a pro $t = k-1$ nutně máme $j = 0$. Jelikož $G_\varepsilon \simeq E_{b_\varepsilon}$, tak všechny nerozložitelné prvky v G_ε, různé od 1, jsou podle věty 3.5 právě prvky tvaru $x + y\delta$, kde $\dfrac{x}{y}$ je horní polokonvergent čísla b_ε. Jelikož $\gamma_{t,j} = p_{t,j} + q_{t,j}\delta$, tak vidíme, že nás zajímají polokonvergenty tvaru $\dfrac{p_{t,j}}{q_{t,j}}$.

V předchozí větě 3.13 jsme odvodili tvar řetězového zlomku racionálního čísla

b_ε, ze kterého vidíme, že horní polokonvergenty čísla b_ε jsou opravdu tvaru $\frac{p_{t,j}}{q_{t,j}}$ kde t je liché číslo vyhovující podmínce $-1 \leq t \leq k-1$ a $0 \leq j < a_{t+2}$, přičemž pro případ $t = k-2$ zároveň musí platit $j \leq a_0$, pro případ $t = k-1$ nutně platí $j = 0$ a pro $t = -1$ naopak máme $j \neq 0$, nicméně případ $t = -1$ a $j = 0$ odpovídá nerozložitelnému prvku 1, proto při výčtu nerozložitelných prvků okruhu $\mathcal{O}_K^{+,0}$ nemusíme tento případ zakazovat, čímž byl důkaz tohoto důsledku dokončen. □

Nyní chceme pomocí počtu horních polokonvergentů čísla b_ε určit počet nerozložitelných prvků okruhu $\mathcal{O}_K^{+,0}$, až na násobení ε^{2z}. K určení počtu horních polokonvergentů čísla α budeme potřebovat lemma 2.11 a přesný tvar řetězového zlomku čísla b_ε, který jsme určili ve větě 3.13. Řetězový zlomek čísla b_ε vypadá podle věty 3.13 následovně:

$$b_\varepsilon = \begin{cases} [a_0, a_1, \ldots, a_{k-1}], & \text{pokud } N(\varepsilon) = 1, \\ [a_0, a_1, \ldots, a_{k-1}, a_0], & \text{pokud } N(\varepsilon) = -1 \text{ a } D \equiv 2, 3 \bmod 4, \\ [a_0, a_1, \ldots, a_{k-1}, a_0, 1, 1], & \text{pokud } N(\varepsilon) = -1 \text{ a } D \equiv 1 \bmod 4. \end{cases}$$

Počet nerozložitelných prvků okruhu $\mathcal{O}_K^{+,0}$, až na násobení ε^{2z}, dostaneme tak, že počet horních polokonvergentů čísla b_ε vynásobíme 2 (protože za každý horní polokonvergent $\frac{x}{y}$ čísla α máme nerozložitelné prvky $x + y\delta$ a $x + y\delta'$), a k výslednému počtu přičteme 1 za nerozložitelný prvek 1, který nemůžeme dostat pohledem na horní polokonvergenty čísla α. Počet horních polokonvergentů čísla α určíme podle lemmatu 2.11 a celkově se dostaneme k následujícímu počtu nerozložitelných prvků v $\mathcal{O}_K^{+,0}$, až na násobení ε^{2z}:

$$\begin{cases} 2(a_1 + a_3 + \ldots + a_{k-1}) + 1, & \text{pokud } N(\varepsilon) = 1, \\ 2(a_1 + a_3 + \ldots + a_{k-2} + a_0) + 1, & \text{pokud } N(\varepsilon) = -1 \text{ a } D \equiv 2, 3 \bmod 4, \\ 2(a_1 + a_3 + \ldots + a_{k-2} + a_0) + 1, & \text{pokud } N(\varepsilon) = -1 \text{ a } D \equiv 1 \bmod 4, \end{cases}$$

kde v posledním případě navíc využíváme toho, že b_ε v tomto případě není horní polokonvergent čísla α. Jinými slovy, v případě $N(\varepsilon) = -1$ a $D \equiv 1 \bmod 4$ má parametr b_ε celkem $a_1 + a_3 + \ldots + a_{k-2} + a_0 + 1$ horních polokonvergentů, ale jeden z těchto horních polokonvergentů není horním polokonvergentem čísla α (a tímto horním polokonvergentem je samotné číslo b_ε).

3.2.3 Popis až na násobení čtvercem jednotky - druhý důkaz

V této části této sekce provedeme jiný důkaz toho, že popis nerozložitelných prvků v $\mathcal{O}_K^+$ z důsledku 3.14 skutečně odpovídá jejich popisu z věty 3.8. K tomu nebudeme vůbec potřebovat žádné polomřížky, ale přímo ukážeme, že pro parametry D, δ a $\alpha = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo a $K = \mathbb{Q}(\sqrt{D})$, přičemž uvažujeme jednotku $\varepsilon = p_{k-1} + q_{k-1}\delta \in \mathcal{O}_K$

(tato jednotka nemusí být fundamentální, tedy parametr k nevolíme minimální možný). Označme γ_t a $\gamma_{t,j}$ podle rovností (2.25) a (2.26). Poté množina

$$\{\varepsilon^{2z}\gamma_{t,j} \mid z \in \mathbb{Z}, t \equiv 1 \bmod 2, \text{indexy } t,j \text{ dle tabulky 3.1}\} \cup \tag{3.25}$$

$$\cup\{\varepsilon^{2z}\gamma'_{t,j} \mid z \in \mathbb{Z}, t \equiv 1 \bmod 2, \text{indexy } t,j \text{ dle tabulky 3.1}\}, \tag{3.26}$$

je rovna množině

$$\{\gamma_{t,j} \mid t \geq -1, t \equiv 1 \bmod 2, 0 \leq j < a_{t+2}\} \cup \tag{3.27}$$

$$\cup\{\gamma'_{t,j} \mid t \geq -1, t \equiv 1 \bmod 2, 0 \leq j < a_{t+2}\}. \tag{3.28}$$

Jedinými prostředky, které při důkazu rovnosti těchto množin využijeme, budou tvrzení 2.25 a 2.26. V první řadě si uvědomíme, že stačí pro parametr $z \in \mathbb{Z}$ z rovností (3.25) a (3.26) stačí uvažovat $z \in \mathbb{N}_0$. Platí totiž následující vztahy:

$$\varepsilon^{2(-z)}\gamma_{t,j} = \frac{1}{\varepsilon^{2z}}\gamma_{t,j} = \frac{(\varepsilon')^{2z}}{(\varepsilon\varepsilon')^{2z}}\gamma_{t,j} = \frac{(\varepsilon')^{2z}}{(N(\varepsilon))^{2z}}\gamma_{t,j} = (\varepsilon^{2z})'\gamma_{t,j} = (\varepsilon^{2z}\gamma'_{t,j})',$$

díky čemuž nám stačí ukázat, že pokud v množinách ve vztazích (3.25) a (3.26) navíc přidáme podmínku $z \in \mathbb{N}_0$, tak jejich sjednocením dostaneme přesně množinu ve vztahu (3.27), neboť prvky množiny ze vztahu (3.28) bychom dostali z prvků množin ve vztazích (3.25) a (3.26) pro $z \leq 0$. Začneme zkoumáním množiny zadefinované ve vztahu 3.25, příslušný vztah pro její prvky $\varepsilon^{2z}\gamma_{t,j}$ vyslovíme a dokážeme v následujícím lemmatu:

Lemma 3.15. *Uvažujme parametry D, δ a $\alpha = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo a $K = \mathbb{Q}(\sqrt{D})$, dále uvažujme $z \in \mathbb{N}_0$, jednotku $\varepsilon = p_{k-1} + q_{k-1}\delta \in \mathcal{O}_K$ (tato jednotka nemusí být fundamentální, tedy parametr k nevolíme minimální možný) a parametry t, j podle tabulky 3.1, kde t je navíc liché. Pokud označíme parametry γ_t a $\gamma_{t,j}$ podle rovností* (2.25) *a* (2.26)*, poté platí*

$$\varepsilon^{2z}\gamma_{t,j} = \gamma_{t+2zk,j} \tag{3.29}$$

Důkaz. Po použití rovnosti (2.26) a tvrzení 2.25 platí následující vztahy:

$$\varepsilon^{2z}\gamma_{t,j} \overset{(2.26)}{=} \varepsilon^{2z}\gamma_t + j\varepsilon^{2z}\gamma_{t+1} \overset{2.25}{=} \gamma_{t+2zk} + j\gamma_{t+2zk+1} \overset{(2.26)}{=} \gamma_{t+2zk,j},$$

čímž jsme přesně ukázali rovnost (3.29), tím byl důkaz tohoto lemmatu dokončen. □

Jelikož opakované násobení jednotkou ε^2 nám posouvá index t u výrazu $\gamma_{t,j}$ o $2k$, tak nám stačí ukázat, že prvky $\gamma_{t,j}$ pro t liché, $-1 \leq t < 2k-1$ a $0 \leq j < a_{t+2}$ patří buď do množiny zadefinované ve vztahu (3.25), nebo do množiny zadefinované ve vztahu (3.26). Přímo z definice množiny ve vztahu (3.25) dostáváme, že pro prvky t, j podle tabulky 3.1 patří prvek $\gamma_{t,j}$ právě do této množiny. V tuto chvíli je potřeba ukázat, že pro indexy t, j, kde t je liché, $-1 \leq t < 2t-1$ a $0 \leq j < a_{t+2}$, které nejsou zahrnuty v tabulce 3.1, patří prvek $\gamma_{t,j}$ buď do množiny zadefinované ve vztahu (3.25), nebo do množiny zadefinované ve vztahu

(3.26). Takové indexy t, j, které tedy nevyhovují podmínkám v tabulce 3.1, budeme nadále označovat t_0, j_0 a jejich přípustné hodnoty jsou uvedeny v následující tabulce:

Tabulka 3.2: Hledané indexy t_0, j_0

t_0	j_0
$k \leq t_0 \leq 2k-3$	$0 \leq j_0 < a_{t+2}$
$t_0 = k-1$	$0 < j_0 < a_{t+2}$
$t_0 = k-2$	$a_0 < j_0 < a_{t+2}$

Podle lemmatu 3.15 však zřejmě prvky γ_{t_0,j_0} nemůžou patřit do množiny ve vztahu (3.25), musíme tedy zkoumat množinu zadefinovanou ve vztahu (3.26), tedy musíme zkoumat výraz $\varepsilon^{2z}\gamma'_{t,j}$.

Ukazuje se, že je dostačující zkoumat tento výraz zkoumat pro $z = 1$, neboť již po prvním přenásobení jednotkou ε^2 dostaneme výraz tvaru $\varepsilon^{2z-2}\gamma_{t_0,j_0}$ pro vhodné indexy t_0 a j_0 z tabulky 3.2, čímž se dostaneme do již známé situace z předchozího lemmatu 3.15. Chceme tedy ukázat, že výraz $\varepsilon^2\gamma'_{t,j}$ pro liché t a indexy t, j z tabulky 3.1 je roven nějakému výrazu γ_{t_0,j_0}, kde t_0 je liché a indexy t_0, j_0 odpovídají tabulce 3.2.

Nejprve se budeme věnovat jednoduššímu případu $j = 0$, pro který podle tabulky 3.1 platí $-1 \leq t \leq k-1$ (a stále předpokládáme, že t je liché). Budeme tedy zkoumat výraz $\varepsilon^2\gamma'_t$ a ukážeme, že je roven γ_{2k-t-2}, což pro $-1 \leq t < k-2$ dává přesně potřebné indexy t_0 za podmínky $j_0 = 0$ podle tabulky 3.2, pro $t = k-1$ se bude jednat o téměř triviální rovnost jednotek, která nám však dosvědčuje, že množiny zadefinované ve vztazích (3.25) a (3.26) nejsou disjunktní. Požadovanou rovnost z tohoto odstavce si dokážeme v následujícím lemmatu:

Lemma 3.16. *Uvažujme parametry D, δ a $\alpha = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo a $K = \mathbb{Q}(\sqrt{D})$, dále uvažujme $z \in \mathbb{N}_0$, jednotku $\varepsilon = p_{k-1} + q_{k-1}\delta \in \mathcal{O}_K$ (tato jednotka nemusí být fundamentální, tedy parametr k nevolíme minimální možný) a parametry t, j podle tabulky 3.1, kde t je navíc liché. Pokud označíme parametr γ_t podle rovnosti* (2.25)*, poté platí*

$$\varepsilon^2\gamma'_t = \gamma_{2k-t-2}. \tag{3.30}$$

Důkaz. Požadovaná rovnost (3.30) plyne okamžitě z tvrzení 2.26:

$$\varepsilon^2\gamma'_t = \gamma_{2k-1}\gamma'_t \overset{2.26}{=} (-1)^{t+1}\gamma_{2k-t-2} = \gamma_{2k-t-2},$$

kde v poslední rovnosti jsme využili toho, že t je liché. Tím byl důkaz tohoto lemmatu dokončen. □

V následujícím lemmatu se podíváme na chování výrazu $\varepsilon^2\gamma'_{t,j}$ pro případ $j \neq 0$ a ukážeme, že tím opravdu popíšeme všechny zbylé nerozložitelné prvky, neboť se výraz $\varepsilon^2\gamma'_{t,j}$ bude rovnat $\gamma_{2k-t-4,a_{t+2}-j}$, což nám pro $-1 \leq t \leq k-2$ skutečně popíše všechny prvky γ_{t_0,j_0} dle tabulky 3.2 pro $j_0 \neq 0$:

Lemma 3.17. *Uvažujme parametry D, δ a $\alpha = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo a $K = \mathbb{Q}(\sqrt{D})$, dále uvažujme $z \in \mathbb{N}_0$, jednotku $\varepsilon = p_{k-1} + q_{k-1}\delta \in \mathcal{O}_K$ (tato jednotka nemusí být fundamentální, tedy parametr k nevolíme minimální možný) a parametry t, j podle tabulky 3.1, kde t je navíc liché a $j \neq 0$ (tím pádem rovněž platí $t \leq k-2$, neboť pro případ $t = k-1$ v tabulce 3.1 povolujeme pouze případ $j = 0$). Pokud označíme parametry γ_t a $\gamma_{t,j}$ podle rovností* (2.25) *a* (2.26)*, poté platí*

$$\varepsilon^2 \gamma'_{t,j} = \gamma_{2k-t-4, a_{t+2}-j}. \tag{3.31}$$

Důkaz. Obdobně jako v důkazu předchozího lemmatu budeme využívat tvrzení 2.26, postup bude následující:

$$\varepsilon^2 \gamma'_{t,j} \overset{(2.26)}{=} \gamma_{2k-1}\gamma'_t + j\gamma_{2k-1}\gamma'_{t+1} \overset{2.26}{=} (-1)^{t+1}\gamma_{2k-t-2} + j(-1)^{t+2}\gamma_{2k-t-3} \overset{t \text{ liché}}{=}$$

$$= \gamma_{2k-t-2} - j\gamma_{2k-t-3} = a_{2k-t-2}\gamma_{2k-t-3} + \gamma_{2k-t-4} - j\gamma_{2k-t-3} =$$

$$= \gamma_{2k-t-4} + (a_{2k-t-2} - j)\gamma_{2k-t-3} \overset{(2.26)}{=} \gamma_{2k-t-4, a_{2k-t-2}-j}.$$

V tuto chvíli stačí ukázat rovnost

$$a_{2k-t-2} = a_{t+2}, \tag{3.32}$$

pro všechna možná lichá $t \leq k-2$, přičemž k tomu použijeme, že řetězový zlomek čísla α má periodu délky k (tedy $a_{k+i} = a_i$ pro všechna $i \in \mathbb{N}$) a také symetrii této periody, neboli $a_i = a_{k-i}$ pro všechna i od 1 do $k-1$. Pro $t = k-2$ je rovnost (3.32) triviální, stačí pouze dosadit za t. Pro $t < k-2$ postupujme následovně:

$$a_{2k-t-2} = a_{2k-(t+2)} = a_{k-(t+2)} = a_{t+2},$$

kde ve druhé rovnosti jsme použili fakt, že příslušná perioda má délku k (pro $i = k-(t+2)$) a ve třetí rovnosti jsme využili symetrii této periody (pro $i = t+2$). Tím byla úspěšně rovnost (3.32), čímž jsme přesně ověřili i rovnost (3.31) a důkaz tohoto lemmatu je dokončen. □

Nyní si položme otázku, co nám právě dokázané lemmata říkají o tom, zdali jsou množiny zadefinované ve vztazích (3.25) a (3.26) disjunktní. Pro k sudé jsme si již všimli, že pro případ $t = k-1$ (a tedy i $j = 0$ dle tabulky 3.1) nám lemma 3.16 dává rovnost $\varepsilon^2\gamma'_{k-1} = \gamma_{k-1}$, tento prvek tedy patří do obou množin zadefinovaných ve vztazích (3.25) a (3.26). Pro $t < k-1$ nám lemma 3.16 žádný prvek do průniku zkoumaných množin nepřidá. Co se týká lemmatu 3.17, tak pro $t < k-2$ a $j \neq 0$ žádné prvky do průniku zkoumaných množin nedostaneme, pro $t = k-2$ je situace následující:

$$\varepsilon^2 \gamma'_{k-2,j} = \gamma_{k-2, a_k-j}.$$

Připomeňme, že v tomto případě platí $0 \leq j \leq a_0$ podle tabulky 3.1. Pro $j < a_0$ vždy platí $a_k - j > a_0$, pro $j = a_0$ však dostaneme jeden prvek do průniku množin zadefinovaných ve vztazích (3.25) a (3.26), právě když platí $a_k = 2a_0$, neboli právě když $D \equiv 2, 3 \bmod 4$ podle věty 2.22. Tím jsme prozkoumali všechny prvky množin zadefinovaných ve vztazích (3.25) a (3.26).

Celkově jsme tedy v této části práce došli k následujícímu závěru:

Věta 3.18. *Sjednocení množin ze vztahů* (3.25) *a* (3.26) *je rovno sjednocení množin ze vztahů* (3.27) *a* (3.28). *Navíc, množiny zadefinované ve vztazích* (3.25) *a* (3.26) *jsou disjunktní, právě když je k liché a zároveň $D \equiv 1 \bmod 4$. Pokud tyto množiny nejsou disjunktní, tak jejich průnik je následující:*

$$\begin{cases} \{\varepsilon^{2z}\gamma_{k-1} \mid z \in \mathbb{Z}\}, & \text{pokud } k \text{ je sudé,} \\ \{\varepsilon^{2z}\gamma_{k-2,a_0} \mid z \in \mathbb{Z}\}, & \text{pokud } k \text{ je liché a } D \equiv 2, 3 \bmod 4. \end{cases}$$

4. Odhady na normu nerozložitelných prvků v Minkowského prostoru

V předchozí kapitole jsme dvěma způsoby charakterizovali všechny nerozložitelné prvky v $\mathcal{O}_K^+$ pro K reálné kvadratické číselné těleso, čímž jsme zároveň popsali i nerozložitelné prvky v polomřížce $\sigma(\mathcal{O}_K^{+,0})$, kde σ je Minkowského vnoření, které jsme si představili v sekci 2.4, kde je zároveň vysvětleno, proč tato množina tvoří polomřížku. Monoid $\mathcal{O}_K^{+,0}$ a polomřížka $\sigma(\mathcal{O}_K^{+,0})$ jsou totiž izomorfní, příslušným izomorfismem je právě Minkowského vnoření σ. V této kapitole se budeme zabývat otázkou, jakou normu v Minkowského prostoru mohou nerozložitelné prvky dané polomřížky, přičemž speciální pozornost bude věnována právě polomřížkám $\sigma(\mathcal{O}_K^{+,0})$, dokonce pro K libovolné totálně reálné číselné těleso, ale zároveň pro případ reálných kvadratických číselných těles dosáhneme přesnějších výsledků. Jakou normu v polomřížkách budeme vlastně zkoumat, si nyní zadefinujeme:

Definice 4.1. *Nechť $L \subseteq \mathbb{R}^n$ je polomřížka a uvažujme prvek $\beta = (x_1, x_2, \ldots, x_n)$ polomřížky L.* Normou v polomřížce L *prvku β, kterou značíme $||\beta||_L$, rozumíme číslo $x_1 x_2 \ldots x_n$.*

Zkoumání této normy dává smysl ve všech polomřížkách, nicméně její nejdůležitější význam (a proč se této hodnotě říká norma), pochází z polomřížek $\sigma(\mathcal{O}_K^{+,0})$, kde K je libovolné totálně reálné číselné těleso. V těchto polomřížkách totiž platí, že norma v polomřížce $\sigma(\mathcal{O}_K^{+,0})$ prvku β je přesně norma prvku $\sigma^{-1}(\beta) \in \mathcal{O}_K^{+,0}$, ve smyslu definice normy 2.28 z kontextu algebraické teorie čísel.

Ukážeme si, že v polomřížkách $\sigma(\mathcal{O}_K^{+,0})$ mají všechny nerozložitelné prvky omezenou normu ve své polomřížce, přičemž konstanta omezující tyto normy bude diskriminant číselného tělesa K, který značíme Δ_K a definovali jsme jej v definici 2.32. V případech kvadratických číselných těles ukážeme lepší odhad na tuto normu, přičemž tento odhad bude těsný v případech, kdy okruh $\mathcal{O}_K$ obsahuje jednotku normy -1. Poté si ukážeme příklad polomřížky v libovolné dimenzi, kde budou mít nerozložitelné prvky libovolně velkou normu ve své polomřížce.

4.1 Polomřížky $\sigma(\mathcal{O}_K^{+,0})$

V této sekci se budeme věnovat polomřížkám $\sigma(\mathcal{O}_K^{+,0})$ pro K totálně reálné číselné těleso. Začneme případem reálných kvadratických těles, kterým jsme se věnovali celou minulou kapitolu. Místo normy v polomřížce $\sigma(\mathcal{O}_K^{+,0})$ budeme zkoumat standardní normu v $\mathcal{O}_K^+$, tyto dvě normy si však jsou v tomto případě rovny, a navíc nám situace bez uvažování Minkowského vnoření je povědomá z minulé kapitoly. V následující větě ukážeme, že každý prvek s normou větší než $-N(\delta)$ je nutně rozložitelný v $\mathcal{O}_K^+$, kde budeme používat značení pro α a δ z minulé kapitoly, které si explicitně připomeneme. Navíc ukážeme, že pokud existuje jednotka s normou -1 v $\mathcal{O}_K$, tak daný odhad je těsný.

Věta 4.2 ([3], Theorem 3)**.** *Mějme parametry D, δ a $\alpha = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$ (parametr k nemusí být minimální možný) z tabulky 2.1, kde $D \neq 1$ je bezčtvercové přirozené číslo a $K = \mathbb{Q}(\sqrt{D})$. Dále uvažujme posloupnosti $\{\alpha_i\}_{i=0}^{\infty}$, $\{r_i\}_{i=0}^{\infty}$ a $\{s_i\}_{i=0}^{\infty}$ dle definic ve vztazích (2.5) a (2.44). Uvažujme prvek $\beta = x + y\delta \in \mathcal{O}_K^+$ pro x,y $\in \mathbb{Z}$ takový, že $N(\beta) > -N(\delta)$. Poté je β rozložitelný prvek v $\mathcal{O}_K^+$. Zároveň platí, že pokud existuje v $\mathcal{O}_K$ jednotka s normou -1, pak existuje nerozložitelný prvek v $\mathcal{O}_K^+$ s normou $-N(\delta)$, a proto je v tomto případě daný odhad na normu nerozložitelných prvků těsný.*

Důkaz. Důkaz bude proveden sporem, nechť $\beta = x + y\delta$ je nerozložitelný prvek v $\mathcal{O}_K^+$. Podle věty 3.5 je $\dfrac{x}{y}$ horní polokonvergent čísla α, proto platí vztahy $x = p_{t,j}$ a $y = q_{t,j}$ pro nějaké liché $t \geq -1$ a $0 \leq j < a_{t+2}$. Poté platí následující rovnice:

$$N(\beta) = N(p_{t,j}+q_{t,j}\delta) = N(p_t+jp_{t+1}+q_t\delta+q_{t+1}\delta) = N(p_t+q_t\delta+j(p_{t+1}+q_{t+1}\delta)) =$$

$$\overset{N(\beta)=N(\beta')}{=} N(p_t + q_t\delta' + j(p_{t+1} + q_{t+1}\delta')) \overset{\delta'=-\alpha}{=} N(p_t - q_t\alpha + j(p_{t+1} - q_{t+1}\alpha)) =$$

$$= (p_t - q_t\alpha + j(p_{t+1} - q_{t+1}\alpha))(p_t - q_t\alpha' + j(p_{t+1} - q_{t+1}\alpha')) =$$

$$= N(p_t - q_t\alpha) + j^2N(p_{t+1} - q_{t+1}\alpha) + jTr((p_t - q_t\alpha')(p_{t+1} - q_{t+1}\alpha)) =$$

$$\overset{\text{Lemma 2.34}}{=} (-1)^{t+1}\frac{s_{t+1}}{s_0} + j^2(-1)^{t+2}\frac{s_{t+2}}{s_0} + j(-1)^{t+1}\frac{2r_{t+2}}{s_0} =$$

$$\frac{s_{t+1}}{s_0} - j^2\frac{s_{t+2}}{s_0} + j\frac{2r_{t+2}}{s_0} =: \frac{1}{s_0}f(j).$$

Nyní se zaměřme na funkci $f(j) = -j^2s_{t+2} + 2jr_{t+2} + s_{t+1}$ a dívejme se na ní jako reálnou kvadratickou funkci jedné reálné proměnné j, našim úkolem je určit maximum této funkce na $\mathbb{R}$ a jeho hodnotu, neboť tato hodnota bude horním odhadem pro $N(\beta)$. Toto maximum existuje, neboť kvadratický člen u předpisu funkce f je záporný, k čemuž je potřeba ověřit nerovnost $s_{t+2} > 0$. Tato nerovnost však plyne z lemmatu 2.35, části b), přičemž toto lemma můžeme použít, protože jistě platí $s_0 > 0$ a $r_0 < D$. Proto maximum funkce f existuje a zároveň se ho bude nabývat v jediném bodě lokálního extrému funkce f, čili v jediném bodě, kde má funkce f nulovou první derivaci. Nyní určíme první derivaci funkce f v bodě $j \in \mathbb{R}$:

$$f'(j) = -2js_{t+2} + 2r_{t+2}.$$

Vidíme, že první derivace funkce f je nulová právě v bodě $j = \dfrac{r_{t+2}}{s_{t+2}}$ a proto platí následující odhady:

$$N(\beta) = \frac{1}{s_0}f(j) \leq \frac{1}{s_0}f\left(\frac{r_{t+2}}{s_{t+2}}\right) = \frac{1}{s_0}\left(-\frac{r_{t+2}^2}{s_{t+2}} + 2\frac{r_{t+2}^2}{s_{t+2}} + s_{t+1}\right) =$$

$$\frac{r_{t+2}^2 + s_{t+1}s_{t+2}}{s_0s_{t+2}} \overset{(2.45)}{=} \frac{D}{s_0s_{t+2}}.$$

Jelikož $\beta \in \mathcal{O}_K$, tak $N(\beta) \in \mathbb{Z}$, a proto platí odhad

$$N(\beta) \leq \left\lfloor \frac{D}{s_0s_{t+2}} \right\rfloor, \tag{4.1}$$

díky čemuž nám nyní stačí ukázat platnost odhadu

$$\left\lfloor \frac{D}{s_0 s_{t+2}} \right\rfloor \leq -N(\delta), \tag{4.2}$$

neboť tento odhad nám dá spolu s již ověřeným odhadem (4.1) spor s tím, že $N(\beta) > -N(\delta)$. Pro ověření odhadu (4.2) odlišíme 2 případy podle toho, čemu je D kongruentní modulo 4.

Nejprve předpokládejme, že $D \equiv 2, 3 \bmod 4$. Potom $\delta = \sqrt{D}$, $-N(\delta) = D$ a po dalším použití lemmatu 2.35 části b) (dle kterého s_0 i s_{t+2} jsou kladné) a toho, že funkce dolní celé části je neklesající, dostáváme následující odhad:

$$\left\lfloor \frac{D}{s_0 s_{t+2}} \right\rfloor \leq \lfloor D \rfloor = D = -N(\delta),$$

čímž byl v tomto případě odhad (4.2) ověřen.

Nyní se stačí zabývat případem $D \equiv 1 \bmod 4$. V tomto případě platí

$$\delta = \frac{\sqrt{D}+1}{2}, -N(\delta) = \frac{D-1}{4}, \alpha = \frac{\sqrt{D}-1}{2}, r_0 = -1, s_0 = 2.$$

Zde použijeme opět lemma 2.35, části b) a c), dle kterých je s_{t+2} sudé kladné číslo, tedy $s_{t+2} \geq 2$. Část c) zmíněného lemmatu 2.35 můžeme použít díky tomu, že r_0 i s_0 jsou celočíselné, $s_0 = 2$ je sudé, a zároveň $D \equiv r_0^2 \bmod 2s_0$, neboť po dosazení za r_0 a s_0 do této kongruence přesně dostáváme $D \equiv 1 \bmod 4$. Proto $s_{t+2} \geq 2$ a ze stejných důvodů jako v minulém případě, platí následující odhady:

$$\left\lfloor \frac{D}{s_0 s_{t+2}} \right\rfloor = \left\lfloor \frac{D}{2s_{t+2}} \right\rfloor \leq \left\lfloor \frac{D}{4} \right\rfloor = \frac{D-1}{4} = -N(\delta),$$

čímž jsme i v tomto případě ověřili odhad (4.2). Proto opravdu platí nerovnost $N(\beta) \leq -N(\delta)$ a dostáváme spor s předpokladem, že platí opačná ostrá nerovnost.

V tuto chvíli nám stačí ukázat, že pokud existuje jednotka v $\mathcal{O}_K$ s normou -1, tak právě dokázaný odhad na normu nerozložitelných prvků v $\mathcal{O}_K$ je těsný, tedy chceme nalézt nerozložitelný prvek s normou $-N(\delta)$. Nechť $\varepsilon = p_{k-1} + q_{k-1}\delta$ je jednotka s normou -1 a pro tuto jednotku použijme důsledek 3.14, dle kterého, jelikož k je liché (což plyne z lemmatu 2.34) je prvek $p_{k-2,a_0} + q_{k-2,a_0}\delta$ nerozložitelný v $\mathcal{O}_K$ (v důsledku 3.14 tedy volíme $z = 0, t = k-2$ a $j = a_0$). Tento nerozložitelný prvek má normu $-N(\delta)$, což nyní ověříme:

$$N(p_{k-2,a_0} + q_{k-2,a_0}\delta) \overset{\text{Lemma } 2.27}{=} N(-\varepsilon\delta') = N(-\varepsilon)N(\delta') = N(\varepsilon)N(\delta) = -N(\delta),$$

čímž jsme skutečně v případě existence jednotky s normou -1 skutečně ověřili, že prokázaný odhad na normu nerozložitelných prvků je těsný, čímž je celý důkaz této věty dokončen. □

Zamysleme se nad tím, pro které případy reálných kvadratických číselných těles platí, že dané odhady norem nerozložitelných prvků z předchozí věty 4.2 jsou skutečně optimální, tedy kdy existuje jednotka $\mathcal{O}_K^+$ s normou -1. Budeme se zabývat pouze případem $D \equiv 2, 3 \bmod 4$, kdy $\mathcal{O}_K = \mathbb{Z}[\sqrt{D}]$ a tak existence

jednotky s normou -1 odpovídá existenci celočíselného řešení (x, y) tzv. Pellovy rovnice ve formě

$$x^2 - Dy^2 = -1.$$

Existence řešení této rovnice záleží na paritě k v rámci řetězového zlomku $\sqrt{D} = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k}]$, podle věty 35 z článku [9] (nebo též z lemmatu 2.34, části a)) platí, že daná rovnice má řešení, právě když je k liché (v článku [9] je uvažován řetězový zlomek $\sqrt{D} = [a_0, \overline{a_1, \ldots, a_{k-1}, a_k, 2a_0}]$, a tak je zde uvedena parita k obráceně oproti situaci v této práci). Jakým způsobem lze zvolit posloupnost $(a_1, a_2, \ldots, a_k)$, to nám říká věta 33 z téhož článku [9]. Abychom uvedli konkrétní příklad, tak pro D tvaru $t^2 + 1$, pokud je D bezčtvercové, platí $\sqrt{D} = [a_0, \overline{2a_0}]$, tedy máme $k = 1$ a příslušné odhady na normu nerozložitelných prvků jsou v tomto případě skutečně optimální, konkrétně pro $D = t^2 + 1$ máme jednotku s normou -1 tvaru $t + \sqrt{D}$. Tyto úvahy platí bez ohledu na to, čemu je D kongruentní modulo 4. Naopak platí $\sqrt{3} = [1, \overline{1, 2}]$, tedy v případě $D = 3$ máme $k = 2$, a tak v tomto případě neexistuje jednotka s normou -1 (což odpovídá neexistenci celočíselného řešení diofantické rovnice $x^2 - 3y^2 = -1$). Podle věty 4.2 mají rozložitelné prvky v $\mathbb{Z}[\sqrt{3}]$ normu alespoň $-N(\delta) = -N(\sqrt{3}) = 3$, ale tento odhad není optimální, neboť v $\mathbb{Z}[\sqrt{3}]$ neexistuje nerozložitelný prvek s normou 3 (dokonce neexistuje vůbec žádný prvek s normou 3, neboť diofantická rovnice $x^2 - 3y^2 = 3$ nemá žádné celočíselné řešení). Z obdobného důvodu neexistuje žádný prvek v $\mathbb{Z}[\sqrt{3}]$ s normou 2, neboť ani rovnice $x^2 - 3y^2 = 2$ nemá žádné celočíselné řešení. Proto všechny nerozložitelné prvky v $\mathcal{O}_K^{+,0}$ pro $K = \mathbb{Q}(\sqrt{3})$ mají normu 1.

Nyní se již podíváme na to, jaká je situace s horním odhadem normy nerozložitelných prvků v polomřížkách $\sigma(\mathcal{O}_K^{+,0})$ pro K libovolné totálně reálné číselné těleso. Tento obecný odhad platí i pro reálná kvadratická číselná tělesa, ale bude hrubší, což je důvod, proč jsme jemnější odhad pro kvadratická číselná tělesa udělali samostatně. Opět budeme pro jednoduchost místo normy v polomřížce $\sigma(\mathcal{O}_K^{+,0})$ uvažovat standardní normu v $\mathcal{O}_K$. Tento důkaz pro obecná totálně reálná číselná tělesa využije jako hlavní nástroj Minkowského větu o mřížových bodech, kterou známe ze sekce 2.4, přičemž tento důkaz bude reprodukován z článku [8].

Věta 4.3 ([8], Theorem 5)**.** *Nechť K je totálně reálné číselné těleso stupně n s diskriminantem Δ_K a mějme prvek $\gamma \in \mathcal{O}_K^+$, který má normu ostře větší než Δ_K. Poté je prvek γ rozložitelný v $\mathcal{O}_K^+$, navíc existuje prvek tvaru β^2 pro nějaké $\beta \in \mathcal{O}_K$, který je totálně menší než γ.*

Důkaz. Důkaz je založen na použití Minkowského věty o mřížových bodech, kterou jsme si připomenuli v sekci 2.4, konkrétně jde o větu 2.36. Tuto větu budeme aplikovat na úplnou mřížku $\sigma(\mathcal{O}_K)$, kde σ je Minkowského vnoření (jedná se o úplnou mřížku podle Proposition 4.26 z knihy [11], jak jsme zmínili na konci 2. kapitoly po znění věty 2.36). Objem základního rovnoběžnostěnu této mřížky je $\mu(P) = \sqrt{\Delta_K}$, což jsme rovněž zmínili krátce po znění věty 2.36 (zde využíváme předpokladu, že těleso K je totálně reálné, a proto $s = 0$, kde s je počet vnoření tělesa K, pro které existují nějaké prvky, které se nezobrazí do reálných čísel). Jako množinu T ve znění věty 2.36 zvolíme množinu

$$T := \{x = (x_1, x_2, \ldots, x_n) \in \mathbb{R}^n \mid |x_i| \leq \sqrt{\sigma_i(\gamma)} - \iota\}, \tag{4.3}$$

kde $\sigma_1, \sigma_2, \ldots, \sigma_n$ jsou všechna vnoření K do $\mathbb{R}$ a $\iota > 0$ je dostatečně malý parametr takový, aby platilo

$$\prod_{i=1}^{n}(\sqrt{\sigma_i(\gamma)} - \iota) > \sqrt{\Delta_K}, \tag{4.4}$$

přičemž existence takového parametru $\iota > 0$ plyne z toho, že

$$\prod_{i=1}^{n}(\sqrt{\sigma_i(\gamma)}) = \sqrt{N(\gamma)} > \sqrt{\Delta_K}.$$

Množina T, zadefinovaná ve (4.3) je jistě konvexní, kompaktní a symetrická podle počátku, zároveň z nerovnice (4.4) je vidět, že Lebesgueova míra množiny T je větší než $2^n\sqrt{\Delta_K} = 2^n\mu(P)$, z čehož plyne, že opravdu můžeme použít Minkowského větu o mřížových bodech, větu 2.36 a dostáváme, že existuje nenulový bod v průniku T a $\sigma(\mathcal{O}_K)$, což přesně znamená existenci prvku $\beta \in \mathcal{O}_K$, pro který platí, že

$$\sigma_i(\beta) \leq |\sigma_i(\beta)| \leq \sqrt{\sigma_i(\gamma)} - \iota < \sqrt{\sigma_i(\gamma)},$$

což platí pro všechna i od 1 do n. Po umocnění na druhou a jelikož σ_i je okruhový homomorfismus dostáváme, že pro všechna i od 1 do n máme

$$\sigma_i(\beta^2) < \sigma_i(\gamma).$$

To však přesně znamená, že prvek $\gamma - \beta^2$ je nejen celistvý, ale i totálně kladný, a proto

$$\gamma = \beta^2 + (\gamma - \beta^2),$$

což znamená, že jsme nalezli netriviální rozklad prvku γ v $\mathcal{O}_K^+$, čímž jsme ověřili, že prvek γ je rozložitelný v $\mathcal{O}_K^+$ a věta je dokázána. □

Připomeňme, že tato věta 4.3 nezobecňuje větu 4.2, neboť ve větě 4.2 jsme dokázali přesnější odhad pro normu nerozložitelných prvků v případě reálných kvadratických číselných těles. Skutečně, z věty 4.3 je rozložitelný každý prvek s normou alespoň Δ_K, což v případě reálných kvadratických číselných těles znamená $4D$, pokud $D \equiv 2, 3 \bmod 4$ a D, pokud $D \equiv 1 \bmod 4$. Ve větě 4.2 jsme však ukázali, že každý prvek s normou větší než $-N(\delta)$ je rozložitelný, ale $-N(\delta)$ je D, pokud $D \equiv 2, 3 \bmod 4$ a $\dfrac{D-1}{4}$, pokud $D \equiv 1 \bmod 4$, čili ve větě 4.2 máme opravdu lepší odhady na normu nerozložitelných prvků v příslušné polomřížce.

4.2 Obecné polomřížky

V této sekci si představíme příklad polomřížky, kde nerozložitelné prvky mohou mít libovolně velkou normu ve své polomřížce, na rozdíl od polomřížek $\sigma(\mathcal{O}_K^{+,0})$, jak jsme se přesvědčili v minulé sekci.

Nástrojem, který použijeme ke konstrukci této polomřížky, bude tvrzení 1.16, bude se tedy jednat o polomřížku generovanou nějakou diskrétní množinou, která je obsažena v nějakém kuželi. Příslušnou množinou bude množina tvaru

$$X \times \{1\} \times \{1\} \times \ldots \times \{1\} \subseteq \mathbb{R}^n,$$

kde $X \subseteq \mathbb{R}$ je nekonečná diskrétní množina, která je obsažena v nějakém kuželi, bez újmy na obecnosti předpokládejme, že jde o kužel $\mathbb{R}_0^+$, zde se opíráme o charakterizaci kuželů v $\mathbb{R}$, kterou jsme zmínili před tvrzením 1.11. Povšimněme si, že opravdu můžeme použít tvrzení 1.16, dle kterého zkoumaný monoid $\langle X \times \{1\} \times \{1\} \times \ldots \times \{1\}\rangle$ tvoří polomřížku. Diskrétnost generující množiny $X \times \{1\} \times \{1\} \times \ldots \times \{1\}$ plyne okamžitě z diskrétnosti množiny X, zároveň celá tato generující množina je obsažena v kuželi $(\mathbb{R}^+)^n$. Proto náš zkoumaný monoid opravdu tvoří polomřížku.

Co se týká nerozložitelných prvků v této polomřížce, tak je potřeba odlišit 2 případy podle dimenze, neboť případ takové polomřížky v jedné dimenzi bude složitější a nebude obecně fungovat, neboť je zde potřeba mít více požadavků na množinu X, abychom i v tomto případě dostali polomřížku s nerozložitelnými prvky libovolně velké normy ve své polomřížce.

Jedná-li se o polomřížku ve dvou a více dimenzích, pak je situace velice jednoduchá. Pohledem na druhou souřadnici (nebo i libovolnou jinou souřadnici než první) zjistíme, že každý prvek množiny, jenž z definice generuje naši zkoumanou polomřížku, je v této polomřížce i nerozložitelný. Jinými slovy, každý prvek množiny $X \times \{1\} \times \{1\} \times \ldots \times \{1\}$ je ve své polomřížce nerozložitelný. Zároveň platí, že norma libovolného prvku této množiny ve zkoumané polomřížce je přesně rovna jeho první souřadnici, tedy nějakému prvku množiny X. Jelikož množina X je nekonečná a diskrétní, poté je množina X i neomezená (kdyby množina X byla omezená, poté by jistě obsahovala hromadný bod a nejednalo by se o diskrétní množinu). Prvky množiny X mohou tedy být libovolně velké, proto ve zkoumané polomřížce mají nerozložitelné prvky libovolně velkou normu ve své polomřížce.

Co se týká případu, kdy zkoumáme naši polomřížku v jedné dimenzi, tak je situace složitější. Nemůžeme se totiž opřít o souřadnice, které mají všechny prvky generující množiny rovny 1, což v minulém případě dosvědčovalo jejich nerozložitelnost. V tomto případě zkoumáme polomřížku $\langle X\rangle$, což je velmi obecný případ. My potřebujeme zvolit množinu X tak, aby žádný prvek množiny X nebyl součtem jiných prvků množiny X, abychom mohli dosáhnout stejné situace, kdy každý generátor definující zkoumanou polomřížku byl nerozložitelný a měl tedy libovolně velkou normu ve své polomřížce. Ukazuje se, že dostačující je volba $X := \{\sqrt{D} \mid D > 1 \text{ je bezčtvercové přirozené číslo}\}$. Taková množina X je jistě nekonečná, je tvořena pouze kladnými čísly a diskrétnost této množiny se snadno ověří pomocí tvrzení 1.5. To, že žádný prvek takové množiny X není součtem jiných prvků z X, se dá vyjádřit neexistencí řešení jisté diofantické rovnice, kterou si přesně zformulujeme v následujícím lemmatu:

Lemma 4.4. *Nechť $t \in \mathbb{N}$ a mějme bezčtvercová přirozená čísla $x, z_1, z_2, \ldots, z_t$, která jsou větší než 1. Poté následující diofantická rovnice nemá žádné řešení v přirozených číslech:*

$$\sqrt{x} = \sum_{i=1}^{t} b_i \sqrt{z_i}. \tag{4.5}$$

To znamená, že neexistují žádná přirozená čísla $b_1, b_2, \ldots, b_t$, která vyhovují podmínce (4.5).

Důkaz. Důkaz je zpracován v o mnoho obecnější podobě ve větě 2.29 ve skriptech [6], kde předpoklad „pro každou neprázdnou podmnožinu $I \subset \{1, 2, \ldots n\}$ máme

$\prod_{i\in I}\sqrt{a_i} \notin \mathbb{Q}$“ odpovídá tomu, že čísla $x, z_1, z_2, \ldots, z_t$ jsou bezčtvercová a větší než 1. □

Tímto lemmatem jsme si tedy ověřili, že i v případě polomřížek v jedné dimenzi nám příklad polomřížky $\langle X \times \{1\} \times \{1\} \times \ldots \times \{1\}\rangle$ dosvědčil existenci polomřížek s nerozložitelnými prvky libovolně velké normy ve své polomřížce. V těchto polomřížkách platí, že každý generátor definující tuto polomřížku je v ní i nerozložitelný a jeho norma ve své polomřížce je rovna jeho první souřadnici. Nicméně první souřadnice prvků generující množiny může nabývat libovolně velkých hodnot, proto mají nerozložitelné prvky v těchto polomřížkách neomezenou normu ve své polomřížce. Shrňme si právě dokázané výsledky do následující věty.

Věta 4.5. *Pro všechna $x \in \mathbb{R}$ a pro všechna $n \in \mathbb{N}$ existuje polomřížka $L \subseteq \mathbb{R}^n$ taková, že v polomřížce L existuje nerozložitelný prvek s normou v polomřížce L větší než x. Lze volit*

$$L = \langle X \times \{1\} \times \{1\} \times \ldots \times \{1\}\rangle, \tag{4.6}$$

kde $X = \{\sqrt{D} \mid D > 1$ je bezčtvercové přirozené číslo$\}$, pokud $n = 1$, v případě $n > 1$ stačí, aby X byla libovolná nekonečná diskrétní podmnožina kladných reálných čísel.

Na závěr si snadno uvědomíme, že pro polomřížky, kterým jsme se v této sekci věnovali, platí nejen to, že nerozložitelné prvky mají libovolně velkou normu ve své polomřížce, ale rovněž tyto nerozložitelné prvky mají libovolně velkou eukleidovskou normu $||\cdot||_2$.

Závěr

V této práci jsme se zaměřili na teorii polomřížek a jejich nerozložitelných prvků. Největší pozornost byla věnována polomřížkám S_K, jejíž prvky odpovídají takovým totálně nezáporným prvkům z $\mathcal{O}_K$, které jsou větší nebo rovny svému konjugátu, pro reálné kvadratické číselné těleso K. Explicitně jsme popsali nerozložitelné prvky těchto polomřížek a tento popis jsme jakožto matematické tvrzení dokázali dvěma způsoby, nejprve v důsledku 3.14, kde jsme postupovali podle článku [3], a poté i ve větě 3.18, jejíž důkaz je vlastním dílem autora. Nabízí se několik cest, kudy by se výsledky této práce daly rozšířit.

Například by šlo věnovat více pozornosti samotné teorii polomřížek a snažit se zobecnit do libovolného počtu dimenzí výsledky z článku [14], čemuž jsme se částečně věnovali v první kapitole práce. Nebo by šlo se zaměřit na jiný zajímavý příklad polomřížek, kupříkladu zajímavým příkladem polomřížek jsou tzv. numerické pologrupy, což odpovídá takovým jednodimenzionálním polomřížkám, které jsou podmnožiny $\mathbb{N}$ a jejíž množina nerozložitelných prvků je konečná a navíc tyto nerozložitelné prvky nemají žádného společného dělitele v $\mathbb{Z}$, různého od ± 1. Teorii numerických pologrup se věnuje například článek [12]

Co se týká situace polomřížek S_K, kterým jsme se věnovali velkou část práce, tak bychom se ještě mohli podrobněji zaměřit na optimalitu odhadu normy nerozložitelných prvků z věty 4.2 a zabývat se případy, kdy tyto odhady nejsou optimální (tedy kdy v příslušném okruhu celistvých prvků mají všechny jednotky normu 1). Na konci 3. kapitoly článku [3] se bez důkazu tvrdí, že v tomto případě by optimální odhad na normu nerozložitelných prvků měl být řádově menší (vzhledem k tomu, jak tento odhad závisí na diskriminantu Δ_K).

Dále bychom se rovněž mohli věnovat jiným případům číselných těles K, než jsou reálná kvadratická číselná tělesa, což však může být relativně obtížné například proto, že neznáme jednoduchou charakterizaci celistvých prvků $\mathcal{O}_K$. V článku [7] můžeme najít charakterizaci nerozložitelných prvků pro některá číselná tělesa stupně 3 (konkrétně se jedná o Theorem 1.2.).

Seznam použité literatury

[1] BERGMAN, Clifford. *Universal algebra: Fundamentals and Selected topics*. CRC Press, 2012.

[2] BLOMER, Valentin a KALA, Vítězslav. On the rank of universal quadratic forms over real quadratic fields. *Documenta Mathematica*, vol. 23 (2018), s. 15–34.

[3] DRESS, Andreas a SCHARLAU, Rudolf. Indecomposable totally positive numbers in real quadratic orders. *Journal of Number Theory*, vol. 14 (1982), no. 3, s. 292–306.

[4] VON EITZEN, Hagen a RZEPECKI, Tomasz. Is the semigroup generated by wellordered positive set wellordered?. In: *math.stackexchange.com* [online]. 6. 10. 2012 [cit. 10. 1. 2024]. Dostupné z: `https://math.stackexchange.com/q/207897`.

[5] HEJDA, Tomáš a KALA, Vítězslav. Additive structure of totally positive quadratic integers. *Manuscripta Mathematica*, vol. 163 (2020), no. 1-2, s. 263–278.

[6] KALA, Vítězslav. *Úvod do komutativní algebry* [online]. 5. 1. 2023 [cit. 10. 1. 2024]. Dostupné z: `http://karlin.mff.cuni.cz/~kala/files/UKA22.pdf`

[7] KALA, Vítězslav a TINKOVÁ, Magdaléna. Universal quadratic forms, small norms, and traces in families of number fields. *International Mathematics Research Notices. IMRN*, (2023), no. 9, s. 7541–7577.

[8] KALA, Vítězslav a YATSYNA, Pavlo. On Kitaoka's conjecture and lifting problem for universal quadratic forms. *Bulletin of the London Mathematical Society*, vol. 55 (2023), s. 854–864.

[9] KUDĚJ, Martin. Řetězové zlomky s předepsanou periodou. *Pokroky matematiky, fyziky a astronomie*, roč. 66 (2021), č. 1, s. 11–32.

[10] MARTINY, Ian. *The 3N+1 problem: Scope, history and results*. Pittsburgh, 2015. Diplomová práce. University of Pittsburgh. Kenneth P. Dietrich School of Arts and Sciences.

[11] MILNE, James. *Algebraic number theory* [online], 19. 7. 2020 [cit. 10. 1. 2024]. Dostupné z: `https://www.jmilne.org/math/CourseNotes/ant.html`

[12] MOREE, Pieter. Numerical semigroups, cyclotomic polynomials, and Bernoulli numbers. *American Mathematical Monthly*, vol. 121 (2014), s. 890–902.

[13] SHURMAN, Jerry. *The unit group of a real quadratic field* [online]. 31. 7. 2022 [cit. 10. 1. 2024]. Dostupné z: `https://people.reed.edu/~jerry/361/lectures/rqunits.pdf`

[14] TUTAJ, Edward. Like$\mathbb{N}$'s – a point of view on natural numbers. *Annales Universitatis Paedagogicae Cracoviensis. Studia Mathematica*, vol. 16 (2017), s. 95–115.