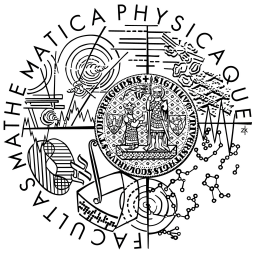

MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Veronika Hájková

Pythagorova čísla řádů v číselných tělesech

Katedra algebry

Vedoucí bakalářské práce: Mgr. Vítězslav Kala, Ph.D.

Studijní program: Matematika

Studijní obor: Obecná matematika

Praha 2020

Prohlašuji, že jsem tuto bakalářskou práci vypracovala samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů.

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

Tímto bych ráda poděkovala svému vedoucímu bakalářské práce, Mgr. Vítězslavu Kalovi, Ph.D., za cenné rady a připomínky v průběhu psaní práce. Dále bych ráda poděkovala rodině a přítelovi za psychickou podporu.

Název práce: Pythagorova čísla řádů v číselných tělesech

Autor: Veronika Hájková

Katedra: Katedra algebry

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

Abstrakt: Tato práce se zabývá zkoumáním Pythagorových čísel řádů v číselných tělesech. Po krátkém úvodu, kde opakuji a definuji nové pojmy důležité k porozumění této práce, se zabývám potřebnými vlastnostmi stopy. Práce dále dokazuje existenci řádů v totálně reálných číselných tělesech, jejichž Pythagorova čísla jsou libovolně velká, a končí důkazem, že pro libovolné $N \in \mathbb{N}$ existuje totálně reálné číselné těleso, jehož maximální řád má Pythagorovo číslo alespoň N.

Klíčová slova: Pythagorovo číslo, totálně reálné číselné těleso, řád

Title: Pythagoras numbers of orders in number fields

Author: Veronika Hájková

Department: Department of Algebra

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

Abstract: This thesis deals with the investigation of Pythagoras numbers of orders in number fields. After a short introduction, where I repeat and define new concepts important for understanding this work, I deal with the necessary characteristics of the trace. The thesis further proves the existence of orders in totally real number fields whose Pythagoras numbers are arbitrarily large and ends with a proof that for any $N \in \mathbb{N}$, there is a totally real number field whose maximum order has a Pythagoras number of at least N.

Keywords: Pythagoras number, totally real number field, order

Obsah

Úvod

V roce 1770 Lagrange dokázal, že každé přirozené číslo se dá napsat jako součet nejvýše čtyř čtverců přirozených čísel. Podobně každé nezáporné racionální číslo se dá napsat jako součet nejvýše 4 čtverců racionálních čísel. Tento výsledek vede přirozeně k pojmu Pythagorova čísla komutativního okruhu (definice 1.7.4), tedy pokud R je komutativní okruh, jeho Pythagorovo číslo je definováno jako nejmenší přirozené číslo $P(R)$ takové, že každá suma čtverců v R se dá reprezentovat sumou $P(R)$ čtverců prvků z R. Pokud takové $P(R)$ neexistuje, položíme Pythagorovo číslo rovno ∞.

Problému existence a hodnoty Pythagorova čísla pro různé komutativní okruhy se věnovala řada matematiků. Jako příklad můžeme uvést následující výsledky. Hilbert v roce 1900 [2] zformuloval větu, která tvrdí, že $P(K) \leq 4$ pro libovolné číselné těleso K (definice 1.1.5). Pravdivost Hilbertova tvrzení dokázal Siegel [12] v roce 1919.

Naše práce se bude týkat specificky Pythagorových čísel pro řády (definice 1.6.1) v algebraických číselných tělesech. V roce 1980 Peters [8] dokázal, že v řádech v číselných tělesech, která nejsou totálně reálná (definice [1.7.2]), je hodnota Pythagorova čísla nejvýše 5. V totálně reálném případě tento výsledek neplatí. Scharlau ve svém článku [10] zkonstruoval posloupnost řádů v totálně reálných číselných tělesech, jejichž Pythagorovo číslo dosahuje libovolně velké hodnoty. Přesněji řečeno, Scharlau sestrojil posloupnost přirozených čísel $\{d_1, d_2, \dots\}$ takovou, že Pythagorovo číslo řádu $\mathbb{Z}\left[\sqrt{d_1}, \dots, \sqrt{d_N}\right]$ v tělese $K_N := \mathbb{Q}\left(\sqrt{d_1}, \dots, \sqrt{d_N}\right)$ je alespoň N.

Ve druhé části svého článku Scharlau zavádí jinou posloupnost přirozených čísel $\{d_1, d_2, \dots\}$ a formuluje tvrzení, podle kterého Pythagorovo číslo maximálního řádu $\mathcal{O}_K$ číselného tělesa K je rovněž alespoň N. Důkaz tohoto tvrzení v článku není obsažen s poznámkou, že důkaz lze provést pomocí formálních změn v důkazu jeho předchozího výsledku. Hlavním cílem mé bakalářské práce bude tento důkaz formálně správně sepsat (věta 2.4.1). Věty, které byly dokázány na přednáškách, a hlubší věty z algebry a teorie čísel uvádíme bez důkazů.

1. Základní definice a věty

V této úvodní části si připomeneme některé základní definice a tvrzení. Část těchto výsledků lze nalézt v učebnici Základy algebry [13]. Zbylá tvrzení jsou hlubší povahy a lze je nalézt buď v knize Şabana Alaca [1], nebo ve článcích citovaných v seznamu referencí.

1.1 Tělesová rozšíření

Definice 1.1.1. *Nadtěleso $T \leq S$ lze považovat za vektorový prostor nad tělesem T: sčítání a odčítání přebereme beze změny a místo násobení jako operace $S \times S \to S$ uvažujeme pouze restrikci $T \times S \to S$, tj. násobíme prvky většího tělesa S (vektory) pouze prvky menšího tělesa T (skaláry). Dimenzi tohoto vektorového prostoru budeme značit $[S : T]$ a nazveme jej stupněm rozšíření.*

Definice 1.1.2. *Buď $T \leq S$ rozšíření těles. Je-li stupeň $[S : T]$ konečný, říkáme, že jde o rozšíření konečného stupně.*

Definice 1.1.3. *Buď $T \leq S$ rozšíření těles a $a \in S$. Řekneme, že prvek a je algebraický nad T, pokud existuje nenulový polynom z $T[x]$, jehož je a kořenem. V opačném případě se prvek a nazývá transcendentní nad T. Je-li každý prvek tělesa S algebraický nad T, hovoříme o algebraickém rozšíření.*

Věta 1.1.4. [[13], *tvrzení* 25.1] *Rozšíření konečného stupně jsou algebraická.*

Definice 1.1.5. *(Algebraické) číselné těleso je libovolné nadtěleso $\mathbb{Q}$ konečného stupně.*

Definice 1.1.6. *Nechť $T \leq S$ je konečné rozšíření těles, $[S : T] = n$. Předpokládejme, že $a_1, \ldots, a_n$ je báze vektorového prostoru S nad T, $a \in S$. Pak $aa_i = \sum_j b_{ij} a_j$, kde $b_{ij} \in T$. Označme B matici s prvky b_{ij}. Pak definujeme*

(i) normu a jako $N_{S/T}(a) = det(B)$ a

(ii) stopu a jako $\mathrm{tr}_{S/T}(a) = \sum_i b_{ii}$.

Věta 1.1.7. *Stopa a norma prvku nezávisí na volbě báze S jako vektorového prostoru nad T.*

Důkaz. Důkaz plyne z lineární algebry, neboť každému lineárnímu zobrazení z $\mathbb{Q}^n$ do $\mathbb{Q}^n$ je jednoznačně přiřazena jeho stopa i norma. Při reprezentaci tohoto zobrazení maticí vzhledem k určité bázi je stopa určena součtem prvků na diagonále matice a norma je určena jejím determinantem. Tyto hodnoty nezávisí na výběru báze, neboť matice podobné mají stejnou stopu i determinant, tedy normu. □

Definice 1.1.8. *Buď R okruh s jednotkou. Jeho charakteristikou rozumíme nejmenší $n \in \mathbb{N}$ takové, že $n \cdot 1 = 0$. Pokud takové n neexistuje, je $char(R) = 0$.*

Věta 1.1.9. *Je-li R těleso, pak je jeho charakteristika buď rovna nule, nebo je to prvočíslo.*

Důkaz. Kdyby $n = a \cdot b$, pak bychom měli $0 = n \cdot 1 = (a \cdot 1) \cdot (b \cdot 1)$, tedy $a \cdot 1 = 0$ nebo $b \cdot 1 = 0$, což by byl spor s minimalitou n. □

Řekneme, že $S \geq T$ je algebraický uzávěr tělesa T, pokud je S algebraicky uzavřené těleso, tedy pokud má každý polynom z $S[x]$ stupně ≥ 1 v S kořen a zároveň je algebraickým rozšířením tělesa T.

Lemma 1.1.10. [[14], *lemma* 1] *Mějme těleso T charakteristiky různé od 2 a S jeho algebraický uzávěr. Pro $a \in T$ nechť $\sqrt{a} \in S$ značí nějaký kořen polynomu $x^2 - a \in T[x]$. Buď $L \leq S$, $a, b \in L$ takové, že $\sqrt{a}, \sqrt{b}, \sqrt{ab} \notin L$. Potom $[L(\sqrt{a}, \sqrt{b}) : L] = 4$.*

Důkaz. Z předpokladů našeho lemmatu víme, že $[L(\sqrt{a}) : L] = 2$. Nyní ukážeme sporem, že $\sqrt{b} \notin L(\sqrt{a})$. Nechť tedy $\sqrt{b} = x + y\sqrt{a}$, kde $x, y \in L$. Potom

$$\sqrt{b} - y\sqrt{a} = x \in L,$$

$$b - 2y\sqrt{ab} + y^2 a = x^2 \in L,$$

$\sqrt{ab} = \frac{b+y^2a-x^2}{2y} \in L$, což je spor s předpoklady lemmatu.

Odtud plyne, že $[L(\sqrt{a}, \sqrt{b}) : L(\sqrt{a})] = 2$, a tedy $[L(\sqrt{a}, \sqrt{b}) : L] = 4$. □

Věta 1.1.11. [[14], *tvrzení* 2] *Buď T těleso charakteristiky různé od 2, $n \in \mathbb{N}$ a $M = \{\sqrt{d_1}, \ldots, \sqrt{d_n}\}$, kde $d_i \in T$ a pro libovolnou neprázdnou $F \subseteq \{1, \ldots, n\}$ platí, že $\prod_{k \in F} \sqrt{d_k} \notin T$. Potom $[T(M) : T] = 2^n$.*

Důkaz. Indukcí dle n. Pro $n = 1$ je to zřejmé. Pro $n = 2$ nám to plyne z předchozího lemmatu. Indukční krok $n - 1 \to n$.

Označme $L = T(\sqrt{d_1}, \ldots, \sqrt{d_{n-2}})$. Pak z indukčního předpokladu víme, že $[L : T] = 2^{n-2}$. Stačí tedy dokázat, že $[T(M) : L] = 4$. Dle předchozího lemmatu k tomu stačí vědět, že $\sqrt{d_{n-1}}, \sqrt{d_n}, \sqrt{d_{n-1}d_n} \notin L$. To ovšem plyne z indukčního předpokladu pro $n - 1$, který dává $[L(\sqrt{d_{n-1}}) : T] = 2^{n-1}$, tedy $\sqrt{d_{n-1}} \notin L$. Podobně pro zbylé dvě odmocniny. □

V následujícím lemmatu 1.1.12 ukážeme, že příkladem splňujícím předpoklady věty 1.1.11 jsou bezčtvercová, navzájem nesoudělná, přirozená čísla $d_1, \ldots, d_n$.

Číslo $d \in \mathbb{Z}$ nazveme bezčtvercové (nad $\mathbb{Z}$), pokud ve svém prvočíselném rozkladu neobsahuje žádnou druhou mocninu. Je zřejmé, že součin bezčtvercových, navzájem nesoudělných, přirozených čísel je opět bezčtvercové číslo.

Lemma 1.1.12. *Pokud je $d \in \mathbb{Z}$ bezčtvercové, pak $\sqrt{d} \notin \mathbb{Q}$.*

Důkaz. Jelikož d je bezčtvercové, víme, že v prvočíselném rozkladu $d = p_1 \cdots p_n$ budou všechna prvočísla $p_1, \ldots, p_n$ v první mocnině. Sporem předpokládejme, že $\sqrt{d} \in \mathbb{Q}$, tedy že existují nesoudělná $u \in \mathbb{Z}$ a $v \in \mathbb{N}$ taková, že $\sqrt{d} = \frac{u}{v}$. Označme si

$$u = u_1^{i_1} \cdots u_k^{i_k}$$
$$v = v_1^{j_1} \cdots v_l^{j_l}$$

prvočíselné rozklady u a v. Pak platí:

$$\sqrt{d} = \frac{u}{v} \Leftrightarrow d = \frac{u^2}{v^2} \Leftrightarrow p_1 \cdots p_n \cdot v_1^{2j_1} \cdots v_l^{2j_l} = u_1^{2i_1} \cdots u_k^{2i_k}$$

Z nesoudělnosti u a v plyne, že pro každé p_i existuje právě jedno u_j takové, že se rovnají. Bez újmy na obecnosti nechť $p_i = u_i$ pro všechna $i \in \{1, \ldots, n\}$. Pak:

$$v_1^{2j_1} \cdots v_l^{2j_l} = u_1^{2i_1 - 1} \cdots u_n^{2i_n - 1} \cdots u_k^{2i_k},$$

což je spor s nesoudělností u a v. □

Zaveďme si nyní jednotné značení, které bude platit v celé této práci:

Definice 1.1.13. *Definujeme*

$$K_0 := \mathbb{Q}; \qquad K_{t+1} := K_t(\sqrt{d_{t+1}}),\ t = 0, \ldots, n-1,$$

kde $d_1, \ldots, d_n$ je posloupnost přirozených čísel taková, že $K_{t+1} \neq K_t$.

Tedy $[K_t : K_{t-1}] = 2$ a $[K_n : \mathbb{Q}] = 2^n$.

1.2 Ideály

V této práci budeme písmenem R vždy označovat komutativní okruhy s jednotkou.

Definice 1.2.1. *Nechť R je komutativní okruh s jednotkou. Potom $\emptyset \neq I \subseteq R$ je ideál, pokud platí:*

(i) $\forall a, b \in I$ *je* $a - b \in I$,

(ii) $\forall a \in I$ *a* $\forall r \in R$ *je* $r \cdot a \in I$.

Definice 1.2.2. *Říkáme, že I je hlavní ideál v okruhu R, pokud $I = aR$ pro nějaké a z R.*

Definice 1.2.3. *Definujeme součin ideálů I, J jako*

$$I \cdot J = \left\{ \sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}, a_i \in I, b_i \in J \right\}.$$

Standardním postupem lze ukázat, že tento součin je opět ideál.

Definice 1.2.4. *Ideál P ($\neq R$) okruhu R je prvoideál, pokud pro všechny ideály $I, J < R$ platí:*

$$IJ \subset P \Rightarrow I \subset P \vee J \subset P.$$

Definice 1.2.5. *Dedekindův obor je takový obor integrity, v němž se každý ideál, který není roven celému oboru integrity, jednoznačně rozkládá na konečný součin prvoideálů.*

1.3 Celistvé prvky

Definice 1.3.1. *Nechť R je podokruh okruhu S. Potom říkáme, že $v \in S$ je celistvý nad R, pokud je kořenem nějakého monického polynomu $f \in R[x]$. Okruh S je celistvý nad svým podokruhem R, pokud je každý prvek $v \in S$ celistvý nad R.*

Věta 1.3.2. [[1], *věta* 8.1.1] *Nechť K je číselné těleso. Potom množina všech celistvých prvků tělesa K nad $\mathbb{Z}$*

$$\mathcal{O}_K := \{\alpha \in K \mid \alpha \text{ celistvý nad } \mathbb{Z}\} \text{ tvoří Dedekindův obor.}$$

V našem případě budeme nejvíce využívat celistvých prvků nad $\mathbb{Z}$. Pokud tedy nebude řečeno jinak, pojem celistvý prvek budeme automaticky považovat za celistvý prvek nad $\mathbb{Z}$.

Věta 1.3.3. [[1], *věta* 4.2.4] *Nechť K je číselné těleso. Pak platí:*

(i) $\mathcal{O}_K \cap \mathbb{Q} = \mathbb{Z}$,

(ii) každé $\alpha \in K$ *lze napsat ve tvaru* $\alpha = \frac{\beta}{n}$, $\beta \in \mathcal{O}_K$, $n \in \mathbb{N}$.

1.4 Diskriminant číselného tělesa

Pokud $[K : \mathbb{Q}] = n$, potom z Galoisovy teorie víme, že existuje $\alpha \in \mathbb{C}$ takové, že $K = \mathbb{Q}(\alpha)$, kde minimální polynom $m_\alpha \in \mathbb{Q}[x]$ má stupeň n. Tento polynom má n různých kořenů $\alpha_1, \ldots, \alpha_n$ [[13], *tvrzení* 25.3]. Odtud plyne, že existuje právě n různých $\mathbb{Q}$-homomorfismů (nebo zkráceně vnoření) $K \to \mathbb{C}$, které si označíme $\sigma_1, \ldots, \sigma_n$, a každé toto vnoření je určeno vztahem $\sigma_j(\alpha) = \alpha_j$.

Definice 1.4.1. *Nechť K je číselné těleso, $[K : \mathbb{Q}] = n$ a $x_1, \ldots, x_n$ prvky z K. Označme $\sigma_1, \ldots, \sigma_n$ všechna vnoření $K \to \mathbb{C}$. Dále si označme $\omega_{ij} = \sigma_i(x_j)$. Pak diskriminant n-prvkové množiny $\{x_1, \ldots, x_n\}$ je definován výrazem:*

$$D(x_1, \ldots, x_n) = \left(det \begin{pmatrix} \omega_{11} & \omega_{12} & \cdots & \omega_{1n} \\ \omega_{21} & \omega_{22} & \cdots & \omega_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_{n1} & \omega_{n2} & \cdots & \omega_{nn} \end{pmatrix} \right)^2 .$$

Pomocí tohoto pojmu dále budeme definovat diskriminant ideálu v $\mathcal{O}_K$ a diskriminant tělesa K následujícím způsobem.

Věta 1.4.2. [[1], *věta* 6.5.2] *Nechť K je číselné těleso, $[K : \mathbb{Q}] = n$, $I \subset \mathcal{O}_K$ ideál. Potom existuje báze $b_1, \ldots, b_n \in I$ ideálu I jako $\mathbb{Z}$-modulu, pro kterou platí:*

$$I = \{\textstyle\sum_{i=1}^n a_i b_i | a_i \in \mathbb{Z}\}.$$

V tomto případě říkáme, že $b_1, \ldots, b_n$ je celistvá báze ideálu I. Pokud $I = \mathcal{O}_K$, pak celistvou bázi $\mathcal{O}_K$ nazýváme celistvou bází K.

Definice 1.4.3. *Nechť I je ideál v $\mathcal{O}_K$ s celistvou bází $b_1, \ldots, b_n$. Potom diskriminant ideálu I je definován jako $D(I) = D(b_1, \ldots, b_n)$.*

Lze ukázat, že diskriminant ideálu $D(I)$ nezávisí na volbě báze $b_1, \ldots, b_n$.
Speciální případ věty 1.4.2 s použitím věty 1.3.3 (ii) je následující věta.

Definice 1.4.4. *Nechť K je číselné těleso, $[K : \mathbb{Q}] = n$ a $b_1, \ldots, b_n$ celistvá báze K. Pak diskriminant K je definován výrazem:*

$$d(K) = D(b_1, \ldots, b_n).$$

Opět platí, že $d(K)$ nezávisí na výběru báze, naše definice je tedy korektní.

Definice 1.4.5. *Nechť I je ideál v $\mathcal{O}_K$ s celistvou bází $b_1, \ldots, b_n$. Potom definujeme normu ideálu I jako*

$$N(I) = \sqrt{\frac{D(I)}{d(K)}}.$$

Věta 1.4.6. [[1], *věta* 10.1.2] *Nechť K je číselné těleso, $p \in \mathbb{Z}$ je prvočíslo a $(p) = \prod_{i=1}^{k} P_i^{\alpha_i}$, $\alpha_i \geq 1$, je jednoznačný rozklad ideálu (p) na součin prvoideálů v $\mathcal{O}_K$. Potom norma*

$$N(P_j) = p^{\beta_j} \text{ pro nějaké } \beta_j \in \mathbb{N}.$$

Tedy norma každého z prvoideálů P_j je mocninou čísla p.

Věta 1.4.7. [[1], *věta* 7.1.2] *Nechť $d \in \mathbb{Z}$ bezčtvercové. Pak se diskriminant $\mathbb{Q}(\sqrt{d})$ rovná*

$$d\left(\mathbb{Q}(\sqrt{d})\right) = \begin{cases} 4d & \text{pokud } d \equiv 2, 3 \pmod 4, \\ d & \text{pokud } d \equiv 1 \pmod 4. \end{cases}$$

Tato věta má následující zobecnění.

Věta 1.4.8. [[11], *věta* 2.1] *Předpokládejme, že $d_1, \ldots, d_n$ jsou po dvou nesoudělná, $d_i \equiv 1 \pmod 4$ pro všechna i, a dále platí, že $\prod_{i=1}^{n} d_i = \prod_{j=1}^{s} p_j^{m_j}$, kde p_j jsou navzájem různá prvočísla. Potom platí:*

$$d(K_n) = \left(\prod_{j=1}^{s} p_j\right)^{2^{n-1}}.$$

Definice 1.4.9. *Nechť K je číselné těleso. Mějme prvočíslo $p \in \mathbb{Z}$ a rozklad hlavního ideálu v $\mathcal{O}_K$ generovaného p v $\mathcal{O}_K$ na prvoideály $(p) = \prod_{i=1}^{n} P_i^{l_i}$. Řekneme, že p se větví v $\mathcal{O}_K$, pokud $l_i > 1$ pro alespoň jedno i.*

Věta 1.4.10. [[1], *Dedekindova věta* 10.1.5] *Nechť K je číselné těleso. Potom prvočíslo $p \in \mathbb{Z}$ se větví v $\mathcal{O}_K$ právě tehdy, když $p \mid d(K)$.*

Nyní shrneme bez důkazů některá základní fakta z teorie lomených ideálů, která jsou obsažena v knize Şabana Alaca [[1], *str.* $196 - 215$]. Množinu všech prvoideálů v $\mathcal{O}_K$ lze použít k definování Abelovské grupy sestávající z formálních součinů $\{P_1^{\alpha_1} \cdots P_n^{\alpha_n}\}$, kde P_i jsou navzájem různé prvoideály a $\alpha_i \in \mathbb{Z}$ pro všechna i, s přirozeně definovanou operací násobení, tzn.

$$(P_1^{\alpha_1} \cdots P_k^{\alpha_k}) \cdot \left(P_1^{\beta_1} \cdots P_k^{\beta_k}\right) = P_1^{\alpha_1+\beta_1} \cdots P_k^{\alpha_k+\beta_k}.$$

Existuje vnoření ϕ multiplikativní grupy tělesa $K \setminus \{0\}$ do této Abelovské grupy, které je jednoznačně určeno předpisem $\phi(x) = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$ pro libovolný prvek $x \in \mathcal{O}_K$, $(x) = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$, kde zřejmě $\alpha_1, \ldots, \alpha_k > 0$ je rozklad hlavního ideálu generovaného x na součin prvoideálů v $\mathcal{O}_K$. Existence rozšíření takto definovaného ϕ na celé těleso K plyne z toho, že těleso K je podílovým tělesem oboru integrity $\mathcal{O}_K$. Tedy $\phi\left(\frac{x}{y}\right) = \phi(x) \cdot \phi^{-1}(y)$ pro $x, y \in \mathcal{O}_K$. Přesněji, pokud

$(x) = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$, kde $\alpha_1, \ldots, \alpha_k > 0$ a

$(y) = R_1^{\gamma_1} \cdots R_l^{\gamma_l}$, kde $\gamma_1, \ldots, \gamma_l > 0$, potom

$\phi\left(\frac{x}{y}\right) = P_1^{\alpha_1} \cdots P_k^{\alpha_k} \cdot R_1^{-\gamma_1} \cdots R_l^{-\gamma_l}$.

Důležitým faktem je následující tvrzení.

Věta 1.4.11. [[1], *věta* 8.4.3] *Pokud* $\phi(x) = P_1^{\alpha_1} \cdots P_k^{\alpha_k}$, *kde* $x \in K$ *a* $\alpha_i \in \mathbb{Z}$, *potom* $x \in \mathcal{O}_K$ *právě když všechna* $\alpha_i \geq 0$.

1.5 Vlastnosti celistvých prvků

Věta 1.5.1. [[1], *věta* 5.4.2] *Buď* $d \neq 1$ *bezčtvercový prvek,* $d \in \mathbb{Z}$, $K := \mathbb{Q}(\sqrt{d})$. *Pak platí:*

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{d}] & \text{pokud } d \equiv 2, 3 \pmod 4, \\ \mathbb{Z}[\frac{1+\sqrt{d}}{2}] & \text{pokud } d \equiv 1 \pmod 4. \end{cases}$$

Odsud je vidět, že $\mathcal{O}_K \subset \frac{1}{2}\mathbb{Z}[\sqrt{d}]$ pro libovolné přirozené bezčtvercové d. Toto tvrzení lze dále zobecnit. K tomuto účelu budeme potřebovat následující lemmata.

Lemma 1.5.2. *Nechť* L *je číselné těleso,* $d \in \mathbb{Z}$ *bezčtvercové a* $K = L(\sqrt{d})$ *je rozšíření* L *stupně 2. Pokud* $\alpha = \xi + \eta\sqrt{d}$ *je celistvý prvek v* $\mathcal{O}_K$, *pak* $\mathrm{tr}_{K/L}(\alpha), N_{K/L}(\alpha) \in \mathcal{O}_L$.

Důkaz. Z předpokladů věty víme, že $[K : L] = 2$. Tedy α je kořenem nějakého kvadratického monického polynomu $x^2 + bx + c$, kde $b, c \in L$. Nechť je $\alpha' = \xi' + \eta'\sqrt{d}$ druhým kořenem tohoto polynomu. Pak

$$\begin{aligned} &(x - \alpha)(x - \alpha') = 0, \text{ tedy} \\ &x^2 + (\alpha + \alpha')x + \alpha\alpha' = 0. \end{aligned}$$

Podle předpokladu musí $(\alpha + \alpha')$ i $\alpha\alpha'$ patřit do L. Takže:

$$\begin{aligned} (\alpha + \alpha') &= \xi + \xi' + (\eta + \eta')\sqrt{d}, \text{ tedy nutně } \eta = -\eta' \text{ a} \\ \alpha\alpha' &= \xi\xi' + (\eta\xi' - \xi\eta)\sqrt{d} - \eta^2 d, \text{ tedy nutně } \xi = \xi'. \end{aligned}$$

Jinými slovy, $\xi - \eta\sqrt{d}$ je druhým kořenem polynomu $x^2 + bx + c$.

Z předpokladů lemmatu je naše $\alpha = \xi + \eta\sqrt{d}$ z K celistvý prvek nad $\mathbb{Z}$, tedy je kořenem nějakého monického polynomu $P(x) \in \mathbb{Z}[x]$. Představíme-li si tento polynom jako polynom v $L[x]$, pak se dá podle věty o rozkladu polynomu na ireducibilní součinitele napsat jako součin ireducibilních polynomů $P(x) = Q_1(x)\cdots Q_n(x)$, $n \in \mathbb{N}$, z $L[x]$. Tedy existuje polynom $Q_i(x)$, $i \in \{1,\ldots,n\}$, jehož je α kořenem. Tento polynom nemůže být lineární, neboť by pak α muselo být z L, a také nemůže mít vyšší stupeň než 2, neboť již víme, že je α kořenem kvadratického polynomu nad L. Na začátku tohoto důkazu jsme však ukázali, že je-li kořenem polynomu $Q_i(x)$ prvek $\alpha = \xi + \eta\sqrt{d}$, pak je jeho kořenem i prvek $\alpha' = \xi - \eta\sqrt{d}$.

Jinými slovy, je-li $\xi + \eta\sqrt{d}$ celistvý prvek K, pak je jím nutně i $\xi - \eta\sqrt{d}$. Zároveň víme, že celistvost se zachová při sčítání i násobení. Tedy

$$\alpha + \alpha' \in \mathcal{O}_K \ \wedge \ \alpha + \alpha' = 2\xi \in L.$$

Z toho již nutně plyne, že $\mathrm{tr}_{K/L}(\alpha) = 2\xi \in \mathcal{O}_L$. Podobně

$$\alpha\alpha' \in \mathcal{O}_K \ \wedge \ \alpha\alpha' = \xi^2 - \eta^2 d \in L,$$

tedy $N_{K/L}(\alpha) = \xi^2 - \eta^2 d \in \mathcal{O}_L$. □

Lemma 1.5.3. *Nechť L je číselné těleso, $d \in \mathbb{Z}$ bezčtvercové a nesoudělné s diskriminantem $d(L)$ a $K = L(\sqrt{d})$ je rozšíření L stupně 2. Pokud $\alpha = \xi + \eta\sqrt{d}$ je celistvý prvek v $\mathcal{O}_K$, $\xi, \eta \in L$, pak $2\xi, 2\eta \in \mathcal{O}_L$.*

Důkaz. V lemmatu 1.5.2 jsme zjistili, že stopa a norma jsou celistvé prvky z $\mathcal{O}_L$. Dále platí, že i $4N(\alpha) = (2\xi)^2 - (2\eta)^2 d \in \mathcal{O}_L$. Protože $2\xi \in \mathcal{O}_L$, z toho plyne, že i $(2\eta)^2 d \in \mathcal{O}_L$. Nyní ukážeme, že již nutně musí $2\eta \in \mathcal{O}_L$. Sporem předpokládejme, že $2\eta \in L$ není celistvý prvek. Nechť $\phi(2\eta) = P_1^{\alpha_1}\cdots P_k^{\alpha_k}$, $\alpha_i \in \mathbb{Z}$ a $\phi(d) = Q_1^{\beta_1}\cdots Q_m^{\beta_m}$, $\beta_j \in \mathbb{N}$, kde P_i, Q_i jsou prvoideály. Protože prvočíselný rozklad $d = p_1 \cdot \ldots \cdot p_l$ je bezčtvercový a protože d je nesoudělné s $d(L)$, z věty 1.4.10 víme, že p_i se pro všechna i nevětví v $\mathcal{O}_L$. Tedy $\phi(p_i) = S_1 \cdot \ldots \cdot S_l$, kde S_i jsou navzájem různé prvoideály. Navíc z věty 1.4.6 pro $i \neq j$ platí, že $\phi(p_i)$ a $\phi(p_j)$ nemají ve svém rozkladu žádné společné prvoideály, tedy $\beta_j = 1$ pro $j = 1,\ldots,m$. Odtud plyne, že

$$\phi((2\eta)^2 d) = \phi(2\eta)\phi(2\eta)\phi(d) = P_1^{2\alpha_1}\cdots P_k^{2\alpha_k}\cdot Q_1\cdots Q_m.$$

Pokud by některé z α_i bylo menší než 0, potom by to znamenalo, že $\phi((2\eta)^2 d)$ stále obsahuje prvoideál se zápornou mocninou, což je podle věty 1.4.11 spor s tím, že $(2\eta)^2 d$ je prvkem $\mathcal{O}_L$. Tedy $\alpha_i > 0$ pro $i = 1,\ldots,k$. Odtud plyne, že $2\eta \in \mathcal{O}_L$. □

Věta 1.5.4. [[4], *věta* 2.1] *Nechť $d_1,\ldots,d_n$ jsou po dvou nesoudělná, bezčtvercová, přirozená čísla a $d_i \equiv 1 \pmod 4$. Potom platí:*

$$\mathcal{O}_{K_n} \subset \frac{1}{2^n}\mathbb{Z}\left[\sqrt{d_1},\ldots,\sqrt{d_n}\right].$$

Důkaz. Důkaz provedeme indukcí podle n. Pro $n = 1$ to plyne z věty 1.5.1. V indukčním kroku tedy stačí ukázat, že $\mathcal{O}_{K_n} \subset \frac{1}{2}\mathcal{O}_{K_{n-1}}[\sqrt{d_n}]$ pro $n \geq 2$. Podle předpokladu věty $d_j = \prod_i p_i^{(j)}$, $j = 1, \ldots, n$, kde $p_i^{(j)}$ jsou pro různé dvojice indexů (i, j) různá lichá prvočísla. Podle věty 1.1.11 je zřejmé, že $[K_n : K_{n-1}] = 2$, a podle 1.4.8 platí

$$d(K_{n-1}) = \left(\prod_{j=1}^{n-1} \prod_i p_i^{(j)} \right)^{2^{n-2}}.$$

Je zřejmé, že d_n je nesoudělné s $d(K_{n-1})$. Tedy podle lemmatu 1.5.3, pokud $\alpha = \xi + \eta\sqrt{d_n} \in \mathcal{O}_{K_n}$, potom $2\xi, 2\eta \in \mathcal{O}_{K_{n-1}}$. Podle indukčního předpokladu

$$\xi, \eta \in \frac{1}{2} \cdot \frac{1}{2^{n-1}} \mathbb{Z}\left[\sqrt{d_1}, \ldots, \sqrt{d_{n-1}}\right],$$
$$\text{a tedy } \alpha \in \frac{1}{2^n} \mathbb{Z}\left[\sqrt{d_1}, \ldots, \sqrt{d_n}\right].$$

□

1.6 Řád

Definice 1.6.1. *Nechť K je číselné těleso. $R \subset \mathcal{O}_K$ je řád, pokud platí, že*

(i) R je okruh,

(ii) $R(+)$ je podgrupa $\mathcal{O}_K(+)$ konečného indexu.

Poznámka 1.6.2. *Druhá část definice je ekvivalentní následující podmínce:*

(ii) Existuje báze $\alpha_1, \ldots, \alpha_n \in R$ taková, že*

- *$\alpha_1, \ldots, \alpha_n$ je báze K jako vektorového prostoru nad $\mathbb{Q}$,*
- *$\alpha_1, \ldots, \alpha_n$ je báze R jako $\mathbb{Z}-$modulu, tedy $R = \{\sum_i \alpha_i \ v_i \mid v_i \in \mathbb{Z}\}$.*

Definice 1.6.3. *Řád R v číselném tělese K se nazývá maximální řád, pokud $R = \mathcal{O}_K$.*

1.7 Totálně reálné číselné těleso

Definice 1.7.1. *Řekneme, že $\mathbb{Q}$-homomorfismus $\sigma : K \to \mathbb{C}$ je reálné vnoření, pokud $Im(\sigma) \subset \mathbb{R}$.*

Definice 1.7.2. *Říkáme, že K je totálně reálné číselné těleso, pokud všechna jeho vnoření do $\mathbb{C}$ jsou reálná.*

Nechť $K = \mathbb{Q}(\alpha)$ je číselné těleso, $\alpha_1, \ldots, \alpha_n$ jsou všechny kořeny minimálního polynomu α. Je zřejmé, že K je totálně reálné číselné těleso právě tehdy, když všechna α_i jsou reálná.

Definice 1.7.3. *Prvek $x \in K$ se nazývá totálně kladný, pokud pro každé vnoření $\sigma : K \to \mathbb{R}$ platí, že $\sigma(x) > 0$.*

Označíme K^+, resp. $\mathcal{O}_K^+$, množinu všech totálně kladných prvků z K, resp. z $\mathcal{O}_K$. Je zřejmé, že pokud $x = \sum_{i=1}^m y_i^2$ pro nějaká $y_i \in K$, potom $x \in K^+$. Opačnou implikaci dokázal Landau v roce 1919, tedy pokud $x \in K^+$, kde K je číselné těleso, potom $x = \sum_{i=1}^m y_i^2$ pro nějaká $y_i \in K$.

Definice 1.7.4. *Pokud R je komutativní okruh, jeho Pythagorovo číslo je definováno jako nejmenší přirozené číslo $P(R)$ takové, že každá suma čtverců v R se dá reprezentovat sumou $P(R)$ čtverců. Pokud takové $P(R)$ neexistuje, položíme Pythagorovo číslo rovno ∞.*

Tedy pro komutativní okruh R s Pythagorovým číslem $P < \infty$ platí, že je-li $x \in R$, $\alpha = \sum_{i=1}^m a_i^2$ pro nějaké $m \in \mathbb{N}$ a $a_i \in R$, pak existují $b_i \in R$ taková, že $x = \sum_{i=1}^{P(R)} b_i^2$.

2. Pythagorova čísla řádů v číselných tělesech

2.1 Značení a vlastnosti

Začněme zavedením jednotného značení, které bude platit do sekce 2.3.

$K_0 := \mathbb{Q}$; $\qquad K_{t+1} := K_t(\sqrt{d_{t+1}})$, $t = 0, \dots, n-1$,

kde $d_1, \dots, d_n$ je posloupnost přirozených čísel taková, že $K_{t+1} \neq K_t$.

$R_0 := \mathbb{Z}$; $\qquad R_{t+1} := R_t[\sqrt{d_{t+1}}]$, $t \in \mathbb{N}_0$,

$\beta_0 := 1$; $\qquad \beta_{t+1} := \beta_t + (1 + \sqrt{d_{t+1}})^2$, $t \in \mathbb{N}_0$,

$\mathrm{tr}_t : K_t \to \mathbb{Q}$ stopa,

$q_J := \prod_{i \in J} \sqrt{d_i}$, $J \subseteq \{1, \dots, t\}$.

Nyní si dokažme pár důležitých vlastností našich právě definovaných objektů.

Lemma 2.1.1. *Platí:*

$$\mathrm{tr}_t \left(\sum_{J \subseteq \{1,\dots,t\}} a_J q_J \right) = a_\emptyset \cdot 2^t.$$

Důkaz. Víme, že $[K_t : \mathbb{Q}] = 2^t$, a z věty 1.1.7 víme, že stopa nezávisí na volbě báze K_t jako vektorového prostoru nad $\mathbb{Q}$. Zvolme si tedy bázi $\{q_J\}_{J \subset \{1,\dots,t\}}$, jinými slovy bázi

$$\left\{ 1, \sqrt{d_1}, \dots, \sqrt{d_t}, \sqrt{d_1 d_2}, \dots, \sqrt{d_{t-1} d_t}, \dots, \sqrt{d_1 \cdots d_t} \right\}.$$

Pak se každý prvek $a \in K_t$ dá napsat jako $a = \sum_{J \subseteq \{1,\dots,t\}} a_J q_J$, kde $a_J \in \mathbb{Q}$ pro všechny indexy (podmnožiny) $J \subseteq \{1, \dots, t\}$. Stopa prvku a je z definice 1.1.6 rovna stopě matice B, kde

$$aq_I = \sum_{J \subseteq \{1,\dots,t\}} a_J q_I q_J = \sum_{J \subseteq \{1,\dots,t\}} b_{IJ} q_J \ \text{ pro každé } \ I \subset \{1, \dots, t\}, \ \text{ a tedy}$$

$$B = \begin{pmatrix} b_{\emptyset\emptyset} & b_{\emptyset\{1\}} & \cdots & b_{\emptyset\{1,\dots,t\}} \\ b_{\{1\}\emptyset} & b_{\{1\}\{1\}} & \cdots & b_{\{1\}\{1,\dots,t\}} \\ \vdots & \vdots & \ddots & \vdots \\ b_{\{1,\dots,t\}\emptyset} & b_{\{1,\dots,t\}\emptyset} & \cdots & b_{\{1,\dots,t\}\{1,\dots,t\}} \end{pmatrix}.$$

Matice B má zřejmě řád 2^t. Pro výpočet stopy prvku nás budou zajímat pouze prvky b_{JJ} na její diagonále. Naším cílem je ukázat, že každý takový prvek na diagonále je roven prvku $a_\emptyset$. Jinými slovy chceme ukázat, že

$$aq_I = a_\emptyset q_I + \sum_{J \subseteq \{1,\dots,t\} \setminus I} b_{IJ} q_J.$$

Roznásobením dostaneme

$$aq_I = a_\emptyset q_I q_\emptyset + a_{\{1\}} q_I q_{\{1\}} + \cdots + a_{\{1,\ldots,t\}} q_I q_{\{1,\ldots,t\}}.$$

Stačí si tedy uvědomit, že

$$q_I q_J = q_{I\cap J}^2 \cdot q_{(I\cup J)\setminus(I\cap J)},\ J \subseteq \{1,\ldots,t\},$$

a tedy $q_I q_J = q_I$ právě tehdy, když $J = \emptyset$. □

Důsledek 2.1.2. *Stopa prvku* $\left(\sum_{J\subseteq\{1,\ldots,t\}} a_J q_J\right)^2$ *splňuje:*

$$\mathrm{tr}_t\left(\left(\sum_{J\subseteq\{1,\ldots,t\}} a_J q_J\right)^2\right) = \left(\sum_{J\subseteq\{1,\ldots,t\}} a_J^2 q_J^2\right)\cdot 2^t.$$

Důkaz. Nechť $a = \sum_{J\subseteq\{1,\ldots,t\}} a_J q_J$. Označme si

$$a^2 = \sum_{J\subseteq\{1,\ldots,t\}} \sum_{I\subseteq\{1,\ldots,t\}} a_J a_I q_J q_I = \sum_{J\subseteq\{1,\ldots,t\}} A_J q_J.$$

Je zřejmé, že sčítance $a_J a_I q_J q_I \in \mathbb{Q}$ právě tehdy, když $I = J$. Tedy $A_\emptyset = \sum_{J\subseteq\{1,\ldots,t\}} a_J^2 q_J^2$. □

Nyní si spočítáme následující stopu prvku potřebnou k našemu pozdějšímu důkazu.

Lemma 2.1.3. *Stopa prvku* $\beta_t + 1 + d_{t+1}$ *v* K_t *se rovná*

$$\left(t + 2 + \sum_{s=1}^{t+1} d_s\right)\cdot 2^t.$$

Důkaz. Z lemmatu 2.1.1 již víme, že

$$\mathrm{tr}_t\left(a_0 + a_1\sqrt{d_1} + \cdots + a_{2^t}\sqrt{d_1\cdots d_t}\right) = a_0\cdot 2^t.$$

V našem případě

$$\beta_t + 1 + d_{t+1} = 1 + \sum_{s=1}^{t}(1+\sqrt{d_s})^2 + 1 + d_{t+1} =$$
$$1 + 2\sum_{s=1}^{t}\sqrt{d_s} + \sum_{s=1}^{t}(d_s+1) + 1 + d_{t+1}.$$

Tedy koeficient a_0 pro $\beta_t + 1 + d_{t+1}$ je roven $1 + \sum_{s=1}^{t}(d_s+1) + 1 + d_{t+1} = t + 2 + \sum_{s=1}^{t+1} d_s$. □

V dalších částech naší práce budeme potřebovat následující netriviální odhad stopy totálně kladných celistvých prvků.

Věta 2.1.4. [[4], *lemma* 5] *Nechť* $d_1,\ldots,d_n$ *jsou po dvou nesoudělná, bezčtvercová čísla taková, že* $d_i \equiv 1 \pmod 4$ *a nechť* $\alpha = \sum_{J\subseteq\{1,\ldots,n\}} a_J q_J \in \mathcal{O}_{K_n}^+$, $a_J \in \mathbb{Q}$. *Pokud* $a_J \neq 0$, *pak* $\mathrm{tr}_{K_n/\mathbb{Q}}(\alpha) > q_J$.

Důkaz. Nechť automorfismus $\sigma_i : K_n \to K_n$ je definován pomocí vztahů

$$\sigma_i(\sqrt{d_j}) = (-1)^{\delta_{ij}}\sqrt{d_j}, \;\; i,j \in \{1,\dots,n\},$$

kde δ_{ij} je Kroneckerovo delta. Pro $I \subset \{1,\dots,n\}$, nechť $\sigma_I = \prod_{i\in I}\sigma_i$. Protože α je totálně kladné, pro každé J platí, že $\sigma_J(\alpha) > 0$. Nyní dokážeme, že platí:

$$(I) \sum_{J,\, \#J\cap I \text{ sudé}} \sigma_J(\alpha) = 2^{n-1}(a_\emptyset + a_I q_I) > 0,$$
$$(II) \sum_{J,\, \#J\cap I \text{ liché}} \sigma_J(\alpha) = 2^{n-1}(a_\emptyset - a_I q_I) > 0.$$

Dokážeme případ, kdy počet prvků v $J \cap I$ je sudý. Pro lichý počet prvků je důkaz analogický.

Nejprve si uvědomíme, že pro naše výše pevně zvolené I platí, že

$$\sigma_J(q_I) = q_I, \text{ pro všechna } J \text{ taková, že } \#J \cap I \text{ sudé.}$$

Pro obecnou podmnožinu $K \subset \{1,\dots,n\}$ tedy platí:

$$\sigma_J(q_K) = (-1)^{\#J\cap K}\cdot q_K, \text{ pro všechna } J \subset \{1,\dots,n\}.$$

Nyní dokážeme, že pro $K \neq \emptyset, I$ platí, že

$$\sum_{J,\, \#J\cap I \text{ sudé}} \sigma_J(q_K) = 0.$$

Nejprve předpokládejme, že K je takové, že existuje $k \in K \setminus I$. Pak si množinu všech J takových, že $\#J \cap I$ sudé, rozdělíme na dvě podmnožiny

$$\Omega_1^k = \{J : \#J \cap I sudé, k \in J\},$$
$$\Omega_2^k = \{J : \#J \cap I sudé, k \notin J\}.$$

Mezi těmito dvěma množinami zřejmě existuje bijekce, která $J \in \Omega_2^k$ přiřadí $J \cup \{k\} \in \Omega_1^k$. Pak platí:

$$\sum_{J,\, \#J\cap I \text{ sudé}} \sigma_J(q_K) = \sum_{J\in\Omega_1^k} \sigma_J(q_K) + \sum_{J\in\Omega_2^k} \sigma_J(q_K) = 0,$$

neboť pro každé $J \in \Omega_2^k$ platí:

$$\sigma_{J\cup\{k\}}(q_K) + \sigma_J(q_K) = \left((-1)^{\#J\cup\{k\}\cap K} + (-1)^{\#J\cap K}\right)\cdot q_K = 0.$$

Nyní předpokládejme, že $\emptyset \neq K \subsetneq I$. Nechť $i \in I \setminus K$ a $k \in K$. Opět si rozdělíme množinu všech J takových, že $\#J \cap I$ sudé na dvě podmnožiny

$$\Omega_1^i = \{J : \#J \cap I sudé, i \in J\},$$
$$\Omega_2^i = \{J : \#J \cap I sudé, i \notin J\}.$$

Mezi těmito dvěma množinami zřejmě existuje bijekce, která $J \in \Omega_2^i$, $k \notin J$, přiřadí $J \cup \{i,k\} \in \Omega_1^i$, a která $J \in \Omega_2^i$, $k \in J$, přiřadí $(J \cup \{i\}) \setminus \{k\} \in \Omega_1^i$. Je

zřejmé, že tato bijekce zachovává paritu $J \cap I$ a zároveň mění paritu $J \cap K$. Tedy opět platí:

$$\sum_{J,\, \#J\cap I \text{ sudé}} \sigma_J(q_K) = \sum_{J\in\Omega_1^i} \sigma_J(q_K) + \sum_{J\in\Omega_2^i} \sigma_J(q_K) = 0.$$

Z toho plyne, že

$$\sum_{J,\, \#J\cap I \text{ sudé}} \sigma_J(\alpha) = \sum_{J,\, \#J\cap I \text{ sudé}} \sigma_J\left(\sum_{K\subset\{1,\dots,n\}} a_K q_K\right) =$$
$$= \sum_{K\subset\{1,\dots,n\}} a_K \sum_{J,\, \#J\cap I \text{ sudé}} \sigma_J(q_K) = 2^{n-1}(a_\emptyset + a_I q_I),$$

neboť počet J takových, že $\#J \cap I$ sudé, je 2^{n-1}.

Porovnáním dvou nerovností (I) a (II) tedy získáme $a_\emptyset > |a_I|\, q_I \geq \frac{1}{2^n} q_I$, neboť $a_I \neq 0$, a tedy z 1.5.4 $a_I \in \frac{1}{2^n}\mathbb{Z}$. Toto implikuje, že $\mathrm{tr}_{K_n/\mathbb{Q}}(\alpha) = 2^n a_\emptyset > q_I$. □

2.2 Řády v totálně reálných číselných tělesech

Věta 2.2.1. [[10], *tvrzení* 1] *Existují řády v totálně reálných číselných tělesech, jejichž Pythagorova čísla jsou libovolně velká.*

Vzhledem k tomu, že $\beta_t \in R_t$, $t \in \mathbb{N}$, důkaz této věty plyne z následujícího lemmatu.

Lemma 2.2.2. [[10], *lemma* 2] *Předpokládejme, že pro všechna t přirozená platí*

(o) $d_{t+1} > t + 2 + \sum_{s=1}^{t} d_s$.

Pak β_t nelze reprezentovat méně než t+1 čtverci v R_t.

Důkaz. Budeme postupovat indukcí.

Pro $t = 0$ zřejmě β_t nemůže být reprezentováno méně než jedním čtvercem.

Indukční krok $t \longrightarrow t + 1$.

Předpokládejme sporem, že $\beta_{t+1} = \sum_{i=1}^{m} {\alpha_i}^2$, $\alpha_i \in R_{t+1}$ a $m < t + 2$.

Označme $\alpha_i = \xi_i + \eta_i\sqrt{d_{t+1}}$, kde $\xi_i, \eta_i \in R_t$. Pak

$\beta_{t+1} = \sum_{i=1}^{m} {\alpha_i}^2 = \sum_{i=1}^{m}(\xi_i^2 + d_{t+1}\eta_i^2) + (\sum_{i=1}^{m} 2\xi_i\eta_i)\sqrt{d_{t+1}}$ a

$\beta_{t+1} = \beta_t + (1 + \sqrt{d_{t+1}})^2 = (\beta_t + 1 + d_{t+1}) + 2\sqrt{d_{t+1}}$.

Porovnáním odpovídajících koeficientů vidíme, že

(*) $\sum_{i=1}^{m}(\xi_i^2 + d_{t+1}\eta_i^2) = \beta_t + 1 + d_{t+1}$,

(**) $\sum_{i=1}^{m} \xi_i\eta_i = 1$.

Z lemmatu 2.1.3 již víme, že stopa prvku $\beta_t + 1 + d_{t+1}$ je rovna

$$\left(t + 2 + \sum_{s=1}^{t+1} d_s\right) \cdot 2^t.$$

Z předpokladu (o) našeho lemmatu pak plyne nerovnost:

$$\mathrm{tr}_t(\beta_t + 1 + d_{t+1}) = \left(t + 2 + \sum_{s=1}^{t+1} d_s\right) \cdot 2^t < 2d_{t+1} \cdot 2^t.$$

Nyní budeme dokazovat, že existuje nejvýše jedno j, pro které $\eta_j \neq 0$, a pro takto zvolené η_j je $|\eta_j| = 1$. Budeme postupovat sporem. Nejprve předpokládejme, že existuje $|\eta_j| > 1$. Označme $\eta_j = \sum_{J\subseteq\{1,\ldots,t\}} a_J q_J$, kde $a_J \in \mathbb{Z}$. Z důsledku 2.1.2 víme, že

$$\mathrm{tr}_t(\eta_j^2) = \mathrm{tr}_t\left(\left(\sum_{J\subseteq\{1,\ldots,t\}} a_J q_J\right)^2\right) = \left(\sum_{J\subseteq\{1,\ldots,t\}} a_J^2 q_J^2\right) \cdot 2^t.$$

Všimněme si, že q_J^2 jsou přirozená čísla a pro $J \neq \emptyset$ máme $q_J^2 \geq 2$. Pokud tedy $|\eta_j| > 1$, potom $\left(\sum_{J\subseteq\{1,\ldots,t\}} a_J^2 q_J^2\right) \geq 2$.

Z toho plyne, že platí nerovnost:

$$\mathrm{tr}_t(d_{t+1}\eta_j^2) = d_{t+1} \cdot \mathrm{tr}_t(\eta_j^2) \geq d_{t+1} \cdot 2 \cdot 2^t.$$

Z vlastnosti aditivity stopy a důsledku 2.1.2 pak navíc máme:

$$\mathrm{tr}_t\left(\sum_{i=1}^{m}(\xi_i^2 + d_{t+1}\eta_i^2)\right) \geq \mathrm{tr}_t(d_{t+1}\eta_j^2).$$

Tedy

$$2d_{t+1} \cdot 2^t > \left(t + 2 + \sum_{s=1}^{t+1} d_s\right) \cdot 2^t = \mathrm{tr}_t(\beta_t + 1 + d_{t+1}) =$$
$$= \mathrm{tr}_t\left(\sum_{i=1}^{m}(\xi_i^2 + d_{t+1}\eta_i^2)\right) \geq \mathrm{tr}_t(d_{t+1}\eta_j^2) \geq d_{t+1} \cdot 2 \cdot 2^t,$$

což je spor. Z toho plyne, že $|\eta_j| \leq 1$ pro všechna j. Pokud $|\eta_j| = 1$, potom $\eta_i = 0$ pro všechna $i \neq j$, protože jinak by stopa levé strany $(*)$ byla $\geq 2d_{t+1} \cdot 2^t$. Tedy $(**)$ je nyní ekvivalentní rovnosti $\xi_j = \pm 1$ a $(*)$ zase rovnosti

$$\sum_{i=1, i\neq j}^{m} \xi_i^2 = \beta_t,\ \xi_i \in R_t.$$

Takže β_t je součtem $m-1$ čtverců z R_t, kde jsme předpokládali, že $m-1 < t+1$. To je ovšem spor s indukčním předpokladem, že β_t není součtem méně než $t+1$ čtverců. □

Řády R_t obecně nejsou maximální pro $t \geq 2$. Například

$$\mathcal{O}_{\mathbb{Q}_{(\sqrt{2},\sqrt{3})}} = \left\{a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\frac{\sqrt{2}+\sqrt{6}}{2} \mid a_0, a_1, a_2, a_3 \in \mathbb{Z}\right\} \neq \mathbb{Z}[\sqrt{2}, \sqrt{3}].$$

V následujících sekcích si ukážeme, že věta platí i tak, pokud se zaměříme na maximální řády.

2.3 Značení a vlastnosti

Nechť $N \in \mathbb{N}$ a nechť $d_1, \ldots, d_N$ jsou bezčtvercová, po dvou nesoudělná čísla větší než 2^{4N+2} taková, že $d_t \equiv 1 \pmod 4$, a taková, aby platilo:

$$(\bullet) \quad \frac{d_{t+1}}{4} > 2 + d_1 + \sum_{s=2}^{t} \frac{d_1 + d_s}{4} + \frac{d_1}{4},\ t = 1, \ldots, N-1.$$

Tedy $d_1, \ldots, d_N$ je rostoucí posloupnost. Dále nechť:

$$K_0 := \mathbb{Q}; \qquad K_{t+1} := K_t(\sqrt{d_{t+1}}),\ t = 0, \ldots, N-1,$$

$$R_0 := \mathbb{Z}; \qquad R_{t+1} := \mathcal{O}_{K_{t+1}}.$$

Položme $\beta_0 := 1$ a definujme:

$$\beta_1 := \beta_0 + \left(1 + \sqrt{d_1}\right)^2; \qquad \beta_{t+1} := \beta_t + \left(\frac{\sqrt{d_1} + \sqrt{d_{t+1}}}{2}\right)^2, t = 1, \ldots, N-1.$$

Lemma 2.3.1. *$\beta_t \in K_t$ pro všechna $t \leq N$.*

Důkaz. Důkaz provedeme indukcí. Pro $t = 0, 1$ je to zřejmé. Z 1.5.1 dále víme, že je-li $d_{t+1} \equiv 1 \pmod 4$, pak $\mathcal{O}_{\mathbb{Q}[\sqrt{d_{t+1}}]} = \mathbb{Z}\left[\frac{1+\sqrt{d_{t+1}}}{2}\right]$. Rozepsáním

$$\left(\frac{\sqrt{d_1} + \sqrt{d_{t+1}}}{2}\right) = \left(\frac{1 + \sqrt{d_1}}{2}\right) + \left(\frac{1 + \sqrt{d_{t+1}}}{2}\right) - 1$$

vidíme, že $\left(\frac{\sqrt{d_1}+\sqrt{d_{t+1}}}{2}\right) \in K_{t+1}$. Tedy i $\beta_{t+1} = \beta_t + \left(\frac{\sqrt{d_1}+\sqrt{d_{t+1}}}{2}\right)^2 \in K_{t+1}$ pro všechna $t < N$. □

Nyní si spočítáme následující stopu prvku potřebnou k našemu pozdějšímu důkazu.

Lemma 2.3.2. *Stopa prvku $\beta_t + \frac{d_1+d_{t+1}}{4}$ v K_t se rovná*

$$\left(2 + d_1 + \sum_{s=2}^{t+1} \frac{d_1 + d_s}{4}\right) \cdot 2^t.$$

Důkaz. Víme, že

$$\beta_t + \frac{d_1 + d_{t+1}}{4} = \frac{d_1 + d_{t+1}}{4} + 2 + d_1 + 2\sqrt{d_1} + \sum_{s=2}^{t} \left(\frac{\sqrt{d_1} + \sqrt{d_s}}{2}\right)^2 =$$

$$= 2 + d_1 + 2\sqrt{d_1} + \sum_{s=2}^{t+1} \frac{d_1 + d_s}{4} + \sum_{s=2}^{t} \frac{\sqrt{d_1}}{2}\sqrt{d_s}.$$

Dále víme, že $[K_t : \mathbb{Q}] = 2^t$ a z věty 1.1.7 již víme, že stopa prvku nezávisí na volbě báze vektorového prostoru K_t nad $\mathbb{Q}$. Zvolme si tedy zase bázi $\{q_J\}_{J \subset \{1,\ldots,t\}}$. Z lemmatu 2.1.1 pak plyne, že

$$\mathrm{tr}_t\left(\beta_t + \frac{d_1 + d_{t+1}}{4}\right) = \left(2 + d_1 + \sum_{s=2}^{t+1} \frac{d_1 + d_s}{4}\right) \cdot 2^t.$$

□

2.4 Pythagorova čísla maximálních řádů

Věta 2.4.1. [[10], *tvrzení* 3] *Pro libovolné $N \in \mathbb{N}$ existuje totálně reálné číselné těleso, jehož maximální řád má Pythagorovo číslo alespoň N.*

Důkaz. Budeme dokazovat indukcí pro $t = 1, \ldots, N$, že $\beta_t \in R_t$ nelze napsat jako součet méně než $t+1$ čtverců v R_t. Tedy Pythagorovo číslo R_t je alespoň $t+1$ a speciálně Pythagorovo číslo R_N je alespoň $N+1$.

Pro $t = 0$ zřejmě β_t nemůže být reprezentováno méně než jedním čtvercem.

Indukční krok $t \longrightarrow t+1$.

Předpokládejme sporem, že $\beta_{t+1} = \sum_{i=1}^{m} {\alpha_i}^2$, $\alpha_i \in R_{t+1}$ a $m < t+2$.

Označme $\alpha_i = \xi_i + \eta_i\sqrt{d_{t+1}}$, kde z 1.5.3 již víme, že $2\xi_i, 2\eta_i \in R_t$. Stejně jako v důkazu lemmatu 2.2.2 porovnáním koeficientů

$\beta_{t+1} = \sum_{i=1}^{m} {\alpha_i}^2 = \sum_{i=1}^{m}(\xi_i^2 + d_{t+1}\eta_i^2) + (\sum_{i=1}^{m} 2\xi_i\eta_i)\sqrt{d_{t+1}}$ a

$\beta_{t+1} = \left(\beta_t + \frac{d_1+d_{t+1}}{4}\right) + \frac{2\sqrt{d_1}}{4}\sqrt{d_{t+1}}$ získáme:

(*) $\sum_{i=1}^{m}(\xi_i^2 + d_{t+1}\eta_i^2) = \beta_t + \frac{d_1+d_{t+1}}{4}$,

(**) $\sum_{i=1}^{m} \xi_i\eta_i = \frac{\sqrt{d_1}}{4}$.

Z lemmatu 2.3.2 již víme, že stopa prvku $\beta_t + \frac{d_1+d_{t+1}}{4}$ je rovna

$$\left(2 + d_1 + \sum_{s=2}^{t+1} \frac{d_1+d_s}{4}\right) \cdot 2^t.$$

Z předpokladu (•) ze začátku sekce 2.3 pak plyne nerovnost:

$$\mathrm{tr}_t\left(\beta_t + \frac{d_1+d_{t+1}}{4}\right) = \left(\frac{d_{t+1}}{4} + 2 + d_1 + \sum_{s=2}^{t} \frac{d_1+d_s}{4} + \frac{d_1}{4}\right) \cdot 2^t < \left(\frac{d_{t+1}}{2}\right) \cdot 2^t.$$

Nyní dokážeme, že existuje nejvýše jedno j tak, aby $\eta_j \neq 0$, a navíc pro takto vybrané j platí, že $|2\eta_j| = 1$. Budeme postupovat sporem.

Nechť j je takové, že $\eta_j \neq 0$ a $(2\eta_j)^2 = \sum_{J\subseteq\{1,\ldots,t\}} c_J q_J$, $c_J \in \mathbb{Q}$. Všimněme si, že $(2\eta_j)^2$ je totálně kladný prvek. Nyní sporem dokážeme, že $(2\eta_j)^2 \in \mathbb{Q}$. Kdyby ne, pak $c_J \neq 0$ pro nějaké $J \neq \emptyset$, a z věty 2.1.4 pak plyne, že

$\mathrm{tr}_t((2\eta_j)^2) > q_J \geq \sqrt{d_1} > 2^{2N+1} \geq 2^{t+1}$, a tedy

$\mathrm{tr}_t(d_{t+1}\eta_j^2) = \frac{1}{4}d_{t+1} \cdot \mathrm{tr}_t((2\eta_j)^2) > \frac{1}{4}d_{t+1} \cdot 2^{t+1}$.

Z vlastnosti aditivity stopy a důsledku 2.1.2 navíc máme

$$\mathrm{tr}_t\left(\sum_{i=1}^{m}(\xi_i^2 + d_{t+1}\eta_i^2)\right) \geq \mathrm{tr}_t(d_{t+1}\eta_j^2).$$

Z toho plyne, že

$$\left(\frac{d_{t+1}}{2}\right) \cdot 2^t > \left(2 + d_1 + \sum_{s=2}^{t+1} \frac{d_1+d_s}{4}\right) \cdot 2^t = \mathrm{tr}_t\left(\beta_t + \frac{d_1+d_{t+1}}{4}\right) =$$
$$= \mathrm{tr}_t\left(\sum_{i=1}^{m}(\xi_i^2 + d_{t+1}\eta_i^2)\right) \geq \mathrm{tr}_t(d_{t+1}\eta_j^2) > d_{t+1} \cdot \frac{1}{2} \cdot 2^t,$$

což je spor. Tedy $(2\eta_j)^2$ je prvkem $\mathbb{Q}$.

Nechť $2\eta_j = \sum_{J\subseteq\{1,\dots,t\}} h_J q_J$, kde z věty 1.5.4 víme, že $h_J \in \frac{\mathbb{Z}}{2^t}$. Vidíme, že existuje právě jedno J, pro které $h_J \neq 0$, protože $(2\eta_j)^2 \in \mathbb{Q}$. Kdyby $J \neq \emptyset$, potom

$$\mathrm{tr}_t((2\eta_j)^2) = h_J^2 \cdot q_J^2 \geq \frac{q_J^2}{2^{2t}} > 2^{t+1}.$$

Toto vede opět ke sporu, stejně jako v předchozím případě.

Takže $J = \emptyset$, a tedy $2\eta_j \in \mathbb{Q}$. Tento prvek je celistvý nad $\mathbb{Z}$, a tedy musí z věty 1.3.3 (i) být již nutně prvkem $\mathbb{Z}$. Z toho plyne, že $\eta_j = \pm\frac{1}{2}$, protože jinak by nebyla splněna rovnost $(*)$. Navíc $\eta_i = 0$ pro všechna $i \neq j$, protože jinak by stopa levé strany $(*)$ byla $\geq \left(\frac{d_{t+1}}{2}\right) \cdot 2^t$. Tedy $(**)$ je nyní ekvivalentní rovnosti $\xi_j = \pm\frac{\sqrt{d_1}}{2}$ a $(*)$ zase rovnosti

$$\sum_{i=1, i\neq j}^{m} \xi_i^2 = \beta_t.$$

Na začátku tohoto důkazu jsme předpokládali, že $\alpha_i = \xi_i + \eta_i\sqrt{d_{t+1}} = \xi_i \in R_{t+1}$ pro i různá od j. Navíc víme, že $\xi_i \in K_t$, a tedy již musí nutně $\xi_i \in R_t$ pro všechna i různá od j.

Tedy β_t je součtem $m-1$ čtverců z R_t, kde jsme předpokládali, že $m-1 < t+1$. To je ovšem spor s indukčním předpokladem, že β_t není součtem méně než $t+1$ čtverců. □

Závěr

Hlavním cílem této bakalářské práce bylo srozumitelně a formálně správně sepsat druhý Scharlauův důkaz z článku [10]. Tohoto cíle se mi podařilo dosáhnout za cenu modifikací předpokladů i důkazu. Z technického hlediska moje formulace využívá jiné předpoklady na posloupnost $\{d_1, \ldots, d_N\}$. Zatímco Scharlau předpokládá, že $d_i \equiv 3 \pmod 4$, mé tvrzení využívá předpokladu, že $d_i \equiv 1 \pmod 4$. To ovšem není jediný rozdíl. Zatímco Scharlau navrhuje použít nekonečnou posloupnost $\{d_1, d_2, \ldots\}$, ze které lze vybrat libovolný počáteční úsek $\{d_1, \ldots, d_N\}$, a pro takto zvolený počáteční úsek již platí, že $P(\mathcal{O}_{K_N}) \geq N$, můj důkaz pro pevně zvolené N vyžaduje odlišnou posloupnost $\{d_1, \ldots, d_N\}$. Můj důkaz navíc využívá především výsledky o hodnotě diskriminantu a dále využívá odhadu stopy totálně kladných prvků z článku [4].

Povšimněme si, že v těchto výsledcích řád, který má Pythagorovo číslo alespoň N, je zkonstruován uvnitř číselného tělesa, jehož stupeň rozšíření je alespoň 2^N. To vede k přirozené otázce, kterou Scharlau na konci svého článku pokládá, zdali existuje funkce $f : \mathbb{N} \to \mathbb{N}$ taková, že pokud stupeň rozšíření číselného tělesa K je $[K : Q] \leq N$, potom Pythagorovo číslo každého řádu v K je rovno nejvýše $f(N)$. Bylo dokázáno, že toto tvrzení skutečně platí, v článku [5] V. Kaly a P. Yatsyna.

Seznam použité literatury

[1] Ş. Alaca, K. S. Williams, *Introductory algebraic number theory* (2004), Cambridge University Press

[2] D. Hilbert, *Theorie der algebraischen Zahlkörper*, in Encyklopädie der Mathematischen Wissenschaften, Volume 1, Part 2 of Arithmetik und Algebra, Leipzig (1900 - 1904)

[3] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory* (1982), Springer-Verlag

[4] V. Kala, J. Svoboda, *Universal quadratic forms over multiquadratic fields*, Ramanujan J. 48 (2019), 151–157

[5] V. Kala, P. Yatsyna, *Lifting problem for universal quadratic forms* (2017), Naposledy navštíveno 14. 4. 2020. URL `https://arxiv.org/abs/1808.02262`

[6] J. L. Lagrange, *Démonstration d'un Théoréme D'Arithmétique*, Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin (1770)

[7] E. Landau, *Uber die Zerlegung total positiver Zahlen in Quadrate*, Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, mathematischphysikalische Klasse, Jahrgang (1919), 392–396

[8] M. Peters, *Summen von Quadraten in Zahlringen*, J. reine angew. Math. 268/269 (1974), 318—323

[9] A. Pfister, *Quadratic forms with applications to algebraic geometry and topology*, London Math. Soc. Lect. Notes 217 (1995), Cambridge University Press

[10] R. Scharlau, *On the Pythagoras number of orders in totally real number fields* (1980), J. Reine Angew. Math. 316, 208-210

[11] B. Schmal, *Diskriminanten, $\mathbb{Z}$-Ganzheitsbasen und relative Ganzheitsbasen bei multiquadratischen Zahlkörpern*, Arch. Math. 52 (1989), 245-257

[12] C. Siegel, *Darstellung total positiver Zahlen durch Quadrate*, Math. Zeit., 11 (1921), 246–275

[13] D. Stanovský, *Základy algebry* (2009), Matfyzpress

[14] J. Šaroch, *Lineární nezávislost druhých mocnin*, Naposledy navštíveno 12. 2. 2020. URL `http://karlin.mff.cuni.cz/~kala/1819%20ko/odm.pdf`