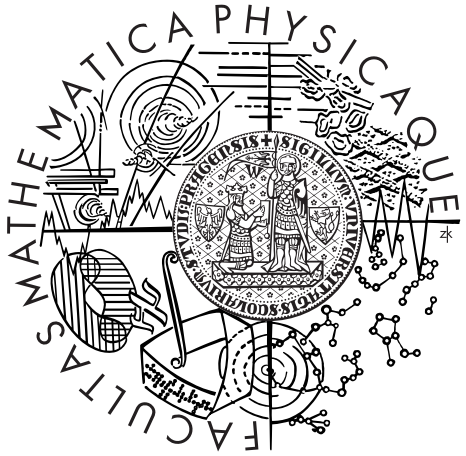
Univerzita Karlova v Praze
Matematicko-fyzikální fakulta

BAKALÁŘSKÁ PRÁCE



Kristýna Zemková

Normově-euklidovská kvadratická rozšíření tělesa racionálních čísel

Katedra algebry

Vedoucí bakalářské práce: Mgr. Jan Šaroch, Ph.D.

Studijní program: Matematika

Studijní obor: Obecná matematika

Praha 2015

Ráda bych poděkovala Mgr. Janu Šarochovi, Ph.D. za vedení a odborné rady v průběhu zpracování této bakalářské práce. Dále bych chtěla poděkovat svým rodičům, kteří mě vždy podporovali v mé zálibě v matematice.

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) 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 v Praze má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ..... Podpis autora

Název práce: Normově-euklidovská kvadratická rozšíření tělesa racionálních čísel

Autor: Kristýna Zemková

Katedra: Katedra algebry

Vedoucí bakalářské práce: Mgr. Jan Šaroch, Ph.D., Katedra algebry

Abstrakt: Cílem této práce je podat ucelenou charakterizaci všech normově-euklidovských kvadratických rozšíření $\mathbb{Q}$. Práce obsahuje kompletně zpracovanou část pro imaginární kvadratická rozšíření. V případě reálných kvadratických rozšíření uvádíme úplný seznam diskriminantů D, pro něž je těleso $\mathbb{Q}(\sqrt{D})$ normově-euklidovské. Dále je v práci obsažen důkaz odhadu $D < 2^{14}$ pro všechna $\mathbb{Q}(\sqrt{D})$ normově-euklidovská a podrobně rozebraný případ $D \not\equiv 1 \pmod 4$. Pro případ $D \equiv 1 \pmod 4$ jsou v práci uvedeny odkazy na výsledky jiných autorů.

Klíčová slova: euklidovská norma, kvadratické rozšíření, diskriminant

Title: Norm-euclidean quadratic extensions of the field of rational numbers

Author: Kristýna Zemková

Department: Department of Algebra

Supervisor: Mgr. Jan Šaroch, Ph.D., Department of Algebra

Abstract: The goal of this work is to characterize all norm-euclidean quadratic extensions of $\mathbb{Q}$. The work treats completely the part of imaginary quadratic extensions. In the case of real quadratic extensions, we give a list of such discriminants D that the field $\mathbb{Q}(\sqrt{D})$ is norm-euclidean. Furthermore, we prove an estimate $D < 2^{14}$ for all norm-euclidean fields $\mathbb{Q}(\sqrt{D})$. Subsequently, the case $D \not\equiv 1 \pmod 4$ is discussed in detail. For the case $D \equiv 1 \pmod 4$ we mention references to the results of other authors.

Keywords: euclidean norm, quadratic extension, discriminant

Obsah

Úvod

Všichni známe celá a racionální čísla a snad každý z nás se na základní škole učil dělit se zbytkem, později na střední škole se mnozí potkali s komplexními čísly. Asi jen málokdo si pod pojmem komplexní číslo představí číslo $\pi - \frac{\sqrt{3}}{5}\,\mathrm{i}$, většinou nám spíše vytane na mysli něco na způsob $2 + 3\,\mathrm{i}$. Snad díky jejich intuitivnosti dostala čísla tvaru $a + b\,\mathrm{i}$, $a, b \in \mathbb{Z}$, svůj vlastní název – jde o Gaussova celá čísla. Podobně jako na celých číslech můžeme i zde dělit se zbytkem. Tuto operaci lze dobře definovat také například na číslech $\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\right\}$.

Mohlo by se zdát, že takto můžeme k množině celých čísel přidat prakticky cokoliv a dělení se zbytkem bude stále fungovat, avšak není tomu tak. U dělení se zbytkem totiž požadujeme, aby byl zbytek „menší“ než číslo, kterým dělíme. Zatímco na celých číslech je jednoduché rozhodnout, které číslo je menší, pro Gaussova celá čísla již potřebujeme zavést nějakou „velikost“ čísla, tzv. normu. Tato norma by měla Gaussovu celému číslu přiřadit nějaké přirozené číslo, protože ta umíme mezi sebou dobře porovnávat. Kromě toho samozřejmě požadujeme, aby zbytek po dělení měl menší normu než dělitel. Intuitivně můžeme tuto normu volit jako druhou mocninu absolutní hodnoty komplexního čísla, tedy $|a + b\,\mathrm{i}|^2 = a^2 + b^2$ (druhá mocnina je zde proto, abychom se vyhnuli nepříjemnému odmocňování). Ukazuje se, že tato volba splňuje všechny naše požadavky. Obdobně v $\mathbb{Z}[\sqrt{2}]$ za normu čísla $a + b\sqrt{2}$ položíme číslo $|a^2 - 2b^2|$. Není těžké si ověřit, že pak je například $(10 + 4\sqrt{2}) : (3 - \sqrt{2}) = 5 + 3\sqrt{2}$ (zb. 1), kde norma zbytku je 1 a norma čísla $3 - \sqrt{2}$ je 7. Pokud bychom ale stejným způsobem chtěli počítat v $\mathbb{Z}[\sqrt{5}]$ s normou $|a^2 - 5b^2|$, narazíme na problém. Je $(1 + \sqrt{5}) : 2 = 0$ (zb. $1 + \sqrt{5}$) a přitom norma obou čísel je rovna 4. Dokonce platí, že $4 = 2 \cdot 2 = (1 + \sqrt{5})(-1 + \sqrt{5})$, tedy v $\mathbb{Z}[\sqrt{5}]$ nemáme analogii jednoznačného rozkladu na prvočísla a tento fakt platí nezávisle na volbě normy. Na stejný problém narazíme také třeba v $\mathbb{Z}[\sqrt{23}]$, kde $22 = 2 \cdot 11 = (1 + \sqrt{23})(-1 + \sqrt{23})$.

Na principu dělení se zbytkem je založen Euklidův algoritmus, který je lidstvu známý již od dob starověku, kdy jej Euklides uvedl ve svém díle Základy. Proto dostaly číselné obory, ve kterých dobře funguje dělení se zbytkem, název podle tohoto filozofa – Euklidovy obory. Podobně, jako jsou celá čísla přirozeným způsobem vnořena do tělesa racionálních čísel, můžeme také čísla ze $\mathbb{Z}[\sqrt{2}]$ vnořit do tělesa $\mathbb{Q}(\sqrt{2}) = \left\{r + s\sqrt{2} \mid r, s \in \mathbb{Q}\right\}$. Tělesa, jejichž „celá čísla“ tvoří Euklidův obor, se pak nazývají normově-euklidovská. Například tělesa $\mathbb{Q}(\mathrm{i})$, $\mathbb{Q}(\sqrt{2})$ jsou normově-euklidovská, zatímco těleso $\mathbb{Q}(\sqrt{23})$ normově-euklidovské není. Překvapivý může být fakt, že $\mathbb{Q}(\sqrt{5})$ je normově-euklidovské těleso, přestože jsme si řekli, že $\mathbb{Z}[\sqrt{5}]$ není Euklidův obor. To je ovšem způsobeno tím, že „celá čísla“ (přesněji celá algebraická čísla) v $\mathbb{Q}(\sqrt{5})$ nejsou čísla $\mathbb{Z}[\sqrt{5}]$, nýbrž čísla tvaru $\frac{a}{2} + \frac{b}{2}\sqrt{5}$, kde a, b jsou celá čísla, která jsou buďto obě sudá, nebo obě lichá.

Cílem této práce je popsat všechna celá čísla D, pro která je těleso $\mathbb{Q}(\sqrt{D})$ normově-euklidovské. Tento problém je již kompletně vyřešený, nicméně je roztříštěný do mnoha publikací a článků. Úkolem tedy bude především všechny tyto střípky sjednotit do jedné práce a důkazy pokud možno zjednodušit.

V práci jsou uvedeny definice všech důležitých pojmů, přesto však od čtenáře očekáváme základní znalosti algebry. Kapitola 1 se zabývá pouze jednoduchými a obecně známými fakty z obecné algebry, čtenář obeznámený s touto partií matematiky ji proto může vynechat. V kapitole 2 již uvedeme přesnou definici normově-euklidovského tělesa a rozebereme poměrně jednoduchý případ imaginárních kvadratických rozšíření, tedy těles $\mathbb{Q}(\sqrt{D})$ s $D < 0$. V kapitole 3 pomocí geometrické představy čísel z $\mathbb{Q}(\sqrt{D})$ jakožto bodů v rovině a středoškolské matematiky ukážeme jednoduchým, avšak poměrně pracným způsobem, že pro některá daná čísla D už je těleso $\mathbb{Q}(\sqrt{D})$ normově-euklidovské. V závěrečné sekci 3.3 se také ještě krátce vrátíme k imaginárním kvadratickým rozšířením, abychom ukázali na geometrické představě jejich odlišnost od reálných kvadratických rozšíření, a současně převedeme důkaz ze druhé kapitoly do „geometrické“ podoby. Kapitola 4 si klade za cíl ukázat, že reálných kvadratických rozšíření může existovat jen konečně mnoho, je proto plná technických odhadů a nerovností. Čtenář nelpící na detailním důkazu může bez obav přeskočit až na sekci 4.4 této kapitoly, která obsahuje veškeré důležité myšlenky. V závěrečné kapitole 5 se pokusíme překlenout mezeru mezi výsledky třetí a čtvrté kapitoly, tedy budeme chtít ukázat, že ve třetí kapitole jsme skutečně popsali všechna reálná normově-euklidovská kvadratická rozšíření tělesa racionálních čísel.

Kapitola 1

Základní pojmy

V této kapitole se zaměříme na základní definice, značení a jednoduchá pozorování, která využijeme v dalších kapitolách. Tato fakta lze najít ve většině učebnic Algebry, např. DRÁPAL (2006).

1.1 Rozšíření těles

Definice 1. *Dvojici těles* $\mathbf{T}$ *a* $\mathbf{S}$ *nazveme* rozšíření tělesa $\mathbf{T}$ tělesem $\mathbf{S}$ *(nebo zkráceně jen* rozšíření těles*), jestliže* $\mathbf{T}$ *je podokruh tělesa* $\mathbf{S}$*; značíme* $\mathbf{S}/\mathbf{T}$. Stupněm rozšíření $\mathbf{S}$ *nad* $\mathbf{T}$ *rozumíme dimenzi* $\mathbf{S}$ *jakožto vektorového prostoru nad tělesem* $\mathbf{T}$*; značíme* $[\mathbf{S} : \mathbf{T}]$*. Řekneme, že rozšíření těles* $\mathbf{S}/\mathbf{T}$ *je* konečné*, jestliže* $[\mathbf{S} : \mathbf{T}] < \infty$.

Lemma 1. *Buď* $\mathbf{U}/\mathbf{S}$ *a* $\mathbf{S}/\mathbf{T}$ *rozšíření těles konečného stupně. Potom* $[\mathbf{U} : \mathbf{T}] = [\mathbf{U} : \mathbf{S}] \cdot [\mathbf{S} : \mathbf{T}]$.

Důkaz. Označme $\{u_i \mid i \in I\}$ bázi vektorového prostoru $\mathbf{U}$ nad $\mathbf{S}$ a $\{s_j \mid j \in J\}$ bázi vektorového prostoru $\mathbf{S}$ nad $\mathbf{T}$. Ukážeme, že $B = \{u_i s_j \mid i \in I, j \in J\}$ je báze vektorového prostoru $\mathbf{U}$ nad $\mathbf{T}$.

Nejprve ověříme, že B generuje $\mathbf{U}$ nad $\mathbf{T}$: Nechť $u \in \mathbf{U}$, pak existují prvky $\widetilde{s}_i \in \mathbf{S}$, $i \in I$, tak, že

$$u = \sum_{i \in I} \widetilde{s}_i u_i.$$

Dále pro každé $i \in I$ existují prvky $t_{ij} \in \mathbf{T}$, $j \in J$, takové, že

$$\widetilde{s}_i = \sum_{j \in J} t_{ij} s_j.$$

Celkem tak máme

$$u = \sum_{i \in I} \left(\sum_{j \in J} t_{ij} s_j \right) u_i = \sum_{i \in I} \sum_{j \in J} t_{ij} \left(s_j u_i \right).$$

Ale $t_{ij} \in \mathbf{T}$ a $s_j u_i \in B$, tedy jsme nalezli vyjádření prvku u jako lineární kombinaci prvků B.

Nyní dokážeme, že B je lineárně nezávislá: Nechť pro nějaká $i \in I$, $j \in J$, $t_{ij} \in \mathbf{T}$ je

$$0 = \sum_{i \in I} \sum_{j \in J} t_{ij} s_j u_i.$$

Jelikož u_i jsou lineárně nezávislé nad $\mathbf{S}$, dostáváme $\sum_{j \in J} t_{ij} s_j = 0$ pro každé $i \in I$. Jelikož ale s_j jsou prvky báze prostoru $\mathbf{S}$ nad $\mathbf{T}$, musí být $t_{ij} = 0$ pro každé $i \in I$ a $j \in J$, což jsme potřebovali.

□

Je-li $\mathbf{S}/\mathbf{T}$ rozšíření těles a $\alpha_1, \ldots, \alpha_n \in \mathbf{S}, n \in \mathbb{N}$, pak označíme $\mathbf{T}[\alpha_1, \ldots, \alpha_n]$ nejmenší podokruh $\mathbf{S}$ obsahující $\mathbf{T} \cup \{\alpha_1, \ldots, \alpha_n\}$ a $\mathbf{T}(\alpha_1, \ldots, \alpha_n)$ nejmenší podtěleso $\mathbf{S}$ obsahující $\mathbf{T} \cup \{\alpha_1, \ldots, \alpha_n\}$.

Definice 2. *Nechť $\mathbf{S}/\mathbf{T}$ je rozšíření těles. Řekneme, že prvek $\alpha \in \mathbf{S}$ je* algebraický nad $\mathbf{T}$*, jestliže existuje nenulový polynom $p \in \mathbf{T}[x]$ takový, že $p(\alpha) = 0$. Rozšíření těles $\mathbf{S}/\mathbf{T}$ nazveme* algebraické*, jestliže pro každé $\alpha \in \mathbf{S}$ je α algebraický prvek nad $\mathbf{T}$. Těleso $\mathbf{S}$ je* algebraicky uzavřené*, jestliže každý polynom $p \in \mathbf{S}[x]$ stupně alespoň jedna má v $\mathbf{S}$ kořen. $\mathbf{S}$ je* algebraický uzávěr $\mathbf{T}$*, je-li rozšíření $\mathbf{S}/\mathbf{T}$ algebraické a $\mathbf{S}$ je algebraicky uzavřené.*

Definice 3. *Nechť $\mathbf{S}/\mathbf{T}$ je rozšíření těles a $\alpha \in \mathbf{S}$ je algebraický prvek nad $\mathbf{T}$. Nenulový polynom $m_\alpha \in \mathbf{T}[x]$ nazveme* minimálním polynomem prvku α nad $\mathbf{T}$*, jestliže*

- *m_α je monický polynom,*
- *$m_\alpha(\alpha) = 0$,*
- *$\forall p \in \mathbf{T}[x] : p(\alpha) = 0 \Rightarrow m_\alpha | p$ v $\mathbf{T}[x]$.*

Lemma 2. *Buď $\mathbf{S}/\mathbf{T}$ rozšíření těles, $\alpha \in \mathbf{S}$ algebraický prvek nad $\mathbf{T}$ a $m_\alpha \in \mathbf{T}[x]$ minimální polynom prvku α nad $\mathbf{T}$. Potom $[\mathbf{T}(\alpha) : \mathbf{T}] = \deg m_\alpha$.*

Důkaz. Definujme homomorfismus $d_\alpha : \mathbf{T}[x] \to \mathbf{T}[\alpha]$ předpisem $d_\alpha(p) = p(\alpha)$. Potom $\mathrm{Ker}(d_\alpha) = (m_\alpha)$ (tj. ideál generovaný polynomem m_α) a $\mathrm{Im}(d_\alpha) = \mathbf{T}[\alpha]$. Podle 1. věty o izomorfismu je tedy $\mathbf{T}[x]/(m_\alpha) \simeq \mathbf{T}[\alpha]$. Je-li $n = \deg m_\alpha$, pak $(1 + (m_\alpha),\ x + (m_\alpha),\ x^2 + (m_\alpha), \ldots,\ x^{n-1} + (m_\alpha))$ je báze vektorového prostoru $\mathbf{T}[x]/(m_\alpha)$ nad tělesem $\mathbf{T}$, tedy $\dim_{\mathbf{T}} (\mathbf{T}[x]/(m_\alpha)) = n$. Zbývá ukázat, že $\mathbf{T}[\alpha] = \mathbf{T}(\alpha)$. Jelikož je polynom m_α ireducibilní, je ideál (m_α) maximální, a tedy $\mathbf{T}[x]/(m_\alpha)$ je těleso. Tedy také $\mathbf{T}[\alpha]$ je těleso a zřejmě $\mathbf{T}[\alpha] \subseteq \mathbf{T}(\alpha)$, odtud $\mathbf{T}[\alpha] = \mathbf{T}(\alpha)$.

□

Poznámka. Z důkazu lemmatu vyplývá, že $(\alpha^0, \alpha^1, \ldots, \alpha^{n-1})$ je báze $\mathbf{T}(\alpha)$ nad $\mathbf{T}$ (kde $n = \deg m_\alpha$).

Lemma 3. *Je-li $\mathbf{T}$ těleso charakteristiky 0, $\mathbf{\Omega}$ jeho algebraický uzávěr a $p \in \mathbf{T}[x]$ ireducibilní polynom, pak polynom p nemá v $\mathbf{\Omega}$ žádné vícenásobné kořeny.*

Důkaz. Pro spor předpokládejme, že p má v $\mathbf{\Omega}$ vícenásobný kořen α. Potom $p'(\alpha) = 0$, $p' \in \mathbf{T}[x]$, kde p' značí formální derivaci polynomu p. Odtud plyne, že $\mathrm{NSD}(p, p') \in \mathbf{T}[x]$ (největší společný dělitel polynomů p a p') je nenulový a má v tělese $\mathbf{\Omega}$ kořen α, tedy $\deg \mathrm{NSD}(p, p') > 0$. Jelikož p je dle předpokladu ireducibilní, je $\mathrm{NSD}(p, p') = p$. Současně ale $\deg p' < \deg p$, tedy $p' = 0$, což je spor. □

Věta 4. *Buď* $\mathbf{T}$ *těleso charakteristiky 0 a* $\mathbf{S}/\mathbf{T}$ *konečné rozšíření těles. Pak existuje* $\gamma \in \mathbf{S}$ *takové, že* $\mathbf{S} = \mathbf{T}(\gamma)$.

Důkaz. Nechť $\mathbf{S} = \mathbf{T}(\gamma_1, \ldots, \gamma_n)$, větu dokážeme indukcí podle n. Pro $n = 1$ platí věta triviálně, k indukčnímu kroku předpokládejme $\mathbf{S} = \mathbf{T}(\alpha, \beta)$.

Označme $\mathbf{\Omega}$ algebraický uzávěr tělesa $\mathbf{S}$ a $m_\alpha, m_\beta \in \mathbf{T}[x]$ minimální polynomy prvků α, β. Z předchozího lemmatu víme, že m_α má v $\mathbf{\Omega}$ právě $\deg m_\alpha$ různých kořenů, označme je α_i, $i = 1, \ldots, \deg m_\alpha$. Obdobně uvažme β_j, $j = 1, \ldots, \deg m_\beta$, kořeny polynomu m_β v $\mathbf{\Omega}$. Protože těleso $\mathbf{T}$ je nekonečné, lze najít $t \in \mathbf{T}$ tak, že jsou prvky $\alpha_i + t\beta_j$ pro $i = 1, \ldots, \deg m_\alpha$, $j = 1, \ldots, \deg m_\beta$ po dvou různé. Položme $\gamma = \alpha + t\beta$ a definujme polynom $p = m_\alpha(\gamma - tx) \in \mathbf{T}(\gamma)[x]$. Potom $p(\beta) = m_\alpha(\alpha) = 0$ a pro všechna $\beta_j \neq \beta$ z definice prvku t plyne $\gamma - t\beta_j \neq \alpha_i$ pro každé $i = 1, \ldots, \deg m_\alpha$, a tedy $p(\beta_j) = m_\alpha(\gamma - t\beta_j) \neq 0$. Polynomy m_β a p mají tedy v $\mathbf{\Omega}$ právě jeden společný kořen, kterým je β.

Buď $d = \mathrm{NSD}(m_\beta, p)$ v $\mathbf{T}(\gamma)[x]$, d monický, pak se d v $\mathbf{\Omega}$ rozkládá na lineární faktory. Z předchozího lemmatu navíc plyne, že jsou tyto faktory po dvou různé. Každý kořen d musí ale současně být kořenem p, tedy jediné možnosti pro polynom d jsou $d = 1$ a $d = x - \beta$. Ale m_β a p mají v $\mathbf{\Omega}$ společný kořen, tedy $d = 1$ vede ke sporu s Bézoutovou rovností v $\mathbf{\Omega}[x]$. Odtud $d = x - \beta \in \mathbf{T}(\gamma)[x]$, a tudíž $\beta \in \mathbf{T}(\gamma)$, z čehož již plyne také $\alpha \in \mathbf{T}(\gamma)$. □

Definice 4. *Buď* $\mathbf{S}/\mathbf{T}$ *rozšíření těles a* $\mathbf{\Omega}$ *algebraický uzávěr* $\mathbf{S}$.[1] *Řekneme, že homomorfismus* $\varphi : \mathbf{S} \to \mathbf{\Omega}$ *je* $\mathbf{T}$-homomorfismus, *jestliže* $\varphi|_{\mathbf{T}} = \mathrm{id}_{\mathbf{T}}$. *Množinu všech* $\mathbf{T}$*-homomorfismů značíme* $\mathrm{Hom}_{\mathbf{T}}(\mathbf{S}, \mathbf{\Omega})$.

Lemma 5. *Je-li* $\mathbf{\Omega}$ *algebraický uzávěr tělesa* $\mathbf{T}$, $p \in \mathbf{T}[x]$, $\alpha \in \mathbf{\Omega}$ *kořen polynomu* p *a* $f \in \mathrm{Hom}_{\mathbf{T}}(\mathbf{S}, \mathbf{\Omega})$, *pak* $f(\alpha)$ *je také kořen polynomu* p.

Důkaz. Označme $p = p_n x^n + p_{n-1} x^{n-1} + \cdots + p_0$. Potom

$$\begin{aligned} 0 = f(0) = f(p(\alpha)) &= f(p_n \alpha^n + p_{n-1} \alpha^{n-1} + \cdots + p_0) = \\ &= f(p_n) f(\alpha^n) + f(p_{n-1}) f(\alpha^{n-1}) + \cdots + f(p_0) = \\ &= p_n f(\alpha^n) + p_{n-1} f(\alpha^{n-1}) + \cdots + p_0 = p(f(\alpha)), \end{aligned}$$

kde čtvrtá rovnost plyne z toho, že f je homomorfismus, a v předposlední rovnosti využijeme, že f je $\mathbf{T}$-homomorfismus a koeficienty polynomu p leží v $\mathbf{T}$. □

[1] $\mathbf{T}$-homomorfismus lze obdobným způsobem definovat obecněji mezi dvěma libovolnými nadtělesy tělesa $\mathbf{T}$.

Lemma 6. *Nechť $\mathbf{\Omega}$ je algebraický uzávěr tělesa $\mathbf{T}$, $\alpha \in \mathbf{\Omega}$ a m_α je minimální polynom prvku α nad $\mathbf{T}$. Označme k počet různých kořenů polynomu m_α. Potom $|\mathrm{Hom}_{\mathbf{T}}(\mathbf{T}(\alpha), \mathbf{\Omega})| = k$.*

Důkaz. Uvažme $f \in \mathrm{Hom}_{\mathbf{T}}(\mathbf{T}(\alpha), \mathbf{\Omega})$, pak z předchozího lemmatu plyne, že homomorfismus f je určen obrazem prvku α a zobrazuje kořeny polynomu m_α opět na kořeny polynomu m_α. Odtud $|\mathrm{Hom}_{\mathbf{T}}(\mathbf{T}(\alpha), \mathbf{\Omega})| \leq k$.

Zbývá ukázat, že pro libovolný kořen β polynomu m_α lze zobrazení $\alpha \mapsto \beta$ rozšířit na $\mathbf{T}$-homomorfismus. Jelikož je β kořenem polynomu m_α, je m_α minimálním polynomem prvku β nad $\mathbf{T}$. Uvažme homomorfismy $d_\alpha : \mathbf{T}[x] \to \mathbf{T}(\alpha)$, definovaný předpisem $d_\alpha(p) = p(\alpha)$, a $d_\beta : \mathbf{T}[x] \to \mathbf{T}(\beta)$, definovaný předpisem $d_\beta(p) = p(\beta)$. Potom $\mathrm{Ker}(d_\alpha) = (m_\alpha) = \mathrm{Ker}(d_\beta)$, tedy z 1. věty o izomorfismu dostáváme $\mathbf{T}(\beta) \cong \mathbf{T}[x]/(m_\alpha) \cong \mathbf{T}(\alpha)$. Odtud plyne $\mathbf{T}(\alpha) \cong \mathbf{T}(\beta)$ a izomorfismus $f : \mathbf{T}(\alpha) \to \mathbf{T}(\beta)$ je hledaný $\mathbf{T}$-homomorfismus.

□

Důsledek. Pro $\mathbb{C}/\mathbf{T}/\mathbb{Q}$ a $\alpha \in \mathbb{C}$ je $|\mathrm{Hom}_{\mathbf{T}}(\mathbf{T}(\alpha), \mathbb{C})| = [\mathbf{T}(\alpha) : \mathbf{T}]$.

Důkaz. Je-li m_α minimální polynom prvku α nad $\mathbf{T}$, pak z Lemmatu 2 plyne $[\mathbf{T}(\alpha) : \mathbf{T}] = \deg m_\alpha$. Podle základní věty algebry má m_α v $\mathbb{C}$ právě $\deg m_\alpha$ kořenů, které jsou podle Lemmatu 3 po dvou různé.

□

Definice 5. *Je-li $\mathbf{S}/\mathbf{T}$ rozšíření těles, $\alpha \in \mathbf{S}$ a $m_\alpha \in \mathbf{T}[x]$ minimální polynom prvku α, potom se kořeny $\alpha = \alpha_1, \ldots, \alpha_n$ polynomu m_α nazývají* konjugované prvky *v $\mathbf{S}$.*

Definice 6. *Nechť $\mathbf{T}$ je těleso charakteristiky 0, $\mathbf{S}/\mathbf{T}$ rozšíření těles, $\mathbf{\Omega}$ algebraický uzávěr $\mathbf{S}$ a buď $\mathrm{Hom}_{\mathbf{T}}(\mathbf{S}, \mathbf{\Omega}) = \{f_1, \ldots, f_n\}$. Pro $x \in \mathbf{S}$ definujeme* normu

$$N_{\mathbf{S}/\mathbf{T}}(x) = \prod_{i=1}^{n} f_i(x).$$

1.2 Rozšíření tělesa $\mathbb{Q}$

Definice 7. *O $\alpha \in \mathbb{C}$ řekneme, že je* algebraické číslo*, jestliže existuje nenulový polynom $p \in \mathbb{Q}[x]$ takový, že $p(\alpha) = 0$, a že je* celé algebraické číslo*, jestliže existuje nenulový monický polynom $q \in \mathbb{Z}[x]$ takový, že $q(\alpha) = 0$.*

Jestliže je $\mathbf{K}$ konečné rozšíření tělesa $\mathbb{Q}$, pak množinu všech celých algebraických čísel z $\mathbf{K}$ budeme značit $\mathbf{R_K}$. Za pomoci následujícího lemmatu ukážeme, že $\mathbf{R_K}$ tvoří okruh (obecnější verzi lemmatu i jeho důsledku lze najít v NARKIEWICZ (2004, 1.6)).

Lemma 7. *Číslo $a \in \mathbf{K}$ je celé algebraické právě tehdy, když existuje nenulová konečně generovaná podgrupa $\mathbf{G}$ aditivní grupy tělesa $\mathbf{K}$ taková, že $a\mathbf{G} \subset \mathbf{G}$.*

Důkaz. Buď nejprve a celé algebraické, tj. existují $p_{n-1}, \ldots, p_0 \in \mathbb{Z}$ taková, že a je kořenem polynomu $x^n + p_{n-1}x^{n-1} + \cdots + p_0 = 0$. Tedy $1, a, \ldots, a^{n-1}$ generují $\mathbb{Z}[a]$. Označíme-li $\mathbf{G} = \mathbb{Z}[a]$, pak $\mathbf{G}$ je hledaná konečně generovaná grupa splňující $a\mathbf{G} \subset \mathbf{G}$.

Uvažme nyní podgrupu $\mathbf{G}$ aditivní grupy tělesa $\mathbf{K}$, $g_1, \ldots, g_r$ její generátory. Jelikož $a\mathbf{G} \subset \mathbf{G}$, existují pro každé $i = 1, \ldots, r$ prvky $b_{ij} \in \mathbb{Z}$ takové, že

$$ag_i = \sum_{j=1}^{r} b_{ij} g_j,$$

což lze přepsat jako

$$\sum_{j=1}^{r} (b_{ij} - a\delta_j^i) g_j = 0,$$

kde

$$\delta_j^i = \begin{cases} 1, \text{ pokud } i = j, \\ 0, \text{ pokud } i \neq j. \end{cases}$$

Odtud dostáváme

$$\det(b_{ij} - a\delta_j^i)_{i,j=1}^r = 0.$$

Potom rozepsáním determinantu

$$\det(b_{ij} - x\delta_j^i)_{i,j=1}^r$$

získáme právě monický polynom s celočíselnými koeficienty, jehož je a kořenem, tedy a je celé algebarické.

□

Důsledek. $\mathbf{R_K}$ je okruh.

Důkaz. Buď $a, b \in \mathbf{R_K}$. Dle předchozího lemmatu nalezneme nenulové podgrupy $\mathbf{G}$, $\mathbf{H}$ aditivní grupy tělesa $\mathbf{K}$ takové, že $a\mathbf{G} \subset \mathbf{G}$ a $b\mathbf{H} \subset \mathbf{H}$. Potom

$$\mathbf{GH} = \left\{ \sum_{j=1}^{k} g_j h_j \mid k \in \mathbb{N}, g_j \in \mathbf{G}, h_j \in \mathbf{H} \right\}$$

je konečně generovaná grupa a máme

$$(a \pm b)\mathbf{GH} = a\mathbf{GH} \pm b\mathbf{GH} \subset \mathbf{GH},$$

neboť $a\mathbf{GH} = (a\mathbf{G})\mathbf{H} \subset \mathbf{GH}$ a $b\mathbf{GH} = \mathbf{G}(b\mathbf{H}) \subset \mathbf{GH}$. Podobně

$$(ab)\mathbf{GH} = (a\mathbf{G})(b\mathbf{H}) \subset \mathbf{GH}.$$

Tedy $a \pm b, ab \in \mathbf{R_K}$ a $\mathbf{R_K}$ je okruh.

□

Na závěr této kapitoly si ukážeme, že všechna konečná rozšíření tělesa $\mathbb{Q}$ lze sestrojit přidáním jediného prvku, který navíc je možné vybrat z okruhu celých algebraických čísel.

Věta 8. *Je-li* $\mathbf{K}$ *konečné rozšíření tělesa* $\mathbb{Q}$*, pak existuje* $\gamma \in \mathbf{R_K}$ *takové, že* $\mathbf{K} = \mathbb{Q}(\gamma)$.

Důkaz. Existence prvku $\gamma \in \mathbb{C}$ takového, že $\mathbf{K} = \mathbb{Q}(\gamma)$, plyne z Věty 4. Stačí tedy ukázat, že lze volit $\gamma \in \mathbf{R_K}$.

Buď $m_\gamma = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ minimální polynom prvku γ nad $\mathbb{Q}$, tedy $a_{n-1}, \ldots, a_0 \in \mathbb{Q}$. Potom nalezneme $r \in \mathbb{Z}$ takové, že $ra_{n-1}, \ldots, ra_0 \in \mathbb{Z}$. Definujme polynom $p = r^n m_\gamma(\frac{x}{r})$, tedy $p = x^n + ra_{n-1}x^{n-1} + \cdots + r^n a_0$. Zřejmě $p \in \mathbb{Z}[x]$ a $p(r\gamma) = r^n m_\gamma(\gamma) = 0$, odkud plyne $r\gamma \in \mathbf{R_K}$. Zbývá si již jen uvědomit, že $\mathbb{Q}(\gamma) = \mathbb{Q}(r\gamma)$.

□

Kapitola 2

Imaginární kvadratická rozšíření

Cílem kapitoly je nalézt celá záporná čísla D, pro která na okruhu všech celých algebraických čísel tělesa $\mathbb{Q}(\sqrt{D})$ existuje Euklidův algoritmus, a ukázat, že žádná jiná neexistují. Nejdříve je však nutné seznámit se s několika důležitými pojmy.

2.1 Kvadratická rozšíření tělesa $\mathbb{Q}$

Kvadratickým rozšířením tělesa $\mathbb{Q}$ nazýváme takové těleso $\mathbf{K}$, kde $\mathbf{K}/\mathbb{Q}$ je rozšíření těles, že platí $[\mathbf{K} : \mathbb{Q}] = 2$. Je zřejmé, že $\mathbf{K}$ je kvadratickým rozšířením tělesa $\mathbb{Q}$ právě tehdy, když je $\mathbf{K} = \mathbb{Q}(\sqrt{D})$ pro nějaké bezčtvercové číslo[1] $D \neq 0, 1$. Jestliže je $D > 0$, mluvíme o reálných kvadratických rozšířeních, naopak pro $D < 0$ nazýváme těleso $\mathbb{Q}(\sqrt{D})$ imaginárním kvadratickým rozšířením.

Lemma 9. *Buď $\mathbf{K}$ konečné rozšíření tělesa $\mathbb{Q}$. Potom $\alpha \in \mathbf{K}$ je celé algebraické právě tehdy, když má jeho minimální polynom nad $\mathbb{Q}$ celočíselné koeficienty.*

Důkaz. Implikace $\Leftarrow$ plyne přímo z definice, ukážeme $\Rightarrow$. Začneme pomocným tvrzením: Pro polynom $f \in \mathbb{Z}[x]$ označme $f_0, \ldots, f_n$ jeho koeficienty a $\mathrm{ct}(f)$ největší společný dělitel $f_0, \ldots, f_n$. Potom pro polynomy $f, g \in \mathbb{Z}[x]$ takové, že $\mathrm{ct}(f) = \mathrm{ct}(g) = 1$ platí $\mathrm{ct}(fg) = 1$. Kdyby totiž ne, existovalo by $u \in \mathbb{N}$, $u > 1$, takové, že $u \mid \mathrm{ct}(fg)$. Přitom ale existují i, j, pro která $u \nmid f_i$ a $u \nmid g_j$, zvolme i a j nejmenší taková. Koeficient polynomu fg u členu x^{i+j} je

$$f_0 g_{i+j} + f_1 g_{i+j-1} + \cdots + f_i g_j + \cdots + f_{i+j} g_0.$$

Jelikož (díky minimalitě i a j)

$$u \mid f_0, \ldots, f_{i-1}, g_{j-1}, \ldots, g_0,$$

je také

$$u \mid f_0 g_{i+j}, f_1 g_{i+j-1}, \ldots, f_{i-1} g_{j+1}, f_{i+1} g_{j-1}, \ldots, f_{i+j} g_0.$$

Současně ale $u \nmid f_i g_j$, a tedy u nedělí koeficient polynomu fg u členu x^{i+j}, což je spor.

[1] Bezčtvercovým číslem nazýváme číslo, které není dělitelné druhou mocninou žádného prvočísla.

Buď tedy $p \in \mathbb{Z}[x]$ nenulový monický polynom takový, že $p(\alpha) = 0$, a m_α minimální polynom prvku α nad $\mathbb{Q}$. Potom $m_\alpha | p$ nad $\mathbb{Q}$, tedy existuje polynom $h \in \mathbb{Q}[x]$ takový, že $p = m_\alpha h$. Buďte $A, B \in \mathbb{N}$ nejmenší taková, že $Am_\alpha, Bh \in \mathbb{Z}[x]$. Potom $\operatorname{ct}(Am_\alpha) = \operatorname{ct}(Bh) = 1$ (jinak by A, B nebyla nejmenší), a tedy dle pomocného tvrzení také $\operatorname{ct}(Am_\alpha Bh) = 1$. Jelikož ale polynom $m_\alpha h$ má celočíselné koeficienty, je každý koeficient polynomu $Am_\alpha Bh$ dělitelný číslem AB, tedy $AB | \operatorname{ct}(Am_\alpha Bh) = 1$, neboli $AB = 1$. Odtud již $|A| = |B| = 1$ a $m_\alpha \in \mathbb{Z}[x]$, což jsme přesně chtěli dokázat.

□

Podívejme se nyní, jak vypadá těleso $\mathbb{Q}(\sqrt{D})$ pro bezčtvercové celé číslo D. Všechny prvky tohoto tělesa jsou tvaru $a + b\sqrt{D}$, $a, b \in \mathbb{Q}$, a pro $b \neq 0$ je zřejmě

$$m_{a+b\sqrt{D}} = (x - (a + b\sqrt{D}))(x - (a - b\sqrt{D})) = x^2 - 2ax + a^2 - b^2 D$$

minimální polynom prvku $a+b\sqrt{D}$. S pomocí předchozího lemmatu tedy můžeme popsat prvky okruhu $\mathbf{R_K}$:

Věta 10. *Nechť D je bezčtvercové celé číslo a označme $\mathbf{K} = \mathbb{Q}(\sqrt{D})$. Potom*

$$\mathbf{R_K} = \begin{cases} \left\{ \frac{a+b\sqrt{D}}{2} \mid a, b \in \mathbb{Z}, a \equiv b \pmod 2 \right\}, & \text{pokud } D \equiv 1 \pmod 4, \\ \left\{ a + b\sqrt{D} \mid a, b \in \mathbb{Z} \right\}, & \text{pokud } D \not\equiv 1 \pmod 4. \end{cases}$$

Důkaz. Inkluze $\mathbb{Z} \subseteq \mathbf{R_K}$ je zřejmá. Stačí se tedy zaměřit na prvky $a + b\sqrt{D}$ pro $b \neq 0$. Z předchozího lemmatu a tvaru minimálního polynomu víme, že

$$a + b\sqrt{D} \in \mathbf{R_K} \Leftrightarrow 2a \in \mathbb{Z} \ \&\ a^2 - b^2 D \in \mathbb{Z}.$$

Označme $a = \frac{p}{q}$, $b = \frac{r}{s}$, $p, r \in \mathbb{Z}$, $q, s \in \mathbb{N}$, dvojice p, q a r, s nesoudělné. Potom první podmínka $2a = \frac{2p}{q} \in \mathbb{Z}$ nastane právě tehdy, když $q = 1$ nebo $q = 2$.

Buď nejprve $q = 1$. Druhá podmínka

$$a^2 - b^2 D = p^2 - \frac{r^2 D}{s^2} \in \mathbb{Z}$$

je ekvivalentní podmínce $s^2 | r^2 D$. Jelikož jsou r, s nesoudělná a D bezčtvercové (tj. $s^2 \nmid D$), dostáváme $s = 1$. Jinými slovy $a, b \in \mathbb{Z}$ a pak již zřejmě $a + b\sqrt{D} \in \mathbf{R_K}$.

Nechť nyní $q = 2$. Možnost $a = 0$ můžeme zahrnout do předchozí možnosti, nechť tedy nyní $a \neq 0$. Z druhé podmínky pak dostáváme

$$a^2 - b^2 D = \frac{p^2}{4} - \frac{r^2 D}{s^2} = \frac{p^2 s^2 - 4r^2 D}{4s^2} \in \mathbb{Z}.$$

Odtud $4 | p^2 s^2$ a jelikož jsou p, q nesoudělná, tedy $2 \nmid p$, dostáváme $4 | s^2$, neboli $2 | s$. Podobně $s^2 | 4r^2 D$ dává (spolu s podmínkami r, s nesoudělná a D bezčtvercové) $s^2 | 4$, tedy $s | 2$. Celkem tak $s = 2$. Nyní $\frac{p^2 - r^2 D}{4} \in \mathbb{Z}$, tedy $p^2 \equiv r^2 D \pmod 4$. Jelikož $2 \nmid p, r$, je $p^2, r^2 \equiv 1 \pmod 4$. Odtud již vyplývá $D \equiv 1 \pmod 4$. Naopak pro lichá $p, r \in \mathbb{Z}$ a $D \equiv 1 \pmod 4$ je $\frac{p + r\sqrt{D}}{2} \in \mathbf{R_K}$, neboť je to kořen polynomu $x^2 - px + \frac{p^2 - r^2 D}{4} = 0$ a $p^2 - r^2 D \equiv 0 \pmod 4$.

□

Nakonec se ještě podíváme, jak vypadá v našem konkrétním případě norma $N_{\mathbf{S}/\mathbf{T}}(x)$:

Lemma 11. *Nechť D je bezčtvercové celé číslo a označme $\mathbf{K} = \mathbb{Q}(\sqrt{D})$. Potom pro $a, b \in \mathbb{Q}$ je $N_{\mathbf{K}/\mathbb{Q}}(a + b\sqrt{D}) = a^2 - b^2 D$.*

Důkaz. Uvažme $f_1, \ldots, f_n$ všechny $\mathbb{Q}$-homomorfismy z $\mathbf{K}$ do $\mathbb{C}$ a $m = x^2 - D$ buď minimální polynom prvku $\sqrt{D}$ nad $\mathbb{Q}$. Potom z Lemmatu 5 je $f_i(\sqrt{D})$ pro $i = 1, \ldots, n$ kořenem polynomu m. Odtud plyne $f_i(\sqrt{D}) = \pm\sqrt{D}$ a $n = 2$. Nyní již snadno spočítáme

$$N_{\mathbf{K}/\mathbb{Q}}(a + b\sqrt{D}) = f_1(a + b\sqrt{D}) \cdot f_2(a + b\sqrt{D}) =$$

$$= (f_1(a)+f_1(b)\cdot f_1(\sqrt{D}))(f_2(a)+f_2(b)\cdot f_2(\sqrt{D})) = (a+b\sqrt{D})(a-b\sqrt{D}) = a^2-b^2D.$$

□

Poznámka. Z důkazu Lemmatu také vidíme, že prvky $a + b\sqrt{D}$ a $a - b\sqrt{D}$ jsou konjugované v $\mathbb{Q}(\sqrt{D})$, a dále, že je-li $\alpha \in \mathbb{Q}(\sqrt{D})$ a α' prvek konjugovaný k α, pak platí $N_{\mathbf{K}/\mathbb{Q}}(\alpha) = \alpha\alpha'$.

2.2 Normově-euklidovská rozšíření

V této podkapitole budeme tělesem $\mathbf{K}$ rozumět konečné rozšíření tělesa $\mathbb{Q}$.

Definice 8. *Obor $\mathbf{R}$ nazveme* Euklidův obor*, pokud existuje funkce $\nu : \mathbf{R} \to \mathbb{N} \cup \{0\}$ splňující:*

(i) $\nu(x) = 0$ *právě tehdy, když* $x = 0$,

(ii) $\nu(a) \leq \nu(ab)$ *pro všechna* $a, b \in \mathbf{R}$, $a, b \neq 0$,

(iii) pokud $a, b \in \mathbf{R}$, $b \neq 0$, *potom existují* $q, r \in \mathbf{R}$ *tak, že* $a = bq + r$ *a* $\nu(r) < \nu(b)$.

Těleso $\mathbf{K}$ nazveme normově-euklidovské*, pokud je $\mathbf{R}_\mathbf{K}$ Euklidův s $\nu(x) = \left|N_{\mathbf{K}/\mathbb{Q}}(x)\right|$.*

Lemma 12. *Každý prvek tělesa $\mathbf{K}$ lze zapsat jako podíl dvou prvků z okruhu $\mathbf{R}_\mathbf{K}$.*

Důkaz. Z Věty 8 víme, že existuje $\alpha \in \mathbf{R}_\mathbf{K}$ takové, že $\mathbf{K} = \mathbb{Q}(\alpha)$. Prvky tělesa $\mathbf{K}$ jsou tedy tvaru $\frac{p}{q} + \frac{r}{s}\alpha$, kde $p, q, r, s \in \mathbb{Z}$. Platí ale

$$\frac{p}{q} + \frac{r}{s}\alpha = \frac{ps + qr\alpha}{qs}$$

a $ps + qr\alpha, qs \in \mathbf{R}_\mathbf{K}$, což jsme chtěli.

□

Následující lemma je převzato z publikace NARKIEWICZ (2004, 3.30) a poskytne nám důležitou charakterizaci normově-euklidovských těles.

Lemma 13. *Těleso* $\mathbf{K}$ *je normově-euklidovské právě tehdy, když pro každé* $a \in \mathbf{K}$ *existuje* $t \in \mathbf{R_K}$ *takové, že* $\left|N_{\mathbf{K}/\mathbb{Q}}(a-t)\right| < 1$.

Důkaz. $\mathbf{R_K}$ je Euklidův, právě když pro všechna $a, b \in \mathbf{R_K}$ existují $q, r \in \mathbf{R_K}$ taková, že $a = bq + r$ a $\left|N_{\mathbf{K}/\mathbb{Q}}(r)\right| < \left|N_{\mathbf{K}/\mathbb{Q}}(b)\right|$, neboli $\left|N_{\mathbf{K}/\mathbb{Q}}(a-bq)\right| < \left|N_{\mathbf{K}/\mathbb{Q}}(b)\right|$. To je ekvivalentní podmínce $\left|N_{\mathbf{K}/\mathbb{Q}}(ab^{-1}-q)\right| < 1$, jelikož norma je zřejmě multiplikativní. Stačí již tedy jen aplikovat předchozí lemma.

□

2.3 Imaginární normově-euklidovská rozšíření $\mathbb{Q}$

V tuto chvíli jjiž máme připraveny všechny prostředky k důkazu věty charakterizující všechna imaginární normově-euklidovská rozšíření tělesa racionálních čísel, kterou lze najít také v publikaci NARKIEWICZ (2004, Důsledek 3.30).

Věta 14. *Pro* $D < 0$ *je těleso* $\mathbf{K} = \mathbb{Q}(\sqrt{D})$ *normově-euklidovské právě tehdy, když* $D \in \{-1, -2, -3, -7, -11\}$.

Důkaz. Důkaz rozdělíme na jednotlivé případy podle hodnoty D.

1. případ: $D \not\equiv 1 (\mathrm{mod}\ 4)$.

Nechť nejdříve $D \in \{-1, -2\}$. Každý prvek okruhu $\mathbf{R_K}$ je podle Věty 10 tvaru $a + b\sqrt{D}$, $a, b \in \mathbb{Z}$. Vezměme $x + y\sqrt{D}$ libovolný prvek z $\mathbf{K}$ (tedy $x, y \in \mathbb{Q}$). Pak existují $a, b \in \mathbb{Z}$ taková, že $|x-a| \leq \frac{1}{2}$ a $|y-b| \leq \frac{1}{2}$, a tedy podle Lemmatu 11 je

$$\left|N_{\mathbf{K}/\mathbb{Q}}\left(\left(x+y\sqrt{D}\right)-\left(a+b\sqrt{D}\right)\right)\right| = \left|(x-a)^2-(y-b)^2 D\right| =$$

$$= (x-a)^2 + (y-b)^2 |D| \leq \frac{1+|D|}{4} < 1.$$

Podle Lemmatu 13 je tedy $\mathbf{K}$ normově-euklidovské těleso.

Naopak, buď $\mathbf{K}$ normově-euklidovské těleso a buď $x = \frac{\sqrt{D}}{2}$. Podle Lemmatu 13 nalezneme $a + b\sqrt{D} \in \mathbf{R_K}$ (tedy $a, b \in \mathbb{Z}$) tak, že

$$\left|N_{\mathbf{K}/\mathbb{Q}}\left(x-\left(a+b\sqrt{D}\right)\right)\right| < 1.$$

Víme

$$\left|N_{\mathbf{K}/\mathbb{Q}}\left(x-\left(a+b\sqrt{D}\right)\right)\right| = \left|N_{\mathbf{K}/\mathbb{Q}}\left(a+\left(\frac{1}{2}-b\right)\sqrt{D}\right)\right| = a^2+\left(\frac{1}{2}-b\right)^2|D|,$$

tedy

$$a^2+\left(\frac{1}{2}-b\right)^2|D| < 1.$$

Jelikož ale pro každé $b \in \mathbb{Z}$ je $\left(\frac{1}{2}-b\right)^2 \geq \frac{1}{4}$, máme $\frac{|D|}{4} < 1-a^2 \leq 1$, tedy $|D| < 4$, odkud již $D \in \{-1, -2\}$.

2. případ: $D \equiv 1 (\mathrm{mod}\ 4)$.

Nechť nyní $D \in \{-3, -7, -11\}$. Z Věty 10 víme, že každý prvek $\mathbf{R_K}$ je tvaru $\frac{a+b\sqrt{D}}{2}$, $a, b \in \mathbb{Z}$, $a \equiv b \pmod 2$. Uvažme opět $x+y\sqrt{D}$, $x, y \in \mathbb{Q}$ libovolný prvek z $\mathbf{K}$. Pak najdeme nejprve $b \in \mathbb{Z}$ takové, že $\left|y - \frac{b}{2}\right| \leq \frac{1}{4}$ a poté $a \in \mathbb{Z}$ takové, že $\left|x - \frac{a}{2}\right| \leq \frac{1}{2}$ a $a \equiv b \pmod 2$. Potom je

$$\left| N_{\mathbf{K}/\mathbb{Q}} \left(\left(x + y\sqrt{D} \right) - \left(\frac{a}{2} + \frac{b}{2}\sqrt{D} \right) \right) \right| = \left| \left(x - \frac{a}{2} \right)^2 - \left(y - \frac{b}{2} \right)^2 D \right| =$$

$$= \left(x - \frac{a}{2} \right)^2 + \left(y - \frac{b}{2} \right)^2 |D| \leq \frac{1}{4} + \frac{|D|}{16} = \frac{4 + |D|}{16} \leq \frac{15}{16} < 1.$$

Podle Lemmatu 13 je $\mathbf{K}$ normově-euklidovské těleso.

Nyní naopak buď $\mathbf{K}$ normově-euklidovské těleso a nechť $x = \frac{1+\sqrt{D}}{4}$. Opět podle Lemmatu 13 nalezneme $\frac{a+b\sqrt{D}}{2} \in \mathbf{R_K}$ (tedy $a, b \in \mathbb{Z}$, $a \equiv b \pmod 2$) tak, že

$$\left| N_{\mathbf{K}/\mathbb{Q}} \left(x - \frac{a + b\sqrt{D}}{2} \right) \right| < 1,$$

a tedy

$$\left| N_{\mathbf{K}/\mathbb{Q}} \left(x - \frac{a + b\sqrt{D}}{2} \right) \right| = \left| N_{\mathbf{K}/\mathbb{Q}} \left(\frac{1 + \sqrt{D}}{4} - \frac{a + b\sqrt{D}}{2} \right) \right| =$$

$$= \left(\frac{1}{4} - \frac{a}{2} \right)^2 + \left(\frac{1}{4} - \frac{b}{2} \right)^2 |D| < 1.$$

Jelikož pro každé $t \in \mathbb{Z}$ platí $\left|\frac{1}{4} - \frac{t}{2}\right| \geq \frac{1}{4}$, dostáváme $1 + |D| < 16$, odkud již $D \in \{-3, -7, -11\}$.

□

Kapitola 3

Reálná kvadratická rozšíření I

V této kapitole se na problém kvadratických rozšíření podíváme z geometrického hlediska (viz článek EGGLETON a kol. (1992)) a popíšeme všechna kladná bezčtvercová čísla D, pro která je rozšíření $\mathbb{Q}(\sqrt{D})$ normově-euklidovské. Důkaz, že jiná skutečně neexistují, ale ponecháme až do následujících kapitol. Krátce se také vrátíme k imaginárním kvadratickým rozšířením a ukážeme souvislost důkazu z druhé kapitoly s nynějším geometrickým náhledem.

3.1 Geometrická reprezentace

Všechny prvky tělesa $\mathbb{Q}(\sqrt{D})$ jsou tvaru $\frac{a_1}{a_2} + \frac{b_1}{b_2}\sqrt{D}$, kde $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Můžeme tedy definovat vnoření

$$\begin{array}{rcl} \psi : \mathbb{Q}(\sqrt{D}) & \to & \mathbb{Q}^2 \\ \frac{a_1}{a_2} + \frac{b_1}{b_2}\sqrt{D} & \mapsto & \left(\frac{a_1}{a_2}, \frac{b_1}{b_2}\right). \end{array}$$

Jinými slovy znázorníme těleso $\mathbb{Q}(\sqrt{D})$ jako body v rovině s racionálními souřadnicemi. Připomeňme, že značíme $\mathbf{K} = \mathbb{Q}(\sqrt{D})$ a že $\mathbf{R_K}$ je okruh všech celých algebraických čísel z $\mathbf{K}$. Ve Větě 10 jsme popsali prvky okruhu $\mathbf{R_K}$ v závislosti na hodnotě D. Označme nyní $M_D = \psi(\mathbf{R_K})$, potom

- $M_D = \mathbb{Z}^2$, pokud $D \not\equiv 1 \pmod 4$,
- $M_D = \left\{(a,b) \mid (a,b) \in \mathbb{Z}^2 \text{ nebo } (a,b) \in \mathbb{Z}^2 + \left(\frac{1}{2}, \frac{1}{2}\right)\right\}$, pokud $D \equiv 1 \pmod 4$.

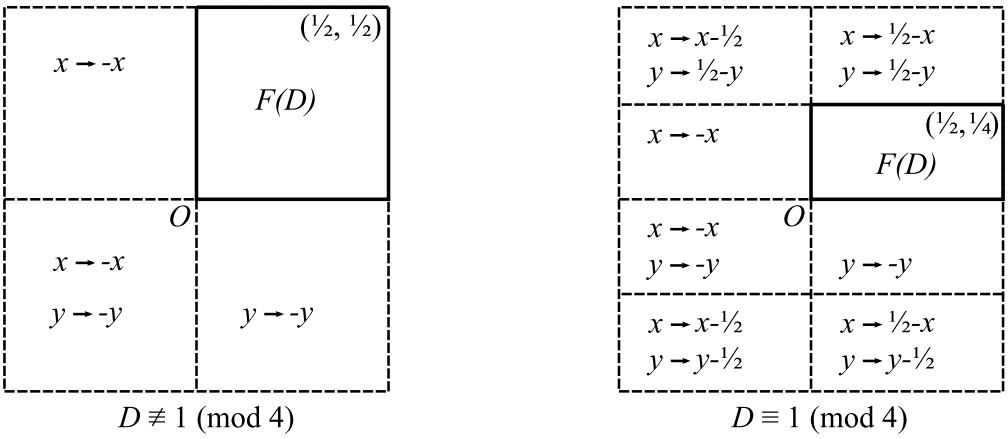
Definice 9. Jednotkovým okolím *prvku* $\alpha \in \mathbf{R_K}$ *rozumíme množinu*

$$U(\alpha) = \left\{\lambda \in \mathbb{Q}(\sqrt{D}) \mid \left|N_{\mathbf{K}/\mathbb{Q}}(\lambda - \alpha)\right| < 1\right\}.$$

Jestliže $\alpha = a + b\sqrt{D}$ a $\lambda = x + y\sqrt{D}$, pak podle Lemmatu 11 máme pro normu $N_{\mathbf{K}/\mathbb{Q}}(\lambda - \alpha) = (x-a)^2 - (y-b)^2 D$. To nás přivádí k následující definici:

Definice 10. Jednotkové okolí *bodu* $(a,b) \in M_D$ *definujeme jako množinu*

$$U(a,b) = \left\{(x,y) \in \mathbb{Q}^2 \mid \left|(x-a)^2 - (y-b)^2 D\right| < 1\right\}.$$



Obrázek 3.1: Základní oblast $F(D)$ pro $\mathbb{Q}(\sqrt{D})$.

Následující lemma je zřejmým důsledkem Lemmatu 13:

Lemma 15. *Těleso $\mathbb{Q}(\sqrt{D})$ je normově-euklidovské právě tehdy, když pro každý bod $(x, y) \in \mathbb{Q}^2$ existuje bod $(a, b) \in M_D$ takový, že $(x, y) \in U(a, b)$.*

Definice 11. *Definujme* základní oblast $F(D)$ *pro* $\mathbb{Q}(\sqrt{D})$ *jako*

$$F(D) = \begin{cases} \left\{(x,y) \in \mathbb{Q}^2 \mid 0 \le x \le \frac{1}{2},\ 0 \le y \le \frac{1}{2}\right\}, \text{ pokud } D \not\equiv 1 \pmod 4, \\ \left\{(x,y) \in \mathbb{Q}^2 \mid 0 \le x \le \frac{1}{2},\ 0 \le y \le \frac{1}{4}\right\}, \text{ pokud } D \equiv 1 \pmod 4. \end{cases}$$

Lemma 16. *Těleso $\mathbb{Q}(\sqrt{D})$ je normově-euklidovské právě tehdy, když*

$$F(D) \subseteq \bigcup_{(a,b)\in M_D} U(a,b).$$

Důkaz. Je zřejmé, že bez újmy na obecnosti se můžeme zaměřit na množinu bodů $\mathbb{Q}^2 \cap \left[-\frac{1}{2},\frac{1}{2}\right]^2 \subset F(D)$. Na Obrázku 3.1 je dále znázorněna symetrie $\mathbb{Q}^2$ a M_D. Tvrzení pak již plyne z předchozího lemmatu.

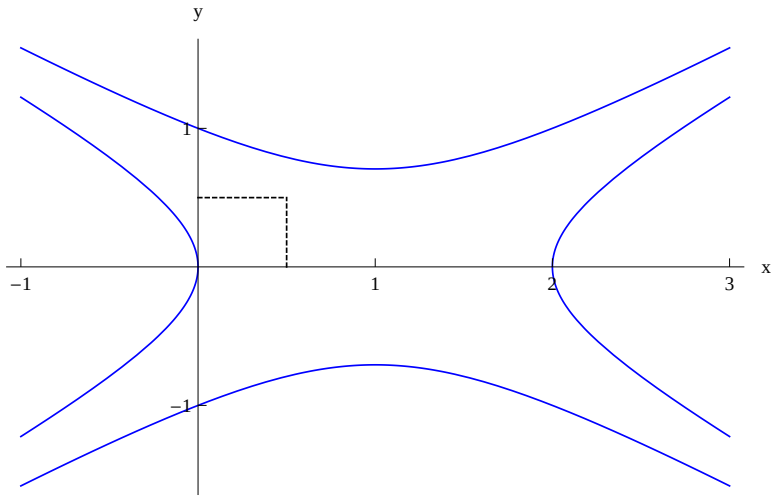
□

3.2 Reálná normově-euklidovská rozšíření $\mathbb{Q}$

Celou podkapitolu věnujeme důkazu tvrzení, ve kterém popíšeme reálná kvadratická rozšíření tělesa racionálních čísel. Důkaz je převzat z článku autorů EGGLETON a kol. (1992, 6.1).

Věta 17. *Jestliže $D \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$, pak je těleso $\mathbb{Q}(\sqrt{D})$ normově-euklidovské.*

Důkaz. Jelikož $(0, 0) \in U(0, 0)$ pro libovolné D, stačí nám pomocí jednotkových okolí bodů z M_D pokrýt množinu bodů $F(D) \setminus \{(0, 0)\}$. Protože uvažujeme pouze $D > 0$, tvoří hranici jednotkového okolí $U(a, b)$ dvě konjugované hyperboly dané předpisy $(x-a)^2-(y-b)^2D = 1$ (levá a pravá hranice) a $(x-a)^2-(y-b)^2D = -1$ (horní a dolní hranice).



Obrázek 3.2: Hranice $U(1,0)$ pro $D = 2$.

1. případ: $D \in \{2, 3, 5, 13, 17\}$.

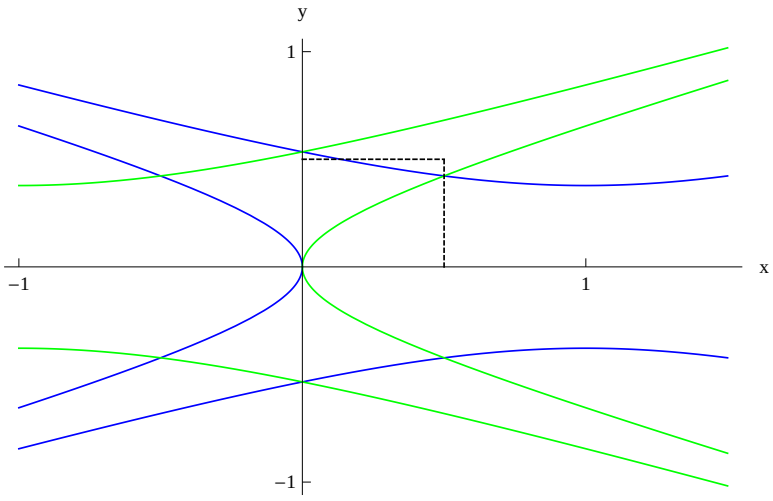
Podívejme se na jednotkové okolí bodu $(1,0)$, které je zobrazeno na Obrázku 3.2. Horní hranice prochází body $\left(0, \frac{\sqrt{2}}{\sqrt{D}}\right)$ a $\left(\frac{1}{2}, \frac{\sqrt{5}}{2\sqrt{D}}\right)$. Jelikož $\frac{\sqrt{2}}{\sqrt{D}} > \frac{\sqrt{5}}{2\sqrt{D}}$ pro libovolné $D > 0$, dostáváme pro $D \not\equiv 1 \pmod 4$ podmínku $\frac{\sqrt{5}}{2\sqrt{D}} > \frac{1}{2}$, neboli $D < 5$, a pro $D \equiv 1 \pmod 4$ podmínku $\frac{\sqrt{5}}{2\sqrt{D}} > \frac{1}{4}$, neboli $D < 20$. V obou případech jsou podmínky splněny, tedy $F(D) \setminus \{(0,0)\} \subseteq U(1,0)$.

2. případ: $D \in \{6, 7, 21, 29\}$.

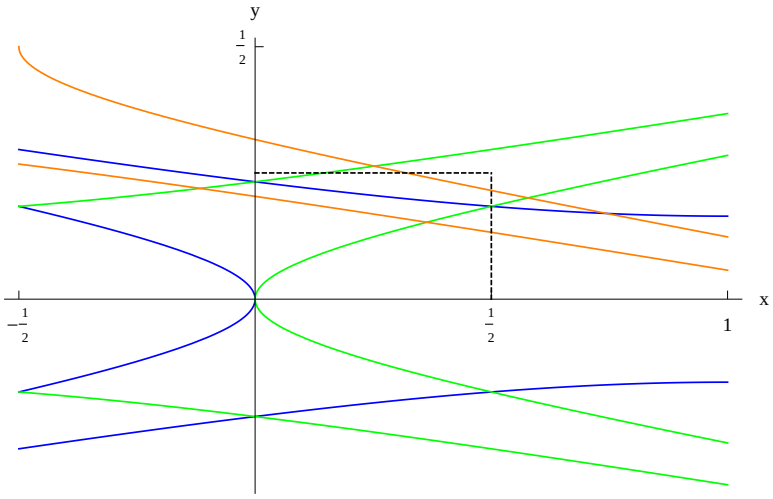
K pokrytí nyní využijeme jednotková okolí bodů $(-1,0)$ a $(1,0)$ jako na Obrázku 3.3. Pravá hranice $U(-1,0)$ a horní hranice $U(1,0)$ se protínají v bodě $\left(\frac{1}{2}, \frac{\sqrt{5}}{2\sqrt{D}}\right)$ (jelikož uvažujeme $D > 5$ bezčtvercové, není číslo $\frac{\sqrt{5}}{2\sqrt{D}}$ racionální, a tedy $\left(\frac{1}{2}, \frac{\sqrt{5}}{2\sqrt{D}}\right) \notin F(D)$). Dále horní hranice $U(-1,0)$ a horní hranice $U(1,0)$ se protínají v bodě $\left(0, \frac{\sqrt{2}}{\sqrt{D}}\right)$, což nám pro $D \not\equiv 1 \pmod 4$ dává podmínku $\frac{\sqrt{2}}{\sqrt{D}} > \frac{1}{2}$, neboli $D < 8$, a pro $D \equiv 1 \pmod 4$ podmínku $\frac{\sqrt{2}}{\sqrt{D}} > \frac{1}{4}$, neboli $D < 32$. Nyní si již jen stačí uvědomit, že horní hranice $U(-1,0)$ je na intervalu $(-1, \infty)$ tvořena rostoucí funkcí.

3. případ: $D \in \{33, 37, 41\}$.

Tentokrát uvažujeme pouze $D \equiv 1 \pmod 4$. Opět využijeme jednotkových okolí $U(-1,0)$ a $U(1,0)$. Horní hranice okolí $U(-1,0)$ prochází body $\left(0, \frac{\sqrt{2}}{\sqrt{D}}\right)$ a $\left(\frac{\sqrt{D-16}}{4} - 1, \frac{1}{4}\right)$ a zřejmě $\frac{\sqrt{2}}{\sqrt{D}} < \frac{1}{4}$ a $\frac{\sqrt{D-16}}{4} - 1 > 0$. Zbytek základní oblasti pokryjeme jednotkovým okolím bodu $\left(-\frac{3}{2}, \frac{1}{2}\right)$, situace je znázorněna na Obrázku 3.4. Dolní hranice tohoto jednotkového okolí prochází bodem $\left(0, \frac{\sqrt{D}-\sqrt{13}}{2\sqrt{D}}\right)$ a $\frac{\sqrt{D}-\sqrt{13}}{2\sqrt{D}} < \frac{\sqrt{2}}{\sqrt{D}}$ je ekvivalentní s $D < \left(2\sqrt{2} + \sqrt{13}\right)^2 \doteq 41{,}396$, což zřejmě platí. Dále pravá hranice $U\left(-\frac{3}{2}, \frac{1}{2}\right)$ prochází body $\left(0, \frac{\sqrt{D}-\sqrt{5}}{2\sqrt{D}}\right)$ a $\left(\frac{\sqrt{D+16}}{4} - \frac{3}{2}, \frac{1}{4}\right)$, kde $\frac{\sqrt{D}-\sqrt{5}}{2\sqrt{D}} > \frac{1}{4}$ je ekvivalentní s $D > 20$ a $\frac{\sqrt{D+16}}{4} - \frac{3}{2} > \frac{\sqrt{D-16}}{4} - 1$ je ekvivalentní s $D < 65$. Obě podmínky jsou splněny z předpokladu pro D.



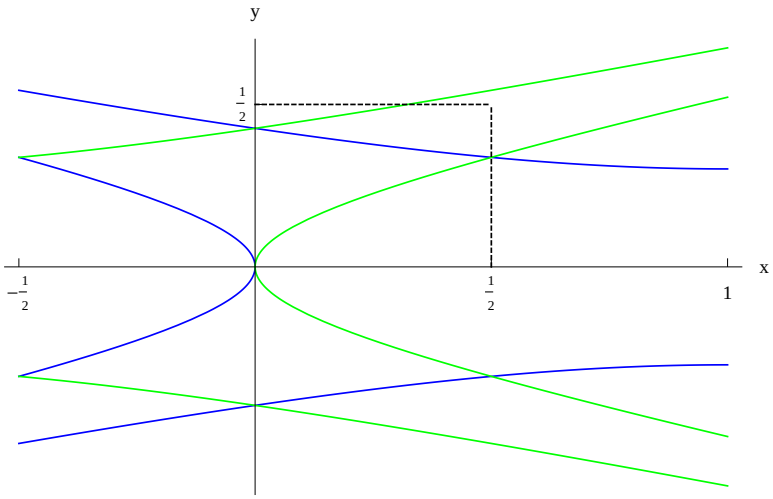
Obrázek 3.3: Hranice $U(-1,0)$ a $U(1,0)$ pro $D = 7$.



Obrázek 3.4: Hranice $U(-1,0)$, $U(1,0)$ a $U\left(-\frac{3}{2},\frac{1}{2}\right)$ pro $D = 37$.

4. případ: $D = 11$.

Nejprve si uvědomíme, že většinu $F(11)$ máme pokrytou jednotkovými okolími bodů $(-1,0)$ a $(1,0)$ (viz Obrázek 3.5), přičemž horní hranice $U(-1,0)$ prochází bodem $\left(0,\frac{\sqrt{2}}{\sqrt{11}}\right)$, kde $\frac{\sqrt{2}}{\sqrt{11}} \doteq 0{,}426$. Ukážeme, že zbytek $F(11)$ pokryjeme pomocí $U(2,1)$ a $U(-5,-1)$. Dolní hranice $U(2,1)$ prochází body $\left(0,1-\frac{\sqrt{5}}{\sqrt{11}}\right)$, kde $1-\frac{\sqrt{5}}{\sqrt{11}} \doteq 0{,}326 < 0{,}426$, a $\left(2-\frac{\sqrt{7}}{2},\frac{1}{2}\right)$, kde $2-\frac{\sqrt{7}}{2} \doteq 0{,}677 > \frac{1}{2}$. Jinými slovy, dolní hranice $U(2,1)$ leží na intervalu $\left[0,\frac{1}{2}\right]$ „pod“ horní hranicí $U(-1,0)$. Dále levá hranice $U(2,1)$ prochází body $\left(0,1-\frac{\sqrt{3}}{\sqrt{11}}\right)$, kde $1-\frac{\sqrt{3}}{\sqrt{11}} \doteq 0{,}478$, a $\left(2-\frac{\sqrt{15}}{2},\frac{1}{2}\right)$, kde $2-\frac{\sqrt{15}}{2} \doteq 0{,}064 > 0$. Zbývá tedy pokrýt část $F(11)$ na intervalu $\left[0,2-\frac{\sqrt{15}}{2}\right]$ ležící „nad“ levou hranicí $U(2,1)$. Horní hranice $U(-5,-1)$ prochází bodem $\left(0,\frac{\sqrt{26}}{\sqrt{11}}-1\right)$, kde $\frac{\sqrt{26}}{\sqrt{11}}-1 \doteq 0{,}537 > \frac{1}{2}$, a pravá hranice prochází bodem $\left(0,\frac{2\sqrt{6}}{\sqrt{11}}-1\right)$, kde $\frac{2\sqrt{6}}{\sqrt{11}}-1 \doteq 0{,}477 < 0{,}478$ (jinými slovy pravá hranice



Obrázek 3.5: Hranice $U(-1,0)$ a $U(1,0)$ pro $D = 11$.

$U(-5,-1)$ je v nule „níže“, než levá hranice $U(2,1)$). Nakonec pravá hranice $U(-5,-1)$ prochází bodem $\left(\frac{\sqrt{9D+4}}{2} - 5, \frac{1}{2}\right)$, kde $\frac{\sqrt{9D+4}}{2} - 5 \doteq 0.074 > 0{,}064$, což jsme potřebovali.

5. případ: $D = 19$.

Základní oblast $F(19)$ je pokryta jednotkovými okolími bodů $(0,0)$, $(1,0)$, $(-1,0)$, $(3,1)$, $(2,0)$, $(6,-1)$, $(7,-1)$, $(19,-4)$, $(-2,1)$, $(-7,2)$, $(-90,21)$ a $(-430,99)$. Podrobný rozbor by byl obdobný jako v předchozím případě.

6. případ: $D = 57$.

Zde si vystačíme s množinami $U(0,0)$, $U(1,0)$, $U(-1,0)$, $U\left(\frac{5}{2},\frac{1}{2}\right)$, $U(-6,1)$, $U(2,0)$ a $U\left(\frac{11}{2},-\frac{1}{2}\right)$.

7. případ: $D = 73$.

Základní oblast $F(73)$ pokryjeme pomocí $U(0,0)$, $U(1,0)$, $U(-1,0)$, $U(2,0)$, $U\left(-\frac{21}{2},\frac{3}{2}\right)$, $U(-10,-1)$, $U(-27,-3)$, $U\left(\frac{5}{2},\frac{1}{2}\right)$, $U(7,1)$ a $U\left(\frac{57}{2},\frac{7}{2}\right)$.

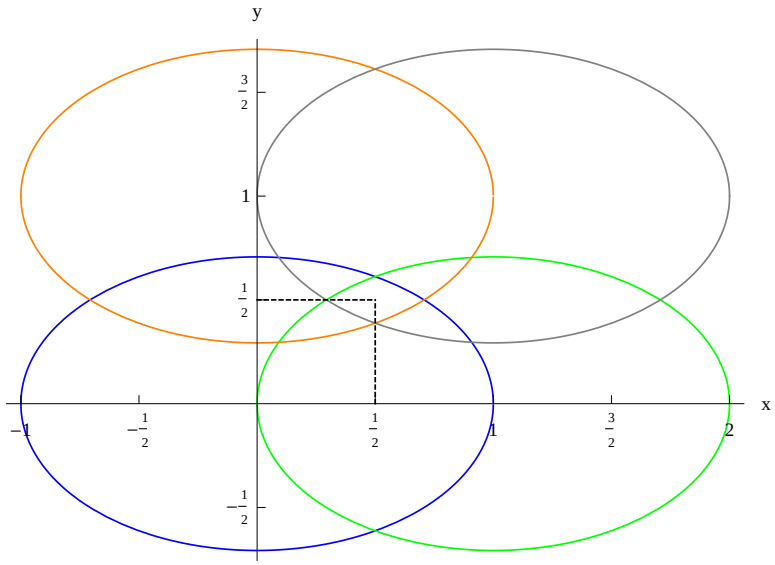
□

Jako zajímavost ještě uveďme, že v roce 1942 Rédei (RÉDEI (1942)) podal důkaz, že také těleso $\mathbb{Q}(\sqrt{97})$ je normově-euklidovské. Teprve v roce 1952 Barnes & Swinnerton-Dyer (BARNES a SWINNERTON-DYER (1952)) ukázali, že tomu tak není.

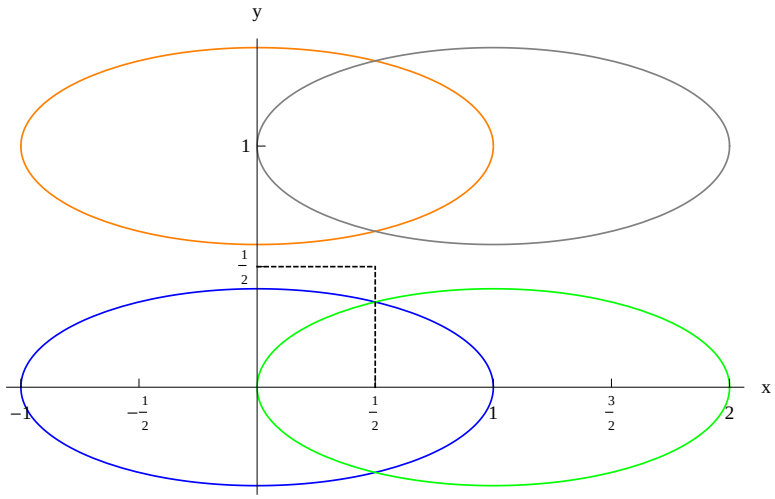
3.3 Geometrický pohled na imaginární kvadratická rozšíření

Pro $D < 0$ a $(a,b) \in M_D$ má hranice jednotkového okolí $U(a,b)$ předpis $(x-a)^2 + (y-b)^2 |D| = 1$, tedy jde o elipsu s hlavní poloosou velikosti 1 a vedlejší poloosou velikosti $\frac{1}{\sqrt{|D|}}$ (viz Obrázek 3.6). Využijeme tohoto pozorování spolu s Lemmatem 16 k alternativnímu důkazu Věty 14.

Věta 14. *Pro $D < 0$ je těleso $\mathbb{Q}(\sqrt{D})$ normově-euklidovské právě tehdy, když $D \in \{-1,-2,-3,-7,-11\}$.*



Obrázek 3.6: Hranice $U(0,0)$, $U(1,0)$, $U(0,1)$ a $U(1,1)$ pro $D=-2$.



Obrázek 3.7: Hranice $U(0,0)$, $U(1,0)$, $U(0,1)$ a $U(1,1)$ pro $D=-6$.

Důkaz. Důkaz opět rozdělíme na jednotlivé případy podle hodnoty D.

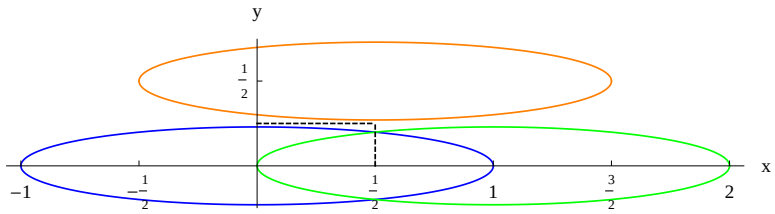
1. případ: $D \not\equiv 1 \pmod 4$.

Je-li $|D| < 3$, pak pro $(x,y) \in F(D)$ je $x^2 + y^2\,|D| \leq \frac{1}{4} + \frac{|D|}{4} < 1$, tedy $(x,y) \in U(0,0)$, a tedy pro $D=-1$ a $D=-2$ je těleso $\mathbb{Q}(\sqrt{D})$ normově-euklidovské.

Naopak, nechť $|D| \geq 3$ a uvažme bod $\left(\frac{1}{2},\frac{1}{2}\right) \in F(D)$. Tento bod neleží v žádném z jednotkových okolí bodů $(0,0)$, $(1,0)$, $(0,1)$ a $(1,1)$, neboť jistě platí $\left(\pm\frac{1}{2}\right)^2 + \left(\pm\frac{1}{2}\right)^2 |D| = \frac{1}{4} + \frac{|D|}{4} > 1$, tedy jistě $\left(\frac{1}{2},\frac{1}{2}\right) \notin \bigcup_{(a,b)\in M_D} U(a,b)$ (jako například na Obrázku 3.7), a tedy těleso $\mathbb{Q}(\sqrt{D})$ není normově-euklidovské.

2. případ: $D \equiv 1 \pmod 4$.

Nechť $|D| < 12$, pak pro $(x,y) \in F(D)$ platí $x^2 + y^2\,|D| \leq \frac{1}{4} + \frac{|D|}{16} < 1$, tedy $(x,y) \in U(0,0)$. Odtud dostáváme, že těleso $\mathbb{Q}(\sqrt{D})$ je normově-euklidovské pro $D \in \{-3,-7,-11\}$.



Obrázek 3.8: Hranice $U(0,0)$, $U(1,0)$ a $U\left(\frac{1}{2},\frac{1}{2}\right)$ pro $D=-19$.

Předpokládejme naopak $|D|\geq 12$. Jelikož uvažujeme pouze $D\equiv 1 \pmod 4$, máme dokonce $|D|\geq 15$. Podívejme se na bod $\left(\frac{1}{4},\frac{1}{4}\right)\in F(D)$. Ten může ležet jen v jednotkovém okolí bodu $(0,0)$ nebo $\left(\frac{1}{2},\frac{1}{2}\right)$. Jelikož ale platí $\left(\frac{1}{4}\right)^2+\left(\frac{1}{4}\right)^2|D| = \left(\frac{1}{4}-\frac{1}{2}\right)^2+\left(\frac{1}{4}-\frac{1}{2}\right)^2|D| = \frac{1+|D|}{16}\geq 1$, neboli $\left(\frac{1}{4},\frac{1}{4}\right)\notin U(0,0)\cup U\left(\frac{1}{2},\frac{1}{2}\right)$ (viz také Obrázek 3.8), není pro uvažovaná D těleso $\mathbb{Q}(\sqrt{D})$ normově-euklidovské.

□

Kapitola 4

Reálná kvadratická rozšíření II

Již víme, že pro $D \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$ je těleso $\mathbb{Q}(\sqrt{D})$ normově-euklidovské. Nyní je na řadě ukázat, že žádné jiné takové $D > 0$ neexistuje. Tento důkaz je však výrazně obtížnější, než v případě imaginárních kvadratických rozšíření, který jsme rozebrali ve druhé kapitole. Nejprve se proto zaměříme na nalezení nějaké horní závory takové, že pro všechna větší D již těleso $\mathbb{Q}(\sqrt{D})$ není normově-euklidovské, díky čemuž nám do další kapitoly zbyde ověřit již jen konečně mnoho možností. V této kapitole vycházíme z článku DAVENPORT (1951).

4.1 Podpůrné definice a tvrzení

Než se pustíme do hledání horní závory, uvedeme si pojem binární kvadratická forma a odvodíme některé její základní vlastnosti. Poté postupně zavedeme posloupnosti čísel, které nás budou provázet po zbytek kapitoly. Nevyhneme se ani několika ryze technickým tvrzením, pomocí kterých však později budeme schopni dokázat, že pro všechna normově-euklidovská tělesa $\mathbb{Q}(\sqrt{D})$ musí být $D < 2^{14}$.

Definice 12. Binární kvadratickou formou *rozumíme homogenní polynom dvou proměnných stupně 2, tedy* $f(x, y) = ax^2 + bxy + cy^2$, *kde* $a, b, c \in \mathbb{R}$.

Definujeme diskriminant *δ binární kvadratické formy* $f(x, y) = ax^2+bxy+cy^2$ *jako* $\delta = b^2 - 4ac$.

Binární kvadratickou formu f nazveme pozitivně definitní *(resp.* negativně definitní*), jestliže pro všechny dvojice $x, y \in \mathbb{R}$, kde alespoň jedno z čísel x a y je nenulové, platí $f(x, y) > 0$ (resp. $f(x, y) < 0$). Pokud binární kvadratická forma nabývá kladných i záporných hodnot, nazveme ji* indefinitní.

Řekneme, že binární kvadratické formy f a g jsou ekvivalentní*, jestliže existují $p, q, r, s \in \mathbb{R}$ taková, že $f(x, y) = g(px + qy, rx + sy)$ a $ps - qr = \pm 1$.*[1]

Jelikož zde nebude moci dojít k omylu, budeme často místo binární kvadraticka forma psát jen krátce forma.

Poznámka. Je-li $f(x, y) = ax^2+bxy+cy^2 = a(x+\theta y)(x+\theta' y)$, potom $b = a(\theta+\theta')$ a $c = a\theta\theta'$, a tedy $\delta = b^2 - 4ac = a^2(\theta - \theta')^2$.

[1] Nerozlišujeme zde tedy mezi tzv. silnou (pro $ps - qr = 1$) a tzv. slabou (pro $ps - qr = -1$) ekvivalencí.

Lemma 18. *Ekvivalentní binární kvadratické formy mají stejný diskriminant.*

Důkaz. Je-li $f(x,y) = ax^2 + bxy + cy^2$, můžeme také psát

$$f(x,y) = \begin{pmatrix} x & y \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Potom formy $f(x,y) = ax^2+bxy+cy^2$ a $g(x,y) = \alpha x^2+\beta xy+\gamma y^2$ jsou ekvivalentní právě tehdy, když existují p, q, r, s taková, že

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix} = \begin{pmatrix} \alpha & \frac{\beta}{2} \\ \frac{\beta}{2} & \gamma \end{pmatrix}$$

a

$$\begin{vmatrix} p & q \\ r & s \end{vmatrix} = \pm 1.$$

Odtud již plyne rovnost

$$\begin{vmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{vmatrix} = \begin{vmatrix} \alpha & \frac{\beta}{2} \\ \frac{\beta}{2} & \gamma \end{vmatrix},$$

neboli $b^2 - 4ac = \beta^2 - 4\alpha\gamma$.

□

Lemma 19. *Buď f binární kvadratická forma s reálnými koeficienty a $p, r \in \mathbb{Z}$ nesoudělná. Potom existuje ekvivalentní binární kvadratická forma g, jejíž koeficient u x^2 je roven hodnotě $f(p,r)$.*

Důkaz. Jelikož jsou čísla p, r nesoudělná, najdeme Bézoutovy koeficienty $q, s \in \mathbb{Z}$, $ps - qr = 1$. Je-li $f(x,y) = ax^2 + bxy + cy^2$, stačí formu g definovat jako formu určenou maticí

$$\begin{pmatrix} p & r \\ q & s \end{pmatrix} \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix} \begin{pmatrix} p & q \\ r & s \end{pmatrix},$$

neboť pak je první koeficient této formy roven právě $ap^2 + bpr + cr^2 = f(p,r)$.

□

Definice 13. *Indefinitní binární kvadratickou formu*

$$f(x,y) = ax^2 + bxy + cy^2 = a(x + \theta y)(x + \theta' y),$$

kde $a, b, c, \theta, \theta' \in \mathbb{R}$, nazveme redukovanou, *jestliže*

$$\theta > 2, \qquad \frac{1-\sqrt{5}}{2} \leq \theta' \leq \frac{3-\sqrt{5}}{2}. \tag{4.1}$$

Poznamenejme, že z praktických důvodů budeme pro čísla v posledí nerovnosti využívat jejich desetinný zápis, budeme tedy psát $-0{,}618\ldots$ místo $\frac{1-\sqrt{5}}{2}$ a $0{,}382\ldots$ místo $\frac{3-\sqrt{5}}{2}$.

Tvrzení 20. *Je-li* $f(x,y) = ax^2+bxy+cy^2 = a(x+\theta y)(x+\theta' y)$ *indefinitní binární kvadratická forma s nenulovým diskriminantem taková, že* θ *a* θ' *jsou iracionální, pak* $f(x,y)$ *je ekvivalentní nějaké redukované binární kvadratické formě.*

Důkaz. Označme $m = \inf\{|f(x,y)| \mid x,y \in \mathbb{Z},\ x \neq 0 \text{ nebo } y \neq 0\}$

1. případ: $m = 0$.

Podle Lemmatu 19 existuje forma

$$g(x,y) = \alpha x^2 + \beta xy + \gamma y^2 = \alpha(x+\vartheta y)(x+\vartheta' y)$$

ekvivalentní formě f, pro kterou je $|\alpha|$ libovolně malé (ovšem nenulové, neboť θ a θ' jsou iracionální). Jelikož podle Lemmatu 18 mají formy f a g stejný diskriminant $a^2(\theta-\theta')^2 = \alpha^2(\vartheta-\vartheta')^2$, je $|\vartheta-\vartheta'|$ libovolně velké. Bez újmy na obecnosti můžeme předpokládat $\vartheta > \vartheta'$. Nalezneme $n \in \mathbb{N}$ takové, že

$$-0{,}618\ldots < \vartheta' + n \leq 0{,}382\ldots.$$

Označíme $\vartheta_1 = \vartheta + n$ a $\vartheta_1' = \vartheta' + n$. Potom jsou binární kvadratické formy $\alpha(x+\vartheta y)(x+\vartheta' y)$ a $\alpha(x+\vartheta_1 y)(x+\vartheta_1' y)$ ekvivalentní, neboť je

$$\alpha((px+qy)+\vartheta(rx+sy))((px+qy)+\vartheta'(rx+sy)) = \alpha(x+(\vartheta+n)y)(x+(\vartheta'+n)y)$$

pro $p=1$, $q=n$, $r=0$, $s=1$. Navíc je $\vartheta_1 - \vartheta_1' = \vartheta - \vartheta'$ libovolně velké, můžeme proto bez újmy na obecnosti předpokládat, že $\vartheta > 2$. Potom forma $\alpha(x+\vartheta_1 y)(x+\vartheta_1' y)$ splňuje podmínky (4.1), je tedy redukovaná a ekvivalentní formě f.

2. případ: $m > 0$.

Můžeme předpokládat, že $\theta > \theta'$. Podobně jako v 1. případě nalezneme $n \in \mathbb{N}$ takové, že

$$-0{,}618\ldots < \theta' + n \leq 0{,}382\ldots,$$

a opět položíme $\theta_1 = \theta + n$ a $\theta_1' = \theta' + n$. Buď $\epsilon > 0$ libovolně malé. Přechodem k ekvivalentní formě můžeme bez újmy na obecnosti předpokládat, že

$$m \leq |a| < \frac{m}{1-\epsilon}.$$

Potom

$$1-\epsilon < \frac{m}{|a|} < \frac{f(x,y)}{|a|} = |(x+\theta_1 y)(x+\theta_1' y)|$$

pro všechna $x,y \in \mathbb{Z}$, $x \neq 0$ nebo $y \neq 0$. Ve speciálním případě $x=0$, $y=1$ dostáváme

$$|\theta_1\theta_1'| > 1-\epsilon,$$

odkud

$$\theta_1 > \frac{(1-\epsilon)}{|\theta_1'|} > 1{,}618\ldots(1-\epsilon).$$

Ukážeme, že alespoň jedna z forem určených některou ze tří dvojic

$$\theta_1,\ \theta_1';\ 2-\theta_1,\ 2-\theta_1';\ 1-\frac{1}{\theta_1},\ 1-\frac{1}{\theta_1'}$$

splňuje podmínku redukované formy. Pokud je $\theta_1 > 2$, jsme hotovi. Můžeme tedy předpokládat, že $\theta_1 < 2$. Potom z nerovností

$$|\theta_1\theta_1'| > 1 - \epsilon \text{ a } -0{,}618\ldots < \theta_1' \leq 0{,}382\ldots$$

dostáváme $\theta_1' < 0$, odkud máme $2 - \theta_1' > 2$ a $1 - \frac{1}{\theta_1'} > 2$. Zbývá tedy jen ukázat, že $2 - \theta_1$ nebo $1 - \frac{1}{\theta_1}$ splňuje druhou nerovnost v (4.1). Je ale

$$0 < 2 - \theta_1 \leq 0{,}382\ldots, \text{ pokud } \theta_1 \geq 1{,}618\ldots,$$

$$0 < 1 - \frac{1}{\theta_1} \leq 0{,}382\ldots, \text{ pokud } \theta_1 \leq 1{,}618\ldots.$$

Nyní si stačí uvědomit, že forma určená libovolnou z těchto tří dvojic je ekvivalentní formě f.

□

Lemma 21. *Nechť*

$$f_0(x, y) = a_0(x + \theta_0 y)(x + \theta_0' y)$$

je redukovaná forma a předpokládejme, že θ_0 a θ_0' jsou iracionální. Potom existují celá čísla

$$\ldots, t_{-2}, t_{-1}, t_0, t_1, t_2, \ldots$$

a čísla

$$\ldots, \mu_{-2}, \mu_{-1}, \mu_0, \mu_1, \mu_2, \ldots,$$

každé rovno ± 1, taková, že pro každou dvojici čísel θ_n a θ_n', definovaných pro $n > 0$ a $n < 0$ rekurentně vztahy

$$\theta_n = t_n + \frac{\mu_{n+1}}{\theta_{n+1}}, \qquad \theta_n' = t_n + \frac{\mu_{n+1}}{\theta_{n+1}'}, \tag{4.2}$$

je příslušná forma redukovaná. Navíc μ_{n+1} má opačné znaménko než θ_{n+1}'. Pro každé $n \in \mathbb{Z}$ pak existuje redukovaná forma

$$f_n(x, y) = a_n(x + \theta_n y)(x + \theta_n' y)$$

ekvivalentní formě $f_0(x, y)$ a ekvivalenci mezi $f_n(x, y)$ a $f_{n+1}(x, y)$ lze vyjádřit jako $f_n(x, y) = f_{n+1}(y, \mu_{n+1}(x + t_n y))$.

Důkaz. Postupujme induktivně. Předpokládejme, že $n \geq 0$ a máme již zkonstruováno $\theta_n > 2$, které je iracionální. Pak definujeme $t_n \in \mathbb{Z}$ tak, aby $|t_n - \theta_n|$ bylo nejmenší možné, a položíme

$$\theta_{n+1} = \frac{\mu_{n+1}}{\theta_n - t_n}.$$

Z iracionality θ_0 pak plyne iracionalita θ_n, a tedy $0 < |t_n - \theta_n| < \frac{1}{2}$ pro všechna $n \geq 0$. Proto lze vybrat $\mu_{n+1} \in \{1, -1\}$ tak, aby platilo $\theta_{n+1} > 2$. Tím máme definované posloupnosti čísel $t_0, t_1, \ldots; \theta_0, \theta_1, \ldots;$ $\mu_0, \mu_1, \ldots$, kde $\theta_n > 2$ a $t_n \geq 2$ pro každé $n \geq 0$, a pokud $\mu_{n+1} = -1$, pak dokonce $t_n = \theta_n + \frac{1}{\theta_{n+1}} > 2$, neboli $t_n \geq 3$. Dále definujeme

$$\theta_{n+1}' = -\frac{\mu_{n+1}}{t_n - \theta_n'}.$$

Ukážeme, že

$$-0{,}618\ldots \le \theta'_n \le 0{,}382\ldots$$

pro každé $n \ge 0$: Pro $n = 0$ platí z předpokladu, a platí-li pro $n \ge 0$, pak pro $n+1$ máme

$$t_n - \theta'_n \ge \begin{cases} 2 - 0{,}382\ldots = 1{,}618\ldots \text{ vždy,} \\ 3 - 0{,}382\ldots = 2{,}618\ldots \text{ pro } \mu_{n+1} = -1, \text{ neboť pak je } t_n \ge 3. \end{cases}$$

Platí $\frac{1}{1{,}618\ldots} = 0{,}618\ldots$ a $\frac{1}{2{,}618\ldots} = 0{,}382\ldots$, navíc μ_{n+1} má zřejmě opačné znaménko než θ'_{n+1}.

Nyní zvolíme $\mu_0 \in \{1, -1\}$ tak, aby mělo opačné znaménko než θ'_0. Dále předpokládejme, že již máme pro $n > 0$ zkonstruováno iracionální θ'_{-n} splňující $-0{,}618\ldots < \theta'_{-n} \le 0{,}382\ldots$. Volíme $\mu_{-n} \in \{1, -1\}$ vždy tak, aby mělo opačné znaménko než θ'_{-n}. Potom nalezneme $t_{-n-1} \in \mathbb{Z}$ takové, že pro

$$\theta'_{-n-1} = t_{-n-1} + \frac{\mu_{-n}}{\theta'_{-n}}$$

platí $-0{,}618\ldots < \theta'_{-n-1} \le 0{,}382\ldots$. Pak máme

$$t_{-n-1} > -0{,}618\ldots + \frac{1}{|\theta'_{-n}|} \ge -0{,}618\ldots + 1{,}618\ldots = 1,$$

neboli $t_{-n-1} \ge 2$. Je-li navíc $\mu_{-n} = -1$, dostáváme dokonce

$$t_{-n-1} > -0{,}618\ldots + \frac{1}{\theta'_{-n}} \ge -0{,}618\ldots + 2{,}618\ldots = 2,$$

neboli $t_{-n-1} \ge 3$. Tímto máme definovány posloupnosti $t_0, t_{-1}, \ldots; \theta'_0, \theta'_{-1}, \ldots;$ $\mu_0, \mu_{-1}, \ldots$. Dále položíme

$$\theta_{-n-1} = t_{-n-1} + \frac{\mu_{-n}}{\theta_{-n}}$$

a ukážeme, že $\theta_{-n} > 2$ pro všechna $n \ge 0$: Pro $n = 0$ to plyne přímo z předpokladu, a jestliže to platí pro $n \ge 0$, pak pro $n+1$ máme

$$\theta_{-n-1} = t_{-n-1} + \frac{\mu_{-n}}{\theta_{-n}} > \begin{cases} 2 & \text{pro } \mu_{-n} = 1, \\ 3 - \frac{1}{2} & \text{pro } \mu_{-n} = -1. \end{cases}$$

Odtud pak také plyne, že t_{-n-1} je nejbližší celé číslo k θ_{-n-1}. Poznamenejme ještě, že θ_n i θ'_n jsou díky iracionalitě θ_0 a θ'_0 nenulová pro všechna $n \in \mathbb{Z}$.

Zbývá dokázat existenci redukovaných forem $f_n(x, y) = a_n(x + \theta_n y)(x + \theta'_n y)$ ekvivalentních formě $f_0(x, y)$. Z (4.2) dostáváme

$$x + \theta_n y = x + \left(t_n + \frac{\mu_{n+1}}{\theta_{n+1}}\right) y = \frac{\mu_{n+1}}{\theta_{n+1}} \left(X + \theta_{n+1} Y\right),$$

kde $X = y$ a $Y = \mu_{n+1}(x + t_n y)$. Podobně lze vyjádřit θ'_n pomocí θ'_{n+1}, a tedy

$$(x + \theta y)(x + \theta' y) = \frac{1}{\theta_{n+1}\theta'_{n+1}} (X + \theta_{n+1} Y)(X + \theta'_{n+1} Y).$$

Spolu s $f_0(x,y) = a_0(x+\theta_n y)(x+\theta'_n y)$ takto dostáváme rekurentní předpis pro funkce f_n pro $n > 0$ a $n < 0$. Navíc je $X = px + qy$ a $Y = rx + sy$ pro $p = 0, q = 1, r = \mu_{n+1}, s = \mu_{n+1}t_n$, tedy $ps - rq = \mu_{n+1} = \pm 1$. Odtud přímo plyne ekvivalence forem f_0 a f_n pro všechna n. Nakonec první koeficient a_n formy f_n je definován rekurentním vztahem $a_n = \theta_{n+1}\theta'_{n+1}a_{n+1}$.

□

Definujme nyní ϕ_n pro všechna n předpisem

$$\phi_n = -\frac{\mu_n}{\theta'_n}. \tag{4.3}$$

Zřejmě je potom $\phi_n > 0$ a z nerovností $-0{,}618\ldots < \theta'_n \leq 0{,}382\ldots$ plyne

$$\phi_n \geq \begin{cases} 1{,}618\ldots \quad \text{vždy,} \\ 2{,}618\ldots, \text{ pokud } \mu_n = -1. \end{cases}$$

Dosadíme-li do definice ϕ_n za θ'_n, dostaneme pro ϕ_n rekurentní předpis:

$$\phi_n = -\frac{\mu_n}{\frac{\mu_n}{\theta'_{n-1}-t_{n-1}}} = t_{n-1} - \theta'_{n-1} = t_{n-1} + \frac{\mu_{n-1}}{\phi_{n-1}}. \tag{4.4}$$

Dále definujme

$$v_n = \left\lfloor \frac{\theta_n}{2} \right\rfloor,$$

tedy $v_n \in \mathbb{N}$, a položme

$$\beta_n = v_n + \frac{\mu_{n+1}}{\theta_{n+1}}v_{n+1} + \frac{\mu_{n+1}\mu_{n+2}}{\theta_{n+1}\theta_{n+2}}v_{n+2} + \cdots, \tag{4.5}$$

$$\beta'_n = \frac{v_{n-1}}{\phi_n} - \frac{v_{n-2}}{\phi_n\phi_{n-1}} + \frac{v_{n-3}}{\phi_n\phi_{n-1}\phi_{n-2}} - \cdots, \tag{4.6}$$

pro všechna $n \in \mathbb{Z}$. Nahlédneme, že obě řady jsou konvergentní, a tedy β_n a β'_n jsou dobře definované. Konvergence první řady plyne z odhadů

$$\frac{v_{n+k}}{\theta_{n+1}\cdots\theta_{n+k}} < \frac{\frac{\theta_{n+k}}{2}}{\theta_{n+1}\cdots\theta_{n+k}} < \frac{1}{2^k},$$

neboť potom je

$$|\beta_n| < \sum_{k=0}^{\infty} \frac{1}{2^k} = 2$$

a navíc zřejmě $\beta_n > 0$. Pro druhou řadu využijeme odhad

$$v_{m-1} < \frac{\theta_{m-1}}{2} = \frac{1}{2}\left(t_{m-1} + \frac{\mu_m}{\theta_m}\right) < \frac{t_{m-1}}{2} + \frac{1}{4} < \frac{t_{m-1}}{2} + 1 - 0{,}618\ldots \leq$$

$$\leq \frac{t_{m-1}}{2} + \frac{t_{m-1}}{2} - 0{,}618\ldots = t_{m-1} - 0{,}618\ldots \leq t_{m-1} + \frac{\mu_{m-1}}{\phi_{m-1}} = \phi_m,$$

ze kterého plyne

$$\frac{v_{m-1}}{\phi_m} < 1,$$

a tedy

$$\frac{v_{n-k-1}}{\phi_n\phi_{n-1}\cdots\phi_{n-k}} < \frac{1}{\phi_n\phi_{n-1}\cdots\phi_{n-k+1}} \leq \frac{v_{n-k}}{\phi_n\phi_{n-1}\cdots\phi_{n-k+1}}.$$

Jinými slovy absolutní hodnota členů této řady klesá a znaménka členů alternují, odkud již vyplývá konvergence (podle Leibnizova kritéria). Z nerovnosti

$$0 < \frac{v_{m-1}}{\phi_m} < 1$$

dostáváme dále

$$0 < \beta'_n < 1.$$

Nakonec uveďme ještě rekurentní vztahy, které plynou přímo z definic:

$$\beta_n = v_n + \frac{\mu_{n+1}\beta_{n+1}}{\theta_{n+1}}, \tag{4.7}$$

$$\beta'_n = \frac{v_{n-1} - \beta'_{n-1}}{\phi_n}. \tag{4.8}$$

Lemma 22. *Pro všechna $n \in \mathbb{Z}$ platí*

$$\beta_n \leq \frac{3}{4}\theta_n. \tag{4.9}$$

Důkaz. Začneme důkazem slabší nerovnosti $\beta_n < \theta_n$, která plyne z nerovnosti $v_k \leq \frac{1}{2}\theta_k$ a z (4.5) :

$$\frac{\beta_n}{\theta_n} \leq \frac{v_n}{\theta_n} + \frac{v_{n+1}}{\theta_n\theta_{n+1}} + \frac{v_{n+2}}{\theta_n\theta_{n+1}\theta_{n+2}} + \cdots < \frac{1}{2}\left(1 + \frac{1}{2} + \frac{1}{2^2} + \cdots\right) = 1.$$

Buď nejprve $\theta_n > 4$, pak z (4.7) dostáváme

$$\frac{\beta_n}{\theta_n} \leq \frac{1}{\theta_n}\left(v_n + \frac{\beta_{n+1}}{\theta_{n+1}}\right) < \frac{1}{\theta_n}\left(\frac{\theta_n}{2} + 1\right) = \frac{1}{2} + \frac{1}{\theta_n} < \frac{1}{2} + \frac{1}{4} = \frac{3}{4}.$$

Dále můžeme předpokládat $\theta_n < 4$ (je $\theta_n \neq 4$ vždy, neboť θ_n je iracionální), z čehož plyne $v_n = 1$. Z první rovnosti v (4.2) a z již dokázané nerovnosti $t_n \geq 2$ máme

$$\theta_n = t_n + \frac{\mu_{n+1}}{\theta_{n+1}} \geq 2 + \frac{1}{\theta_{n+1}},$$

což nám spolu s (4.7) dává

$$\frac{\beta_n}{\theta_n} \leq \frac{1}{\theta_n}\left(v_n + \frac{\beta_{n+1}}{\theta_{n+1}}\right) = \frac{1}{\theta_n}\frac{\theta_{n+1} + \beta_{n+1}}{\theta_{n+1}} \leq \frac{1}{2 + \frac{1}{\theta_{n+1}}}\frac{\theta_{n+1} + \beta_{n+1}}{\theta_{n+1}} =$$

$$= \frac{\theta_{n+1} + \beta_{n+1}}{2\theta_{n+1} + 1} \leq \frac{1}{2\theta_{n+1} + 1}\left(\theta_{n+1} + v_{n+1} + \frac{\beta_{n+2}}{\theta_{n+2}}\right) < \frac{1}{2\theta_{n+1} + 1}\left(\frac{3}{2}\theta_{n+1} + \frac{\beta_{n+2}}{\theta_{n+2}}\right),$$

a tedy

$$\frac{\beta_n}{\theta_n} - \frac{3}{4} < \frac{1}{2\theta_{n+1} + 1}\left(\frac{3}{2}\theta_{n+1} + \frac{\beta_{n+2}}{\theta_{n+2}}\right) - \frac{3}{4} = \frac{1}{2\theta_{n+1} + 1}\left(\frac{\beta_{n+2}}{\theta_{n+2}} - \frac{3}{4}\right).$$

Nyní je-li $\beta_{n+2} \leq \frac{3}{4}\theta_{n+2}$, plyne tvrzení přímo z nerovnosti výše. V opačném případě můžeme argument zopakovat pro $n+2$. Jelikož $2\theta_{n+1}+1 > 5$, dostaneme po k krocích

$$\frac{\beta_n}{\theta_n} - \frac{3}{4} < \frac{1}{5^k}\frac{\beta_{n+2k}}{\theta_{n+2k}} < \frac{1}{5^k}.$$

Tato nerovnost ale platí pro libovolně velké k, a tedy odtud plyne $\frac{\beta_n}{\theta_n} - \frac{3}{4} \leq 0$. □

Důsledek. Z (4.7) a (4.9) plyne

$$|\beta_n - v_n| = \frac{\beta_{n+1}}{\theta_{n+1}} \leq \frac{3}{4}.$$

Speciálně platí

$$\beta_n \geq \frac{1}{4}.$$

Lemma 23. *Pro všechna $n \in \mathbb{Z}$ platí*

$$\beta'_n \leq \frac{1}{2}.$$

Důkaz. Z (4.4) máme

$$\phi_n = t_{n-1} + \frac{\mu_{n-1}}{\phi_{n-1}} \geq t_{n-1} - \frac{1}{\phi_{n-1}}.$$

Dále víme

$$2v_{n-1} < \theta_{n-1} < t_{n-1} + \frac{1}{2},$$

odkud $2v_{n-1} \leq t_{n-1}$. Dohromady pak dostáváme

$$\phi_n \geq 2v_{n-1} - \frac{1}{\phi_{n-1}} > 0.$$

Použijeme-li vztah (4.8), získáme

$$\beta'_n = \frac{v_{n-1} - \beta'_{n-1}}{\phi_n} \leq \frac{v_{n-1} - \beta'_{n-1}}{2v_{n-1} - \frac{1}{\phi_{n-1}}} =$$

$$= \frac{\phi_{n-1}(v_{n-1} - \beta'_{n-1})}{2v_{n-1}\phi_{n-1} - 1} = \frac{\phi_{n-1}v_{n-1} - v_{n-2} + \beta'_{n-2}}{2v_{n-1}\phi_{n-1} - 1}.$$

Odtud pak

$$\beta'_n - \frac{1}{2} \leq \frac{\phi_{n-1}v_{n-1} - v_{n-2} + \beta'_{n-2} - \frac{1}{2}(2v_{n-1}\phi_{n-1} - 1)}{2v_{n-1}\phi_{n-1} - 1} =$$

$$= \frac{\beta'_{n-2} - v_{n-2} + \frac{1}{2}}{2v_{n-1}\phi_{n-1} - 1} \leq \frac{\beta'_{n-2} - \frac{1}{2}}{2v_{n-1}\phi_{n-1} - 1}.$$

Pokud $\beta'_{n-2} \leq \frac{1}{2}$, je důkaz hotov. V opačném případě z $\phi_n \geq 1{,}618\ldots = \frac{1+\sqrt{5}}{2}$ plyne

$$2v_{n-1}\phi_{n-1} - 1 \geq 2\frac{1+\sqrt{5}}{2} - 1 = \sqrt{5},$$

a tedy

$$\beta'_n - \frac{1}{2} \leq \frac{\beta'_{n-2} - \frac{1}{2}}{2v_{n-1}\phi_{n-1} - 1} \leq \frac{\beta'_{n-2} - \frac{1}{2}}{\sqrt{5}}.$$

Stejný argument však můžeme zopakovat k krát pro libovolně velké k, s použitím nerovnosti $0 < \beta'_{n-2k} < 1$ tak dostaneme

$$\beta'_n - \frac{1}{2} \leq \frac{1}{\left(\sqrt{5}\right)^k}\left(\beta'_{n-2k} - \frac{1}{2}\right) < \frac{1}{2\left(\sqrt{5}\right)^k},$$

odkud již

$$\beta'_n - \frac{1}{2} \leq 0.$$

□

Lemma 24. *Pro všechna $n \in \mathbb{Z}$ platí*

$$\frac{\beta_n \beta'_n}{\theta_n - \theta'_n} > \frac{1}{128}.$$

Důkaz. Nejprve ukážeme nerovnost

$$\frac{\beta_n}{\theta_n - \theta'_n} > \frac{1}{4\left(4 - \frac{1}{3} - \theta'_n\right)}. \tag{4.10}$$

Je-li $\mu_{n+1} = 1$, máme z (4.3) $\theta_n = t_n + \frac{1}{\theta_{n+1}}$, a tedy

$$v_n = \left\lfloor \frac{1}{2}\theta_n \right\rfloor = \left\lfloor \frac{1}{2}\left(t_n + \frac{1}{\theta_{n+1}}\right) \right\rfloor,$$

odkud $v_n = \frac{t_n}{2}$, je-li t_n sudé, a $v_n = \frac{t_n - 1}{2}$, je-li t_n liché. V obou případech však platí $t_n \leq 2v_n + 1$. Jelikož je $\beta_{n+1}, \theta_{n+1} > 0$, dostáváme ze (4.7) nerovnost

$$\beta_n = v_n + \frac{\beta_{n+1}}{\theta_{n+1}} > v_n.$$

Dohromady pak

$$\theta_n \leq 2v_n + 1 + \frac{1}{\theta_{n+1}} < 2v_n + \frac{3}{2},$$

a tedy (spolu s faktem, že $v_n \geq 1$)

$$\frac{\beta_n}{\theta_n - \theta'_n} > \frac{v_n}{2v_n + \frac{3}{2} - \theta'_n} \geq \frac{1}{\frac{7}{2} - \theta'_n} > \frac{1}{4\left(4 - \frac{1}{3} - \theta'_n\right)}.$$

Buď nyní $\mu_{n+1} = -1$. Z (4.2) máme $\theta_n = t_n - \frac{1}{\theta_{n+1}}$, a tedy

$$v_n = \left\lfloor \frac{1}{2}\theta_n \right\rfloor = \left\lfloor \frac{1}{2}\left(t_n - \frac{1}{\theta_{n+1}}\right) \right\rfloor = \left\lfloor \frac{1}{2}\left(t_n - 1\right) \right\rfloor,$$

odkud máme, že $v_n = \frac{t_n-1}{2}$, je-li t_n liché, a $v_n = \frac{t_n-2}{2}$, je-li t_n sudé. Jistě tedy platí $t_n \leq 2v_n + 2$. Odtud dostáváme

$$\theta_n \leq 2v_n + 2 - \frac{1}{\theta_{n+1}}.$$

Dále podle (4.7) je $\beta_n = v_n - \frac{\beta_{n+1}}{\theta_{n+1}}$. Předpokládejme nejprve, že $\theta_{n+1} < 3$. Potom díky (4.9) platí

$$\frac{\beta_n}{\theta_n - \theta'_n} = \frac{v_n - \frac{\beta_{n+1}}{\theta_{n+1}}}{\theta_n - \theta'_n} \geq \frac{v_n - \frac{3}{4}}{2v_n + 2 - \frac{1}{3} - \theta'_n}.$$

Výraz na pravé straně je ale rostoucí ve v_n, což lze snadno ověřit derivováním. Stačí tedy dosadit $v_n = 1$:

$$\frac{\beta_n}{\theta_n - \theta'_n} \geq \frac{1 - \frac{3}{4}}{2 \cdot 1 + 2 - \frac{1}{3} - \theta'_n} = \frac{1}{4\left(4 - \frac{1}{3} - \theta'_n\right)}.$$

Buď nyní $\theta_{n+1} > 3$. Jelikož

$$\frac{\beta_{n+1}}{\theta_{n+1}} \leq \frac{v_{n+1} + \frac{\beta_{n+2}}{\theta_{n+2}}}{\theta_{n+1}} = \frac{v_{n+1}}{\theta_{n+1}} + \frac{\beta_{n+2}}{\theta_{n+2}}\frac{1}{\theta_{n+1}} < \frac{1}{2} + \frac{3}{4}\frac{1}{\theta_{n+1}},$$

platí

$$\frac{\beta_n}{\theta_n - \theta'_n} = \frac{v_n - \frac{\beta_{n+1}}{\theta_{n+1}}}{\theta_n - \theta'_n} > \frac{v_n - \frac{1}{2} - \frac{3}{4\theta_{n+1}}}{2v_n + 2 - \frac{1}{\theta_{n+1}} - \theta'_n}.$$

Výraz napravo je opět rostoucí ve v_n, tedy

$$\frac{\beta_n}{\theta_n - \theta'_n} > \frac{1 - \frac{1}{2} - \frac{3}{4\theta_{n+1}}}{2 \cdot 1 + 2 - \frac{1}{\theta_{n+1}} - \theta'_n} = \frac{\frac{1}{2} - \frac{3}{4\theta_{n+1}}}{4 - \frac{1}{\theta_{n+1}} - \theta'_n}.$$

Teno výraz je ale rostoucí v proměnné θ_{n+1}, dosazením $\theta_{n+1} = 3$ tak dostaneme

$$\frac{\beta_n}{\theta_n - \theta'_n} > \frac{\frac{1}{2} - \frac{1}{4}}{4 - \frac{1}{3} - \theta'_n} = \frac{1}{4\left(4 - \frac{1}{3} - \theta'_n\right)}.$$

Nyní se již můžeme podívat na požadovanou nerovnost. Za použití výše uvedeného odhadu, (4.3), (4.8) a Lemmatu 23 dostáváme

$$\frac{\beta_n\beta'_n}{\theta_n - \theta'_n} > \frac{\beta'_n}{4\left(\frac{11}{3} - \theta'_n\right)} = \frac{\frac{v_{n-1} - \beta'_{n-1}}{\phi_n}}{4\left(\frac{11}{3} + \frac{\mu_n}{\phi_n}\right)} = \frac{v_{n-1} - \beta'_{n-1}}{4\left(\frac{11}{3}\phi_n + \mu_n\right)} \geq \frac{v_{n-1} - \frac{1}{2}}{4\left(\frac{11}{3}\phi_n + \mu_n\right)}.$$

Předpokládejme $v_{n-1} \geq 2$. Z (4.4) dostáváme

$$\phi_n = t_{n-1} + \frac{\mu_{n-1}}{\phi_{n-1}} \leq 2v_{n-1} + 2 + 0{,}618\ldots,$$

tedy

$$\frac{\beta_n\beta'_n}{\theta_n - \theta'_n} > \frac{v_{n-1} - \frac{1}{2}}{4\left(\frac{22}{3}v_{n-1} + \frac{11}{3}(2{,}618\ldots) + \mu_n\right)} > \frac{\frac{3}{2}}{4\left(\frac{22}{3} \cdot 2 + \frac{11}{3}(2{,}618\ldots) + 1\right)} > \frac{1}{70},$$

kde v prostřední nerovnosti využíváme monotonie výrazu v proměnné v_{n-1}.

Zbývá nám vyřešit případ $v_{n-1} = 1$. Potom je nutně $\theta_{n-1} < 4$, $t_{n-1} \leq 4$ vždy a $t_{n-1} \leq 3$ pro $\mu_n = 1$. Pokud $\mu_n = 1$, dostáváme ze (4.4)

$$\phi_n \leq t_{n-1} + \frac{1}{\phi_{n-1}} \leq 3 + \frac{1}{1{,}618\ldots} = 3{,}618\ldots,$$

a tedy

$$\frac{\beta_n \beta_n'}{\theta_n - \theta_n'} > \frac{1 - \frac{1}{2}}{4\left(\frac{11}{3}(3{,}618\ldots) + 1\right)} > \frac{1}{115}.$$

Jestliže naopak $\mu_n = -1$, máme ze (4.4)

$$\phi_n \leq t_{n-1} + \frac{1}{\phi_{n-1}} \leq 4 + \frac{1}{1{,}618\ldots} = 4{,}618\ldots,$$

odkud

$$\frac{\beta_n \beta_n'}{\theta_n - \theta_n'} > \frac{1 - \frac{1}{2}}{4\left(\frac{11}{3}(4{,}618\ldots) - 1\right)} > \frac{1}{128}.$$

Tím je důkaz hotov.

□

4.2 Obecné indefinitní binární kvadratické formy

Celou sekci věnujeme důkazu následující věty:

Věta 25. *Nechť*

$$f(x,y) = ax^2 + bxy + cy^2 = a(x + \theta y)(x + \theta' y)$$

je indefinitní binární kvadratická forma s reálnými koeficienty a, b, c. Předpokládejme, že $a \neq 0$ a že θ a θ' jsou různá iracionální čísla. Potom existují reálná čísla p, q taková, že

$$|f(x + p, y + q)| > \frac{1}{128}\sqrt{\delta}$$

pro všechna celá čísla x, y, kde $\delta = b^2 - 4ac$ je diskriminant formy f.

Podle Tvrzení 20 stačí tuto větu dokázat pro redukovanou binární kvadratickou formu $f_0(x, y) = a_0(x + \theta_0 y)(x + \theta_0' y)$. Jestliže

$$|f_0(x + p_0, y + q_0)| > \frac{1}{128}\sqrt{\delta} \tag{4.11}$$

pro všechna $x, y \in \mathbb{Z}$, příslušná $p, q \in \mathbb{R}$ z tvrzení věty získáme z čísel p_0, q_0 právě přechodem od formy $f_0(x, y)$ k formě $f(x, y)$.

Za použití značení a definic předchozí sekce definujeme p_0, q_0 jako řešení soustavy rovnic

$$p_0 + \theta_0 q_0 = \beta_0, \qquad p_0 + \theta_0' q_0 = \beta_0'.$$

Protože platí $\delta = a_0^2(\theta_0 - \theta_0')^2$, je nerovnost (4.11), kterou potřebujeme dokázat, ekvivalentní nerovnosti

$$|(x + \theta_0 y + \beta_0)(x + \theta_0' y + \beta_0')| > \frac{\theta_0 - \theta_0'}{128}. \tag{4.12}$$

Ve zbytku sekce budeme uvažovat existenci čísel $x_0, y_0 \in \mathbb{Z}$ nesplňujících nerovnost (4.12) a ukážeme, že tento předpoklad nutně vede ke sporu.

Lemma 26. *Předpokládejme, že existují čísla $x_0, y_0 \in \mathbb{Z}$, která nesplňují (4.12). Potom existují $n \in \mathbb{Z}$ a $x, y \in \mathbb{Z}$ taková, že*

$$|x + \theta_n y + \beta_n| \leq \frac{\theta_n}{\sqrt{128}}, \tag{4.13}$$

$$|x + \theta'_n y + \beta'_n| \leq \frac{\theta_n - \theta'_n}{\sqrt{128}}, \tag{4.14}$$

$$|(x + \theta_n y + \beta_n)(x + \theta'_n y + \beta'_n)| \leq \frac{\theta_n - \theta'_n}{128}. \tag{4.15}$$

Důkaz. Označme

$$L_n(x, y) = x + \theta_n y + \beta_n, \quad L'_n(x, y) = x + \theta'_n y + \beta'_n.$$

Z (4.2) a (4.7) plyne

$$L_n(x, y) = x + \left(t_n + \frac{\mu_{n+1}}{\theta_{n+1}}\right) y + v_n + \frac{\mu_{n+1}\beta_{n+1}}{\theta_{n+1}},$$

a tedy

$$L_n(x, y) = \frac{\mu_{n+1}}{\theta_{n+1}} L_{n+1}(y, \mu_{n+1}(x + t_n y + v_n)), \tag{4.16}$$

podobně pro čárkované symboly. Definujme proto nyní pro $n > 0$ a $n < 0$ čísla $x_n, y_n \in \mathbb{Z}$ jako

$$x_{n+1} = y_n, \quad y_{n+1} = \mu_{n+1}(x_n + t_n y + v_n).$$

Dále z (4.2) dostáváme, že

$$\theta_n - \theta'_n = \mu_{n+1} \frac{\theta'_{n+1} - \theta_{n+1}}{\theta'_{n+1}\theta_{n+1}},$$

neboli

$$\frac{1}{\theta'_{n+1}\theta_{n+1}} = -\mu_{n+1} \frac{\theta_{n+1} - \theta'_{n+1}}{\theta_n - \theta'_n}.$$

Jelikož dle předpokladu

$$|L_0(x_0, y_0) L'_0(x_0, y_0)| \leq \frac{\theta_0 - \theta'_0}{128},$$

dostaneme pomocí indukce, že také

$$|L_n(x_n, y_n) L'_n(x_n, y_n)| \leq \frac{\theta_n - \theta'_n}{128} \tag{4.17}$$

pro všechna $n \in \mathbb{Z}$. Odtud plyne (4.15).

Předpokládejme nejprve, že $L_n(x_n, y_n) \neq 0$ pro všechna $n \in \mathbb{Z}$. Jelikož

$$\left| \frac{L_{n+1}(x_{n+1}, y_{n+1})}{L_n(x_n, y_n)} \right| = \theta_{n+1} > 2,$$

je $|L_n(x_n, y_n)| \overset{n\to-\infty}{\longrightarrow} 0$ a $|L_n(x_n, y_n)| \overset{n\to\infty}{\longrightarrow} \infty$. Tedy existuje právě jedno $n \in \mathbb{Z}$ takové, že

$$|L_{n-1}(x_{n-1}, y_{n-1})| < \frac{1}{\sqrt{128}} \leq |L_n(x_n, y_n)|\,. \tag{4.18}$$

Potom

$$|L_n(x_n, y_n)| = \theta_n\,|L_{n-1}(x_{n-1}, y_{n-1})| < \frac{\theta_n}{\sqrt{128}}.$$

Dále z (4.17) a (4.18)

$$\frac{|L'_n(x_n, y_n)|}{\sqrt{128}} \leq |L_n(x_n, y_n)L'_n(x_n, y_n)| \leq \frac{\theta_n - \theta'_n}{128},$$

odkud

$$|L'_n(x_n, y_n)| \leq \frac{\theta_n - \theta'_n}{\sqrt{128}}.$$

Stačí tedy volit $x = x_n$, $y = y_n$ a nerovnosti (4.13), (4.14) a (4.15) jsou splněny.

Nechť $L_n(x_n, y_n) = 0$ pro nějaké $n \in \mathbb{Z}$. Potom z (4.16) plyne $L_n(x_n, y_n) = 0$ pro všechna $n \in \mathbb{Z}$, tedy nerovnosti (4.13) a (4.15) jsou triviálně splněny pro všechna $n \in \mathbb{Z}$. Dále víme, že

$$\left|L'_{n+1}(x_{n+1}, y_{n+1})\right| = \left|\theta'_{n+1}L'_n(x_n, y_n)\right|$$

a $\left|\theta'_{n+1}\right| \leq 0{,}618\ldots$, odkud $|L'_n(x_n, y_n)| \overset{n\to\infty}{\longrightarrow} 0$. Existuje tedy $k \in \mathbb{N}$ takové, že nerovnost (4.14) platí pro všechna $n > k$, stačí položit $x = x_n$ a $y = y_n$.

□

Lemma 27. *Pokud čísla x,$y \in \mathbb{Z}$ splňují nerovnosti (4.13) a (4.14), potom $y = 0$.*

Důkaz. Z trojúhelníkové nerovnosti je

$$|(x + \theta_n y + \beta_n) - (x + \theta'_n y + \beta'_n)| \leq |x + \theta_n y + \beta_n| + |x + \theta'_n y + \beta'_n|\,,$$

sečtením (4.13) a (4.14) pak dostáváme

$$|(\theta_n - \theta'_n)y + \beta_n - \beta'_n| \leq \frac{2\theta_n - \theta'_n}{\sqrt{128}}. \tag{4.19}$$

Je-li $y \geq 1$, plyne odtud

$$\theta_n - \theta'_n + \beta_n - \beta'_n \leq \frac{2\theta_n - \theta'_n}{\sqrt{128}}.$$

Z Důsledku Lemmatu 22 plyne $\beta_n \geq v_n - \frac{3}{4}$ a z Lemmatu 23 máme $\beta'_n \leq \frac{1}{2}$. Odtud

$$\theta_n - \theta'_n + v_n - \frac{5}{4} \leq \frac{2\theta_n - \theta'_n}{\sqrt{128}},$$

$$\left(1 - \frac{2}{\sqrt{128}}\right)\theta_n \leq \left(1 - \frac{1}{\sqrt{128}}\right)\theta'_n - v_n + \frac{5}{4} \leq \left(1 - \frac{1}{\sqrt{128}}\right)\frac{3 - \sqrt{5}}{2} - 1 + \frac{5}{4},$$

$$\theta_n < 0{,}727\ldots,$$

což je spor, neboť máme $\theta_n > 2$.

Pokud $y \leq -2$, z (4.19) plyne

$$2(\theta_n - \theta'_n) - (\beta_n - \beta'_n) \leq \frac{2\theta_n - \theta'_n}{\sqrt{128}}.$$

Podle Lemmatu 22 je $\beta_n \leq \frac{3}{4}$ a víme $\beta'_n > 0$, a tedy

$$\frac{5}{4}\theta_n - 2\theta'_n < \frac{2\theta_n - \theta'_n}{\sqrt{128}},$$

neboli

$$\left(\frac{5}{4} - \frac{2}{\sqrt{128}}\right)\theta_n < \left(2 - \frac{1}{\sqrt{128}}\right)\theta'_n < \left(2 - \frac{1}{\sqrt{128}}\right)\frac{3-\sqrt{5}}{2},$$

$$\theta_n < 0{,}680\ldots,$$

což je opět spor.

Nakonec pro $y = -1$ mají (4.17) a (4.18) tvar

$$|x - \theta_n + \beta_n| \leq \frac{\theta_n}{\sqrt{128}},$$

$$|x - \theta'_n + \beta'_n| \leq \frac{\theta_n - \theta'_n}{\sqrt{128}}.$$

Odtud a z Lemmatu 22 máme

$$x \geq \left(1 - \frac{1}{\sqrt{128}}\right)\theta_n - \beta_n \geq \left(\frac{1}{4} - \frac{1}{\sqrt{128}}\right)\theta_n. \tag{4.20}$$

Podobně je

$$x \leq \frac{\theta_n}{\sqrt{128}} + \left(1 - \frac{1}{\sqrt{128}}\right)\theta'_n - \beta'_n < \frac{\theta_n}{\sqrt{128}} + \left(1 - \frac{1}{\sqrt{128}}\right)\frac{3-\sqrt{5}}{2}. \tag{4.21}$$

Celkem tak

$$\left(\frac{1}{4} - \frac{1}{\sqrt{128}}\right)\theta_n < \frac{\theta_n}{\sqrt{128}} + \left(1 - \frac{1}{\sqrt{128}}\right)\frac{3-\sqrt{5}}{2},$$

$$\left(\frac{1}{4} - \frac{2}{\sqrt{128}}\right)\theta_n < \left(1 - \frac{1}{\sqrt{128}}\right)\frac{3-\sqrt{5}}{2},$$

tedy jistě $\theta < 5$. Ale z (4.21) máme nyní

$$x < \frac{5}{\sqrt{128}} + \left(1 - \frac{1}{\sqrt{128}}\right)\frac{3-\sqrt{5}}{2} < 1$$

a současně z (4.20) zřejmě plyne $x > 0$, tedy pro $y = -1$ neexistuje žádné vhodné $x \in \mathbb{Z}$.

□

Lemma 28. *Nerovnosti (4.13), (4.14) a (4.15) nemají řešení pro $y = 0$.*

Důkaz. Pro $y = 0$ mají nerovnosti (4.13) a (4.14) tvar

$$|x + \beta_n| \leq \frac{\theta_n}{\sqrt{128}}, \tag{4.22}$$

$$|x + \beta'_n| \leq \frac{\theta_n - \theta'_n}{\sqrt{128}}, \tag{4.23}$$

tedy (s použitím trojúhelníkové nerovnosti podobně jako v důkazu předchozího lemmatu)

$$\beta_n - \beta'_n \leq \frac{2\theta_n - \theta'_n}{\sqrt{128}}.$$

Z Důsledku za Lemmatem 22 a z Lemmatu 23 pak máme

$$v_n - \frac{3}{4} - \frac{1}{2} \leq \frac{2\theta_n - \theta'_n}{\sqrt{128}},$$

dále

$$v_n \geq \frac{\theta_n}{2} - 1,$$

tedy

$$\frac{\theta_n}{2} - \frac{9}{4} \leq \frac{2\theta_n - \theta'_n}{\sqrt{128}},$$

$$\left(\frac{1}{2} - \frac{2}{\sqrt{128}}\right)\theta_n \leq \frac{9}{4} - \frac{\theta'_n}{\sqrt{128}} \leq \frac{9}{4} - \frac{1}{\sqrt{128}}\frac{1-\sqrt{5}}{2},$$

$$\theta_n < 7{,}14.$$

Z (4.22) nyní dostáváme

$$x \leq -\beta_n + \frac{\theta_n}{\sqrt{128}} \leq -v_n + \frac{3}{4} + \frac{7{,}14}{\sqrt{128}} < 1$$

a z (4.23) je

$$x \geq -\beta'_n - \frac{\theta_n - \theta'_n}{\sqrt{128}} > -\frac{1}{2} - \frac{7{,}14 + 0{,}618\ldots}{\sqrt{128}} > -2.$$

Je-li $x = 0$, dává nám nerovnost (4.15) vztah

$$\beta_n \beta'_n \leq \frac{\theta_n - \theta'_n}{\sqrt{128}},$$

což je spor s Lemmatem 24.

Zbývá pouze možnost $x = -1$. Potom z (4.23) a z Lemmatu 23 plyne

$$\theta_n - \theta'_n \geq \frac{\sqrt{128}}{2},$$

tedy

$$\theta_n \geq \frac{\sqrt{128}}{2} + \frac{1-\sqrt{5}}{2} > 5.$$

Potom $v_n \geq 2$. Celkem

$$|(x+\beta_n)(x+\beta'_n)| = (\beta_n - 1)(1-\beta'_n) \geq \left(v_n - \frac{3}{4} - 1\right)\frac{1}{2} =$$

$$= \frac{v_n}{16} > \frac{1}{16}\left(\frac{\theta_n}{2} - 1\right) > \frac{1}{16}\left(\frac{\theta_n}{2} - \frac{\theta_n}{5}\right) = \frac{3\theta_n}{160},$$

kde používáme po řadě nerovnosti $\beta_n \geq v_n - \frac{3}{4}$, $v_n \geq 2$, $v_n > \frac{\theta_n}{2} - 1$ a $\theta_n > 5$. Spolu s (4.23) dostáváme

$$\frac{\theta_n - \theta'_n}{\sqrt{128}} > \frac{3\theta_n}{160},$$

což po úpravách dává

$$\theta_n < -\frac{5}{7}\theta'_n < \frac{5}{7}0{,}618\ldots < 1.$$

To je ale spor s $\theta_n > 5$.

□

Tímto jsme dokázali Větu 25.

4.3 Formy s celočíselnými koeficienty

Věta 29. *Nechť $f(x,y) = ax^2+bxy+cy^2$ je indefinitní binární kvadratická forma s koeficienty $a, b, c \in \mathbb{Z}$, jejíž diskriminant δ není druhou mocninou přirozeného čísla. Potom existují $p, q \in \mathbb{Q}$ taková, že*

$$|f(x+p, y+q)| > \frac{1}{128}\sqrt{\delta}$$

platí pro všechna $x, y \in \mathbb{Z}$.

Použijeme-li Větu 25, stačí nám ukázat, že pro formy s celočíselnými exponenty jsou čísla p_0, q_0 z důkazu této věty racionální. K tomu však potřebujeme nejprve ukázat, že posloupnosti $\{\mu_n\}, \{t_n\}, \{\theta_n\}, \{\theta'_n\}$ zavedené v sekci 4.2 jsou v tomto případě periodické.

Lemma 30. *Jestliže má forma $f_0(x,y)$ celočíselné koeficienty a její diskriminant není druhou mocninou přirozeného čísla, potom existuje $N \in \mathbb{N}$ takové, že*

$$\theta_{n+N} = \theta_n, \quad \theta'_{n+N} = \theta'_n, \quad \mu_{n+N} = \mu_n, \quad t_{n+N} = t_n$$

pro všechna $n \in \mathbb{Z}$.

Důkaz. Pro formy $f_n(x,y)$ z Lemmatu 21 označme $f_n(x,y) = a_n x^2 + b_n xy + c_n y^2$. Podle Lemmatu 18 mají všechny tyto formy stejný diskriminant δ. Potom

$$|a_n| = \frac{\sqrt{\delta}}{\theta_n - \theta'_n} < \frac{\sqrt{\delta}}{2 - 0{,}382\ldots}$$

pro všechna $n \in \mathbb{Z}$, tedy posloupnost $\{a_n\}$ je omezená. Dále z rekurentního vztahu $f_n(x,y) = f_{n+1}(y, \mu_{n+1}(x + t_n y))$ máme

$$a_n = f_n(1,0) = f_{n+1}(0, \pm 1) = c_{n+1},$$

odkud plyne, že posloupnost $\{b_n\}$ je rovněž omezená. Potom ale musí být omezená i posloupnost $\{b_n\}$, neboť $b_n^2 - 4a_n c_n = \delta$. Připomeňme, že $a_n, b_n, c_n \in \mathbb{Z}$, tedy nutně existují čísla $k \in \mathbb{Z}$ a $N \in \mathbb{N}$ taková, že

$$a_k = a_{k+N}, \quad b_k = b_{k+N}, \quad c_k = c_{k+N},$$

z čehož plyne

$$\theta_k = \theta_{k+N}, \quad \theta'_k = \theta'_{k+N}.$$

Jelikož jsou posloupnosti $\{\theta_n\}$ a $\{\theta'_n\}$ definovány rekurentními vztahy, dostáváme

$$\theta_0 = \theta_N, \quad \theta'_0 = \theta'_N,$$

odkud již plyne $\theta_{n+N} = \theta_n$, $\theta'_{n+N} = \theta'_n$, $\mu_{n+N} = \mu_n$ a $t_{n+N} = t_n$ pro všechna $n \in \mathbb{Z}$.

□

Lemma 31. *Nechť má forma $f_0(x,y)$ celočíselné koeficienty a nechť její diskriminant není druhou mocninou přirozeného čísla. Potom čísla β_0, β'_0 definovaná v (4.5) a (4.6) lze zapsat ve tvaru*

$$\beta_0 = p_0 + \theta_0 q_0, \quad \beta'_0 = p_0 + \theta'_0 q_0,$$

kde $p_0, q_0 \in \mathbb{Q}$.

Důkaz. Buď D největší bezčtvercový dělitel diskriminantu formy $f_0(x,y)$. Podle předpokladu jsou θ_0, θ'_0 iracionální. Navíc to jsou kořeny monického polynomu s racionálními koeficienty, totiž polynomu $\frac{1}{a_0} f_0(x,-1) = (x - \theta_0)(x - \theta'_0)$. Jelikož obor $\mathbb{Q}[x]$ je Gaussův, je tento polynom ireducibilní, a tedy je to minimální polynom prvků θ_0 a θ'_0. Proto jsou θ_0, θ'_0 konjugované v $\mathbb{Q}(\sqrt{D})$. Potom z rekurentních vyjádření v Lemmatu 21 plyne, že také θ_n a θ'_n jsou (jakožto iracionální kořeny monického polynomu $\frac{1}{a_n} f_n(x,-1)$) konjugované v $\mathbb{Q}(\sqrt{D})$. Jelikož je podle definice $v_n = \left\lfloor \frac{1}{2}\theta_n \right\rfloor$ plyne z předchozího Lemmatu $v_n = v_{n+N}$ pro každé $n \in \mathbb{Z}$. Z (4.5) a (4.6) pak plyne

$$\begin{aligned}
\beta_0 &= \left(v_0 + \frac{\mu_1}{\theta_1} v_1 + \cdots + \frac{\mu_1 \cdots \mu_{N-1}}{\theta_1 \cdots \theta_{N-1}} v_{N-1} \right) \cdot \\
&\qquad \cdot \left(1 + \frac{\mu_1 \cdots \mu_N}{\theta_1 \cdots \theta_N} + \left(\frac{\mu_1 \cdots \mu_N}{\theta_1 \cdots \theta_N} \right)^2 + \cdots \right) = \\
&= \left(v_0 + \frac{\mu_1}{\theta_1} v_1 + \cdots + \frac{\mu_1 \cdots \mu_{N-1}}{\theta_1 \cdots \theta_{N-1}} v_{N-1} \right) \left(1 - \frac{\mu_1 \cdots \mu_N}{\theta_1 \cdots \theta_N} \right)^{-1},
\end{aligned}$$

$$\beta_0' = \left(\frac{v_{-1}}{\phi_0} - \frac{v_{-2}}{\phi_0\phi_{-1}} + \cdots + \frac{(-1)^{N-1}v_{-N}}{\phi_0\phi_{-1}\cdots\phi_{-N+1}}\right) \cdot$$

$$\cdot \left(1 + \frac{(-1)^N}{\phi_{-1}\cdots\phi_{-N}} + \left(\frac{(-1)^N}{\phi_{-1}\cdots\phi_{-N}}\right)^2 + \cdots\right)$$

$$= \left(\frac{v_{-1}}{\phi_0} - \frac{v_{-2}}{\phi_0\phi_{-1}} + \cdots + \frac{(-1)^{N-1}v_{-N}}{\phi_0\phi_{-1}\cdots\phi_{-N+1}}\right)\left(1 - \frac{(-1)^N}{\phi_{-1}\cdots\phi_{-N}}\right)^{-1}.$$

Z těchto vyjádření již vidíme, že $\beta_0, \beta_0' \in \mathbb{Q}(\sqrt{D})$. Nyní stačí dokázat, že β_0 a β_0' jsou konjugované v $\mathbb{Q}(\sqrt{D})$, neboť je-li

$$\theta_0 = r + s\sqrt{D}, \quad \theta_0' = r - s\sqrt{D},$$

$$\beta_0 = i + j\sqrt{D}, \quad \beta_0' = i - j\sqrt{D},$$

pro $i, j, r, s \in \mathbb{Q}$, pak jsou čísla $p_0 = i - \frac{jr}{s}$ a $q_0 = \frac{j}{s}$ racionální a splňují požadovaný vztah $\beta_0 = p_0 + \theta_0 q_0$, $\beta_0' = p_0 + \theta_0' q_0$.

Abychom ukázali, že prvky β_0 a β_0' jsou konjugované, nahradíme ve vyjádření β_0 všechna θ_k za θ_k'. Tímto pro β_0 tvaru $i + j\sqrt{D}$ dostaneme právě prvek $i - j\sqrt{D}$, který je konjugovaný k β_0. Využijeme-li vztah (4.3), dostaneme

$$\frac{v_0 - v_1\phi_1 + v_2\phi_1\phi_2 - \cdots + (-1)^{N-1}v_{N-1}\phi_1\phi_2\cdots\phi_{N-1}}{1 - (-1)^{N-1}\phi_1\phi_2\cdots\phi_{N-1}} =$$

$$= \frac{v_0 - v_1\phi_1 + v_2\phi_1\phi_2 - \cdots + (-1)^{N-1}v_{N-1}\phi_1\phi_2\cdots\phi_{N-1}}{1 - (-1)^{N-1}\phi_1\phi_2\cdots\phi_{N-1}} \cdot \frac{(-1)^{N-1}\phi_1\phi_2\cdots\phi_N}{(-1)^{N-1}\phi_1\phi_2\cdots\phi_N} =$$

$$= \frac{\frac{(-1)^{N-1}v_0}{\phi_N\phi_{N-1}\cdots\phi_1} + \cdots - \frac{v_{N-2}}{\phi_N\phi_{N-1}} + \frac{v_{N-1}}{\phi_N}}{\frac{1}{(-1)^{N-1}\phi_1\phi_2\cdots\phi_N} - (-1)} = \frac{\frac{v_{N-1}}{\phi_N} - \frac{v_{N-2}}{\phi_N\phi_{N-1}} + \cdots + \frac{(-1)^{N-1}v_0}{\phi_N\phi_{N-1}\cdots\phi_1}}{1 - \frac{(-1)^N}{\phi_1\phi_2\cdots\phi_N}} = \beta_0',$$

přičemž v poslední rovnosti využíváme periodičnosti ϕ_k a v_k.

□

Nyní je důkaz Věty 29 hotov.

4.4 Důsledek pro reálná kvadratická rozšíření

V tuto chvíli již máme vše připraveno k důkazu stěžejní věty celé kapitoly. Připomeňme, že značíme $\mathbf{K} = \mathbb{Q}(\sqrt{D})$ a $\mathbf{R_K}$ je okruh všech celých algebraických čísel z $\mathbf{K}$.

Věta 32. *Pro $D > 128^2$ není těleso $\mathbb{Q}(\sqrt{D})$ normově-euklidovské.*

Důkaz. Podle Lemmatu 13 je těleso $\mathbb{Q}(\sqrt{D})$ normově-euklidovské právě tehdy, když pro každé $\xi \in \mathbb{Q}(\sqrt{D})$ existuje $t \in \mathbf{R_K}$ takové, že

$$\left|N_{K/\mathbb{Q}}(\xi - t)\right| < 1 \tag{4.24}$$

a víme, že $N_{K/\mathbb{Q}}(\xi - t) = (\xi - t)(\xi - t)' = (\xi - t)(\xi' - t')$, kde čárka značí konjugaci. Z Věty 10 plyne, že prvky $\mathbf{R_K}$ jsou tvaru $x + \theta y$, kde $x, y \in \mathbb{Z}$ a

$$\theta = \begin{cases} \sqrt{D}, \text{ pokud } D \not\equiv 1 \pmod 4, \\ \frac{1+\sqrt{D}}{2}, \text{ pokud } D \equiv 1 \pmod 4. \end{cases}$$

Dále víme

$$\theta' = \begin{cases} -\sqrt{D}, \text{ pokud } D \not\equiv 1 \pmod 4, \\ \frac{1-\sqrt{D}}{2}, \text{ pokud } D \equiv 1 \pmod 4, \end{cases}$$

Označme $\xi = p + \theta q$, $p, q \in \mathbb{Q}$, a $t = -x - \theta y$, $x, y \in \mathbb{Z}$. Potom $\xi' = p + \theta' q$ a $t' = -x - \theta' y$, nerovnost (4.24) je tedy ekvivalentní s nerovností

$$|(x + \theta y + p + \theta q)(x + \theta' y + p + \theta' q)| < 1. \tag{4.25}$$

Dále platí

$$(x + \theta y + p + \theta q)(x + \theta' y + p + \theta' q) =$$

$$= \begin{cases} (x+p)^2 - D(y+q)^2, \text{ pokud } D \not\equiv 1 \pmod 4, \\ (x+p)^2 + (x+p)(y+q) + \frac{1-D}{4}(y+q)^2, \text{ pokud } D \equiv 1 \pmod 4. \end{cases}$$

Označme proto

$$f(x, y) = \begin{cases} x^2 - Dy^2, \text{ pokud } D \not\equiv 1 (\text{mod } 4), \\ x^2 + xy + \frac{1-D}{4} y^2, \text{ pokud } D \equiv 1 (\text{mod } 4), \end{cases}$$

diskriminant δ této binární kvadratické formy je roven $4D$, resp. D. Potom je podmínka (4.25) ekvivalentní s

$$|f(x + p, y + q)| < 1. \tag{4.26}$$

Z Věty 29 ale víme, že existují $p, q \in \mathbb{Q}$ taková, že

$$|f(x + p, y + q)| > \frac{1}{128}\sqrt{\delta}$$

pro všechna $x, y \in \mathbb{Z}$, odkud pro $\delta > 128^2$ dostáváme

$$|f(x + p, y + q)| > 1,$$

což je spor s podmínkou (4.26).

□

Poznámka. Z důkazu vidíme, že v případě $D \not\equiv 1 (\text{mod } 4)$ platí dokonce silnější tvrzení: Těleso $\mathbb{Q}(\sqrt{D})$ není normově-euklidovské pro $\delta = 4D > 128^2$, tedy pro $D > 64^2$.

Kapitola 5

Reálná kvadratická rozšíření III

V poslední kapitole této práce dokončíme charakterizaci reálných kvadratických rozšíření tělesa racionálních čísel. Případ $D \not\equiv 1 \pmod 4$ rozebereme podrobně, pro $D \equiv 1 \pmod 4$ již jen shrneme výsledky jiných autorů.

5.1 Euklidův obor

Tvrzení 33. *V každém Euklidově oboru jsou všechny ideály hlavní.*

Důkaz. Buď $\mathbf{R}$ Euklidův obor s normou ν a $\mathbf{I}$ ideál v $\mathbf{R}$. Zvolme $b \in \mathbf{I} \setminus \{0\}$ tak, že $\nu(b)$ je nejmenší možné. Potom pro libovolné $a \in \mathbf{I}$ existuje $q \in \mathbf{I}$ takové, že $\nu(a + bq) < \nu(b)$. Odtud ale plyne $\nu(a + bq) = 0$, a tedy $a + bq = 0$, což implikuje $b|a$. Jelikož jsme však volili a libovolně, dostáváme $\mathbf{I} = b\mathbf{R}$.

□

Nyní uvedeme bez důkazu spíše pro zajímavost tvrzení, které společne s Tvrzením 33 omezuje možná $D > 0$ taková, že těleso $\mathbb{Q}(\sqrt{D})$ je normově-euklidovské. Tvrzení lze najít i s důkazem v BEHRBOHM a RÉDEI (1936).

Tvrzení 34. *Je-li $\mathbb{Q}(\sqrt{D})$ obor integrity hlavních ideálů, pak mohou nastat jen následující případy:*

I. $D = p \equiv 1 \pmod 4$,

II. $D = pq \equiv 1 \pmod 4$, $p \equiv q \equiv 3 \pmod 4$,

III. $D = 2$ *nebo* $D = 2p$, $p \equiv 3 \pmod 4$

IV. $D = p \equiv 3 \pmod 4$,

kde p, q značí kladná prvočísla.

5.2 Jednodušší případ

V této sekci využijeme některé pojmy z kapitoly 3 a popíšeme situaci pro $D \not\equiv 1 \pmod 4$, čímž vyřešíme případy III. a IV. z Tvrzení 34. Samotný důkaz

však bude odlišný od důkazů uvedených v kapitole 3, místo geometrickým náhledem a hyperbolami se budeme zabývat řešením diofantických rovnic, respektive dokazováním, že žádné řešení neexistuje.

Připomeňme, že v kapitole 2 jsme si popsali, jak v případě $D \not\equiv 1 \pmod 4$ vypadají všechna celá algebraická čísla v tělese $\mathbb{Q}(\sqrt{D})$. Jsou to právě čísla tvaru $a+b\sqrt{D}$, $a, b \in \mathbb{Z}$. Nyní pro tento případ ukážeme, že jsme v kapitole 3 skutečně nalezli všechna kvadratická rozšíření tělesa $\mathbb{Q}$. Tento důkaz lze najít také v článku EGGLETON a kol. (1992).

Věta 35. *Jestliže je D bezčtvercové kladné celé číslo takové, že $D \not\equiv 1 \pmod 4$ a $D \notin \{2, 3, 6, 7, 11, 19\}$, pak těleso $\mathbb{Q}(\sqrt{D})$ není normově-euklidovské.*

Důkaz. Použijeme značení z kapitoly 3 a ukážeme, že pro D splňující podmínky věty některý z bodů $\left(\frac{1}{2}, \frac{1}{2}\right)$ a $\left(0, \frac{t}{D}\right)$, kde $t \in \mathbb{N}$, neleží v jednotkovém okolí $U(a, b)$ pro žádná $a, b \in \mathbb{Z}$, a tedy $\mathbb{Q}(\sqrt{D})$ nemůže být normově-euklidovské.

Předpokládejme, že $\left(0, \frac{t}{D}\right) \in U(a, b)$. Potom

$$\left|(0-a)^2 - \left(\frac{t}{D} - b\right)^2 D\right| < 1,$$

neboli

$$\left|a^2 D - (t - Db)^2\right| < D. \tag{5.1}$$

Označíme-li $z = t - Db$, potom máme

$$\left|z^2 - Da^2\right| < D.$$

Navíc platí

$$z^2 - Da^2 = t^2 - 2Dtb + D^2b^2 - Da^2 \equiv t^2 \pmod D,$$

a tedy pro pevné t může výraz $z^2 - Da^2$ nabývat pouze dvou různých hodnot.

1. případ: $D \equiv 2 \pmod 4$.

Nejprve předpokládejme, že existuje liché $t \in \mathbb{N}$ takové, že $2D < t^2 < 3D$. Potom $z^2 - Da^2 = t^2 - mD$, kde $m = 2$, nebo $m = 3$. Odtud pak $z^2 - t^2 = D(a^2 - m)$. Z předpokladu $D \equiv 2 \pmod 4$ plyne $D \equiv 2$, nebo $6 \pmod 8$, přičemž kvadratické zbytky modulo 8 jsou 0, 1 a 4,[1] tedy $a^2 \equiv 0, 1$, nebo $4 \pmod 8$. Rozebráním jednotlivých možností pak dostaneme, že $D(a^2 - m) \equiv 2, 4$, nebo $6 \pmod 8$. Současně je ale podle předpokladu t liché, odkud plyne $t^2 \equiv 1 \pmod 8$, celkem tedy $z^2 - t^2 \equiv 0, 3, 7 \pmod 8$. Potom rovnice $z^2 - t^2 = D(a^2 - m)$ nemá pro a a z řešení, odkud již plyne, že $\left(0, \frac{t}{D}\right)$ neleží v žádném jednotkovém okolí $U(a, b)$.

Jestliže neexistuje žádné liché t takové, že $2D < t^2 < 3D$, pak nutně platí $(2k-1)^2 < 2D < 3D \leq (2k+1)^2$ pro nějaké $k \in \mathbb{N}$. Odtud dostaneme nerovnost $3(2k-1)^2 < 2(2k+1)^2$, což dává po úpravě $(2k-5)^2 < 24$. Poslední nerovnost však zřejmě neplatí pro $k \geq 5$. Z $3D > 2D \geq (2k-1)^2 \geq (2 \cdot 5 - 1)^2 = 9^2$ pak plyne $D > 27$ a pro tato D již tedy vždy najdeme vhodné liché t. Dále platí $2 \cdot 10 < 5^2 < 3 \cdot 10$, tedy pro $D = 10$ lze volit $t = 5$, a $2 \cdot 22 < 7^2 < 3 \cdot 22$, tudíž pro $D = 22$ stačí položit $t = 7$.

[1] Kvadratickými zbytky modulo p rozumíme čísla $m^2 \mod p$ kde $m \in \mathbb{Z}$.

Pro $D = 26$ buď $t = 39$, potom máme splněnou nerovnost $58D < t^2 < 59D$ a výše uvedený argument stačí jen lehce poupravit. Nyní máme rovnici $z^2 - t^2 = D(a^2 - m)$ s $m = 58$, nebo $m = 59$, a tedy $m \equiv 2$, nebo $3 \pmod 8$. Stejně jako výše pak $D(a^2 - m) \equiv 2, 4$, nebo $6 \pmod 8$ a současně $z^2 - t^2 \equiv 0, 3, 7 \pmod 8$. Odtud plyne, že rovnice $z^2 - t^2 = D(a^2 - m)$ nemá pro a a z řešení, a tedy $\left(0, \frac{39}{26}\right)$ neleží v žádném jednotkovém okolí $U(a, b)$.

Nakonec pro $D = 14$ uvažme bod $\left(\frac{1}{2}, \frac{1}{2}\right)$, potom předpoklad $\left(\frac{1}{2}, \frac{1}{2}\right) \in U(a, b)$ implikuje platnost nerovnosti $|(2a-1)^2 - 14(2b-1)^2| < 4$. Jelikož však platí $(2a-1)^2 - 14(2b-1)^2 \equiv 4a^2 - 4a + 1 + 2(4b^2 - 4b + 1) \equiv 4a(a+1) + 3 \equiv 3 \pmod 8$, musí již nutně nastat $(2a-1)^2 - 14(2b-1)^2 = 3$. Avšak $(2a-1)^2 \equiv 3 \pmod 7$ a kvadratické zbytky modulo 7 jsou 0, 1, 2 a 4, rovnice $(2a-1)^2 - 14(2b-1)^2 = 3$ tedy nemá řešení. Tím jsme rozebrali všechny možnosti pro bezčtvercová čísla $D \equiv 2 \pmod 4$.

2. případ: $D \equiv 3 \pmod 4$.

Podívejme se na nerovnost $(2k-1)^2 < 5D < 6D \leq (2k+1)^2$. Ta je ekvivalentní s nerovností $(2k-11)^2 < 120$, která zřejmě neplatí pro $k \geq 11$. Potom máme $6D > 5D > (2k-1)^2 \geq (2 \cdot 11 - 1)^2 = 441$ a odtud dostáváme, že pro všechna $D \geq 74$ existuje liché t splňující $5D < t^2 \leq 6D$. Také pro $D = 15, 23, 31, 39, 43, 51, 55, 67$ a 71 lze nalézt vhodná lichá t s touto vlastností. Podobně jako v předchozím případě se proto nyní podívejme na rovnici $z^2 - t^2 = D(a^2 - m)$, kde tentokrát $m = 5$, nebo $m = 6$. Opět víme, že $z^2 - t^2 \equiv 0, 3, 7 \pmod 8$ a rozborem jednotlivých možností snadno zjistíme, že $D(a^2 - m) \equiv 1, 2, 4, 5, 6 \pmod 8$, tedy uvedená rovnice nemá v proměnných a a z řešení. Zbývá vyřešit již jen možnosti $D = 35, 47$ a 59.

Pro $D = 47$ položme $t = 25$, potom $13D < t^2 < 14D$ a zaměříme se na rovnici $z^2 - t^2 = D(a^2 - m)$, kde $m = 13$, nebo $m = 14$. Levá strana opět dává po dělení 8 zbytky 0, 3, 7, na pravé straně pak dostáváme zbytky 1, 2, 4, 5 a 6, odkud plyne, že rovnice nemá řešení, a tedy bod $\left(0, \frac{25}{47}\right)$ neleží v žádném jednotkovém okolí.

Jestliže $D = 59$, stačí volit $t = 47$, neboť pak máme $37D < t^2 < 38D$ a opět stejnou úvahou ověříme, že rovnice $z^2 - t^2 = D(a^2 - m)$ nemá pro $m = 37$ ani pro $m = 38$ žádné řešení, odkud plyne $\left(0, \frac{47}{59}\right) \notin U(a, b)$ pro všechna $a, b \in \mathbb{Z}$.

Nakonec buď $D = 35$ a předpokládejme, že $\left(\frac{1}{2}, \frac{1}{2}\right) \in U(a, b)$ pro nějaká $a, b \in \mathbb{Z}$. Potom musí platit nerovnost $|(2a-1)^2 - 35(2b-1)^2| < 4$ a jelikož $(2a-1)^2 - 35(2b-1)^2 \equiv 4a(a-1) + 5 \cdot 4b(b-1) + 6 \equiv 6 \pmod 8$, platí $(2a-1)^2 - 35(2b-1)^2 = -2$. Podíváme-li se na tuto rovnost modulo 5, dostaneme $(2a-1)^2 \equiv 3 \pmod 5$, což je ovšem spor, neboť 3 není kvadratický zbytek modulo 5.

□

5.3 Obtížnější případ

Důkaz neexistence reálných normově-euklidovských těles $\mathbb{Q}(\sqrt{D})$ jiných než pro $D \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$ vyžaduje v případě $D \equiv 1 \pmod 4$ větší úsilí než v případě $D \not\equiv 1 \pmod 4$. Souvisí to především

s tvarem celých algebraických čísel v tělese $\mathbb{Q}(\sqrt{D})$, neboť nyní máme

$$\mathbf{R_K} = \left\{ \frac{a+b\sqrt{D}}{2} \mid a,b \in \mathbb{Z}, a \equiv b \pmod 2 \right\},$$

proto podmínka analogická (5.1) by zde měla tvar: Jestliže $(x,y) \in U\left(\frac{a}{2},\frac{b}{2}\right)$, kde $x,y \in \mathbb{Q}(\sqrt{D})$ a $a,b \in \mathbb{Z}$, $a \equiv b \pmod 2$, pak

$$\left|(2x-a)^2 - D(2y-b)^2\right| < 4.$$

Ani jedna z voleb $(x,y) = \left(0,\frac{t}{D}\right)$ a $(x,y) = \left(\frac{1}{2},\frac{1}{4}\right)$ zde nevede k přímočarému sporu, jako tomu bylo v případě $D \not\equiv 1 \pmod 4$, problémy nám činí právě číslo 4 na pravé straně nerovnosti. Pomůžeme si proto rozdělením problému na jemnější případy. Nejprve však uveďme větu, která hned v několika případech usnadňuje práci. Její důkaz lze nalézt například v ERDÖS a KO (1938).

Věta 36. *Nechť p je prvočíslo tvaru $4n+1$. Potom těleso $\mathbb{Q}(\sqrt{p})$ není normově-euklidovské, jestliže p lze zapsat ve tvaru*

$$p = q_1 m_1 + q_2 m_2,$$

kde $m_1, m_2, q_1, q_2 > 0$ nejsou kvadratické zbytky modulo p, q_1, q_2 jsou lichá prvočísla a m_i není dělitelné lichou mocninou čísla p_i pro $i = 1,2$.

- H. Chatland (CHATLAND (1949)), neznaje starších výsledků K. Inkeriho (INKERI (1947)), vyřešil případ $D \equiv 1 \pmod{24}$ s výjimkou možností 193, 241, 313, 337 a 457.
- Pro $D \equiv 5 \pmod{24}$ lze najít poměrně přímočarý důkaz v článku BEHR-BOHM a RÉDEI (1936).
- Případem $D \equiv 9 \pmod{24}$ se ve své práci zabýval L. Schuster (SCHUSTER (1938)).
- Za pomoci Věty 36 vyřešili P. Erdös a Chao Ko (ERDÖS a KO (1938)) případ $D \equiv 13 \pmod{24}$ pro velká D. Jejich práci později vylepšil A. Brauer (BRAUER (1940)), zbývající možnosti $D = 61$ a $D = 109$ doplnil L. Rédei (RÉDEI (1942)).
- L. Rédei (RÉDEI (1942)) se také vypořádal s případem $D \equiv 17 \pmod{24}$.
- Možnost $D \equiv 21 \pmod{24}$ rozebral N. Hofreiter (HOFREITER (1935)).
- Nakonec K. Inkeri ve výše zmíněném článku INKERI (1947) ukázal, že všechna normově-euklidovská tělesa $\mathbb{Q}(\sqrt{D})$ splňující $\delta < 5000$ jsou již známá, kde stejně jako v důkazu Věty 32 značíme $\delta = D$, pokud $D \equiv 1 \pmod 4$, a $\delta = 4D$, pokud $D \not\equiv 1 \pmod 4$.

Tím jsou vyřešeny případy I. a II. z Tvrzení 34, a tedy i kompletně dokončena charakterizace normově-euklidovských kvadratických rozšíření tělesa racionálních čísel.

Závěr

Téma práce se ukázalo jako poměrně obsáhlé, myslím si však, že i přesto se z velké míry podařilo splnit cíl a podat ucelený popis všech normově-euklidovských kvadratických rozšíření tělesa racionálních čísel. Bohužel se nezdařilo zcela naplnit mou představu o zjednodušení a zkrácení důkazů, stále však vidím velký přínos práce ve sjednocení terminologie a značení. Jediný větší ústupek jsem byla nucena učinit v poslední kapitole, kde jsou namísto kompletního důkazu uvedeny pouze odkazy na jiné články a publikace, neboť podrobný rozbor by práci neúměrně prodloužil.

Dále se pak nabízí otázka, pro která D je okruh celých algebraických čísel tělesa $\mathbb{Q}(\sqrt{D})$ Euklidův s jinou než euklidovskou normou. Pokud je mi známo, není na rozdíl od normově-euklidovských kvadratických rozšíření dosud tento problém zcela vyřešen.

Literatura

BARNES, E. S. a SWINNERTON-DYER, H. P. F. (1952). The Inhomogeneous Minima of Binary Quadratic Forms I. *Acta Math.*, **87**, 259–323.

BEHRBOHM, H. a RÉDEI, L. (1936). Der Euklidische Algorithmus in quadratischen Körpern. *J. Reine Angew. Math.*, **4**(174), 192–205.

BRAUER, A. (1940). On the Non-Existence of the Euclidean Algorithm in Certain Quadratic Number Fields. *American Journal of Mathematics*, **62**(1), 697–716.

CHATLAND, H. (1949). On the Euclidean Algorithm in Quadratic Number Fields. *Bull. Amer. Math. Soc.*, **55**(10), 948–953.

DAVENPORT, H. (1951). Indefinite Binary Quadratic Forms, and Euclid's Algorithm in Real Quadratic Fields. *Proc. London Math. Soc.*, **53**(2), 65–82.

DRÁPAL, A. (2006). *Text k přednášce Komutativní okruhy.* Praha.

EGGLETON, R. B., LACAMPAGNE, C. B. a SELFRIDGE, J. L. (1992). Euclidean Quadratic Fields. *The American Mathematical Monthly*, **99**(9), 829–837.

ERDÖS, P. a KO, C. (1938). Note on the Euclidean Algorithm. *J. London Math. Soc.*, **13**, 3–8.

HOFREITER, N. (1935). Quadratische Zahlkörper mit und ohne Euklidischen Algorithmus. *Monatsh. Math. Phys.*, **42**, 397–400.

INKERI, K. (1947). Über den Euklidischen Algorithmus in quadratischen Zahlkörpern. *Ann. Acad. Sci. Fenn. Ser. A. I. Math.-Phys.*, (41), 1–35.

NARKIEWICZ, W. (2004). *Elementary and Analytic Theory of Algebraic Numbers.* Third Edition. Springer, Berlin. ISBN 3-540-21902-1.

RÉDEI, L. (1942). Zur Frage des Euklidischen Algorithmus in quadratischen Zahlkörpern. *Math. Ann.*, **118**, 588–608.

SCHUSTER, L. (1938). Reellquadratische Zahlkörper ohne Euklidischen Algorithmus. *Monatsh. Math. Phys.*, **47**, 117–127.

Seznam obrázků