

**MATEMATICKO-FYZIKÁLNÍ  
FAKULTA**  
Univerzita Karlova

## **BAKALÁŘSKÁ PRÁCE**

Bára Tížková

# **Univerzální kvadratické formy a odhady stop celistvých prvků**

Katedra algebry

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

Studijní program: Matematika

Studijní obor: Obecná matematika

Praha 2021

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

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

V Praze dne 25. 5. 2021

.....

Podpis autora

Chtěla bych poděkovat svému vedoucímu práce Mgr. Vítězslavu Kalovi, Ph.D. za ochotný a trpělivý přístup, cenné rady a věnovaný čas. Moc si toho vážím. Dále děkuji spolužáku Michalu Koškovi za užitečné připomínky.

Název práce: Univerzální kvadratické formy a odhady stop celistvých prvků

Autor: Bára Tížková

Katedra: Katedra algebry

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

Abstrakt: Cílem této práce je studovat počet proměnných univerzálních kvadratických forem v číselných tělesech. Konkrétně, uvádíme zde celý důkaz věty o existenci nekonečně mnoha totálně reálných kvadratických forem libovolného stupně  $2n$ , nad kterými je počet proměnných univerzálních kvadratických forem libovolně velký. Klíčovým krokem důkazu je odhad stopy celistvého prvku za pomoci jednoho ze Stieltjesových odhadů diskriminantu. Na tyto odhady se v práci více zaměřujeme a uvádíme nástroje pro jejich důkazy. Dále se v práci zabýváme elementárními odhady počtu celistvých prvků s omezenou stopou a uvádíme přehled potřebné teorie ke stopám a diskriminantům.

Klíčová slova: kvadratická forma, číselné těleso, stopa, diskriminant

Title: Universal quadratic forms and estimates of traces of algebraic integers

Author: Bára Tížková

Department: Department of Algebra

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

Abstract: The aim of this work is to study the number of variables of universal quadratic forms in number fields. In particular, we provide the whole proof of the following theorem: In each degree  $2n$ , there are infinitely many totally real number fields that require universal quadratic forms to have arbitrarily large rank. The key step in this proof is to estimate the trace of an algebraic integer using one of the Stieltjes's bounds of discriminant. We focus on these bounds and introduce tools for proving them. Furthermore, we deal with some elementary estimates of the number of algebraic integers whose trace is bounded and summarize the relevant theory of traces and discriminants.

Keywords: quadratic form, number field, trace, discriminant

# Obsah

Úvod	2
<b>1 Základní definice a fakta</b>	<b>4</b>
1.1 Tělesová rozšíření . . . . .	4
1.2 Číselné těleso, celistvé prvky . . . . .	5
1.3 Stopa, diskriminant prvku, diskriminant tělesa . . . . .	6
1.4 Univerzální kvadratické formy . . . . .	8
<b>2 Totálně kladné celistvé prvky s omezenou stopou</b>	<b>11</b>
2.1 Konečný počet pro daný stupeň . . . . .	11
2.2 Počet pro stupeň 2 . . . . .	12
2.3 Počet pro stupeň 3 . . . . .	13
<b>3 Stieltjesovy odhady diskriminantu</b>	<b>14</b>
3.1 Gegenbauerovy polynomy . . . . .	14
3.2 Stieltjesova věta o maximálním diskriminantu . . . . .	17
3.3 Další Stieltjesovy věty . . . . .	22
3.4 Odhad stopy celistvého prvku . . . . .	23
<b>4 Univerzální formy v tělesech stupně <math>2n</math></b>	<b>25</b>
4.1 Permutační grupy . . . . .	25
4.2 Galoisovy grupy . . . . .	26
4.3 Důkaz hlavní věty . . . . .	28
4.4 Odhad diskriminantu z důkazu . . . . .	30
<b>Seznam použité literatury</b>	<b>32</b>

# Úvod

Studium univerzálních kvadratických forem započalo již v roce 1770 Lagrangeovou slavnou větou o čtyřech čtvercích, která říká, že každé přirozené číslo je součtem čtyř druhých mocnin. Nejprve byly univerzální kvadratické formy studovány nad celými čísly, což vedlo k několika pěkným výsledkům, jako například „věta 290“ [1] nebo „věta 15“ [2]. Lze je však studovat i nad jinými strukturami, konkrétně nad okruhem celistvých prvků číselných těles.

Předmětem našeho zájmu bude počet proměnných univerzálních kvadratických forem v číselných tělesech, přesněji, kolik nejméně proměnných mohou mít. Například pro  $\mathbb{Q}$  je nejmenší možný počet proměnných 4, protože univerzální kvadratické formy s celočíselnými koeficienty o 3 proměnných neexistují, avšak pro  $\mathbb{Q}(\sqrt{2})$ ,  $\mathbb{Q}(\sqrt{3})$  a  $\mathbb{Q}(\sqrt{5})$  je toto minimum 3 [3].

Vedoucí této práce Vítězslav Kala [4] dokázal, že pro libovolné přirozené  $M$  existuje nekonečně mnoho reálných kvadratických těles, ve kterých má každá univerzální kvadratická forma alespoň  $M$  proměnných. Na tento výsledek navázal obecnější větou, která už nehovoří pouze o kvadratických tělesech: pro libovolné přirozené  $M$  a  $d$  dělitelné 2 nebo 3 existuje nekonečně mnoho totálně reálných číselných těles stupně  $d$ , ve kterých má každá univerzální kvadratická forma alespoň  $M$  proměnných [5].

V této práci formálně sepíšeme důkaz obecnější věty pro  $d = 2n$  (věta 4.11, dále ji nazýváme *hlavní větou*). Budeme se v jistém smyslu opírat o platnost věty 1.28 pro kvadratická tělesa; při zobecňování ošetříme případy, které předtím nastat nemohly. Klíčovým krokem bude odhad stopy celistvého prvku, který odvodíme z jedné ze Stieltjesových vět o odhadu diskriminantu  $\prod_{i < j} (x_i - x_j)^2$  (věta 3.15). Důkaz jedné ze Stieltjesových vět zde také formálně rozepíšeme (věta 3.13). Dalším záměrem této práce je více se obeznámit s pojmem stopy, a to samostatným vypracováním odhadů počtu totálně kladných celistvých prvků s omezenou stopou.

V první kapitole představíme základní pojmy a poznatky z algebry a algebraické teorie čísel, zavedeme univerzální kvadratické formy.

Ve druhé kapitole zodpovíme otázky týkající se počtu celistvých prvků s omezenou stopou. Budeme se zabývat konečností počtu a konkrétními případy pro stupeň minimálního polynomu 2 a 3. Tato kapitola slouží pouze k přiblížení pojmu stopy celistvého prvku, k důkazu hlavní věty nebude potřebná. Důkazy vypracuje autorka samostatně s pomocí vedoucího práce.

Ve třetí kapitole se budeme zabývat odhadem diskriminantu  $\prod_{i < j} (x_i - x_j)^2$  na základě různých podmínek kladených na proměnné - tyto odhady jsou prezentovány ve třech Stieltjesových větách. Zadefinujeme si systémy ortogonálních polynomů, které se ve větách využívají, zaměříme se na jejich vlastnosti a samostatně dokážeme několik rekurentních vztahů. Dvě Stieltjesovy věty pouze zformulujeme, u jedné uvedeme celý důkaz. Vycházíme ze Schurova článku [6], kde důkaz není příliš detailní, a tak bylo třeba řadu kroků doplnit. Nakonec provedeme odhad stopy celistvého prvku.

Ve čtvrté kapitole nejprve věnujeme dvě kratší sekce poznatkům z oblasti permutačních a Galoisových grup. Zprvu nebude zřejmé, k čemu nám budou

lemmata užitečná, protože zde pracujeme s velmi konkrétním systémem těles, který se vyskytuje v důkazu hlavní věty. Konečně, sepíšeme důkaz hlavní věty, opět jej oproti článku [5] doplníme o několik chybějících kroků a pomocných lemmat. Na závěr provedeme diskuzi k odhadu diskriminantu tělesa figurujícího v důkazu.

# 1. Základní definice a fakta

V této kapitole shrneme základní pojmy a tvrzení, jež jsou součástí kurzů algebry, komutativních okruhů a algebraické teorie čísel, a proto je uvádíme převážně bez důkazů a explicitních referencí.

## 1.1 Tělesová rozšíření

Nechť  $T \leq S$  jsou tělesa. Potom  $S$  má přirozenou strukturu vektorového prostoru nad  $T$ , kde násobení skalárem  $T \times S \rightarrow S$  definujeme jako zúžení násobení  $S \times S \rightarrow S$ . Proto můžeme zadefinovat *stupeň rozšíření* těles  $T \leq S$  jako dimenzi vektorového prostoru  $S$  nad tělesem  $T$ , značíme  $[S : T]$ . Pro  $T \leq S \leq U$  rozšíření těles nám věta o iterovaném rozšíření dává  $[U : T] = [U : S][S : T]$ .

Dále říkáme, že  $a \in S$  je *algebraický prvek nad  $T$* , pokud existuje nekonstantní polynom  $f \in T[x]$  takový, že  $f(a) = 0$ . Pokud jsou všechny prvky v  $S$  algebraické nad  $T$ , nazveme  $S$  *algebraickým rozšířením  $T$* .

Připomeňme, že pro  $a \in S$  algebraický nad  $T$  je *minimální polynom  $m_{a,T}$*  prvku  $a$  nad  $T$  monický polynom nejmenšího (nenulového) stupně takový, že  $m_{a,T}(a) = 0$ .

**Tvrzení 1.1.** *Bud  $T \leq S$  rozšíření těles. Je-li  $a \in S$  algebraický prvek nad  $T$ , potom  $[T(a) : T] = \deg(m_{a,T})$ .*

Pro tělesa  $T \leq U, T \leq V$  nazveme homomorfismus  $\varphi : U \rightarrow V$   *$T$ -homomorfismem*, pokud  $\varphi(t) = t$  pro všechna  $t \in T$ . Potom pro  $T \leq U$  rozšíření těles definujeme *Galoisovu grupu* jako množinu všech  $T$ -automorfismů  $U \rightarrow U$  spolu s operací skládání, značíme  $\text{Gal}(U/T)$ . Připomeňme, že  $S$  je *rozkladové nadtěleso* polynomu  $f$ , pokud je to nejmenší možné těleso takové, že se v něm  $f$  rozkládá na lineární činitele.

K zadefinování Galoisových rozšíření těles budou potřeba pojmy algebraický uzávěr, separabilní a normální rozšíření.

**Definice 1.2.** Těleso  $T$  je *algebraicky uzavřené*, pokud v něm každý polynom  $f \in T[x]$  má kořen. *Algebraický uzávěr* tělesa  $T$  potom definujeme jako algebraicky uzavřené těleso  $S \geq T$ , které je algebraickým rozšířením  $T$ , značíme  $\bar{T}$ .

**Definice 1.3.** Bud  $T \leq U$  rozšíření těles.  $f \in T[x]$  je *separabilní polynom*, pokud nemá násobné kořeny v  $\bar{T}$ .  $\alpha \in U$  je *separabilní prvek*, pokud je minimální polynom pro  $\alpha$  nad  $T$  separabilní.  $U$  je *separabilní rozšíření  $T$* , pokud je každý prvek  $a \in U$  separabilní.

Ekvivalentně, pro rozšíření konečného stupně separabilita  $U$  znamená, že  $U = T(\alpha_1, \dots, \alpha_k)$  pro  $\alpha_1, \dots, \alpha_k$  separabilní. V této práci se setkáme pouze s rozšířeními  $\mathbb{Q}$ , která jsou vždy separabilní, protože se jedná o algebraická rozšíření tělesa charakteristiky 0.

**Definice 1.4.** Tělesové rozšíření  $T \leq U$  je *jednoduché*, pokud  $U = T(\alpha)$  pro nějaký prvek  $\alpha \in U$  algebraický nad  $T$ .

**Věta 1.5.** *Každé separabilní rozšíření konečného stupně je jednoduché.*

**Definice 1.6.** Tělesové rozšíření  $T \leq U$  je *normální*, pokud je algebraické a pro každý  $T$ -homomorfismus  $\varphi : U \rightarrow \bar{U}$  platí  $\varphi(U) \subset U$ .

Pro  $U \geq T$  normální a  $f \in T[x]$  ireducibilní platí, že má-li  $f$  v  $U$  jeden kořen, pak už tam má všechny kořeny. Dále máme následující vztah normálního rozšíření a rozkladového nadtělesa: Rozšíření  $U \geq T$  je normální právě tehdy, když existuje množina  $\mathcal{M} \subseteq T[x]$  taková, že  $U$  je rozkladové nadtěleso  $\mathcal{M}$  nad  $T$ , což znamená, že se každý polynom  $f \in \mathcal{M}$  rozkládá v  $U$  na lineární činitele a  $U = T[M]$ , kde  $M$  je množina všech kořenů polynomů  $f \in \mathcal{M}$ .

**Definice 1.7.** *Galoisovo rozšíření* definujeme jako normální, separabilní rozšíření konečného stupně.

**Věta 1.8** (Hlavní věta Galoisovy teorie). *Pro  $T \leq U$  Galoisovo rozšíření platí  $|\text{Gal}(U/T)| = [U : T]$ .*

**Definice 1.9.** *Galoisův uzávěr* separabilního rozšíření těles  $T \leq U$  je minimální Galoisovo rozšíření  $T$  obsahující  $U$ .

Galoisova teorie nám dává důležitou korespondenci mezi tělesy a Galoisovými grupami. Konkrétně, máme-li  $T \leq U$  Galoisovo rozšíření, dostáváme antiisomorfismus uspořádaných množin

$$\begin{aligned} \{V \text{ těleso} \mid T \leq V \leq U\} &\longleftrightarrow \{\text{podgrupy } H < \text{Gal}(U/V)\} \\ V &\longmapsto \text{Gal}(U/V) \\ \text{Fix}(U, H) &\longleftarrow H, \end{aligned}$$

kde  $\text{Fix}(U, H) = \{u \in U \mid h(u) = u \ \forall h \in H\}$ .

## 1.2 Číselné těleso, celistvé prvky

**Definice 1.10.** Těleso  $K$  nazveme *číselným tělesem*, pokud je to tělesové rozšíření  $\mathbb{Q}$  konečného stupně.

**Definice 1.11.** Buď  $R \subset S$  okruhy. Prvek  $\alpha \in S$  nazveme *celistvý* nad  $R$ , pokud je kořenem nějakého monického polynomu v  $R[x]$ .

Poznamenejme, že množina celistvých prvků okruhu  $S$  nad okruhem  $R$  tvoří podokruh v  $S$ .

Protože se v této práci zabýváme kvadratickými formami nad číselnými tělesy, budeme pojem celistvého prvku zmiňovat pouze ve významu celistvosti nad  $\mathbb{Z}$ . Pro číselné těleso  $K$  značíme okruh prvků  $K$ , jež jsou celistvé nad  $\mathbb{Z}$ , jako  $\mathcal{O}_K$ .

**Příklad 1.12.** Pro  $K = \mathbb{Q}(\sqrt{D})$ , kde  $D \neq 0, 1$  je bezčtvercové celé, máme

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

### 1.3 Stopa, diskriminant prvku, diskriminant tělesa

V této kapitole shrneme základní vlastnosti stop a diskriminantů, které jsou probírány na předmětu algebraická teorie čísel, proto nebudeme dokazovat vše, anebo důkaz jen naznačíme.

Mějme  $K$  číselné těleso konečného stupně  $[K : \mathbb{Q}] = n$ . Protože je  $K$  separabilní nad  $\mathbb{Q}$ , je dle věty 1.5 tvaru  $K = \mathbb{Q}(\alpha)$  pro nějaké  $\alpha \in K$ . Každý prostý tělesový  $\mathbb{Q}$ -homomorfismus (zkráceně vnoření)  $K \hookrightarrow \mathbb{C}$  je jednoznačně určen obrazem prvku  $\alpha$  a z Galoisovy teorie víme, že  $\alpha$  se musí zobrazit na jeden z kořenů jeho minimálního polynomu  $m_{\alpha, \mathbb{Q}}$ . Ten má dle tvrzení 1.1 stupeň  $n$ , a tedy ze separability  $n$  různých kořenů. Čili máme právě  $n$  vnoření  $\sigma_1, \dots, \sigma_n: K \hookrightarrow \mathbb{C}$ , která budeme využívat v dalších definicích.

**Definice 1.13.** Číselné těleso  $K$  nazveme *totálně reálné*, pokud každé vnoření  $\sigma : K \hookrightarrow \mathbb{C}$  má obor hodnot v  $\mathbb{R}$ .

**Definice 1.14.** Buď  $K$  číselné těleso. Řekneme, že prvek  $\alpha \in K$  je *totálně kladný*, pokud  $\sigma(\alpha) > 0$  pro každé vnoření  $\sigma : K \hookrightarrow \mathbb{R}$ , značíme  $\alpha \succ 0$ . Dále píšeme  $\alpha \succeq \beta$ , pokud  $\alpha - \beta \succ 0$  nebo  $\alpha = \beta$ . Množinu všech totálně kladných prvků  $K$  značíme  $K^+$  a množinu všech totálně kladných celistvých prvků značíme  $\mathcal{O}_K^+$ .

**Definice 1.15.** Buď  $K$  číselné těleso stupně  $n$ . Pro prvek  $\alpha \in K$  definujeme jeho *stopu* jako

$$\mathrm{Tr}_{K/\mathbb{Q}}(\alpha) = \sum_{1 \leq i \leq n} \sigma_i(\alpha).$$

Často budeme psát jen  $\mathrm{Tr}$ , pokud bude zřejmé, o jakém tělese mluvíme. V této práci se zaměříme především na stopy prvků z  $\mathcal{O}_K$  a  $\mathcal{O}_K^+$ .

**Lemma 1.16.** *Buď  $K$  číselné těleso. Pokud  $\alpha \in \mathcal{O}_K$ , resp.  $\alpha \in \mathcal{O}_K^+$ , pak  $\mathrm{Tr}(\alpha) \in \mathbb{Z}$ , resp.  $\mathrm{Tr}(\alpha) \in \mathbb{N}$ .*

*Důkaz.* Je-li prvek  $\alpha$  kořenem minimálního polynomu  $m_{\alpha, \mathbb{Q}} = x^n + a_{n-1}x^{n-1} + \dots + a_0 \in \mathbb{Z}[x]$ , pak obrazy  $\sigma_1(\alpha), \dots, \sigma_n(\alpha)$  všech vnoření  $K \hookrightarrow \mathbb{C}$  tvoří množinu všech kořenů  $m_{\alpha, \mathbb{Q}}$ . Neboli z Viètových vztahů  $\sum_{1 \leq i \leq n} \sigma_i(\alpha) = -a_{n-1} \in \mathbb{Z}$ . Pro  $\alpha \in \mathcal{O}_K^+$  plyne přímo z definice totálně kladného prvku  $\mathrm{Tr}(\alpha) = \sum_{1 \leq i \leq n} \sigma_i(\alpha) \in \mathbb{N}$ .  $\square$

**Lemma 1.17.** *Nechť  $L \geq K$  jsou číselná tělesa,  $[L : K] = n$ . Potom  $\mathrm{Tr}_{L/\mathbb{Q}}(\alpha) = n\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$  pro každé  $\alpha \in K$ .*

*Důkaz.* Pro těleso  $K$  stupně  $d$  máme  $d$  vnoření  $\sigma_1, \dots, \sigma_d: K \hookrightarrow \mathbb{C}$ , přičemž každé  $\sigma_i$  můžeme rozšířit na  $n$  vnoření  $\varphi_{i1}, \dots, \varphi_{in}: L \hookrightarrow \mathbb{C}$ . Potom pro  $\alpha \in K$  můžeme psát  $\mathrm{Tr}_{L/\mathbb{Q}}(\alpha) = (\varphi_{11}(\alpha) + \dots + \varphi_{1n}(\alpha)) + (\varphi_{21}(\alpha) + \dots + \varphi_{2n}(\alpha)) + \dots + (\varphi_{d1}(\alpha) + \dots + \varphi_{dn}(\alpha)) = n\sigma_1(\alpha) + n\sigma_2(\alpha) + \dots + n\sigma_d(\alpha) = n\mathrm{Tr}_{K/\mathbb{Q}}(\alpha)$ .  $\square$

Nyní si zadefinujeme pojem diskriminantu prvku. Ten se na první pohled liší od diskriminantu polynomu, jak ho známe ze základní algebry. Ukážeme však, že existuje jisté propojení mezi těmito dvěma koncepty.

**Definice 1.18.** Pro číselné těleso  $K$  stupně  $n$  a prvky  $a_1, \dots, a_n \in K$  definujeme *diskriminant* jako

$$\Delta_{K/\mathbb{Q}}(a_1, \dots, a_n) = \det((\text{Tr}(a_i a_j))_{n \times n}).$$

*Diskriminant prvku*  $\alpha \in K$  potom definujeme jako

$$\Delta_{K/\mathbb{Q}}(\alpha) = \Delta(1, \alpha, \alpha^2, \dots, \alpha^{n-1}).$$

Často budeme psát jen  $\Delta$ , pokud bude zřejmé, o jakém tělese mluvíme.

Uvedme si nyní ekvivalentní definici diskriminantu prvku, ve které figurují vnoření  $\sigma_i: K \hookrightarrow \mathbb{C}$ . Mějme matici

$$M = \begin{pmatrix} \sigma_1(1) & \sigma_1(\alpha) & \dots & \sigma_1(\alpha^{n-1}) \\ \sigma_2(1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(1) & \dots & \dots & \sigma_n(\alpha^{n-1}) \end{pmatrix}.$$

Potom prvek na pozici  $(i, j)$  matice  $M^T M$  je roven

$$\sum_{k=1}^n \sigma_k(\alpha^{i-1}) \sigma_k(\alpha^{j-1}) = \sum_{k=1}^n \sigma_k(\alpha^{i-1} \alpha^{j-1}) = \text{Tr}_{K/\mathbb{Q}}(\alpha^{i-1} \alpha^{j-1}),$$

a odtud

$$\begin{aligned} \Delta_{K/\mathbb{Q}}(\alpha) &= \Delta(1, \alpha, \alpha^2, \dots, \alpha^{n-1}) = \det((\text{Tr}(\alpha^{i-1} \alpha^{j-1}))_{n \times n}) = \\ &= \det(M^T M) = \det(M)^2 = \det(\sigma_i(\alpha^{j-1}))^2. \end{aligned}$$

Toto vyjádření využijeme v tvrzení 1.20, které dává do souvislosti diskriminant prvku a diskriminant z následující definice, jemuž se budeme více věnovat v kapitole 3.2.

**Definice 1.19.** *Diskriminantem* o  $n$  proměnných  $x_1, x_2, \dots, x_n$  rozumíme výraz

$$\tilde{\Delta}(x_1, x_2, \dots, x_n) = \prod_{i < j} (x_i - x_j)^2.$$

Explicitně upozorňujeme, že dva různé diskriminanty z definic 1.18 a 1.19 odlišíme značením  $\Delta, \tilde{\Delta}$ .

**Tvrzení 1.20.** *Pro  $K$  číselné těleso stupně  $n$ , vnoření  $\sigma_1, \dots, \sigma_n: K \hookrightarrow \mathbb{C}$  a  $\alpha \in K$  platí*

$$\Delta_{K/\mathbb{Q}}(\alpha) = \prod_{i < j} (\sigma_i(\alpha) - \sigma_j(\alpha))^2 = \tilde{\Delta}(\sigma_1(\alpha), \dots, \sigma_n(\alpha)).$$

*Důkaz.* (náznak) Protože  $\Delta_{K/\mathbb{Q}}(\alpha) = \det(M)^2$ , stačí ukázat, že

$$\det(M) = \det \begin{pmatrix} \sigma_1(1) & \sigma_1(\alpha) & \dots & \sigma_1(\alpha)^{n-1} \\ \sigma_2(1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(1) & \dots & \dots & \sigma_n(\alpha)^{n-1} \end{pmatrix} = \pm \prod_{i < j} (\sigma_i(\alpha) - \sigma_j(\alpha)).$$

Díváme-li se na tento determinant jako na výraz v proměnné  $\sigma_i(\alpha)$ , potom pro  $j \neq i$  platí  $(\sigma_i(\alpha) - \sigma_j(\alpha)) \mid \det(M)$  (po dosazení  $\sigma_j(\alpha)$  za  $\sigma_i(\alpha)$  počítáme determinant matice se dvěma shodnými řádky). Odtud  $\prod_{i < j} (\sigma_i(\alpha) - \sigma_j(\alpha)) \mid \det(M)$ . Porovnáním stupňů obou polynomů dostaneme (až na násobek  $-1$ ) rovnost.  $\square$

**Lemma 1.21.** *Nechť  $K$  je číselné těleso,  $b \in K$  a  $\Delta_{K/\mathbb{Q}}(b) = 0$ . Potom  $\mathbb{Q}(b) \not\subseteq K$ .*

*Důkaz.* Nechť  $[K : \mathbb{Q}] = n$ , mějme vnoření  $\sigma_1, \dots, \sigma_n: K \hookrightarrow \mathbb{C}$ . Z ekvivalentní definice diskriminantu prvku (tvrzení 1.20) snadno nahlédneme, že  $\Delta_{K/\mathbb{Q}}(b) = \prod_{i < j} (\sigma_i(b) - \sigma_j(b))^2 = 0$  právě tehdy, když existují indexy  $i \neq j$  takové, že  $\sigma_i(b) = \sigma_j(b)$ . Pokud by platilo  $\mathbb{Q}(b) = K$ , pak bychom takové indexy nenašli, protože  $\sigma_1, \dots, \sigma_n$  by musely být jednoznačně určeny obrazem prvku  $b$ , ale zároveň jsou navzájem různé. Tedy  $\mathbb{Q}(b) \not\subseteq K$ .  $\square$

**Definice 1.22.** Nechť  $K$  je číselné těleso a  $b_1, \dots, b_n$  je celistvá báze  $\mathcal{O}_K$ , tj.  $\mathcal{O}_K = \mathbb{Z}b_1 + \dots + \mathbb{Z}b_n$ . *Diskriminantem číselného tělesa  $K$  rozumíme*

$$\text{disc}_K = \Delta(b_1, \dots, b_n).$$

Poznamenejme, že diskriminant nezávisí na volbě celistvé báze, tudíž je definice korektní.

Podobně jako u diskriminantu prvku máme ekvivalentní definici využívající vnoření  $\sigma_1, \dots, \sigma_n: K \hookrightarrow \mathbb{C}$

$$\text{disc}_K = \det \begin{pmatrix} \sigma_1(b_1) & \sigma_1(b_2) & \dots & \sigma_1(b_n) \\ \sigma_2(b_1) & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \sigma_n(b_1) & \dots & \dots & \sigma_n(b_n) \end{pmatrix}^2.$$

Užitečné pozorování je, že každé dva diskriminanty se liší přenásobením druhou mocninou, přesněji pro  $\alpha_1, \dots, \alpha_n, \beta_1, \dots, \beta_n \in K$ ,  $b_j = \sum_i p_{ij} \alpha_i$ ,  $p_{ij} \in K$ ,  $P = (p_{ij})$  platí

$$\Delta(\beta_1, \dots, \beta_n) = (\det P)^2 \Delta(\alpha_1, \dots, \alpha_n).$$

Odtud máme následující vztah diskriminantu celistvého prvku a diskriminantu tělesa:

**Lemma 1.23.** *Bud'  $K$  číselné těleso. Pak*

$$\forall \alpha \in \mathcal{O}_K : \text{disc}_K \mid \Delta_{K/\mathbb{Q}}(\alpha).$$

*Důkaz.* Plyne z rovnosti  $\Delta(1, \alpha, \dots, \alpha^{n-1}) = (\det P)^2 \Delta_K$ , kde  $P$  je matice vyjádření prvků  $1, \alpha, \dots, \alpha^{n-1}$  pomocí celistvé báze  $\mathcal{O}_K$ .  $\square$

**Lemma 1.24.** *Pro  $K \leq F$  číselná tělesa platí*

$$\text{disc}_F \geq \text{disc}_K^{[F:K]}.$$

*Důkaz.* Vyplývá to například ze vztahu v [7, Cor. III.2.10].  $\square$

## 1.4 Univerzální kvadratické formy

V této sekci zadefinujeme klíčové pojmy potřebné ke studiu univerzálních kvadratických forem.

**Definice 1.25.** Kvadratickou formou nad okruhem  $R$  rozumíme polynom  $Q(x_1, \dots, x_n) = \sum_{i \leq j} a_{ij} x_i x_j$ , kde  $a_{ij} \in R$ .

V této práci se budeme potýkat pouze s případem, kdy okruh  $R$  je okruhem celistvých prvků nějakého číselného tělesa.

Positivně definitní kvadratickou formu v  $\mathbb{Z}$  nazveme *univerzální*, pokud reprezentuje všechna přirozená čísla, neboli pokud pro každé  $n \in \mathbb{N}$  nalezneme  $x_1, \dots, x_n \in \mathbb{Z}$  splňující  $Q(x_1, \dots, x_n) = n$ .

Analogickou definici nyní zavedeme v číselných tělesech. Zobecněním celých čísel jsou celistvé prvky, zobecněním přirozených zase totálně kladné celistvé prvky. Analogií k pozitivně definitním kvadratickým formám jsou totálně pozitivně definitní kvadratické formy.

**Definice 1.26.** Buď  $F$  totálně reálné číselné těleso. Kvadratickou formu  $Q$  (v  $n$  proměnných) nad  $\mathcal{O}_F$  nazveme *totálně pozitivně definitní*, pokud  $Q(v) \in \mathcal{O}_F^+$  pro každý nenulový vektor  $v \in \mathcal{O}_F^n$ .

**Definice 1.27.** Buď  $F$  totálně reálné číselné těleso. Totálně pozitivně definitní kvadratická forma  $Q$  nad  $\mathcal{O}_F$  je *univerzální* nad  $F$ , pokud reprezentuje všechny totálně kladné prvky z  $\mathcal{O}_F$ .

Protože s vyšším počtem proměnných mohou kvadratické formy reprezentovat více totálně kladných celistvých prvků, dává smysl pátrat po nejmenším možném počtu proměnných univerzálních kvadratických forem v daném číselném tělese. Počet proměnných kvadratické formy budeme zkráceně nazývat *hodnost*, tedy nás zajímá nejmenší možná hodnost  $m(F)$  univerzálních kvadratických forem v totálně reálném číselném tělese  $F$ . Například máme  $m(\mathbb{Q}) = 4$ , protože univerzální kvadratická forma nad  $\mathbb{Z}$  o 4 proměnných je například  $x^2 + y^2 + z^2 + w^2$ , na druhou stranu žádné kvadratické formy o 3 proměnných nad  $\mathbb{Z}$  neexistují.

Mezi důležité dosavadní výsledky studia hodnosti univerzálních kvadratických forem patří následující věta:

**Věta 1.28.** [4, Th. 1.1] *Pro každé  $m \in \mathbb{N}$  existuje nekonečně mnoho reálných kvadratických těles, nad kterými je počet proměnných každé univerzální kvadratické formy alespoň  $m$ .*

Zobecnění této věty říká, že dokonce pro každá  $m, d \in \mathbb{N}$ , kde  $d$  je dělitelné 2 nebo 3, existuje nekonečně mnoho totálně reálných číselných těles  $F$  stupně  $d$  splňujících  $m(F) \geq m$  [5, Th. 1]. Tato práce bude směřovat k podrobnému rozebrání důkazu této obecnější věty, avšak pouze pro stupeň  $d = 2n$ .

Věta 1.28 ke svému důkazu využívá pomocného tvrzení 1.29, které v této práci také budeme potřebovat. Říká nám, za jaké podmínky má každá univerzální kvadratická forma alespoň nějaký námi zvolený počet proměnných.

**Tvrzení 1.29.** [4, Prop. 2.1] *Nechť existují totálně kladné prvky  $a_1, a_2, \dots, a_m \in \mathcal{O}_F$  splňující, že pokud platí  $4a_i a_j \succeq b^2$  pro nějaká  $1 \leq i < j \leq m$  a nějaké  $b \in \mathcal{O}_F$ , pak  $b = 0$ . Potom má každá univerzální kvadratická forma nad  $\mathcal{O}_F$  alespoň  $m$  proměnných.*

Zavedeme značení navazující na tvrzení 1.29: prvky  $a_1, \dots, a_m \in \mathcal{O}_F$  nazveme *ortogonální* v  $F$ , pokud  $4a_i a_j \succeq b^2$  pro nějaká  $1 \leq i < j \leq m$  a nějaké  $b \in \mathcal{O}_F$  implikuje  $b = 0$ .

Princip důkazu věty 1.28 je pro každé  $m$  ukázat existenci nekonečně mnoha kvadratických těles, v nichž existuje  $m$  totálně kladných ortogonálních prvků. Pro naše účely bude ovšem stačit, že existuje jedno takové:

**Tvrzení 1.30.** [4, sekce 4] *Pro každé  $m \in \mathbb{N}$  existuje těleso  $\mathbb{Q}(\sqrt{D})$  s  $D > 1$  bezčtvercovým takové, že v něm existuje  $m$  totálně kladných ortogonálních prvků.*

## 2. Totálně kladné celistvé prvky s omezenou stopou

V této kapitole si více přiblížíme pojem stopy celistvého prvku nad  $\mathbb{Z}$ . Konkrétně nás bude zajímat, kolik existuje totálně kladných celistvých prvků takových, že jejich stopa je shora omezená nějakým přirozeným číslem. Ukážeme, že pro daný stupeň jejich minimálního polynomu je jich vždy konečně mnoho, provedeme přesný výpočet pro stupeň 2 a okomentujeme jejich počet pro stupeň 3. Výsledky v této kapitole můžeme považovat za víceméně známé, avšak jejich důkazy jsme vypracovali samostatně.

### 2.1 Konečný počet pro daný stupeň

**Věta 2.1.** *Nechť  $n, X \in \mathbb{N}$ . Potom existuje nejvýše konečně mnoho totálně kladných celistvých prvků  $\alpha$  nad  $\mathbb{Z}$  takových, že  $\deg(m_{\alpha, \mathbb{Q}}) = n$  a  $\text{Tr}(\alpha) \leq X$ .*

*Důkaz.* Ukážeme, že existuje nejvýše konečně mnoho monických celočíselných polynomů stupně  $n$ , jejichž kořeny jsou kladné reálné se součtem nejvýše  $X$ . Protože každý totálně kladný celistvý prvek  $\alpha$  s  $\deg(m_{\alpha, \mathbb{Q}}) = n$  a  $\text{Tr}(\alpha) \leq X$  je kořenem nějakého takového polynomu a každý polynom má konečně mnoho kořenů, dostaneme konečnost počtu těchto prvků.

Koeficienty polynomu  $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0$  můžeme zapsat jako  $\pm$  elementární symetrické polynomy, do kterých dosadíme kořeny  $x_1, \dots, x_n$ . Konkrétně, koeficient u členu stupně  $(n-i)$  je tvaru

$$a_{n-i} = (-1)^i s_i(x_1, \dots, x_n) = (-1)^i \sum_{1 \leq j_1 < j_2 < \dots < j_i \leq n} x_{j_1} \cdots x_{j_i}.$$

Speciálně,  $0 < -a_{n-1} = x_1 + \dots + x_n = \text{Tr}(\alpha) \leq X$ , kde  $\alpha$  je jeden z kořenů  $x_1, \dots, x_n$ . Tedy  $a_{n-1}$  může nabývat jen konečně mnoha hodnot. Ostatní koeficienty omezíme v závislosti na  $a_{n-1}$ . Máme

$$\begin{aligned} 0 &< \sum_{1 \leq j_1 < j_2 < \dots < j_i \leq n} x_{j_1} \cdots x_{j_i} \leq \sum_{1 \leq j_1 < j_2 < \dots < j_i \leq n} \left( \frac{x_{j_1} + \dots + x_{j_i}}{i} \right)^i \leq \\ &\leq \sum_{1 \leq j_1 < j_2 < \dots < j_i \leq n} \frac{(x_1 + x_2 + \dots + x_n)^i}{i^i} = \sum_{1 \leq j_1 < j_2 < \dots < j_i \leq n} \frac{(-a_{n-1})^i}{i^i} = \\ &= \binom{n}{i} (-1)^i \frac{a_{n-1}^i}{i^i}, \end{aligned}$$

kde jsme ve druhé nerovnosti použili A-G nerovnost. Pro koeficienty  $a_{n-i}$  tedy máme následující odhad:

$$0 < (-1)^i a_{n-i} \leq \binom{n}{i} (-1)^i \frac{a_{n-1}^i}{i^i},$$

neboli

- pro sudá  $i$ :  $0 < a_{n-i} \leq \binom{n}{i} \frac{a_{n-1}^i}{i^i}$
- pro lichá  $i$ :  $\binom{n}{i} \frac{a_{n-1}^i}{i^i} \leq a_{n-i} < 0$

Tudíž koeficienty monických celočíselných polynomů stupně  $n$ , jejichž kořeny jsou kladné reálné se součtem nejvýše  $X$ , mohou nabývat pouze konečně mnoha hodnot.  $\square$

## 2.2 Počet pro stupeň 2

Pojďme nyní určit přesný počet totálně kladných celistvých prvků stupně 2. Tento počet se rovná dvojnásobku počtu příslušných polynomů:

**Věta 2.2.** *Nechť  $X \in \mathbb{N}$ . Počet monických ireducibilních polynomů nad  $\mathbb{Z}$  stupně 2 s kořeny  $x_1, x_2 \in \mathbb{R}^+ \setminus \mathbb{N}$  splňujícími  $x_1 + x_2 \leq X$  je pro*

$$\begin{aligned} X \text{ sudé: } & \frac{1}{12}X^3 - \frac{1}{8}X^2 - \frac{1}{12}X, \\ X \text{ liché: } & \frac{1}{12}X^3 - \frac{1}{8}X^2 - \frac{1}{12}X + \frac{1}{8}. \end{aligned}$$

*Důkaz.* Určíme počet polynomů pro  $x_1, x_2 \in \mathbb{R}^+$  a od něj odečteme počet polynomů pro  $x_1, x_2 \in \mathbb{N}$ .

Nechť  $x_1, x_2 \in \mathbb{R}^+$ . Pro polynom  $x^2 + bx + c$  musí být splněny podmínky

$$\begin{aligned} 0 < -b = x_1 + x_2 &\leq X, \\ 0 < c = x_1x_2. \end{aligned}$$

Protože  $x_1, x_2 \in \mathbb{R}$ , platí pro diskriminant  $D = b^2 - 4c \geq 0$ , neboli  $c \leq \frac{1}{4}b^2$ . Tedy  $b$  můžeme volit libovolně (v příslušných mezích) a každé hodnotě  $b$  odpovídá  $\lfloor \frac{b^2}{4} \rfloor$  hodnot  $c$ , čili počet polynomů můžeme vyjádřit jako

$$\sum_{i=1}^X \left\lfloor \frac{i^2}{4} \right\rfloor = \sum_{i=1}^X \frac{i^2}{4} - \frac{1}{4}L,$$

kde  $L$  je počet lichých  $i \in \mathbb{Z}$ ,  $1 \leq i \leq X$ . Tedy pro  $X$  sudé dostáváme

$$\sum_{i=1}^X \frac{i^2}{4} - \frac{1}{4} \frac{X}{2} = \frac{1}{24}(2X^3 + 3X^2 + X) - \frac{1}{8}X = \frac{1}{12}X^3 + \frac{1}{8}X^2 - \frac{1}{12}X,$$

pro  $X$  liché máme

$$\sum_{i=1}^X \frac{i^2}{4} - \frac{1}{4} \frac{X+1}{2} = \frac{1}{24}(2X^3 + 3X^2 + X) - \frac{1}{8}(X+1) = \frac{1}{12}X^3 + \frac{1}{8}X^2 - \frac{1}{12}X - \frac{1}{8}.$$

Nyní určíme počet polynomů s kořeny  $x_1, x_2 \in \mathbb{N}$ , ekvivalentně, určíme počet dvojic  $(x_1, x_2) \in \mathbb{N}^2$  takových, že  $x_1 + x_2 \leq X$ ,  $x_1 \leq x_2$ . Možné hodnoty pro  $x_1$  jsou  $1, \dots, \lfloor \frac{X}{2} \rfloor$ , podle toho pro  $x_2$  máme vždy  $X - 2x_1 + 1$  možností, tedy počet všech takových dvojic je

$$\sum_{i=1}^{\lfloor \frac{X}{2} \rfloor} (X - 2i + 1) = X \left\lfloor \frac{X}{2} \right\rfloor - \left\lfloor \frac{X}{2} \right\rfloor \left( \left\lfloor \frac{X}{2} \right\rfloor + 1 \right) + \left\lfloor \frac{X}{2} \right\rfloor = X \left\lfloor \frac{X}{2} \right\rfloor - \left\lfloor \frac{X}{2} \right\rfloor^2,$$

což se pro sudá  $X$  rovná  $\frac{X^2}{4}$  a pro lichá  $\frac{X^2-1}{4}$ .

Nyní už můžeme určit výsledný počet polynomů s neceločíselnými kořeny:

$$X \text{ sudé: } \frac{1}{12}X^3 + \frac{1}{8}X^2 - \frac{1}{12}X - \frac{1}{4}X^2 = \frac{1}{12}X^3 - \frac{1}{8}X^2 - \frac{1}{12}X,$$

$$X \text{ liché: } \frac{1}{12}X^3 + \frac{1}{8}X^2 - \frac{1}{12}X - \frac{1}{8} - \frac{1}{4}(X^2 - 1) = \frac{1}{12}X^3 - \frac{1}{8}X^2 - \frac{1}{12}X + \frac{1}{8}.$$

□

## 2.3 Počet pro stupeň 3

Počty monických polynomů nad  $\mathbb{Z}$  s ryze reálnými kladnými kořeny a jejich omezeným součtem se dá zkoumat i pro polynomy vyššího stupně. Počet monických kubických polynomů nad  $\mathbb{Z}$  s kořeny  $x_1, x_2, x_3 \in \mathbb{R}^+ \setminus \mathbb{N}$ ,  $x_1 + x_2 + x_3 \leq X$  je asymptoticky roven  $X^6$ , z kapacitních důvodů však toto pozorování nebudeme dokazovat a ponecháváme jej pouze jako neformální poznámku. Asymptotickým počtem zde myslíme existenci konstant  $c_1, c_2$  takových, že tento počet je omezen zdola  $c_1 X^6$  a shora  $c_2 X^6$  pro všechna  $X \in \mathbb{N}$ .

Postup by spočíval v asymptotickém odhadu celkového počtu kubických polynomů s kořeny z  $\mathbb{R}^+ \setminus \mathbb{N}$  (vyjde  $\approx X^6$ ) a následném odečtení těch polynomů, které mají nějaký celočíselný kořen (vyjde  $\approx X^4$ ).

Naznačíme alespoň druhou část důkazu, tedy určení počtu polynomů s alespoň jedním celočíselným kořenem. Rozlišíme dva případy:

**A)** Všechny 3 kořeny jsou celočíselné.

Uřídíme počet trojic  $(x_1, x_2, x_3) \in \mathbb{N}^3$ , kde  $x_1 + x_2 + x_3 \leq X, x_1 \leq x_2 \leq x_3$ . Možné hodnoty pro  $x_1$  jsou  $1, \dots, \lfloor \frac{X}{3} \rfloor$ , na základě toho  $x_2$  může nabývat hodnot  $x_1, \dots, \lfloor \frac{X-x_1}{2} \rfloor$  (horní hranice zaručí existenci  $x_3$ ). Podle toho pro  $x_3$  máme vždy  $X - x_1 - 2x_2 + 1$  možností, tedy počet takových trojic je

$$\sum_{i=1}^{\lfloor \frac{X}{3} \rfloor} \sum_{j=i}^{\lfloor \frac{X-i}{2} \rfloor} (X - i - 2j + 1).$$

Pro přesný výsledek bychom rozlišili 6 případů podle zbytků  $X$  po dělení 3 a 2.

**B)** Právě 1 kořen je celočíselný.

Využijeme věty 2.2. Celočíselný kořen může nabývat hodnot  $1, \dots, X - 1$ , tedy maximální součet pro zbylé 2 ryze reálné kořeny také nabývá hodnot  $1, \dots, X - 1$ .

Počty takových polynomů tedy jsou pro

$$X \text{ sudé: } \sum_{k=1}^{X-1} \left( \frac{1}{12}k^3 - \frac{1}{8}k^2 - \frac{1}{12}k \right) = \frac{X^4}{48} - \frac{X^3}{12} + \frac{X^2}{24} + \frac{X}{48},$$

$$X \text{ liché: } \sum_{k=1}^{X-1} \left( \frac{1}{12}k^3 - \frac{1}{8}k^2 - \frac{1}{12}k + \frac{1}{8} \right) = \frac{X^4}{48} - \frac{X^3}{12} + \frac{X^2}{24} + \frac{7X}{48} - \frac{1}{8}.$$

Počet polynomů, který musíme odečíst, je tedy asymptoticky roven  $X^4$ .

# 3. Stieltjesovy odhady diskriminantu

Hlavním výstupem této kapitoly bude dolní odhad stopy druhé mocniny celistvého prvku. K důkazu využijeme jednu ze Stieltjesových vět odhadujících diskriminant z definice 1.19.

Uvedeme celkem tři Stieltjesovy věty (všechny převzaté z článku [6]) a podrobně rozebereme důkaz jedné z nich. Před formulací každé z vět zadefinujeme systém ortogonálních polynomů, se kterým se v dané větě pracuje.

## 3.1 Gegenbauerovy polynomy

V této podkapitole dokážeme několik rekurentních vztahů pro Gegenbauerovy polynomy, které později využijeme v důkazu Stieltjesovy věty I.

**Definice 3.1.** *Gegenbauerovy polynomy*  $C_n^{(\alpha)}$  definujeme vztahem

$$(1 - 2xz + z^2)^{-\alpha} = \sum_{n=0}^{\infty} C_n^{(\alpha)}(x)z^n.$$

Nechť po zbytek sekce  $F_n = C_n^{(-\frac{1}{2})}$ , zajímá nás tedy pouze verze definice 3.1 pro  $\alpha = -\frac{1}{2}$ :

$$\sqrt{1 - 2xz + z^2} = \sum_{n=0}^{\infty} F_n(x)z^n. \quad (3.1)$$

Nyní si blíže ukážeme, jak takové polynomy vypadají a jaké vztahy splňují.

**Příklad 3.2.** Spočteme polynomy  $F_0, F_1$ . Zobecněná binomická věta nám dává

$$\begin{aligned} (1 + (z^2 - 2xz))^{\frac{1}{2}} &= \binom{\frac{1}{2}}{0} + \binom{\frac{1}{2}}{1}(z^2 - 2xz) + \binom{\frac{1}{2}}{2}(z^2 - 2xz)^2 + \dots = \\ &= 1 + \frac{1}{2}(z^2 - 2xz) + \frac{\frac{1}{2}(-\frac{1}{2})}{2}(z^2 - 2xz)^2 + \dots \end{aligned}$$

Odtud  $F_0(x) = 1, F_1(x) = -x$ .

Dále označme  $\varphi = \sqrt{1 - 2xz + z^2}$ . První a druhé parciální derivace podle proměnných  $x, z$  jsou

$$\begin{aligned} \frac{\partial \varphi}{\partial x} &= \frac{-z}{\sqrt{1 - 2xz + z^2}}, & \frac{\partial^2 \varphi}{\partial x^2} &= \frac{-z^2}{(1 - 2xz + z^2)^{3/2}}, \\ \frac{\partial \varphi}{\partial z} &= \frac{z - x}{\sqrt{1 - 2xz + z^2}}, & \frac{\partial^2 \varphi}{\partial z^2} &= \frac{-x^2 + 1}{(1 - 2xz + z^2)^{3/2}}, \end{aligned}$$

což využijeme v následujících dvou lemmatech:

**Lemma 3.3.** *Polynomy  $F_n$  pro  $n \geq 1$  splňují*

$$nF_n = xF_n' - F_{n-1}'.$$

*Důkaz.* Ze vztahu prvních parciálních derivací

$$z \frac{\partial \varphi}{\partial z} = (x - z) \frac{\partial \varphi}{\partial x}$$

máme po dosazení ze vztahu (3.1)

$$\begin{aligned} z \sum_{n=0}^{\infty} n F_n(x) z^{n-1} &= (x - z) \sum_{n=0}^{\infty} F'_n(x) z^n, \\ \sum_{n=0}^{\infty} n F_n(x) z^n &= \sum_{n=0}^{\infty} x F'_n(x) z^n - \sum_{n=0}^{\infty} F'_n(x) z^{n+1}, \\ \sum_{n=1}^{\infty} n F_n(x) z^n &= \sum_{n=1}^{\infty} x F'_n(x) z^n - \sum_{n=0}^{\infty} F'_n(x) z^{n+1}, \end{aligned}$$

kde jsme v posledním řádku využili, že  $F'_0(x) = 0$ . Přeindexováním  $\sum_{n=0}^{\infty} F'_n(x) z^{n+1} = \sum_{m=1}^{\infty} F'_{m-1}(x) z^m$  již dostaneme

$$\sum_{n=1}^{\infty} n F_n(x) z^n = \sum_{n=1}^{\infty} x F'_n(x) z^n - \sum_{n=1}^{\infty} F'_{n-1}(x) z^n = \sum_{n=1}^{\infty} (x F'_n(x) - F'_{n-1}(x)) z^n.$$

□

**Lemma 3.4.** *Polynomy  $F_n$  pro  $n \geq 2$  splňují*

$$(n - 1)F'_n - (2n - 3)x F'_{n-1} + (n - 2)F'_{n-2} = 0.$$

*Důkaz.* Ze vztahu druhých parciálních derivací

$$(x^2 - 1) \frac{\partial^2 \varphi}{\partial x^2} = z^2 \frac{\partial^2 \varphi}{\partial z^2}$$

máme po dosazení ze vztahu (3.1)

$$(x^2 - 1) \sum_{n=0}^{\infty} F''_n(x) z^n = z^2 \sum_{n=0}^{\infty} n(n - 1) F_n(x) z^{n-2},$$

neboli  $F''_n = \frac{n(n-1)}{x^2-1} F_n$ . Zderivováním vztahu z lemmatu 3.3 dostaneme

$$n F'_n = F'_n + x F''_n - F''_{n-1} = F'_n + x \frac{n(n-1)}{x^2-1} F_n - \frac{(n-1)(n-2)}{x^2-1} F_{n-1}$$

a opět použijeme lemma 3.3 pro  $n, n - 1$ :

$$\begin{aligned} n F'_n &= F'_n + x \frac{n(n-1)}{x^2-1} \frac{1}{n} (x F'_n - F'_{n-1}) - \frac{(n-1)(n-2)}{x^2-1} \frac{1}{n-1} (x F'_{n-1} - F'_{n-2}) = \\ &= \frac{x^2 n - 1}{x^2 - 1} F'_n + \frac{-2x n + 3x}{x^2 - 1} F'_{n-1} + \frac{n - 2}{x^2 - 1} F'_{n-2}, \end{aligned}$$

což vede na dokazovanou rekurenci. □

**Lemma 3.5.** *Polynomy  $F_n$  splňují pro  $n \geq 2$  rekurentní vztah*

$$F_n = \frac{1}{n} [x(2n - 3) F_{n-1} - (n - 3) F_{n-2}].$$

*Důkaz.* Podle lemmatu 3.3 dosadíme do dokazované rovnosti

$$\begin{aligned} F_n &= \frac{1}{n}(xF'_n - F'_{n-1}), \\ F_{n-1} &= \frac{1}{n-1}(xF'_{n-1} - F'_{n-2}), \\ F_{n-2} &= \frac{1}{n-2}(xF'_{n-2} - F'_{n-3}), \end{aligned}$$

zároveň z lemmatu 3.4 dosadíme

$$F'_n = \frac{1}{n-1}[(2n-3)xF'_{n-1} - (n-2)F'_{n-2}],$$

tedy celkem máme

$$\begin{aligned} &\frac{1}{n} \left[ x \frac{1}{n-1} \left( (2n-3)xF'_{n-1} - (n-2)F'_{n-2} \right) - F'_{n-1} \right] = \\ &= \frac{1}{n} \left[ x(2n-3) \frac{1}{n-1} (xF'_{n-1} - F'_{n-2}) - (n-3) \frac{1}{n-2} (xF'_{n-2} - F'_{n-3}) \right], \end{aligned}$$

neboli

$$\begin{aligned} &x^2 \frac{2n-3}{n-1} F'_{n-1} - x \frac{n-2}{n-1} F'_{n-2} - F'_{n-1} = \\ &= x^2 \frac{2n-3}{n-1} F'_{n-1} - x \frac{2n-3}{n-1} F'_{n-2} - x \frac{n-3}{n-2} F'_{n-2} + \frac{n-3}{n-2} F'_{n-3}. \end{aligned}$$

Rovnost dále upravujeme:

$$\begin{aligned} &-F'_{n-1} - x \left[ \frac{n-2}{n-1} - \frac{2n-3}{n-1} - \frac{n-3}{n-2} \right] F'_{n-2} - \frac{n-3}{n-2} F'_{n-3} = 0, \\ &(n-2)F'_{n-1} + x \left[ \frac{(n-2)^2}{n-1} - \frac{(2n-3)(n-2)}{n-1} - (n-3) \right] F'_{n-2} + (n-3)F'_{n-3} = 0. \end{aligned}$$

Upravíme prostřední závorku poslední rovnosti:

$$\begin{aligned} &\frac{(n-2)^2}{n-1} - \frac{(2n-3)(n-2)}{n-1} - (n-3) = \\ &= \frac{-2n^2 + 7n - 5}{n-1} = -\frac{(2n-5)(n-1)}{n-1} = -(2n-5). \end{aligned}$$

Po dosazení získáváme vztah

$$(n-2)F'_{n-1} - (2n-5)xF'_{n-2} + (n-3)F'_{n-3} = 0,$$

který po přeindexování odpovídá vztahu z lemmatu 3.4, tedy rovnost, ze které jsme vycházeli, byla správná.  $\square$

**Příklad 3.6.** S využitím lemmatu 3.5 spočteme další polynomy  $F_n$ :

- $F_2(x) = -\frac{1}{2}x^2 + \frac{1}{2}$

- $F_3(x) = -\frac{1}{2}x^3 + \frac{1}{2}x$
- $F_4(x) = -\frac{5}{8}x^4 + \frac{3}{4}x^2 - \frac{1}{8}$

**Lemma 3.7.** *Polynom  $F_n$  má stupeň  $n$  a pro vedoucí koeficient  $c_n$  pro  $n \geq 2$  platí*

$$c_n = -\frac{1 \cdot 3 \cdots (2n-3)}{1 \cdot 2 \cdots n}.$$

*Důkaz.* Stupeň  $n$  získáme použitím indukce, konkrétně z příkladu 3.2 a rekurence z lemmatu 3.5. Vzorec pro  $c_n$  dokážeme také indukcí. Z příkladu 3.6 máme  $c_2 = -\frac{1}{2}$ . Předpokládejme, že vztah platí pro  $n-1$ . V rekurentním vztahu

$$(n-1)F'_n - (2n-3)x F'_{n-1} + (n-2)F'_{n-2} = 0$$

z lemmatu 3.3 máme speciálně rovnost koeficientů u členu  $x^{n-1}$ , tedy

$$(n-1)nc_n - (2n-3)(n-1)c_{n-1} = 0,$$

$$c_n = \frac{2n-3}{n}c_{n-1},$$

což s využitím indukčního předpokladu vede na dokazovaný vztah.  $\square$

## 3.2 Stieltjesova věta o maximálním diskriminantu

V této sekci vyslovíme a dokážeme první Stieltjesovu větu o tom, jak je omezen diskriminant proměnných  $x_1, \dots, x_n$ , pokud pro každou proměnnou  $x_i$  platí  $-1 \leq x_i \leq 1$  (věta 3.13). Protože je důkaz poněkud rozsáhlý, rozdělíme Stieltjesovu větu I na dvě části. Nejprve bez důkazů uvedeme tři věty z matematické analýzy, které poté využijeme v důkazu lemmatu 3.11 (první část Stieltjesovy věty I). V celé sekci uvažujeme  $n \geq 2$ .

**Věta 3.8** (kompaktnost v  $\mathbb{R}^n$ ). *Nechť  $n \in \mathbb{N}$  a  $K \subset \mathbb{R}^n$ . Potom  $K$  je kompaktní právě tehdy, když je omezená a uzavřená.*

**Věta 3.9** (extrémy spojité funkce na kompaktu). *Nechť  $K \subset \mathbb{R}^n$  je kompaktní a  $f : K \rightarrow \mathbb{R}$  spojitá. Potom  $f$  nabývá na  $K$  svého maxima i svého minima.*

**Věta 3.10** (nutná podmínka existence lokálního extrému). *Nechť  $n \in \mathbb{N}$ ,  $G \subset \mathbb{R}^n$  je otevřená,  $a \in G$  a  $i \in \{1, \dots, n\}$ . Nechť funkce  $f : G \rightarrow \mathbb{R}$  má v bodě  $a$  lokální extrém. Potom buď  $\frac{\partial f}{\partial x_i}(a)$  neexistuje nebo  $\frac{\partial f}{\partial x_i}(a) = 0$ .*

**Lemma 3.11** (1. část Stieltjesovy věty I). *Nechť  $x_1, x_2, \dots, x_n$  jsou reálná čísla splňující  $-1 \leq x_i \leq 1$  pro  $i = 1, \dots, n$ . Potom  $\tilde{\Delta}(x_1, x_2, \dots, x_n)$  nabývá maxima v bodě  $(x_1, \dots, x_n)$ , kde  $x_1, \dots, x_n$  jsou kořeny polynomu  $F_n$ .*

*Důkaz.* Množina  $\{-1 \leq x_i \leq 1 \mid -1 \leq i \leq n\} \subset \mathbb{R}^n$  je zřejmě omezená a uzavřená, tudíž je dle věty 3.8 kompaktní. Funkce  $\tilde{\Delta}(x_1, x_2, \dots, x_n)$  je jakožto polynom  $n$  proměnných spojitá, proto dle věty 3.9 nabývá na kompaktní množině  $\{-1 \leq x_i \leq 1 \mid -1 \leq i \leq n\}$  svého maxima. Protože se jedná o nezápornou funkci, která je nulová, pokud  $x_i = x_j$  pro nějaké  $i \neq j$ , a my hledáme taková

$x_1, \dots, x_n$ , ve kterých se nabývá maxima, můžeme bez újmy na obecnosti předpokládat, že  $x_1 < x_2 < \dots < x_n$ . Protože  $\tilde{\Delta}$  je hladká funkce (čili má všude derivaci), musí pro taková  $x_1, \dots, x_n$  dle věty 3.10 platit buď  $\frac{\partial \tilde{\Delta}}{\partial x_\nu} = 0$ , anebo  $x_\nu = \pm 1$  (krajní body intervalu). Pokud  $n = 2$ , maximum funkce  $(x_1 - x_2)^2 = x_1^2 - 2x_1x_2 + x_2^2$  je nabyto pro  $x_1 = -1, x_2 = 1$ , protože parciální derivace  $2x_1 - 2x_2, -2x_1 + 2x_2$  jsou rovny 0 pro  $x_1 = x_2$  a funkce zde nabývá 0, kdežto v krajních bodech intervalů je rovna 4.

Nyní necht'  $n > 2$ . Ukažme si nyní, co znamená, že je pro  $x_\nu$  splněna podmínka  $\frac{\partial \tilde{\Delta}}{\partial x_\nu} = 0$  (pro  $-1 < x_\nu < 1$ , kde  $1 < \nu < n$ , tato podmínka platit musí, protože parciální derivace existují, a ukáže se, že pro  $x_1, x_n$  musí platit druhá varianta z nutné podmínky extrému, totiž  $x_1 = -1, x_n = 1$ ). Protože

$$\begin{aligned} \frac{1}{\tilde{\Delta}} \frac{\partial \tilde{\Delta}}{\partial x_\nu} &= \frac{1}{\prod_{i \neq \nu} (x_\nu - x_i)^2 \prod_{j < k; j, k \neq \nu} (x_j - x_k)^2} \\ &\cdot \frac{\partial (\prod_{i \neq \nu} (x_\nu - x_i)^2 \prod_{j < k; j, k \neq \nu} (x_j - x_k)^2)}{\partial x_\nu} = \frac{2 \prod_{i \neq \nu} (x_\nu - x_i)}{\prod_{i \neq \nu} (x_\nu - x_i)^2} \cdot \frac{\partial (\prod_{i \neq \nu} (x_\nu - x_i))}{\partial x_\nu} = \\ &= \frac{2}{\prod_{i \neq \nu} (x_\nu - x_i)} \cdot \frac{\partial (\prod_{i \neq \nu} (x_\nu - x_i))}{\partial x_\nu} = 2 \frac{\sum_{i \neq \nu} (\prod_{j \neq i} (x_\nu - x_j))}{\prod_{i \neq \nu} (x_\nu - x_i)} = 2 \sum_{\substack{i=1 \\ i \neq \nu}}^n \frac{1}{x_\nu - x_i}, \end{aligned}$$

řešíme

$$\sum_{\substack{i=1 \\ i \neq \nu}}^n \frac{1}{x_\nu - x_i} = 0.$$

Levou stranu si vyjádříme jiným způsobem. Definujme polynomy

$$f(x) = \prod_{i=1}^n (x - x_i), \quad f_\nu(x) = \prod_{\substack{i=1 \\ i \neq \nu}}^n (x - x_i).$$

Tyto polynomy splňují

$$\begin{aligned} \frac{f'_\nu(x)}{f_\nu(x)} &= \left( \frac{f(x)}{x - x_\nu} \right)' \frac{x - x_\nu}{f(x)} = \frac{f'(x)(x - x_\nu) - f(x)}{(x - x_\nu)^2} \cdot \frac{x - x_\nu}{f(x)} = \frac{f'(x)}{f(x)} - \frac{1}{x - x_\nu} = \\ &= \frac{(x - x_2) \cdots (x - x_n) + \cdots + (x - x_1) \cdots (x - x_{n-1})}{(x - x_1) \cdots (x - x_n)} - \frac{1}{x - x_\nu} = \\ &= \sum_{\substack{i=1 \\ i \neq \nu}}^n \frac{1}{x - x_i}. \end{aligned}$$

Tedy pokud  $\frac{\partial \tilde{\Delta}}{\partial x_\nu} = 0$ , pak musí platit  $\frac{f'_\nu(x_\nu)}{f_\nu(x_\nu)} = 0$ . Máme

$$\begin{aligned} f''(x) &= \left( \sum_{1 \leq i_1 < \dots < i_{n-1} \leq n} (x - x_{i_1}) \cdots (x - x_{i_{n-1}}) \right)' = \\ &= \sum_{1 \leq i_1 < \dots < i_{n-1} \leq n} \left( (x - x_{i_1}) \cdots (x - x_{i_{n-1}}) \right)' = \end{aligned}$$

$$\begin{aligned}
&= \sum_{1 \leq i_1 < \dots < i_{n-1} \leq n} \left( \sum_{1 \leq j_1 < \dots < j_{n-2} \leq n} ((x - x_{j_1}) \cdots (x - x_{j_{n-2}})) \right) = \\
&= 2 \sum_{1 \leq i_1 < \dots < i_{n-2} \leq n} (x - x_{i_1}) \cdots (x - x_{i_{n-2}}),
\end{aligned}$$

tedy  $f''(x_\nu) = 2f'_\nu(x_\nu)$  a podmínka  $\frac{f'_\nu(x_\nu)}{f_\nu(x_\nu)} = 0$  implikuje  $f''(x_\nu) = 0$ .

Dostali jsme, že pokud  $\frac{\partial \tilde{\Delta}}{\partial x_\nu} = 0$ , pak  $f''(x_\nu) = 0$ . Tedy  $x_2, \dots, x_{n-1}$  jsou nutně kořeny polynomu  $f''(x)$ . Protože počet kořenů  $f''(x)$  je  $(n-2)$ , nemohou již  $x_1, x_n$  být jeho kořeny, tedy musí platit  $x_1 = -1, x_n = 1$ . Protože víme, že maxima diskriminantu je nabyto, jsou nutné podmínky zároveň postačující a v takto popsaném bodě  $(x_1, \dots, x_n)$  se maxima opravdu nabývá.

Nyní se pokusíme  $x_2, \dots, x_{n-1}$  jakožto kořeny polynomu  $f''(x)$  popsat jiným způsobem, to jest jako kořeny funkce, jejíž předpis na nich nezávisí. Polynomy  $f(x)$  a  $(x^2 - 1)f''(x)$  mají stejné kořeny, tedy jsou si až na násobek konstanty rovny. Porovnáním koeficientů u  $x^n$  dostaneme, že  $(x^2 - 1)f''(x) = n(n-1)f(x)$  (koeficient u  $x^{n-2}$  v  $f''(x)$  je  $2\binom{n}{2}$ ). Protože je  $f$  polynom, je řešení této diferenciální rovnice jednoznačné až na konstantu. Ukážeme, že rovnici řeší právě polynom  $F_n$ , který je definován vztahem

$$\varphi(x, z) = \sqrt{1 - 2xz + z^2} = \sum_{n=0}^{\infty} F_n(x)z^n.$$

Ze vztahů

$$\begin{aligned}
\frac{\partial \varphi}{\partial x} &= \frac{-z}{\sqrt{1 - 2xz + z^2}}, & \frac{\partial^2 \varphi}{\partial x^2} &= \frac{-z^2}{(1 - 2xz + z^2)^{3/2}}, \\
\frac{\partial \varphi}{\partial z} &= \frac{z - x}{\sqrt{1 - 2xz + z^2}}, & \frac{\partial^2 \varphi}{\partial z^2} &= \frac{-x^2 + 1}{(1 - 2xz + z^2)^{3/2}}
\end{aligned}$$

vyplývá

$$(x^2 - 1) \frac{\partial^2 \varphi}{\partial x^2} = z^2 \frac{\partial^2 \varphi}{\partial z^2}. \quad (3.2)$$

Protože druhé parciální derivace můžeme zapsat také jako

$$\frac{\partial^2 \varphi}{\partial x^2} = \sum_{n=0}^{\infty} F_n''(x)z^n, \quad \frac{\partial^2 \varphi}{\partial z^2} = \sum_{n=0}^{\infty} n(n-1)F_n(x)z^{n-2},$$

dostaneme užitím vztahu (3.2)

$$\begin{aligned}
(x^2 - 1) \sum_{n=0}^{\infty} F_n''(x)z^n &= z^2 \sum_{n=0}^{\infty} n(n-1)F_n(x)z^{n-2}, \\
\sum_{n=0}^{\infty} (x^2 - 1)F_n''(x)z^n &= \sum_{n=0}^{\infty} n(n-1)F_n(x)z^n.
\end{aligned}$$

Tedy polynom  $F_n$  vyhovuje rovnici  $(x^2 - 1)f''(x) = n(n-1)f(x)$ . Složky  $x_1, \dots, x_n$  bodu, ve kterém diskriminant nabývá maxima, jsme charakterizovali jako kořeny polynomu  $f''(x)$  spolu s  $-1, 1$ , a tudíž je rovněž můžeme charakterizovat jako kořeny  $F_n$ .  $\square$

**Lemma 3.12** (2. část Stieltjesovy věty I). *Nechť  $x_1, x_2, \dots, x_n$  jsou reálná čísla splňující  $-1 \leq x_i \leq 1$  pro  $i = 1, \dots, n$ . Potom maximum výrazu  $\tilde{\Delta}(x_1, x_2, \dots, x_n)$  je rovno*

$$M_n = \frac{2^2 \cdot 3^3 \dots n^n \cdot 2^2 \cdot 3^3 \dots (n-2)^{(n-2)}}{3^3 \cdot 5^5 \dots (2n-3)^{(2n-3)}}.$$

*Důkaz.* V lemmatu 3.11 jsme ukázali, že maximum  $M_n$  je nabyto pro  $x_1, \dots, x_n$  kořeny polynomu  $F_n$ . Označme  $F_n(x) = c_n x^n + \tilde{c}_n x^{n-1} + \dots$ , kde  $c_n = -\frac{1 \cdot 3 \dots (2n-3)}{1 \cdot 2 \dots n}$  z lemmatu 3.7. Dále necht'  $y_1, \dots, y_{n-1}$  a  $z_1, \dots, z_{n-2}$  popořadě označují kořeny polynomů  $F'_n, F'_{n-1}$ .

Strategie nalezení maximálního diskriminantu  $M_n$  bude následující: Vyjádříme  $M_n$  zvláště pomocí  $F'_{n-1}$  a  $F'_{n-2}$ , poté díky přeindexování ve vztahu  $M_n$  a  $F'_{n-1}$  vyjádříme  $M_{n-1}$  pomocí  $F'_{n-2}$ , a nakonec určíme podíl  $\frac{M_n}{M_{n-1}}$ , kde se figurující polynomy  $F'_{n-2}$  zkrátí. Z tohoto podílu již bude patrný předpis pro  $M_n$ .

Platí

$$(-1)^{\frac{n(n-1)}{2}} M_n = \frac{1}{c_n^n} \prod_{\alpha=1}^n F'_n(x_\alpha) = \frac{n^n}{c_n^{n-1}} \prod_{\beta=1}^{n-1} F'_n(y_\beta), \quad (3.3)$$

kde první rovnost v (3.3) plyne z následujících úprav a kroků:

$$\begin{aligned} F_n(x) &= c_n(x-x_1) \cdots (x-x_n), \\ F'_n(x) &= c_n[(x-x_2) \cdots (x-x_n) + \cdots + (x-x_1) \cdots (x-x_{n-1})], \\ F'_n(x_\alpha) &= c_n(x_\alpha-x_1) \cdots (x_\alpha-x_{\alpha-1})(x_\alpha-x_{\alpha+1}) \cdots (x_\alpha-x_n), \\ \prod_{\alpha=1}^n F'_n(x_\alpha) &= c_n^n \prod_{i < j} (-1)^{\binom{n}{2}} (x_i - x_j)^2, \end{aligned}$$

kde jsme využili, že každá závorka  $(x_i - x_j)$  se v součinu vyskytne dvakrát, po každé s jiným pořadím členů, a všech dvojic je  $\binom{n}{2}$ .

Druhá rovnost v (3.3) potom plyne z úprav

$$\begin{aligned} F'_n(x) &= c_n n x^{n-1} + \tilde{c}_n (n-1) x^{n-2} + \cdots = c_n n (x-y_1) \cdots (x-y_{n-1}), \\ \frac{1}{c_n^n} \prod_{\alpha=1}^n F'_n(x_\alpha) &= n^n [(x_1-y_1) \cdots (x_1-y_{n-1})] \cdots [(x_n-y_1) \cdots (x_n-y_{n-1})] = \\ &= n^n (-1)^{n(n-1)} \prod_{\beta=1}^{n-1} [(y_\beta-x_1) \cdots (y_\beta-x_n)] = \\ &= \frac{n^n}{c_n^{n-1}} \prod_{\beta=1}^{n-1} F'_n(y_\beta). \end{aligned}$$

Nyní do rekurentního vztahu z lemmatu 3.3 za  $x$  dosadíme  $y_\beta$ , kořen  $F'_n$ , čímž dostaneme  $n F'_n(y_\beta) = -F'_{n-1}(y_\beta)$ . V rovnosti (3.3) tedy můžeme nahradit  $F'_n(y_\beta) = -\frac{1}{n} F'_{n-1}(y_\beta)$ :

$$(-1)^{\frac{n(n-1)}{2}} M_n = \frac{n^n}{c_n^{n-1}} \frac{(-1)^{n-1}}{n^{n-1}} \prod_{\beta=1}^{n-1} F'_{n-1}(y_\beta) =$$

$$= \frac{(-1)^{n-1}(n-1)^{n-1}c_{n-1}^{n-1}}{n^{n-3}c_n^{2n-3}} \prod_{\gamma=1}^{n-2} F'_n(z_\gamma), \quad (3.4)$$

kde druhou rovnost dostaneme pomocí následujících kroků:

$$\begin{aligned} F_{n-1}(x) &= c_{n-1}x^{n-1} + \tilde{c}_{n-1}x^{n-2} + \dots, \\ F'_{n-1}(x) &= c_{n-1}(n-1)(x-z_1)\cdots(x-z_{n-2}), \end{aligned}$$

$$\begin{aligned} \prod_{\beta=1}^{n-1} F'_{n-1}(y_\beta) &= \prod_{\beta=1}^{n-1} c_{n-1}(n-1)(y_\beta-z_1)\cdots(y_\beta-z_{n-2}) = \\ &= c_{n-1}^{n-1}(n-1)^{n-1}(-1)^{(n-1)(n-2)} \prod_{\gamma=1}^{n-2} (z_\gamma-y_1)\cdots(z_\gamma-y_{n-1}) = \\ &= \frac{c_{n-1}^{n-1}(n-1)^{n-1}}{c_n^{n-2}n^{n-2}} \prod_{\gamma=1}^{n-2} F'_n(z_\gamma). \end{aligned}$$

Nyní do rekurentního vztahu z lemmatu 3.4 za  $x$  dosadíme  $z_\gamma$ , kořen  $F'_{n-1}$ , čímž dostaneme  $(n-1)F'_n(z_\gamma) = -(n-2)F'_{n-2}(z_\gamma)$ . V rovnosti (3.4) dosadíme  $F'_n(z_\gamma) = \frac{-(n-2)}{(n-1)}F'_{n-2}(z_\gamma)$ :

$$\begin{aligned} (-1)^{\frac{n(n-1)}{2}} M_n &= \frac{(-1)^{n-1}(n-1)^{n-1}c_{n-1}^{n-1}}{n^{n-3}c_n^{2n-3}} \cdot \frac{(-1)^{n-2}(n-2)^{n-2}}{(n-1)^{n-2}} \prod_{\gamma=1}^{n-2} F'_{n-2}(z_\gamma) = \\ &= -\frac{(n-1)(n-2)^{n-2}c_{n-1}^{n-1}}{n^{n-3}c_n^{2n-3}} \prod_{\gamma=1}^{n-2} F'_{n-2}(z_\gamma). \end{aligned} \quad (3.5)$$

Zároveň první rovnost ze vztahu (3.4)

$$(-1)^{\frac{n(n-1)}{2}} M_n = \frac{(-1)^{n-1}n^{n-1}}{c_n^{n-1}} \prod_{\beta=1}^{n-1} F'_{n-1}(y_\beta)$$

dává po substituci  $n-1$  za  $n$ :

$$(-1)^{\frac{1}{2}(n-1)(n-2)} M_{n-1} = \frac{(-1)^{n-2}(n-1)^{n-2}}{c_{n-1}^{n-2}} \prod_{\gamma=1}^{n-2} F'_{n-2}(z_\gamma). \quad (3.6)$$

Nyní již ze vztahů (3.5) a (3.6) můžeme vyjádřit podíl  $\frac{M_n}{M_{n-1}}$ :

$$\frac{M_n}{M_{n-1}} = \frac{(n-2)^{n-2}}{n^{n-3}} \left(\frac{c_{n-1}}{c_n}\right)^{2n-3} = \frac{(n-2)^{n-2}}{n^{n-3}} \left(\frac{n}{2n-3}\right)^{2n-3} = \frac{n^n(n-2)^{n-2}}{(2n-3)^{2n-3}}.$$

Indukcí už lze snadno dokázat, že

$$M_n = \frac{2^2 \cdot 3^3 \cdots n^n \cdot 2^2 \cdot 3^3 \cdots (n-2)^{n-2}}{3^3 \cdot 5^5 \cdots (2n-3)^{2n-3}}:$$

- Pro  $n=2$  jsme v úvodu důkazu lemmatu 3.11 spočetli, že maximum výrazu  $(x_1 - x_2)^2$  je 4, což souhlasí s  $M_n = \frac{2^2}{1} = 4$  (poznamenejme, že se v  $M_2$  vyskytují 2 prázdné součiny, které jsou z definice rovny 1).

- Pro  $k \in \mathbb{N}$  máme s použitím indukčního předpokladu

$$\begin{aligned}
M_k &= M_{k-1} \cdot \frac{k^k (k-2)^{k-2}}{(2k-3)^{2k-3}} = \\
&= \frac{2^2 \cdot 3^3 \cdots (k-1)^{k-1} \cdot 2^2 \cdot 3^3 \cdots (k-3)^{k-3}}{3^3 \cdot 5^5 \cdots (2k-5)^{2k-5}} \cdot \frac{k^k (k-2)^{k-2}}{(2k-3)^{2k-3}} = \\
&= \frac{2^2 \cdot 3^3 \cdots k^k \cdot 2^2 \cdot 3^3 \cdots (k-2)^{k-2}}{3^3 \cdot 5^5 \cdots (2k-3)^{2k-3}}.
\end{aligned}$$

□

Nyní obě lemmata shrneme do jedné věty.

**Věta 3.13.** [6, Par.1, Th.I](Stieltjesova věta I) *Nechť  $x_1, x_2, \dots, x_n$  jsou reálná čísla splňující  $-1 \leq x_i \leq 1$  pro  $i = 1, \dots, n$ . Potom výraz  $\tilde{\Delta}(x_1, x_2, \dots, x_n)$  nabývá maxima*

$$M_n = \frac{2^2 \cdot 3^3 \cdots n^n \cdot 2^2 \cdot 3^3 \cdots (n-2)^{(n-2)}}{3^3 \cdot 5^5 \cdots (2n-3)^{(2n-3)}}$$

*v bodě  $(x_1, \dots, x_n)$ , kde  $x_1, \dots, x_n$  jsou kořeny polynomu  $F_n$ , který vystupuje jako koeficient u  $z^n$  ve výrazu*

$$\varphi = \sqrt{1 - 2xz + z^2} = \sum_{n=0}^{\infty} F_n(x) z^n.$$

### 3.3 Další Stieltjesovy věty

V této sekci zmíníme další dvě Stieltjesovy věty, které se týkají omezení diskriminantu, avšak tentokrát v předpokladu omezíme součet proměnných, nikoli každou proměnnou zvlášť. Před každou větou si opět zadefinujeme systém ortogonálních polynomů, který bude potřeba k formulaci věty anebo bude s formulací nějak souviset (vlastnosti zdefinovaných polynomů jsme rovněž převzali z článku [6]). Opět předpokládáme  $n \geq 2$ .

**Definice 3.14.** *Hermitovy polynomy* definujeme jako

$$H_n(x) = (-1)^n e^{\frac{x^2}{2}} \frac{d^n}{dx^n} (e^{-\frac{x^2}{2}}).$$

Ekvivalentně,

$$H_n(x) = \frac{x}{1!} - \binom{n-1}{1} \frac{x^2}{2!} + \binom{n-1}{2} \frac{x^3}{3!} - \cdots + (-1)^{n+1} \frac{x^n}{n!}.$$

**Věta 3.15** (Stieltjesova věta II). *Pro reálná čísla  $x_1, x_2, \dots, x_n$  splňující  $x_1^2 + \cdots + x_n^2 \leq 1$  je maximum  $M'_n$  výrazu  $\tilde{\Delta}(x_1, x_2, \dots, x_n)$  rovno*

$$M'_n = \frac{2^2 \cdot 3^3 \cdots n^n}{(n^2 - n)^{(n^2 - n)/2}}.$$

*Toto maximum je nabyto právě tehdy, když jsou  $x_i \sqrt{n^2 - n}$  pro  $1 \leq i \leq n$  kořeny  $n$ -tého Hermitova polynomu.*

*Důkaz.* Je hodně technický, nebudeme jej uvádět. Pouze poznamenejme, že prvním krokem je vyjádření proměnných pomocí polárních souřadnic:

$$x_1 = \cos \mu_1, x_2 = \sin \mu_1 \cos \mu_2, \dots, x_{n-1} = \sin \mu_1 \dots \sin \mu_{n-2} \cos \mu_{n-1},$$

$x_n = \sin \mu_1 \dots \sin \mu_{n-2} \sin \mu_{n-1}$ . Dále se maximum diskriminantu hledá pro proměnné  $\mu_1, \dots, \mu_{n-1}$ . Důkaz najdete v článku [6, Par.2, Th.II].  $\square$

**Definice 3.16.** *Laguerrovy polynomy* definujeme jako

$$L_n(x) = \frac{e^x}{n!} \frac{d^n}{dx^n} (x^n e^{-x}).$$

**Poznámka 3.17.** Polynom  $G_n$  definovaný jako  $G_n(x) = \frac{x}{1!} - \binom{n-1}{1} \frac{x^2}{2!} + \binom{n-1}{2} \frac{x^3}{3!} - \dots + (-1)^{n+1} \frac{x^n}{n!}$  splňuje  $G_n = \int_0^x L_{n-1} dx$ .

**Věta 3.18** (Stieltjesova věta III). *Pro nezáporná reálná čísla  $x_1, x_2, \dots, x_n$  splňující  $x_1 + \dots + x_n \leq 1$  je maximum  $M_n''$  výrazu  $\tilde{\Delta}(x_1, x_2, \dots, x_n)$  rovno*

$$M_n'' = \frac{2^2 \cdot 3^3 \dots n^n \cdot 2^2 \cdot 3^3 \dots (n-1)^{(n-1)}}{(n^2 - n)^{n^2 - n}}.$$

*Toto maximum je nabyto právě tehdy, když jsou  $(n^2 - n)x_i$  pro  $1 \leq i \leq n$  kořeny polynomu*

$$G_n(x) = \frac{x}{1!} - \binom{n-1}{1} \frac{x^2}{2!} + \binom{n-1}{2} \frac{x^3}{3!} - \dots + (-1)^{n+1} \frac{x^n}{n!}.$$

*Důkaz.* Opět využívá goniometrických substitucí, nebudeme jej uvádět. Najdete jej v článku [6, Par.3, Th.III].  $\square$

### 3.4 Odhad stopy celistvého prvku

Dostáváme se k aplikaci jedné ze Stieltjesových vět. Sestrojíme dolní odhad stopy druhé mocniny celistvého prvku, v němž figuruje diskriminant celistvého prvku.

**Tvrzení 3.19.** *Nechť  $F$  je totálně reálné číselné těleso stupně  $[F : \mathbb{Q}] = N \geq 2$ . Pokud  $\beta \in \mathcal{O}_F$ , pak*

$$\mathrm{Tr}_{F/\mathbb{Q}}(\beta^2) \geq c_N \Delta_{F/\mathbb{Q}}(\beta)^{2/(N^2-N)},$$

kde

$$c_N = \frac{N^2 - N}{(2^2 \cdot 3^3 \cdot 4^4 \dots (N-1)^{N-1} \cdot N^N)^{2/(N^2-N)}}.$$

*Důkaz.* Z věty 3.15 máme, že pro reálná čísla  $x_1, x_2, \dots, x_N$  splňující  $x_1^2 + \dots + x_N^2 \leq 1$  je maximum  $M'_N$  výrazu  $\tilde{\Delta}(x_1, x_2, \dots, x_N) = \prod_{i < j} (x_i - x_j)^2$  rovno

$$M'_N = \frac{2^2 \cdot 3^3 \dots N^N}{(N^2 - N)^{(N^2-N)/2}},$$

což je při našem označení rovno  $c_N^{-(N^2-N)/2}$ . Označme  $x_i = \frac{\sigma_i(\beta)}{\sqrt{\mathrm{Tr}(\beta^2)}}$ , kde

$\sigma_1, \dots, \sigma_N$  jsou vnoření  $F \hookrightarrow \mathbb{C}$ . Protože platí

$$x_1^2 + \dots + x_N^2 = \frac{\sigma_1(\beta)^2 + \dots + \sigma_N(\beta)^2}{\mathrm{Tr}(\beta^2)} = \frac{\sigma_1(\beta^2) + \dots + \sigma_N(\beta^2)}{\mathrm{Tr}(\beta^2)} = \frac{\mathrm{Tr}(\beta^2)}{\mathrm{Tr}(\beta^2)} = 1,$$

můžeme použít Stieltjesův odhad pro výraz

$$\begin{aligned}\tilde{\Delta}(x_1, x_2, \dots, x_N) &= \prod_{i < j} (x_i - x_j)^2 = \prod_{i < j} \left( \frac{\sigma_i(\beta)}{\sqrt{\text{Tr}(\beta^2)}} - \frac{\sigma_j(\beta)}{\sqrt{\text{Tr}(\beta^2)}} \right)^2 = \\ &= \frac{\tilde{\Delta}(\sigma_1(\beta), \dots, \sigma_N(\beta))}{\text{Tr}(\beta^2)^{\binom{n}{2}}},\end{aligned}$$

tedy dostáváme

$$\frac{\tilde{\Delta}(\sigma_1(\beta), \dots, \sigma_N(\beta))}{\text{Tr}(\beta^2)^{\binom{n}{2}}} \leq c_N^{-(N^2-N)/2},$$

neboli

$$\text{Tr}(\beta^2) \geq c_N \tilde{\Delta}(\sigma_1(\beta), \dots, \sigma_N(\beta))^{2/(N^2-N)}.$$

Konečně,  $\tilde{\Delta}(\sigma_1(\beta), \dots, \sigma_N(\beta)) = \Delta_{F/\mathbb{Q}}(\beta)$  z tvrzení 1.20. □

# 4. Univerzální formy v tělesech stupně $2n$

## 4.1 Permutační grupy

Připomeňme si, že grupě všech permutací nějaké konečné množiny s operací skládání a identitou jakožto neutrálním prvkem říkáme *symetrická grupa*. Symetrickou grupu na množině  $\{1, \dots, n\}$  budeme dále značit  $S_n$ . Prvky  $\pi, \sigma \in S_n$  nazveme konjugované, pokud existuje prvek  $\rho \in S_n$  takový, že  $\pi = \rho\sigma\rho^{-1}$ . Platí:

- Permutace  $\pi, \sigma$  jsou v  $S_n$  konjugované právě tehdy, když jsou stejného typu (tj. mají stejný počet cyklů každé délky).
- Pro permutace  $\pi, \sigma \in S_n$ , kde  $\pi = (a_1, \dots, a_k)(b_1, \dots, b_l) \dots$ , platí  $\sigma\pi\sigma^{-1} = (\sigma(a_1), \dots, \sigma(a_k))(\sigma(b_1), \dots, \sigma(b_l)) \dots$ .

Dále necht  $A_n \leq S_n$  značí grupu všech sudých permutací na  $\{1, \dots, n\}$  a  $C_2$  cyklickou grupu řádu 2 obsahující prvky  $1, u$ . Grupou  $S_{n-1}$  uvažujeme jako podgrupu  $S_n$  tvořenou všemi permutacemi na  $\{1, \dots, n\}$ , které fixují prvek  $n$ . V následujících lemmatech předpokládáme, že  $n \geq 2$ .

**Lemma 4.1.** *Jediná podgrupa  $S_n$  indexu 2 je  $A_n$ .*

*Důkaz.* Mějme podgrupu  $H \leq S_n$  indexu 2. Potom je  $H$  normální podgrupa a  $S_n/H \simeq C_2$ . Odtud máme s použitím první věty o isomorfismu surjektivní homomorfismus  $\varphi : S_n \rightarrow C_2$  s jádrem  $H$ . Pro každé dvě transpozice  $t_1, t_2$  máme  $t_1 = \sigma t_2 \sigma^{-1}$  pro nějakou  $\sigma \in S_n$ , a odtud  $\varphi(t_1) = \varphi(\sigma t_2 \sigma^{-1}) = \varphi(t_2)$ . Protože  $S_n$  je generována transpozicemi,  $C_2$  musí být generována  $\varphi(t)$  pro libovolnou transpozici  $t$ , čili  $\varphi(t) = u$ . Grupa  $H$  jakožto jádro  $\varphi$  tedy obsahuje všechny sudé permutace a z porovnání velikostí již  $H = A_n$ .  $\square$

**Lemma 4.2.**  *$S_{n-1}$  je maximální podgrupa v  $S_n$ .*

*Důkaz.* Necht  $S_{n-1} \subsetneq G \leq S_n$  a  $G$  obsahuje permutaci obsahující cyklus  $(a, b, \dots, n)$ , označme ji  $\sigma$ . Potom pro  $\pi \in S_{n-1}$ ,  $\pi(a) = b$  máme  $\pi \circ \sigma = (b, n)(\dots)$ . Složením s vhodnou permutací z  $S_{n-1}$  dostaneme  $(b, n)$ , složením s další vhodnou permutací z  $S_{n-1}$  dostaneme libovolnou transpozici  $(c, n)$  a ty společně s  $S_{n-1}$  generují celou  $S_n$ .  $\square$

**Lemma 4.3.** *Pokud grupa  $G$  splňuje  $\{1\} \times S_{n-1} \subsetneq G \subsetneq C_2 \times S_n$ , pak  $G = \{1\} \times S_n$  nebo  $G = C_2 \times S_{n-1}$ .*

*Důkaz.* Mějme grupu  $G$  splňující  $\{1\} \times S_{n-1} \subsetneq G \leq C_2 \times S_n$ .

- Pokud  $(1, \pi) \in G$  pro  $\pi \in S_n \setminus S_{n-1}$ , pak  $G \supseteq \{1\} \times S_n$  z lemmatu 4.2.
- Pokud  $(u, \pi) \in G$  pro  $\pi \in S_{n-1}$ , pak  $G \supseteq C_2 \times S_{n-1}$ .

- Pokud  $(u, \pi) \in G$  pro  $\pi \in S_n \setminus S_{n-1}$ , označíme cyklus v  $\pi$  obsahující  $n$  jako  $(a, \dots, b, n)$  a vezmeme permutaci  $\sigma = (b, c) \in S_{n-1}$ . Potom

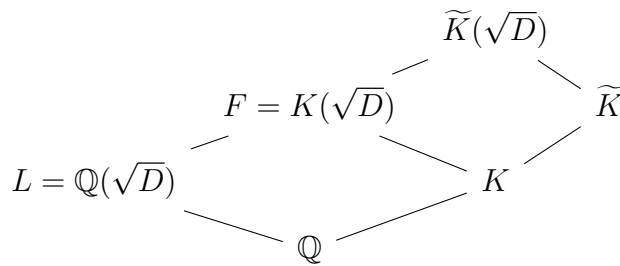
$$(u, \pi)(1, \sigma)(u, \pi^{-1}) = (1, \tau), \text{ kde } \tau \in S_n \setminus S_{n-1},$$

neboť z pozorování o konjugacích máme  $\pi\sigma\pi^{-1} = (\pi(b), \pi(c)) = (n, d)$  pro nějaké  $d \neq n$ , neboli  $\pi\sigma\pi^{-1} \in S_n \setminus S_{n-1}$ . Tedy opět z lemmatu 4.2 dostáváme  $\{1\} \times S_n \subseteq G$ . Dále pro jakýkoliv  $(u, \nu) \in \{u\} \times S_n$  platí  $(u, \nu) = (u, \pi)(1, \pi^{-1}\nu) \in G$ , tedy také  $\{u\} \times S_n \subseteq G$ , což už implikuje  $G = C_2 \times S_n$ .

Tedy jsme dokázali, že jediné podgrupy  $C_2 \times S_n$  obsahující  $\{1\} \times S_{n-1}$  jsou  $\{1\} \times S_{n-1}$ ,  $\{1\} \times S_n$ ,  $C_2 \times S_{n-1}$  a  $C_2 \times S_n$ . □

## 4.2 Galoisovy grupy

Dokážeme několik lemmat, která využijeme při důkazu hlavní věty. V celé této sekci uvažujeme tuto situaci: ať  $K$  je číselné těleso,  $[K : \mathbb{Q}] = n$ ,  $\widetilde{K}$  Galoisův uzávěr  $K$ ,  $\text{Gal}(\widetilde{K}/\mathbb{Q}) \simeq S_n$  a  $D > 1$  je bezčtvercové a nesoudělné s  $\text{disc}_K$ .



- $D > 0$  bezčtvercové, nesoudělné s  $\text{disc}_K$
- $[K : \mathbb{Q}] = n$
- $\widetilde{K}$  je Galoisův uzávěr  $K$
- $\text{Gal}(\widetilde{K}/\mathbb{Q}) \simeq S_n$

**Lemma 4.4.** *Existuje ireducibilní polynom  $f \in \mathbb{Q}[x]$  stupně  $n$  takový, že  $K$  je kořenovým nadtělesem a  $\widetilde{K}$  je rozkladovým nadtělesem tohoto polynomu. To znamená, že  $K = \mathbb{Q}(a_n)$ ,  $\widetilde{K} = \mathbb{Q}(a_1, \dots, a_n)$  pro  $a_1, \dots, a_n$ , kořeny  $f$ .*

*Důkaz.*  $K$  je jakožto separabilní rozšíření konečného stupně jednoduché (věta 1.5), a tedy  $K = \mathbb{Q}(a_n)$  pro nějaké  $a_n \notin \mathbb{Q}$ . Minimální polynom  $f = m_{a_n, \mathbb{Q}}$  pak má stupeň  $n$  dle věty 1.1. Protože má  $f$  v  $\widetilde{K}$  kořen  $a_n$  a  $\widetilde{K}$  je Galoisův uzávěr  $K$ , tedy konkrétně normální rozšíření  $\mathbb{Q}$ , má  $f$  v  $\widetilde{K}$  všechny kořeny, kterých je  $n$  ze separability  $\widetilde{K}$ . □

**Značení.** Ve zbytku sekce budeme uvažovat situaci z lemmatu 4.4, tedy  $f$  značí polynom z tohoto lemmatu,  $a_1, \dots, a_n$  jeho kořeny,  $K = \mathbb{Q}(a_n)$ ,  $\widetilde{K} = \mathbb{Q}(a_1, \dots, a_n)$ .

**Lemma 4.5.**  $\mathbb{Q}(\sqrt{D}) \cap \widetilde{K} = \mathbb{Q}$ , neboli  $\sqrt{D} \notin \widetilde{K}$ .

*Důkaz.* Nejprve dokážeme, že  $\widetilde{K}$  má právě jedno kvadratické podtěleso. Pro kvadratické podtěleso  $M$  platí  $[M : \mathbb{Q}] = 2$ , a tedy z Galoisovy korespondence  $[\text{Gal}(\widetilde{K}/\mathbb{Q}) : \text{Gal}(\widetilde{K}/M)] = 2$ . Protože  $\text{Gal}(\widetilde{K}/\mathbb{Q}) \simeq S_n$  a jediná podgrupa indexu 2 v  $S_n$  je  $A_n$  dle lemmatu 4.1, máme jediné kvadratické podtěleso  $M = \text{Fix}(\widetilde{K}, A_n)$ .

Nyní ukážeme, že  $M = \mathbb{Q}(\sqrt{\text{disc}_K})$ . Zvolme prvek  $\alpha \in \mathcal{O}_K \setminus \mathbb{Z}$ . Potom  $\Delta_{K/\mathbb{Q}}(\alpha) = t^2 \cdot \text{disc}_K$ , kde  $t$  je determinant matice vyjádření prvků  $1, \alpha, \dots, \alpha^{n-1}$  pomocí celistvé báze  $\mathcal{O}_K$  dle odstavce za definicí 1.22, a odtud

$$\mathbb{Q}(\sqrt{\text{disc}_K}) = \mathbb{Q}(\sqrt{\Delta(\alpha)}).$$

Protože z lemmatu 1.20 máme po odmocnění  $\sqrt{\Delta(\alpha)} = \pm \prod_{i < j} (\sigma_i(\alpha) - \sigma_j(\alpha))$ , pro permutace  $\pi$  množiny  $\{\sigma_1, \dots, \sigma_n\}$  se sudým počtem transpozic  $2s$  platí

$$\pm \prod_{i < j} (\pi(\sigma_i)(\alpha) - \pi(\sigma_j)(\alpha)) = \pm \prod_{i < j} (-1)^{2s} (\sigma_i(\alpha) - \sigma_j(\alpha)) = \sqrt{\Delta(\alpha)},$$

odtud  $\sqrt{\Delta(\alpha)} \in \text{Fix}(\widetilde{K}, A_n)$ , neboli  $\mathbb{Q}(\sqrt{\Delta(\alpha)}) \subseteq \text{Fix}(\widetilde{K}, A_n)$ . Protože však obě tato tělesa jsou stupně 2, máme rovnost, tedy  $M = \mathbb{Q}(\sqrt{\Delta(\alpha)}) = \mathbb{Q}(\sqrt{\text{disc}_K})$ .

Konečně,  $\mathbb{Q}(\sqrt{D}) \neq \mathbb{Q}(\sqrt{\text{disc}_K})$  díky podmínce nesoudělnosti  $D$  a  $\text{disc}_K$ , proto  $\mathbb{Q}(\sqrt{D}) \not\subseteq \widetilde{K}$ .  $\square$

**Lemma 4.6.**  $\widetilde{K}(\sqrt{D})$  je Galoisovo rozšíření  $\mathbb{Q}$  stupně  $2n!$ .

*Důkaz.* Podívejme se nejprve na stupeň rozšíření. Protože  $\sqrt{D} \notin \widetilde{K} = \mathbb{Q}(a_1, \dots, a_n)$  z lemmatu 4.5, má minimální polynom pro  $\sqrt{D}$  nad  $\mathbb{Q}(a_1, \dots, a_n)$  stupeň minimálně 2. Zároveň  $\sqrt{D}$  je kořenem  $x^2 - D$ , tudíž z tvrzení 1.1 máme

$$[\mathbb{Q}(a_1, \dots, a_n, \sqrt{D}) : \mathbb{Q}(a_1, \dots, a_n)] = \deg(m_{\sqrt{D}, \widetilde{K}}) = 2.$$

Dále z naší volby  $K$  tak, že  $\text{Gal}(\widetilde{K}/\mathbb{Q}) \simeq S_n$ , a věty 1.8 vyplývá, že

$$[\mathbb{Q}(a_1, \dots, a_n) : \mathbb{Q}] = |S_n| = n!.$$

Celkem užitím věty o iterovaném rozšíření těles dostáváme

$$[\widetilde{K}(\sqrt{D}) : \mathbb{Q}] = [\mathbb{Q}(a_1, \dots, a_n, \sqrt{D}) : \mathbb{Q}(a_1, \dots, a_n)] [\mathbb{Q}(a_1, \dots, a_n) : \mathbb{Q}] = 2 \cdot n!.$$

Rozšíření  $\widetilde{K}(\sqrt{D}) > \mathbb{Q}$  je normální, neboť je rozkladovým nadtělesem množiny polynomů  $\{f, x^2 - D\}$ . Konečný stupeň rozšíření máme z předchozího výpočtu. Konečně,  $\widetilde{K}(\sqrt{D})$  je jakožto algebraické rozšíření  $\mathbb{Q}$  separabilní.  $\square$

**Lemma 4.7.**  $\text{Gal}(\widetilde{K}/K) \simeq S_{n-1}$ .

*Důkaz.* Protože  $\widetilde{K} = K(a_1, \dots, a_{n-1})$ , je každý  $K$ -automorfismus tělesa  $\widetilde{K}$  popsán obrazy prvků  $a_1, \dots, a_{n-1}$ , proto  $\text{Gal}(\widetilde{K}/K) \hookrightarrow S_{n-1}$ . Každé zobrazení  $\widetilde{K} \rightarrow \widetilde{K}$  určené nějakou permutací na množině  $\{a_1, \dots, a_{n-1}\}$  je automorfismus na  $\widetilde{K}$ , neboť  $S_{n-1} \subseteq S_n \simeq \text{Gal}(\widetilde{K}/\mathbb{Q})$ . Dále je každé takové zobrazení  $K$ -homomorfismus, neboť je to konkrétně  $\mathbb{Q}$ -homomorfismus a  $a_n$  zobrazí na  $a_n$ . Celkem máme, že každá permutace na  $\{a_1, \dots, a_{n-1}\}$  nám dává  $K$ -automorfismus  $\widetilde{K}$ , odtud  $\text{Gal}(\widetilde{K}/K) \simeq S_{n-1}$ .  $\square$

**Lemma 4.8.**  $\text{Gal}(\widetilde{K}(\sqrt{D})/K(\sqrt{D})) \simeq \{1\} \times S_{n-1}$ .

*Důkaz.* analogický důkazu lemmatu 4.7.  $\square$

**Lemma 4.9.**  $\text{Gal}(\widetilde{K}(\sqrt{D})/\mathbb{Q}) \simeq \text{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q}) \times \text{Gal}(\widetilde{K}/\mathbb{Q}) \simeq C_2 \times S_n$ .

*Důkaz.* Protože  $|\text{Gal}(\widetilde{K}(\sqrt{D})/\mathbb{Q})| = [\widetilde{K}(\sqrt{D}) : \mathbb{Q}] = 2n!$  (lemma 4.6), tak každý  $\mathbb{Q}$ -homomorfismus  $\varphi_{i_1, \dots, i_n, \varepsilon} : \widetilde{K}(\sqrt{D}) \mapsto \widetilde{K}(\sqrt{D})$  definovaný předpis

$$\begin{aligned} a_1 &\mapsto a_{i_1} \\ &\vdots \\ a_n &\mapsto a_{i_n} \\ \sqrt{D} &\mapsto \varepsilon\sqrt{D} \end{aligned}$$

pro  $\{i_1, \dots, i_n\} = \{1, \dots, n\}, \varepsilon = \pm 1$ , je korektně definovaný prvek  $\text{Gal}(\widetilde{K}(\sqrt{D})/\mathbb{Q})$  (každý prvek  $a_i$  se musí zobrazit na kořen polynomu  $f$ ,  $\sqrt{D}$  se musí zobrazit na kořen  $x^2 - D$  a díky velikosti Galoisovy grupy jakákoliv možnost funguje). Definujme zobrazení z  $\text{Gal}(\widetilde{K}(\sqrt{D})/\mathbb{Q})$  do  $\text{Gal}(\mathbb{Q}(\sqrt{D})/\mathbb{Q}) \times \text{Gal}(\widetilde{K}/\mathbb{Q})$  předpisem  $\varphi_{i_1, \dots, i_n, \varepsilon} \mapsto \varphi_\varepsilon \times \varphi_{i_1, \dots, i_n}$ , kde  $\varphi_\varepsilon, \varphi_{i_1, \dots, i_n}$  jsou definována analogicky jako  $\varphi_{i_1, \dots, i_n, \varepsilon}$ . Toto zobrazení je bijekce; pokud se  $\varphi, \psi \in \text{Gal}(\widetilde{K}(\sqrt{D})/\mathbb{Q})$  liší v některém z indexů  $\{i_1, \dots, i_n, \varepsilon\}$ , pak se liší i příslušné složky jejich obrazů obsahující tento index. Surjektivita plyne z podmínky  $\sqrt{D} \notin \mathbb{Q}(a_1, \dots, a_n)$ , tedy faktu, že každé  $\varphi \in \text{Gal}(\widetilde{K}(\sqrt{D})/\mathbb{Q})$  můžeme zvlášť definovat na množině  $\{a_1, \dots, a_{n-1}\}$  a zvlášť na  $\sqrt{D}$ . Popsané zobrazení je navíc homomorfismus, neboť  $\varphi_{\pi_1(1, \dots, n), \varepsilon_1} \circ \varphi_{\pi_2(1, \dots, n), \varepsilon_2} = \varphi_{\pi_1 \circ \pi_2(1, \dots, n), \varepsilon_1 \varepsilon_2}$ .  $\square$

Není jasné, že situace z této sekce může nastat. Naštěstí nám to ale zaručuje následující věta:

**Věta 4.10.** *Pro každá  $n, D, X \geq 2$  existuje nekonečně mnoho totálně reálných číselných těles  $K$  stupně  $n = [K : \mathbb{Q}]$  takových, že  $\text{disc}_K > X$  je nesoudělný s  $D$  a jejich Galoisův uzávěr  $\widetilde{K}$  má Galoisovu grupu  $\text{Gal}(\widetilde{K}/\mathbb{Q}) \simeq S_n$ .*

*Důkaz.* článek [5, Prop. 3]. Důkaz by byl nad rámec bakalářské práce, proto ho neuvádíme.  $\square$

### 4.3 Důkaz hlavní věty

**Věta 4.11** (Hlavní věta). *Pro všechna přirozená čísla  $m, n$  existuje nekonečně mnoho totálně reálných číselných těles  $F$  stupně  $[F : \mathbb{Q}] = 2n$ , nad kterými je počet proměnných každé univerzální kvadratické formy alespoň  $m$ .*

*Důkaz.* Pro  $n = 1$  se odvolajme na větu 1.28 a dále předpokládejme  $n \geq 2$ . Dle tvrzení 1.30 můžeme volit těleso  $L = \mathbb{Q}(\sqrt{D})$  takové, že v něm existuje  $m$  totálně kladných ortogonálních prvků  $a_1, \dots, a_m$ . Označme

$$T = 4 \max\{\text{Tr}_{L/\mathbb{Q}}(a_i a_j) \mid 1 \leq i < j \leq m\}.$$

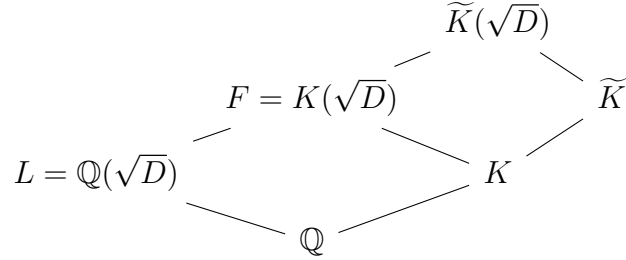
Položme  $F = K(\sqrt{D})$ , kde  $[K : \mathbb{Q}] = n$ , Galoisův uzávěr  $\widetilde{K}$  tělesa  $K$  má Galoisovu grupu  $\text{Gal}(\widetilde{K}/\mathbb{Q}) \simeq S_n$ ,  $\text{disc}_K$  je nesoudělný s  $D$  a

$$\text{disc}_K > B = \max\left\{ \left(\frac{nT}{c_{2n}}\right)^{(2n^2-n)/2}, \left(\frac{nT}{2c_n}\right)^{(n^2-n)/2} \right\},$$

přičemž  $c_N$  bude v tomto důkazu vždy značit konstantu z tvrzení 3.19. Dle tvrzení 4.10 existuje takových těles  $K$  nekonečně mnoho, z máme i nekonečný počet těles  $F$ .

Z lemmatu 4.5 máme  $\sqrt{D} \notin \widetilde{K}$ , tudíž  $\sqrt{D} \notin K$ , a proto  $[F : \mathbb{Q}] = [K(\sqrt{D}) : K][K : \mathbb{Q}] = 2n$ .

Nyní ukážeme, že v takových tělesech  $F$  má každá univerzální kvadratická forma alespoň  $m$  proměnných. Necht' naše zvolené totálně kladné prvky  $a_1, a_2, \dots, a_m \in \mathcal{O}_L$  splňují  $4a_i a_j \succeq b^2$  pro nějaká  $1 \leq i < j \leq m$  a pro nějaké  $b \in \mathcal{O}_F$ . Naším cílem je ukázat, že  $b = 0$  a moct tak použít tvrzení 1.29.



Z definice stopy prvku máme, že  $4a_i a_j \succeq b^2$  implikuje  $4\text{Tr}_{F/\mathbb{Q}}(a_i a_j) \geq \text{Tr}_{F/\mathbb{Q}}(b^2)$ . Levou stranu nerovnosti odhadneme shora, pravou zdola:

- Podle tvrzení 1.17 máme  $\text{Tr}_{F/\mathbb{Q}}(a_i a_j) = n\text{Tr}_{L/\mathbb{Q}}(a_i a_j)$ , neboť  $[F : L] = \frac{[F:\mathbb{Q}]}{[L:\mathbb{Q}]} = \frac{2n}{2} = n$ . Tedy  $nT \geq 4n\text{Tr}_{L/\mathbb{Q}}(a_i a_j) = 4\text{Tr}_{F/\mathbb{Q}}(a_i a_j)$ .
- Z tvrzení 3.19 dostaneme  $\text{Tr}_{F/\mathbb{Q}}(b^2) \geq c_{2n}\Delta(b)^{2/((2n)^2-(2n))}$ .

Odhad  $\text{disc}_K$  můžeme přepsat jako

$$\text{disc}_K > B = \max_M \left( \left( \frac{neT}{2c_{ne}} \right)^{(n^2e-n)/2} \right),$$

kde  $M = F = K(\sqrt{D})$  nebo  $M = K$ ,  $e = [M : K]$ . Konkrétně,

$$B = \max\{B_F, B_K\}, \text{ kde } B_F = \left( \frac{nT}{c_{2n}} \right)^{(2n^2-n)/2}, B_K = \left( \frac{nT}{2c_n} \right)^{(n^2-n)/2}.$$

Z lemmatu 1.23 máme  $\text{disc}_F \mid \Delta_{F/\mathbb{Q}}(\alpha) \quad \forall \alpha \in \mathcal{O}_F$ . Pokud  $\Delta_{F/\mathbb{Q}}(b) \neq 0$ , dostáváme  $\Delta_{F/\mathbb{Q}}(b) \geq \text{disc}_F$  a sérii nerovností

$$\begin{aligned}
 nT &\geq 4n\text{Tr}_{L/\mathbb{Q}}(a_i a_j) = 4\text{Tr}_{F/\mathbb{Q}}(a_i a_j) \geq \text{Tr}_{F/\mathbb{Q}}(b^2) \geq c_{2n}\Delta_{F/\mathbb{Q}}(b)^{2/((2n)^2-(2n))} \geq \\
 &\geq c_{2n}\text{disc}_F^{1/(2n^2-n)} \geq c_{2n}\text{disc}_K^{2/(2n^2-n)} > c_{2n}B_F^{2/(2n^2-n)} = c_{2n} \left( \frac{nT}{c_{2n}} \right) = nT
 \end{aligned}$$

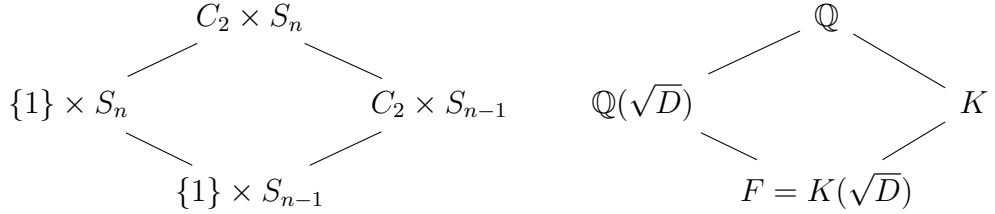
( $\text{disc}_F \geq \text{disc}_K^2$  z lemmatu 1.24), což vede ke sporu. Proto nutně  $\Delta_{F/\mathbb{Q}}(b) = 0$ , neboli dle tvrzení 1.21 leží  $b$  v nějakém netriviálním podtělese  $F$ .

Nyní s využitím lemmat ze sekcí 4.1, 4.2 a Galoisovy korespondence ukážeme, že netriviálními podtělesy  $F$  jsou pouze  $\mathbb{Q}, \mathbb{Q}(\sqrt{D})$  a  $K$ . Dle lemmat 4.9 a 4.8 máme pro těleso  $\widetilde{K}(\sqrt{D})$  a jeho podtěleso  $K(\sqrt{D})$

$$\text{Gal}(\widetilde{K}(\sqrt{D})/\mathbb{Q}) \simeq C_2 \times S_n,$$

$$\text{Gal}(\widetilde{K}(\sqrt{D})/K(\sqrt{D})) \simeq \{1\} \times S_{n-1}.$$

Protože  $\widetilde{K}(\sqrt{D})$  je Galoisovo rozšíření  $\mathbb{Q}$ , z Galoisovy korespondence musejí mezi tělesy těles  $\mathbb{Q}$  a  $K(\sqrt{D})$  korespondovat s mezigrupami grup  $\{1\} \times S_{n-1}$  a  $C_2 \times S_n$  (jakožto tělesa, která jsou těmito grupami fixována). V lemmatu 4.3 jsme dokázali, že jediné netriviální mezigrupy  $\{1\} \times S_{n-1}$  a  $C_2 \times S_n$  jsou  $\{1\} \times S_n$  a  $C_2 \times S_{n-1}$ . Proto jsou  $\mathbb{Q}(\sqrt{D}), K$  jedinými netriviálními mezitělesy  $\mathbb{Q}$  a  $F$  (konkrétně,  $\mathbb{Q}(\sqrt{D})$  je fixováno grupou  $\{1\} \times S_n$  a  $K$  je fixováno grupou  $C_2 \times S_{n-1}$ ).



Dostali jsme, že  $b$  leží buď v  $\mathbb{Q}(\sqrt{D})$ , anebo v  $K$ . První případ je vyřešen v článku [4], kde je věta dokázána pro kvadratická rozšíření.

Vyšetříme případ, kdy  $b \in K$ . Provedeme stejnou sérii odhadů jako výše, akorát pro  $M = K$ . Pokud  $\Delta_{K/\mathbb{Q}}(b) \neq 0$ , dostáváme

$$\begin{aligned}
 nT &\geq 4n \text{Tr}_{L/\mathbb{Q}}(a_i a_j) = 4 \text{Tr}_{F/\mathbb{Q}}(a_i a_j) \geq \text{Tr}_{F/\mathbb{Q}}(b^2) = 2 \text{Tr}_{K/\mathbb{Q}}(b^2) \\
 &\geq 2c_n \Delta_{K/\mathbb{Q}}(b)^{2/(n^2-n)} \geq 2c_n \text{disc}_K^{2/(n^2-n)} > 2c_n B_K^{2/(n^2-n)} = 2c_n \left( \frac{nT}{2c_n} \right) = nT,
 \end{aligned}$$

což opět vede ke sporu. Proto  $\Delta_{K/\mathbb{Q}}(b) = 0$ , neboli  $b$  leží v nějakém netriviálním podtělese  $K$ , což může být jedině  $\mathbb{Q}$  z předchozího vyšetření podtěles  $F$ . Speciálně,  $b \in \mathbb{Q}(\sqrt{D})$ , tedy se znovu odvoláme na článek [4], kde je tento případ vyřešen.  $\square$

## 4.4 Odhad diskriminantu z důkazu

Závěrem provedme diskuzi k volbě spodního odhadu pro  $\text{disc}_K$ . V důkazu volíme  $B = \max\{B_K, B_F\}$ , kde

$$\begin{aligned}
 B_K &= \left( \frac{nT}{2c_n} \right)^{(n^2-n)/2} = T^{\frac{n^2-n}{2}} \frac{(2^2 \cdot 3^3 \cdot 4^4 \cdots (n-1)^{n-1} \cdot n^n)}{(2n-2)^{(n^2-n)/2}}, \\
 B_F &= \left( \frac{nT}{c_{2n}} \right)^{(2n^2-n)/2} = T^{\frac{2n^2-n}{2}} \frac{(2^2 \cdot 3^3 \cdot 4^4 \cdots (2n-1)^{2n-1} \cdot (2n)^{2n})^{1/2}}{(4n-2n)^{(2n^2-n)/2}}.
 \end{aligned}$$

Zdá se ale, že ve skutečnosti  $B_K < B_F$  pro všechna  $n \geq 2$ , pojdme si vysvětlit, proč. Nerovnost přepíšeme na

$$T^{\frac{n^2-n}{2}} \frac{(2^2 \cdot 3^3 \cdot 4^4 \cdots n^n)}{(2n-2)^{(n^2-n)/2}} < T^{\frac{2n^2-n}{2}} \frac{(2^2 \cdot 3^3 \cdot 4^4 \cdots (2n)^{2n})^{1/2}}{(4n-2n)^{(2n^2-n)/2}},$$

což upravíme na

$$\frac{2^2 \cdot 3^3 \cdot 4^4 \cdots (n-1)^{n-1} \cdot n^n}{\sqrt{2^2 \cdot 3^3 \cdot 4^4 \cdots (2n-1)^{2n-1} \cdot (2n)^{2n}}} \cdot \frac{(2n-1)^{(2n^2-n)/2}}{(n-1)^{(n^2-n)/2}} \cdot 2^{\frac{n^2}{2}} < T^{\frac{n^2}{2}},$$

$$\left( \frac{(2^2 \cdot 3^3 \cdot 4^4 \cdots (n-1)^{n-1} \cdot n^n)^2}{2^2 \cdot 3^3 \cdot 4^4 \cdots (2n-1)^{2n-1} \cdot (2n)^{2n}} \right)^{\frac{1}{n^2}} \cdot \frac{(2n-1)^{2-\frac{1}{n}}}{(n-1)^{1-\frac{1}{n}}} \cdot 2 < T.$$

Protože  $T = 4 \max\{\text{Tr}_{L/\mathbb{Q}}(a_i a_j) \mid 1 \leq i < j \leq m\}$  a  $a_i \in \mathcal{O}_L^+$  pro všechna  $1 \leq i \leq m$ , lemma 1.16 nám dává  $T \geq 4$ . Dále učiníme odhad

$$\frac{(2n-1)^{2-\frac{1}{n}}}{(n-1)^{1-\frac{1}{n}}} \leq \frac{(2n)^{2-\frac{1}{n}}}{n^{1-\frac{1}{n}}},$$

který je zřejmý z přepsání

$$\left( \frac{n}{n-1} \right)^{1-\frac{1}{n}} \leq \left( \frac{2n}{2n-1} \right)^{2-\frac{1}{n}}.$$

Tedy k důkazu nerovnosti  $B_K < B_F$  pro všechna  $n \geq 2$  by nám stačilo dokázat

$$\begin{aligned} & \left( \frac{(2^2 \cdot 3^3 \cdot 4^4 \cdots (n-1)^{n-1} \cdot n^n)^2}{2^2 \cdot 3^3 \cdot 4^4 \cdots (2n-1)^{2n-1} \cdot (2n)^{2n}} \right)^{\frac{1}{n^2}} \cdot \frac{(2n)^{2-\frac{1}{n}}}{n^{1-\frac{1}{n}}} \cdot 2 < 4, \\ & \left( \frac{(2^2 \cdot 3^3 \cdot 4^4 \cdots (n-1)^{n-1} \cdot n^n)^2}{2^2 \cdot 3^3 \cdot 4^4 \cdots (2n-1)^{2n-1} \cdot (2n)^{2n}} \right)^{\frac{1}{n^2}} \cdot 2^{2-\frac{1}{n}} \cdot n < 2. \end{aligned}$$

Označme

$$\lambda(n) = \left( \frac{(2^2 \cdot 3^3 \cdot 4^4 \cdots (n-1)^{n-1} \cdot n^n)^2}{2^2 \cdot 3^3 \cdot 4^4 \cdots (2n-1)^{2n-1} \cdot (2n)^{2n}} \right)^{\frac{1}{n^2}} \cdot 2^{2-\frac{1}{n}} \cdot n.$$

Dokážeme, že  $\lim_{n \rightarrow \infty} \lambda(n) < 2$ . Pro hyperfaktoriál

$$H(n) = 2^2 \cdot 3^3 \cdot 4^4 \cdots (n-1)^{n-1} \cdot n^n$$

máme asymptotický odhad  $H(n) \sim A n^{(6n^2+6n+1)/12} e^{-n^2/4}$  (ve smyslu  $\lim_{n \rightarrow \infty} \frac{H(n)}{A n^{(6n^2+6n+1)/12} e^{-n^2/4}} = 1$ ), kde  $A = 1.2824 \dots$  je Glaisher–Kinkelinova konstanta [8].

$$\begin{aligned} & \lim_{n \rightarrow \infty} \left( \frac{H(n)^2}{H(2n)} \right)^{\frac{1}{n^2}} \cdot 2^{2-\frac{1}{n}} \cdot n = \lim_{n \rightarrow \infty} \left( \frac{A^2 \cdot n^{(12n^2+12n+2)/12} e^{-n^2/2}}{A \cdot (2n)^{(24n^2+12n+1)/12} e^{-n^2}} \right)^{\frac{1}{n^2}} \cdot 2^{2-\frac{1}{n}} \cdot n = \\ & = \lim_{n \rightarrow \infty} \sqrt{e} \cdot A^{\frac{1}{n^2}} \cdot 2^{-\frac{2}{n} - \frac{1}{12n^2}} \cdot n^{\frac{1}{12n^2}} = \sqrt{e} < 2. \end{aligned}$$

Tím pádem by už jen stačilo ukázat, že  $\lambda(n)$  je ryze rostoucí funkce pro  $n \geq 2$ , což z rozsahových důvodů dělat nebudeme.

# Seznam použité literatury

- [1] Manjul Bhargava and Jonathan Hanke. Universal quadratic forms and the 290-theorem. *preprint*, 2005.
- [2] Manjul Bhargava. On the Conway-Schneeberger fifteen theorem. *Contemporary Mathematics*, 272:27–38, 2000.
- [3] Wai Kiu Chan, Myung-Hwan Kim, and S Raghavan. Ternary universal integral quadratic forms over real quadratic fields. *Japanese journal of mathematics. New series*, 22(2):263–273, 1996.
- [4] Vítězslav Kala. Universal quadratic forms and elements of small norm in real quadratic fields. *Bulletin of the Australian Mathematical Society*, 94(1):7–14, 2016.
- [5] Vítězslav Kala. Number fields without universal quadratic forms of small rank exist in most degrees. *arXiv preprint arXiv:2101.10364*, 2021.
- [6] Issai Schur. Über die Verteilung der Wurzeln bei gewissen algebraischen Gleichungen mit ganzzahligen Koeffizienten. *Mathematische Zeitschrift*, 1(4):377–402, 1918.
- [7] Jürgen Neukirch. *Algebraic number theory*, volume 322. Springer Science & Business Media, 2013.
- [8] Chao-Ping Chen. Glaisher–Kinkelin constant. *Integral Transforms and Special Functions*, 23(11):785–792, 2012.