STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Kvaterniony a zobecnění vět o čtyřech čtvercích

Matěj Doležálek
Kraj Vysočina

Humpolec, 2019

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Kvaterniony a zobecnění vět o čtyřech čtvercích

Quaternions and generalizations of four-square theorems

Autor: Matěj Doležálek
Škola: Gymnázium dr. A. Hrdličky, Komenského 147, 396 01 Humpolec
Kraj: Vysočina
Konzultant: Mgr. Vítězslav Kala, Ph.D.

Humpolec, 2019

Prohlášení

Prohlašuji, že jsem svou práci SOČ vypracoval samostatně a použil jsem pouze prameny a literaturu uvedené v seznamu bibliografických záznamů.

Prohlašuji, že tištěná verze a elektronická verze soutěžní práce SOČ jsou shodné.

Nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů.

V Humpolci dne ..... Podpis:.....

Poděkování

Děkuji Mgr. Vítězslavu Kalovi, Ph.D. za cenné rady a ochotnou pomoc při psaní této práce.

Anotace

Cílem této práce je využít kvaternionů ke zkoumání vyjádřitelnosti přirozených čísel kvadratickými formami čtyř proměnných. Toho je dosaženo především definováním oboru na nějaké množině kvaternionů takové, že daná kvadratická forma vyjadřuje normu jeho prvků. Odvozením jistých algebraických vlastností takového oboru je pak dokázána univerzálnost některých těchto forem a pro část z nich je dokázán i explicitní vzorec pro počet vyjádření libovolného přirozeného čísla danou kvadratickou formou. Tyto výsledky představují zobecnění po řadě Lagrangeovy věty o čtyřech čtvercích a Jacobiho věty o čtyřech čtvercích pro další kvadratické formy.

Klíčová slova

Kvaternion, kvadratická forma, Lagrangeova věta o čtyřech čtvercích, Jacobiho věta o čtyřech čtvercích, obor hlavních ideálů.

Annotation

The goal of this thesis is to use quaternions to study representability of natural numbers by quadratic forms in four variables. This is achieved mainly by defining a domain on some set of quaternions, such that the given quadratic form represents the norm of its elements. Universality of some of these forms is then proved by deriving certain algebraic properties of said domain and, for a portion of these forms, an explicit formula for the number represantations of any natural number by a given quadratic form is also proved. These results constitute generalizations of Lagrange's four-square theorem and Jacobi's four-square theorem respectively for other quadratic forms.

Keywords

Quaternion, quadratic form, Lagrange's four-square theorem, Jacobi's four-square theorem, principal ideal domain.

Obsah

Úvod

Lagrangeovu větu o čtyřech čtvercích dokázal poprvé v roce 1770 francouzský matematik italského původu Joseph-Louis Lagrange. Zní:

Každé přirozené číslo lze zapsat jako součet čtyř čtverců celých čísel.

Historie tohoto tvrzení je však delší. Před jeho důkazem bylo známo jako *Bachetova domněnka*, podle Clauda Gasparda Bacheta de Méziriac, který roku 1621 ve svém latinském překladu Diofantovy *Aritmetiky* poznamenal, že Diofantos toto tvrzení zdánlivě zná a předpokládá. Roku 1834 pak dokázal německý matematik Carl Gustav Jakob Jacobi metodami matematické analýzy svou vlastní větu o čtyřech čtvercích:

Pro přirozené n má rovnice $x^2 + y^2 + z^2 + w^2 = n$ právě [1]

$$8 \sum_{4 \nmid d \mid n} d$$

celočíselných řešení (x, y, z, w).

Později byly nalezeny důkazy těchto tvrzení využívající odlišných metod. Německý matematik Adolf Hurwitz dokázal pomocí zkoumání algebraických vlastností kvaternionů obě věty o čtyřech čtvercích. V této práci bude užit velmi podobný postup, kromě samotných vět o čtyřech čtvercích bude dokázáno i několik jejich zobecnění v podobě analogických výsledků pro jiné kvadratické formy než $x^2 + y^2 + z^2 + w^2$ (viz tabulky 2 a 5).

Hlavním výsledkem a přínosem této práce tedy bude zobecnění kvaternionového důkazu vět o čtyřech čtvercích. Nejprve v kapitole 1 zavedeme nezbytnou teorii okruhů, oborů, ideálů a matic. V kapitole 2 pak definujeme samotné kvaterniony a obor Hurwitzových kvaternionů a formulujeme obecnou větu (věta 2.3.7), z níž speciálně jako důsledek vyplyne Lagrangeova věta o čtyřech čtvercích. Důkazy v této kapitole vycházejí z těch v [3] a mírně je zobecňují. V kapitole 3 pak zkonstruujeme další kvaternionové obory, s jejichž pomocí dokážeme univerzálnost jim odpovídajících kvadratických forem. Konečně v kapitole 4 zobecníme některé výsledky z [3] a [5], s jejichž pomocí pak dokážeme Jacobiho větu o čtyřech čtvercích a její zobecnění pro některé další kvadratické formy. V sekci 4.4 také Jacobiho větu využijeme k odvození vzorce vyjadřujícího π pomocí nekonečné řady a vyřešení tzv. *Basilejského problému*, tedy určení součtu nekonečné řady

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} + \ldots$$

Již dopředu můžeme předeslat, že tento součet je roven $\frac{\pi^2}{6}$.

[1] Suma v tomto výrazu značí součet všech těch přirozených d, jež dělí n, ale nejsou násobky čtyř.

Užité značení

$\wedge$, $\vee$, $\Longrightarrow$, $\Longleftrightarrow$	Logické spojky konjunkce, disjunkce, implikace a ekvivalence.
$\forall$, $\exists$, $\exists!$	Logické kvantifikátory obecný („pro každé“), existenční („existuje“) a jednoznačné existence („existuje právě jedno“).
$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$	Množiny po řadě přirozených ($0 \notin \mathbb{N}$ – množinu nezáporných celých čísel značme $\mathbb{N}_0$), celých, racionálních a reálných čísel.
$\in$, $\subseteq$, $\subset$	Náleží, je podmnožinou, je vlastní podmnožinou.
$f : A \to B$	Zobrazení f, jež každému $x \in A$ přiřazuje nějaké $f(x) \in B$. Potom A zvěme *definičním oborem* f.
$\{f(x) : \varphi(x)\}$	Množina hodnot $f(x)$ pro všechna x splňující podmínku $\varphi(x)$. Kupříkladu množina všech sudých čísel $\{2x : x \in \mathbb{Z}\} = \{x : x \in \mathbb{Z} \wedge 2 \mid x\}$. Analogicky pro více proměnných $x_1, x_2, \ldots$
$\operatorname{Im} f$	*Obraz* zobrazení f s definičním oborem D, tj. množina $\{f(x) : x \in D\}$.
$A \setminus B$	Rozdíl množin A, B, tj. $\{x : x \in A \wedge x \notin B\}$.
max, min	Maximum, minimum.
$a \mid b$	a dělí b.
$a \equiv b \pmod{n}$	a je kongruentní b modulo n. Ekvivalentní $n \mid (a - b)$.
m^{-1}	V kongruenci prvek inverzní k m, tedy takové n, že $m \cdot n \equiv 1$.
$\operatorname{NSD}(a, b)$	Největší společný dělitel čísel $a, b \in \mathbb{Z}$.
$\sigma(n)$	Součet dělitelů přirozeného čísla n, tj. $\sigma(n) = \sum_{d \mid n} d$.
$\mathbb{Z}_n$	Okruh zbytkových tříd modulo n.
$\mathrm{M}_n(R)$	Okruh čtvercových matic $n \times n$ nad okruhem R (viz definici 1.2.1).
$\det A$	Determinant čtvercové matice A (viz definici 1.2.2).
$\operatorname{Vol} M$	n-rozměrný objem (tj. speciálně délka, obsah, objem pro $n \in \{1, 2, 3\}$) množiny $M \subseteq \mathbb{R}^n$ (pokud tento pojem dává smysl).
$\mathbb{H}(\mathbb{R})$	Množina kvaternionů (viz definici 2.1.1).
$\overline{\theta}$, $N(\theta)$	Sdružený kvaternion a norma kvaternionu $\theta \in \mathbb{H}(\mathbb{R})$ (viz definici 2.1.1).
$\mathbb{H}(\mathbb{Z})$, $\mathbb{J}$	Obory celočíselných a Hurwitzových kvaternionů (viz sekci 2.2).
$r_M(n)$	Počet prvků množiny $M \subseteq \mathbb{H}(\mathbb{R})$, jejichž norma je rovna n (viz definici 4.0.1).

Je-li $\circ$ binární operace definovaná na množině M, pak pro $A, B \subseteq M, x \in M$ značme

$$x \circ A = \{x \circ a : a \in A\}, \quad A \circ x = \{a \circ x : a \in A\}, \quad A \circ B = \{a \circ b : a \in A \wedge b \in B\}.$$

Pro množinu A a přirozené číslo n nechť A^n značí množinu uspořádaných n-tic prvků A.

Kapitola 1

Okruhy

V této kapitole zavedeme několik algebraických pojmů jako okruh, obor, ideál či matice a odvodíme některé jejich základní vlastnosti. Tuto teorii později využijeme ke zkoumání kvaternionů a s nimi spojených kvadratických forem.

1.1 Obory a ideály

Definice 1.1.1. *Okruhem* rozumějme množinu R s binárními operacemi $+$, $\cdot$ (ty zvěme po řadě *sčítáním* a *násobením*[2]), splňujícími pro každé $a, b, c \in R$ podmínky

(i) $a + b \in R$,

(ii) $a + b = b + a$,

(iii) $(a + b) + c = a + (b + c)$,

(iv) $a \cdot b \in R$,

(v) $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

(vi) $a \cdot (b + c) = a \cdot b + a \cdot c \wedge (a + b) \cdot c = a \cdot c + b \cdot c$,

(vii) $(\exists! 1 \in R)\,(\forall r \in R)\,(1 \cdot r = r \cdot 1 = r)$,

(viii) $(\exists! 0 \in R)\,(\forall r \in R)\,(r + 0 = 0 + r = r \wedge 0 \cdot r = r \cdot 0 = 0)$,

(ix) $(\exists!(-a) \in R)\,(a + (-a) = 0)$.

Pokud je navíc splněna podmínka

(x) $(\forall a, b \in R \setminus \{0\})\,(ab \neq 0)$,

zvěme $(R, +, \cdot)$ *oborem*.

Definice 1.1.2. Budiž $(R, +, \cdot)$ obor. Prvek $u \in R$ nazvěme *jednotkou*, pokud existuje $v \in R$ takové, že $uv = 1$. Nejednotkové $q \in R$ nazvěme *ireducibilním*, pokud neexistují nejednotková $a, b \in R$ splňující $q = ab$.

[2] Tam, kde tím nedojde k nedorozumění, pišme namísto $a \cdot b$ libovolně pouze ab.

Poznámka. Pokud $uv = 1$, pak už jistě i

$$\begin{aligned} vuv &= v, \\ (vu - 1) \cdot v &= 0, \\ vu - 1 &= 0, \\ vu &= 1. \end{aligned}$$

Okruhy, resp. obory jsou algebraickými strukturami, které v jistém smyslu zobecňují aritmetiku celých čísel – jejich prvky lze sčítat a násobit za platnosti většiny „obvyklých" vlastností těchto operací. Na rozdíl od oboru celých, racionálních, reálných nebo i komplexních čísel však není zaručeno, že násobení je komutativní, tedy ab nemusí obecně býti rovno ba. Dále jsou ireducibilní prvky jistou obdobou prvočísel – nemusí však mít ani zdaleka tak silné vlastnosti.

Definice 1.1.3. Budiž $(R, +, \cdot)$ okruh a mějme $a, b \in R$. Řekněme, že a, b *komutují*, pokud $ab = ba$.

Definice 1.1.4. Budiž $(R, +, \cdot)$ okruh. Neprázdnou množinu $I \subseteq R$ nazvěme *levým ideálem* R, pokud pro každá $x, y \in I$ a $r \in R$ platí

(i) $x + y \in I$,

(ii) $rx \in I$.

Pravý ideál definujme analogicky psaním xr namísto rx v druhé podmínce. Množinu I zvěme *oboustranným ideálem* nebo prostě *ideálem*, pakliže je zároveň levým i pravým ideálem. Levý (resp. pravý) ideál nazvěme *hlavním*, pokud je tvaru $Ra = \{ra : r \in R\}$ (resp. aR) pro nějaké $a \in R$.

Ideály si lze představit jako zobecnění představy dělitelnosti do nekomutativní algebry. Dělitelnost celých čísel lze totiž následovně přeformulovat: $a \mid b$, pokud $b \in \mathbb{Z}b$ (nebo $b\mathbb{Z}$ – díky komutativitě násobení jsou v $\mathbb{Z}$ všechny ideály oboustranné). Množina všech násobků b je tedy taková množina, jež obsahuje b a je uzavřená na tvorbě lineárních kombinací – poslední vlastnost je přitom ale přesně definicí ideálu. Ne všechny ideály však musí být hlavní. V oborech, s nimiž budeme v této práci povětšinou pracovat, toto sice bude platit, což nám bude velmi užitečným nástrojem, obecně to však vůbec nemusí platit.

Lemma 1.1.5. *Budiž $(R, +, \cdot)$ okruh a I, J jeho levé (resp. pravé) ideály. Potom je*

$$I + J = \{x + y : x \in I, y \in J\}$$

levý (resp. pravý) ideál R.

Důkaz. Důkaz proveďme pro levé ideály, pro pravé lze postupovat obdobně.

Mějme libovolné $x_1, x_2 \in I$, $y_1, y_2 \in J$. Potom z definice ideálu $x_1 + x_2 \in I$, $y_1 + y_2 \in J$, z čehož i

$$(x_1 + y_1) + (x_2 + y_2) = (x_1 + x_2) + (y_1 + y_2) \in (I + J)\,.$$

Dále pro libovolné $r \in R$ jistě $rx_1 \in I$, $ry_1 \in J$, z čehož i

$$r\,(x_1 + y_1) = rx_1 + ry_1 \in (I + J)\,.$$

Tímto je důkaz hotov. □

Lemma 1.1.6. *V oboru $(R,+,\cdot)$ jsou dva levé (resp. pravé) hlavní ideály Ra, Rb (resp. aR, bR) totožné, právě pokud existuje jednotka $u \in R$ taková, že $a = ub$ (resp. $a = bu$).*

Důkaz. Důkaz proveďme pro levé ideály, pro pravé lze postupovat obdobně.

Platí $R \cdot 0 = \{0\}$, pročež lemma platí, pokud je alespoň jedno z a, b rovno nule – pak jsou totiž Ra, Rb totožné, právě pokud $a = b = 0$, což už značí $a = 1 \cdot b$. Nadále tedy předpokládejme $a, b \in R \setminus \{0\}$.

Nejprve nechť je $a = ub$ pro jednotku u. Potom pro každé $r \in R$ platí

$$ra = (ru)b \in Rb,$$

neboli $Ra \subseteq Rb$. Jistě však existuje jednotka $v \in R$ taková, že $uv = vu = 1$, z čehož i $b = va$, a tedy $Rb \subseteq Ra$, neboli $Ra = Rb$.

Nyní nechť $Ra = Rb$. Potom jistě $1 \cdot a \in Ra = Rb$, neboli existuje $c \in R$ takové, že $a = cb$. Analogicky existuje $d \in R$ takové, že $b = da$, z čehož dohromady

$$\begin{aligned} a &= cb = cda, \\ (1 - cd) \cdot a &= 0, \\ 1 - cd &= 0, \\ 1 &= cd, \end{aligned}$$

neboli jsou obě c, d jednotkami. □

Definice 1.1.7. Obor $(R,+,\cdot)$ nazvěme *zleva Eukleidovským*, pokud existuje funkce $d : R \setminus \{0\} \to \mathbb{N}$ taková, že pro každá $a, b \in R \setminus \{0\}$ existují $x, y \in R$ splňující

$$a = xb + y, \qquad\qquad y = 0 \vee d(y) < d(b).$$

Zprava Eukleidovský obor definujme analogicky psaním bx namísto xb v podmínce.

Definice 1.1.8. Obor $(R,+,\cdot)$ nazvěme *zleva slabě Eukleidovským*, pokud existuje funkce $d : R \to \mathbb{N}_0$ taková, že $d(a) = 0$, právě pokud $a = 0$, a pro každá $a, b \in R \setminus \{0\}$ buďto $a \in Rb$, nebo existují $x, y \in R$ taková, že

$$0 < d(xa - yb) < d(b).$$

Zprava slabě Eukleidovský obor definujme analogicky psaním bR, ax, by namísto xa, yb, Rb.

Pozorování. Každý zleva (resp. zprava) Eukleidovský obor je i zleva (resp. zprava) slabě Eukleidovský.

Definice 1.1.9. Obor $(R,+,\cdot)$ nazvěme *levým oborem hlavních ideálů*, pokud je každý levý ideál $I \subseteq R$ hlavní. *Pravý obor hlavních ideálů* definujme analogicky.

Lemma 1.1.10. *Budiž $(R,+,\cdot)$ zleva (resp. zprava) slabě Eukleidovský obor s funkcí d popsaných vlastností. Potom je R levý (resp. pravý) obor hlavních ideálů.*

Důkaz. Důkaz proveďme pro levé ideály, pro pravé lze postupovat obdobně.

Budiž I levý ideál R a uvažujme funkci d popsanou v definici zleva slabě Eukleidovského oboru. Zvolme $g \in I \setminus \{0\}$ tak, že $d(g)$ je minimální. Dále mějme libovolné $s \in I \setminus \{0\}$. Pro spor nechť $s \notin Rg$ – potom z definice slabě Eukleidovského okruhu existují x, y taková, že

$$0 < d(xs - yg) < d(g).$$

Z uzavřenosti levého ideálu na násobení prvkem R zleva a na sčítání je $xs - yg \in I$, zároveň ale $xs - yg \neq 0$. To je dohromady spor s volbou g, pročež pro každé $s \in I \setminus \{0\}$ platí $s \in Rg$. Vzhledem k $0 \in Rg$ pak tedy $I \subseteq Rg$. Z definice ideálu ale $Rg \subseteq I$, čili dohromady $I = Rg$. □

Definice 1.1.11. Buďte R, S okruhy. Zobrazení $\varphi : R \to S$ nazvěme *homomorfizmem*, splňuje-li pro každé $a, b \in R$

(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$,

(ii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$,

kde sčítání i násobení bereme na levé straně v R, na pravé v S. Homomorfizmus, který je zároveň bijekcí, nazvěme *izomorfizmem*. Pokud z oboru R do oboru S vede nějaký izomorfizmus, řekněme, že jsou *izomorfní*.

Pozorování. Obraz homomorfizmu $\varphi : R \to S$, tj. množina

$$\operatorname{Im}\varphi = \{\varphi(x) : x \in R\},$$

tvoří s operacemi $+, \cdot$ (v S) okruh. Toto plyne z toho, že pro každá $\varphi(a), \varphi(b), \varphi(c) \in \operatorname{Im}\varphi$ (kde $a, b, c \in R$) plyne splnění podmínek definice 1.1.1 už z toho, že je splňují a, b, c – např.

$$\begin{aligned}
\varphi(a) + \varphi(b) &= \varphi(a + b) \in \operatorname{Im}\varphi, \\
\varphi(a)(\varphi(b) + \varphi(c)) &= \varphi(a)\varphi(b + c) = \varphi(a(b + c)) = \varphi(ab + ac) = \\
&= \varphi(ab) + \varphi(ac) = \varphi(a)\varphi(b) + \varphi(a)\varphi(c), \\
\varphi(1)\varphi(a) &= \varphi(1 \cdot a) = \varphi(a) = \varphi(a \cdot 1) = \varphi(a)\varphi(1)
\end{aligned}$$

atp.

Dále pokud existuje izomorfizmus $\varphi : R \to S$, pak už existuje i izomorfizmus $\psi : S \to R$ – je jím např. to zobrazení ψ, jež je inverzním k φ (to existuje, neboť φ je z definice izomorfizmu bijekce).

1.2 Maticové okruhy

Definice 1.2.1. Budiž $(R, +, \cdot)$ okruh. *Maticí $m \times n$ nad R* rozumějme obdélníkové schéma

$$\begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1} & a_{m2} & \cdots & a_{mn}
\end{pmatrix}$$

obsahující mn prvků $a_{11}, \ldots, a_{1n}, \ldots, a_{mn}$ okruhu R. Matici nazývejme *čtvercovou*, pokud $m = n$ – množinu všech čtvercových matic $n \times n$ značme $\mathrm{M}_n(R)$. Součet matic

$$A = \begin{pmatrix}
a_{11} & a_{12} & \cdots & a_{1n} \\
a_{21} & a_{22} & \cdots & a_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
a_{m1} & a_{m2} & \cdots & a_{mn}
\end{pmatrix}, \qquad B = \begin{pmatrix}
b_{11} & b_{12} & \cdots & b_{1n} \\
b_{21} & b_{22} & \cdots & b_{2n} \\
\vdots & \vdots & \ddots & \vdots \\
b_{m1} & b_{m2} & \cdots & b_{mn}
\end{pmatrix}$$

definujme jako

$$A+B=\begin{pmatrix} a_{11}+b_{11} & a_{12}+b_{12} & \cdots & a_{1n}+b_{1n} \\ a_{21}+b_{21} & a_{22}+b_{22} & \cdots & a_{2n}+b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}+b_{m1} & a_{m2}+b_{m2} & \cdots & a_{mn}+b_{mn} \end{pmatrix}.$$

Dále součiny $r \in R$ s maticí A zleva a zprava definujme jako

$$r \cdot A=\begin{pmatrix} ra_{11} & ra_{12} & \cdots & ra_{1n} \\ ra_{21} & ra_{22} & \cdots & ra_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ ra_{m1} & ra_{m2} & \cdots & ra_{mn} \end{pmatrix}, \qquad A \cdot r=\begin{pmatrix} a_{11}r & a_{12}r & \cdots & a_{1n}r \\ a_{21}r & a_{22}r & \cdots & a_{2n}r \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1}r & a_{m2}r & \cdots & a_{mn}r \end{pmatrix}.$$

Konečně součin matice A rozměrů $m \times n$ s maticí B rozměrů $n \times p$ definujme jako matici C rozměrů $m \times p$ danou předpisem

$$A \cdot B = C = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1p} \\ c_{21} & c_{22} & \cdots & c_{2p} \\ \vdots & \vdots & \ddots & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mp} \end{pmatrix},$$

$$c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}.$$

Ukažme, že je-li R okruh, pak i čtvercové matice $n \times n$ tvoří okruh $\mathrm{M}_n(R)$. V něm totiž existuje neutrální prvek vzhledem k násobení v podobě jednotkové matice

$$I=\begin{pmatrix} e_{11} & e_{12} & \cdots & e_{1n} \\ e_{21} & e_{22} & \cdots & e_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ e_{n1} & e_{n2} & \cdots & e_{nn} \end{pmatrix},$$

$$e_{ij} = \begin{cases} 1, & \text{pokud } i=j, \\ 0, & \text{jinak} \end{cases}$$

s vlastností $AI = IA = A$ pro každou matici $A \in \mathrm{M}_n(R)$ a nulová matice

$$N=\begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix}$$

s vlastností $A+N = A, AN = NA = N$ pro libovolnou $A \in \mathrm{M}_n(R)$. Uzavřenost na sčítání i násobení je zřejmá (součin dvou matic $n \times n$ je opět matice $n \times n$), stejně tak komutativita a asociativita sčítání a existence $-A$ pro každé A. Zbývá tedy dokázat asociativitu násobení.

Mějme nad R matice A, B, C po řadě o rozměrech $m \times p$, $p \times q$, $q \times n$ a zaveďme

$$D = AB, \qquad E = BC,$$
$$F = DC, \qquad G = AE.$$

Dále buďte $a_{ij}, b_{ij}, c_{ij}, d_{ij}, e_{ij}, f_{ij}, g_{ij}$ prvky příslušných matic. Potom z definice maticového násobení plyne

$$f_{ij} = \sum_{v=1}^{q} d_{iv}c_{vj} = \sum_{v=1}^{q} \left(\sum_{u=1}^{p} a_{iu}b_{uv} \right) c_{vj} = \sum_{u=1}^{p}\sum_{v=1}^{q} a_{iu}b_{uv}c_{vj},$$
$$g_{ij} = \sum_{u=1}^{p} a_{iu}e_{uj} = \sum_{u=1}^{p} a_{iu} \left(\sum_{v=1}^{q} b_{uv}c_{vj} \right) = \sum_{u=1}^{p}\sum_{v=1}^{q} a_{iu}b_{uv}c_{vj},$$

což znamená $F = G$, neboli $(AB)C = A(BC)$. □

Definice 1.2.2. *Permutací* konečné množiny M rozumějme bijekci $\sigma : M \to M$. Nechť je S_n množinou všech permutací množiny $\{1, \ldots, n\}$. *Znaménko* permutace $\sigma \in S_n$ definujeme jako $\operatorname{sgn}(\sigma) = (-1)^s$, kde s je počet uspořádaných dvojic (i, j) takových, že $i < j$ a zároveň $\sigma(i) > \sigma(j)$.

Budiž R okruh a $A \in \mathrm{M}_n(R)$. *Determinant* matice A definujeme jako

$$\sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod_{k=1}^{n} a_{k\sigma(k)}$$

a značme jej $\det A$ nebo $|A|$.

Takováto definice se může zdát dosti nahodilá. Determinant má však mnoho elegantních a užitečných vlastností. Speciálně pro $A \in \mathrm{M}_2(R)$ je

$$\det A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21}.$$

Dále determinant splňuje dva užitečně vztahy (zde je nebudeme dokazovat). Zaprvé pro dvě matice $A, B \in \mathrm{M}_n(R)$ platí

$$\det(AB) = \det A \cdot \det B,$$

zadruhé, je-li $M \subseteq \mathbb{R}^n$, $\operatorname{Vol} M$ dává smysl a máme dánu matici $A \in \mathrm{M}_n(\mathbb{R})$, pak pro lineární zobrazení $\varphi : M \to \mathbb{R}^n$ zadané maticí A, tj.

$$\varphi((x_1, \ldots, x_n)) = (X_1, \ldots, X_n),$$
$$\begin{pmatrix} X_1 \\ \vdots \\ X_n \end{pmatrix} = A \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix},$$

platí[3] $\operatorname{Vol}(\operatorname{Im}\varphi) = |\det A| \cdot \operatorname{Vol} M$.

[3] Řečeno slovy: φ zobrazuje M na nějakou množinu o $|\det A|$-násobném objemu.

Kapitola 2

Kvaterniony

V této kapitole definujeme kvaterniony a využijeme je k důkazu Lagrangeovy věty o čtyřech čtvercích.

2.1 Základní vlastnosti kvaternionů

Definice 2.1.1. Uvažujme okruh $\mathrm{M}_4(\mathbb{R})$ a pojmenujme v něm matice

$$1 = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad i = \begin{pmatrix} 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 \end{pmatrix},$$

$$j = \begin{pmatrix} 0 & 0 & 0 & -1 \\ 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \qquad k = \begin{pmatrix} 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 \end{pmatrix}.$$

Potom platí

$$i^2 = j^2 = k^2 = ijk = -1. \tag{2.1}$$

Kvaterniony definujme jako prvky množiny

$$\mathbb{H}(\mathbb{R}) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}.$$

Pro kvaternion $\theta = a + bi + cj + dk$ definujme

(i) jeho *sdružený kvaternion* $\overline{\theta} = a - bi - cj - dk$,

(ii) jeho *normu* $N(\theta) = \theta\overline{\theta} = \overline{\theta}\theta = a^2 + b^2 + c^2 + d^2$.

Poznámka. Obecněji lze definovat kvaterniony nad okruhem R tak, že v předchozí definici píšeme vždy R namísto $\mathbb{R}$.

Z vlastností sčítání a násobení matic, existence jednotkové matice 1 a nulové matice

$$0 = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

a konečně platnosti rovností (2.1) je $(\mathbb{H}(\mathbb{R}), +, \cdot)$ jistě okruhem – všechny definující vlastnosti okruhu jsou zaručeny tím, že $\mathbb{H}(\mathbb{R}) \subset \mathrm{M}_4(\mathbb{R})$, a rovnostmi (2.1). Ukažme, že je i oborem. Nahlédněme, že libovolné reálné číslo r a libovolný kvaternion $\theta = a + bi + cj + dk$ díky komutativitě násobení reálných čísel, resp. díky tomu, že jednotková matice komutuje s libovolnou jinou maticí stejného rozměru, komutují:

$$\begin{aligned} r\theta = r \cdot (a + bi + cj + dk) &= ra + rbi + rcj + rdk = \\ &= ar + bir + cjr + dkr = (a + bi + cj + dk) \cdot r = \theta r \end{aligned}$$

Z (2.1) lze vyvodit

$$ij = k, \qquad jk = i, \qquad ki = j, \qquad ji = -k, \qquad kj = -i, \qquad ik = -j,$$

dále jistě platí $\overline{(\overline{\theta})} = \theta$. Ověřme

$$\begin{aligned} \theta\overline{\theta} = (a + bi + cj + dk)\,(a - bi - cj - dk) &= (a^2 - abi - acj - adk) + \\ + (abi + b^2 - bck + bdj) + (acj + bck + c^2 - cdi) + (adk - bdj + cdi + d^2) &= \\ = a^2 + b^2 + c^2 + d^2, \end{aligned}$$

obdobně

$$\overline{\theta}\theta = \overline{\theta} \cdot \overline{(\overline{\theta})} = N\left(\overline{\theta}\right) = a^2 + (-b)^2 + (-c)^2 + (-d)^2 = a^2 + b^2 + c^2 + d^2.$$

V reálných číslech platí nerovnost $x^2 \geq 0$ pro každé $x \in \mathbb{R}$, přičemž rovnost nastává právě pro $x = 0$, z čehož zřejmě pro $\theta \in \mathbb{H}(\mathbb{R})$ platí $N(\theta) \geq 0$ a rovnost nastává právě pro $\theta = 0$.

Mějme nyní $\alpha, \beta \in \mathbb{H}(\mathbb{R}) \setminus \{0\}$. Jistě $N(\alpha), N(\beta) > 0$, pročež by z $\alpha\beta = 0$ plynulo

$$\begin{aligned} \alpha\beta \cdot \frac{\overline{\beta}}{N(\beta)} &= 0 \cdot \frac{\overline{\beta}}{N(\beta)}, \\ \frac{\alpha \cdot N(\beta)}{N(\beta)} &= 0, \\ \alpha &= 0, \end{aligned}$$

což je spor. $(\mathbb{H}(\mathbb{R}), +, \cdot)$ je tedy vskutku obor.

Lemma 2.1.2. *Pro libovolná $\alpha, \beta \in \mathbb{H}(\mathbb{R})$ platí*

$$\overline{(\alpha + \beta)} = \overline{\alpha} + \overline{\beta}, \qquad\qquad \overline{(\alpha \cdot \beta)} = \overline{\beta} \cdot \overline{\alpha}.$$

Důkaz. Budiž $\alpha = a + bi + cj + dk$, $\beta = e + fi + gj + hk$. Stačí ověřit:

$$\begin{aligned} \overline{(\alpha + \beta)} &= \overline{((a + e) + (b + f)i + (c + g)j + (d + h)k)} = (a + e) - (b + f)i - \\ &\quad - (c + g)j - (d + h)k = (a - bi - cj - dk) + (e - fi - gj - hk) = \overline{\alpha} + \overline{\beta} \\ \overline{(\alpha \cdot \beta)} &= \overline{((a + bi + cj + dk)(e + fi + gj + hk))} = \overline{(ae + afi + agj + ahk) + } \\ &\quad \overline{+(bei - bf + bgk - bhj) + (cej - cfk - cg + chi) + (dek + dfj - dgi - dh)} = \\ &= ae - afi - agj - ahk - bei - bf - bgk + bhj - cej + cfk - cg - chi - \\ &\quad - dek - dfj + dgi - dh = (ea - ebi - ecj - edk) + (-fai - fb + fck - \\ &\quad - fdj) + (-gaj - gbk - gc + gdi) + (-hak + hbj - hci - hd) = \\ &= (e - fi - gj - hk)(a - bi - cj - dk) = \overline{\beta} \cdot \overline{\alpha} \end{aligned}$$

□

Důsledek. *Norma je úplně multiplikativní, neboli pro libovolná $\alpha, \beta \in \mathbb{H}(\mathbb{R})$ platí*

$$N(\alpha\beta) = (\alpha\beta) \cdot \overline{(\alpha\beta)} = \alpha \cdot \beta \cdot \overline{\beta} \cdot \overline{\alpha} = \alpha \cdot N(\beta) \cdot \overline{\alpha} = \alpha \cdot \overline{\alpha} \cdot N(\beta) = N(\alpha)N(\beta).$$

2.2 Hurwitzovy kvaterniony

Zaveďme množiny

$$\mathbb{H}(\mathbb{Z}) = \{a + bi + cj + dk : a, b, c, d \in \mathbb{Z}\},$$
$$\mathbb{J} = \left\{ \frac{a + bi + cj + dk}{2} : a, b, c, d \in \mathbb{Z} \wedge a \equiv b \equiv c \equiv d \pmod 2 \right\}.$$

Prvky množiny $\mathbb{H}(\mathbb{Z})$ nazývejme *celočíselnými kvaterniony*[4]. Účel jejich zkoumání je snad zjevný – Lagrangeova věta hovoří o součtech čtyř čtverců celých čísel, což jsou ale přesně normy prvků $\mathbb{H}(\mathbb{Z})$. Méně zjevného účelu již může být zavedení $\mathbb{J}$. Důvodem je to, že $\mathbb{J}$ má mnohé užitečné vlastnosti, které $\mathbb{H}(\mathbb{Z})$ postrádá.

Okamžitě je zřejmé, že $\mathbb{H}(\mathbb{Z})$ je obor. Ukažme, že i $\mathbb{J}$ je oborem – jeho prvky zvěme *Hurwitzovými kvaterniony*. Komutativita sčítání, asociativita sčítání i násobení, distributivita násobení na sčítání i nenulovost součinu nenulových prvků jsou zaručeny už díky $\mathbb{J} \subset \mathbb{H}(\mathbb{R})$. Dále jistě $0, 1 \in \mathbb{J}$ a

$$\theta \in \mathbb{J} \iff (-\theta) \in \mathbb{J}.$$

Zbývá tedy zkontrolovat uzavřenost na sčítání a násobení.

Zavedeme-li $\zeta = \frac{1+i+j+k}{2}$, lze $\mathbb{J}$ přepsat jako

$$\{a\zeta + bi + cj + dk : a, b, c, d \in \mathbb{Z}\}.$$

Potom je uzavřenost na sčítání zřejmá ($\mathbb{J}$ je právě množinou všech celočíselných lineárních kombinací ζ, i, j, k). Přitom snadno ověříme $\theta_1\theta_2 \in \mathbb{J}$ pro $\theta_1, \theta_2 \in \{\zeta, i, j, k\}$ (viz tabulku 1). Z toho už distributivitou jistě $\alpha\beta \in \mathbb{J}$ pro každá $\alpha, \beta \in \mathbb{J}$.

	ζ	i	j	k
ζ	$-\zeta + i + j + k$	$-\zeta + i + j$	$-\zeta + j + k$	$-\zeta + k + i$
i	$-\zeta + i + k$	$-2\zeta + i + j + k$	k	$-j$
j	$-\zeta + j + i$	$-k$	$-2\zeta + i + j + k$	i
k	$-\zeta + k + j$	j	$-i$	$-2\zeta + i + j + k$

Tabulka 1: Multiplikační tabulka bází oboru $\mathbb{J}$.

Povšimněme si dále toho, že pro $a \equiv b \equiv c \equiv d \pmod 2$ je $a^2 + b^2 + c^2 + d^2 \equiv 0 \pmod 4$, z čehož pro $\theta = \frac{a+bi+cj+dk}{2} \in \mathbb{J}$ plyne

$$N(\theta) = \frac{a^2 + b^2 + c^2 + d^2}{4} \in \mathbb{Z},$$

neboli norma Hurwitzova kvaternionu je vždy celé (nezáporné) číslo. Díky tomuto je $u \in \mathbb{J}$ jednotkou, právě pokud $N(u) = 1$ – pokud $uv = 1$, pak i $N(u)N(v) = 1$, naopak pokud $N(u) = 1$, pak už $u\overline{u} = 1$. Takových kvaternionů existuje právě 24 – jsou to $\pm 1, \pm i, \pm j, \pm k$ a všech šestnáct kvaternionů tvaru

$$\frac{\pm 1 \pm i \pm j \pm k}{2},$$

kde každé ze čtyř znamének volíme nezávisle.

[4] Nazývají se též *Lipschitzovými kvaterniony*, podle německého matematika Rudolfa Lipschitze.

Věta 2.2.1. $(\mathbb{J}, +, \cdot)$ *je zleva i zprava Eukleidovský obor.*

Důkaz. Dokažme, že $(\mathbb{J}, +, \cdot)$ je zleva Eukleidovský – důkaz eukleidovskosti zprava je analogický. Za funkci d z definice zleva Eukleidovského oboru poslouží norma.

Mějme libovolná $\alpha, \beta \in \mathbb{J} \setminus \{0\}$. Položíme-li $\varphi = \frac{\alpha\overline{\beta}}{N(\beta)}$, platí v $\mathbb{H}(\mathbb{R})$ jistě rovnost

$$\alpha = \varphi\beta.$$

Budiž $\varphi = a + bi + cj + dk$ a zvolme $e, f, g, h \in \mathbb{Z}$ tak, že

$$|a - e|, |b - f|, |c - g|, |d - h| \leq \frac{1}{2}$$

– to jistě lze (jednoduše zaokrouhlíme a, b, c, d vždy na nejbližší celé číslo). Budiž potom $\gamma = e + fi + gj + hk$ (tedy $\gamma \in \mathbb{H}(\mathbb{Z})$) a položme

$$\delta = \alpha - \gamma\beta = (\varphi - \gamma)\,\beta.$$

Nyní je $N(\delta) = N(\varphi - \gamma)\,N(\beta)$. Přitom

$$N(\varphi - \gamma) = |a - e|^2 + |b - f|^2 + |c - g|^2 + |d - h|^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} + \frac{1}{4} = 1.$$

Pokud v předchozí nerovnosti nenastane rovnost, pak jsme hotovi, neboť potom $N(\delta) < N(\beta)$ a Eukleidovskost zleva je naplněna. Pokud rovnost nastane, pak musí být

$$|a - e| = |b - f| = |c - g| = |d - h| = \frac{1}{2},$$

což ale znamená $\varphi = \gamma + \frac{\pm 1 \pm i \pm j \pm k}{2}$ pro nějakou volbu znamének, neboli $\varphi \in \mathbb{J}$. To znamená $\alpha = \varphi\beta + 0$, neboli je Eukleidovskost zleva znovu naplněna. Tím je důkaz hotov. □

Důsledek. $\mathbb{J}$ *je levým i pravým oborem hlavních ideálů.*

Závěrem sekce ještě dokažme dvě užitečné lemmata, s jejichž pomocí Hurwitzovy kvaterniony v následující sekci snadno využijeme k důkazu Lagrangeovy věty o čtyřech čtvercích.

Lemma 2.2.2. *Pro libovolné prvočíslo p existuje $\theta \in \mathbb{J}$ takové, že $N(\theta)$ je násobkem p, ale nikoliv p^2.*

Důkaz. Pro $p = 2$ máme triviálně $N(1 + i) = 2$, pročež nadále uvažujme p liché.

Položme $S = \left\{0, 1, \ldots, \frac{p-1}{2}\right\}$. Pro $x \in S$ výraz $x^2 \pmod p$ nabývá $\frac{p+1}{2}$ různých hodnot, neboť pro $x_1, x_2 \in S \setminus \{0\}$ díky $0 < x_1 + x_2 \leq p - 1 < p$ (tedy $p \nmid x_1 + x_2$) z $x_1^2 \equiv x_2^2 \pmod p$ plyne

$$\begin{aligned} x_1^2 - x_2^2 &\equiv 0 \pmod p, \\ (x_1 - x_2)(x_1 + x_2) &\equiv 0 \pmod p, \\ x_1 - x_2 &\equiv 0 \pmod p, \\ x_1 &\equiv x_2 \pmod p, \end{aligned}$$

zatímco $x^2 \equiv 0 \pmod p$, právě pokud $x \equiv 0 \pmod p$. Obdobně pro $y \in S$ výraz $-y^2 - 1 \pmod p$ nabývá taktéž $\frac{p+1}{2}$ různých hodnot. Pojmenujeme-li tedy

$$U = \left\{x^2 \pmod p : x \in S\right\}, \qquad V = \left\{-y^2 - 1 \pmod p : y \in S\right\},$$

platí $|U| + |V| = p + 1 > p = |\mathbb{Z}_p|$ a zároveň $U, V \subseteq \mathbb{Z}_p$, čímž z Dirichletova principu nejsou U, V disjunktní. Existují tedy $x, y \in S$ taková, že

$$\begin{aligned} x^2 &\equiv -y^2 - 1 \pmod{p}, \\ x^2 + y^2 + 1 &\equiv 0 \pmod{p}. \end{aligned}$$

Máme tedy $N(1 + xi + yj) = mp$ pro

$$m = \frac{x^2 + y^2 + 1}{p} \leq \frac{2 \cdot \left(\frac{p-1}{2}\right)^2 + 1}{p} < \frac{2 \cdot \frac{p^2}{4} + 1}{p} \leq \frac{\frac{3}{4}p^2}{p} \leq \frac{3}{4}p < p,$$

přitom jistě $x^2 + y^2 + 1 \geq 1 > 0$. Z toho dohromady $p \nmid m$, čímž je důkaz hotov. □

Lemma 2.2.3. *Mějme $n \in \mathbb{N}$ a $\alpha \in \mathbb{J}$ takové, že $N(\alpha) = n$. Potom existuje $\beta \in \mathbb{H}(\mathbb{Z})$ splňující $N(\beta) = n$.*

Důkaz. Pokud $\alpha \in \mathbb{H}(\mathbb{Z})$, stačí vzít $\beta = \alpha$ – nadále tedy předpokládejme $\alpha \in \mathbb{J} \setminus \mathbb{H}(\mathbb{Z})$, neboli $\alpha = \frac{a+bi+cj+dk}{2}$ pro nějaká lichá celá čísla a, b, c, d. Zvolme $e, f, g, h \in \{\pm 1\}$ tak, že

$$a - e, \qquad b - f, \qquad c - g, \qquad d - h$$

jsou násobky čtyř (to lze). Potom položíme-li $\delta = \frac{e+fi+gj+hk}{2}$, je $\delta \in \mathbb{J}$ a zároveň $N(\delta) = 1$, navíc platí

$$\alpha - \delta = \frac{(a-e) + (b-f)i + (c-g)j + (d-h)k}{2} = 2\gamma$$

pro nějaké $\gamma \in \mathbb{H}(\mathbb{Z})$. Z toho ale

$$\begin{aligned} \overline{\delta} \cdot \alpha &= \overline{\delta}\,(2\gamma + \delta) = \overline{\delta} \cdot 2\gamma + \overline{\delta} \cdot \delta = \left(2\overline{\delta}\right) \cdot \gamma + 1, \\ N\left(\overline{\delta} \cdot \alpha\right) &= N(\overline{\delta}) \cdot N(\alpha) = n. \end{aligned}$$

Uvažme nyní, že pro libovolné $\theta \in \mathbb{J}$ platí $2\theta \in \mathbb{H}(\mathbb{Z})$, z čehož $(2\overline{\delta})\gamma + 1 \in \mathbb{H}(\mathbb{Z})$. Vzetím $\beta = \overline{\delta} \cdot \alpha$ je tedy důkaz hotov. □

2.3 Lagrangeova věta

S pomocí Hurwitzových kvaternionů a znalostí, že tvoří obor hlavních ideálů, již svedeme postupně dokázat Lagrangeovu větu. Postačí však k tomu pouze několik vlastností tohoto oboru, pročež úvahy povedeme obecně pouze z nich. Toto dobře poslouží v dalších kapitolách, kde sestrojíme další obory se stejnými vlastnostmi.

Definice 2.3.1. H nazvěme *silným kvaternionovým oborem*, pokud platí, že

(i) $\mathbb{Z} \subseteq H \subseteq \mathbb{H}(\mathbb{R})$,

(ii) H tvoří se sčítáním a násobením kvaternionů obor,

(iii) $N(\theta) \in \mathbb{N}_0$ pro každé $\theta \in H$,

(iv) H je levým i pravým oborem hlavních ideálů.

Poznámka. Hurwitzovy kvaterniony tedy představují silný kvaternionový obor.

Lemma 2.3.2. *Budiž H silný kvaternionový obor. Potom je $\varepsilon \in H$ jednotkou, právě pokud $N(\varepsilon) = 1$.*

Důkaz. Pokud $N(\varepsilon) = 1$, pak $\varepsilon\overline{\varepsilon} = 1$, přičemž z

$$\varepsilon + \overline{\varepsilon} = (\varepsilon + 1)(\overline{\varepsilon} + 1) - \varepsilon\overline{\varepsilon} - 1 = N(\varepsilon + 1) - N(\varepsilon) - 1 \in \mathbb{Z} \subseteq H$$

je i $\overline{\varepsilon} \in H$, pročež je ε jednotkou. Naopak pokud je ε jednotkou, pak existuje $\varphi \in H$ takové, že $\varepsilon\varphi = 1$. Potom ale vzetím norem díky $N(\varepsilon), N(\varphi) \in \mathbb{N}_0$ nutně $N(\varepsilon) = N(\varphi) = 1$. □

Věta 2.3.3. *Budiž H silný kvaternionový obor. Pro libovolná nenulová $\theta \in H, m \in \mathbb{Z}$ nechť je $g = \mathrm{NSD}(m, N(\theta))$. Potom platí $H\theta + Hm = H\lambda$ (resp. $\theta H + mH = \lambda H$) pro nějaké $\lambda \in H$ splňující $g \mid N(\lambda)$.*

Důkaz. Důkaz proveďme pro levé ideály, pro pravé lze postupovat obdobně.
$H\theta + Hm$ je levým ideálem H, pročež z definice silného kvaternionového oboru musí být hlavní, neboli roven $H\lambda$ pro nějaké $\lambda \in H$. Platnost $H\theta + Hm = H\lambda$ speciálně implikuje existenci $\alpha, \beta \in H$ takových, že

$$\begin{aligned} \alpha\theta + \beta m &= \lambda, \\ \alpha\theta &= \lambda - \beta m. \end{aligned}$$

Vzetím normy na obou stranách pak

$$\begin{aligned} N(\alpha)N(\theta) &= (\lambda - \beta m)\,\overline{(\lambda - \beta m)} = \\ &= (\lambda - \beta m)\left(\overline{\lambda} - \overline{\beta} m\right) = N(\lambda) - m\left(\beta\overline{\lambda} + \lambda\overline{\beta}\right) + m^2 N(\beta). \end{aligned} \tag{2.2}$$

Platí

$$\begin{aligned} \beta\overline{\lambda} + \lambda\overline{\beta} &= \left(\beta\overline{\beta} + \beta\overline{\lambda} + \lambda\overline{\beta} + \lambda\overline{\lambda}\right) - \beta\overline{\beta} - \lambda\overline{\lambda} = \\ &= (\beta + \lambda) \cdot \overline{(\beta + \lambda)} - \beta\overline{\beta} - \lambda\overline{\lambda} = N(\beta + \lambda) - N(\beta) - N(\lambda), \end{aligned}$$

což vzhledem k definici silného kvaternionového oboru musí být celé číslo. V rovnici (2.2) tedy vystupují celá čísla, pročež vzetím mod g obdržíme

$$0 \equiv N(\lambda) \pmod{g}.$$ □

Věta 2.3.4. *Budiž H silný kvaternionový obor. Mějme ireducibilní $\pi \in H$ a uvažujme libovolné prvočíslo p, jež dělí $N(\pi)$. Potom $p \in H\pi$.*

Důkaz. Pro spor nechť $p \notin H\pi$. Nechť je $H\pi + Hp = H\lambda$ – větou 2.3.3 je potom $p = \mathrm{NSD}\,(p, N(\pi)) \mid N(\lambda)$, neboli λ není jednotkou. Platí $\pi \in H\lambda$, neboli $\pi = \alpha\lambda$ pro nějaké $\alpha \in H$. Dále je $p \in H\lambda$, ale zároveň $p \notin H\pi$, pročež určitě $H\pi \neq H\lambda$, a tudíž α není jednotkou. Vyjádřili jsme tedy π jako součin dvou nejednotek – musí tak být reducibilní, což je spor. □

Definice 2.3.5. Obor $H \subseteq \mathbb{H}(\mathbb{R})$ nazvěme *prvorozloženým*, pokud pro každé prvočíslo p existuje $\theta \in H$ takové, že $p \mid N(\theta)$, ale $p^2 \nmid N(\theta)$.

Poznámka. Hurwitzovy kvaterniony jsou tedy dle lemmatu 2.2.2 prvorozloženým oborem.

Věta 2.3.6. *Budiž H prvorozložený silný kvaternionový obor. Potom je libovolné prvočíslo p v H reducibilní.*

Důkaz. Z definice 2.3.5 existuje alespoň jedno $n \in \mathbb{N}, p \nmid n$ takové, že existuje $\theta \in H$ splňující $N(\theta) = np$. Zvolme nejmenší přirozené n s touto vlastností a uvažujme příslušné θ – to pak uvážením normy nemůže být jednotkou. Pro spor nechť je p ireducibilní v H. Potom musí být $n > 1$, neboť jinak $p = \theta\overline{\theta}$, což značí reducibilitu p.

Ukažme, že θ je reducibilní. Nechť je pro spor ireducibilní – potom větou 2.3.4 platí $p \in H\theta$, neboli existuje $\eta \in H$ splňující $p = \eta\theta$. Potom vzetím normy na obou stranách obdržíme

$$\begin{aligned} p^2 &= N(\eta) \cdot np, \\ p &= n \cdot N(\eta) = n\eta\overline{\eta}. \end{aligned}$$

Z ireducibility p musí právě dvě z $n, \eta, \overline{\eta}$ být jednotkami. Přitom ale vzhledem k $N(\eta) = N(\overline{\eta})$ je η jednotkou, právě pokud je jí $\overline{\eta}$. Obě $\eta, \overline{\eta}$ nemohou být nejednotkami, jsou tedy obě jednotkami. Z toho

$$p = nN(\eta) = n.$$

Přitom ale máme $p \nmid n$ – tedy spor.

θ je tedy reducibilní, neboli platí $\theta = \theta_1\theta_2$ pro nějaké nejednotky $\theta_1, \theta_2 \in H$. Zřejmě právě jedna z norem $N(\theta_1), N(\theta_2)$ musí být násobkem p. Nechť je to bez újmy na obecnosti $N(\theta_1)$, tj. budiž $N(\theta_1) = n_1 p$ pro nějaké $n_1 \in \mathbb{N}, p \nmid n_1$. Pokud $n_1 = n$, pak nutně $N(\theta_2) = 1$, pročež je θ_2 jednotkou, což je spor. Nutně tedy musí být $n_1 < n$. Přitom ale n_1 má tu vlastnost, že existuje $\theta_1 \in H$ splňující $N(\theta_1) = n_1 p$. To je spor s tím, jak bylo zvoleno původní n, pročež p nemůže být ireducibilní. □

Věta 2.3.7. *Budiž H prvorozložený silný kvaternionový obor. Potom pro libovolné $n \in \mathbb{N}$ existuje $\theta \in H$ splňující $N(\theta) = n$.*

Důkaz. Začněme případem, kdy je n rovno nějakému prvočíslu p. Dle věty 2.3.6 je p reducibilní v H, neboli existují nejednotková $\alpha, \beta \in H$ splňující $p = \alpha\beta$. Z toho vzetím normy na obou stranách

$$p^2 = N(p) = N(\alpha)N(\beta).$$

Vzhledem k $N(\alpha), N(\beta) > 1$ pak jistě $N(\alpha) = N(\beta) = p$, pročež věta pro prvočísla vskutku platí.

Mějme nyní libovolné přirozené n. Pokud $n = 1$, máme splněno skrze $N(1) = 1$. Nadále tedy berme $n > 1$ a uvažujme nějaký rozklad

$$n = \prod_{s=1}^{m} p_s,$$

kde $m \geq 1$ a všechna p_s jsou (ne nutně různá) prvočísla. Z platnosti věty pro prvočísla pro každé $s \in \{1, \ldots, m\}$ existuje $\theta_s \in H$ splňující $N(\theta_s) = p_s$. Potom stačí vzít

$$\theta = \prod_{s=1}^{m} \theta_s,$$

čímž bude zaručeno

$$N(\theta) = N\left(\prod_{s=1}^{m} \theta_s\right) = \prod_{s=1}^{m} N(\theta_s) = \prod_{s=1}^{m} p_s = n. \qquad \square$$

Důsledek (Lagrangeova věta o čtyřech čtvercích)**.** *Každé přirozené číslo n lze vyjádřit jako součet čtyř čtverců.*

Důkaz. $\mathbb{J}$ je prvorozložený silný kvaternionový obor, pročež právě dokázanou větou existuje $\theta \in \mathbb{J}$ takové, že $N(\theta) = n$. Potom lemmatem 2.2.3 existuje i $\lambda \in \mathbb{H}(\mathbb{Z})$ takové, že $N(\lambda) = n$. Přitom ale $\lambda = x + yi + zj + wk$ pro nějaká $x, y, z, w \in \mathbb{Z}$, čímž

$$n = N(\lambda) = x^2 + y^2 + z^2 + w^2. \qquad \square$$

Kapitola 3

Zobecnění Lagrangeovy věty

V této kapitole zavedeme několik nových oborů, o nichž ukážeme, že jsou silnými kvaternionovými obory. Spolu s teorií předchozí kapitoly nám toto umožní ukázat, že kvadratické formy, které udávají jejich normu, nabývají všech nezáporných celých hodnot, neboli dokážeme obdobu Lagrangeovy věty pro některé další kvadratické formy.

Po celou tuto kapitolu držme následující značení: buďte zvolena $A, B \in \mathbb{N}, \mu, \nu \in \mathbb{Z}$ a pojmenujme

$$S = 4A - \mu^2, \qquad T = BS - \nu^2;$$

uvažujme pouze takové čtveřice (A, B, μ, ν), pro něž je $S, T > 0$. Zkoumat pak budeme formy tvaru

$$(x^2 + \mu xy + Ay^2) + \nu(yz - xw) + B(z^2 + \mu zw + Aw^2). \tag{3.1}$$

Ty, jejichž univerzálnost (viz sekci 3.1) dokážeme, jsou zaneseny v tabulce 2. Jak také ukážeme, tyto formy jsou po dvou neekvivalentní, což plyne vždy buď z různosti jejich T (viz sekci 3.1), nebo z různosti počtu vyjádření některého přirozeného n těmito formami (viz výsledky kapitoly 4).

T	S	(A, B, μ, ν)	Kvadratická forma (3.1)
2	3	$(1, 1, 1, 1)$	$(x^2 + xy + y^2) + (yz - xw) + (z^2 + zw + w^2)$
3	3	$(1, 1, 1, 0)$	$(x^2 + xy + y^2) + (z^2 + zw + w^2)$
5	3	$(1, 2, 1, 1)$	$(x^2 + xy + y^2) + (yz - xw) + 2(z^2 + zw + w^2)$
6	7	$(2, 1, 1, 1)$	$(x^2 + xy + 2y^2) + (yz - xw) + (z^2 + zw + 2w^2)$
	3	$(1, 2, 1, 0)$	$(x^2 + xy + y^2) + 2(z^2 + zw + w^2)$
7	7	$(2, 1, 1, 0)$	$(x^2 + xy + 2y^2) + (z^2 + zw + 2w^2)$
10	7	$(2, 2, 1, 2)$	$(x^2 + xy + 2y^2) + 2(yz - xw) + 2(z^2 + zw + 2w^2)$
	11	$(3, 1, 1, 0)$	$(x^2 + xy + 3y^2) + (z^2 + zw + 3w^2)$
14	7	$(2, 2, 1, 0)$	$(x^2 + xy + 2y^2) + 2(z^2 + zw + 2w^2)$
15	8	$(2, 2, 0, 1)$	$(x^2 + 2y^2) + (yz - xw) + 2(z^2 + 2w^2)$
21	7	$(2, 3, 1, 0)$	$(x^2 + xy + 2y^2) + 3(z^2 + zw + 2w^2)$
22	11	$(3, 2, 1, 0)$	$(x^2 + xy + 3y^2) + 2(z^2 + zw + 3w^2)$

Tabulka 2: Formy tvaru (3.1), jejichž univerzálnost bude dokázána.

3.1 Ekvivalence kvadratických forem

Definice 3.1.1. *Kvadratickou formou* rozumějme homogenní kvadratický polynom (v jedné či více proměnných) s celočíselnými koeficienty. O dvou kvadratických formách f, g v m proměnných řekněme, že jsou *ekvivalentní*, existuje-li

$$A = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1m} \\ a_{21} & a_{22} & \cdots & a_{2m} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mm} \end{pmatrix} \in \mathrm{M}_m(\mathbb{Z})$$

splňující $|\det A| = 1$ a zároveň

$$g(x_1, \ldots, x_m) = f\left(\sum_{\ell=1}^{m} a_{1\ell}x_\ell, \ldots, \sum_{\ell=1}^{m} a_{m\ell}x_\ell\right).$$

Konečně nazvěme kvadratickou formu f v m proměnných *univerzální*, pokud pro každé $n \in \mathbb{N}$ existují $x_1, \ldots, x_m \in \mathbb{Z}$ taková, že $f(x_1, \ldots, x_m) = n$.

Pojem ekvivalence kvadratických forem si lze vyložit následovně: formy f, g jsou ekvivalentní, pokud f přechází v g dosazením vždy nějaké celočíselné lineární kombinace proměnných $x_1, \ldots, x_n$ za každé z $x_1, \ldots, x_n$. Podmínka $|\det A| = 1$ zaručuje, že existuje inverzní matice $A^{-1} \in \mathrm{M}_n(\mathbb{Z})$ (toto tvrzení ponechme bez důkazu), jež splní

$$AA^{-1} = A^{-1}A = I$$

(kde I značí jednotkovou matici $n \times n$) a která tedy představuje substituci, kterou g přejde nazpět v f. Tím je tak zaručeno, že ekvivalence představuje tzv. *symetrickou* relaci – f je ekvivalentní g, právě pokud je g ekvivalentní f.

Věta 3.1.2. *Pojmenujme $f(x, y, z, w)$ kvadratickou formu* (3.1)*. Potom je f až na ekvivalenci jednoznačně určena trojicí $(S, T, \nu \pmod S)$.*

Důkaz. Forma f je zřejmě jednoznačně určena čtveřicí (S, T, ν, μ), neboť A, B lze z těchto čísel dopočíst[5]. Ukažme nejprve, že f je jednoznačně určena trojicí (S, T, ν).

Parita μ je dána paritou S. Uzřeme nyní

$$\begin{aligned} f(x \pm y, y, z \pm w, w) &= (x \pm y)^2 + \mu(x \pm y)y + Ay^2 + \nu(y(z \pm w) - (x \pm y)w) + \\ &\quad + B((z \pm w)^2 + \mu(z \pm w)w + Aw^2) \\ &= (x^2 + (\mu \pm 2)xy + (A \pm \mu + 1)y^2) + \nu(yz - xw) + \\ &\quad + B(z^2 + (\mu \pm 2)zw + (A \pm \mu + 1)w^2). \end{aligned}$$

Přitom

$$4(A \pm \mu + 1) - (\mu \pm 2)^2 = 4A - \mu^2 \pm 4\mu + 4 \mp 4\mu - 4 = 4A - \mu^2 = S,$$

takže forma s odpovídající čtveřicí (S, T, μ, ν) je ekvivalentní formě s čtveřicí $(S, T, \mu \pm 2, \nu)$. Z toho je vzhledem k pevně dané paritě μ tato forma ekvivalentní všem s danými hodnotami (S, T, ν).

[5] To však neznamená, že každé čtveřici (S, T, μ, ν) přísluší nějaká odpovídající čtveřice (A, B, μ, ν).

Nyní proveďme obdobnou věc pro ν. Uzřeme

$$\begin{aligned}&f(x \mp \mu z \mp 2Aw, y \pm 2z \pm \mu w, z, w) = (x \mp \mu z \mp 2Aw)^2 + \\ &+ \mu(x \mp \mu z \mp 2Aw)(y \pm 2z \pm \mu w) + A(y \pm 2z \pm \mu w)^2 + \nu((y \pm 2z \pm \mu w)z - \\ &- (x \mp \mu z \mp 2Aw)w) + B(z^2 + \mu zw + Aw^2) = \\ &= x^2 + \mu xy + Ay^2 + (\nu \pm S)(yz - xw) + (B + S \pm 2\nu)(z^2 + \mu zw + Aw^2).\end{aligned}$$

Přitom

$$(B + S \pm 2\nu)S - (\nu \pm S)^2 = BS - \nu^2 + S^2 \pm 2S\nu \mp 2S\nu - S^2 = BS - \nu^2 = T,$$

takže forma s odpovídající trojicí (S, T, ν) je ekvivalentní formě s odpovídající trojicí $(S, T, \nu \pm S)$. Z toho je tedy ekvivalentní všem formám s danými hodnotami (S, T) a s ν dávajícím týž zbytek mod S. Tímto je věta dokázána. □

Důsledek. *Až na ekvivalenci existuje jen konečně mnoho forem tvaru* (3.1) *s danými hodnotami* S, T.

Povšimnout si lze též toho, že

$$f(-x, -y, z, w) = (x^2 + \mu xy + Ay^2) - \nu(yz - xw) + B(z^2 + \mu zw + Aw^2),$$

neboli forma s odpovídající trojicí (S, T, ν) a forma s trojicí $(S, T, -\nu)$ jsou si ekvivalentní. Pro ta S, jež mají tu vlastnost, že $a^2 \equiv b^2 \pmod S$, právě pokud $a \equiv \pm b \pmod S$ (to jsou právě čísla $2, 4$ a $p^\ell, 2p^\ell$ pro liché prvočíslo p a $\ell \in \mathbb{N}$), je tedy forma (3.1) jednoznačně dána už dvojicí (S, T). Dále si povšimněme, že pro $B = 1$ platí

$$f(-x, w, z, y) = x^2 + \nu xy + Ay^2 + \mu(yz - xw) + z^2 + \nu zw + Aw^2,$$

neboli forma s odpovídající trojicí (S, T, ν) je ekvivalentní formě s trojicí (S, T, μ).

V sekci 3.3 (s využitím poznatků sekcí 3.2 a 2.3) dokážeme univerzálnost několika forem s využitím bezčtvercovosti T a podmínky $\frac{12}{T} - \frac{S}{T} - \frac{4}{S} > 0$ – zde ukážeme, že všechny formy toto splňující jsou již uvedeny (až na ekvivalenci) v tabulce 2. Univerzálnost zbylých forem pak dokážeme v sekci 3.4 odlišnou metodou – nalezneme obor $G \supset H$, o němž ukážeme, že je izomorfní některému oboru, jehož prvorozloženost a silná kvaternionovost je již známa, a následně z toho vyvodíme, že i v H pro každé $n \in \mathbb{N}$ existuje λ takové, že $N(\lambda) = n$.

Nejprve $\frac{12}{T} - \frac{S}{T} - \frac{4}{S} > 0$ ekvivalentně upravme do tvaru

$$\begin{aligned}12S - S^2 - 4T > 0,& \\ T < 3S - \frac{S^2}{4} = 9 - \left(\frac{S}{2} - 3\right)^2 \leq 9.&\end{aligned}$$

Tuto nerovnost lze též upravit do tvaru

$$\begin{aligned}S^2 - 12S + 4T < 0,& \\ 6 - 2\sqrt{9 - T} < S < 6 + 2\sqrt{9 - T}.&\end{aligned} \tag{3.2}$$

Často též budeme využívat toho, že $\nu^2 = BS - T \equiv -T \pmod S$ musí být kvadratický zbytek mod S. Projděme tedy postupně bezčtvercová přirozená T menší než 9, tj. $T \in \{1, 2, 3, 5, 6, 7\}$.

(i) $T = 1$. Potom musí $\nu^2 = BS - 1 \equiv -1 \pmod{S}$ být kvadratický zbytek mod S. Přitom ale S je vzhledem k $S = 4A - \mu^2$ buďto násobek čtyř, anebo dává zbytek $-1 \pmod 4$. V prvém případě tedy -1 nemůže být kvadratickým zbytkem mod 4, a tedy ani mod S. V druhém případě je mezi děliteli S nějaké prvočíslo q, jež dává zbytek $-1 \pmod 4$, přitom je známo, že pro takové q není $-1 \pmod q$ kvadratickým zbytkem (toto plyne z Eulerova kritéria). Toto je dohromady spor, pročež $T = 1$ nemůže nastat.

(ii) $T = 2$. Potom dle (3.2) uvažujeme $1 \leq S \leq 11$, tj. $S \in \{3, 4, 7, 8, 11\}$. Přitom -2 není kvadratickým zbytkem mod 4, mod 7 a mod 8. Dále jsou 3 a 11 prvočísla, pročež existuje až na ekvivalenci pouze jedna forma s $(S, T) = (3, 2)$ a pouze jedna s $(S, T) = (11, 2)$. Stačí tedy ukázat, že tyto dvě formy si jsou ekvivalentní. To uzřeme následovně: forma s $(A, B, \mu, \nu) = (3, 1, 1, 3)$ má $(S, T) = (11, 2)$, přitom ale díky $B = 1$ lze, jak bylo ukázáno výše, zaměnit μ a ν a obdržet formu $(A, B, \mu, \nu) = (3, 1, 3, 1)$, neboli $(S, T) = (3, 2)$.

(iii) $T = 3$. Potom dle (3.2) uvažujeme $2 \leq S \leq 10$, tj. $S \in \{3, 4, 7, 8\}$. Přitom -3 není kvadratickým zbytkem mod 8. Dále mají 3, 4 a 7 tu vlastnost, že existuje až na ekvivalenci pouze jedna forma s každým $(S, T) = (3, 3)$, $(S, T) = (4, 3)$ a $(S, T) = (7, 3)$. Stačí tedy ukázat, že tyto tři formy jsou si navzájem ekvivalentní. Forma s $(A, B, \mu, \nu) = (1, 1, 0, 1)$ má $(S, T) = (4, 3)$, přitom ale záměnou μ, ν je ekvivalentní formě s $(A, B, \mu, \nu) = (1, 1, 1, 0)$, neboli $(S, T) = (3, 3)$. Podobně forma s $(A, B, \mu, \nu) = (2, 1, 1, 2)$, tj. $(S, T) = (7, 3)$, je ekvivalentní formě s $(A, B, \mu, \nu) = (2, 1, 2, 1)$, tj. $(S, T) = (4, 3)$.

(iv) $T = 5$. Potom dle (3.2) uvažujeme $3 \leq S \leq 9$, tj. $S \in \{3, 4, 7, 8\}$. Přitom -5 není kvadratickým zbytkem mod 4 a mod 8. Budiž $f(x, y, z, w)$ forma (3.1) při volbě $(A, B, \mu, \nu) = (2, 2, 1, 3)$, tedy $(S, T) = (7, 5)$. Potom platí

$$\begin{aligned} f(x + w, y, -y - z - w, w) &= (x + w)^2 + (x + w)y + 2y^2 - 3y(y + z + w) - \\ &\quad - 3(x + w)w + 2((y + z + w)^2 - (y + z + w)w + 2w^2), \\ &= (x^2 + xy + y^2) + (yz - xw) + (z^2 + zw + w^2), \end{aligned}$$

což je forma s $(S, T) = (3, 5)$.

(v) $T = 6$. Potom dle (3.2) uvažujeme $3 \leq S \leq 9$, tj. $S \in \{3, 4, 7, 8\}$. Přitom -6 není kvadratickým zbytkem mod 4 a mod 8. Zbývají tedy formy s $S \in \{3, 7\}$, jež jsou obě zastoupeny v tabulce 2.

(vi) $T = 7$. Potom dle (3.2) uvažujeme $4 \leq S \leq 8$, tj. $S \in \{4, 7, 8\}$. Ukažme nejprve, že všechny formy s $(S, T) = (8, 7)$ jsou si navzájem ekvivalentní. Díky větě 3.1.2 jsou si jistě ekvivalentní všechny takové formy s $\nu \equiv \pm 1 \pmod 8$ a všechny s $\nu \equiv \pm 3 \pmod 8$. Pojmenujeme-li $f(x, y, z, w)$ formu (3.1) pro $(A, B, \mu, \nu) = (2, 1, 0, 1)$, platí

$$\begin{aligned} f(x + 2w, y - z, z, w) &= (x + 2w)^2 + 2(y - z)^2 + z^2 + 2w^2 + (y - z)z - (x + 2w)w, \\ &= (x^2 + 2y^2) - 3(yz - xw) + 2(z^2 + 2w^2), \end{aligned}$$

což je forma s $(S, T) = (8, 7)$ a zároveň $\nu \equiv -3 \pmod 8$. Dále záměnou μ, ν je f ekvivalentní formě s $(A, B, \mu, \nu) = (2, 1, 1, 0)$, tj. $(S, T) = (7, 7)$. Podobně pokud

$g(x,y,z,w)$ je forma (3.1) s $(A,B,\mu,\nu)=(1,2,0,1)$, a tedy $(S,T)=(4,7)$, pak

$$f(x,z,w,-y)=(x^2+xy+2y^2)+(z^2+zw+2w^2),$$

což je opět forma s $(S,T)=(7,7)$.

Tímto je tedy dokázáno, že podmínku $\frac{12}{T}-\frac{S}{T}-\frac{4}{S}>0$ splňují až na ekvivalenci právě formy zanesené v tabulce 2.

Závěrem sekce stručně zmiňme, že pokud jsou dvě formy tvaru 3.1 ekvivalentní, pak už jim určitě přísluší stejné T. Pro libovolnou formu f tvaru 3.1 totiž platí

$$f(x,y,z,w)=\left(x+y\frac{\mu}{2}-w\frac{\nu}{2}\right)^2+\left(y\frac{\sqrt{S}}{2}+z\frac{\nu}{\sqrt{S}}+w\frac{\mu\nu}{2\sqrt{S}}\right)^2+$$
$$+\left(z\sqrt{\frac{T}{S}}+w\frac{\mu}{2}\sqrt{\frac{T}{S}}\right)^2+\left(w\frac{\sqrt{T}}{2}\right)^2,$$
$$\begin{vmatrix}1&\frac{\mu}{2}&0&-\frac{\nu}{2}\\0&\frac{\sqrt{S}}{2}&\frac{\nu}{\sqrt{S}}&\frac{\mu\nu}{2\sqrt{S}}\\0&0&\sqrt{\frac{T}{S}}&\frac{\mu}{2}\sqrt{\frac{T}{S}}\\0&0&0&\frac{\sqrt{T}}{2}\end{vmatrix}=\frac{T}{4},$$

neboli forma $x^2+y^2+z^2+w^2$ přechází v f substitucí o determinantu $\frac{T}{4}$. Potom se naopak množina

$$M_f=\{(x,y,z,w):x,y,z,w\in\mathbb{R}\wedge f(x,y,z,w)\leq 1\}$$

v lineárním zobrazení daném maticí této substituce obrazuje na jednotkovou nadkouli se středem v počátku. Z toho musí nadobjem jednotkové nadkoule být $\frac{T}{4}$-násobkem $\operatorname{Vol} M_f$ (viz sekci 1.2). Jsou-li pak f,g dvě ekvivalentní formy tvaru (3.1) s příslušejícími čísly T_f,T_g a množinami M_f,M_g definovanými tak jako výše, musí platit

$$\frac{\operatorname{Vol} M_f}{\operatorname{Vol} M_g}=\frac{T_g}{T_f}.$$

Formy f,g jsou však ekvivalentní, neboli existuje substituce o determinantu ±1, kterou f přechází v g. Potom se ale opět v lineárním zobrazení daném maticí této substituce musí M_g zobrazovat na M_f, neboli

$$\operatorname{Vol} M_f=|\pm1|\cdot\operatorname{Vol} M_g.$$

Z toho už snadno $T_f=T_g$.

3.2 Další silné kvaternionové obory

Předpokládáme $S,T>0$. Zaveďme tedy

$$\alpha_1=\frac{\mu}{2},\qquad \beta_1=\frac{\nu}{\sqrt{S}},$$
$$\alpha_2=\frac{\sqrt{S}}{2},\qquad \beta_2=\sqrt{\frac{T}{S}},$$
$$\alpha=\alpha_1+\alpha_2 i,\qquad \beta=\beta_1 i+\beta_2 j$$

a (jak ukážeme) obor

$$H = \{x + y\alpha + z\beta + w\alpha\beta : x, y, z, w \in \mathbb{Z}\}, \tag{3.3}$$

který představuje podobor oboru $\mathbb{H}(\mathbb{R})$. Toto značení opět držme po zbytek kapitoly. Povšimněme si též, že $\mathbb{H}(\mathbb{Z})$ je speciálním případem oboru H (volbou $A = B = 1, \mu = \nu = 0$).

Věta 3.2.1. *Množina H zadaná vztahem* (3.3) *tvoří se sčítáním a násobením kvaternionů obor a navíc splňuje i podmínky* (i) *a* (iii) *definice 2.3.1.*

Důkaz. Splnění podmínky (i) je zcela zřejmé. Dále vypočtěme

$$\alpha\beta = -\alpha_2\beta_1 + \alpha_1\beta_1 i + \alpha_1\beta_2 j + \alpha_2\beta_2 k.$$

Poté uzřeme

$$\begin{aligned}
\alpha + \overline{\alpha} &= 2\alpha_1 = \mu \in \mathbb{Z}, \\
\beta + \overline{\beta} &= \beta - \beta = 0 \in \mathbb{Z}, \\
\alpha\beta + \overline{(\alpha\beta)} &= -2\alpha_2\beta_1 = -2 \cdot \frac{\sqrt{4A - \mu^2}}{2} \cdot \frac{\nu}{\sqrt{4A - \mu^2}} = -\nu \in \mathbb{Z}.
\end{aligned}$$

Z toho už pro libovolné $\theta = x + y\alpha + z\beta + w\alpha\beta \in H$ musí být

$$\theta + \overline{\theta} = 2x + y\left(\alpha + \overline{\alpha}\right) + z\left(\beta + \overline{\beta}\right) + \left(\alpha\beta + \overline{(\alpha\beta)}\right) = 2x + y\mu - w\nu \in \mathbb{Z}.$$

Nyní dokažme, že H splňuje podmínku (ii) definice 2.3.1, tj. že tvoří obor. Vzhledem k $H \subseteq \mathbb{H}(\mathbb{R})$ stačí dokázat jeho uzavřenost na sčítání a násobení. Díky tomu, že prvky H jsou právě všechny celočíselné lineární kombinace $1, \alpha, \beta, \alpha\beta$, je uzavřenost na sčítání zcela zřejmá. Dokažme tedy uzavřenost na násobení. K tomu (vzhledem k distributivitě násobení na sčítání) postačí ukázat $\theta_1\theta_2 \in H$ pro $\theta_1, \theta_2 \in \{1, \alpha, \beta, \alpha\beta\}$.

Pro $1 \in \{\theta_1, \theta_2\}$ je toto zcela zřejmo. Dále si postupně povšimněme

$$\begin{aligned}
\alpha^2 &= \alpha_1^2 - \alpha_2^2 + 2\alpha_1\alpha_2 i = \frac{\mu^2 - (4A - \mu^2) + 2\mu i\sqrt{4A - \mu^2}}{4} = \\
&= -A + \mu \cdot \frac{\mu + i\sqrt{4A - \mu^2}}{2} = \mu\alpha - A \in H, \\
\beta^2 &= \beta \cdot \left(-\overline{\beta}\right) = -N(\beta) = -\frac{\nu^2 + 4AB - B\mu^2 - \nu^2}{4A - \mu^2} = -\frac{4AB - B\mu^2}{4A - \mu^2} = -B, \\
\beta\alpha &= \overline{\left(\overline{\alpha}\overline{\beta}\right)} = \overline{(\mu - \alpha)(-\beta)} = \overline{\alpha\beta - \mu\beta} = \overline{\alpha\beta} - \mu\overline{\beta} = -\nu - \alpha\beta + \mu\beta \in H.
\end{aligned}$$

Z těchto tří vztahů již snadno odvodíme i

$$\begin{aligned}
\alpha \cdot \alpha\beta &= \alpha^2\beta = (\mu\alpha - A)\beta = \mu\alpha\beta - A\beta \in H, \\
\alpha\beta \cdot \alpha &= \alpha \cdot \beta\alpha = \alpha(-\nu - \alpha\beta + \mu\beta) = -\nu\alpha + \mu\alpha\beta - \alpha^2\beta = \\
&= -\nu\alpha + \mu\alpha\beta - (\mu\alpha\beta - A\beta) = -\nu\alpha + A\beta \in H, \\
\alpha\beta \cdot \beta &= \alpha \cdot \beta^2 = -B\alpha \in H, \\
\beta \cdot \alpha\beta &= \beta\alpha \cdot \beta = (-\nu - \alpha\beta + \mu\beta)\beta = -\nu\beta - \alpha\beta^2 + \mu\beta^2 = -\nu\beta - (-B\alpha) - B\mu = \\
&= -\nu\beta + B\alpha - B\mu \in H, \\
\alpha\beta \cdot \alpha\beta &= (\alpha\beta\alpha)\beta = (-\nu\alpha + A\beta)\beta = -\nu\alpha\beta + A\beta^2 = -\nu\alpha\beta - AB \in H.
\end{aligned}$$

	1	α	β	$\alpha\beta$
1	1	α	β	$\alpha\beta$
α	α	$\mu\alpha - A$	$\alpha\beta$	$\mu\alpha\beta - A\beta$
β	β	$-\nu - \alpha\beta + \mu\beta$	$-B$	$-\nu\beta + B\alpha - B\mu$
$\alpha\beta$	$\alpha\beta$	$-\nu\alpha + A\beta$	$-B\alpha$	$-\nu\alpha\beta - AB$

Tabulka 3: Multiplikační tabulka bází oboru H.

Toto lze shrnout tabulkou 3. Tímto je dokázáno, že H je obor.

Konečně dokažme splnění podmínky (iii). Doplňme ještě, že platí

$$N(\alpha) = \frac{1}{4}\left(\mu^2 + 4A - \mu^2\right) = A,$$
$$N(\beta) = \frac{\nu^2 + 4AB - B\mu^2 - \nu^2}{4A - \mu^2} = \frac{4AB - B\mu^2}{4A - \mu^2} = B.$$

Pro $\theta = x + y\alpha + z\beta + w\alpha\beta \in H$ pak platí

$$\begin{aligned}
N(\theta) &= (x + y\alpha_1 - w\alpha_2\beta_1)^2 + (y\alpha_2 + z\beta_1 + w\alpha_1\beta_1)^2 + (z\beta_2 + w\alpha_1\beta_2)^2 + (w\alpha_2\beta_2)^2 = \\
&= x^2 + y^2\left(\alpha_1^2 + \alpha_2^2\right) + z^2\left(\beta_1^2 + \beta_2^2\right) + w^2\left((\alpha_2\beta_1)^2 + (\alpha_1\beta_1)^2 + (\alpha_1\beta_2)^2 + (\alpha_2\beta_2)^2\right) + \\
&\quad + 2\alpha_1 xy - 2\alpha_2\beta_1 xw + 2\alpha_2\beta_1 yz + 2zw\left(\alpha_1\beta_1^2 + \alpha_1\beta_2^2\right) + \\
&\quad + 2yw\left(-\alpha_1\alpha_2\beta + \alpha_2\alpha_1\beta\right) = \\
&= x^2 + Ay^2 + Bz^2 + w^2 N(\alpha\beta) + \mu xy - \nu xw + \nu yz + 2\alpha_1 Bzw = \\
&= \left(x^2 + \mu xy + Ay^2\right) + \nu\left(yz - xw\right) + B\left(z^2 + \mu zw + Aw^2\right),
\end{aligned}$$

což je zcela zřejmě celé číslo. Na závěr důkazu ještě zmiňme, že pokud $\theta = 0$, musí být

$$w\alpha_2\beta_2 = z\beta_2 + w\alpha_1\beta_2 = y\alpha_2 + z\beta_1 + w\alpha_1\beta_1 = x + y\alpha_1 - w\alpha_2\beta_1 = 0,$$

z čehož postupně $x = y = z = w = 0$, což značí, že zobrazení $(x, y, z, w) \mapsto x + y\alpha + z\beta + w\alpha\beta$ je prosté. □

Nyní postupně dokažme, že pro bezčtvercové T (takové, které není dělitelné čtvercem žádného přirozeného čísla) je obor H prvorozložený.

Lemma 3.2.2. *Budiž p liché prvočíslo a mějme $a, b, c \in \mathbb{Z}$ taková, že alespoň jedno z a, b není násobkem p. Potom polynom $ax^2 + bx + c$ nabývá* mod p *alespoň $\frac{p+1}{2}$ různých hodnot.*

Důkaz. Uvažujme $x, y \in \mathbb{Z}$ taková, že

$$ax^2 + bx + c \equiv ay^2 + by + c \pmod{p}. \tag{3.4}$$

To je ekvivalentní

$$a(x^2 - y^2) + b(x - y) \equiv 0 \pmod{p},$$
$$(x - y)(a(x + y) + b) \equiv 0 \pmod{p}.$$

Poslední kongruence je splněna, právě pokud $x \equiv y \pmod{p}$ nebo $a(x+y)+b \equiv 0 \pmod{p}$. Pokud $p \mid a$, pak z podmínky $p \nmid b$, pročež nikdy neplatí $a(x + y) + b \equiv 0 \pmod{p}$, neboli (3.4) platí, právě pokud $x \equiv y \pmod{p}$. Polynom $ax^2 + bx + c$ tedy nabývá $p > \frac{p+1}{2}$ různých hodnot.

Dále nechť $p \nmid a$. Potom platí $a(x + y) + b \equiv 0 \pmod{p}$, právě pokud $x \equiv -a^{-1}b - y \pmod{p}$. Všechna y kromě $-(2a)^{-1}b$ tak k sobě mají právě jedno různé x, které splní (3.4). Tento polynom tedy dohromady dává $\frac{p-1}{2} + 1 = \frac{p+1}{2}$ různých hodnot. □

Lemma 3.2.3. *Budiž p prvočíslo, jež nedělí T. Potom existují $x, z \in \mathbb{Z}$ taková, že $p \mid N(x+\alpha+z\beta)$.*

Poznámka. Toto je zobecnění myšlenky z důkazu lemmatu 2.2.2.

Důkaz. Pojmenujme $\theta = x+\alpha+z\beta$ pro zatím nespecifikovaná x, z. Rozlišme dva případy.

(i) Je $p = 2$. Potom díky $x^2 \equiv x \pmod 2$ platí

$$N(\theta) = x^2 + \mu x + A + \nu z + Bz^2 \equiv A + (\mu+1)x + (B+\nu)z \pmod 2.$$

Pokud $\mu + 1 \not\equiv 0 \pmod 2$, pak jistě pro $x \equiv 0$ a $x \equiv 1 \pmod 2$ nabude $N(\theta)$ dvou různých hodnot mod 2, neboli $N(\theta) \equiv 0 \pmod 2$ bude mít řešení. Obdobně pokud $B+\nu \not\equiv 0 \pmod 2$, má $N(\theta) \equiv 0 \pmod 2$ řešení. Pokud $\mu+1 \equiv B+\nu \equiv 0 \pmod 2$, pak nutně $\mu \equiv 1 \pmod 2$, čímž

$$T = 4AB - B\mu^2 - \nu^2 \equiv B + \nu^2 \equiv B + \nu \equiv 0 \pmod 2,$$

což je spor s $2 \nmid T$. Případ $\mu + 1 \equiv B + \nu \equiv 0 \pmod 2$ tedy nemůže nastat.

(ii) p je liché. Máme $\theta = x + \alpha + z\beta$, pročež

$$N(\theta) = x^2 + \mu x + A + Bz^2 + \nu z.$$

Dle lemmatu 3.2.2 polynom $x^2 + \mu + A$ nabývá mod p alespoň $\frac{p+1}{2}$ různých hodnot, neboť určitě $p \nmid 1$. Podobně neplatí $p \mid B, \nu$ (to by znamenalo i $p \mid T$), pročež lemmatem 3.2.2 nabývá polynom $-Bz^2 - \nu z$ alespoň $\frac{p+1}{2}$ různých hodnot mod p. Platí $\frac{p+1}{2} + \frac{p+1}{2} = p+1 > p$, pročež Dirichletovým principem musí existovat $x, z \in \mathbb{Z}$ taková, že

$$\begin{aligned} x^2 + \mu x + A &\equiv -Bz^2 - \nu z \pmod p, \\ x^2 + \mu x + A + Bz^2 + \nu z &\equiv 0 \pmod p, \end{aligned}$$

což jsme přesně chtěli. □

Lemma 3.2.4. *Budiž $a, b, c \in \mathbb{Z}$ a p prvočíslo.* Derivací *kvadratického polynomu $ax^2 + bx + c$ nazvěme polynom $2ax + b$. Potom pokud existuje $x \in \mathbb{Z}$ takové, že $p \mid (ax^2 + bx + c)$ a zároveň $p \nmid (2ax + b)$, pak existuje $y \in \mathbb{Z}$ takové, že $y \equiv x \pmod p$, $ay^2 + by + c$ je násobek p, ale nikoliv násobek p^2.*

Důkaz. Položme $y = x + \ell p$ pro zatím neznámé ℓ a nechť $ax^2 + bx + c = mp$ pro nějaké $m \in \mathbb{Z}$. Potom z $y \equiv x \pmod p$ nutně $p \mid (ay^2 + by + c)$, zatímco $p^2 \mid (ay^2 + by + c)$ je ekvivalentní

$$\begin{aligned} ay^2 + by + c &\equiv 0 \pmod{p^2}, \\ ax^2 + 2a\ell px + a\ell^2 p^2 + bx + b\ell p + c &\equiv 0 \pmod{p^2}, \\ mp + \ell p(2ax + b) &\equiv 0 \pmod{p^2}, \\ \ell(2ax + b) &\equiv -m \pmod p, \\ \ell &\equiv -m \cdot (2ax + b)^{-1} \pmod p. \end{aligned}$$

Nyní tedy stačí zvolit ℓ tak, aby poslední kongruence neplatila. □

Lemma 3.2.5. *Budiž p prvočíslo, jež nedělí T. Potom pro $x, y, z, w \in \mathbb{Z}$ platí soustava kongruencí*

$$\begin{aligned} 2x + \mu y - \nu w &\equiv 0 \pmod{p}, \\ 2Ay + \mu x + \nu z &\equiv 0 \pmod{p}, \\ 2Bz + B\mu w + \nu y &\equiv 0 \pmod{p}, \\ 2ABw + B\mu z - \nu x &\equiv 0 \pmod{p} \end{aligned}$$

právě tehdy, pokud $x \equiv y \equiv z \equiv w \equiv 0 \pmod{p}$.

Důkaz. V celém důkazu uvažujme o A, B, μ, ν, T jako o prvcích $\mathbb{Z}_p$. Zaveďme nad okruhem $\mathbb{Z}_p$

$$M = \begin{pmatrix} 2 & \mu & 0 & -\nu \\ \mu & 2A & \nu & 0 \\ 0 & \nu & 2B & B\mu \\ -\nu & 0 & B\mu & 2AB \end{pmatrix}, \qquad X = \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix},$$

$$I = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \qquad N = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

Potom lze zadanou soustavu kongruencí přepsat jako rovnost

$$MX = N. \tag{3.5}$$

Jeden směr dokazovaného lemmatu je zřejmý – pokud $x \equiv y \equiv z \equiv w \equiv 0 \pmod{p}$, neboli $X = N$, pak jistě (3.5) platí.

Nyní tedy předpokládejme platnost (3.5). Je zadáno $p \nmid T$, pročež má T mod p inverzní prvek T^{-1}. Pak položme

$$L = T^{-1} \cdot \begin{pmatrix} 2AB & -B\mu & 0 & \nu \\ -B\mu & 2B & -\nu & 0 \\ 0 & -\nu & 2A & -\mu \\ \nu & 0 & -\mu & 2 \end{pmatrix},$$

což dá

$$\begin{aligned} LM &= T^{-1} \cdot \begin{pmatrix} 2AB & -B\mu & 0 & \nu \\ -B\mu & 2B & -\nu & 0 \\ 0 & -\nu & 2A & -\mu \\ \nu & 0 & -\mu & 2 \end{pmatrix} \cdot \begin{pmatrix} 2 & \mu & 0 & -\nu \\ \mu & 2A & \nu & 0 \\ 0 & \nu & 2B & B\mu \\ -\nu & 0 & B\mu & 2AB \end{pmatrix} = \\ &= T^{-1} \cdot \begin{pmatrix} T & 0 & 0 & 0 \\ 0 & T & 0 & 0 \\ 0 & 0 & T & 0 \\ 0 & 0 & 0 & T \end{pmatrix} = I \end{aligned}$$

(využíváme $T = 4AB - B\mu^2 - \nu^2$). Potom násobením maticí L zleva v (3.5) obdržíme

$$\begin{aligned} LMX &= LN, \\ IX &= N, \\ X &= N, \end{aligned}$$

neboli $x \equiv y \equiv z \equiv w \equiv 0 \pmod{p}$. Tímto je důkaz hotov. □

Věta 3.2.6. *Obor H je pro bezčtvercové T prvorozložený.*

Důkaz. Uvažujme libovolné prvočíslo p. Rozlišme dva případy.

(i) Pokud $p \mid T$, stačí vzít $\theta = \nu - \mu\beta + 2\alpha\beta$, což dá

$$N(\theta) = \nu^2 - \nu \cdot \nu \cdot 2 + B(\mu^2 - \mu \cdot \mu \cdot 2 + 4A) = 4AB - B\mu^2 - \nu^2 = T.$$

Přitom $p^2 \mid T$ by znamenalo spor s bezčtvercovostí T, pročež je $N(\theta)$ násobkem p, ale nikoliv p^2, jak se chtělo.

(ii) Nechť nyní $p \nmid T$. Mějme $\theta = x + y\alpha + z\beta + w\alpha\beta$ a položme $y = 1, w = 0$ – potom dle lemmatu 3.2.3 lze zvolit x, z tak, že $p \mid N(\theta)$. Ukažme, že x, y, z, w lze navolit i tak, aby zároveň platilo i $p^2 \nmid N(\theta)$ – tímto bude důkaz lemmatu hotov. Využijeme lemmatu 3.2.4 – pokud by derivace polynomu

$$N(\theta) = \left(x^2 + \mu xy + Ay^2\right) + \nu\,(yz - xw) + B\left(z^2 + \mu zw + Aw^2\right)$$

vzhledem k některému z x, y, z, w nebyla pro zvolené hodnoty x, y, z, w násobkem p, bylo by lemmatem 3.2.4 možno zvolit x, y, z, w i tak, aby bylo splněno i $p^2 \nmid N(\theta)$, čímž by důkaz byl hotov. Předpokládejme tedy pro spor, že všechny čtyři derivace jsou násobky p, tj. že platí

$$\begin{aligned} 2x + \mu y - \nu w &\equiv 0 \pmod p, \\ 2Ay + \mu x + \nu z &\equiv 0 \pmod p, \\ 2Bz + B\mu w + \nu y &\equiv 0 \pmod p, \\ 2ABw + B\mu z - \nu x &\equiv 0 \pmod p. \end{aligned}$$

To je ale vzhledem k $p \nmid T$ lemmatem 3.2.5 ekvivalentní $x \equiv y \equiv z \equiv w \equiv 0 \pmod p$, což vzhledem k $y = 1$ neplatí, což je spor. □

3.3 Důkazy slabé Eukleidovskosti

Nyní přistupme k důkazům slabé Eukleidovskosti některých z oborů H zadaných vztahem (3.3). Po celou sekci uvažujme pouze takové čtveřice (A, B, μ, ν) a příslušné obory H, pro něž

$$\frac{12}{T} - \frac{S}{T} - \frac{4}{S} > 0.$$

Úmluva. *Délkou* intervalu s krajními body $a \le b$ rozumějme, nehledě na jeho otevřenost či uzavřenost, $b - a$.

Lemma 3.3.1. *Pro $a, b, c \in \mathbb{R}, a > 0$ uvažujme nerovnici*

$$ax^2 + bx + c < 0. \tag{3.6}$$

Položme $D = b^2 - 4ac$. Potom existuje otevřený interval I délky vyšší něž r splňující (3.6) *pro každé $x \in I$, právě pokud platí*

$$D > (ar)^2. \tag{3.7}$$

Důkaz. Pokud $D \leq 0$, pak má polynom $ax^2 + bx + c$ nanejvýš jeden reálný kořen, pročež vzhledem k $a > 0$ nabývá pouze nezáporných hodnot, neboli (3.6) nemá reálná řešení. Zároveň je z podmínek $ar > 0$, z čehož i $(ar)^2 > 0$, čímž neplatí (3.7), a platnost dokazovaného tvrzení je v tomto případě ověřena.

Budiž nyní $D > 0$. Pak má polynom $ax^2 + bx + c$ reálné kořeny

$$x_1 = \frac{-b - \sqrt{D}}{2a}, \qquad x_2 = \frac{-b + \sqrt{D}}{2a}$$

a řešeními nerovnice (3.6) jsou právě všechna $x \in (x_1, x_2)$. Přitom

$$x_2 - x_1 = \frac{\sqrt{D}}{a}.$$

Nerovnost (3.7) je pro $D > 0$ ekvivalentní nerovnosti $\frac{\sqrt{D}}{a} > r$, pročež pokud tato nerovnost platí, lze zvolit $I = (x_1, x_2)$. Naopak pokud (3.7) neplatí, nemůže vyhovující interval I existovat, neboť všechna řešení nerovnice (3.6) náleží intervalu (x_1, x_2), jenž má délku nejvýše r, a nemůže tedy jako podmnožinu obsahovat interval délky vyšší než r. □

Lemma 3.3.2. *Budiž $\lambda = x_0 + y_0\alpha + z_0\beta + w_0\alpha\beta$ pro $x_0, y_0, z_0, w_0 \in \mathbb{R}$ a zaveďme $L = \frac{1}{2}\sqrt{\frac{12}{T} - \frac{S}{T} - \frac{4}{S}}$. Potom pokud w_0 náleží množině*

$$(-L, L) + \mathbb{Z} = \bigcup_{m \in \mathbb{Z}} (m - L, m + L),$$

pak lze zvolit $\gamma \in H$ tak, že $N(\lambda - \gamma) < 1$.

Důkaz. Položme $\lambda - \gamma = x + y\alpha + z\beta + w\alpha\beta$ pro zatím neznámá $x, y, z, w \in \mathbb{R}$ taková, že $x - x_0 \in \mathbb{Z}$ apod. Pak je

$$N(\lambda - \gamma) = \left(x^2 + \mu xy + Ay^2\right) + \nu\left(yz - xw\right) + B\left(z^2 + \mu zw + Aw^2\right). \tag{3.8}$$

Hleďme na tento výraz jako na kvadratický polynom v x (jakoby y, z, w již byly pevně zvoleny) a zajímejme se o nerovnost

$$N(\lambda - \gamma) - 1 = \left(x^2 + \mu xy + Ay^2\right) + \nu\left(yz - xw\right) + B\left(z^2 + \mu zw + Aw^2\right) - 1 < 0, \tag{3.9}$$

jejíž diskriminant je D_x. Potom dle lemmatu 3.3.1 existuje otevřený interval délky větší než 1, jehož každý prvek x splní (3.9), neboli $N(\lambda - \gamma) < 1$, právě pokud $D_x > 1$. To dává nerovnici

$$\begin{aligned}
D_x &> 1,\\
(\mu y - \nu w)^2 - 4 \cdot \left(-1 + Ay^2 + \nu yz + B\left(z^2 + \mu zw + Aw^2\right)\right) &> 1,\\
y^2\left(\mu^2 - 4A\right) - y\left(2\mu\nu w + 4\nu z\right) + \nu^2 w^2 - 4B\left(z^2 + \mu zw + Aw^2\right) + 3 &> 0,\\
-Sy^2 - 2\nu y\left(\mu w + 2z\right) + \nu^2 w^2 + 3 - 4B\left(z^2 + \mu zw + Aw^2\right) &> 0,\\
Sy^2 + 2\nu y\left(\mu w + 2z\right) - \nu^2 w^2 - 3 + 4B\left(z^2 + \mu zw + Aw^2\right) &< 0.
\end{aligned} \tag{3.10}$$

Zde lze použitou myšlenku zopakovat – hleďme nyní na výraz na levé straně (3.10) jako na kvadratický polynom v y, jehož diskriminant je roven D_y. Opětovným použitím lemmatu 3.3.1 existuje otevřený interval délky větší než 1, jehož každý prvek y splní (3.10),

právě pokud

$$\begin{aligned}
D_y &> S^2,\\
4\nu^2\left(\mu w+2z\right)^2-4S\left(-\nu^2w^2-3+4B\left(z^2+\mu zw+Aw^2\right)\right) &> S^2,\\
z^2\left(4\nu^2\cdot 4-4S\cdot 4B\right)+zw\left(4\nu^2\cdot 2\cdot\mu\cdot 2-4S\cdot 4B\cdot\mu\right)+&\\
+w^2\left(4\nu^2\cdot\mu^2+4S\nu^2-4S\cdot 4B\cdot A\right)+12S-S^2 &> 0,\\
16z^2\left(\nu^2-BS\right)+16\mu zw\left(\nu^2-BS\right)+&\\
+4w^2\left(\nu^2\left(\mu^2+S\right)-4ABS\right)+12S-S^2 &> 0,\\
-16Tz^2-16T\mu zw+4w^2\left(\nu^2\cdot A-4ABS\right)+12S-S^2 &> 0,\\
-16Tz^2-16T\mu zw-16TAw^2+12S-S^2 &> 0,\\
16T\left(z^2+\mu zw+Aw^2\right)+S^2-12S &< 0. \qquad (3.11)
\end{aligned}$$

Na levou stranu (3.11) hleďme opět jako na kvadratický polynom v z o diskriminantu D_z. Interval délky větší než 1, jehož každý prvek z (3.11) splní, existuje, právě pokud

$$\begin{aligned}
D_z &> \left(16T\right)^2,\\
256T^2\mu^2w^2-4\cdot 16T\left(16TAw^2+S^2-12S\right) &> 256T^2,\\
4T\mu^2w^2-\left(16TAw^2+S^2-12S\right) &> 4T,\\
4Tw^2\left(\mu^2-4A\right)-S^2+12S-4T &> 0,\\
-4STw^2-S^2+12S-4T &> 0,\\
4STw^2+S^2-12S+4T &< 0,\\
|w| &< \frac{1}{2}\sqrt{\frac{12}{T}-\frac{S}{T}-\frac{4}{S}}=L. \qquad (3.12)
\end{aligned}$$

Toto však z předpokladu lemmatu lze splnit. Uvědomme si, že pokud existuje (otevřený) interval délky větší než 1, jehož každý prvek r splní nějakou danou podmínku, pak určitě pro libovolné dané $r_0\in\mathbb{R}$ existuje $r\in\mathbb{R}$ takové, jež zmíněné podmínce vyhovuje a zároveň splňuje $r-r_0\in\mathbb{Z}$ (neboť v intervalu délky větší než 1 jistě existuje reálné číslo se stejnou necelou částí jako r_0). Tím lze tedy z vykonaných výpočtů vyvodit následující: je-li splněna nerovnost (3.12), pak lze zvolit z (vyhovujíce tomu, že $z-z_0$ je celé číslo) tak, že bude splněna nerovnost (3.11). Z toho obdobně lze zvolit y (vyhovujíce $y-y_0\in\mathbb{Z}$) tak, že bude splněna (3.10). To konečně značí, že lze zvolit x (vyhovujíce $x-x_0\in\mathbb{Z}$) tak, aby bylo $N(\lambda-\gamma)<1$. Přitom ale z podmínky lemmatu existuje $w\in\mathbb{R}$ takové, že $|w|<L$ a zároveň $w-w_0\in\mathbb{Z}$. Tímto je důkaz hotov. □

S pomocí právě dokázaného lemmatu vyslovíme postačující podmínku slabé Eukleidovskosti pro obory, jež zkoumáme.

Definice 3.3.3. Definujme

$$Q=\left\{\frac{\lambda}{r}:\lambda\in H\wedge r\in\mathbb{N}\right\}.$$

O zlomku $\frac{\lambda}{r}$ pro $\lambda\in H, r\in\mathbb{N}$ řekněme, že je *v základním tvaru*, pokud $\lambda=x+y\alpha+z\beta+w\alpha\beta$ a $\mathrm{NSD}(x,y,z,w,r)=1$.

Lemma 3.3.4. *Budiž G takový obor, pro nějž $H \subseteq G \subset Q$ a jehož prvky se normou zobrazují do celých nezáporných čísel. Potom pokud pro každé přirozené r splňující*

$$1 < r \leq \frac{2}{\sqrt{\frac{12}{T} - \frac{S}{T} - \frac{4}{S}}}$$

pro každé $\lambda = x+y\alpha+z\beta+w\alpha\beta \in H$ splňující $0 \leq x, y, z, w < r \wedge \mathrm{NSD}(w, r) = 1 \wedge \frac{\lambda}{r} \notin G$ existuje $\delta \in G$ takové, že

$$\delta\lambda = a + b\alpha + c\beta + d\alpha\beta$$

pro nějaká $a, b, c, d \in \mathbb{Z}$ taková, že $d \equiv 0 \pmod{r}$ a r nedělí všechna čtyři a, b, c, d, pak je G zleva slabě Eukleidovský. Obdobně je G zprava slabě Eukleidovský, píšeme-li $\lambda\delta$ namísto $\delta\lambda$.

Důkaz. Proveďme důkaz slabé Eukleidovskosti zleva, slabou Eukleidovskost zprava lze dokázat zcela analogicky.

Dokažme nejprve, že pokud pro každé $\frac{\lambda}{r} \in Q$, jež nenáleží G, existují $\delta, \gamma \in G$ taková, že

$$0 < N\left(\frac{\delta\lambda}{r} - \gamma\right) < 1,$$

pak je G zleva slabě Eukleidovský. Mějme libovolná $\eta, \theta \in G$ taková, že $\eta \notin G\theta$. Máme ukázat, že existují $\delta, \gamma \in G$ taková, že $0 < N(\delta\eta - \gamma\theta) < N(\theta)$. Přitom ale vzhledem k $G \subset Q$ jistě $\frac{\eta\bar{\theta}}{N(\theta)} \in Q$. Mějme tedy $\frac{\lambda}{r} \in Q$ v základním tvaru takové, že $\frac{\eta\bar{\theta}}{N(\theta)} = \frac{\lambda}{r}$. Díky tomu je ale

$$N(\delta\eta - \gamma\theta) = N\left(\left(\frac{\delta\lambda}{r} - \gamma\right)\theta\right) = N\left(\frac{\delta\lambda}{r} - \gamma\right) N(\theta),$$

pročež je nerovnost $0 < N(\delta\eta - \gamma\theta) < N(\theta)$ ekvivalentní nerovnosti

$$0 < N\left(\frac{\delta\lambda}{r} - \gamma\right) < 1.$$

Přitom $\eta \in G\theta$, právě pokud $\frac{\lambda}{r} = \frac{\eta\bar{\theta}}{N(\theta)} \in G$, čímž je tato část důkazu hotova.

Pojmenujme $L = \frac{1}{2}\sqrt{\frac{12}{T} - \frac{S}{T} - \frac{4}{S}}$. Dále si uvědomme, že pokud $\gamma \in H, \frac{\delta\lambda}{r} \notin H$, pak už jistě $N\left(\frac{\delta\lambda}{r} - \gamma\right) > 0$. To plyne z toho, že $N\left(\frac{\delta\lambda}{r} - \gamma\right) = 0$ může nastat pouze pro $\frac{\delta\lambda}{r} = \gamma \in H$, což by byl spor. Z toho plyne, že pokud existuje $\delta \in G$ takové, že

$$\delta\lambda = a + b\alpha + c\beta + d\alpha\beta$$

pro nějaká $a, b, c, d \in \mathbb{Z}$, pro něž $\frac{\delta\lambda}{r} \notin H$ a zároveň

$$\frac{d}{r} \in (-L, L) + \mathbb{Z},$$

pak lemmatem 3.3.2 existuje $\gamma \in H$ takové, že $N\left(\frac{\delta\lambda}{r} - \gamma\right) < 1$, čímž už díky $\frac{\delta\lambda}{r} \notin H$ už dokonce

$$0 < N\left(\frac{\delta\lambda}{r} - \gamma\right) < 1,$$

jak chceme.

Mějme tedy $\lambda = x+y\alpha+z\beta+w\alpha\beta \in H$. Uvažujme nejprve w, r soudělná. Potom vzetím $\delta = \frac{r}{\mathrm{NSD}(w,r)}$ obdržíme

$$\frac{\delta\lambda}{r} = \frac{x+y\alpha+z\beta+w\alpha\beta}{\mathrm{NSD}(w,r)}.$$

Toto jistě není prvek H, neboť potom by původní $\frac{\lambda}{r}$ nebylo v základním tvaru. Přitom ale $\mathrm{NSD}(w,r) \mid w$, pročež z předchozího odstavce existuje $\gamma \in H$ tak, že

$$0 < N\left(\frac{\delta\lambda}{r} - \gamma\right) < 1.$$

Nadále tedy nechť jsou w, r nesoudělná. Uvažujme nyní $r > \frac{2}{\sqrt{\frac{12}{T}-\frac{S}{T}-\frac{4}{S}}}$. Potom jistě $\frac{1}{r} < \frac{1}{2}\sqrt{\frac{12}{T}-\frac{S}{T}-\frac{4}{S}}$. Z nesoudělnosti w, r nyní existuje $\delta \in \mathbb{N}$ takové, že $\delta w \equiv 1 \pmod{r}$. Toto δ je přitom jistě nesoudělné s r, pročež

$$\frac{\delta\lambda}{r} \notin H,$$

zároveň ale $\frac{\delta w}{r}$ náleží

$$(-L, L) + \mathbb{Z},$$

čímž existuje $\gamma \in H$ takové, že $0 < N\left(\frac{\delta\lambda}{r} - \gamma\right) < 1$.

Slabou Eukleidovskost zleva tedy máme dokázánu pro $r > \frac{2}{\sqrt{\frac{12}{T}-\frac{S}{T}-\frac{4}{S}}}$, uvažujme tedy $1 < r \leq \frac{2}{\sqrt{\frac{12}{T}-\frac{S}{T}-\frac{4}{S}}}$. Zaveďme

$$H_r = \{x+y\alpha+z\beta+w\alpha\beta : x, y, z, w \in \{0, \ldots, r-1\}\}.$$

Potom každé $\lambda \in H$ lze zapsat jako $\lambda = \lambda_0 + r\gamma_1$ pro nějaké $\lambda_0 \in H_r, \gamma_1 \in H$. Z předpokladu lemmatu pro každé $\lambda_0 \in H_r$ existuje $\delta \in G$, že

$$\delta\lambda_0 = a + b\alpha + c\beta + d\alpha\beta$$

a přitom $\frac{\delta\lambda_0}{r} \notin H, r \mid d$. Potom tedy jistě

$$\frac{d}{r} \in \mathbb{Z} \subseteq (-L, L) + \mathbb{Z},$$

pročež existuje $\gamma_2 \in H$ takové, že $0 < N\left(\frac{\delta\lambda_0}{r} - \gamma_2\right) < 1$. Nyní tedy stačí položit $\gamma = \delta\gamma_1 + \gamma_2$, čímž

$$\frac{\delta\lambda}{r} - \gamma = \frac{\delta(\lambda_0 + r\gamma_1)}{r} - \gamma = \frac{\delta\lambda_0}{r} + \delta\gamma_1 - \delta\gamma_1 - \gamma_2 = \frac{\delta\lambda_0}{r} - \gamma_2.$$

Tímto je pro tato r důkaz hotov.

Konečně uvažujme $r = 1$. Potom ale $\frac{\lambda}{r} \in H$, pročež tento případ není třeba zvažovat. Důkaz lemmatu je tímto hotov. □

Uvědomme si, že právě dokázané lemma vlastně pro $\frac{12}{T} - \frac{S}{T} - \frac{4}{S}$ redukuje důkaz slabé Eukleidovskosti G na zkontrolování konečně mnoha případů. S tímto kritériem již svedeme dokázat slabou Eukleidovskost několika dalších oborů. Pokud se jedná o obor H, pak už z toho plyne, že H je silný kvaternionový obor. Pokud je zároveň T bezčtvercové, bude potom skrze výsledky kapitoly 2 kvadratická forma

$$(x^2 + \mu xy + Ay^2) + \nu(yz - xw) + B(z^2 + \mu zw + Aw^2)$$

muset být univerzální.

Věta 3.3.5. *Pro $(A, B, \mu, \nu) = (1, 1, 1, 0)$ je obor H zleva i zprava slabě Eukleidovský.*

Důkaz. Pro tuto volbu A, B, μ, ν je $S = 3, T = 3$. Přitom

$$\frac{2}{\sqrt{\frac{12}{T} - \frac{S}{T} - \frac{4}{S}}} = 2\sqrt{\frac{3}{5}} < 2,$$

pročež lemmatem 3.3.4 není třeba kontrolovat žádné speciální případy. □

Důsledek. *H je prvorozložený silný kvaternionový obor, pročež je kvadratická forma*

$$(x^2 + xy + y^2) + (z^2 + zw + w^2)$$

univerzální.

Věta 3.3.6. *Pro $(A, B, \mu, \nu) = (1, 2, 1, 1)$ je obor H zleva i zprava slabě Eukleidovský.*

Důkaz. Dokažme slabou Eukleidovskost zleva, slabou Eukleidovskost zprava lze dokázat obdobným způsobem.

Platí $S = 3, T = 5$, pročež

$$\frac{2}{\sqrt{\frac{12}{T} - \frac{S}{T} - \frac{4}{S}}} = 2\sqrt{\frac{15}{7}} < 3.$$

Podle lemmatu 3.3.4 pak tedy stačí pro $r = 2$ dokázat, že pro $x + y\alpha + z\beta + w\alpha\beta = \lambda$ takové, že $\frac{\lambda}{r}$ je v základním tvaru a $0 \leq x, y, z, w < r$, existuje $\delta \in H$ tak, že

$$\delta\lambda = a + b\alpha + c\beta + d\alpha\beta$$

tak, že $r \mid d$ a zároveň $\frac{\delta\lambda}{r} \notin H$.

Pokud $w = 0$, stačí vzít $\delta = 1$ – nadále tedy předpokládejme $w = 1$. Pokud nyní $z = 1$, pak vzetím $\delta = \alpha$ budeme mít

$$\delta\lambda = \alpha\,(x + y\alpha + \beta + \alpha\beta) = -y + (x + y)\alpha - \beta + 2\alpha\beta.$$

Přitom díky koeficientu -1 u β jistě $\frac{\delta\lambda}{2} \notin H$, zároveň ale $2 \mid 2$, čímž je hotovo. Nadále tedy předpokládejme i $z = 0$. Potom konečně vzetím $\delta = \alpha + 1$ bude

$$\delta\lambda = (\alpha + 1)(x + y\alpha + \alpha\beta) = (x - y) + \alpha(x + 2y) - \beta + 2\alpha\beta$$

Přitom opět $\frac{\delta\lambda}{2} \notin H$, ale $2 \mid 2$, pročež je tímto speciální případ $r = 2$ vyřešen, čímž je důkaz věty hotov. □

Důsledek. *H je prvorozložený silný kvaternionový obor, pročež je kvadratická forma*

$$(x^2 + xy + y^2) + (yz - xw) + 2(z^2 + zw + w^2)$$

univerzální.

Věta 3.3.7. *Pro $(A, B, \mu, \nu) = (2, 1, 1, 0)$ je obor H zleva i zprava slabě Eukleidovský.*

Důkaz. Dokažme slabou Eukleidovskost zleva, slabou Eukleidovskost zprava lze dokázat obdobným způsobem.

Platí $S = T = 7$, pročež

$$\frac{2}{\sqrt{\frac{12}{T} - \frac{S}{T} - \frac{4}{S}}} = 2\sqrt{7} < 6.$$

Podle lemmatu 3.3.4 pak tedy stačí pro $r \in \{2, 3, 4, 5\}$ dokázat, že pro $x+y\alpha+z\beta+w\alpha\beta = \lambda$ takové, že $\frac{\lambda}{r}$ je v základním tvaru a $0 \leq x, y, z, w < r$, existuje $\delta \in H$ tak, že

$$\delta\lambda = a + b\alpha + c\beta + d\alpha\beta$$

tak, že $r \mid d$ a zároveň $\frac{\delta\lambda}{r} \notin H$. Rozlišme tedy čtyři případy.

(i) $r = 2$. Pokud $w = 0$, stačí vzít $\delta = 1$ – nadále tedy předpokládejme $w = 1$. Pokud nyní $y = 0$, pak vzetím $\delta = \beta$ obdržíme

$$\delta\lambda = \beta(x + z\beta + \alpha\beta) = (-z - 1) + \alpha + x\beta.$$

Přitom díky koeficientu 1 u α jistě $\frac{\delta\lambda}{2} \notin H$, zároveň ale $2 \mid 0$, čímž je hotovo. Nadále tedy předpokládejme i $y = 1$.

Pokud nyní $x = z$, pak jistě $2 \mid (\pm x \pm z)$ pro libovolná znaménka. Přitom vzetím $\delta = 1 + \beta$ obdržíme

$$\delta\lambda = (1 + \beta)(x + \alpha + z\beta + \alpha\beta) = (x - z - 1) + 2\alpha + (x + z + 1)\beta.$$

Přitom jistě $2 \nmid (x - z - 1)$, pročež $\frac{\delta\lambda}{2} \notin H$, nicméně $2 \mid 0$, čímž je hotovo. Dále pro $x = 0, z = 1$ stačí vzít $\delta = \alpha$, což dá

$$\delta\lambda = \alpha(\alpha + \beta + \alpha\beta) = -2 + \alpha - 2\beta + 2\alpha\beta,$$

což zřejmě vyhovuje, a konečně pro $x = 1, z = 0$ stačí vzít $\delta = 1 + \alpha$, což dá

$$\delta\lambda = (1 + \alpha)(1 + \alpha + \alpha\beta) = -1 + 3\alpha - 2\beta + 2\alpha\beta.$$

Tímto je případ $r = 2$ vyřešen.

(ii) $r = 3$. Pokud $w = 0$, stačí vzít $\delta = 1$, pročež nadále předpokládejme $w \neq 0$. Nyní pokud $y = 0$, pak vzetím $\delta = \beta$ obdržíme

$$\delta\lambda = \beta(x + z\beta + w\alpha\beta) = (-z - w) + w\alpha + x\beta.$$

Přitom díky koeficientu w u α jistě $\frac{\delta\lambda}{3} \notin H$, zároveň ale $2 \mid 0$, čímž je hotovo. Nadále tedy předpokládejme $y \neq 0$

Díky $y \not\equiv 0 \not\equiv w \pmod 3$ pak jistě $w^2 \equiv y^2 \equiv 1 \pmod 3$, neboli $w^2 - y^2 \equiv 0 \pmod 3$, ale $3 \nmid 2yw$. Vzetím $\delta = w + y\beta$ tak obdržíme

$$\begin{aligned}\delta\lambda &= (w + y\beta)(x + y\alpha + z\beta + w\alpha\beta) = \\ &= (xw - yz - yw) + 2yw\alpha + (zw + xy + y^2)\beta + (w^2 - y^2)\alpha\beta,\end{aligned}$$

čímž je případ $r = 3$ vyřešen.

(iii) $r = 4$. Pokud $w = 0$, stačí vzít $\delta = 1$. Pokud $w = 2$, vezmeme $\delta = 2$, neboť díky tomu, že $\frac{\lambda}{r}$ je v základním tvaru, musí jedno z x, y, z být liché. Nadále tedy předpokládejme $w \in \{1, 3\}$. Dále pokud $y = 0$, postačí analogicky s předchozími případy opět $\delta = \beta$. Pokud $y = 2$, vezmeme $\delta = 2\beta$, čímž obdržíme

$$\delta\lambda = 2\beta(x + 2\alpha + z\beta + w\alpha\beta) = -2(z + w) + 2w\alpha + 2\beta(x + y) - 4\alpha\beta,$$

čímž je díky $4 \nmid 2w$ (máme w liché) a $4 \mid 4$ hotovo. Dále tedy předpokládejme $y \in \{1, 3\}$.

Máme tedy $y \equiv w \equiv 1 \pmod 2$, z čehož opět $y^2 \equiv w^2 \equiv 1 \pmod 4$, ale $4 \nmid 2yw$. Stejně jako v případě $r = 3$ tedy postačí $\delta = w + y\beta$. Případ $r = 4$ je tímto vyřešen.

(iv) $r = 5$. Jako v předchozích případech není třeba řešit $w = 0$. Zaveďme $\delta = m + \alpha\beta$, kde $m \in \mathbb{Z}$ je takové číslo, pro něž platí $m \equiv -xw^{-1} \pmod 5$. Potom platí

$$\begin{aligned}\delta\lambda &= (m + \alpha\beta)(x + y\alpha + z\beta + w\alpha\beta) = \\ &= (mx - 2w) + (my - z)\alpha + (mz + 2y)\beta + (mw + x)\alpha\beta.\end{aligned}$$

Z toho, jak bylo zvoleno m, nyní musí platit $5 \mid (mw + x)$. Ukažme, že $5 \nmid (mx - 2w)$. Pro spor nechť $5 \mid (mx - 2w)$. Potom

$$\begin{aligned} mx &\equiv 2w \pmod 5, \\ -x^2w^{-1} &\equiv 2w \pmod 5, \\ (xw^{-1})^2 &\equiv -2 \equiv 3 \pmod 5, \end{aligned}$$

neboli 3 je kvadratický zbytek mod 5. Jenže kvadratickými zbytky mod 5 jsou právě $0, 1, 4$. Toto je spor, čímž nutně $5 \nmid (mx - 2w)$. Tímto je případ $r = 5$, a tedy i celý důkaz, hotov. □

Důsledek. *H je prvorozložený silný kvaternionový obor, pročež je kvadratická forma*

$$(x^2 + xy + 2y^2) + (z^2 + zw + 2w^2)$$

univerzální.

3.4 Izomorfizmy kvaternionových oborů

V této sekci dokážeme univerzálnost několika kvadratických forem tvaru (3.1) tím, že k příslušnému oboru H uvážíme ještě nějaký obor $G \supset H$, o němž ukážeme, že je izomorfní nějakému oboru R, o němž je již známo, že je prvorozložený silný kvaternionový. Izomorfizmy φ, které sestrojíme, budou také splňovat $N(\varphi(\theta)) = N(\theta)$ pro každé $\theta \in R$ – o takovém izomorfizmu φ řekněme, že *zachovává normu*. Nahlédněme, že pokud má tuto vlastnost φ, pak má tuto vlastnost (pro každé $\theta \in G$) i izomorfizmus $\psi : G \to R$, jež je inverzní k φ. Následně dokážeme, že pokud rovnice $N(\theta) = n$ má pro $n \in \mathbb{N}$ řešení $\theta \in G$, pak už má i řešení $\theta \in H$.

Stručně ukažme, že pokud $R, S \subseteq \mathbb{H}(\mathbb{R})$, R je prvorozložený silný kvaternionový obor a existuje izomorfizmus $\varphi : R \to S$, který zachovává normu, pak už je i S prvorozloženým silným kvaternionovým oborem. Zkontrolujme postupně splnění všech čtyř podmínek definice 2.3.1. Zaprvé z definice izomorfizmu musí být $\varphi(0) = \varphi(0 + 1) - \varphi(1) = 0$. Zadruhé

z bijektivity φ určitě $\varphi(1) \neq 0$, pročež z $\varphi(1) = \varphi(1 \cdot 1) = (\varphi(1))^2$ nutně $\varphi(1) = 1$. Z toho pak

$$\varphi(-1) + \varphi(1) = \varphi(-1+1) = \varphi(0) = 0,$$
$$\varphi(-1) = -\varphi(1) = -1,$$

z čehož dále skrze $\varphi(m \pm 1) = \varphi(m) \pm 1$ jednoduchou indukcí plyne $\varphi(m) = m$ pro $m \in \mathbb{Z}$. Z toho vzhledem k $\mathbb{Z} \subseteq R$ musí být i $\mathbb{Z} \subseteq S$, neboli je splněna podmínka (i). Podmínka (ii) musí být splněna, neboť S musí být okruhem jakožto obraz izomorfizmu (viz poznámku k definici 1.1.11) a oborem je už díky $S \subset \mathbb{H}(\mathbb{R})$, což je obor. Splnění podmínky (iii) je, stejně jako prvorozloženost S, přímým důsledkem toho, že φ zachovává normu. Též musí pro libovolné $n \in \mathbb{N}$ být v R i S stejný počet kvaternionů s normou n, neboť množiny takových kvaternionů po řadě v R a v S se musí izomorfizmem φ jedna na druhou zobrazovat (opět protože φ zachovává normu).

Dokažme nyní splnění podmínky (iv). Budiž $I \subseteq S$ libovolný levý ideál (pro pravé ideály lze postupovat obdobně). Budiž $\psi : S \to \varphi$ izomorfizmus inverzní k R (takový existuje) a označme

$$J = \{\psi(\theta) : \theta \in I\}$$

– potom jistě naopak i $I = \{\varphi(\theta) : \theta \in J\}$. Z vlastností izomorfizmů musí J být levým ideálem v R, z čehož nutně $J = R\lambda$ pro nějaké $\lambda \in R$. Potom ale nazpět i $I = S\varphi(\lambda)$, neboli je S hlavní.

Lemma 3.4.1. *Buďte $\gamma, \delta \in \mathbb{H}(\mathbb{R})$ taková, že*

$$\gamma^2 = \mu\gamma - A, \qquad \delta^2 = -B, \qquad \delta\gamma = -\nu - \gamma\delta + \mu\delta.$$

Potom existuje izomorfizmus

$$\varphi : H \to \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\},$$

který zachovává normu.

Důkaz. Pro $\theta = x + y\alpha + z\beta + w\alpha\beta \in H$ definujme

$$\varphi(\theta) = x + y\gamma + z\delta + w\gamma\delta.$$

Potom zcela zřejmě platí $\varphi(\theta_1 + \theta_2) = \varphi(\theta_1) + \varphi(\theta_2)$ a $\varphi(m) = m$ pro $m \in \mathbb{Z}$. Ze zadaných rovností platí

$$\begin{aligned}
\varphi(\alpha)^2 = \gamma^2 = \mu\gamma - A = \mu\varphi(\alpha) - A = \varphi(\mu\alpha - A) = \varphi(\alpha^2),\\
\varphi(\beta)^2 = \delta^2 = -B = \varphi(-B) = \varphi(\beta^2),\\
\varphi(\alpha)\varphi(\beta) = \gamma\delta = \varphi(\alpha\beta),\\
\varphi(\beta)\varphi(\alpha) = \delta\gamma = -\nu - \gamma\delta + \mu\delta = -\nu - \varphi(\alpha\beta) + \mu\varphi(\beta) = \varphi(-\nu - \alpha\beta + \mu\beta) = \varphi(\beta\alpha).
\end{aligned}$$

Ze těchto rovností lze (analogicky s příslušnou částí důkazu věty 3.2.1) již odvodit všechny ostatní rovnosti $\varphi(\lambda_1)\varphi(\lambda_2) = \varphi(\lambda_1\lambda_2)$ pro $\lambda_1, \lambda_2 \in \{1, \alpha, \beta, \alpha\beta\}$.

Z tohoto již distributivitou plyne platnost $\varphi(\theta_1\theta_2) = \varphi(\theta_1)\varphi(\theta_2)$ pro libovolná $\theta_1, \theta_2 \in H$. Položíme-li totiž $\theta_1 = x_1 + y_1\alpha + z_1\beta + w_1\alpha\beta$, $\theta_2 = x_2 + y_2\alpha + z_2\beta + w_2\alpha\beta$, pak je

$$\varphi(\theta_1\theta_2) = \varphi\left((x_1 + y_1\alpha + z_1\beta + w_1\alpha\beta)(x_2 + y_2\alpha + z_2\beta + w_2\alpha\beta)\right)$$

roznásobením vnitřní závorky rovno součtu členů tvaru $\varphi(c_1c_2\lambda_1\lambda_2)$, kde

$$c_1 \in \{x_1, y_1, z_1, w_1\}, \qquad c_2 \in \{x_2, y_2, z_2, w_2\}, \qquad \lambda_1, \lambda_2 \in \{1, \alpha, \beta, \alpha\beta\}.$$

Z již dokázaného však lze každý takový člen přepsat na $\varphi(c_1\lambda_1)\varphi(c_2\lambda_2)$ a tyto členy opět vytknout, čímž obdržíme

$$(\varphi(x_1)+\varphi(y_1\alpha)+\varphi(z_1\beta)+\varphi(w_1\alpha\beta))(\varphi(x_2)+\varphi(y_2\alpha)+\varphi(z_2\beta)+\varphi(w_2\alpha\beta)) = \varphi(\theta_1)\varphi(\theta_2).$$

Toto již značí, že φ je homomorfizmus.

Ukažme dále, že platí $\varphi(\overline{\theta}) = \overline{\varphi(\theta)}$. Nejprve nechť $\varphi(\theta) \notin \mathbb{R}$. Vzhledem k $\theta + \overline{\theta} \in \mathbb{Z}$ platí

$$\varphi(\theta) + \varphi(\overline{\theta}) = \varphi(\theta + \overline{\theta}) = \theta + \overline{\theta} \in \mathbb{Z}.$$

Zároveň také už z $\varphi(\theta) \in \mathbb{H}(\mathbb{R})$ plyne $\varphi(\theta)+\overline{\varphi(\theta)} \in \mathbb{R}$, z čehož dohromady $\varphi(\overline{\theta}) = \overline{\varphi(\theta)}+r$ pro nějaké $r \in \mathbb{R}$. Nechť pro spor $r \neq 0$. Potom

$$N(\theta) = \varphi(N(\theta)) = \varphi(\theta)\varphi(\overline{\theta}) = \varphi(\theta)\overline{\varphi(\theta)} + r\varphi(\theta) = N(\varphi(\theta)) + r\varphi(\theta),$$
$$\varphi(\theta) = \frac{N(\theta) - N(\varphi(\theta))}{r} \in \mathbb{R},$$

což je spor. Pro θ takové, že $\varphi(\theta) \notin \mathbb{R}$, tedy musí nutně být $\varphi(\overline{\theta}) = \overline{\varphi(\theta)}$.

Nyní uvažujme θ takové, že $\varphi(\theta) \in \mathbb{R}$. Vzhledem k $\delta^2 = -B < 0$ určitě $\delta \notin \mathbb{R}$. Z toho $\varphi(\beta) = \delta \notin \mathbb{R}$ a $\varphi(\beta + \theta) = \varphi(\beta) + \varphi(\theta) \notin \mathbb{R}$, takže

$$\varphi(\overline{\theta}) = \varphi(\overline{(\beta+\theta)}) - \varphi(\overline{\beta}) = \overline{\varphi(\beta+\theta)} - \overline{\varphi(\beta)} = \overline{(\varphi(\beta+\theta) - \varphi(\beta))} = \overline{\varphi(\theta)}.$$

Dohromady tedy již $\varphi(\overline{\theta}) = \overline{\varphi(\theta)}$ pro libovolné $\theta \in H$. Z toho už snadno

$$N(\varphi(\theta)) = \varphi(\theta)\overline{\varphi(\theta)} = \varphi(\theta)\varphi(\overline{\theta}) = \varphi(\theta\overline{\theta}) = \varphi(N(\theta)) = N(\theta).$$

Z $N(\varphi(\theta)) = N(\theta)$ speciálně plyne $\varphi(\theta) = 0$, právě pokud $\theta = 0$. Pokud nyní $\varphi(\theta_1) = \varphi(\theta_2)$ pro nějaká $\theta_1, \theta_2 \in H$, pak

$$\varphi(\theta_1) - \varphi(\theta_2) = \varphi(\theta_1 - \theta_2) = 0,$$
$$\theta_1 - \theta_2 = 0,$$
$$\theta_1 = \theta_2.$$

Zobrazení φ je tedy prosté, pročež už musí být bijekcí do svého obrazu. Celkově je tedy φ izomorfizmem z H do

$$\operatorname{Im}\varphi = \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\}.$$

Tímto je důkaz hotov. □

Věta 3.4.2. *Budiž $(A, B, \mu, \nu) = (1, 1, 1, 1)$. Potom existuje izomorfizmus $\varphi : H \to \mathbb{J}$, který zachovává normu.*

Důkaz. Položme

$$\gamma = \frac{1 + i + j + k}{2}, \qquad \delta = j.$$

Potom platí

$$\gamma\delta = \frac{1+i+j+k}{2}\cdot j = \frac{-1-i+j+k}{2},$$
$$\gamma^2 = \left(\frac{1+i+j+k}{2}\right)^2 = \frac{-1+i+j+k}{2} = \frac{1+i+j+k}{2} - 1 = \mu\gamma - A,$$
$$\delta^2 = j^2 = -1 = -B,$$
$$\delta\gamma = j\cdot\frac{1+i+j+k}{2} = \frac{-1+i+j-k}{2} = -1 - \frac{-1-i+j+k}{2} + j = -\nu - \gamma\delta + \mu\delta.$$

Lemmatem 3.4.1 tedy existuje izomorfizmus

$$\varphi : H \to \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\},$$

který zachovává normu. Zbývá tedy ukázat

$$\operatorname{Im}\varphi = \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\} = \mathbb{J} =$$
$$= \left\{x + yi + zj + w\cdot\frac{1+i+j+k}{2} : x, y, z, w \in \mathbb{Z}\right\}.$$

Zřejmě $\gamma, \delta, \gamma\delta \in \mathbb{J}$, takže z uzavřenosti $\mathbb{J}$ na tvorbu lineárních kombinací s celočíselnými koeficienty musí být $\operatorname{Im}\varphi \subseteq \mathbb{J}$. Naopak ale i

$$i = -1 + \gamma - \gamma\delta, \qquad j = \delta, \qquad \frac{1+i+j+k}{2} = \gamma,$$

takže analogicky $\mathbb{J} \subseteq \operatorname{Im}\varphi$, z čehož dohromady $\operatorname{Im}\varphi = \mathbb{J}$, a důkaz je tedy hotov. □

Důsledek. *H je prvorozložený silný kvaternionový obor, čímž speciálně pro každé $n \in \mathbb{N}$ existuje $\theta \in H$ takové, že $N(\theta) = n$.*

Věta 3.4.3. *Uvažujme*

$$G = \left\{\frac{x + y\alpha + z\beta + w\alpha\beta}{2} : x, y, z, w \in \mathbb{Z} \wedge x \equiv y \equiv z \equiv w \pmod 2\right\},$$

kde $(A, B, \mu, \nu) = (2, 1, 1, 1)$, a

$$H = \{x + y\alpha + z\beta + w\alpha\beta : x, y, z, w \in \mathbb{Z}\},$$

kde $(A, B, \mu, \nu) = (1, 1, 1, 0)$. Potom existuje izomorfizmus $\varphi : H \to G$, který zachovává normu.

Důkaz. Pro vyvarování se nedorozumění opatřme znaky $A, B, \mu, \nu, \alpha, \beta$ indexem G nebo H dle toho, která sada je míněna. Položme

$$\gamma = \frac{1 + \alpha_G - \beta_G + \alpha_G\beta_G}{2}, \qquad \delta = \beta_G.$$

Potom platí

$$\gamma\delta = \frac{1 + \alpha_G - \beta_G + \alpha_G\beta_G}{2}\cdot\beta_G = \frac{1 - \alpha_G + \beta_G + \alpha_G\beta_G}{2},$$

$$\gamma^2 = \left(\frac{1+\alpha_G-\beta_G+\alpha_G\beta_G}{2}\right)^2 = \frac{-1+\alpha_G-\beta_G+\alpha_G\beta_G}{2} = \frac{1+\alpha_G-\beta_G+\alpha_G\beta_G}{2} - 1 =$$
$$= \mu_H\gamma - A_H,$$
$$\delta^2 = \beta_G^2 = -1 = -B_H,$$
$$\delta\gamma = \beta_G \cdot \frac{1+\alpha_G-\beta_G+\alpha_G\beta_G}{2} = \frac{-1+\alpha_G+\beta_G-\alpha_G\beta_G}{2} =$$
$$= -\frac{1-\alpha_G+\beta_G+\alpha_G\beta_G}{2} + \beta_G = -\nu_H - \gamma\delta + \mu_H\delta.$$

Lemmatem 3.4.1 tedy existuje izomorfizmus

$$\varphi : H \to \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\},$$

který zachovává normu. Zbývá tedy ukázat

$$\operatorname{Im}\varphi = \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\} = G =$$
$$= \left\{x + y\alpha_G + z\beta_G + w \cdot \frac{1+\alpha_G+\beta_G+\alpha_G\beta_G}{2} : x, y, z, w \in \mathbb{Z}\right\}.$$

Zřejmě $\gamma, \delta, \gamma\delta \in G$, takže z uzavřenosti G na tvorbu lineárních kombinací s celočíselnými koeficienty musí být $\operatorname{Im}\varphi \subseteq G$. Naopak ale i

$$\alpha_G = \gamma + \delta - \gamma\delta, \qquad \beta_G = \delta, \qquad \frac{1+\alpha_G+\beta_G+\alpha_G\beta_G}{2} = \gamma + \delta,$$

takže analogicky $G \subseteq \operatorname{Im}\varphi$, z čehož dohromady $\operatorname{Im}\varphi = G$, a důkaz je tedy hotov. □

Důsledek. *G je prvorozložený silný kvaternionový obor, čímž speciálně pro každé $n \in \mathbb{N}$ existuje $\theta \in G$ takové, že $N(\theta) = n$.*

Věta 3.4.4. *Uvažujme*

$$G = \left\{\frac{x + y\alpha + z\beta + w\alpha\beta}{3} : x, y, z, w \in \mathbb{Z} \wedge x \equiv y \equiv z \equiv w \pmod 3\right\},$$

kde $(A, B, \mu, \nu) = (1, 2, 1, 0)$, a

$$H = \{x + y\alpha + z\beta + w\alpha\beta : x, y, z, w \in \mathbb{Z}\},$$

kde $(A, B, \mu, \nu) = (1, 1, 1, 1)$. Potom existuje izomorfizmus $\varphi : H \to G$, který zachovává normu.

Důkaz. Pro vyvarování se nedorozumění opatřme znaky $A, B, \mu, \nu, \alpha, \beta$ indexem G nebo H dle toho, která sada je míněna. Položme

$$\gamma = \alpha_G, \qquad \delta = \frac{-1+2\alpha_G-\beta_G-\alpha_G\beta_G}{3}.$$

Potom platí

$$\gamma\delta = \alpha_G \cdot \frac{-1+2\alpha_G-\beta_G-\alpha_G\beta_G}{3} = \frac{-2+\alpha_G+\beta_G-2\alpha_G\beta_G}{3},$$
$$\gamma^2 = \alpha_G^2 = \alpha_G - 1 = \mu_H\gamma - A_H,$$
$$\delta^2 = \left(\frac{-1+2\alpha_G-\beta_G-\alpha_G\beta_G}{3}\right)^2 = -1 = -B_H,$$
$$\delta\gamma = \frac{-1+2\alpha_G-\beta_G-\alpha_G\beta_G}{3} \cdot \alpha_G = \frac{-2+\alpha_G-2\beta_G+\alpha_G\beta_G}{3} =$$
$$= -1 - \frac{-2+\alpha_G+\beta_G-2\alpha_G\beta_G}{3} + \frac{-1+2\alpha_G-\beta_G-\alpha_G\beta_G}{3} = -\nu_H - \gamma\delta + \mu_H\delta.$$

Lemmatem 3.4.1 tedy existuje izomorfizmus

$$\varphi : H \to \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\},$$

který zachovává normu. Zbývá tedy ukázat

$$\begin{aligned}\operatorname{Im}\varphi &= \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\} = G = \\ &= \left\{x + y\alpha_G + z\beta_G + w \cdot \frac{1 + \alpha_G + \beta_G + \alpha_G\beta_G}{3} : x, y, z, w \in \mathbb{Z}\right\}.\end{aligned}$$

Zřejmě $\gamma, \delta, \gamma\delta \in G$, takže z uzavřenosti G na tvorbu lineárních kombinací s celočíselnými koeficienty musí být $\operatorname{Im}\varphi \subseteq G$. Naopak ale i

$$\alpha_G = \gamma + \delta - \gamma\delta, \qquad \beta_G = \gamma - 2\delta + \gamma\delta, \qquad \frac{1 + \alpha_G + \beta_G + \alpha_G\beta_G}{3} = \gamma - \delta,$$

takže analogicky $G \subseteq \operatorname{Im}\varphi$, z čehož dohromady $\operatorname{Im}\varphi = G$, a důkaz je tedy hotov. □

Důsledek. *G je prvorozložený silný kvaternionový obor, čímž speciálně pro každé $n \in \mathbb{N}$ existuje $\theta \in G$ takové, že $N(\theta) = n$.*

Věta 3.4.5. *Uvažujme*

$$G = \left\{x + y\alpha + z\beta + \frac{w\alpha\beta}{2} : x, y, z, w \in \mathbb{Z}\right\},$$

kde $(A, B, \mu, \nu) = (2, 2, 1, 2)$, a

$$H = \{x + y\alpha + z\beta + w\alpha\beta : x, y, z, w \in \mathbb{Z}\},$$

kde $(A, B, \mu, \nu) = (1, 2, 1, 1)$. Potom existuje izomorfizmus $\varphi : H \to G$, který zachovává normu.

Důkaz. Pro vyvarování se nedorozumění opatřme znaky $A, B, \mu, \nu, \alpha, \beta$ indexem G nebo H dle toho, která sada je míněna. Položme

$$\gamma = -\frac{\alpha_G\beta_G}{2}, \qquad \delta = -\beta_G.$$

Potom platí

$$\begin{aligned}\gamma\delta &= -\frac{\alpha_G\beta_G}{2} \cdot (-\beta_G) = -\alpha_G, \\ \gamma^2 &= \left(-\frac{\alpha_G\beta_G}{2}\right)^2 = \frac{1}{4}(-2\alpha_G\beta_G - 4) = \mu_H\gamma - A_H, \\ \delta^2 &= (-\beta_G)^2 = -2 = -B_H, \\ \delta\gamma &= -\beta_G \cdot \left(-\frac{\alpha_G\beta_G}{2}\right) = \frac{1}{2}(-2\beta_G + 2\alpha_G - 2) = -1 + \alpha_G - \beta_G = -\nu_H - \gamma\delta + \mu_H\delta.\end{aligned}$$

Lemmatem 3.4.1 tedy existuje izomorfizmus

$$\varphi : H \to \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\},$$

který zachovává normu. Zbývá tedy ukázat

$$\operatorname{Im}\varphi = \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\} = G.$$

Zřejmě $\gamma, \delta, \gamma\delta \in G$, takže z uzavřenosti G na tvorbu lineárních kombinací s celočíselnými koeficienty musí být $\operatorname{Im}\varphi \subseteq G$. Naopak ale i

$$\alpha_G = -\gamma\delta, \qquad \beta_G = \delta, \qquad \frac{\alpha_G\beta_G}{2} = -\gamma,$$

takže analogicky $G \subseteq \operatorname{Im}\varphi$, z čehož dohromady $\operatorname{Im}\varphi = G$, a důkaz je tedy hotov. □

Důsledek. *G je prvorozložený silný kvaternionový obor, čímž speciálně pro každé $n \in \mathbb{N}$ existuje $\theta \in G$ takové, že $N(\theta) = n$.*

Věta 3.4.6. *Uvažujme*

$$G = \left\{ \frac{x + y\alpha + z\beta + w\alpha\beta}{5} : x, y, z, w \in \mathbb{Z} \wedge 2x \equiv y \equiv z \equiv -2w \pmod 5 \right\},$$

kde $(A, B, \mu, \nu) = (3, 1, 1, 1)$, a

$$H = \{x + y\alpha + z\beta + w\alpha\beta : x, y, z, w \in \mathbb{Z}\},$$

kde $(A, B, \mu, \nu) = (1, 1, 1, 1)$. Potom existuje izomorfizmus $\varphi : H \to G$, který zachovává normu.

Důkaz. Pro vyvarování se nedorozumění opatřme znaky $A, B, \mu, \nu, \alpha, \beta$ indexem G nebo H dle toho, která sada je míněna. Položme

$$\gamma = \frac{1 + 2\alpha_G + 2\beta_G - \alpha_G\beta_G}{5}, \qquad \delta = \beta_G.$$

Potom platí

$$\begin{aligned}
\gamma\delta &= \frac{1 + 2\alpha_G + 2\beta_G - \alpha_G\beta_G}{5} \cdot \beta_G = \frac{-2 + \alpha + \beta + 2\alpha\beta}{5}, \\
\gamma^2 &= \left(\frac{1 + 2\alpha_G + 2\beta_G - \alpha_G\beta_G}{5}\right)^2 = \frac{-4 + 2\alpha_G + 2\beta_G - \alpha_G\beta_G}{5} = \\
&= \frac{1 + 2\alpha_G + 2\beta_G - \alpha_G\beta_G}{5} - 1 = \mu_H\gamma - A_H, \\
\delta^2 &= (-\beta_G)^2 = -1 = -B_H, \\
\delta\gamma &= \beta_G \cdot \frac{1 + 2\alpha_G + 2\beta_G - \alpha_G\beta_G}{5} = \frac{-3 - \alpha_G + 4\beta_G - 2\alpha_G\beta_G}{5} = \\
&= -1 - \frac{-2 + \alpha + \beta + 2\alpha\beta}{5} + \beta_G = -\nu_H - \gamma\delta + \mu_H\delta.
\end{aligned}$$

Lemmatem 3.4.1 tedy existuje izomorfizmus

$$\varphi : H \to \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\},$$

který zachovává normu. Zbývá tedy ukázat

$$\begin{aligned}
\operatorname{Im}\varphi &= \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\} = G = \\
&= \left\{ x + y\alpha_G + z\beta_G + w \cdot \frac{1 + 2\alpha_G + 2\beta_G - \alpha_G\beta_G}{5} : x, y, z, w \in \mathbb{Z} \right\}.
\end{aligned}$$

Zřejmě $\gamma, \delta, \gamma\delta \in G$, takže z uzavřenosti G na tvorbu lineárních kombinací s celočíselnými koeficienty musí být $\operatorname{Im}\varphi \subseteq G$. Naopak ale i

$$\alpha_G = 2\gamma - \delta + \gamma\delta, \qquad \beta_G = \delta, \qquad \frac{1 + 2\alpha_G + 2\beta_G - \alpha_G\beta_G}{5} = \gamma,$$

takže analogicky $G \subseteq \operatorname{Im}\varphi$, z čehož dohromady $\operatorname{Im}\varphi = G$, a důkaz je tedy hotov. □

Důsledek. *G je prvorozložený silný kvaternionový obor, čímž speciálně pro každé $n \in \mathbb{N}$ existuje $\theta \in G$ takové, že $N(\theta) = n$.*

Věta 3.4.7. *Uvažujme*

$$G = \left\{ x + y\alpha + z\beta + \frac{w\alpha\beta}{2} : x, y, z, w \in \mathbb{Z} \right\},$$

kde $(A, B, \mu, \nu) = (2, 2, 1, 0)$, a

$$H = \{ x + y\alpha + z\beta + w\alpha\beta : x, y, z, w \in \mathbb{Z} \},$$

kde $(A, B, \mu, \nu) = (2, 1, 1, 0)$. Potom existuje izomorfizmus $\varphi : H \to G$, který zachovává normu.

Důkaz. Pro vyvarování se nedorozumění opatřme znaky $A, B, \mu, \nu, \alpha, \beta$ indexem G nebo H dle toho, která sada je míněna. Položme

$$\gamma = \alpha_G, \qquad \delta = \frac{\alpha_G\beta_G}{2}.$$

Potom platí

$$\begin{aligned}
\gamma\delta &= \alpha_G \cdot \frac{\alpha_G\beta_G}{2} = \frac{\alpha_G\beta_G}{2} - \beta, \\
\gamma^2 &= \alpha_G^2 = \alpha_G - 2 = \mu_H\gamma - A_H, \\
\delta^2 &= \left(\frac{\alpha_G\beta_G}{2}\right)^2 = \frac{1}{4} \cdot (-4) = -1 = -B_H, \\
\delta\gamma &= \frac{\alpha_G\beta_G}{2} \cdot \alpha_G = \frac{1}{2}(2\beta) = \beta = -\left(\frac{\alpha_G\beta_G}{2} - \beta\right) - \frac{\alpha_G\beta_G}{2} = -\nu_H - \gamma\delta + \mu_H\delta.
\end{aligned}$$

Lemmatem 3.4.1 tedy existuje izomorfizmus

$$\varphi : H \to \{ x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z} \},$$

který zachovává normu. Zbývá tedy ukázat

$$\operatorname{Im}\varphi = \{ x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z} \} = G.$$

Zřejmě $\gamma, \delta, \gamma\delta \in G$, takže z uzavřenosti G na tvorbu lineárních kombinací s celočíselnými koeficienty musí být $\operatorname{Im}\varphi \subseteq G$. Naopak ale i

$$\alpha_G = \gamma, \qquad \beta_G = \delta\gamma = \delta - \gamma\delta, \qquad \frac{\alpha_G\beta_G}{2} = \delta,$$

takže analogicky $G \subseteq \operatorname{Im}\varphi$, z čehož dohromady $\operatorname{Im}\varphi = G$, a důkaz je tedy hotov. □

Důsledek. *G je prvorozložený silný kvaternionový obor, čímž speciálně pro každé $n \in \mathbb{N}$ existuje $\theta \in G$ takové, že $N(\theta) = n$.*

Věta 3.4.8. *Uvažujme*

$$G = \left\{ \frac{x + y\alpha + z\beta + w\alpha\beta}{3} : x, y, z, w \in \mathbb{Z} \wedge x \equiv -y \equiv z \equiv -w \pmod 3 \right\},$$

kde $(A, B, \mu, \nu) = (2, 2, 0, 1)$, a

$$H = \{x + y\alpha + z\beta + w\alpha\beta : x, y, z, w \in \mathbb{Z}\},$$

kde $(A, B, \mu, \nu) = (1, 2, 1, 1)$. Potom existuje izomorfizmus $\varphi : H \to G$, který zachovává normu.

Důkaz. Pro vyvarování se nedorozumění opatřme znaky $A, B, \mu, \nu, \alpha, \beta$ indexem G nebo H dle toho, která sada je míněna. Položme

$$\gamma = \frac{1 - \alpha_G + \beta_G - \alpha_G\beta_G}{3}, \qquad \delta = \beta_G.$$

Potom platí

$$\begin{aligned}
\gamma\delta &= \frac{1 - \alpha_G + \beta_G - \alpha_G\beta_G}{3} \cdot \beta_G = \frac{-2 + 2\alpha_G + \beta_G - \alpha_G\beta_G}{3}, \\
\gamma^2 &= \left(\frac{1 - \alpha_G + \beta_G - \alpha_G\beta_G}{3} \right)^2 = \frac{-2 - \alpha + \beta - \alpha\beta}{3} = \frac{1 - \alpha_G + \beta_G - \alpha_G\beta_G}{3} - 1 = \\
&= \mu_H\gamma - A_H, \\
\delta^2 &= \beta_G^2 = -2 = -B_H, \\
\delta\gamma &= \beta_G \cdot \frac{1 - \alpha_G + \beta_G - \alpha_G\beta_G}{3} = \frac{-1 - 2\alpha_G + 2\beta_G + \alpha_G\beta_G}{3} = \\
&= -1 - \frac{-2 + 2\alpha_G + \beta_G - \alpha_G\beta_G}{3} + \beta = -\nu_H - \gamma\delta + \mu_H\delta.
\end{aligned}$$

Lemmatem 3.4.1 tedy existuje izomorfizmus

$$\varphi : H \to \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\},$$

který zachovává normu. Zbývá tedy ukázat

$$\begin{aligned}
\operatorname{Im}\varphi &= \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\} = G = \\
&= \left\{ x + y\alpha_G + z\beta_G + w \cdot \frac{1 - \alpha_G + \beta_G - \alpha_G\beta_G}{3} : x, y, z, w \in \mathbb{Z} \right\}.
\end{aligned}$$

Zřejmě $\gamma, \delta, \gamma\delta \in G$, takže z uzavřenosti G na tvorbu lineárních kombinací s celočíselnými koeficienty musí být $\operatorname{Im}\varphi \subseteq G$. Naopak ale i

$$\alpha_G = 1 - \gamma + \gamma\delta, \qquad \beta_G = \delta, \qquad \frac{1 - \alpha_G + \beta_G - \alpha_G\beta_G}{3} = \gamma,$$

takže analogicky $G \subseteq \operatorname{Im}\varphi$, z čehož dohromady $\operatorname{Im}\varphi = G$, a důkaz je tedy hotov. □

Důsledek. *G je prvorozložený silný kvaternionový obor, čímž speciálně pro každé $n \in \mathbb{N}$ existuje $\theta \in G$ takové, že $N(\theta) = n$.*

Věta 3.4.9. *Uvažujme*

$$G = \left\{ \frac{x + y\alpha + z\beta + w\alpha\beta}{7} : x, y, z, w \in \mathbb{Z} \wedge x \equiv 3y \equiv 2z \equiv -w \pmod 7 \right\},$$

kde $(A, B, \mu, \nu) = (2, 3, 1, 0)$*, a*

$$H = \{x + y\alpha + z\beta + w\alpha\beta : x, y, z, w \in \mathbb{Z}\},$$

kde $(A, B, \mu, \nu) = (1, 1, 1, 0)$*. Potom existuje izomorfizmus* $\varphi : H \to G$*, který zachovává normu.*

Důkaz. Pro vyvarování se nedorozumění opatřme znaky $A, B, \mu, \nu, \alpha, \beta$ indexem G nebo H dle toho, která sada je míněna. Položme

$$\gamma = \frac{2 + 3\alpha_G + \beta_G - 2\alpha_G\beta_G}{7}, \qquad \delta = \frac{-2 + 4\alpha_G - \beta_G + 2\alpha_G\beta_G}{7}.$$

Potom platí

$$\begin{aligned}
\gamma\delta &= \frac{2 + 3\alpha_G + \beta_G - 2\alpha_G\beta_G}{7} \cdot \frac{-2 + 4\alpha_G - \beta_G + 2\alpha_G\beta_G}{7} = \frac{-1 + 2\alpha_G - 4\beta_G + \alpha_G\beta_G}{7}, \\
\gamma^2 &= \left(\frac{2 + 3\alpha_G + \beta_G - 2\alpha_G\beta_G}{7} \right)^2 = \frac{-5 + 3\alpha_G + \beta_G - 2\alpha_G\beta_G}{7} = \\
&= \frac{2 + 3\alpha_G + \beta_G - 2\alpha_G\beta_G}{7} - 1 = \mu_H\gamma - A_H, \\
\delta^2 &= \left(\frac{-2 + 4\alpha_G - \beta_G + 2\alpha_G\beta_G}{7} \right)^2 = -1 = -B_H, \\
\delta\gamma &= \frac{-2 + 4\alpha_G - \beta_G + 2\alpha_G\beta_G}{7} \cdot \frac{2 + 3\alpha_G + \beta_G - 2\alpha_G\beta_G}{7} = \frac{-1 + 2\alpha_G + 3\beta_G + \alpha_G\beta_G}{7} = \\
&= -\frac{-1 + 2\alpha_G - 4\beta_G + \alpha_G\beta_G}{7} + \frac{-2 + 4\alpha_G - \beta_G + 2\alpha_G\beta_G}{7} = -\nu_H - \gamma\delta + \mu_H\delta.
\end{aligned}$$

Lemmatem 3.4.1 tedy existuje izomorfizmus

$$\varphi : H \to \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\},$$

který zachovává normu. Zbývá tedy ukázat

$$\begin{aligned}
\operatorname{Im}\varphi &= \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\} = G = \\
&= \left\{ x + y\alpha_G + z\beta_G + w \cdot \frac{-1 + 2\alpha_G - 4\beta_G + \alpha_G\beta_G}{7} : x, y, z, w \in \mathbb{Z} \right\}.
\end{aligned}$$

Zřejmě $\gamma, \delta, \gamma\delta \in G$, takže z uzavřenosti G na tvorbu lineárních kombinací s celočíselnými koeficienty musí být $\operatorname{Im}\varphi \subseteq G$. Naopak ale i

$$\alpha_G = \gamma + \delta, \qquad \beta_G = \delta - 2\gamma\delta, \qquad \frac{-1 + 2\alpha_G - 4\beta_G + \alpha_G\beta_G}{7} = \gamma\delta,$$

takže analogicky $G \subseteq \operatorname{Im}\varphi$, z čehož dohromady $\operatorname{Im}\varphi = G$, a důkaz je tedy hotov. □

Důsledek. *G je prvorozložený silný kvaternionový obor, čímž speciálně pro každé $n \in \mathbb{N}$ existuje $\theta \in G$ takové, že $N(\theta) = n$.*

Věta 3.4.10. *Uvažujme*

$$G = \left\{ \frac{x + y\alpha + z\beta + w\alpha\beta}{11} : x, y, z, w \in \mathbb{Z} \wedge 3x \equiv 4y \equiv -2z \equiv w \pmod{11} \right\},$$

kde $(A, B, \mu, \nu) = (3, 2, 1, 0)$, *a*

$$H = \{x + y\alpha + z\beta + w\alpha\beta : x, y, z, w \in \mathbb{Z}\},$$

kde $(A, B, \mu, \nu) = (1, 1, 1, 1)$. *Potom existuje izomorfizmus* $\varphi : H \to G$, *který zachovává normu.*

Důkaz. Pro vyvarování se nedorozumění opatřme znaky $A, B, \mu, \nu, \alpha, \beta$ indexem G nebo H dle toho, která sada je míněna. Položme

$$\gamma = \frac{4 + 3\alpha_G - 6\beta_G + \alpha_G\beta_G}{11}, \qquad \delta = \frac{-3 + 6\alpha_G - \beta_G + 2\alpha_G\beta_G}{11}.$$

Potom platí

$$\begin{aligned}
\gamma\delta &= \frac{4 + 3\alpha_G - 6\beta_G + \alpha_G\beta_G}{11} \cdot \frac{-3 + 6\alpha_G - \beta_G + 2\alpha_G\beta_G}{11} = \frac{-6 + \alpha_G - 2\beta_G + 4\alpha_G\beta_G}{11}, \\
\gamma^2 &= \left(\frac{4 + 3\alpha_G - 6\beta_G + \alpha_G\beta_G}{11} \right)^2 = \frac{-3 + 3\alpha_G - 6\beta_G + \alpha_G\beta_G}{11} = \\
&= \frac{4 + 3\alpha_G - 6\beta_G + \alpha_G\beta_G}{11} - 1 = \mu_H\gamma - A_H, \\
\delta^2 &= \left(\frac{-3 + 6\alpha_G - \beta_G + 2\alpha_G\beta_G}{11} \right)^2 = -1 = -B_H, \\
\delta\gamma &= \frac{-3 + 6\alpha_G - \beta_G + 2\alpha_G\beta_G}{11} \cdot \frac{4 + 3\alpha_G - 6\beta_G + \alpha_G\beta_G}{11} = \frac{-8 + 5\alpha_G + \beta_G - 2\alpha_G\beta_G}{11} = \\
&= -1 - \frac{-6 + \alpha_G - 2\beta_G + 4\alpha_G\beta_G}{11} + \frac{-3 + 6\alpha_G - \beta_G + 2\alpha_G\beta_G}{11} = -\nu_H - \gamma\delta + \mu_H\delta.
\end{aligned}$$

Lemmatem 3.4.1 tedy existuje izomorfizmus

$$\varphi : H \to \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\},$$

který zachovává normu. Zbývá tedy ukázat

$$\begin{aligned}
\operatorname{Im}\varphi &= \{x + y\gamma + z\delta + w\gamma\delta : x, y, z, w \in \mathbb{Z}\} = G = \\
&= \left\{ x + y\alpha_G + z\beta_G + w \cdot \frac{4 + 3\alpha_G - 6\beta_G + \alpha_G\beta_G}{11} : x, y, z, w \in \mathbb{Z} \right\}.
\end{aligned}$$

Zřejmě $\gamma, \delta, \gamma\delta \in G$, takže z uzavřenosti G na tvorbu lineárních kombinací s celočíselnými koeficienty musí být $\operatorname{Im}\varphi \subseteq G$. Naopak ale i

$$\alpha_G = 2\delta - \gamma\delta, \qquad \beta_G = \delta - 2\gamma + 1, \qquad \frac{4 + 3\alpha_G - 6\beta_G + \alpha_G\beta_G}{11} = \gamma,$$

takže analogicky $G \subseteq \operatorname{Im}\varphi$, z čehož dohromady $\operatorname{Im}\varphi = G$, a důkaz je tedy hotov. □

Důsledek. *G je prvorozložený silný kvaternionový obor, čímž speciálně pro každé $n \in \mathbb{N}$ existuje $\theta \in G$ takové, že $N(\theta) = n$.*

Lemma 3.4.11. *Budiž G obor splňující*

$$G = \{x + y\alpha + z\beta + w\zeta : x, y, z, w \in \mathbb{Z}\}$$

pro nějaké $\zeta = \frac{\zeta_0}{p}$ v základním tvaru, kde $\zeta_0 \in H$ a p je prvočíslo. Potom množiny jednotek U_H, U_G po řadě v H, G splňují

$$\frac{|U_G|}{|U_H|} \leq p + 1, \tag{3.13}$$

a pokud nastává rovnost, pak už pro každé $\theta \in G$ existuje jednotka $\varepsilon \in U_G$ taková, že $\varepsilon\theta \in H$.

Důkaz. Platí $p\zeta \in H$, pročež lze zřejmě libovolný prvek G vyjádřit jako $\lambda + \ell\zeta$ pro nějaká $\lambda \in H, \ell \in \{0, \ldots, p-1\}$. Speciálně tedy pro každé $\theta \in G$ platí $\zeta\theta = \lambda + \ell\zeta$ pro nějaká λ, ℓ, z čehož už $\zeta(\theta - \ell) = \lambda \in H$. Speciálně tedy existují $\ell_1, \ell_2, \ell_3 \in \{0, \ldots, p-1\}$ taková, že

$$\zeta(\alpha - \ell_1) \in H, \qquad \zeta(\beta - \ell_2) \in H, \qquad \zeta(\alpha\beta - \ell_3) \in H.$$

Pro každé $\theta_0 \in H$ tvaru

$$px + y(\alpha - \ell_1) + z(\beta - \ell_2) + w(\alpha\beta - \ell_3), \tag{3.14}$$

kde $x, y, z, w \in \mathbb{Z}$, pak tedy platí $\zeta\theta_0 \in H$, resp. dokonce $(\rho\zeta + \tau)\theta_0 \in H$ pro libovolná $\rho, \tau \in H$. Tvarem $\rho\zeta + \tau$ však lze popsat libovolný prvek G.

Nyní lze libovolné $\theta \in G \setminus H$ zapsat tvarem

$$\theta = m(\zeta + \ell) + \theta_0$$

pro $m \in \{1, \ldots, p-1\}, \ell \in \{0, \ldots, p-1\}$, a to dokonce jednoznačně. Zaveďme tedy zobrazení $\chi : G \setminus H \to \{0, \ldots, p-1\}$ předpisem $\chi(\theta) = \ell \pmod p$. Ukažme nyní, že pro $\varepsilon \in U_G \setminus U_H$ a $\theta \in G \setminus H$ platí $\varepsilon\theta \in H$, právě pokud $\chi(\theta) = \chi(\overline{\varepsilon})$. Zaprvé jistě platí $\overline{\varepsilon} = m(\zeta + \chi(\overline{\varepsilon})) + \varepsilon_0$ pro nějaké ε_0 tvaru (3.14) a $m \in \{1, \ldots, p-1\}$. Potom z $\varepsilon\overline{\varepsilon} = 1 \in H$ platí

$$\varepsilon \cdot m(\zeta + \chi(\overline{\varepsilon})) \in H.$$

Pokud by nyní $\varepsilon \cdot (\zeta + \chi(\overline{\varepsilon}))$ nebylo prvkem H, pak by v základním tvaru mělo jmenovatel, který je dělitelem m, a tedy různý od p. To je spor, pročež nutně $\varepsilon \cdot (\zeta + \chi(\overline{\varepsilon})) \in H$. Z toho už pro

$$\theta = m(\zeta + \chi(\overline{\varepsilon})) + \theta_0,$$

kde m je ne nutně stejné jako u $\overline{\varepsilon}$ a θ_0 je tvaru (3.14), snadno plyne

$$\varepsilon\theta = m \cdot \varepsilon(\zeta + \chi(\overline{\varepsilon})) + \varepsilon\theta_0 \in H.$$

Nyní naopak předpokládejme $\varepsilon\theta \in H$ a nechť platí

$$\theta = m(\zeta + \chi(\theta)) + \theta_0$$

pro $m \in \{1, \ldots, p-1\}$. Zaveďme

$$\theta' = m(\zeta + \chi(\overline{\varepsilon})) + \theta_0.$$

Pak $\varepsilon\theta, \varepsilon\theta' \in H$, z čehož

$$\varepsilon \cdot m(\chi(\theta) - \chi(\overline{\varepsilon})) = \varepsilon(\theta - \theta') = \varepsilon\theta - \varepsilon\theta' \in H.$$

Přitom $\varepsilon \notin H$, pročež z tohoto plyne $p \mid m(\chi(\theta) - \chi(\overline{\varepsilon}))$. Číslo m je s p nesoudělné, pročež nutně $p \mid \chi(\theta) - \chi(\overline{\varepsilon})$, což už značí $\chi(\theta) = \chi(\overline{\varepsilon})$.

Zaveďme nyní pro $\ell \in \{0, \ldots, p-1\}$ množinu U_ℓ předpisem

$$U_\ell = \{\varepsilon : \varepsilon \in U_G \setminus U_H \wedge \chi(\overline{\varepsilon}) = \ell\}.$$

Prvky U_ℓ jsou tedy právě ty jednotky $\varepsilon \in U_G \setminus U_H$, pro něž $\varepsilon(\zeta + \ell) \in H$. Ukažme, že pokud U_ℓ je neprázdná a má nějaký prvek ε, pak už je

$$U_\ell = U_H\varepsilon.$$

Zaprvé díky $\varepsilon(\zeta + \ell) \in H$ pro $\varphi \in U_H$ platí $\varphi\varepsilon \cdot (\zeta + \ell) \in H$, neboli $U_H\varepsilon \subseteq U_\ell$. Naopak pokud $\chi(\overline{\varphi}) = \ell = \chi(\overline{\varepsilon})$ pro nějakou jednotku $\varphi \in U_G \setminus U_H$, pak jistě i $\varphi\overline{\varepsilon}$ musí být prvkem H, a uvážením normy dokonce prvkem U_H. Tedy

$$\begin{aligned} \varphi\overline{\varepsilon} &\in U_H, \\ \varphi &\in U_H\varepsilon. \end{aligned}$$

Tímto speciálně máme $|U_\ell| \in \{0, |U_H|\}$. Přitom platí

$$U_G = U_H \cup U_0 \cup \cdots \cup U_{p-1},$$

z čehož už máme

$$|U_G| \leq |U_H| + |U_0| + \cdots + |U_{p-1}| \leq |U_H| \cdot (p+1), \tag{3.15}$$

neboli (3.13). Rozmysleme si dále, že pokud pro $\varepsilon_1, \varepsilon_2 \in U_G$ mají množiny $U_H\varepsilon_1, U_H\varepsilon_2$ společný prvek, pak už jsou totožné[6]. Nechť pro $\varphi_1, \varphi_2 \in U_H$ platí $\varphi_1\varepsilon_1 = \varphi_2\varepsilon_2$. Potom už $\varepsilon_2 = (\overline{\varphi_1}\varphi_2)\varepsilon_1$, přičemž $\overline{\varphi_1}\varphi_2$ je prvek U_H, pročež

$$U_H\varepsilon_2 = (U_H\overline{\varphi_2}\varphi_1)\,\varepsilon_1 = U_H\varepsilon_1.$$

Z tohoto lze tedy usoudit, že v prvé nerovnosti v (3.15) nastává vždy rovnost, neboť jednotlivé U_ℓ jsou disjunktní sobě navzájem i samotné U_H. Z toho plyne, že pokud v (3.13) nastává rovnost, pak nastává rovnost i v (3.15), tj. žádná z U_ℓ není neprázdná, neboli pro libovolné $\theta \in G \setminus H$ existuje $\varepsilon \in U_G \setminus U_H$ splňující $\chi(\overline{\varepsilon}) = \chi(\theta)$, což už znamená $\varepsilon\theta \in H$. Pro $\theta \in H$ pak jednoduše stačí zvolit $\varepsilon = 1$. □

S pomocí tohoto lemmatu nyní pro několik takovýchto oborů $H \subseteq G$, ukážeme, že (ve značení právě dokázaného lemmatu) pro každé $\theta \in G$ existuje $\varepsilon \in U_G$ takové, že $\varepsilon\theta \in H$. Z tohoto spolu s již dokázanými izomorfizmy speciálně vyplyne univerzálnost příslušných forem (3.1).

[6] Slovy teorie grup: U_G tvoří s násobením kvaternionů grupu, přičemž U_H je její podgrupou, pročež jsou navzájem různé pravé kosety $U_H\varepsilon$ disjunktní. Z tohoto také plyne, že $|U_G|$ je násobkem $|U_H|$, neboli je $\frac{|U_G|}{|U_H|}$ vždy přirozené číslo.

Budeme tedy potřebovat stanovit $|U_H|$ a $|U_G|$. V libovolném oboru H daném vztahem (3.3) pro $\theta = x + y\alpha + z\beta + w\alpha\beta \in H$ vzhledem k definici α, β platí

$$\begin{aligned} N(\theta) &= (x^2 + \mu xy + Ay^2) + \nu(yz - xw) + B(z^2 + \mu zw + Aw^2) = \\ &= \left(x + y\frac{\mu}{2} - w\frac{\nu}{2}\right)^2 + \left(y\frac{\sqrt{S}}{2} + z\frac{\nu}{\sqrt{S}} + w\frac{\mu\nu}{2\sqrt{S}}\right)^2 + \frac{T}{S}\left(z + w\frac{\mu}{2}\right)^2 + \frac{T}{4}w^2. \end{aligned}$$

Chceme-li tedy stanovit $|U_H|$, jistě není třeba zvažovat ta θ, pro něž nastává jedna z nerovností

$$\left(x + y\frac{\mu}{2} - w\frac{\nu}{2}\right)^2 > 1, \qquad \left(y\frac{\sqrt{S}}{2} + z\frac{\nu}{\sqrt{S}} + w\frac{\mu\nu}{2\sqrt{S}}\right)^2 > 1,$$
$$\frac{T}{S}\left(z + w\frac{\mu}{2}\right)^2 > 1, \qquad \frac{T}{4}w^2 > 1.$$

Takových θ, pro něž ani jedna z těchto nerovností nenastává, je však jistě pouze konečně mnoho: neplatností poslední nerovnosti je w omezeno na pouze konečně mnoho hodnot (konkrétně $|w| \leq 2\sqrt{\frac{1}{T}}$). Potom je ale i z neplatností předposlední nerovnosti omezeno na konečně mnoho hodnot atp. Velikost U_H lze tedy určit projitím všech možností.

Tento postup lze pak využít i pro stanovení $|U_G|$, kde $H \subseteq G$ a $p \cdot G \subseteq H$ pro nějaké $p \in \mathbb{N}$. Lze totiž nalézt všechna $\theta \in H$, pro něž $N(\theta) = p^2$ (v nerovnostech výše budeme na pravých stranách psát p^2 namísto 1), a posléze z nich vybrat ty kvaterniony θ, pro která $\frac{\theta}{p} \in G$.

Lemma 3.4.12. *Budiž $(A, B, \mu, \nu) = (2, 1, 1, 1)$ a zaveďme*

$$G = \left\{ \frac{x + y\alpha + z\beta + w\alpha\beta}{2} : x, y, z, w \in \mathbb{Z} \wedge x \equiv y \equiv z \equiv w \pmod 2 \right\}.$$

Potom pro každé $\theta \in G$ existuje jednotka $\varepsilon \in G$ taková, že $\varepsilon\theta \in H$.

Důkaz. Označme H_3 obor (3.3) pro $(A, B, \mu, \nu) = (1, 1, 1, 0)$ – potom je dle věty 3.4.3 H_3 izomorfní G. V H_3 jsou (užitím výše popsané metody) jednotkami právě

$$\begin{array}{lll} \pm 1, & \pm \alpha, & \pm (1 - \alpha), \\ \pm \beta, & \pm \alpha\beta, & \pm (\beta - \alpha\beta) \end{array}$$

(znaky α, β jsou zde míněny pro $(A, B, \mu, \nu) = (1, 1, 1, 0)$), pročež existuje v G právě 12 jednotek. V H existují právě jednotky

$$\pm 1, \qquad \pm \beta,$$

tedy jsou celkem 4. Platí $\frac{12}{4} = 3 = 2+1$, pročež je důkaz hotov vzetím $p = 2, \zeta = \frac{1+\alpha+\beta+\alpha\beta}{2}$ v lemmatu 3.4.11. □

Důsledek. *Kvadratická forma*

$$(x^2 + xy + 2y^2) + (yz - xw) + (z^2 + zw + 2w^2)$$

je univerzální.

Lemma 3.4.13. *Budiž* $(A, B, \mu, \nu) = (1, 2, 1, 0)$ *a zaveďme*

$$G = \left\{ \frac{x + y\alpha + z\beta + w\alpha\beta}{3} : x, y, z, w \in \mathbb{Z} \wedge x \equiv y \equiv z \equiv w \pmod 3 \right\}.$$

Potom pro každé $\theta \in G$ *existuje jednotka* $\varepsilon \in G$ *taková, že* $\varepsilon\theta \in H$.

Důkaz. Označme H_2 obor (3.3) pro $(A, B, \mu, \nu) = (1, 1, 1, 1)$ – potom je dle věty 3.4.4 H_2 izomorfní G. Dle věty 3.4.2 je pak H_2 izomorfní $\mathbb{J}$, pročež má G přesně 24 jednotek (viz sekci 2.2). Dále existují v H právě jednotky

$$\pm 1, \qquad \pm \alpha, \qquad \pm (1 - \alpha),$$

tedy je jich celkem 6. Platí $\frac{24}{6} = 4 = 3 + 1$, pročež je důkaz vzetím $p = 3, \zeta = \frac{1+\alpha+\beta+\alpha\beta}{3}$ v lemmatu 3.4.11 hotov. □

Důsledek. *Kvadratická forma*

$$(x^2 + xy + y^2) + 2(z^2 + zw + w^2)$$

je univerzální.

Lemma 3.4.14. *Budiž* $(A, B, \mu, \nu) = (2, 2, 1, 2)$ *a zaveďme*

$$G = \left\{ x + y\alpha + z\beta + \frac{w\alpha\beta}{2} : x, y, z, w \in \mathbb{Z} \right\}.$$

Potom pro každé $\theta \in G$ *existuje jednotka* $\varepsilon \in G$ *taková, že* $\varepsilon\theta \in H$.

Důkaz. Označme H_5 obor (3.3) pro $(A, B, \mu, \nu) = (1, 2, 1, 1)$ – potom je dle věty 3.4.5 H_5 izomorfní G. V H_5 jsou (užitím výše popsané metody) jednotkami právě

$$\pm 1, \qquad \pm \alpha, \qquad \pm (1 - \alpha)$$

(znaky α, β jsou zde míněny pro $(A, B, \mu, \nu) = (1, 2, 1, 1)$), pročež existuje v G právě 6 jednotek. Dále existují v H právě jednotky

$$\pm 1,$$

tedy jsou celkem 2. Platí $\frac{6}{2} = 3 = 2 + 1$, pročež je důkaz hotov vzetím $p = 2, \zeta = \frac{\alpha\beta}{2}$ v lemmatu 3.4.11. □

Důsledek. *Kvadratická forma*

$$(x^2 + xy + 2y^2) + 2(yz - xw) + 2(z^2 + zw + 2w^2)$$

je univerzální.

Lemma 3.4.15. *Budiž* $(A, B, \mu, \nu) = (3, 1, 1, 1)$ *a zaveďme*

$$G = \left\{ \frac{x + y\alpha + z\beta + w\alpha\beta}{5} : x, y, z, w \in \mathbb{Z} \wedge 2x \equiv y \equiv z \equiv -2w \pmod 5 \right\}.$$

Potom pro každé $\theta \in G$ *existuje jednotka* $\varepsilon \in G$ *taková, že* $\varepsilon\theta \in H$.

Důkaz. Označme H_2 obor (3.3) pro $(A, B, \mu, \nu) = (1, 1, 1, 1)$ – potom je dle věty 3.4.4 H_2 izomorfní G. Stejně jako výše má H_2 přesně 24 jednotek, pročež jich týž počet existuje i v G. Dále existují v H právě jednotky

$$\pm 1, \qquad \pm \beta,$$

tedy jsou celkem 4. Platí $\frac{24}{4} = 6 = 5 + 1$, pročež je důkaz vzetím $p = 5, \zeta = \frac{1+2\alpha+2\beta-\alpha\beta}{5}$ v lemmatu 3.4.11 hotov. □

Důsledek. *Kvadratická forma*

$$(x^2 + xy + 3y^2) + (yz - xw) + (z^2 + zw + 3w^2)$$

je univerzální.

Lemma 3.4.16. *Budiž* $(A, B, \mu, \nu) = (3, 2, 1, 0)$ *a zaveďme*

$$G = \left\{ \frac{x + y\alpha + z\beta + w\alpha\beta}{11} : x, y, z, w \in \mathbb{Z} \wedge 3x \equiv 4y \equiv -2z \equiv w \pmod{11} \right\}.$$

Potom pro každé $\theta \in G$ *existuje jednotka* $\varepsilon \in G$ *taková, že* $\varepsilon\theta \in H$.

Důkaz. Označme H_2 obor (3.3) pro $(A, B, \mu, \nu) = (1, 1, 1, 1)$ – potom je dle věty 3.4.4 H_2 izomorfní G. Stejně jako výše má H_2 přesně 24 jednotek, pročež jich týž počet existuje i v G. Dále existují v H právě jednotky

$$\pm 1,$$

tedy jsou celkem 2. Platí $\frac{24}{2} = 12 = 11 + 1$, pročež je důkaz vzetím $p = 11, \zeta = \frac{4+3\alpha-6\beta+\alpha\beta}{11}$ v lemmatu 3.4.11 hotov. □

Důsledek. *Kvadratická forma*

$$(x^2 + xy + 3y^2) + 2(z^2 + zw + 3w^2)$$

je univerzální.

Věta 3.4.17. *Budiž* $(A, B, \mu, \nu) = (2, 2, 1, 0)$. *Potom pro* $n \in \mathbb{N}$ *existuje* $\lambda \in H$ *takové, že* $N(\lambda) = n$.

Důkaz. Nejprve uvažujme n liché. Zaveďme

$$G = \left\{ x + y\alpha + z\beta + \frac{w\alpha\beta}{2} : x, y, z, w \in \mathbb{Z} \right\}.$$

Potom větou 3.4.7 existuje $\theta \in G$ takové, že $N(\theta) = n$. Nechť je $\theta = x + y\alpha + z\beta + w\frac{\alpha\beta}{2}$ a pojmenujme $\zeta = \frac{\alpha\beta}{2}$ – potom

$$\zeta\theta = -w - z\alpha + y\beta + x\frac{\alpha\beta}{2},$$
$$\theta\zeta = -(w + z) + z\alpha - y\beta + (x + y)\frac{\alpha\beta}{2},$$
$$\zeta\theta\zeta = -(x + y) + y\alpha\beta + z\beta - (z + w)\frac{\alpha\beta}{2}.$$

Pro spor nechť žádný z kvaternionů $\theta, \zeta\theta, \theta\zeta, \zeta\theta\zeta$ není prvkem H. Potom určitě žádné z čísel $w, x, x+y, z+w$ není sudé, z čehož

$$x \equiv w \equiv 1 \pmod 2, \qquad\qquad y \equiv z \equiv 0 \pmod 2.$$

Potom ale

$$n = N(\theta) = x^2 + xy + 2y^2 + 2\left(z^2 + \frac{zw}{2} + \frac{2w^2}{4}\right) = x^2 + xy + 2y^2 + w^2 + wz + 2z^2 \equiv$$
$$\equiv 1 + 1 \equiv 0 \pmod 2,$$

což je spor s lichostí n. Alespoň jeden z kvaternionů $\theta, \zeta\theta, \theta\zeta, \zeta\theta\zeta$ je tedy prvkem H – pojmenujme jej λ. Platí $N(\zeta) = 1$, z čehož

$$n = N(\theta) = N(\zeta\theta) = N(\theta\zeta) = N(\zeta\theta\zeta),$$

pročež už určitě $N(\lambda) = n$. Tímto je platnost věty dokázána pro liché n.

Nyní uvažujme n sudé a nechť platí $n = 2^\ell m$ pro liché m a $\ell \in \mathbb{N}$. Z platnosti věty pro liché n určitě existuje $\lambda_0 \in H$ takové, že $N(\lambda_0) = m$. Položme potom $\lambda = \alpha^\ell \lambda_0$. Pak jistě $\lambda \in H$, zároveň ale i

$$N(\lambda) = (N(\alpha))^\ell N(\lambda_0) = 2^\ell m = n. \qquad \square$$

Důsledek. *Kvadratická forma*

$$(x^2 + xy + 2y^2) + 2(z^2 + zw + 2w^2)$$

je univerzální.

Věta 3.4.18. *Budiž $(A, B, \mu, \nu) = (2, 2, 0, 1)$. Potom pro $n \in \mathbb{N}$ existuje $\lambda \in H$ takové, že $N(\lambda) = n$.*

Důkaz. Nejprve uvažujme $3 \nmid n$. Zaveďme

$$G = \left\{ \frac{x + y\alpha + z\beta + w\alpha\beta}{3} : x, y, z, w \in \mathbb{Z} \wedge x \equiv -y \equiv z \equiv -w \pmod 3 \right\}.$$

Potom větou 3.4.8 existuje $\theta \in G$ takové, že $N(\theta) = n$. Pojmenujme $\zeta = \frac{1-\alpha+\beta-\alpha\beta}{3}$ a nechť je

$$\theta = x + y\alpha + z\beta + w\zeta$$

pro nějaká $x, y, z, w \in \mathbb{Z}$ – potom platí

$$N(\theta) = \frac{1}{9}\left((3x + w)^2 + 2\,(3y - w)^2 + (3y - w)(3z + w) - (3x + w)(-w) + \right.$$
$$\left. + 2\,(3z + w)^2 + 4(-w)^2\right) =$$
$$= x^2 + 2y^2 + 2z^2 + w^2 + xw - yw + zw + yz. \tag{3.16}$$

Dále platí

$$\zeta\alpha = \zeta + \alpha - \beta, \qquad\qquad \alpha\zeta = -\zeta + 1 + \beta,$$
$$\zeta\beta = \zeta - 1 + \alpha, \qquad\qquad \beta\zeta = -\zeta + \beta - \alpha,$$
$$\zeta^2 = \zeta - 1.$$

Pro spor nechť žádný z kvaternionů θ, $\zeta\theta$, $\theta\zeta$, $(\zeta-1)\theta$, $\theta(\zeta-1)$, $\zeta\theta\zeta$, $(\zeta-1)\theta\zeta$ nenáleží H. Platí

$$\begin{aligned}
\zeta\theta &= -(z+w)+(y+z)\alpha - y\beta + (x+y+z+w)\zeta,\\
\theta\zeta &= (y-w) - z\alpha + (y+z)\beta + (x-y-z+w)\zeta,\\
(\zeta-1)\theta &= -(x+z+w) + z\alpha - (y+z)\beta + (x+y+z)\zeta,\\
\theta(\zeta-1) &= (-x+y-w) - (y+z)\alpha + y\beta + (x-y-z)\zeta,\\
\zeta\theta\zeta &= -(x+w) + y\alpha + z\beta + (x+y-z)\zeta,\\
(\zeta-1)\theta\zeta &= -(x+y) + (y+z)\alpha - y\beta + (2y-w)\zeta.
\end{aligned}$$

Vzhledem k $\theta \notin H$ jistě $3 \nmid w$. Dále $x+y+z+w \not\equiv 0 \not\equiv x-y-z+w \pmod 3$. Pokud by nyní výrazy $x+y+z+w$, $x-y-z+w$ nebyly mod 3 kongruentní, pak by Dirichletovým principem musel jeden z nich být kongruentní číslu w. Z toho už by plynulo, že 3 dělí jedno z $x+y+z$, $x-y-z$, neboli že jedno z $(\zeta-1)\theta$, $\theta(\zeta-1)$ je prvkem H, což by byl spor. Určitě tedy $x+y+z+w \equiv x-y-z+w \pmod 3$, z čehož $3 \mid (y+z)$ a následně $0 \not\equiv x+y+z \equiv x \pmod 3$.

Pokud by nyní bylo $x \not\equiv w \pmod 3$, pak už jistě $0 \equiv x+w \equiv x+y+z+w \pmod 3$, což by byl spor s $\zeta\theta \notin H$, pročež $x \equiv w \pmod 3$. Víme, že $0 \not\equiv x+y-z \equiv x+2y \pmod 3$ a zároveň $0 \not\equiv 2y-w \equiv -x+2y \pmod 3$. Kdyby bylo $x+2y \equiv -x+2y \pmod 3$, znamenalo by to $3 \mid x$, a tedy $\theta \in H$, což by byl spor, pročež $3 \mid ((x+2y)+(-x+2y)) = 4y$, neboli $3 \mid y, z$. Z tohoto všeho skrze (3.16) plyne

$$n = N(\theta) \equiv x^2 + w^2 + xw \equiv x^2 + x^2 + x^2 \equiv 0 \pmod 3,$$

což je spor. Alespoň jedno z θ, $\zeta\theta$, $\theta\zeta$, $(\zeta-1)\theta$, $\theta(\zeta-1)$, $\zeta\theta\zeta$, $(\zeta-1)\theta\zeta$ tak musí náležet H – pojmenujme jej λ. Přitom ale

$$N(\zeta) = N(\zeta-1) = 1,$$

z čehož $N(\lambda) = N(\theta) = n$. Tímto je věta dokázána pro $3 \nmid n$.

Nyní uvažujme $3 \mid n$ a nechť platí $n = 3^\ell m$ pro $3 \nmid m$ a $\ell \in \mathbb{N}$. Z platnosti věty pro $3 \nmid n$ určitě existuje $\lambda_0 \in H$ takové, že $N(\lambda_0) = m$. Položme potom $\lambda = (\alpha+1)^\ell \lambda_0$. Pak jistě $\lambda \in H$, zároveň ale i

$$N(\lambda) = (N(\alpha+1))^\ell N(\lambda_0) = 3^\ell m = n. \qquad \square$$

Důsledek. *Kvadratická forma*

$$(x^2+2y^2) + (yz-xw) + 2(z^2+2w^2)$$

je univerzální.

Věta 3.4.19. *Budiž $(A,B,\mu,\nu) = (2,3,1,0)$. Potom pro $n \in \mathbb{N}$ existuje $\lambda \in H$ takové, že $N(\lambda) = n$.*

Důkaz. Všechny kongruence v tomto důkazu jsou mod 7. Nejprve uvažujme $7 \nmid n$. Zaveďme

$$G = \left\{ \frac{x+y\alpha+z\beta+w\alpha\beta}{7} : x,y,z,w \in \mathbb{Z} \wedge x \equiv 3y \equiv 2z \equiv -w \pmod 7 \right\}.$$

Potom větou 3.4.9 existuje $\theta \in G$ takové, že $N(\theta) = n$. Pojmenujme $\zeta = \frac{-1+2\alpha-4\beta+\alpha\beta}{7}$ a nechť je

$$\theta = x + y\alpha + z\beta + w\zeta$$

pro nějaká $x, y, z, w \in \mathbb{Z}$ – potom platí

$$N(\theta) = \frac{1}{49}\left((7x-w)^2 + (7x-w)(7y+2w) + 2(7y+2w)^2 + 3(7z-4w)^2 \right.$$
$$\left. +(7z-4w)w + 6w^2\right) = x^2 + xy + 2y^2 + yw + 3z^2 - 3zw + w^2. \qquad (3.17)$$

Dále také je

$$\begin{aligned} \zeta\alpha &= 4\zeta - \alpha + 2\beta, & \alpha\zeta &= -3\zeta - 1 + \alpha - 2\beta, \\ \zeta\beta &= 2\zeta + 2 - \alpha + \beta, & \beta\zeta &= -2\zeta + 1 + \alpha - \beta, \\ \zeta^2 &= -1, & \alpha\beta &= 7\zeta + 1 - 2\alpha + 4\beta. \end{aligned}$$

Jednotkami v oboru G jsou právě

$$\begin{array}{lll} \pm 1, & \pm(2\zeta - \alpha + \beta), & \pm(2\zeta - \alpha + \beta + 1), \\ \pm\zeta, & \pm(\zeta + \beta), & \pm(2\zeta + \beta). \end{array}$$

Pro spor nechť $\varepsilon_1\theta\varepsilon_2 \notin H$ pro libovolná

$$\varepsilon_1, \varepsilon_2 \in \{1, 2\zeta - \alpha + \beta, 2\zeta - \alpha + \beta + 1, \zeta, \zeta + \beta, 2\zeta + \beta\}.$$

Toto značí, že $\chi(\varepsilon_1\theta\varepsilon_2) \not\equiv 0$ pro každá $\varepsilon_1, \varepsilon_2$, kde $\chi(\eta)$ značí pro stručnost pro $\eta \in G$ to celé číslo z množiny $\{0, 1, \ldots, 6\}$, jež splňuje $\eta - \chi(\eta)\zeta \in H$. To lze ekvivalentně formulovat tak, že $\chi(\eta)$ je kongruentní koeficientu při ζ v té lineární kombinaci $1, \alpha, \beta, \zeta$, jež vyjadřuje η.

O x, y, z, w nadále uvažujme jako o prvcích $\mathbb{Z}_7$. Přímými výpočty lze stanovit jednotlivá $\chi(\varepsilon_1\theta\varepsilon_2)$ – vždy se bude jednat o lineární polynomy v x, y, z, w. V tomto důkazu využijeme

$$\begin{aligned} \chi(\zeta\theta\zeta) &\equiv -y + 3z + 2w, \\ \chi(\zeta\theta(\zeta+\beta)) &\equiv 2x - w, \\ \chi(\zeta\theta(2\zeta+\beta)) &\equiv 2x - y + 3z - 2w, \\ \chi(\zeta\theta) &\equiv x + 4y + 2z, \\ \chi(\zeta\theta(2\zeta-\alpha+\beta)) &\equiv -2x - 3y + 2z - 2w, \\ \chi(\zeta\theta(2\zeta-\alpha+\beta+1)) &\equiv -x + y + 4z - 2w \\ \chi((\zeta+\beta)\theta\zeta) &\equiv -2x - 2y - w, \\ \chi((\zeta+\beta)\theta(\zeta+\beta)) &\equiv -y - 3z + 2w, \\ \chi((\zeta+\beta)\theta(2\zeta+\beta)) &\equiv -2x - 3y - 3z + w, \\ \chi((\zeta+\beta)\theta) &\equiv x - 3y + 2z - 2w, \\ \chi((\zeta+\beta)\theta(2\zeta-\alpha+\beta)) &\equiv x + 2y + 3z + 2w, \\ \chi((\zeta+\beta)\theta(2\zeta-\alpha+\beta+1)) &\equiv 2x - y - 2z, \\ \chi((2\zeta+\beta)\theta\zeta) &\equiv -2x - 3y + 3z - 2w, \\ \chi((2\zeta+\beta)\theta(\zeta+\beta)) &\equiv 2x - y - 3z + w, \\ \chi(\theta\zeta) &\equiv x - 3y - 2z, \\ \chi(\theta(\zeta+\beta)) &\equiv x + 4y - 2z + 2w, \\ \chi((2\zeta-\alpha+\beta)\theta\zeta) &\equiv x + 2y + 4z - 2w, \\ \chi((2\zeta-\alpha+\beta)\theta(\zeta+\beta)) &\equiv -2x - 3y - 2z, \\ \chi((2\zeta-\alpha+\beta+1)\theta\zeta) &\equiv 2x - y + 2z - 2w, \end{aligned}$$

$$\chi((2\zeta-\alpha+\beta+1)\theta(\zeta+\beta)) \equiv -x+y+3z+2w,$$
$$\chi((2\zeta-\alpha+\beta)\theta(2\zeta-\alpha+\beta)) \equiv -2x+2y+w,$$
$$\chi((2\zeta-\alpha+\beta+1)\theta(2\zeta-\alpha+\beta+1)) \equiv 2x+4y+w.$$

V $\mathbb{Z}_7$ pojmenujme $a \equiv \chi(\zeta\theta\zeta) \equiv -y+3z-w$, $b \equiv \chi(\zeta\theta(\zeta+\beta)) \equiv 2x-w$, $c \equiv \chi((\zeta+\beta)\theta\zeta) \equiv -2x-2y-w$, $d \equiv \chi((\zeta+\beta)\theta(\zeta+\beta)) \equiv -y-3z+2w$. Potom nad $\mathbb{Z}_7$ platí

$$\begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix} = \begin{pmatrix} 0 & -1 & 3 & -1 \\ 2 & 0 & 0 & -1 \\ -2 & -2 & 0 & -1 \\ 0 & -1 & -3 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix},$$
$$\begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \begin{pmatrix} -1 & -2 & 1 & -1 \\ 2 & 1 & 1 & 2 \\ -2 & 1 & 1 & 0 \\ -2 & 2 & 2 & -2 \end{pmatrix} \begin{pmatrix} 0 & -1 & 3 & -1 \\ 2 & 0 & 0 & -1 \\ -2 & -2 & 0 & -1 \\ 0 & -1 & -3 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \begin{pmatrix} -1 & -2 & 1 & -1 \\ 2 & 1 & 1 & 2 \\ -2 & 1 & 1 & 0 \\ -2 & 2 & 2 & -2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \\ d \end{pmatrix}.$$

S těmito znalostmi lze vypočtené hodnoty $\chi(\varepsilon_1\theta\varepsilon_2)$ (stále mod 7) vyjádřit přehledně pomocí a, b, c, d – viz tabulku 4.

	ζ	$\zeta+\beta$	$2\zeta+\beta$	1	$2\zeta-\alpha+\beta$	$2\zeta-\alpha+\beta+1$
ζ	a	b	$a+b$	$3(a-b)$	$3a-b$	$3b-a$
$\zeta+\beta$	c	d	$c+d$	$3(c-d)$	$3c-d$	$3d-c$
$2\zeta+\beta$	$a+c$	$b+d$				
1	$3(c-a)$	$3(d-b)$				
$2\zeta-\alpha+\beta$	$3c-a$	$3d-b$			$4a+4b+2c+4d$	
$2\zeta-\alpha+\beta+1$	$3a-c$	$3b-d$				$4a+2b+c+4d$

Tabulka 4: Některé hodnoty $\chi(\varepsilon_1\theta\varepsilon_2)$, vyjádřené pomocí a, b, c, d.

Z předpokladu sporu jsou nyní všechny hodnoty v tabulce 4 nenulové mod 7. Zaměřme se nejprve na

$$a, b, a+b, 3(a-b), 3a-b, 3b-a.$$

Z nenulovosti a, b určitě existuje nějaké m splňující $b \equiv ma$, z nenulovosti $a+b, 3(a-b), 3a-b, 3b-a$ je pak vyloučeno $m \in \{-1, 1, 3, -2\}$, z čehož musí být $m \in \{2, 4\}$. Platí tedy (mod 7) $ba^{-1} \in \{2, 4\}$

Analogickou úvahou pro (c, a), (d, b) a (c, d) namísto (a, b) pak i

$$ca^{-1}, db^{-1}, dc^{-1} \in \{2, 4\}.$$

Z rovnice (3.17) platí

$$\begin{aligned} N(\theta) \equiv x^2+xy+2y^2+yw+3z^2-3zw+w^2 \equiv (-a-2b+c-d)^2+ \\ +(-a-2b+c-d)(2a+b+c+2d)+2(2a+b+c+2d)^2+ \\ +(2a+b+c+2d)\cdot 2(-a+b+c-d)+3(-2a+b+c)^2- \\ -3(-2a+b+c)\cdot 2(-a+b+c-d)+(-a+b+c-d)^2 \equiv \\ \equiv 2ad-2bc. \end{aligned}$$

Konečně rozeberme dva podpřípady.

(i) Platí $b \equiv ma$, $d \equiv mc$ pro $m \in \{2, 4\}$. Potom

$$n = N(\theta) \equiv 2a \cdot mc - 2 \cdot ma \cdot c \equiv 0,$$

což je spor s předpokladem $7 \nmid n$.

(ii) Platí $ba^{-1} \equiv m$, $dc^{-1} \equiv m^2$ pro $m \in \{2, 4\}$. Platí $\{2, 4\} = \{m, m^2\}$, takže jistě platí $db^{-1} \equiv \ell$ pro $\ell \in \{m, m^2\}$. Z toho $da^{-1} \equiv m\ell \in \{m^2, m^3\}$. Z toho nemůže být $ca^{-1} \equiv m^2$ (to by značilo $da^{-1} \equiv m^4 \notin \{m^2, m^3\}$, neboť $m^2 \not\equiv 1$ a $m \not\equiv 1$), pročež $ca^{-1} \equiv m$ a $db^{-1} \equiv m^2$. Z toho už

$$\begin{aligned} a &\equiv a, & b &\equiv ma, \\ c &\equiv ma, & d &\equiv m^3 a. \end{aligned}$$

Potom pokud $m \equiv 2$, pak

$$\chi((2\zeta - \alpha + \beta + 1)\theta(2\zeta - \alpha + \beta + 1)) \equiv 4a + 2b + c + 4d \equiv a(4 + 2 \cdot 2 + 2 + 4 \cdot 8) \equiv 0,$$

zatímco pro $m \equiv 4$ je

$$\chi((2\zeta - \alpha + \beta)\theta(2\zeta - \alpha + \beta)) \equiv 4a + 4b + 2c + 4d \equiv a(4 + 4 \cdot 4 + 2 \cdot 4 + 4 \cdot 64) \equiv 0.$$

To je dohromady spor.

V obou podpřípadech jsme vyvodili spor, pročež jistě jeden z kvaternionů $\varepsilon_1\theta\varepsilon_2$ musí být prvkem H – pojmenujme jej λ. Z toho, že $\varepsilon_1, \varepsilon_2$ jsou jednotky, ale plyne

$$N(\lambda) = N(\theta) = n,$$

čímž jsme hotovi.

Nyní uvažujme $7 \mid n$ a nechť platí $n = 7^\ell m$ pro $7 \nmid m$ a $\ell \in \mathbb{N}$. Z platnosti věty pro $7 \nmid n$ určitě existuje $\lambda_0 \in H$ takové, že $N(\lambda_0) = m$. Položme potom $\lambda = (1 + \alpha\beta)^\ell \lambda_0$. Pak jistě $\lambda \in H$, zároveň ale i

$$N(\lambda) = (N(1 + \alpha\beta))^\ell N(\lambda_0) = 7^\ell m = n. \qquad \square$$

Důsledek. *Kvadratická forma*

$$(x^2 + xy + 2y^2) + 3(z^2 + zw + 2w^2)$$

je univerzální.

Kapitola 4

Počet kvaternionů dané normy

V této kapitole přistoupíme k vyčíslení počtu kvaternionů dané normy v daném prvorozloženém silném kvaternionovém oboru. Postupně tedy dokážeme Jacobiho větu o čtyřech čtvercích a její obdoby v dalších silných kvaternionových oborech, čímž podstatně zobecníme Lagrangeovu větu a o čtyřech čtvercích (a její obdoby).

Definice 4.0.1. Pro $M \subseteq \mathbb{H}(\mathbb{R})$ a $n \in \mathbb{N}$ definujme $r_M(n) = |\{\theta : \theta \in M \wedge N(\theta) = n\}|$.

V sekci 4.3 s pomocí poznatků ze sekcí 4.1 a 4.2 explicitně vyjádříme $r_H(n)$ pro několik oborů H tvaru (3.3) – v těchto případech zároveň $r_H(n)$ představuje počet různých vyjádření přirozeného čísla n kvadratickou formou (3.1). Konkrétní obory, resp. formy, pro něž tohoto docílíme, jsou zaneseny v tabulce 5.

(A, B, μ, ν)	Kvadratická forma (3.1)	$r_H(n)$
$(1,1,1,1)$	$(x^2+xy+y^2)+(yz-xw)+(z^2+zw+w^2)$	$24\sum_{2\nmid d\mid n} d$
$(1,1,1,0)$	$(x^2+xy+y^2)+(z^2+zw+w^2)$	$12\sum_{3\nmid d\mid n} d$
$(1,1,0,0)$	$x^2+y^2+z^2+w^2$	$8\sum_{4\nmid d\mid n} d$
$(1,2,1,1)$	$(x^2+xy+y^2)+(yz-xw)+2(z^2+zw+w^2)$	$6\sum_{5\nmid d\mid n} d$
$(2,1,1,0)$	$(x^2+xy+2y^2)+(z^2+zw+2w^2)$	$4\sum_{7\nmid d\mid n} d$
$(2,1,1,1)$	$(x^2+xy+2y^2)+(yz-xw)+(z^2+zw+2w^2)$	$8\sum_{3\nmid d\mid n} d - 4\sum_{2,3\nmid d\mid n} d$
$(1,2,1,0)$	$(x^2+xy+y^2)+2(z^2+zw+w^2)$	$12\sum_{2\nmid d\mid n} d - 6\sum_{2,3\nmid d\mid n} d$
$(2,2,1,2)$	$(x^2+xy+2y^2)+2(yz-xw)+2(z^2+zw+2w^2)$	$4\sum_{5\nmid d\mid n} d - 2\sum_{2,5\nmid d\mid n} d$
$(3,1,1,1)$	$(x^2+xy+3y^2)+(yz-xw)+(z^2+zw+3w^2)$	$8\sum_{2\nmid d\mid n} d - 4\sum_{2,5\nmid d\mid n} d$
$(3,2,1,0)$	$(x^2+xy+3y^2)+2(z^2+zw+3w^2)$	$4\sum_{2\nmid d\mid n} d - 2\sum_{2,11\nmid d\mid n} d$

Tabulka 5: Explicitní vzorce pro $r_H(n)$, kde H je dán vztahem (3.3).

4.1 Faktorizace kvaternionů

Začněme prozkoumáním faktorizace v prvorozložených silných kvaternionových oborech. Cílem bude zredukovat vyčíslení $r_H(n)$ na vyčíslení $r_H(p)$ pro libovolné prvočíslo p.

Věta 4.1.1. *Budiž H prvorozložený silný kvaternionový obor. Potom je $\pi \in H$ ireducibilní, právě pokud je $N(\pi)$ prvočíslo.*

Důkaz. Pokud je $N(\pi)$ prvočíslo, pak libovolná $\theta, \eta \in H$ splňující $\pi = \theta\eta$ splňují taktéž i $N(\theta)N(\eta) = p$, z čehož jedno z nich musí být jednotkou, neboli je π vskutku ireducibilní.

Nyní nechť je π ireducibilní a uvažujme libovolné prvočíslo p, jež dělí $N(\pi)$. Dle věty 2.3.4 platí $p \in H\pi$, neboli existuje η takové, že $p = \eta\pi$. Položme $m = \frac{N(\pi)}{p} \in \mathbb{N}$ – potom máme

$$p^2 = N(\eta) \cdot mp,$$
$$p = N(\eta) \cdot m.$$

Z toho $m \in \{1, p\}$. Pokud $m = p$, musí η být jednotkou, z čehož plyne $\pi = \overline{\eta}p$. Přitom p je ale dle věty 2.3.6 reducibilní, čímž je i π jakožto jeho násobek reducibilní. To je spor, pročež jistě $m = 1$, neboli $N(\pi) = p$. □

Definice 4.1.2. Budiž H prvorozložený silný kvaternionový obor. Pro $n \in \mathbb{N}, \theta \in H$ pišme $n \mid \theta$, pokud $\theta \in nH = Hn$. Řekněme, že θ je *primitivní*, pokud pro žádné $n > 1$ není $n \mid \theta$.

Poznámka. Uvážením normy je zřejmé, že každý ireducibilní prvek i jednotka musí být primitivní.

Lemma 4.1.3. *Budiž H prvorozložený silný kvaternionový obor a uvažujme $m \in \mathbb{N}$, $\theta, \eta \in H$. Potom pokud $m \mid \theta\eta$ a zároveň $\mathrm{NSD}\,(m, N(\theta)) = 1$, pak už nutně $m \mid \eta$.*

Důkaz. $(\mathbb{Z}, +, \cdot)$ je zcela zřejmě zprava i zleva Eukleidovský obor (díky komutativitě násobení tyto pojmy zcela splývají). Budiž $x \in \mathbb{Z}$ takové, že $\mathbb{Z}N(\theta) + \mathbb{Z}m = \mathbb{Z}x$ – potom jistě $x \mid m$ a zároveň $x \mid N(\theta)$, čímž už z jejich nesoudělnosti musí být $x \in \{\pm 1\}$, neboli $\mathbb{Z}N(\theta) + \mathbb{Z}m = \mathbb{Z}$.

Existují tedy $u, v \in \mathbb{Z}$ taková, že $uN(\theta) + vm = 1$. To už ale značí

$$u\overline{\theta}\theta + vm = 1,$$
$$u\overline{\theta}\theta\eta + vm\eta = \eta,$$

neboli díky $m \mid \theta\eta$ nutně $m \mid \eta$. □

Poznámka. Analogicky platí i

$$m \mid \theta\eta \wedge \mathrm{NSD}\,(m, N(\eta)) \Longrightarrow m \mid \theta.$$

Definice 4.1.4. Budiž H prvorozložený silný kvaternionový obor. Uvažujme přirozené $n \geq 2$ a dvě n-tice $(\theta_1, \ldots, \theta_n), (\eta_1, \ldots, \eta_n) \in H^n$. Pokud existují jednotky $\varepsilon_1, \ldots, \varepsilon_{n-1}$ splňující

$$\theta_1\varepsilon_1 = \eta_1,$$
$$\overline{\varepsilon_1}\theta_2\varepsilon_2 = \eta_2,$$
$$\ldots$$
$$\overline{\varepsilon_{n-2}}\theta_{n-1}\varepsilon_{n-1} = \eta_{n-1},$$
$$\overline{\varepsilon_{n-1}}\theta_n = \eta_n,$$

řekněme, že n-tice $(\theta_1, \ldots, \theta_n)$, $(\eta_1, \ldots, \eta_n)$ se liší pouze *jednotkovým přechýlením.*

Poznámka. Je zřejmé, že v této definici nezávisí na pořadí, tj. n-tice (θ_s), (η_s) se liší pouze jednotkovým přechýlením, právě pokud se pouze jednotkovým přechýlením liší n-tice (η_s), (θ_s). Toto snadno vyplývá vzetím $\varepsilon'_s = \overline{\varepsilon_s}$ pro $s \in \{1, \ldots, n-1\}$.

Věta 4.1.5. *Budiž H prvorozložený silný kvaternionový obor. Uvažujme přirozené $n \geq 2$ a dvě n-tice $(\theta_1, \ldots, \theta_n), (\eta_1, \ldots, \eta_n) \in H^n$. Pokud je*

$$\prod_{s=1}^{n} \theta_s = \prod_{s=1}^{n} \eta_s$$

a zároveň pro každé $s \in \{1, \ldots, n\}$ platí

$$N(\theta_s) = N(\eta_s) = m_s > 1$$

pro nějakou n-tici po dvou nesoudělných $m_1, \ldots, m_n \in \mathbb{N}$, pak už se musí $(\theta_1, \ldots, \theta_n)$, $(\eta_1, \ldots, \eta_n)$ lišit pouze jednotkovým přechýlením.

Důkaz. Začněme důkazem pro $n = 2$. Rovnost $\theta_1\theta_2 = \eta_1\eta_2$ upravíme na

$$\theta_1\theta_2\overline{\theta_2} = \eta_1\eta_2\overline{\theta_2}.$$

Nyní $N(\theta_2) \mid \eta_1\left(\eta_2\overline{\theta_2}\right)$ a zároveň $\mathrm{NSD}\left(N(\theta_2), N(\eta_1)\right) = \mathrm{NSD}(m_2, m_1) = 1$, z čehož dle lemmatu 4.1.3 plyne $N(\theta) \mid \eta_2\overline{\theta_2}$. To znamená, že pro nějaké $\varepsilon \in H$ je

$$\begin{aligned} \varepsilon \cdot \theta_2\overline{\theta_2} &= \eta_2\overline{\theta_2}, \\ \varepsilon\theta_2 &= \eta_2. \end{aligned}$$

Uvážením normy musí ε být jednotkou a dosazením do $\theta_1\theta_2 = \eta_1\eta_2$ musí být i $\theta_1\overline{\varepsilon} = \eta_1$.

Nyní pomocí matematické indukce větu dokažme pro obecné n. Uvažujme, že věta je splněna pro $n = x$ a uvažujme $n = x + 1$. Položíme-li

$$\gamma = \prod_{s=1}^{x} \theta_s, \qquad \delta = \prod_{s=1}^{x} \eta_s,$$

máme rovnost $\gamma\theta_{x+1} = \delta\eta_{x+1}$ a čísla $N(\gamma) = N(\delta)$ a $N(\theta_{x+1}) = N(\eta_{x+1})$ jsou nesoudělná. Můžeme tedy aplikovat již dokázaný případ $n = 2$, neboli existuje jednotka ε_x taková, že

$$\gamma\varepsilon_x = \delta, \qquad \overline{\varepsilon_x}\theta_{x+1} = \eta_{x+1}.$$

Z rovnosti $\gamma\varepsilon_x = \delta$ ale můžeme použít indukční předpoklad, tj. platnost věty pro $n = x$, na x-tice $(\theta_1, \ldots, \theta_{x-1}, \theta_x\varepsilon_x)$ a $(\eta_1, \ldots, \eta_x)$. Tedy existují jednotky $\varepsilon_1, \ldots, \varepsilon_{x-1}$ takové, že

$$\begin{aligned} \theta_1\varepsilon_1 &= \eta_1, \\ \overline{\varepsilon_1}\theta_2\varepsilon_2 &= \eta_2, \\ &\ldots \\ \overline{\varepsilon_{x-2}}\theta_{x-1}\varepsilon_{x-1} &= \eta_{x-1}, \\ \overline{\varepsilon_{x-1}}\theta_x\varepsilon_x &= \eta_x. \end{aligned}$$

To je ale dohromady s rovností $\overline{\varepsilon_x}\theta_{x+1} = \eta_{x+1}$ přesně to, že $(\theta_1, \ldots, \theta_{x+1})$ a $(\eta_1, \ldots, \eta_{x+1})$ se liší pouze jednotkovým přechýlením. Tímto je důkaz matematickou indukcí hotov. □

Lemma 4.1.6. *Budiž H prvorozložený silný kvaternionový obor a uvažujme $\theta, \eta, \pi \in H$, kde $N(\pi) = p$ je prvočíslo. Potom pokud $p \mid \theta\pi\eta$ a zároveň $p \nmid \theta\pi$, pak už nutně $p \mid \pi\eta$.*

Důkaz. Mějme $\lambda \in H$ takové, že $H\theta\pi + Hp = H\lambda$. Dle věty 2.3.3 potom platí

$$p = \mathrm{NSD}\,(p, N(\theta\pi)) \mid N(\lambda).$$

Zároveň také $p \in H\lambda$, neboli pro nějaké $\zeta \in H$ je $p = \zeta\lambda$. Uvážením normy potom jistě $N(\zeta) \in \{1, p\}$ (p^2 je vzhledem k $p \mid N(\lambda)$ vyloučeno). Přitom $N(\zeta) = 1$ by znamenalo

$$\theta\pi \in H\lambda = H\overline{\zeta}p = Hp,$$

neboli spor s $p \nmid \theta\pi$. Nutně je tedy $N(\zeta) = p$, a tedy i $N(\lambda) = p$.
Nyní uvažme, že existují $\gamma, \delta \in H$ taková, že

$$\gamma\,(\theta\pi) + \delta p = \lambda.$$

Z toho využitím $p = \overline{\pi}\pi$ plyne

$$\begin{aligned} (\gamma\theta + \delta\overline{\pi})\,\pi &= \lambda, \\ N\,(\gamma\theta + \delta\overline{\pi})\,N(\pi) &= N(\lambda), \\ N\,(\gamma\theta + \delta\overline{\pi}) \cdot p &= p, \\ N\,(\gamma\theta + \delta\overline{\pi}) &= 1. \end{aligned}$$

Nyní již musí nutně $\gamma\theta + \delta\overline{\pi} = \varepsilon$ být jednotkou. Potom ale

$$\begin{aligned} \gamma\,(\theta\pi) + \delta p &= (\gamma\theta + \delta\overline{\pi})\,\pi = \varepsilon\pi, \\ \gamma\theta\pi\eta + \delta p\eta &= \varepsilon\pi\eta, \\ \pi\eta &= \overline{\varepsilon}\,(\gamma\theta\pi\eta + \delta p\eta)\,, \end{aligned}$$

z čehož vzhledem k $p \mid \theta\pi\eta$ jistě musí být $p \mid \pi\eta$. □

Poznámka. Analogicky platí i

$$p \mid \theta\pi\eta \wedge p \nmid \pi\eta \Longrightarrow p \mid \theta\pi.$$

Věta 4.1.7. *Budiž H prvorozložený silný kvaternionový obor a nechť je*

$$1 < n = \prod_{s=1}^{q} p_s$$

rozklad přirozeného čísla na součin (ne nutně různých) prvočísel s pevně daným pořadím těchto prvočísel. Potom pro libovolné primitivní $\theta \in H$ s $N(\theta) = n$ existují ireducibilní $\pi_1, \ldots, \pi_q \in H$ taková, že

$$\theta = \prod_{s=1}^{q} \pi_s$$

a zároveň pro $s \in \{1, \ldots, q\}$ platí $N(\pi_s) = p_s$. Tato faktorizace je navíc až na jednotkové přechýlení jednoznačně určena.

Důkaz. Nejprve dokažme existenci faktorizace. Postupujme matematickou indukcí vzhledem ke q. Pro $q = 1$ je $N(\theta) = n = p_1$ prvočíslo, pročež už je samo θ ireducibilní. Nechť nyní tvrzení platí pro $q = x$ a uvažujme $q = x + 1$. Mějme $H\theta + Hp_{x+1} = H\lambda$ pro nějaké $\lambda \in H$. Dále je $p_{x+1} = \mathrm{NSD}\,(p_{x+1}, N(\theta))$, pročež větou 2.3.3 platí $p_{x+1} \mid N(\lambda)$ – položme $m = \frac{N(\lambda)}{p_{x+1}}$.

Zároveň je $p_{x+1} \in H\lambda$, z čehož pro nějaké $\zeta \in H$ platí

$$\begin{aligned} p_{x+1} &= \zeta\lambda, \\ p_{x+1}^2 = N(p_{x+1}) &= N(\zeta)N(\lambda), \\ p_{x+1} &= mN(\zeta). \end{aligned}$$

Nyní jistě $m \in \{1, p_{x+1}\}$. Pokud $m = p_{x+1}$, pak musí ζ být jednotkou, což by znamenalo

$$\theta \in H\lambda = H\left(\overline{\zeta}p_{x+1}\right) = Hp_{x+1},$$

neboli $p_{x+1} \mid \theta$ – to by byl spor s primitivností θ.

Musí tedy být $m = 1$, tj. $N(\lambda) = p_{x+1}$. λ je tak ireducibilní, přitom ale $\theta \in H\lambda$, pročež existuje $\theta_0 \in H$ takové, že $\theta = \theta_0\lambda$. Označíme-li ještě $n_0 = \frac{n}{p_{x+1}}$, existují z indukčního předpokladu ireducibilní prvky $\pi_1, \ldots, \pi_x \in H$ takové, že

$$\theta_0 = \prod_{s=1}^{x} \pi_s$$

a zároveň $N(\pi_s) = p_s$ pro $s \in \{1, \ldots, x\}$. Nyní stačí položit $\pi_{x+1} = \lambda$ a máme

$$\theta = \theta_0\pi_{x+1} = \prod_{s=1}^{x+1} \pi_s.$$

Důkaz matematickou indukcí je tímto hotov.

Dokažme nyní jednoznačnost této faktorizace až na jednotkové přechýlení. Opět postupujme indukcí vzhledem ke q. Pro $q = 1$ je platnost dokazovaného tvrzení zřejmá, předpokládejme tedy jeho platnost pro $q = x$ a uvažujme $q = x + 1$. Mějme ireducibilní $\pi_1, \ldots, \pi_{x+1}, \rho_1, \ldots, \rho_{x+1} \in H$ taková, že $N(\pi_s) = N(\rho_s) = p_s$ pro každé $s \in \{1, \ldots, x + 1\}$ a zároveň

$$\prod_{s=1}^{x+1} \pi_s = \prod_{s=1}^{x+1} \rho_s = \theta \tag{4.1}$$

je primitivní. Z toho pak

$$\left(\prod_{s=1}^{x+1} \pi_s\right) \overline{\pi_{x+1}} = \left(\prod_{s=1}^{x+1} \rho_s\right) \overline{\pi_{x+1}}.$$

Levá strana je nyní násobkem $\pi_{x+1}\overline{\pi_{x+1}} = p_{x+1}$, pročež jím musí být i pravá strana. Z primitivnosti θ nemůže být

$$p_{x+1} \mid \prod_{s=1}^{x+1} \rho_s,$$

pročež aplikováním lemmatu 4.1.6 na trojici kvaternionů

$$\prod_{s=1}^{x} \rho_s, \qquad \rho_{x+1}, \qquad \overline{\pi_{x+1}}$$

musí být $p_{x+1} \mid \rho_{x+1}\overline{\pi_{x+1}}$. Z toho musí pro nějaké ε_x platit

$$\begin{aligned}\rho_{x+1}\overline{\pi_{x+1}} &= \varepsilon_x p_{x+1},\\ \rho_{x+1}\overline{\pi_{x+1}} &= \varepsilon_x \pi_{x+1}\overline{\pi_{x+1}},\\ \rho_{x+1} &= \varepsilon_x \pi_{x+1}\end{aligned}$$

a ε_x je nutně uvážením normy jednotka.

V (4.1) tedy můžeme zkrátit a obdržet

$$\prod_{s=1}^{x} \pi_s = \left(\prod_{s=1}^{x} \rho_s\right) \varepsilon_x.$$

Nyní však lze aplikovat indukční předpoklad. Máme dvě x-tice ireducibilních kvaternionů $(\pi_1, \ldots, \pi_x)$ a $(\rho_1, \ldots, \rho_{x-1}, \rho_x\varepsilon_x)$, jejichž součinem je v obou případech týž primitivní kvaternion. Proto tedy existují jednotky $\varepsilon_1, \ldots, \varepsilon_{x-1}$ takové, že

$$\begin{aligned}\rho_1 &= \pi_1\overline{\varepsilon_1},\\ \rho_2 &= \varepsilon_1\pi_2\overline{\varepsilon_2},\\ &\ldots\\ \rho_x\varepsilon_x &= \varepsilon_{x-1}\pi_x.\end{aligned}$$

Poslední rovnost nyní stačí upravit na $\rho_x = \varepsilon_{x-1}\pi_x\overline{\varepsilon_x}$. Potom se vzhledem k $\rho_{x+1} = \varepsilon_x\pi_{x+1}$ $(x+1)$-tice (π_s) a (ρ_s) liší pouze jednotkovým přechýlením, jak se mělo dokázat. □

Věta 4.1.8. *Budiž H prvorozložený silný kvaternionový obor. Pro $n \in \mathbb{N}$ uvažujme ireducibilní $\pi_1, \ldots, \pi_n \in H$ splňující $N(\pi_s) = p$ pro každé $s \in \{1, \ldots, n\}$ pro nějaké prvočíslo p. Potom*

$$p \mid \prod_{s=1}^{n} \pi_s,$$

právě pokud $\pi_{x+1} = \overline{\pi_x}\varepsilon$ pro nějaké x a jednotku $\varepsilon \in H$.

Důkaz. Pokud skutečně $\pi_{x+1} = \overline{\pi_x}\varepsilon$ pro nějaké x, pak je

$$p = N(\pi_x) \mid \prod_{s=1}^{n} \pi_s$$

zřejmé. Nyní naopak předpokládejme, že předchozí dělitelnost platí. Uvažme pak nejvyšší x takové, že $p \mid \prod_{s=1}^{x+1} \pi_s$, ale $p \nmid \prod_{s=1}^{x} \pi_s$ – takové x jistě existuje, neboť $p \nmid \pi_1$, ale $p \mid \prod_{s=1}^{n} \pi_s$. Potom vzetím

$$\theta = \prod_{s=1}^{x-1} \pi_s, \qquad \pi = \pi_x, \qquad \eta = \pi_{x+1}$$

v lemmatu 4.1.6 nutně $p \mid \pi_x\pi_{x+1}$. To značí, že pro nějaké $\varepsilon \in H$ je

$$\begin{aligned}\pi_x\pi_{x+1} &= p\varepsilon,\\ \pi_x\pi_{x+1} &= \pi_x\overline{\pi_x}\varepsilon,\\ \pi_{x+1} &= \overline{\pi_x}\varepsilon,\end{aligned}$$

přičemž uvážením norem musí ε být jednotkou. □

Lemma 4.1.9. *Budiž dána n-tice $\theta_1, \ldots, \theta_n \in H \setminus \{0\}$ a dvě $(n-1)$-tice jednotek $\varepsilon_1, \ldots, \varepsilon_{n-1}, \zeta_1, \ldots, \zeta_{n-1} \in H$. Potom*

$$(\theta_1\varepsilon_1, \overline{\varepsilon_1}\theta_2\varepsilon_2, \ldots, \overline{\varepsilon_{n-2}}\theta_{n-1}\varepsilon_{n-1}, \overline{\varepsilon_{n-1}}\theta_n) = \left(\theta_1\zeta_1, \overline{\zeta_1}\theta_2\zeta_2, \ldots, \overline{\zeta_{n-2}}\theta_{n-1}\zeta_{n-1}, \overline{\zeta_{n-1}}\theta_n\right), \quad (4.2)$$

právě pokud

$$(\varepsilon_1, \ldots, \varepsilon_{n-1}) = (\zeta_1, \ldots, \zeta_{n-1}).$$

Důkaz. Rovnost (4.2) nahlížejme postupně po jednotlivých složkách. Všechna θ_s jsou nenulová a H je obor, pročež lze $\theta_1\varepsilon_1 = \theta_1\zeta_1$ zkrátit na $\varepsilon_1 = \zeta_1$. Tímto i $\overline{\varepsilon_1} = \overline{\zeta_1}$, čímž se upraví

$$\begin{aligned}\overline{\varepsilon_1}\theta_2\varepsilon_2 &= \overline{\zeta_1}\theta_2\zeta_2,\\ \theta_2\varepsilon_2 &= \theta_2\zeta_2,\\ \varepsilon_2 &= \zeta_2.\end{aligned}$$

Je zřejmé, že z opakování obdobného postupu již indukcí plyne $\varepsilon_s = \zeta_s$ pro všechna $s \in \{1, \ldots, n-1\}$. □

Věta 4.1.10. *Budiž H prvorozložený silný kvaternionový obor a nechť je*

$$n = \prod_{s=1}^{q} p_s^{t_s}$$

rozklad přirozeného n na prvočísla, kde $q \in \mathbb{N}$, $p_1, \ldots, p_q$ jsou po dvou různá prvočísla a $t_1, \ldots, t_q \in \mathbb{N}_0$. Potom platí

$$r_H(n) = r_H(1) \prod_{s=1}^{q} \frac{\left(\frac{r_H(p_s)}{r_H(1)} - 1\right)^{t_s+1} - 1}{\frac{r_H(p_s)}{r_H(1)} - 2}. \quad (4.3)$$

Důkaz. Nejprve dokažme, že pro prvočíslo p a $t \in \mathbb{N}$ existuje právě

$$r_H(p)\left(\frac{r_H(p_s)}{r_H(1)} - 1\right)^{t-1}$$

různých primitivních $\theta \in H$ takových, že $N(\theta) = p^t$. Každé takové θ lze dle věty 4.1.7 faktorizovat jako

$$\theta = \prod_{s=1}^{t} \pi_s$$

pro nějaká ireducibilní $\pi_1, \ldots, \pi_t$. Tato faktorizace je navíc jednoznačná až na jednotkové přechýlení, tj. mezi všemi možnými t-ticemi (π_s) bude každé θ vzhledem k lemmatu 4.1.9 zastoupeno $r_H(1)^{t-1}$-krát. Zbývá tedy určit, pro kolik takových t-tic (π_s) je θ primitivní. To však dle věty 4.1.8 nastává právě tehdy, pokud nenastává $\pi_{x+1} = \overline{\pi_x}\varepsilon$ pro nějaké x a jednotku $\varepsilon \in H$. Představme si tedy, že jednotlivá π_s volíme postupně, vyhýbajíce se $p \mid \theta$. Pro π_1 se nabízí $r_H(p)$ možností, pro každé následující π_s je však třeba nezvolit žádný z kvaternionů tvaru $\overline{\pi_{s-1}}\varepsilon$, kterých je zřejmě $r_H(1)$, tedy existuje $r_H(p) - r_H(1)$ možností. Dohromady je tedy takových primitivních θ právě

$$\frac{1}{r_H(1)^{t-1}} \cdot r_H(p) \cdot (r_H(p) - r_H(1))^{t-1} = r_H(p)\left(\frac{r_H(p)}{r_H(1)} - 1\right)^{t-1},$$

jak jsme chtěli dokázat.

Nyní dokažme platnost věty pro $q = 1$, tedy v případě, kdy je n prvočíselnou mocninou. Postupujme indukcí vzhledem k t_1. Pro $t_1 \in \{0, 1\}$ zřejmě (4.3) platí (tehdy dá tato rovnice po řadě $r_H(n) = r_H(1)$ a $r_H(n) = r_H(p_1)$). Předpokládejme tedy, že platí pro $t_1 \leq x$ pro nějaké $x \in \mathbb{N}$, a uvažujme $t_1 = x + 1$. Každé $\theta \in H$ splňující $N(\theta) = p_1^{x+1}$ je jednoho ze dvou druhů. Není-li primitivní, pak je tvaru $p\theta_0$ pro nějaké θ_0 s normou p_1^{x-1} – těchto θ je tedy z indukčního předpokladu právě

$$r_H\left(p_1^{x-1}\right) = r_H(1)\frac{\left(\frac{r_H(p_1)}{r_H(1)} - 1\right)^x - 1}{\frac{r_H(p_1)}{r_H(1)} - 2} = r_H(1)\sum_{\ell=0}^{x-1}\left(\frac{r_H(p_1)}{r_H(1)} - 1\right)^\ell.$$

Naopak těch θ, jež jsou primitivní, je, jak jsme dokázali, právě $r_H(p)\left(\frac{r_H(p_s)}{r_H(1)} - 1\right)^x$. Dohromady tedy máme

$$\begin{aligned}
r_H\left(p_1^{x+1}\right) &= r_H(1)\sum_{\ell=0}^{x-1}\left(\frac{r_H(p_1)}{r_H(1)} - 1\right)^\ell + r_H(p_1)\left(\frac{r_H(p_1)}{r_H(1)} - 1\right)^x = \\
&= r_H(1)\left(\sum_{\ell=0}^{x-1}\left(\frac{r_H(p_1)}{r_H(1)} - 1\right)^\ell + \frac{r_H(p_1)}{r_H(1)}\left(\frac{r_H(p_1)}{r_H(1)} - 1\right)^x\right) = \\
&= r_H(1)\left(\sum_{\ell=0}^{x-1}\left(\frac{r_H(p_1)}{r_H(1)} - 1\right)^\ell + \left(\frac{r_H(p_1)}{r_H(1)} - 1\right)^x + \left(\frac{r_H(p_1)}{r_H(1)} - 1\right)^{x+1}\right) = \\
&= r_H(1)\sum_{\ell=0}^{x+1}\left(\frac{r_H(p_1)}{r_H(1)} - 1\right)^\ell = \\
&= r_H(1)\cdot\frac{\left(\frac{r_H(p_1)}{r_H(1)} - 1\right)^{x+2} - 1}{\frac{r_H(p_1)}{r_H(1)} - 2}
\end{aligned}$$

Tímto tedy máme indukcí větu dokázánu pro prvočíselné mocniny.

Nyní konečně uvažujme zcela obecné n. Z věty 4.1.7 plyne, že každé θ s $N(\theta) = n$ lze vyjádřit jako

$$\theta = \prod_{s=1}^{q}\lambda_s,$$

kde $N(\lambda_s) = p_s^{t_s}$ pro každé $s \in \{1, \ldots, q\}$ (jednoduše sdružíme všechny ireducibilní činitele s touž normou do jediného). Přitom podle věty 4.1.5 je tato faktorizace jednoznačná až na jednotkové přechýlení, pročež mezi takovými q-ticemi (λ_s) bude každé θ zastoupeno právě $r_H(1)^{q-1}$-krát. Z platnosti dokazované věty pro prvočíselné mocniny pak už nutně musí být

$$\begin{aligned}
r_H(n) &= \frac{1}{r_H(1)^{q-1}}\prod_{s=1}^{q} r_H(1)\frac{\left(\frac{r_H(p_s)}{r_H(1)} - 1\right)^{t_s+1} - 1}{\frac{r_H(p_s)}{r_H(1)} - 2} = \\
&= r_H(1)\prod_{s=1}^{q}\frac{\left(\frac{r_H(p_s)}{r_H(1)} - 1\right)^{t_s+1} - 1}{\frac{r_H(p_s)}{r_H(1)} - 2},
\end{aligned}$$

což jsme přesně chtěli dokázat. □

Díky této větě tedy zbývá pouze určit $r_H(p)$ pro libovolné prvočíslo p.

4.2 Modulární aritmetika kvaternionů

Navraťme se nyní ke značení z kapitoly 3 (a držme jej opět po zbytek kapitoly) – nechť jsou zvolena $A, B \in \mathbb{N}, \mu, \nu \in \mathbb{Z}$ a pojmenujme

$$S = 4A - \mu^2, \qquad T = BS - \nu^2,$$

přičemž uvažujme pouze ty čtveřice (A, B, μ, ν), pro něž platí $S, T > 0$. Dále zaveďme

$$\begin{aligned} \alpha_1 &= \frac{\mu}{2}, & \beta_1 &= \frac{\nu}{\sqrt{S}}, \\ \alpha_2 &= \frac{\sqrt{S}}{2}, & \beta_2 &= \sqrt{\frac{T}{S}}, \\ \alpha &= \alpha_1 + \alpha_2 i, & \beta &= \beta_1 i + \beta_2 j \end{aligned}$$

a (jak bylo ukázáno v sekci 3.2) obor

$$H = \{x + y\alpha + z\beta + w\alpha\beta : x, y, z, w \in \mathbb{Z}\}.$$

Definice 4.2.1. Pro $m \in \mathbb{N}, \theta, \eta \in H$ nechť $\eta \equiv \theta \pmod{m}$ značí $m \mid (\eta - \theta)$, tj. $(\eta - \theta) \in mH = Hm$. Dále definujme

$$H_m = \{x + y\alpha + z\beta + w\alpha\beta : x, y, z, w \in \{0, \ldots, m-1\}\}.$$

Prvky H_m chápejme jako zbytkové třídy. Snadno si rozmyslíme, že pro různá $\eta, \theta \in H_m$ nemůže nastat $\eta \equiv \theta \pmod{m}$, naopak pro každé $\theta \in H$ existuje právě jedno $\eta \in H_m$ takové, že $\eta \equiv \theta \pmod{m}$. V tomto smyslu (bereme-li sčítání i násobení mod m tak, aby výsledek byl vždy z H_m) tedy potom zřejmě H_m tvoří se sčítáním a násobením okruh (nemusí se však jednat o obor, ač sám H oborem je).

Věta 4.2.2. *Budiž p prvočíslo, jež nedělí T. Potom existuje izomorfizmus*

$$\psi : H_p \to \mathrm{M}_2(\mathbb{Z}_p)$$

takový, že $\det \psi(\theta) \equiv N(\theta) \pmod{p}$.

Důkaz. V celém důkazu uvažujme o A, B, μ, ν, T jako o prvcích $\mathbb{Z}_p$. Mějme libovolné $\theta = x + y\alpha + z\beta + w\alpha\beta \in H_p$. Dle lemmatu 3.2.3 existují $e, f \in \mathbb{Z}$ taková, že $N(e + \alpha + f\beta) \equiv e^2 + \mu e + A + Bf^2 + \nu f \equiv 0 \pmod{p}$. Položme potom

$$\begin{aligned} X &\equiv x + (e + \mu)y + Bfw \pmod{p}, \\ Y &\equiv -fy + z + (e + \mu)w \pmod{p}, \\ Z &\equiv -(Bf + \nu)y - Bz + Bew \pmod{p}, \\ W &\equiv x - ey - (Bf + \nu)w \pmod{p}. \end{aligned}$$

Vezmeme-li nyní $\psi(\theta) = \begin{pmatrix} X & Y \\ Z & W \end{pmatrix}$, bude zaručeno

$$\begin{aligned} \det \psi(\theta) = \begin{vmatrix} X & Y \\ Z & W \end{vmatrix} &= XW - YZ \equiv \\ &\equiv (x + (e + \mu)y + Bfw)(x - ey - (Bf + \nu)w) - \\ &\quad - (-fy + z + (e + \mu)w)(-(Bf + \nu)y - Bz + Bew) \equiv \end{aligned}$$

$$\begin{aligned}
&\equiv x^2 + y^2(-(e+\mu)e - f(Bf+\nu)) + Bz^2 + Bw^2(-f(Bf+\nu) - (e+\mu)e) + \\
&\quad + xy(-e + (e+\mu)) + xw(-(Bf+\nu) + Bf) + yz(-Bf + (Bf+\nu)) + \\
&\quad + yw(-(e+\mu)(Bf+\nu) - Bef + Bef + (e+\mu)(Bf+\nu)) + \\
&\quad + Bzw(-e + (e+\mu)) \equiv \\
&\equiv x^2 + \mu xy - y^2(e^2 + \mu e + Bf^2 + \nu f) + \nu(zy - xw) + \\
&\quad + B(z^2 + \mu zw - w^2(e^2 + \mu e + Bf^2 + \nu f)) \equiv \\
&\equiv (x^2 + \mu xy + Ay^2) + \nu(yz - xw) + B(z^2 + \mu zw + Aw^2) \equiv N(\theta) \pmod p.
\end{aligned}$$

Dále ukažme, že zobrazení ψ je prosté. Nechť pro $\theta_1, \theta_2 \in H_p$, $\theta_1 = x_1 + y_1\alpha + z_1\beta + w_1\alpha\beta$, $\theta_2 = x_2 + y_2\alpha + z_2\beta + w_2\alpha\beta$ platí $\psi(\theta_1) = \psi(\theta_2)$. To značí

$$\begin{aligned}
x_1 + (e+\mu)y_1 + Bfw_1 &\equiv x_2 + (e+\mu)y_2 + Bfw_2 \pmod p, && \text{(X)}\\
-fy_1 + z_1 + (e+\mu)w_1 &\equiv -fy_2 + z_2 + (e+\mu)w_2 \pmod p, && \text{(Y)}\\
-(Bf+\nu)y_1 - Bz_1 + Bew_1 &\equiv -(Bf+\nu)y_2 - Bz_2 + Bew_2 \pmod p, && \text{(Z)}\\
x_1 - ey_1 - (Bf+\nu)w_1 &\equiv x_2 - ey_2 - (Bf+\nu)w_1 \pmod p. && \text{(W)}
\end{aligned}$$

Z toho vzetím lineárních kombinací kongruencí (X) − (W), B(Y) + (Z) obdržíme po řadě

$$\begin{aligned}
(2e+\mu)y_1 + (2Bf+\nu)w_1 &\equiv (2e+\mu)y_2 + (2Bf+\nu)w_2 \pmod p, && (4.4)\\
-(2Bf+\nu)y_1 + B(2e+\mu)w_1 &\equiv -(2Bf+\nu)y_2 + B(2e+\mu)w_2 \pmod p. && (4.5)
\end{aligned}$$

Nyní již vzetím $B(2e+\mu)(4.4) - (2Bf+\nu)(4.5)$ a $(2Bf+\nu)(4.4) + (2e+\mu)(4.5)$ obdržíme po řadě

$$\begin{aligned}
y_1\left(B(2e+\mu)^2 + (2Bf+\nu)^2\right) &\equiv y_2\left(B(2e+\mu)^2 + (2Bf+\nu)^2\right) \pmod p,\\
w_1\left((2Bf+\nu)^2 + B(2e+\mu)^2\right) &\equiv w_2\left((2Bf+\nu)^2 + B(2e+\mu)^2\right) \pmod p,
\end{aligned}$$

což vzhledem k

$$\begin{aligned}
B(2e+\mu)^2 + (2Bf+\nu)^2 &= 4B\left(e^2 + \mu e + Bf^2 + \nu f\right) + B\mu^2 + \nu^2 \equiv\\
&\equiv -4AB + B\mu^2 + \nu^2 \equiv -T \pmod p
\end{aligned}$$

a $p \nmid T$ značí

$$y_1 \equiv y_2 \pmod p, \qquad w_1 \equiv w_2 \pmod p.$$

Z toho již z (X) a (Y) snadno plyne i

$$x_1 \equiv x_2 \pmod p, \qquad z_1 \equiv z_2 \pmod p,$$

což dohromady znamená, že $\psi(\theta_1) = \psi(\theta_2)$, právě pokud $\theta_1 \equiv \theta_2 \pmod p$.

ψ je tedy prosté. Přitom $|\mathrm{M}_2(\mathbb{Z}_p)| = p^4 = |H_p|$, takže ψ už musí být bijekcí. Zbývá tak dokázat, že se jedná o homomorfizmus. Vlastnost $\psi(\theta_1 + \theta_2) = \psi(\theta_1) + \psi(\theta_2)$ je zřejmá. Ukažme tedy $\psi(\theta_1\theta_2) = \psi(\theta_1)\psi(\theta_2)$. Začněme pro $\theta_1, \theta_2 \in \{1, \alpha, \beta, \alpha\beta\}$. Platí

$$\begin{aligned}
\psi(1) &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & \psi(\alpha) &= \begin{pmatrix} e+\mu & -f \\ -Bf-\nu & -e \end{pmatrix},\\
\psi(\beta) &= \begin{pmatrix} 0 & 1 \\ -B & 0 \end{pmatrix}, & \psi(\alpha\beta) &= \begin{pmatrix} Bf & e+\mu \\ Be & -Bf-\nu \end{pmatrix},
\end{aligned}$$

z čehož $\psi(1)\psi(\theta) = \psi(\theta) = \psi(1 \cdot \theta)$ pro libovolné $\theta \in H_p$. Pro $\ell \in \mathbb{Z}_p$ je zřejmé $\ell\psi(\theta) = \psi(\ell\theta)$ a zároveň

$$\begin{aligned}
\psi(\alpha)\psi(\beta) &= \begin{pmatrix} e+\mu & -f \\ -Bf-\nu & -e \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -B & 0 \end{pmatrix} = \begin{pmatrix} Bf & e+\mu \\ Be & -Bf-\nu \end{pmatrix} = \psi(\alpha\beta),\\
\psi(\alpha)\psi(\alpha) &= \begin{pmatrix} e+\mu & -f \\ -Bf-\nu & -e \end{pmatrix}\begin{pmatrix} e+\mu & -f \\ -Bf-\nu & -e \end{pmatrix} = \\
&= \begin{pmatrix} e^2+2e\mu+\mu^2+Bf^2+f\nu & -ef-f\mu+fe \\ (-Bf-\nu)(e+\mu-e) & Bf^2+f\nu+e^2 \end{pmatrix} = \\
&= \begin{pmatrix} (e+\mu)\mu-A & -f\mu \\ (-Bf-\nu)\mu & -A-e\mu \end{pmatrix} = \mu\psi(\alpha) - A\psi(1) = \psi(\mu\alpha - A) = \psi(\alpha^2),\\
\psi(\beta)\psi(\beta) &= \begin{pmatrix} 0 & 1 \\ -B & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ -B & 0 \end{pmatrix} = \begin{pmatrix} -B & 0 \\ 0 & -B \end{pmatrix} = -B\psi(1) = \psi(-B) = \psi(\beta^2),\\
\psi(\beta)\psi(\alpha) &= \begin{pmatrix} 0 & 1 \\ -B & 0 \end{pmatrix}\begin{pmatrix} e+\mu & -f \\ -Bf-\nu & -e \end{pmatrix} = \begin{pmatrix} -Bf-\nu & -e \\ -Be-B\mu & Bf \end{pmatrix} = \\
&= -\nu\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} - \begin{pmatrix} Bf & e+\mu \\ Be & -Bf-\nu \end{pmatrix} + \mu\begin{pmatrix} 0 & 1 \\ -B & 0 \end{pmatrix} = \\
&= -\nu\psi(1) - \psi(\alpha\beta) + \mu\psi(\beta) = \psi(-\nu - \alpha\beta + \mu\beta) = \psi(\beta\alpha).
\end{aligned}$$

Máme tedy rovnosti

$$\psi(\alpha)\psi(\beta) = \psi(\alpha\beta), \qquad \psi(\alpha)^2 = \psi(\alpha^2), \qquad \psi(\beta)^2 = \psi(\beta^2), \qquad \psi(\beta)\psi(\alpha) = \psi(\beta\alpha),$$

z nichž lze (analogicky s příslušnou částí důkazu věty 3.2.1) již odvodit všechny ostatní rovnosti $\psi(\theta_1)\psi(\theta_2) = \psi(\theta_1\theta_2)$ pro $\theta_1, \theta_2 \in \{1, \alpha, \beta, \alpha\beta\}$.

Z tohoto již distributivitou plyne platnost $\psi(\theta_1\theta_2) = \psi(\theta_1)\psi(\theta_2)$ pro libovolná $\theta_1, \theta_2 \in H_p$. Položíme-li totiž $\theta_1 = x_1 + y_1\alpha + z_1\beta + w_1\alpha\beta$, $\theta_2 = x_2 + y_2\alpha + z_2\beta + w_2\alpha\beta$, pak je

$$\psi(\theta_1\theta_2) = \psi\left((x_1 + y_1\alpha + z_1\beta + w_1\alpha\beta)(x_2 + y_2\alpha + z_2\beta + w_2\alpha\beta)\right)$$

roznásobením vnitřní závorky rovno součtu členů tvaru $\psi(c_1c_2\lambda_1\lambda_2)$, kde

$$c_1 \in \{x_1, y_1, z_1, w_1\}, \qquad c_2 \in \{x_2, y_2, z_2, w_2\}, \qquad \lambda_1, \lambda_2 \in \{1, \alpha, \beta, \alpha\beta\}.$$

Z již dokázaného však lze každý takový člen přepsat na $\psi(c_1\lambda_1)\psi(c_2\lambda_2)$ a tyto členy opět vytknout, čímž obdržíme

$$(x_1\psi(1)+y_1\psi(\alpha)+z_1\psi(\beta)+w_1\psi(\alpha\beta))(x_2\psi(1)+y_2\psi(\alpha)+z_2\psi(\beta)+w_2\psi(\alpha\beta)) = \psi(\theta_1)\psi(\theta_2).$$

Důkaz věty je tímto hotov. □

Lemma 4.2.3. *Pro prvočíslo $p \nmid T$ existuje právě $(p^2-1)(p+1)$ kvaternionů $\theta \in H_p$ různých od 0, jejichž norma je násobkem p.*

Důkaz. Dle věty 4.2.2 stačí spočíst matice

$$\begin{pmatrix} x & y \\ z & w \end{pmatrix} \in \mathrm{M}_2(\mathbb{Z}_p)$$

různé od nulové matice, jejichž determinant je násobkem p.

Počítáme tedy čtveřice $x, y, z, w \in \mathbb{Z}_p$ takové, že $xw \equiv yz \pmod p$, ale alespoň jedno z x, y, z, w není násobkem p. Rozeberme několik případů:

(i) $x \equiv w \equiv 0 \pmod{p}$. Potom právě jedno z y, z musí být 0 a druhé musí nabývat libovolné nenulové hodnoty. Tento případ tedy do celkového počtu přispěje přesně $2(p-1)$ maticemi.

(ii) Právě jedno z x, w je nulové. Takových dvojic (x, w) je zřejmě $2(p-1)$. Volba y, z potom vyhoví právě tehdy, pokud nejsou obě nenulová – takových voleb je tedy zřejmě $p^2 - (p-1)^2 = 2p - 1$. Celkem tento případy tedy přispívá

$$2(p-1)(2p-1) = 4p^2 - 6p + 2$$

maticemi.

(iii) Obě x, w jsou nenulová – potom musí být nenulová i y, z. Přitom po zvolení x, y, z je již w jednoznačně určeno kýženou kongruencí, pročež tento případ přispívá $(p-1)^3$ maticemi.

Celkový tedy dostáváme

$$(p-1)^3 + (4p^2 - 6p + 2) + 2(p-1) = p^3 + p^2 - p - 1 = (p^2 - 1)(p+1)$$

vyhovujících matic, čímž je lemma dokázáno. □

Lemma 4.2.4. *Mějme prvočíslo $p \nmid T$ a budiž dáno $\tau \in H_p \setminus \{0\}$ splňující $N(\tau) \equiv 0 \pmod{p}$. Potom výraz $\theta\tau \pmod{p}$ pro $\theta \in H_p$ nabývá právě p^2 různých hodnot, z nichž $p^2 - 1$ je různých od nuly.*

Důkaz. Označme nejprve

$$M_\tau = \{\theta : \theta \in H_p \wedge \theta\tau \equiv 0 \pmod{p}\}$$

a dokažme $|M_\tau| = p^2$. Budiž ψ bijekce s vlastnostmi popsanými ve větě 4.2.2. Potom je $\theta\tau \equiv 0 \pmod{p}$ ekvivalentní

$$\psi(\theta)\psi(\tau) = \psi(0) = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

nad $\mathbb{Z}_p$ Označíme-li $\psi(\tau) = \begin{pmatrix} x & y \\ z & w \end{pmatrix}$, stačí tedy spočíst matice $\psi(\theta) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, pro něž

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}. \tag{4.6}$$

Kongruence (4.6) je přitom ekvivalentní soustavě

$$\begin{aligned} ax + bz &\equiv 0 \pmod{p}, \\ ay + bw &\equiv 0 \pmod{p}, \\ cx + dz &\equiv 0 \pmod{p}, \\ cy + dw &\equiv 0 \pmod{p}. \end{aligned}$$

Matice $\psi(\tau)$ je nenulová, pročež alespoň jedno z x, y, z, w není násobkem p – nechť je to bez újmy na obecnosti x. Potom stačí libovolně zvolit $b, d \in \mathbb{Z}_p$ a položit

$$a \equiv -bzx^{-1} \pmod{p}, \qquad c \equiv -dzx^{-1} \pmod{p},$$

čímž bude díky $xw - yz \equiv 0 \pmod{p}$ zaručeno

$$\begin{aligned} ax + bz &\equiv -bz + bz \equiv 0 \pmod{p}, \\ ay + bw &\equiv -byzx^{-1} + bw \equiv bx^{-1}(-yz + xw) \equiv 0 \pmod{p}, \\ cx + dz &\equiv -dz + dz \equiv 0 \pmod{p}, \\ cy + dw &\equiv -dyzx^{-1} + dw \equiv dx^{-1}(-yz + xw) \equiv 0 \pmod{p}. \end{aligned}$$

Přitom ale ve zvolení obou b, d máme vždy p možností, čímž už musí být $|M_\tau| = p^2$.

Pro $\theta_1, \theta_2 \in H_p$ zřejmě nastane $\theta_1\tau \equiv \theta_2\tau \pmod{p}$ právě tehdy, pokud

$$(\theta_1 - \theta_2)\tau \equiv 0 \pmod{p},$$

neboli pokud $(\theta_1 - \theta_2) \in M_\tau$. To ale znamená, že vždy právě $|M_\tau| = p^2$ různých θ dává stejnou hodnotu výrazu $\theta\tau \pmod{p}$. Uvedený výraz tedy musí nabývat právě $\frac{|H_p|}{|M_\tau|} = p^2$ různých hodnot. Přitom ale právě jedna z těchto hodnot je 0. Počet nenulových hodnot zkoumaného výrazu je tak $p^2 - 1$. Tímto je důkaz lemmatu hotov. □

4.3 Jacobiho věta a její zobecnění

Definice 4.3.1. Budiž G prvorozložený silný kvaternionový obor. Množinu $\Theta \subset G$ nazvěme *levou* (resp. *pravou*) *jednotkovou třídou*, pokud pro každá $\theta_1, \theta_2 \in \Theta$ existuje jednotka $\varepsilon \in G$ splňující $\theta_2 = \varepsilon\theta_1$ (resp. $\theta_2 = \theta_1\varepsilon$) a zároveň pro každou jednotku ε je $\varepsilon\theta_1 \in \Theta$ (resp. $\theta_1\varepsilon \in \Theta$).

Úmluva. Díky vlastnostem jednotek jsou mnohé vlastnosti sdíleny všemi prvky levé (resp. pravé) jednotkové třídy. Pokud tomu tak je, přiřkněme tuto vlastnost i celé jednotkové třídě, konkrétně hovořme o její normě $N(\Theta)$ a říkejme, že je primitivní, jsou-li primitivní všechny její prvky.

Rozmysleme si, že pro $\theta \in G \setminus \{0\}$ (kde G stále značí prvorozložený silný kvaternionový obor) je zobrazení $\varepsilon \mapsto \varepsilon\theta$ (resp. $\varepsilon \mapsto \theta\varepsilon$) prosté, pročež nutně musí pro každou levou (resp. pravou) jednotkovou třídu $\Theta \subset G$ různou od $\{0\}$ být $|\Theta| = r_G(1)$.

Věta 4.3.2. *Budiž G prvorozložený silný kvaternionový obor takový, že $T^m \cdot G \subseteq H \subseteq G$ pro nějaké $m \in \mathbb{N}$. Potom pro prvočíslo $p \nmid T$ existuje právě $p + 1$ různých primitivních levých jednotkových tříd $\Lambda \subset G$ splňujících $N(\Lambda) = p$.*

Poznámka. Celým účelem podmínky $T^m \cdot G \subseteq H$ je umožnit takovou konstrukci q, jež v (4.7) zaručí $\gamma \in H$.

Důkaz. Uvažujme libovolné $\tau = x + y\alpha + z\beta + w\alpha\beta \in H_p \setminus \{0\}$, pro něž je $N(\tau) \equiv 0 \pmod{p}$. Sestrojíme zobrazení f, které každému takovému τ jistým způsobem přiřadí levou jednotkovou třídu $\Lambda \subset G$, pro kterou platí $N(\Lambda) = p$. Ukažme nejprve, že existuje $\rho \in H$ takové, že $\rho \equiv \tau \pmod{p}$ a zároveň $p \mid N(\rho)$, ale $p^2 \nmid N(\rho)$.

Užijme lemmatu 3.2.4. Abychom tímto lemmatem neměli zaručenu existenci vyhovujícího ρ, musely by býti derivace výrazu

$$N(\tau) = (x^2 + \mu xy + Ay^2) + \nu(yz - xw) + B(z^2 + \mu zw + Aw^2)$$

vzhledem ke všem čtyřem x, y, z, w násobky p. To však ale dle lemmatu 3.2.5 nastává pouze pro $x \equiv y \equiv z \equiv w \equiv 0 \pmod{p}$, neboli $\tau \equiv 0 \pmod{p}$, což neplatí. Vyhovující ρ tedy existuje.

Položme $G\tau + Gp = G\lambda$ pro nějaké $\lambda \in G$. Potom $\rho \in G\lambda$, neboť $\rho \equiv \tau \pmod p$ značí $(\rho - \tau) \in Hp \subseteq Gp$ (poslední plyne z $H \subseteq G$). Dále $p \in G\lambda$, z čehož $N(\lambda) \mid N(p) = p^2$, tudíž $N(\lambda) \in \{1, p, p^2\}$. Vzhledem k $\rho \in G\lambda$ obdobně $N(\lambda) \mid N(\rho)$, takže jistě $N(\lambda) \neq p^2$. Konečně větou 2.3.3 musí být $p \mid \mathrm{NSD}(p, N(\tau)) \mid N(\lambda)$, takže nemůže být ani $N(\lambda) = 1$, pročež $N(\lambda) = p$.

Jsme tedy schopni vyjádřit $\rho = \theta\lambda$ pro nějaké $\theta \in G$. Budiž $\Lambda \subset G$ levou jednotkovou třídou, jíž náleží λ. Pro libovolné $\varepsilon\lambda \in \Lambda$ (ε je jednotka) jsme schopni vyjádřit i $\rho = (\theta\overline{\varepsilon})(\varepsilon\lambda)$. Takto je už tedy každému τ jednoznačně přiřazena levá jednotková třída Λ, neboť je-li $G\lambda = G\tau + Gp = G\lambda'$, pak dle lemmatu 1.1.6 musí být $\lambda' = \varepsilon\lambda$ pro nějakou jednotku ε, což už ale znamená $\lambda' \in \Lambda$. Můžeme tak položit $f(\tau) = \Lambda$.

Tažme se nyní, kolika různým τ bude takto přiřazena tatáž jednotková třída Λ. Abychom toto zodpověděli, ukažme nejprve, že $f(\tau_1) = f(\tau_2)$, právě pokud $\tau_2 \equiv \gamma\tau_1 \pmod p$ pro nějaké $\gamma \in H_p$. Jeden směr implikace je zřejmý – pokud vskutku $\tau_2 \equiv \gamma\tau_1$, platí $\rho_1 \equiv \tau_1 \pmod p$, $p^2 \nmid N(\rho_1)$ a $\rho_1 = \theta\lambda$ pro ireducibilní kvaternion $\lambda \in G$ splňující $N(\lambda) = p$, pak už pro každé $\rho_2 \equiv \tau_2 \pmod p$ existuje $\delta \in H$ takové, že platí i

$$\begin{aligned}\rho_2 &\equiv \tau_2 \equiv \gamma\tau_1 \equiv \gamma\rho_1 \equiv \gamma\theta\lambda \pmod p,\\ \rho_2 &= \gamma\theta\lambda + \delta p = \gamma\theta\lambda + \delta\overline{\lambda}\lambda = (\gamma\theta + \delta\overline{\lambda})\lambda,\end{aligned}$$

čímž už jistě $H\tau_2 + Hp = H\lambda$ a tedy $f(\tau_2) = f(\tau_1) = \Lambda$ (kde Λ stále značí levou jednotkovou třídu, jíž náleží λ).

Naopak, pokud $f(\tau_1) = f(\tau_2) = \Lambda \ni \lambda$ a zavedeme ρ_1, ρ_2 vlastnostmi

$$\begin{aligned}&\rho_1 \equiv \tau_1 \pmod p, && \rho_2 \equiv \tau_2 \pmod p,\\ &p^2 \nmid N(\rho_1), && p^2 \nmid N(\rho_2),\end{aligned}$$

pak musí být

$$\rho_1 = \theta_1\lambda, \qquad \rho_2 = \theta_2\lambda$$

pro nějaké $\theta_1, \theta_2 \in G$. Vzetím norem pak jistě $p \nmid N(\theta_1), N(\theta_2)$. Z toho jistě existuje existuje mod p k $N(\theta_1)$ inverzní prvek $(N(\theta_1))^{-1}$. Zároveň je p nesoudělné s T, pročež musí existovat $q \in \mathbb{Z}$ splňující

$$q \equiv (N(\theta_1))^{-1} \pmod p \wedge T^m \mid q.$$

Lze tak položit

$$\gamma = \theta_2 q\overline{\theta_1}, \tag{4.7}$$

přičemž $T^m \mid q$ z podmínky lemmatu zaručuje $\gamma = q \cdot \left(\theta_2\overline{\theta_1}\right) \in H$. Potom už jistě

$$\gamma\tau_1 \equiv \gamma\rho_1 = \theta_2 q\overline{\theta_1} \cdot \theta_1\lambda = \theta_2 q N(\theta_1)\lambda = (qN(\theta_1))(\theta_2\lambda) = (qN(\theta_1))\rho_2 \equiv 1 \cdot \tau_2 \equiv \tau_2 \pmod p.$$

Zodpovězení předeslané otázky se tak zredukuje na zodpovězení, kolika různých nenulových hodnot pro dané $\tau \in H_p \setminus \{0\}$ splňující $N(\tau) \equiv 0 \pmod p$ nabývá výraz $\gamma\tau \pmod p$ pro $\gamma \in H_p$. Tento počet je však podle lemmatu 4.2.4 roven $p^2 - 1$.

Platí tedy, že právě $p^2 - 1$ různých hodnot uvažovaných τ dá stejné $f(\tau)$. Každá levá jednotková třída $\Lambda \subset G$ s $N(\Lambda) = p$ se přitom musí objevit jako některá z hodnot $f(\tau)$. To plyne z toho, že z podmínky lemmatu musí být $T^m\lambda \in H$ a zároveň uvážením normy $p \nmid T^m\lambda$, pročež je $T^m\lambda$ samo jednou z vyhovujících hodnot τ, zároveň ale zřejmě $f\left(T^m\lambda\right) = \Lambda$.

Tímto víme, že f je zobrazení z množiny všech vyhovujících τ do množiny všech vyhovujících Λ, jehož obrazem je celá tato množina. Zároveň se na jedno dané Λ zobrazí právě p^2-1 různých τ. Všech vyhovujících τ je ale podle lemmatu 4.2.3 právě $(p^2-1)(p+1)$, pročež musí všech vyhovujících Λ být právě

$$\frac{(p^2-1)(p+1)}{p^2-1} = p+1,$$

což jsme přesně chtěli dokázat. □

Nechť $\sigma(n)$ značí součet dělitelů přirozeného čísla n. Poznamenejme, že se jedná o multiplikativní funkci, tj. pro nesoudělná $a, b \in \mathbb{N}$ platí $\sigma(ab) = \sigma(a)\sigma(b)$. To plyne z toho, že pro nesoudělná a, b každá dvojice (c, d), kde $c \mid a, d \mid b$, jednoznačně určuje $e = cd$, jež dělí ab, a naopak $e \mid ab$ již jednoznačně určuje (c, d).

Počet (levých) jednotkových tříd v prvorozloženém silném kvaternionovém oboru $G \supseteq H$ s normou n je zřejmě roven $\frac{r_G(n)}{r_G(1)}$. Skrze větu 4.1.10 tak z věty 4.3.2 pro prvočíslo $p \nmid T$ a $t \in \mathbb{N}$ plyne

$$r_G\left(p^t\right) = r_G(1) \cdot \frac{\left(\frac{r_G(p)}{r_G(1)} - 1\right)^{t+1} - 1}{\frac{r_G(p)}{r_G(1)} - 2} = r_G(1) \cdot \frac{p^{t+1}-1}{p-1} = r_G(1) \sum_{s=0}^{t} p^s = r_G(1)\sigma(p^t).$$

S touto větou tedy pro úplné vyčíslení $r_G(n)$ pro libovolné $n \in \mathbb{N}$ stačí určit $r_G(1)$ a $r_G(p)$ pro prvočísla p, jež dělí T – těch je však jistě konečně mnoho. V případech, kdy $G = H$ a T je prvočíslo, svedeme dokázat $r_H(T) = r_H(1)$.

Lemma 4.3.3. *Budiž $\zeta = \nu - \mu\beta + 2\alpha\beta$. Potom platí $\zeta H = H\zeta$.*

Důkaz. Platí $N(\zeta) = T$ a $\overline{\zeta} = -\zeta$. Přímými výpočty dále máme

$$\begin{aligned}
\zeta \cdot 1 \cdot \zeta &= -\zeta\overline{\zeta} = -T,\\
\zeta\alpha\zeta &= (4AB - B\mu^2 - \nu^2)\alpha + (\mu\nu^2 + B\mu^3 - 4AB\mu) = T\alpha - T\mu,\\
\zeta\beta\zeta &= (4AB - B\mu^2 - \nu^2)\beta = T\beta,\\
\zeta\alpha\beta\zeta &= (4AB\mu - B\mu^3 - \mu\nu^2)\beta + (\nu^2 + B\mu^2 - 4AB)\alpha\beta = T\mu\beta - T\alpha\beta,
\end{aligned}$$

z čehož pro $\theta = x + y\alpha + z\beta + w\alpha\beta \in H$ plyne

$$\frac{\zeta\theta\zeta}{T} = (-x - y\mu) + y\alpha + (z + w\mu)\beta - w\alpha\beta \in H.$$

Zobrazení $\psi : H \to H$ dané předpisem $\psi(\theta) = \frac{\zeta\theta\zeta}{T}$ je přitom samo sobě inverzní, neboť

$$\psi(\psi(\theta)) = \frac{\zeta\frac{\zeta\theta\zeta}{T}\zeta}{T} = \frac{(-T)\theta(-T)}{T^2} = \theta.$$

To už značí, že ψ je bijekcí, neboli $\frac{\zeta H\zeta}{T} = H$, což už snadno upravíme na

$$\zeta H = \zeta H \cdot \frac{\zeta\overline{\zeta}}{T} = \frac{\zeta H\zeta}{T} \cdot (-\zeta) = (-H)\zeta = H\zeta.$$ □

Věta 4.3.4. *Budiž H daný vztahem* (3.3) *tak, že T je prvočíslo a H silný kvaternionový obor. Potom v H existuje právě jedna levá jednotková třída normy T.*

Důkaz. Budiž $\zeta = \nu - \mu\beta + 2\alpha\beta$ a pojmenujme Z levou jednotkovou třídu, jíž ζ náleží. Mějme libovolné $\pi \in H$ takové, že $N(\pi) = T$, a ukažme $\pi \in Z$. Pro spor předpokládejme $\pi \notin Z$.

Ukažme nejprve, že $\zeta\overline{\pi}$ je primitivní. Nechť pro spor není. Potom uvážením normy musí být $\zeta\overline{\pi} = \varepsilon T$ pro nějakou jednotku $\varepsilon \in H$. Z toho už

$$\begin{aligned}\zeta &= \zeta \cdot \frac{\overline{\pi}\pi}{T} = \frac{\varepsilon T \pi}{T} = \varepsilon\pi,\\ \pi &= \overline{\varepsilon}\zeta,\end{aligned}$$

neboli $\pi \in Z$, což je spor. Nadále tedy předpokládejme, že $\zeta\overline{\pi}$ je primitivní.

Dle lemmatu 4.3.3 je $\zeta H = H\zeta$, neboli existuje $\rho \in H$ takové, že $\zeta\overline{\pi} = \rho\zeta$. Toto lze upravit na

$$\begin{aligned}\zeta\overline{\pi}\pi &= \rho\zeta\pi,\\ T\zeta &= \rho\zeta\pi.\end{aligned}$$

Nyní tedy jistě $T \mid \rho\zeta\pi$, navíc $N(\zeta) = T$ je prvočíslo a $\rho\zeta = \zeta\overline{\pi}$ je primitivní, z čehož speciálně $T \nmid \rho\zeta$. Dle lemmatu 4.1.6 už tedy musí být $T \mid \zeta\pi$, neboli $\zeta\pi = \varepsilon T$ pro nějaké ε – uvážením normy pak musí ε býti jednotkou. Z této rovnosti ale již plyne

$$\begin{aligned}\zeta\pi &= T\varepsilon = \zeta(-\zeta)\varepsilon,\\ \pi &= -\zeta\varepsilon.\end{aligned}$$

Konečně dle lemmatu 4.3.3 platí $\zeta(-\varepsilon) \in \zeta H = H\zeta$, neboli pro nějaké $\varphi \in H$ platí

$$\pi = -\zeta\varepsilon = \varphi\zeta,$$

přičemž uvážením normy musí být φ jednotkou, což už značí $\pi \in Z$. To je spor s předpokladem $\pi \notin Z$, pročež musí jedinou (levou i pravou) jednotkovou třídou normy T v oboru H být Z. □

V případech, kdy je T prvočíslo a H silný kvaternionový obor, je tímto stanovení $r_H(n)$ zredukováno na stanovení $r_H(1)$. Větou 4.1.10 pro nesoudělná $a, b \in \mathbb{N}$ platí

$$\frac{r_H(ab)}{r_H(1)} = \frac{r_H(a)}{r_H(1)} \cdot \frac{r_H(b)}{r_H(1)},$$

dále pro prvočíslo $p \neq T$ a $\ell \in \mathbb{N}$ je $\frac{r_H\left(p^\ell\right)}{r_H(1)} = \sigma\left(p^\ell\right)$ a konečně $\frac{r_H\left(T^\ell\right)}{r_H(1)} = 1$ (toto plyne z věty 4.3.4 větou 4.1.10). Toto dohromady pro

$$n = T^\ell \prod_{s=1}^{q} p_s^{t_s},$$

kde p_s jsou po dvou různá prvočísla různá od T, dává

$$\begin{aligned}r_H(n) = r_H(1) \cdot r_H\left(T^\ell\right) \cdot \prod_{s=1}^{q} r_H(\left(p_s^{t_s}\right)) = r_H(1) \prod_{s=1}^{q} \sigma\left(p_s^{t_s}\right) =\\ = r_H(1)\sigma\left(\prod_{s=1}^{q} p_s^{t_s}\right) = r_H(1)\sigma\left(\frac{n}{T^\ell}\right) = r_H(1) \sum_{T\nmid d\mid n} d. \qquad (4.8)\end{aligned}$$

Zbývá tedy stanovit $r_H(1)$. Toto lze učinit postupem vyloženým v sekci 3.4, pro některé obory H jsme tak již dokonce učinili.

Věta 4.3.5. *Budiž* $(A, B, \mu, \nu) = (1, 1, 1, 1)$. *Potom pro* $n \in \mathbb{N}$ *platí*

$$r_H(n) = 24 \sum_{2\nmid d \mid n} d.$$

Poznámka. $r_H(n)$ zde představuje počet celočíselných řešení rovnice

$$(x^2 + xy + y^2) + (yz - xw) + (z^2 + zw + w^2) = n.$$

Důkaz. Je $T = 2$, H je prvorozložený silný kvaternionový obor, a jak bylo ukázáno v důkazu lemmatu 3.4.13, platí $r_H(1) = 24$, čímž je hotovo. □

Věta 4.3.6 (Jacobiho o čtyřech čtvercích)**.** *Pro* $n \in \mathbb{N}$ *platí*

$$r_{\mathbb{J}}(n) = 24 \sum_{2\nmid d \mid n} d, \qquad r_{\mathbb{H}(\mathbb{Z})}(n) = 8 \sum_{4\nmid d \mid n} d.$$

Poznámka. Pro $n \in \mathbb{N}$ představuje $r_{\mathbb{H}(\mathbb{Z})}(n)$ počet celočíselných řešení rovnice

$$x^2 + y^2 + z^2 + w^2 = n.$$

Důkaz. Dle věty 3.4.2 je $\mathbb{J}$ izomorfní oboru (3.3) pro $(A, B, \mu, \nu) = (1, 1, 1, 1)$, z čehož už nutně

$$r_{\mathbb{J}}(n) = 24 \sum_{2 \mid d \mid n} d.$$

Dokažme nyní, že pro levou jednotkovou třídu $\Theta \subset \mathbb{J}$ platí

$$|\Theta \cap \mathbb{H}(\mathbb{Z})| = \begin{cases} 8, & \text{pokud } 2 \nmid N(\Theta), \\ 24, & \text{pokud } 2 \mid N(\Theta). \end{cases}$$

V důkazu lemmatu 2.2.3 jsme ukázali, že pro libovolnou levou jednotkovou třídu Θ je $|\Theta \cap \mathbb{H}(\mathbb{Z})| > 0$ – pro každé $\theta \in \mathbb{J} \setminus \mathbb{H}(\mathbb{Z})$ lze totiž zvolit $\gamma \in \mathbb{H}(\mathbb{Z})$, a jednotku $\delta \in \mathbb{J} \setminus \mathbb{H}(\mathbb{Z})$ takové, že $\theta - \delta = 2\gamma$ načež už

$$\lambda = \overline{\delta}\theta = \left(2\overline{\delta}\right)\gamma + 1 \in \mathbb{H}(\mathbb{Z})$$

a zároveň $\lambda = \overline{\delta}\theta$ náleží téže levé jednotkové třídě, jako θ.

Uvažujme levou jednotkovou třídu $\Theta \subset \mathbb{J}$ a $\theta \in \Theta \cap \mathbb{H}(\mathbb{Z})$. Pro jednotku $\varepsilon \in \mathbb{H}(\mathbb{Z})$ jistě $\varepsilon\theta \in \mathbb{H}(\mathbb{Z})$, zbývá tedy pro jednotku $\varepsilon \in \mathbb{J} \setminus \mathbb{H}(\mathbb{Z})$ dokázat, že $\varepsilon\theta \in \mathbb{H}(\mathbb{Z})$, právě pokud $2 \mid N(\Theta)$.

Budiž tedy $\theta = a + bi + cj + dk$ pro $a, b, c, d \in \mathbb{Z}$ a $\varepsilon = \frac{e+fi+gj+hk}{2}$ pro $e, f, g, h \in \{\pm 1\}$. Potom platí

$$\varepsilon\theta = \frac{e + fi + gj + hk}{2} \cdot (a + bi + cj + dk) = \frac{1}{2} \begin{pmatrix} (ea - fb - gc - hd) + \\ +i(eb + fa + gd - hc) + \\ +j(ec + ga + hb - df) + \\ +k(ed + ha + fc - gb) \end{pmatrix}.$$

Díky $e \equiv f \equiv g \equiv h \equiv 1 \equiv -1 \pmod 2$ a identitě $x^2 \equiv x \pmod 2$ platí

$$ea - fb - gc - hd \equiv eb + fa + gd - hc \equiv ec + ga + hb - df \equiv ed + ha + fc - gb \equiv$$
$$\equiv a + b + c + d \equiv a^2 + b^2 + c^2 + d^2 \equiv N(\theta) \pmod 2,$$

pročež jistě

$$\varepsilon\theta \in \mathbb{H}(\mathbb{Z}) \iff 2 \mid N(\theta) = N(\Theta).$$

Z toho již díky znalosti $r_{\mathbb{J}}(n)$ snadno plyne

$$r_{\mathbb{H}(\mathbb{Z})}(n) = \begin{cases} 8\sum_{2\nmid d\mid n} d, & \text{pokud } 2 \nmid n, \\ 24\sum_{2\nmid d\mid n} d, & \text{pokud } 2 \mid n, \end{cases}$$

což lze shrnout jako

$$r_{\mathbb{H}(\mathbb{Z})}(n) = 8\sum_{4\nmid d\mid n} d. \qquad \square$$

Věta 4.3.7. *Budiž $(A, B, \mu, \nu) = (1, 1, 1, 0)$. Potom pro $n \in \mathbb{N}$ platí*

$$r_H(n) = 12\sum_{3\nmid d\mid n} d.$$

Poznámka. $r_H(n)$ zde představuje počet celočíselných řešení rovnice

$$(x^2 + xy + y^2) + (z^2 + zw + w^2) = n.$$

Důkaz. Je $T = 3$, H je prvorozložený silný kvaternionový obor, a jak bylo ukázáno v důkazu lemmatu 3.4.12, platí $r_H(1) = 12$, čímž je hotovo. $\square$

Věta 4.3.8. *Budiž $(A, B, \mu, \nu) = (1, 2, 1, 1)$. Potom pro $n \in \mathbb{N}$ platí*

$$r_H(n) = 6\sum_{5\nmid d\mid n} d.$$

Poznámka. $r_H(n)$ zde představuje počet celočíselných řešení rovnice

$$(x^2 + xy + y^2) + (yz - xw) + 2(z^2 + zw + w^2) = n.$$

Důkaz. Je $T = 5$, H je prvorozložený silný kvaternionový obor, a jak bylo ukázáno v důkazu lemmatu 3.4.14, platí $r_H(1) = 6$, čímž je hotovo. $\square$

Věta 4.3.9. *Budiž $(A, B, \mu, \nu) = (2, 1, 1, 0)$. Potom pro $n \in \mathbb{N}$ platí*

$$r_H(n) = 4\sum_{7\nmid d\mid n} d.$$

Poznámka. $r_H(n)$ zde představuje počet celočíselných řešení rovnice

$$(x^2 + xy + 2y^2) + (z^2 + zw + 2w^2) = n.$$

Důkaz. Platí $T = 7$ a z věty 3.3.7 je H prvorozložený silný kvaternionový obor. Jednotkami v H jsou právě

$$\pm 1, \qquad \pm \beta,$$

z čehož $r_H(1) = 4$, čímž je důkaz hotov. $\square$

Pro co největší zestručnění důkazů několika dalších vět formulujme následující poněkud obecné lemma. V jeho důkazu využijeme tento vztah: pro prvočíslo p a přirozené číslo t platí

$$p\sigma\left(p^{t-1}\right)+\sigma\left(p^{t}\right)=p\sum_{s=0}^{t-1}p^{s}+\sum_{s=0}^{t}p^{s}=2\left(\sum_{s=0}^{t}p^{s}\right)-1=2\sigma(p^{t})-1. \tag{4.9}$$

Lemma 4.3.10. *Budiž G prvorozložený silný kvaternionový obor splňující $H\subset G\subset\mathbb{H}(\mathbb{R})$ a pro $n\in\mathbb{N}$ také*

$$r_G(n)=c\sum_{q\nmid d|n}d$$

pro nějaké $c\in\mathbb{N}$ a prvočíslo q. Potom pokud pro nějaké $\lambda\in H, N(\lambda)=p$, kde $p\neq q$ je prvočíslo splňující $(p+1)\mid c$, pro každou nenulovou levou jednotkovou třídu $\Theta\subset G$ platí

$$|\Theta\cap H|=\begin{cases} c, & \text{pokud } \Theta=\Theta_0\lambda \text{ pro nějakou levou jednotkovou třídu } \Theta_0\subset G,\\ \frac{c}{p+1}, & \text{jinak,}\end{cases}$$

pak už nutně

$$r_H(n)=\frac{2c}{p+1}\sum_{q\nmid d|n}d-\frac{c}{p+1}\sum_{p,q\nmid d|n}d.$$

Důkaz. Platí $N(\lambda)=p$, pročež určitě $|\Theta\cap H|=\frac{c}{p+1}$, není-li $N(\Theta)=n$ násobkem p, čímž

$$r_H(n)=\frac{1}{p+1}r_G(n)=\frac{c}{p+1}\sum_{q\nmid d|n}d.$$

Pro $p\mid N(\theta)=n$ pak z $\frac{r_G(n)}{r_G(1)}=\sum_{q\nmid d|n}d$ levých jednotkových tříd Θ normy n v G je právě $\frac{r_G\left(\frac{n}{p}\right)}{r_G(1)}$ obsaženo v H, čímž pro

$$n=q^{t_0}p^{t_1}\prod_{s=2}^{q}p_s^{t_s},$$

kde p_s jsou po dvou různá prvočísla různá od q i p a $t_1>0$, s využitím (4.9) plyne

$$\begin{aligned}r_H(n)&=r_G\left(\frac{n}{p}\right)+\frac{1}{p+1}\left(r_G(n)-r_G\left(\frac{n}{p}\right)\right)=\frac{r_G(1)}{p+1}\left(p\sigma\left(\frac{n}{p\cdot q^{t_0}}\right)+\sigma\left(\frac{n}{q^{t_0}}\right)\right)=\\&=\frac{r_G(1)}{p+1}\sigma\left(\frac{n}{q^{t_0}p^{t_1}}\right)\left(p\sigma\left(p^{t_1-1}\right)+\sigma\left(p^{t_1}\right)\right)=\frac{r_G(1)}{p+1}\sigma\left(\frac{n}{q^{t_0}p^{t_1}}\right)\left(2\sigma\left(p^{t_1}\right)-1\right)=\\&=\frac{2c}{p+1}\sigma\left(\frac{n}{q^{t_0}}\right)-\frac{c}{p+1}\sigma\left(\frac{n}{q^{t_0}p^{t_1}}\right)=\frac{2c}{p+1}\sum_{q\nmid d|n}d-\frac{c}{p+1}\sum_{p,q\nmid d|n}d.\end{aligned}$$

Poslední rovnost ale platí i pro $p\nmid n$, neboť potom jednoduše

$$\sum_{q\nmid d|n}d=\sum_{p,q\nmid d|n}d.$$

Tímto je důkaz lemmatu hotov. □

Věta 4.3.11. *Budiž* $(A, B, \mu, \nu) = (2, 1, 1, 1)$ *a zaveďme*

$$G = \left\{ \frac{x + z\beta + y\alpha + w\alpha\beta}{2} : x, y, z, w \in \mathbb{Z} \wedge x \equiv y \equiv z \equiv w \pmod 2 \right\}.$$

Potom pro $n \in \mathbb{N}$ *platí*

$$r_G(n) = 12 \sum_{3 \nmid d \mid n} d, \qquad r_H(n) = 8 \sum_{3 \nmid d \mid n} d - 4 \sum_{2,3 \nmid d \mid n} d.$$

Poznámka. $r_H(n)$ zde představuje počet celočíselných řešení rovnice

$$(x^2 + xy + 2y^2) + (yz - xw) + (z^2 + zw + 2w^2) = n.$$

Důkaz. Dle věty 3.4.3 existuje izomorfizmus, který zachovává normu, z G do oboru (3.3) pro $(A, B, \mu, \nu) = (1, 1, 1, 0)$, z čehož větou 4.3.7 plyne

$$r_G(n) = 12 \sum_{3 \nmid d \mid n} d.$$

Budiž Θ levá jednotková třída v G. Dle lemmatu 3.4.12 je množina $\Theta \cap H$ neprázdná, mějme tedy $\theta \in \Theta \cap H$. Budiž U množinou jednotek oboru G – potom $|U| = r_G(1) = 12$ a $U \cap H = \{\pm 1, \pm\beta\}$. Budiž $\theta = x + y\alpha + z\beta + w\alpha\beta$. Libovolná jednotka $\varepsilon \in U \setminus H$ je tvaru $\frac{a+b\alpha+c\beta+d\alpha\beta}{2}$ pro nějaká lichá $a, b, c, d \in \mathbb{Z}$. Z toho

$$\begin{aligned}(2\varepsilon) \cdot \theta &= (a + b\alpha + c\beta + d\alpha\beta)(x + y\alpha + z\beta + w\alpha\beta) \equiv \\ &\equiv (1 + \alpha + \beta + \alpha\beta)(x + y\alpha + z\beta + w\alpha\beta) \equiv \\ &\equiv (x + y + z + w)(1 + \alpha + \beta + \alpha\beta) \pmod 2,\end{aligned}$$

pročež $\varepsilon\theta = \frac{1}{2}(2\varepsilon)\theta \in H$, právě pokud $2 \mid (x + y + z + w)$. Toto lze formulovat jako

$$|\Theta \cap H| = \begin{cases} 4, & \text{pokud } 2 \nmid (x + y + z + w), \\ 12, & \text{pokud } 2 \mid (x + y + z + w). \end{cases}$$

Ukažme dále, že

$$\{\theta : \theta \in H \wedge 2 \mid (x + y + z + w)\} = G(\alpha - 1).$$

Platí $\theta \in G(\alpha - 1)$, právě pokud $\frac{\theta\overline{(\alpha-1)}}{N(\alpha-1)} = \frac{-\theta\alpha}{2} \in G$. Přitom ale

$$\begin{aligned}-\theta\alpha &= -x\alpha - y(\alpha - 2) - z(-1 - \alpha\beta + \beta) - w(-\alpha + 2\beta) \equiv \\ &\equiv z + (x + y + w)\alpha + z\beta + z\alpha\beta \pmod 2\end{aligned}$$

a $z \equiv x + y + w \pmod 2$ je ekvivalentní $2 \mid (x + y + z + w)$. Dohromady tedy musí platit

$$|\Theta \cap H| = \begin{cases} 12, & \text{pokud } \Theta = \Theta_0(\alpha - 1) \text{ pro nějakou levou jednotkovou třídu } \Theta_0 \subset G, \\ 4, & \text{jinak.} \end{cases}$$

Tímto jsou pro $c = 12$, $q = 3$, $p = 2$, $\lambda = \alpha - 1$ naplněny podmínky lemmatu 4.3.10, pročež už

$$r_H(n) = 8 \sum_{3 \nmid d \mid n} d - 4 \sum_{2,3 \nmid d \mid n} d. \qquad \square$$

Věta 4.3.12. *Budiž* $(A, B, \mu, \nu) = (1, 2, 1, 0)$ *a zaveďme*

$$G = \left\{ \frac{x + z\beta + y\alpha + w\alpha\beta}{3} : x, y, z, w \in \mathbb{Z} \wedge x \equiv y \equiv z \equiv w \pmod 3 \right\}.$$

Potom pro $n \in \mathbb{N}$ *platí*

$$r_G(n) = 24 \sum_{2\nmid d \mid n} d, \qquad r_H(n) = 12 \sum_{2\nmid d \mid n} d - 6 \sum_{2,3\nmid d \mid n} d.$$

Poznámka. $r_H(n)$ zde představuje počet celočíselných řešení rovnice

$$(x^2 + xy + y^2) + 2(z^2 + zw + w^2) = n.$$

Důkaz. Dle věty 3.4.4 existuje izomorfizmus, který zachovává normu, z G do oboru (3.3) pro $(A, B, \mu, \nu) = (1, 1, 1, 1)$, z čehož větou 4.3.5 plyne

$$r_G(n) = 24 \sum_{2\nmid d \mid n} d.$$

Budiž Θ levá jednotková třída v G. Dle lemmatu 3.4.13 je množina $\Theta \cap H$ neprázdná, mějme tedy $\theta \in \Theta \cap H$. Budiž U množinou jednotek oboru G – potom $|U| = r_G(1) = 24$ a $U \cap H = \{\pm 1, \pm\alpha, \pm(1-\alpha)\}$. Budiž $\theta = x + y\alpha + z\beta + w\alpha\beta$. Libovolná jednotka $\varepsilon \in U \setminus H$ je tvaru $\frac{a+b\alpha+c\beta+d\alpha\beta}{3}$ pro nějaká $a, b, c, d \in \mathbb{Z}$ splňující $a \equiv b \equiv c \equiv d \equiv m$, kde $m \in \{\pm 1\}$. Z toho

$$\begin{aligned}(3\varepsilon) \cdot \theta &= (a + b\alpha + c\beta + d\alpha\beta)(x + y\alpha + z\beta + w\alpha\beta) \equiv \\ &\equiv m(1 + \alpha + \beta + \alpha\beta)(x + y\alpha + z\beta + w\alpha\beta) \equiv \\ &\equiv m(x - y + z - w)(1 + \alpha + \beta + \alpha\beta) \pmod 3,\end{aligned}$$

pročež $\varepsilon\theta = \frac{1}{3}(3\varepsilon)\theta \in H$, právě pokud $3 \mid m(x-y+z-w)$, tj. právě pokud $3 \mid (x-y+z-w)$. Toto lze formulovat jako

$$|\Theta \cap H| = \begin{cases} 6, & \text{pokud } 3 \nmid (x - y + z - w), \\ 24, & \text{pokud } 3 \mid (x - y + z - w). \end{cases}$$

Ukažme dále, že

$$\{\theta : \theta \in H \wedge 3 \mid (x - y + z - w)\} = G(2 - \alpha).$$

Platí $\theta \in G(2-\alpha)$, právě pokud $\frac{\theta\overline{(2-\alpha)}}{N(2-\alpha)} = \frac{\theta(\alpha+1)}{3} \in G$. Přitom ale

$$\begin{aligned}\theta(\alpha + 1) &= (x - y) + (x + 2y)\alpha + (2z + w)\beta + (-z + w)\alpha\beta \equiv \\ &\equiv (x - y) + (x - y)\alpha + (w - z)\beta + (w - z)\alpha\beta \pmod 3\end{aligned}$$

a $x - y \equiv w - z \pmod 3$ je ekvivalentní $3 \mid (x - y + z - w)$. Dohromady tedy musí platit

$$|\Theta \cap H| = \begin{cases} 24, & \text{pokud } \Theta = \Theta_0(2 - \alpha) \text{ pro nějakou levou jednotkovou třídu } \Theta_0 \subset G, \\ 6, & \text{jinak.} \end{cases}$$

Tímto jsou pro $c = 24$, $q = 2$, $p = 3$, $\lambda = 2 - \alpha$ naplněny podmínky lemmatu 4.3.10, pročež už

$$r_H(n) = 12 \sum_{2\nmid d \mid n} d - 6 \sum_{2,3\nmid d \mid n} d. \qquad \square$$

Věta 4.3.13. *Budiž* $(A, B, \mu, \nu) = (2, 2, 1, 2)$ *a zaveďme*

$$G = \left\{ x + y\alpha + z\beta + \frac{w\alpha\beta}{2} : x, y, z, w \in \mathbb{Z} \right\}.$$

Potom pro $n \in \mathbb{N}$ *platí*

$$r_G(n) = 6 \sum_{5 \nmid d \mid n} d, \qquad r_H(n) = 4 \sum_{5 \nmid d \mid n} d - 2 \sum_{2,5 \nmid d \mid n} d.$$

Poznámka. $r_H(n)$ zde představuje počet celočíselných řešení rovnice

$$(x^2 + xy + 2y^2) + 2(yz - xw) + 2(z^2 + zw + 2w^2) = n.$$

Důkaz. Dle věty 3.4.5 existuje izomorfizmus, který zachovává normu, z G do oboru (3.3) pro $(A, B, \mu, \nu) = (1, 2, 1, 1)$, z čehož větou 4.3.8 plyne

$$r_G(n) = 6 \sum_{5 \nmid d \mid n} d.$$

Budiž Θ levá jednotková třída v G. Dle lemmatu 3.4.14 je množina $\Theta \cap H$ neprázdná, mějme tedy $\theta \in \Theta \cap H$. Budiž U množinou jednotek oboru G – potom $|U| = r_G(1) = 6$ a $U \cap H = \{\pm 1\}$. Budiž $\theta = x + y\alpha + z\beta + w\alpha\beta$. Libovolná jednotka $\varepsilon \in U \setminus H$ je tvaru $a + b\alpha + c\beta + d\frac{\alpha\beta}{2}$ pro nějaká $a, b, c, d \in \mathbb{Z}$ splňující $2 \nmid d$. Z toho

$$\begin{aligned}(2\varepsilon) \cdot \theta &= (2a + 2b\alpha + 2c\beta + d\alpha\beta)(x + y\alpha + z\beta + w\alpha\beta) \equiv \\ &\equiv \alpha\beta(x + y\alpha + z\beta + w\alpha\beta) \equiv \\ &\equiv -4w - 2(y + z)\alpha + 2y\beta + (x - 2w)\alpha\beta \equiv x\alpha\beta \pmod 2,\end{aligned}$$

pročež $\varepsilon\theta = \frac{1}{2}(2\varepsilon)\theta \in H$, právě pokud $2 \mid x$. Toto lze formulovat jako

$$|\Theta \cap H| = \begin{cases} 2, & \text{pokud } 2 \nmid x, \\ 6, & \text{pokud } 2 \mid x. \end{cases}$$

Ukažme dále, že

$$\{\theta : \theta \in H \wedge 2 \mid x\} = G\alpha.$$

Platí $\theta \in G\alpha$, právě pokud $\frac{\theta\overline{\alpha}}{N(\alpha)} = \frac{\theta(1-\alpha)}{2} \in G$. Přitom ale

$$\begin{aligned}\theta(1 - \alpha) &= (x + 2y + 2z) + (2w - x)\alpha - 2w\beta + (-z + w)\alpha\beta \equiv \\ &\equiv x + x\alpha + x\beta + (w + z)\alpha\beta \pmod 2\end{aligned}$$

a $\frac{\theta(1-\alpha)}{2} \in G$, právě pokud jsou v předchozí rovnosti koeficienty při $1, \alpha, \beta$ násobky dvou, tj. právě pokud $2 \mid x$. Dohromady tedy musí platit

$$|\Theta \cap H| = \begin{cases} 6, & \text{pokud } \Theta = \Theta_0\alpha \text{ pro nějakou levou jednotkovou třídu } \Theta_0 \subset G, \\ 2, & \text{jinak.} \end{cases}$$

Tímto jsou pro $c = 6$, $q = 5$, $p = 2$, $\lambda = \alpha$ naplněny podmínky lemmatu 4.3.10, pročež už

$$r_H(n) = 4 \sum_{5 \nmid d \mid n} d - 2 \sum_{2,5 \nmid d \mid n} d. \qquad \square$$

Věta 4.3.14. *Budiž* $(A, B, \mu, \nu) = (3, 1, 1, 1)$ *a zaveďme*

$$G = \left\{ \frac{x + y\alpha + z\beta + w\alpha\beta}{5} : x, y, z, w \in \mathbb{Z} \wedge 2x \equiv y \equiv z \equiv -2w \pmod 5 \right\}.$$

Potom pro $n \in \mathbb{N}$ *platí*

$$r_G(n) = 24 \sum_{2 \nmid d \mid n} d, \qquad r_H(n) = 8 \sum_{2 \nmid d \mid n} d - 4 \sum_{2,5 \nmid d \mid n} d.$$

Poznámka. $r_H(n)$ zde představuje počet celočíselných řešení rovnice

$$(x^2 + xy + 3y^2) + (yz - xw) + (z^2 + zw + 3w^2) = n.$$

Důkaz. Dle věty 3.4.6 existuje izomorfizmus, který zachovává normu, z G do oboru (3.3) pro $(A, B, \mu, \nu) = (1, 1, 1, 1)$, z čehož větou 4.3.5 plyne

$$r_G(n) = 24 \sum_{2 \nmid d \mid n} d.$$

Budiž Θ levá jednotková třída v G. Dle lemmatu 3.4.15 je množina $\Theta \cap H$ neprázdná, mějme tedy $\theta \in \Theta \cap H$. Budiž U množinou jednotek oboru G – potom $|U| = r_G(1) = 24$ a $U \cap H = \{\pm 1, \pm\beta\}$. Budiž $\theta = x + y\alpha + z\beta + w\alpha\beta$. Libovolná jednotka $\varepsilon \in U \setminus H$ je tvaru $\frac{a+b\alpha+c\beta+d\alpha\beta}{5}$ pro nějaká $a, b, c, d \in \mathbb{Z}$ splňující $2a \equiv b \equiv c \equiv -2d \equiv 2m \pmod 5$ pro nějaké $m \in \{1, 2, 3, 4\}$. Z toho

$$\begin{aligned}(5\varepsilon) \cdot \theta &= (a + b\alpha + c\beta + d\alpha\beta)(x + y\alpha + z\beta + w\alpha\beta) \equiv \\ &\equiv m(1 + 2\alpha + 2\beta - \alpha\beta)(x + y\alpha + z\beta + w\alpha\beta) \equiv \\ &\equiv m(x + 2y - 2z + w)(1 + 2\alpha + 2\beta - \alpha\beta) \pmod 5,\end{aligned}$$

pročež $\varepsilon\theta = \frac{1}{5}(5\varepsilon)\theta \in H$, právě pokud $5 \mid (x + 2y - 2z + w)$. Toto lze formulovat jako

$$|\Theta \cap H| = \begin{cases} 4, & \text{pokud } 5 \nmid (x + 2y - 2z + w), \\ 24, & \text{pokud } 5 \mid (x + 2y - 2z + w). \end{cases}$$

Ukažme dále, že

$$\{\theta : \theta \in H \wedge 5 \nmid (x + 2y - 2z + w)\} = G(1 - 2\beta).$$

Platí $\theta \in G(1 - 2\beta)$, právě pokud $\frac{\theta\overline{(1-2\beta)}}{N(1-2\beta)} = \frac{\theta(1+2\beta)}{5} \in G$. Přitom ale

$$\theta(1 + 2\beta) = (x - 2z) + (y - 2w)\alpha + (2x + z)\beta + (w + 2y)\alpha\beta,$$

a tedy $\frac{\theta(1+2\beta)}{2} \in G$, právě pokud

$$2(x - 2z) \equiv y - 2w \equiv 2x + z \equiv -2(w + 2y) \pmod 5. \tag{4.10}$$

Poslední kongruence jsou ale mod 5 po řadě ekvivalentní

$$\begin{aligned} 2x - y - 4z + 2w &\equiv 0, & y - 2w - 2x - z &\equiv 0, & 2x + 4y + z + 2w &\equiv 0, \\ x + 2y - 2z + w &\equiv 0, & x + 2y - 2z + w &\equiv 0, & x + 2y - 2z + w &\equiv 0, \end{aligned}$$

neboli platí (4.10), právě pokud $5 \mid (x + 2y - 2z + w)$. Dohromady tedy musí platit

$$|\Theta \cap H| = \begin{cases} 24, & \text{pokud } \Theta = \Theta_0(1 - 2\beta) \text{ pro nějakou levou jednotkovou třídu } \Theta_0 \subset G, \\ 4, & \text{jinak.} \end{cases}$$

Tímto jsou pro $c = 24$, $q = 2$, $p = 5$, $\lambda = 1 - 2\beta$ naplněny podmínky lemmatu 4.3.10, pročež už

$$r_H(n) = 8 \sum_{2\nmid d \mid n} d - 4 \sum_{2,5\nmid d \mid n} d. \qquad \square$$

Věta 4.3.15. *Budiž* $(A, B, \mu, \nu) = (3, 2, 1, 0)$ *a zaveďme*

$$G = \left\{ \frac{x + y\alpha + z\beta + w\alpha\beta}{11} : x, y, z, w \in \mathbb{Z} \wedge 3x \equiv 4y \equiv -2z \equiv w \pmod{11} \right\}.$$

Potom pro $n \in \mathbb{N}$ *platí*

$$r_G(n) = 24 \sum_{2\nmid d \mid n} d, \qquad r_H(n) = 4 \sum_{2\nmid d \mid n} d - 2 \sum_{2,11\nmid d \mid n} d.$$

Poznámka. $r_H(n)$ zde představuje počet celočíselných řešení rovnice

$$(x^2 + xy + 3y^2) + 2(z^2 + zw + 3w^2) = n.$$

Důkaz. Dle věty 3.4.10 existuje izomorfizmus, který zachovává normu, z G do oboru (3.3) pro $(A, B, \mu, \nu) = (1, 1, 1, 1)$, z čehož větou 4.3.5 plyne

$$r_G(n) = 24 \sum_{2\nmid d \mid n} d.$$

Budiž Θ levá jednotková třída v G. Dle lemmatu 3.4.16 je množina $\Theta \cap H$ neprázdná, mějme tedy $\theta \in \Theta \cap H$. Budiž U množinou jednotek oboru G – potom $|U| = r_G(1) = 24$ a $U \cap H = \{\pm 1\}$. Budiž $\theta = x + y\alpha + z\beta + w\alpha\beta$. Libovolná jednotka $\varepsilon \in U \setminus H$ je tvaru $\frac{a+b\alpha+c\beta+d\alpha\beta}{11}$ pro nějaká $a, b, c, d \in \mathbb{Z}$ splňující $3a \equiv 4b \equiv -2c \equiv d \equiv m \pmod{11}$ pro nějaké $m \in \{1, \ldots, 10\}$. Z toho

$$\begin{aligned} (11\varepsilon) \cdot \theta &= (a + b\alpha + c\beta + d\alpha\beta)(x + y\alpha + z\beta + w\alpha\beta) \equiv \\ &\equiv m(4 + 3\alpha - 6\beta + \alpha\beta)(x + y\alpha + z\beta + w\alpha\beta) \equiv \\ &\equiv m(x - 5y + 3z - 4w)(4 + 3\alpha - 6\beta + \alpha\beta) \pmod{11}, \end{aligned}$$

pročež $\varepsilon\theta = \frac{1}{11}(11\varepsilon)\theta \in H$, právě pokud $11 \mid (x - 5y + 3z - 4w)$. Toto lze formulovat jako

$$|\Theta \cap H| = \begin{cases} 2, & \text{pokud } 11 \nmid (x - 5y + 3z - 4w), \\ 24, & \text{pokud } 11 \mid (x - 5y + 3z - 4w). \end{cases}$$

Ukažme dále, že

$$\{\theta : \theta \in H \wedge 11 \mid (x - 5y + 3z - 4w)\} = G(3 - \beta).$$

Platí $\theta \in G(3 - \beta)$, právě pokud $\frac{\theta\overline{(3-\beta)}}{N(3-\beta)} = \frac{\theta(3+\beta)}{11} \in G$. Přitom ale

$$\theta(3 + \beta) = (3x - 2z) + (3y - 2w)\alpha + (3z + x)\beta + (3w + y)\alpha\beta,$$

a tedy $\frac{\theta(3+\beta)}{11} \in G$, právě pokud

$$3(3x-2z) \equiv 4(3y-2w) \equiv -2(3z+x) \equiv 3w+y \pmod{11}. \tag{4.11}$$

Poslední kongruence jsou ale mod 11 po řadě ekvivalentní

$$\begin{aligned} 9x-12y-6z+8w \equiv 0, \quad & 2x+12y+6z-8w \equiv 0, \quad & -2x-y-6z-3w \equiv 0, \\ x-5y+3z-4w \equiv 0, \quad & x-5y+3z-4w \equiv 0, \quad & x-5y+3z-4w \equiv 0, \end{aligned}$$

neboli platí (4.11), právě pokud $11 \mid (x-5y+3z-4w)$. Dohromady tedy musí platit

$$|\Theta \cap H| = \begin{cases} 24, & \text{pokud } \Theta = \Theta_0(3-\beta) \text{ pro nějakou levou jednotkovou třídu } \Theta_0 \subset G, \\ 2, & \text{jinak.} \end{cases}$$

Tímto jsou pro $c = 24$, $q = 2$, $p = 11$, $\lambda = 3-\beta$ naplněny podmínky lemmatu 4.3.10, pročež už

$$r_H(n) = 4 \sum_{2 \nmid d \mid n} d - 2 \sum_{2,11 \nmid d \mid n} d. \qquad \square$$

4.4 Odvození vzorce pro π

V této sekci (a pouze v této sekci) nechť π značí to reálné číslo, jež je poměrem obvodu a průměru libovolné kružnice. Na závěr kapitoly odvodíme pomocí Jacobiho věty o čtyřech čtvercích vyjádření π pomocí nekonečné řady vzorcem

$$\frac{\pi^2}{6} = \sum_{s=1}^{\infty} \frac{2s+1}{s(s+1)^2} = \sum_{s=1}^{\infty} \frac{1}{s^2}.$$

Z postupu, který využijeme, také vyplyne přímý vztah mezi T a $r_H(1)$ v případech, kdy T je prvočíslo a H silný kvaternionový obor.

Lemma 4.4.1. *Nechť $V_4(R)$ značí nadobjem čtyřrozměrné nadkoule o poloměru R. Potom $V_4(R) = \frac{\pi^2}{2} R^4$.*

Důkaz. Mějme nezáporné $r \leq R$ a $\varphi \in \langle 0, 2\pi)$. Potom je jistě průnikem nadkoule se středem v počátku a poloměrem R s rovinou danou rovnicemi

$$x = r\cos\varphi, \qquad\qquad y = r\sin\varphi$$

kruh s poloměrem $\sqrt{R^2-r^2}$, tj. s obsahem $\pi(R^2-r^2)$. Z toho již určitě

$$V_4(R) = \int_0^R 2\pi r \cdot \pi(R^2-r^2)\,\mathrm{d}r = 2\pi^2 \int_0^R r(R^2-r^2)\,\mathrm{d}r = 2\pi^2 \left(\frac{R^4}{2} - \frac{R^4}{4}\right) = \frac{\pi^2}{2} R^4. \ \square$$

Získejme vzorec pro výpočet π z následující úvahy: čím je $n \in \mathbb{N}$ větší, tím se nadobjem nadkoule o poloměru $\sqrt{n}$ bude blížit počtu mřížových bodů[7] $(a,b,c,d) \in \mathbb{Z}^4$ s $a^2+b^2+c^2+d^2 \leq n$. Formálněji, bude platit

$$\lim_{n\to\infty} \frac{|\{(a,b,c,d) : (a,b,c,d) \in \mathbb{Z}^4 \wedge 0 < a^2+b^2+c^2+d^2 \leq n\}|}{V_4(\sqrt{n})} = 1. \tag{4.12}$$

[7] Bez újmy na celkovém výsledku vyloučíme $(a,b,c,d) = (0,0,0,0)$.

Abychom toto zřeli, přiřaďme každé jednotkové nadkrychli s vrcholy v mřížových bodech ten její vrchol, jenž je nejvzdálenější bodu $(0,0,0,0)$. Potom je každý mřížový bod (a,b,c,d) splňující $0 \notin \{a,b,c,d\}$ takto přiřazen nějaké nadkrychli. Počet těch mřížových bodů, jež leží uvnitř nadkoule se středem v počátku a poloměrem R a splňují $0 \in \{a,b,c,d\}$, je přitom nanejvýš úměrný R^3 (jedná se o mřížové body ležící v průniku uvažované koule s těmi čtyřmi prostory, které jsou kolmé na jednotlivé osy nadprostoru a procházejí počátkem – každý z takových průniků je však jistě koulí o poloměru R). Podobně přesah této nadkoule mimo ten soubor jednotkových nadkrychlí s vrcholy v mřížových bodech, které jsou v nadkouli celé obsaženy, je nanejvýš úměrný „nadpovrchu“ této nadkoule, který je také úměrný R^3 (integrálním počtem lze odvodit, že je roven $2\pi^2 R^3$). Celkově je tedy rozdíl

$$V_4(R) - \left|\left\{(a,b,c,d) : (a,b,c,d) \in \mathbb{Z}^4 \wedge 0 < a^2+b^2+c^2+d^2 \leq R^2\right\}\right|$$

nanejvýš úměrný R^3. Přitom ale nadobjem $V_4(R)$ je úměrný R^4, pročež

$$\lim_{R\to\infty} \frac{V_4(R) - |\{(a,b,c,d) : (a,b,c,d) \in \mathbb{Z}^4 \wedge 0 < a^2+b^2+c^2+d^2 \leq R^2\}|}{V_4(R)} = 0,$$
$$\lim_{R\to\infty} \frac{|\{(a,b,c,d) : (a,b,c,d) \in \mathbb{Z}^4 \wedge 0 < a^2+b^2+c^2+d^2 \leq R^2\}|}{V_4(R)} = \lim_{R\to\infty} \frac{V_4(R)}{V_4(R)} = 1.$$

Tímto je platnost rovnice (4.12) osvětlena.

S pomocí věty 4.3.6 lze nyní upravit

$$\begin{aligned}
\frac{\pi^2}{2} &= \lim_{n\to\infty} \frac{1}{n^2} \sum_{x=1}^{n} r_{\mathbb{H}(\mathbb{Z})}(x), \\
\frac{\pi^2}{2} &= \lim_{n\to\infty} \frac{1}{n^2} \sum_{x=1}^{n} 8 \sum_{4\nmid d \mid x} d, \\
\frac{\pi^2}{16} &= \lim_{n\to\infty} \frac{1}{n^2} \sum_{x=1}^{n} \sum_{4\nmid d \mid x} d.
\end{aligned} \tag{4.13}$$

Dvojitá suma na pravé straně nyní udává součet z d přes všechny dvojice (x,d) splňující

$$1 \leq x \leq n \wedge 4 \nmid d \wedge d \mid x.$$

V tomto součtu je ale započítáno každé d splňující $4 \nmid d \wedge d \leq n$ právě tolikrát, kolik jeho násobků se nachází mezi čísly $1,\ldots,n$. Rovnice (4.13) se touto úvahou převede na

$$\frac{\pi^2}{16} = \lim_{n\to\infty} \frac{1}{n^2} \sum_{\substack{1\leq d\leq n \\ 4\nmid d}} d \cdot \left\lfloor \frac{n}{d} \right\rfloor. \tag{4.14}$$

Položme $n = 4m$ pro $m \in \mathbb{N}$. Potom se n bude zvětšovat nad libovolnou mez, právě pokud se bude nad libovolnou mez zvětšovat m – tedy $\lim_{n\to\infty}$ přejde v $\lim_{m\to\infty}$. Zaveďme funkci

$$F(z) = \sum_{d=1}^{z} d \left\lfloor \frac{z}{d} \right\rfloor.$$

Potom bude platit

$$\sum_{\substack{1\le d\le n\\ 4\nmid d}} d\left\lfloor\frac{n}{d}\right\rfloor = \sum_{d=1}^{4m} d\left\lfloor\frac{4m}{d}\right\rfloor - \sum_{\substack{1\le d\le 4m\\ 4\mid d}} d\left\lfloor\frac{4m}{d}\right\rfloor =$$

$$= F(4m) - \sum_{d=1}^{m} 4d\left\lfloor\frac{4m}{4d}\right\rfloor = F(4m) - 4F(m).$$

Rovnost (4.14) tak přejde ve tvar

$$\pi^2 = \lim_{m\to\infty} \frac{F(4m) - 4F(m)}{m^2}. \tag{4.15}$$

Lemma 4.4.2. *Nechť jsou $z, t \in \mathbb{N}$ taková, že $1, \ldots, t \mid z$, a zaveďme*

$$g(z,t) = \sum_{d=1}^{\frac{z}{t}} d\left\lfloor\frac{z}{d}\right\rfloor.$$

Potom platí

$$F(z) = g(z,t) + \frac{z}{2}\sum_{s=1}^{t-1} \frac{z(2s+1)+s(s+1)}{s(s+1)^2}.$$

Důkaz. Upravme

$$F(z) = \sum_{d=1}^{z} d\left\lfloor\frac{z}{d}\right\rfloor = \sum_{d=1}^{\frac{z}{t}} d\left\lfloor\frac{z}{d}\right\rfloor + \sum_{s=1}^{t-1}\sum_{d=\frac{z}{s+1}+1}^{\frac{z}{s}} d\left\lfloor\frac{z}{d}\right\rfloor.$$

Pro $s \in \{1, \ldots, t-1\}$ a $\frac{z}{s+1} < d \le \frac{z}{s}$ (z podmínek lemmatu jsou obě meze celá čísla) musí platit

$$\frac{1}{s+1} < \frac{d}{z} \le \frac{1}{s},$$
$$s+1 > \frac{z}{d} \ge s,$$

což už značí $\left\lfloor\frac{z}{d}\right\rfloor = s$. Z toho tedy máme

$$F(z) = g(z,t) + \sum_{s=1}^{t-1}\sum_{d=\frac{z}{s+1}+1}^{\frac{z}{s}} ds = g(z,t) + \sum_{s=1}^{t-1} s\cdot\frac{\left(\frac{z}{s}-\frac{z}{s+1}\right)\left(\frac{z}{s}+\frac{z}{s+1}+1\right)}{2} =$$

$$= g(z,t) + \frac{z}{2}\sum_{s=1}^{t-1}\frac{s}{s(s+1)}\cdot\frac{z(2s+1)+s(s+1)}{s(s+1)} =$$

$$= g(z,t) + \frac{z}{2}\sum_{s=1}^{t-1}\frac{z(2s+1)+s(s+1)}{s(s+1)^2}.$$

□

Lemma 4.4.3. *Pro libovolné $w \in \mathbb{N}$ platí*

$$\lim_{t\to\infty}\frac{g(wt!,t)}{(t!)^2} = 0. \tag{4.16}$$

Důkaz. Platí

$$g(wt!,t) = \sum_{d=1}^{w(t-1)!} d\left\lfloor \frac{wt!}{d} \right\rfloor \leq \sum_{d=1}^{w(t-1)!} d \cdot \frac{wt!}{d} = w(t-1)! \cdot wt!.$$

Z toho $\frac{g(wt!,t)}{(t!)^2} \leq \frac{w^2}{t}$, zároveň je ale zcela zřejmé $\frac{g(wt!,t)}{(t!)^2} \geq 0$ neboli

$$0 \leq \lim_{t\to\infty} \frac{g(wt!,t)}{(t!)^2} \leq \lim_{t\to\infty} \frac{w^2}{t} = 0,$$
$$\lim_{t\to\infty} \frac{g(wt!,t)}{(t!)^2} = 0. \qquad \square$$

V (4.15) položme $m = t!$. Potom m roste nad libovolnou mez, právě pokud nad libovolnou mez roste t (faktoriál je rostoucí funkce), neboli $\lim_{m\to\infty}$ přejde v $\lim_{t\to\infty}$. S využitím lemmat 4.4.2 a 4.4.3 pak získáme

$$\begin{aligned}
\pi^2 &= \lim_{t\to\infty} \frac{1}{(t!)^2} \left(g(4t!,t) + 2t! \sum_{s=1}^{t-1} \frac{4t!(2s+1) + s(s+1)}{s(s+1)^2} - \right. \\
&\qquad \left. - 4g(t!,t) - 2t! \sum_{s=1}^{t-1} \frac{t!(2s+1) + s(s+1)}{s(s+1)^2} \right), \\
\pi^2 &= \lim_{t\to\infty} \left(\frac{2}{t!} \sum_{s=1}^{t-1} \frac{(2s+1)(4t! - t!)}{s(s+1)^2} \right) + \lim_{t\to\infty} \left(\frac{g(4t!,t)}{(t!)^2} \right) - 4 \lim_{t\to\infty} \left(\frac{g(t!,t)}{(t!)^2} \right) = \\
&= \lim_{t\to\infty} 2 \sum_{s=1}^{t-1} \frac{3(2s+1)}{s(s+1)^2}, \\
\frac{\pi^2}{6} &= \sum_{s=1}^{\infty} \frac{2s+1}{s(s+1)^2}.
\end{aligned} \tag{4.17}$$

Stejný postup bychom mohli užít s jiným oborem než $\mathbb{H}(\mathbb{Z})$. Mějme obor H daný vztahem (3.3) tak, že T je prvočíslo a H silný kvaternionový obor. Položme

$$M = \left\{ (x,y,z,w) \in \mathbb{R}^4 : \left(x^2 + \mu xy + Ay^2\right) + \nu\,(yz - xw) + B\left(z^2 + \mu zw + Aw^2\right) \leq R^2 \right\}$$

a tažme se, jaký má M objem. Platí

$$\begin{aligned}
&(x^2 + \mu xy + Ay^2) + \nu(yz - xw) + B(z^2 + \mu zw + Aw^2) = \\
&= \left(x + y\frac{\mu}{2} - w\frac{\nu}{2}\right)^2 + \left(y\frac{\sqrt{S}}{2} + z\frac{\nu}{\sqrt{S}} + w\frac{\mu\nu}{2\sqrt{S}}\right)^2 + \frac{T}{S}\left(z + w\frac{\mu}{2}\right)^2 + \frac{T}{4}w^2.
\end{aligned}$$

Pojmenujeme-li tedy

$$L = \begin{pmatrix} 1 & \frac{\mu}{2} & 0 & -\frac{\nu}{2} \\ 0 & \frac{\sqrt{S}}{2} & \frac{\nu}{\sqrt{S}} & \frac{\mu\nu}{2\sqrt{S}} \\ 0 & 0 & \sqrt{\frac{T}{S}} & \frac{\mu}{2}\sqrt{\frac{T}{S}} \\ 0 & 0 & 0 & \frac{\sqrt{T}}{2} \end{pmatrix},$$

pak zobrazení $\varphi : M \to \mathbb{R}^4$ dané předpisem

$$\varphi((x,y,z,w)) = (X,Y,Z,W),$$
$$L \cdot \begin{pmatrix} x \\ y \\ z \\ w \end{pmatrix} = \begin{pmatrix} X \\ Y \\ Z \\ W \end{pmatrix}$$

bijektivně mapuje M na nadkouli se středem v počátku a poloměrem R. Potom tedy platí

$$\mathrm{Vol}(\mathrm{Im}\,\varphi) = |\det L| \cdot \mathrm{Vol}(M)$$

(viz sekci 1.2). Přitom ale $\det L = \frac{T}{4}$, pročež

$$\mathrm{Vol}(M) = \frac{\mathrm{Vol}\,(\mathrm{Im}\,\varphi)}{|\det L|} = \frac{\frac{\pi^2}{2}R^4}{\frac{T}{4}} = \frac{2\pi^2 R^4}{T}.$$

Zcela analogicky s postupem pro $\mathbb{H}(\mathbb{Z})$ tedy můžeme získat

$$\begin{aligned}
1 &= \lim_{n\to\infty} \frac{1}{\frac{2\pi^2 n^2}{T}} \sum_{x=1}^{n} r_H(x), \\
\frac{2\pi^2}{T} &= \lim_{n\to\infty} \frac{1}{n^2} \sum_{x=1}^{n} r_H(1) \sum_{T\nmid d \mid x} d, \\
\frac{2\pi^2}{T r_H(1)} &= \lim_{n\to\infty} \frac{1}{n^2} \sum_{\substack{1\le d\le n \\ T\nmid d}} d \cdot \left\lfloor \frac{n}{d} \right\rfloor, \\
\frac{2\pi^2}{T r_H(1)} &= \lim_{m\to\infty} \frac{1}{(Tm)^2} \sum_{\substack{1\le d\le Tm \\ T\nmid d}} d \cdot \left\lfloor \frac{Tm}{d} \right\rfloor, \qquad (n = Tm), \\
\frac{2T\pi^2}{r_H(1)} &= \lim_{m\to\infty} \frac{1}{m^2} \left(\sum_{d=1}^{Tm} d \left\lfloor \frac{Tm}{d} \right\rfloor - \sum_{d=1}^{m} Td \left\lfloor \frac{Tm}{Td} \right\rfloor \right), \\
\frac{2T\pi^2}{r_H(1)} &= \lim_{m\to\infty} \frac{F(Tm) - TF(m)}{m^2}, \\
\frac{2T\pi^2}{r_H(1)} &= \lim_{t\to\infty} \frac{1}{(t!)^2} \left(g(Tt!,t) + \frac{Tt!}{2} \sum_{s=1}^{t-1} \frac{Tt!(2s+1) + s(s+1)}{s(s+1)^2} - \right. \\
&\qquad \left. - Tg(t!,t) - T \cdot \frac{t!}{2} \sum_{s=1}^{t-1} \frac{t!(2s+1) + s(s+1)}{s(s+1)^2} \right), \qquad (m = t!), \\
\frac{2T\pi^2}{r_H(1)} &= \lim_{t\to\infty} \left(\frac{T}{2t!} \sum_{s=1}^{t-1} \frac{(T-1)t!(2s+1)}{s(s+1)^2} \right) + \lim_{t\to\infty} \left(\frac{g(Tt!,t)}{(t!)^2} \right) - T \lim_{t\to\infty} \left(\frac{g(t!,t)}{(t!)^2} \right), \\
\frac{2T\pi^2}{r_H(1)} &= \frac{T(T-1)}{2} \lim_{t\to\infty} \sum_{s=1}^{t-1} \frac{2s+1}{s(s+1)^2}, \\
\frac{4\pi^2}{(T-1)r_H(1)} &= \sum_{s=1}^{\infty} \frac{2s+1}{s(s+1)^2}.
\end{aligned}$$

Z toho už skrze (4.17) musí být

$$\frac{4\pi^2}{(T-1)r_H(1)} = \frac{\pi^2}{6},$$
$$(T-1)\cdot r_H(1) = 24. \tag{4.18}$$

Pokud je tedy H silný kvaternionový a T je prvočíslo, je již $r_H(n)$ jednoznačně určeno jako

$$\frac{24}{T-1}\sum_{T\nmid d\mid n} d.$$

Naopak lze z tohoto vyvodit, pro která T toto může nastat. Zřejmě musí $r_H(1)$ být sudé číslo, neboť $N(-\theta) = N(\theta)$ pro každé $\theta \in \mathbb{H}(\mathbb{R})$ a $\theta = -\theta$ platí pouze pro $\theta = 0$. To značí $2 \mid r_H(1) = \frac{24}{T-1}$, neboli $(T-1) \mid 12$, což dává jako možnosti

$$T \in \{2, 3, 5, 7, 13\}$$

(požadujeme, aby T bylo prvočíslem).

Závěrem kapitoly ukažme, že nekonečná řada na pravé straně (4.17) má stejný součet jako řada

$$\sum_{s=1}^{\infty} \frac{1}{s^2}.$$

K tomu nejprve dokažme známý teleskopický součet

$$\sum_{s=1}^{\infty} \frac{1}{s(s+1)} = \sum_{s=1}^{\infty}\left(\frac{1}{s} - \frac{1}{s+1}\right) = \lim_{t\to\infty}\sum_{s=1}^{t}\left(\frac{1}{s} - \frac{1}{s+1}\right) = \lim_{t\to\infty}\left(1 - \frac{1}{t+1}\right) = 1.$$

S jeho pomocí už snadno máme

$$\frac{\pi^2}{6} = \sum_{s=1}^{\infty}\frac{2s+1}{s(s+1)^2} = \sum_{s=1}^{\infty}\left(\frac{1}{s(s+1)} + \frac{1}{(s+1)^2}\right) = 1 + \sum_{s=1}^{\infty}\frac{1}{(s+1)^2} =$$
$$= \frac{1}{1^2} + \sum_{s=2}^{\infty}\frac{1}{s^2} = \sum_{s=1}^{\infty}\frac{1}{s^2}.$$

Závěr

Cíle vytyčeného v úvodu – zobecnění kvaternionového důkazu Lagrangeovy a Jacobiho věty o čtyřech čtvercích na další kvadratické formy – jsme úspěšně dosáhli. Získali a dokázali jsme výsledky analogické k Jacobiho větě pro devět kvadratických forem (viz tabulku 5) a navíc univerzalitu tří dalších forem, konkrétně

$$(x^2+xy+2y^2)+2(z^2+zw+2w^2),$$
$$(x^2+2y^2)+(yz-xw)+2(z^2+2w^2),$$
$$(x^2+xy+2y^2)+3(z^2+zw+2w^2).$$

Poznamenejme, že pro tyto formy s největší pravděpodobností neexistuje explicitní vzorec podobný Jacobiho větě, neboť hodnoty $r_H(n)$ se pro příslušné obory H chovají zdánlivě nahodile – kupříkladu pro $(A,B,\mu,\nu)=(2,3,1,0)$, tedy poslední z uvedených forem, dostáváme skrze numerické výpočty hrubou silou pro několik malých prvočíselných n hodnoty

$$\begin{aligned} r_H(2)&=4, & r_H(3)&=2, & r_H(5)&=8, & r_H(7)&=22,\\ r_H(11)&=20, & r_H(13)&=20, & r_H(17)&=24, & r_H(19)&=32,\\ r_H(23)&=36, & r_H(29)&=44, & r_H(31)&=48, & r_H(37)&=60. \end{aligned}$$

Metody užité v této práci by zajisté bylo možno užít i na další kvadratické formy. Zvláštní pozornost zasluhuje forma (3.1) pro $(A,B,\mu,\nu)=(3,2,1,3)$, což dává $T=13$. Vzpomeňme, že v sekci 4.4 jsme při zkoumání vztahu T a $r_H(1)$ v případech, kdy T je prvočíslo a H silný kvaternionový obor, stanovili $T=13$ jako jednu z hodnot, pro kterou by mohl H být silný kvaternionový. Stačilo by tedy v tomto případě pouze dokázat, že H je oborem hlavních ideálů, a okamžitě bychom skrze teorii vybudovanou v této práci obdrželi

$$r_H(n)=2\sum_{13\nmid d\mid n} d,$$

čemuž odpovídají i numerické výpočty pro malá n.

Zajímavým směrem dalšího zkoumání je též význam prvočíselného rozkladu T pro vlastnosti oboru H. Např. se zdá, že pro prvočíselná T existuje vždy až na izomorfizmus právě jeden obor H tvaru (3.3), zatímco při složeném T, pokud má H nějaký (prvorozložený) silný kvaternionový nadobor G, dochází k tomu, že je-li q nejmenší přirozené číslo s vlastností $qG\subseteq H$, pak platí $q\mid T$ a zároveň je G izomorfní nějakému oboru (3.3) s $T'=\frac{T}{q}$. Obecněji se pak lze tázat, zdali existují nějaké silné prvorozložené obory H se složeným T. To obory H, pro něž je T složené a pro které jsme dokázali analog Jacobiho věty, silné kvaternionové určitě nejsou. Pro každý z nich je totiž T součinem dvou různých prvočísel (tedy bezčtvercovým číslem) a navíc jsme dokázali

$$r_H(n)=2c\sum_{q\nmid d\mid n} d-c\sum_{p,q\nmid d\mid n} d$$

pro nějaké $c \in \mathbb{N}$ a různá prvočísla p, q. Platí tedy

$$r_H(p) = c(2p+1), \qquad r_H\left(p^2\right) = c(2p^2+2p+1),$$

ale pokud by byl H zároveň silný kvaternionový obor, pak by větou 4.1.10 plynulo

$$r_H\left(p^2\right) = c \cdot \frac{(2p)^3 - 1}{(2p+1)-2} = c \cdot \frac{8p^3-1}{2p-1} = c(4p^2+2p+1) > c(2p^2+2p+1),$$

což by značilo spor. Zodpovězení této otázky, bližší osvětlení vlastností (prvorozložených) silných kvaternionových $G \supset H$ či počtu různých H tvaru (3.3) pro dané T by tak bylo velmi zajímavým a hodnotným výsledkem.

Úplným závěrem pro úplnost zmiňme, že až na ekvivalenci existuje pouze konečný počet univerzálních (pozitivně definitních – tedy takových, které nabývají vždy pouze nezáporných hodnot a nuly pouze tehdy, jsou-li všechny argumenty rovny nule) kvadratických forem čtyř proměnných. Úplný výčet těchto forem byl stanoven a dokázán na začátku 21. století (viz [2] a [1]).

Úmluva. Řekněme, že kvadratická forma f v m proměnných *reprezentuje* přirozené n, pokud rovnice $f(x_1, \ldots, x_m) = n$ má celočíselné řešení.

Tvrzení (Věta 290)**.** *Pozitivně definitní kvadratická forma reprezentuje všechna přirozená čísla, právě pokud reprezentuje všech* 29 *čísel*

$$1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26,$$
$$29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290.$$

Tvrzení. *Až na ekvivalenci existuje právě* 6436 *univerzálních pozitivně definitních kvadratických forem ve čtyřech proměnných.*

Literatura

[1] Bhargava, Manjul. On the Conway-Schneeberger Fifteen theorem. *Contemporary Mathematics*. Vol. 272, 2000, p. 27-37. Dostupné z: http://www.fen.bilkent.edu.tr/~franz/mat/15.pdf

[2] Bhargava, Manjul a Hanke, Jonathan. Universal quadratic forms and the 290-Theorem. [online]. [cit. 2018-03-27]. Dostupné z: http://www.wordpress.jonhanke.com/wp-content/uploads/2011/09/290-Theorem-preprint.pdf

[3] Coan, Boyd a Perng, Cherng-tiao. Factorization of Hurwitz Quaternions. *International Mathematical Forum*. Vol. 7, 2012, no. 43, 2143-2156. Dostupné z: http://www.m-hikari.com/imf/imf-2012/41-44-2012/perngIMF41-44-2012.pdf

[4] Heath, Thomas Little. *Diophantus of Alexandria; a study in the history of Greek algebra*. 2nd ed. Cambridge: University Press, 1910. p. 188. Dostupné z: https://archive.org/details/diophantusofalex00heatiala/page/n6

[5] Hurwitz, Adolf. Ueber die Zahlentheorie der Quaternionen. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Matematisch-physikalische Klasse.* 1896. 4., s. 313-340. Dostupné z: https://eudml.org/doc/58369

[6] Perić, Veselin a Vuković, Mirjana. Some examples of principal ideal domain which are not Euclidean and some other counterexamples. *Novi Sad Journal of Mathematics*. Vol. 38, No. 1, 2008, 137-154. Dostupné z: http://www.dmi.uns.ac.rs/nsjom/Papers/38_1/NSJOM_38_1_137_154.pdf

[7] Weisstein, Eric W. Quaternion. *MathWorld – A Wolfram Web Resource*. [online]. [cit. 2018-03-27]. Dostupné z: http://mathworld.wolfram.com/Quaternion.html

[8] Weisstein, Eric W. Lagrange's Four-Square Theorem. *MathWorld – A Wolfram Web Resource*. [online]. [cit. 2018-03-27]. Dostupné z: http://mathworld.wolfram.com/LagrangesFour-SquareTheorem.html